

COMPARATIVE ANALYSIS OF NUCLEAR EVENT INVESTIGATION METHODS, TOOLS AND TECHNIQUES

Interim Technical Report

Stanislovas Ziedelis, Marc Noel



EUR 24757 EN - 2011

The mission of the JRC-IE is to provide support to Community policies related to both nuclear and non-nuclear energy in order to ensure sustainable, secure and efficient energy production, distribution and use.

European Commission
Joint Research Centre
Institute for Energy

Contact information

Address: Postbus 2, 1755 ZG Petten, the Netherlands
E-mail: Stanislovas.Ziedelis@ec.europa.eu
Tel.: +31-224-565447
Fax: +31-224-565637

<http://ie.jrc.ec.europa.eu/>
<http://www.jrc.ec.europa.eu/>

Legal Notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

***Europe Direct is a service to help you find answers
to your questions about the European Union***

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server <http://europa.eu/>

JRC 62929

EUR 24757 EN
ISBN 978-92-79-19712-3
ISSN 1018-5593
doi:10.2790/3097

Luxembourg: Publications Office of the European Union

© European Union, 2011

Reproduction is authorised provided the source is acknowledged

Printed in Luxembourg

List of acronyms and definitions

AEB	Accident evolution and barrier function
ASSET	Assessment of Safety Significant Event Team
ATHEANA	A Technique for Human Event Analysis
CAS-HEAR	Computer Aided System for Human Error Analysis in Railway Operations
CCDF	Conditional Core Damage Frequency
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CRT	Current Reality Tree
ESReDA	the European Safety Reliability and Data Association
FRAM	Functional Resonance Analysis Method
HF	Human factors
HFE	Human factors engineering
HFIT	Human Factors Investigation Tool
HPEP	Human Performance Evaluation Process
HPES	Human Performance Enhancement System
HPIP	Human Performance Investigation Process
HRA	Human reliability analysis
IAEA	International Atomic Energy Agency
IE	Institute for Energy; Initiating Event
INES	International Nuclear Event Scale
IRS	Incident Reporting System
JRC	Joint Research Centre of European Commission
LL	Lessons Learned
MORT	Management Oversight and Risk Tree
MTO	Man, technology, organisation
NPP	Nuclear Power Plant
NRC	Safety Nuclear Regulatory Commission
OEF	Operating Experience Feedback
PRCAP	Paks Root Cause Analysis Procedure
PROSPER	Peer Review of the effectiveness of the Operational Safety Performance Experience Review
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
QA, QC	Quality assurance, quality control
RASP	Risk Assessment Program
RCA	Root Cause Analysis
SAR	Safety Analysis Report
SOL	Safety through Organisational Learning
STEP	Sequential Timed Events Plotting
TSO	Technical Supports Organisation
WANO	World Association of Nuclear Operators
WGOE	Working Group of Operational Experience Feedback
3CA	Control Change Cause Analysis

The majority of terms and definitions in this report are used in accordance with IAEA documents [1, 2] and/or IAEA glossary [37]. Some specific or newly suggested definitions are discussed and explained in the text of the report.

Content

Executive summary	6
1. Introduction	8
1.1. Background	11
1.2. Objectives and scope	12
1.3. Structure of the report	13
2. Event investigation methodologies and methods	14
2.1. Root cause analysis methods	18
2.1.1. HPES - Human Performance Enhancement System	22
2.1.2. MORT - Management Oversight and Risk Tree	25
2.1.3. ASSET - Assessment of Safety Significant Event Team	28
2.1.4. RCA methods derived from HPES	34
2.1.4.1. HPIP - Human Performance Investigation Process	34
2.1.4.2. MTO - Man-Technology-Organisation Investigation	36
2.1.4.3. AEB - Accident evolution and barrier function	37
2.1.4.4. PRCAP - The Paks Root Cause Analysis Procedure	39
2.1.5. SOL - Safety through Organisational Learning	39
2.1.6. TRIPOD	43
2.1.7. STEP - Sequential Timed Events Plotting	46
2.1.8. A remedy-oriented event investigation system	48
2.1.9. HF- compatible RCA method	50
2.1.10. 3CA - Control Change Cause Analysis	51
2.1.11. FRAM - Functional Resonance Analysis Method	55
2.1.12. CAS-HEAR - Computer-Aided System for Human Error Analysis & Reduction	57
2.1.12.1. Underlying model of CAS-HEAR	57
2.1.12.2. Procedure of CAS-HEAR	59
2.1.13. Apollo root cause analysis	66
2.1.14. Other RCA related event investigation methods	67
2.1.15. Apparent Cause Analysis	71
2.1.16. HPEP - Human Performance Evaluation Process	72
2.1.17. PROSPER - Peer Review of the effectiveness of the Operational Safety Performance Experience Review process	74
2.2. PSA based event and precursor analysis methods	76
2.2.1. ATHEANA	79
2.2.2. RASP	83
2.2.3. Attributes of PSA and correlation with other event investigation methods	85
2.3. Deterministic safety analyses	90
2.4. Safety Culture Impact Assessment	94
3. Event investigation tools and techniques	99
3.1. Event and causal factor charting and analysis	106
3.2. Cause and effect analysis	115
3.3. Interviewing	117
3.4. Task analysis	120
3.5. Change analysis	121
3.6. Barrier analysis	125
3.7. Fault tree analysis	130
3.8. Event tree analysis	134
3.9. Causal factor tree analysis	136
3.10. Kepner-Tregoe Problem Solving and Decision Making	140

3.11.	Interrelationship diagram	142
3.12.	Current Reality Tree (CRT)	143
3.13.	Human Factors Investigation Tool (HFIT)	145
3.14.	Commercial all-purpose root cause analysis tools	148
3.14.1.	REASON®	148
3.14.2.	PROACT®	150
3.14.3.	RealityCharting®	154
3.14.4.	TapRooT®	158
4.	Comparative analysis of effectiveness and applicability of event investigation methodologies, methods and tools	162
4.1.	General considerations	162
4.2.	Results of comparison of different event analysis methodologies, methods and tools	169
5.	Recommendations	180
6.	Conclusions	193
7.	References	195

Executive summary

The feedback from operating experience is one of the key means of enhancing safety and operational risk management. The focus on risk management is growing in our society, because increasing accident rates and system losses in different industrial sectors endanger safety, threaten economic growth, cause environment pollution, and negatively affect public perception. The effectiveness of learning from experience at nuclear power plants (NPPs) could be maximised, if the best event investigation practices available from a series of methodologies, methods and tools, in the form of a ‘toolbox’ approach, were promoted.

With the development of technology, system reliability has increased dramatically during recent decades, while human reliability has remained unchanged over the same period. Accordingly, human error is now considered the most significant source of accidents or incidents in safety-critical systems. Therefore, there is a need for effective instruments that can help identify the types and causes not only of equipment failures, but also of human errors, and to derive effective countermeasures to prevent or reduce their future recurrence. As a consequence of the prevailing role of human factors in most events and accidents, and the urgent need to increase the reliability of human performance, numerous methodologies, methods, tools and techniques for the analysis of events and incidents have been developed; currently most of these are oriented towards not only technical systems, but also human, organisational and safety culture related factors in particular. Theoretical and practical results and experience accrued by event investigators, scientists and practitioners have established the knowledge related to event investigation as a separate scientific discipline. However, different accident models and analysis methods affect what accident investigators look for, which contributory factors are found, and which recommendations are made. So, the effectiveness of efforts targeted at the enhancement of safety, through learning from operational experience, depends on the ability of investigators to select and implement the most appropriate practices and instruments for event investigation.

Based on available sources of technical, scientific, normative and regulatory information, an inventory, review and brief comparative analysis of the information concerning event investigation methods, tools and techniques, either indicated or already used in the nuclear industry (with some examples from other high risk industry areas), was performed in this study. Its results, including the advantages and drawbacks identified from the different instruments, preliminary recommendations and conclusions, are covered in this report.

One of the first findings identified during the analysis was lack of standardisation in the area of event investigation methodologies: there is no universally accepted system of classification, terms, definitions and criteria for the evaluation of different event investigation methods, tools and techniques. Despite the fact that much information about the individual attributes of numerous event investigation instruments has been published, only a limited number of studies designed to compare the different event investigation methods and tools have been performed. These studies usually aim for specific goals, use different comparison criteria, which are not commonly accepted, are of limited scope, and cover only small number of instruments from the available toolbox. Some results of such comparisons seem to be of a promotional type, one-sided and unfair.

In line with the concept of separating the event investigation instruments of different levels, a classification system comprising three levels (methodologies, methods and tools) was suggested. In pursuance of this classification system, an inventory, review and brief comparative analysis of event investigation methods, tools and techniques, either recently developed or already used in the nuclear industry (with some examples from other high risk industry areas) was performed. Some advantages and drawbacks of these different instruments were identified and analysed. It is demonstrated that the supposed advantages of simple, easy to use root cause analysis (RCA) tools (sometimes actively promoted by providers), requiring neither training nor qualification of the user (especially some software based RCA tools) should be not overestimated. These tools could be used effectively, taking into account their existing limitations.

Lack of means for selecting the appropriate root cause analysis methods and tools, based upon objective performance criteria, was identified. Most of the available recommendations concerning selection and usage of different event investigation methods, tools and techniques are not exhaustive and user-friendly. They usually cover only a few instruments, of different levels, selected without adequate substantiation; event types for which some methods or tools are recommended for use are not adequately specified; and some recommendations contradict others. So, most of the available recommendations are of little practical value, leaving current and future event investigators (including newcomers, who are not yet proficient) to make decisions about the selection of event investigation methods and tools, based on their own knowledge, or providers' promotional materials.

There are no established threshold criteria for performing an event investigation of an appropriate level. Every organisation needs to establish its own threshold criteria for defining the level of analysis, depending on the type of industry, organisation and potential risk of activities. The validity of such an approach could be questioned (especially for high risk industries like nuclear energy), and the potential to institute a system of clearly defined threshold criteria should be considered.

Unstructured processes of root cause analysis put too much emphasis on opinions, take too long, and do not produce effective corrective measures or lasting results. For further improvement of operational reliability and better employment of operational experience feedback in the nuclear industry, it is necessary to establish baseline standards, setting out criteria and minimum requirements for what is to be considered RCA, policies for training, and best practice, using structured root cause analysis methods and tools. The alternative is to continue to assume that existing efforts will somehow produce different, better results.

The results of comparative analysis of nuclear event investigation methods, tools and techniques, presented in this interim report, are preliminary in character. It is assumed that, for the generation of more concrete recommendations concerning the selection of the most effective and appropriate methods and tools for event investigation, new data, from experienced practitioners in the nuclear industry and/or regulatory institutions are needed. It is planned to collect such data, using the prepared questionnaire [156] and the survey currently being performed. This is the second step in carrying out an inventory of, reviewing, comparing and evaluating the most recent data on developments and systematic approaches in event investigation, used by organisations (mainly the utilities) in the EU Member States. After the data from this survey are collected and analysed, the final conclusions and recommendations will be developed and presented in the final report on this topic. This should help current and prospective investigators to choose the most suitable and efficient event investigation methods and tools for their particular needs.

1. Introduction

Effective use of operational performance information is an important element in any plant operator's arrangements for enhancing the operational safety of a nuclear power plant (NPP). This has been recognised in many references (e.g. IAEA Safety Fundamentals and Guides [32, 33, 105], INSAG 12 [106] etc. One of the principles of the safe operation of NPPs is that 'The precursors to accidents have to be identified and analysed, and measures have to be taken to prevent the recurrence of accidents. The feedback of operating experience from facilities and activities and, where relevant, from elsewhere is a key means of enhancing safety. Processes must be put in place for the analysis and feedback of operating experience, including initiating events, accident precursors, near misses, accidents and unauthorised acts, so that lessons may be learned, shared and acted upon'.

This principle is further expanded in the IAEA Safety Standards [33] under the 'Feedback of Operating Experience' which requires that:

- 'Operating experience at the plant shall be evaluated in a systematic way. Abnormal events with important safety implications shall be investigated to establish their direct and root causes. The investigation shall, where appropriate, result in clear recommendations to plant management who shall take appropriate corrective action without undue delay. Information shall be fed back to the plant personnel.'
- 'Similarly, the operating organisation shall obtain and evaluate information from the operational experience at other plants which provides lessons for the operation of their own plant. To this end, the exchange of experience and the contribution to national and international data is of great importance.'
- 'Operating experience shall be carefully examined by designated competent persons to detect any precursors of conditions adverse to safety, so that corrective action can be taken before serious conditions arise.'
- 'All plant personnel shall be required to report all events and encouraged to report near misses relevant to the safety of the plant.'
- 'Plant management shall maintain liaison as appropriate with the organisations (manufacturer, research organisations, designer) involved in the design, with the aims of feeding back operating experience and of obtaining advice, if needed, in the event of equipment failures or abnormal events.'
- 'Data on operating experience shall be collected and retained for use as input for the management of plant ageing, for the evaluation of residual plant life and for probabilistic safety assessment and periodic safety review.'

IAEA Safety Guide No NS-G-2.11 [105] establishes a requirement, that the analysis of any event should be performed by an appropriate method. It is common practice that organisations regularly involved in the evaluation process use standard methods to achieve a consistent approach for the assessment of all events. These standard methods usually involve different tools and techniques. Each tool or technique may have its particular advantages for cause analysis, depending on the type of failure or error. However, currently there are no well-reasoned comprehensive recommendations for selection of event investigation methods, tools and techniques. On the contrary, there is a view that 'it is not possible to recommend any one single technique. Either one technique or a combination of techniques should be used in event analysis to ensure that the relevant causes and contributing factors are identified, which aids in developing effective corrective actions' [1, 2].

Experience of general interest is not limited to events with a direct impact on the operation of a facility, but also relates to conditions, observations and new information of all kinds that could affect nuclear safety. Lessons about risks to nuclear facilities should also be learned from other technical fields, although INSAG-23 [34] recognises that these may be difficult to collect. For example, investigations into accidents at other large, technically sophisticated facilities, such as power plants fired with fossil

fuels or oil refineries, may provide useful insights for nuclear operators and regulators. Operators in the nuclear industry need to be constantly on the lookout, to identify relevant hazards outside of their industry [34].

One of the important threats to a nuclear facility comprised of people, hardware and organisational structures, is from the accumulation of delayed-action hidden failures or ‘latent’ failures in the system, most of which originate from the organisational and managerial areas. A latent failure is either a decision or action with damaging consequences which may lie dormant within the system for a long time. These weaknesses only become evident when they combine with a local triggering factor such as active failure, a technical fault, or atypical system conditions. In many cases they originate from people whose activities are remote from the human-machine interface, such as designers or managers. The more complex, interactive and opaque the system, the greater will be the number of latent failures. In addition, as we move higher up the organisation, greater opportunities exist for generating latent failures, and their reach is broader. In a highly protected system, the probability of an isolated action leading to an accident is very small. But several causal factors can create a ‘trajectory of opportunity’ through the multiple safeguards. In summary, latent failures may lie dormant in the system until a trigger initiates an accident sequence. Thus, the main thrust of accident prevention programmes should be aimed at eliminating these failures [92].

With the development of technology, system reliability has increased dramatically during the past decades, while human reliability has remained unchanged over the same period. Accordingly, human error is now considered the most significant source of accidents or incidents in safety-critical systems. Therefore, there is a need for methods and techniques that can help to identify the types and causes not only of equipment failures, but also of human errors, and to devise effective countermeasures to prevent or reduce their future recurrence.

Reliable human performance is a requirement for safe operations in many settings, including the operations of commercial nuclear power and nuclear materials licensees [4]. Increasing accident rates and system losses in different industrial sectors endanger safety, threaten economic growth and cause pollution damage. Ever since the systematic study of human performance and accidents began, it has been clear that human errors (i.e., inappropriate or inadequate human actions) contribute to a large proportion of accidents and incidents. This has proved true for vehicle operation (aircraft, cars, motorcycles, bicycles), for industry (commercial aviation maintenance, manufacturing, chemical processing, mining), and for electric power generation. According to statistics regarding railway accidents in Korea from 1995 to 2004, 61 % of the train accidents involving collisions, derailments and fires were attributed to human error. In addition, 74 % of level crossing accidents were caused by human error, most of which were violations by car drivers. Also in the United States’ railroad industry, train accidents related to human factors make up a significant proportion of all train accidents [17]. In industries in Japan relating to the operations of railroads, airlines and chemical plants, human errors have in recent years accounted for 40 % to 80 % of all incidents [38]. In nuclear power generation, the proportion of events or mishaps attributed at least in part to human error has ranged from 40 % to 80 %, depending on the study and the specific measures used, but it is consistently reported as having a major role (see Figure 1.1) [35, 40, 107]. Human error is a major cause of accidents and losses in the chemical process industry, contributing within a range of 60-90 % to the occurrence of such accidents [134]. Conventional safety and risk analysis methods focus mainly on describing technological malfunctions and lack a systematic consideration of the human impact, i.e., human error, on the process under consideration.

Human errors may play several different roles in an event sequence. An error may:

- directly cause an event;
- contribute to an event by setting up the conditions that, in combination with other events, or conditions, allowed the event to occur (e.g., leaving a valve open that should be closed);
- make the consequences of an event more severe;
- delay recovery from an event.

The criteria for attributing an incident to human error are very strictly defined in the nuclear industry, in view of their decisive effect on the relevant statistics. Applying the strict criteria thus defined, the frequency of human error incidents has remained through the years preceding 1994 at an almost constant level in the nuclear industry, at around 0.1 incident per year per unit, despite a steady diminution in the overall incident frequency in this industry during the same period [38].

The trend is thus toward a gradually rising proportion of human-related nuclear power plant incidents. Alongside this trend, the complicated mechanisms present in recently-built nuclear power plants are all the more significant: a minor human error caused by a shortcoming in human activity - e. g., a technician with inadequate understanding of the consequences of his act - can potentially lead to extensive damage, the consequences of which are magnified due to the large scale of the plant affected. This adds to the importance of the human factor in plant operations, and applies to all industries in general.

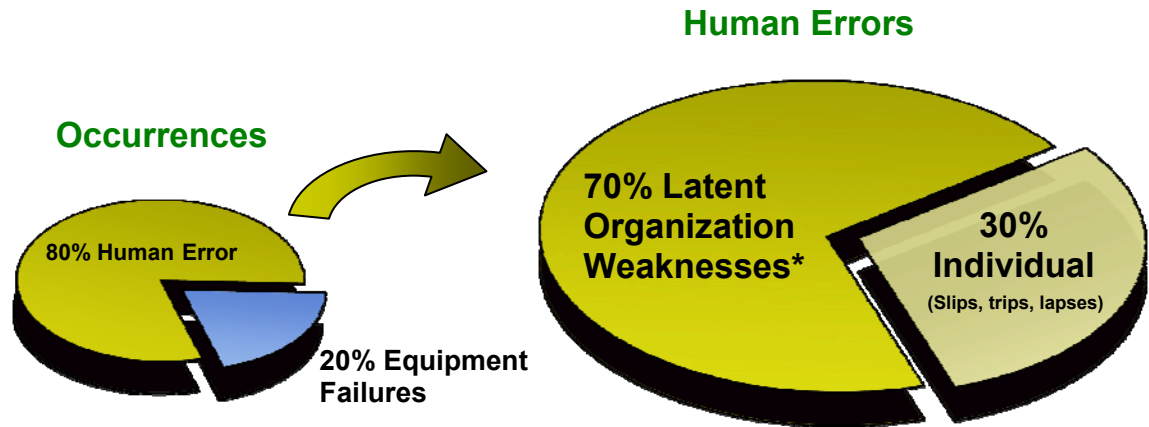


Figure 1.1. Role of different sources contributing to occurrences [40]. *Latent Organisation Weakness – hidden deficiencies in management control process or values creating workplace conditions that can provoke an error and/or degrade the integrity of defences

There is no way to achieve absolute safety, even in the operations of facilities which are not as complex as nuclear power plants. Some likelihood of an incident will always exist. So, it is important to understand why accidents occur, and to find the best way to prevent the root cause. According to data from the Japan Functional Safety Laboratory [35], about 70 to 80% of accidents are caused by human factors.

Accident investigation practices used in different economic sectors in Europe were widely discussed and analysed during the ESReDA (The European Safety Reliability and Data Association) seminar 'Safety Investigation of Accidents', which was organised at IE JRC in Petten in 2003 [97]. The need to develop a common EU approach to accident investigations was expressed [96]. The European Commission indicated that there was a growing need for independent technical investigations geared towards revealing the causes of accidents. Such investigations should:

- be aimed at establishing the root, real and technical causes of accidents;
- be conducted autonomously and impartially (requiring therefore the functional independence of the investigating body or entity);
- be held independently of those responsible for the accident (determination of liability and compensation for damages);
- be independent of the judicial authorities, insurance companies, industry, operators and regulators or any party whose interest could conflict with the task entrusted to the investigating body;
- enable the establishment of safety recommendations and follow-up actions.

In order to enable accident investigations to be carried out with optimum effectiveness, the following general principles should be applied: independence, transparency, credibility and influence. To assist the European Commission in the formulation of common European methodological elements for independent technical accident investigations in the different sectors of EU industry, the Working Group on Accident Investigations (WGAI) was established in 2004 [154]. Its main objective was to improve the quality of accident investigation, and thereby to improve also the ‘learning from experience’ process and safety performance. One of WGAI’s important achievements was the preparation of Guidelines for safety investigation of accidents [155].

There is an increasing focus on risk management in society today. The urgent need to ensure the safe operation of complex technical installations, by increasing the reliability of human performance, has led to the development of numerous methodologies, methods, tools and techniques for analysis of events and incidents. Each of these instruments has different areas of application and different qualities and deficiencies. A combination of several instruments should be used in the comprehensive investigation of complex accidents. As a consequence of the prevailing role of human factors in the majority of events and accidents, most of these instruments are currently oriented not only to technical systems, but also to human, organisational and safety culture related factors in particular. In recent decades, theoretical and practical results and experience gained by event investigators, scientists and practitioners has led to knowledge related to event investigation being seen as a separate scientific discipline. However, different accident models and analysis methods affect what accident investigators look for, which contributory factors are found, and which recommendations are made [119].

There is a lot of information about the individual attributes of different event investigation methods, tools and techniques; however, there is little information regarding the performance of these instruments relative to each other. The extent to which investigators are aware of the pros and cons of specific event investigation methods, tools and techniques has not been explored sufficiently. Thus, problem solvers and decision makers are likely to select what they may consider to be an adequate instrument based on convenience rather than on its actual performance characteristics. So, comparison of the attributes of different event investigation instruments, with the purpose of providing problem solvers with a mechanism that can be used to select the appropriate instrument for the specific event, is an issue of paramount importance.

Another problem facing most event investigators is related to the lack of a commonly accepted system of definitions and classification of terms and concepts used in the literature concerning event investigations. Even such basic terms as ‘root cause’, ‘human factors’, ‘organisational factors’, ‘safety culture’ etc. are ambiguous, with different meanings for different people. For example, there should be a clear distinction between event investigation methodologies, methods and tools. A tool should be distinguished by its limited use, relatively narrow scope and concretely defined inputs, procedures and outputs, while a method may involve many steps and processes and has wide usage. Each event investigation method is realised using one or more (sometimes a combination of several) tools and techniques. However, there is no commonly accepted system for classification of event investigation methods, tools and techniques, and sometimes different authors use different terms to identify the same approach. One of the most comprehensive systems of classification of event investigation methods and tools is presented in [1], but this cannot be considered sufficiently exhaustive, because numerous new tools and techniques are being developed and appearing in different countries each year.

1.1. Background

The European Network on Operational Experience Feedback (OEF) for Nuclear Power Plants (NPP), hereafter referred to as the European Clearinghouse on NPP OEF, was established by several European Nuclear Safety Regulators to promote regional collaboration on operational experience, dissemination of the lessons learned from NPP operation, understanding of the role of operational experience feedback

systems in the safe and economic operation of existing as well as new build NPPs, and promotion of advanced event assessment approaches and methods.

In 2007 general agreement was reached on a common interest in establishing the European Clearinghouse on NPP OEF at the Institute for Energy, Petten site, and an IE institutional project on this was initiated. A multi-partner collaboration arrangement on the European Clearinghouse on NPP OEF was agreed by the Regulatory Bodies from Finland, Hungary, Lithuania, the Netherlands, Romania, Slovenia and Switzerland in February 2008, in Petten. Regulatory Authorities from Spain and the Czech Republic participated as observers. Following the Kick-off Meeting of the Enlarged Clearinghouse (28-29 April 2010, Amsterdam) it currently comprises 13 European Safety Authorities (Finland, Hungary, the Netherlands, Lithuania, Romania, Slovenia, Switzerland, Bulgaria, Czech Republic, France, Germany, Slovak Republic, Spain – the last six being observers) and two European Technical Support Organisations (France, Germany).

The overall objective of the European Clearinghouse on OEF for NPPs is to facilitate efficient sharing and implementation of operational experience feedback to improve the safety of NPPs. In particular, the project is aiming at:

- Improvement of NPP safety through the strengthening of cooperation between licensees, regulatory authorities and their Technical Support Organisations (TSOs) staff to collect, communicate, and evaluate reactor operational events information and apply systematically and in a consistent manner lessons learnt throughout European countries participating in the project.
- Establishment of European best-practice for assessment of NPP operational events, through the use of state-of-the art methods, computer aided assessment tools and information gathered from different national and international sources, such as EU National Regulatory Authorities event reporting systems, Incident Reporting System (IRS) jointly operated by IAEA and OECD/ NEA, etc.
- Provision of EU resource base staff to coordinate the European Clearinghouse on NPP OEF activities and maintain effective communication between experts who are involved in OEF analyses from European Regulatory Authorities and their TSOs.
- Support to the long-term EU policy needs on OEF, through exploitation of the JRC and European TSOs competence in research in nuclear event evaluation methods and techniques.

This report has been prepared on behalf of the European Clearinghouse on NPP Operational Experience Feedback in the framework of technical task ‘Comparative study of event assessment methodologies with recommendations for an optimised approach in the EU’ according to the NUSAC work program for 2010, which was approved during the Technical Meeting of European Clearinghouse (1 December 2009, Petten).

1.2. Objectives and scope

Learning from experience is acknowledged as one of the cornerstones of modern approaches to risk management. Investigations and analyses of events are seen as valuable sources of information related to safety, and thereby constitute important insights towards improvement. In recent years there has been rapid development of knowledge and systematic approaches, methodologies and tools to aid the event investigation practices used within the nuclear industry. However, despite obvious achievements, accidents are still occurring and recurring. They illustrate the multiple organisational failures of risk management processes, including the deficiencies of the OEF process and incidents when lessons are not fully learned. Consequently, it is necessary to evaluate and find ways to improve the quality of the event investigation which is the main vehicle of OEF and risk reduction processes.

This project was launched by JRC/IE SPNR in order to perform the background research in support of specific scientific and technical nuclear safety related areas. The general purpose of this project is further improvement of safety provisions by optimising the application of event investigation methods

and tools to enhance the operational experience feedback process. Based on the results of this project, JRC-IE SPNR intends to provide useful guidance and information for organisations wishing to develop or strengthen their capabilities in this area.

The JRC-IE SPNR implementation plan for this project includes three main steps:

- Carrying out an investigation and preparation of an interim report on the topic ‘Comparative analysis of nuclear event investigation methods, tools and techniques’. Based on available technical, scientific, normative and regulatory documentation, this interim report will include a review and brief comparative analysis of information concerning event investigation methods, tools and techniques, either proposed or already used in the nuclear industry (with some examples from other high risk industry areas). The identified advantages and drawbacks of the different instruments will be covered in this report.
- Preparation of a questionnaire and carrying out a survey, with the aim of collecting available information on practical experience of the individual event investigation methods and tools currently used in the nuclear industry. This is the first step in recording, reviewing, comparing and evaluating the most recent data on developments and systematic approaches in event investigation used by organisations (mainly utilities) in the EU Member States.
- Preparation of the final report, which will be based on the data obtained from the survey and include conclusions and recommendations relating to the most efficient event investigation methods and tools. This should help current and prospective investigators to choose the most suitable one for their particular needs.

With the aiming of achieving readability, and taking into account the limited extent of this interim report, its scope is restricted to providing only the most important, essential information about the basic principles of each selected event investigation method or tool, supported by a minimum number of illustrations. While presentation of more comprehensive descriptions of selected methods or tools, complemented by adequate examples, would be certainly useful, it is beyond the scope of this work.

1.3. Structure of the report

Chapter 1 of this interim report contains a general introduction, some background information, a description of the main objectives and scopes of the report and a brief description of its structure.

Using the suggested system of classification of instruments for event investigation, some of most commonly used event investigation methodologies and methods are briefly reviewed and analysed in chapter 2; more comprehensive information about them can be found, using the references provided.

The main characteristics of the most commonly used event investigation tools and techniques, including their advantages and disadvantages, are presented in chapter 3.

Chapter 4 presents the main results of a comparative analysis of the applicability and effectiveness of event investigation methodologies, methods and tools, outlined and analysed in chapters 2 and 3.

Chapter 5 provides preliminary recommendations (based on available information) regarding the different approaches to selection of the most effective event investigation methodologies, methods and tools; preliminary conclusions are given in chapter 6, and chapter 7 contains a list of references.

2. Event investigation methodologies and methods

The main objective of an event investigation is to enable the identification of corrective actions adequate to prevent recurrence, or reduce its probability, and thereby protect the health and safety of the public, the workers, and the environment. The line of reasoning in the investigation process is:

- Outline what happened (or could happen), step by step.
- Begin with the occurrence and identify the problem (condition, situation, or action that was not wanted and not planned).
- Determine what programme element was supposed to have prevented this occurrence. (Was it lacking or did it fail?)
- Investigate the reasons why this situation was permitted to exist.

This objective of an event investigation could be achieved effectively if the inquiry follows one of the commonly accepted approaches, based on a well structured system of instruments, including methodologies, methods, tools and techniques.

Methodology can be defined as a system of ways of doing or studying something; it is a body of methods, practices, procedures, and rules used by those who work in a discipline or engage in an inquiry. Methodology can properly refer to the theoretical analysis, study or implementation of the methods appropriate to a field or to the body of methods and principles particular to a branch of knowledge. Event investigation methodology can be defined also as merely a thought process – a way of thinking through why things go wrong, or like the category representing the specific approach to conducting event investigation [54].

For the purposes of this report an event investigation methodology is a set of working methods establishing the strategy of an inquiry and describing an integrated system of event investigation activities (study of documents, collection of facts, interviews, observations, analysis, calculations, modelling, etc.), designed to achieve understanding of the real or potential occurrence, its precursors, circumstances, conditions, direct and root causes, and organising the facts and data obtained in order to arrive at a logical set of findings and conclusions, allowing identification of effective corrective actions and/or countermeasures to prevent or reduce probability of future recurrences [1, 11].

Method is a set of practices, procedures, and rules establishing the tactics of an inquiry and providing the discipline and guidance for the user for following a methodology in a particular way. Method may involve many steps and processes and has wide usage; it is realised using one or more (sometimes a combination of several) tools and techniques and usually has its own taxonomy.

A root cause analysis tool is a relatively simple event investigation instrument, developed through experience to assist groups and individuals in identifying root causes, and providing detailed step-by-step working procedures for event analysis that can be recorded, repeated and verified. It is just one of vehicles to implement method; it is distinguished by its limited use, relatively narrow scope and concretely defined inputs, procedures and outputs.

Important desirable characteristics of an event investigation and analysis methodology suitable for application to single events include the following [2]:

- The scope of the event investigation and analysis methodology covers all the systems already described above, i.e. people, technology, organisation and environment.
- The methodologies are flexible to meet the needs of plants with varying levels of event investigation and analysis expertise.
- The methodologies are efficient, economical, and practical.
- The methodologies encourage the use of teams in the investigation and analysis of events.
- The users of the methodologies have adequate training in the methodologies they apply.
- The methodologies counteract human problem solving and decision biases such as: monocausal thinking, early hypothesis formulation and orientation, search for scapegoats, and hindsight bias.
- The methodologies promote proactive actions in order to detect problems before they occur.

- The methodologies are easy to review, making it possible to follow each step in the process up to the conclusions and results.
- Collection of event information and review of significant data.
- Analysis in search of contributing factors.
- Development of focused and practicable corrective actions.
- Determination of the efficacy of the corrective actions.
- Prioritisation among corrective actions.
- Assessment and follow-up of corrective actions.
- Event reporting that emphasises and facilitates learning (including support for event aggregation) in the process of operating experience feedback.

An event analysis methodology suitable for review of event aggregates should have the following characteristics:

- Event trending and analysis should be based on clearly defined data sets (valid high quality data are necessary).
- Methodologies used should consider accessibility and usability of national and international databases for event evaluation purposes.
- The users of the methodologies should have adequate training in statistical methods.

Traditionally, the analysis of operational events has targeted the identification of root causes and the prevention of their reoccurrence. The basic traditional event investigation process is well-established but purely qualitative; it includes five stages:

1. Establish the facts - what happened.
2. Analyse data to determine how it happened, and the causes or why the event occurred.
3. Develop recommended corrective preventive actions.
4. Report the lessons learned, internally and externally.
5. Conduct an Effectiveness Review.

There are four accepted main methodologies for nuclear event investigation, establishing the strategy of an inquiry and describing an integrated system of event investigation activities [23]:

- Root Cause Analyses;
- Probabilistic Safety analysis based methodology (Precursor Analyses);
- Deterministic Transient Analyses;
- Safety Culture Impact Assessment.

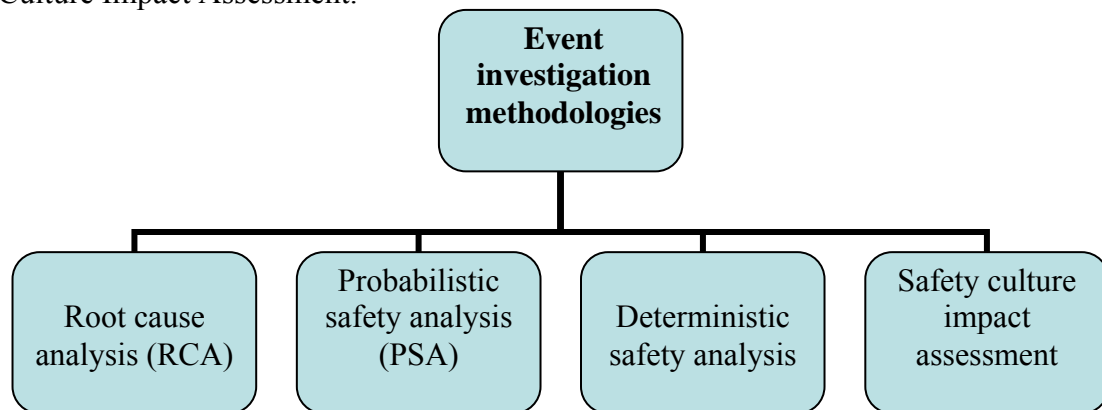


Figure2.1. The main accepted methodologies for nuclear event investigation

Each of these methodologies are represented by the set of working methods establishing the tactics of an investigation and providing the discipline and guidance for the user for following a methodology in a particular way. Unlike the four methodologies, a lot of event investigation methods of different complexity and effectiveness, with different goals and areas of application, exist or are being developed in different countries.

One of the antecedents of event investigation methods currently used in the nuclear industry is the US Aviation Safety Reporting System (ASRS) [112]. The ASRS collects, processes and analyses voluntarily submitted aviation safety incident/situation reports from pilots, controllers, dispatchers, flight attendants, maintenance technicians, and others. Reports submitted to ASRS may describe both unsafe occurrences and hazardous situations. ASRS's particular concern is the quality of human performance in the aviation system. The ASRS acts on the information these reports contain. It identifies system deficiencies, and issues alerting messages to persons in a position to correct them. This system has won reputation for its serving as a criterion for establishing the legal immunity of pilots from prosecutions [39]. In Japan, certain industrial sectors – such as railroads, shipping, chemical and steel manufacture – also practice a reporting system focused on analysing the human errors involved in an incident [38].

Since the Three Mile Island (1979) and Chernobyl (1986) accidents, extensive research on human error has been conducted, especially in the nuclear power industry. HPES (Human Performance Enhancement System) [18], which is based on ASRS, and HPIP (Human Performance Investigation Process) [19] are the two examples of methods for analysing and managing human error in nuclear power plants. These methods include all the steps, from analysing the accident sequence to reporting the results; at each step, a detailed procedure, useful techniques, and worksheets are provided. They have both been updated over time, using continued feedback from field applications and theoretical developments (e.g. [4]). TapRooT®, which has procedures and tools that are similar to those of HPIP but is intended for use in any industry, is being used in a wide variety of industries such as those related to health care, railways, oil, chemicals, airlines, and construction [20]. Moreover, according to a recent survey, TapRooT® software commands nearly 50% of the US market share of all-purpose root cause analysis (RCA) software [17].

In the aviation industry, HFACS (Human Factors Analysis and Classification System) is widely used as a human error analysis technique. Unlike HPES and HPIP, it does not involve all the steps of analysis, but systematically classifies the types and causes of errors by human operators. It was developed based on a model of the causality behind an accident, which is known as the 'Swiss cheese model' [95]. TRACER (Technique for the Retrospective and predictive Analysis of Cognitive Errors in air traffic control) enables analyses of the modes and mechanisms of human error more deeply than HFACS does, and it also includes an analysis of error detection and correction. Recently, the two techniques were adapted to the railway industry: HFACS-RR (railroad) and TRACER for drivers.

In the marine industry, CASMET (Casualty Analysis Methodology for Maritime Operations) was developed as part of the movement towards an integrated system for human factors and accident analysis in Europe. The human factors classification of the Marine Accident Investigation Branch (MAIB) in the UK has also been used in this industry. Recently, HFIT (Human Factors Investigation Tool) was developed to analyse human errors in the UK offshore oil and gas industry. As one of the techniques developed for use in any industry, CREAM (Cognitive Reliability and Error Analysis Method) is well known [17]. It provides detailed classification schemes of erroneous actions and causal links between genotypes, but more specialised classification schemes are needed before it can be used for a specific domain. While other techniques are mainly concerned with the completeness of human error analysis by providing detailed procedures or classification systems, CREAM provides not only detailed procedures and classification schemes, but also effective means of increasing the efficiency of the analysis. One approach is to use the description of common performance conditions (CPCs) as the basis for determining probable causes. This is done using a simple matrix that indicates the relationship between CPCs (e.g. adequacy of organisation, working conditions) and main genotype groups (person, technology and organisation-related genotypes). Another approach is to use the relationships between the classification groups. The possible cause-and-effect relationships between the elements in the classification groups are predefined. These links make it easier to determine the causes of human error and their relationships. For practical use, however, these two means should be refined and specified for a certain domain.

Hazard and Operability studies (HAZOP) technique was developed in the early 1970s by Imperial Chemical Industries Ltd. HAZOP can be defined as the application of a formal, systematic, critical

examination of the process and engineering intentions of new or existing facilities to assess the hazard potential that arises from deviation in design specifications and the consequential effects on the facilities as a whole. This technique gained wide acceptance in process industries as an effective tool for plant safety and operability improvements [45].

The number of computer-aided systems that support RCA and human error analysis is constantly growing. For example, in Korean nuclear power plants, a computerised system of K-HPES, referred to as CAS-HPES [14], has been used since 2000. It has recently been revised as a web-based system [15]. In the railroad industry, RAIT (Rail Accident Investigation Tool) [16], a computer-based tool, was developed based on solid theoretical grounds; however, at present it is difficult to find examples of its application. There are also commercial software tools for root cause analysis (RCA) or human factors analysis (e.g. TapRoot®, Apollo, Realitycharting®, ProAct®, Reason®, RAIDTM). However, they all are intended for use in any industry and for investigating general problems as well as human error. For this reason, their processes and techniques are relatively simple and general, and the supporting features they offer are not sufficient. In addition, they are stand-alone systems that do not have the advantages of web-based systems (e.g. no need for installation, easy updates).

The effort was made [17] to develop a managerial error analysis system, referred to as HEAR (Human Error Analysis & Reduction), for use in the Korean railway industry. HEAR, which includes a detailed procedure, useful tools, and recording forms, was initially developed for human error analysis. CAS-HEAR (Computer-Aided System for HEAR), a web-based system, was then designed to increase the quality and efficiency of human error analysis using the HEAR procedure. To develop HEAR and CAS-HEAR, the advantages and disadvantages of existing techniques for human error analysis were thoroughly reviewed, and a complete model of accident causation was developed, from which the main components of the analysis were derived. For each analysis step, the functional and design requirements for CAS-HEAR were derived in terms of improving the quality and efficiency of the analysis. A prototype of CAS-HEAR, in which some features, such as opening and reporting an analysed case, are not included, was implemented, based on requirements.

The NRC guidance document [41] provides useful information for evaluating the adequacy of a human reliability analysis (HRA), particularly with respect to the HRA method used (considering its strengths, limitations, and underlying knowledge and databases). Depending on the application, some methods may be better suited and, in fact, more appropriate to use than others, particularly if the characteristics of a method are incompatible with those needed, based on the application. For instance, if an application requires an examination of potential causes leading to human failures, and an application submission presents an analysis performed using an HRA method that analyses human failures using a simple time-reliability correlation, whereby time is the surrogate underlying cause for all errors or failures to respond, the use of such a method, by itself, would not be appropriate for that type of application. Thus, knowing how a particular HRA method fares with respect to good practice (and, therefore, when other sources of guidance may be desirable to help address a particular type of good practice), and being knowledgeable about each method's strengths, limitations, and underlying bases, provides a starting point for analysts, reviewers, and users to determine whether an analysis is appropriate and technically adequate to address the specific issue examined. The following HRA methods are compared and analysed in document [41]:

- Technique for Human Error Rate Prediction (THERP);
- Accident Sequence Evaluation Program HRA Procedure (ASEP);
- Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) Method;
- Cause-Based Decision Tree (CBDT) Method;
- Electric Power Research Institute (EPRI) HRA Calculator;
- Success Likelihood Index Methodology (SLIM) Multi-Attribute Utility Decomposition (MAUD);
- Failure Likelihood Index Methodology (FLIM);
- Standardised Plant Analysis Risk Human Reliability Analysis (SPAR-H);

- A Technique for Human Event Analysis (ATHEANA);
- Revised Systematic Human Action Reliability Procedure (SHARP1).

An important contribution to development of nuclear events investigation methodology is made by IAEA. ASSET, introduced in 1991 and then gradually replaced by PROSPER (initiated in 2000), methods developed by IAEA and supplemented by adequate services, are widely used in the nuclear industry and available to all countries with nuclear power plants under commission or in operation. The aim of these IAEA services is to provide advice and assistance to Member States to enhance the safety of nuclear power plants throughout their operational life cycle, from construction and commissioning to decommissioning. The ASSET method is developed for investigating events of high significance with related managerial and organisational issues. PROSPER is not actually an event investigation method; it involves self assessment and peer review of the effectiveness of the operational safety performance experience review.

2.1. Root cause analysis methods

What is RCA? Is it a methodology, method, tool or process? This question is not so simple, because even notable experts cannot agree on it. The most reasonable answer seems to be that RCA is a methodology – a set of working methods based on the same approach on a way of thinking through why things go wrong [54]. It is applicable anywhere and under any circumstances. RCA methods are the particular realisations of RCA methodology representing the various approaches to conducting RCA. These methods have various rules embedded in their approaches and use one or more tools. Rules provide the discipline for following their RCA methodology. Following these rules provides guidance for the user in adhering to the discipline of the method in the hope of a successful outcome. Many users think of the RCA tools as being the RCA methods, but that is not the case. The tools are merely vehicles to implement the method. These tools, be they manual (paper-based) or electronic (software-based), embed the rules from the different methodologies.

Historically, the RCA process has been in use for centuries under a variety of names [138]. As a discipline, root cause analysis has its origins in the nuclear branch of the US Navy [104]. Most of the early root cause analysis methods were developed through collaboration between nuclear Navy personnel and staff at the Atomic Energy Commission (AEC, today called the Nuclear Regulatory Commission or NRC), who were concerned with the design, operation, maintenance and fuelling of naval nuclear reactors. From 1980 to 1990 root cause analysis methods were found to be very effective in analysing specific accidents, and RCA began to creep beyond the field of nuclear operations into the general body of knowledge used by safety professionals in different spheres of human activity. During the last two decades RCA has emerged as one of the common methodologies that can benefit quality, environmental, health and safety practices.

To solve a problem, one must first recognise and understand what is causing it. If the real cause of the problem is not identified, then one is merely addressing the symptoms and the problem will continue to exist. For this reason, identifying and eliminating root causes of problems is of utmost importance [51, 94, 110]. Root cause analysis could be defined as the process of identifying causal factors, using a structured approach and methodology, with adequate methods, tools and techniques, designed to provide a focus for identifying and resolving problems [7].

The general logic of RCA follows the classical process: define the undesired outcome, define the analysis requirements, gather data, analyse data, form conclusions, check conclusions, and recommend corrective action [110, 138]. The theory behind root cause analysis is deceptively simple: event based problems are solved by eliminating or mitigating at least one cause. ‘Event based problem’ means a series of events (conditions, actions, triggers, etc.) that culminated in an unwanted outcome. In some cases, added layers of protection are provided as a means to control or mitigate causes. The effectiveness of a solution depends on several factors, such as the degree to which it prevents recurrence and the cost of the solution. Based on this theory of controlling causes, it can be seen that the more we understand the causes of an event based problem, the better we can control it. The key similarity between all root

cause analysis methods is recognition that controlling causes translates into controlling the problem. Apart from this, RCA methods vary greatly [29].

In general, a root cause analysis repeatedly asks the question ‘Why?’ about the events and conditions that caused or contributed to the event or human performance problem. Once the evidence has been gathered and the important causes for the event or human performance problem have been identified, the root cause analysis then looks for any relationships among the causes. The root cause analysis determines whether the causal factors demonstrate any order or precedence, in terms of either time or scope of effect. If one causal factor preceded another in time and affected it, or if a causal factor accounted for more than one of the human errors that occurred in an event sequence, or among those comprising an adverse human performance trend, it is a candidate root cause. The goal of the analysis is to determine which causal factor(s), if corrected, would prevent (or minimise the risk of) the recurrence of the same and similar errors.

When starting the investigation, definition of the basic concepts is of utmost importance, because ‘you will always find what you are looking for’. However, here the confusion starts: there are no universally accepted standards for RCA. You can call any event based problem solving methodology a Root Cause Analysis, and you are correct. In the absence of an accepted standard or specification, root cause analysis is anything that anybody wants it to be. For the same reason, you can call any cause of a problem a ‘root cause,’ and you are correct. An opinion exists, that the root cause is a myth [60]. Is ‘Root Cause Analysis’ really an appropriate phrase? Seeking the ‘Root Cause’ seems to be an endless exercise because no matter how deep you go there’s always at least one more cause you can look for.

Lack of the common agreement of definitions and concepts within the field of accident investigation (especially regarding the notion of *cause*) leads to a confusion of ideas and makes the comparison of different methods, tools and techniques difficult [54, 56, 68]. Some specialists even recommend avoiding the word *cause* in accident investigations and instead talking about what might have prevented the accident. As a good illustration of such confusion, we may use some of the existing variety of definitions of root cause:

1. Root Causes are the most fundamental reasons for an incident or condition, which if removed will minimise the risk of recurrence of the incident or condition [Conger, 24].
2. A Root Cause is the fundamental cause of an initiating event, correction of which will prevent recurrence of the initiating event (i.e. the root cause is the failure to detect and correct the relevant latent weakness(ess) and the reasons for that failure) [IAEA, 37].
3. Root Cause: any cause in the cause continuum that is acted upon by a solution such that the problem does not recur [Gano, 25].
4. Root causes are specific underlying causes, which can reasonably be identified, controlled to fix by management and those for which effective recommendations for preventing recurrences can be generated [Rooney, 13].
5. It is a myth which mistakenly focuses on finding root causes prior to finding solutions; even usage of the word cause should be avoided in accident investigations; people should rather think and talk about what might have prevented the accident [Gano, 60].
6. A Root Cause is the most basic cause (or causes) that can reasonably be identified that management has control to fix and, when fixed, will prevent (or significantly reduce the likelihood of) the problem’s recurrence [Paradies, 20].
7. A Root Cause is the absence of a best practice or a failure to apply knowledge that would have prevented the problem [Paradies, 110].

Despite the abundance of definitions, no one of them is perfect. For example, the first definition seems to be quite logical; however, it stresses that there should be several root causes, not one. But in that case, all of these root causes should be removed to minimise the risk of recurrence of the incident or condition. Such a recommendation seems not very practical, and the distinction between ‘root cause’ and ‘cause’ is lost. Definition (2) lacks clarity and concreteness, because some other undefined terms are used for explanation, and the requirement ‘to prevent recurrence of the initiating event’ completely seems to be unrealistic. Definitions (4, 6) state that only those causes which ‘can reasonably be

identified, controlled to fix by management' could be defined as root causes; this implies that root causes could only be found at levels below management; moreover, only this cause could be called a 'root cause', for which effective recommendations for preventing recurrences can be generated (definition 4). However, later it will be shown that (according to statistics and the opinions of numerous investigators) frequently root causes lie just inside management, and only improvement in management could help to prevent (or significantly reduce the likelihood of) the problem's recurrence. Lack of concreteness as well as the requirement 'to prevent recurrence of the event or problem' seem to be shortcomings of definitions (3, 7).

For most situations which arise within an organisational context, there are multiple approaches to resolution. These various approaches generally require different levels of resource expenditure to execute. And, due to the immediacy required in addressing most organisational situations, there is an inclination to opt for the solution which is the most expedient in terms of dealing with it. In doing this the tendency is generally to treat the symptom, rather than the underlying fundamental problem that is actually responsible for the situation occurring. Yet, in taking the most expeditious approach and dealing with the symptom, rather than the cause, what is generally ensured is that the situation will, in time, return and need to be dealt with again.

A true RCA process should include the following essential elements [56]:

1. identification of the real problem to be analysed in the first place;
2. identification of the cause-and-effect relationships that combined to cause the undesirable outcome;
3. disciplined data collection and preservation of evidence to support cause-and-effect relationships;
4. identification of all physical, human and latent root causes associated with the undesirable outcome;
5. development of corrective actions/countermeasures to prevent the same and similar problems in the future;
6. effective communication to others of lessons learned from analysis conclusions.

An effective and reliable RCA process additionally must provide three essential qualities [158]:

1. It must take advantage of people's knowledge while preventing their biases from controlling the direction of the investigation.
2. It must depict the facts of the case so that the causal relationships are clear and the causal relevance of those facts can be verified.
3. It must also help the analyst and management understand what actions must be taken to implement potential solutions and who in the organisation needs to take those actions.

Numerous methods of root cause analysis, many having a similar basis, have been developed or are under development to address the connection between root causes and corrective actions. Since there is no single best technique for use for all events, selection of the most appropriate tool for use for the event in question is often a fairly complex problem. Below is a non-exhaustive list of some of the most popular and commonly used RCA methods in the nuclear industry, supplemented by some relatively new but potentially useful methods employed in other industries (see Figure 2.1.1):

1. HPES (human performance enhancement system);
2. MORT (management oversight and risk tree);
3. ASSET (assessment of safety significant event team);
4. Methods, derived from HPES: K-HPES, J-HPES, UK-HPES, HPIP, MTO, AEB, PRCAP, CERCA, CAS-HPES;
5. SOL – Safety through Organisational Learning;
6. TRIPOD;
7. STEP;
8. Remedy-oriented RCA system (Takano, Japan)
9. HF - Compatible RCA method (GRS, Preischl, Germany);
10. 3CA - Control Change Cause Analysis;
11. FRAM;
12. CAS-HEAR;
13. Reality charting (Apollo root cause analysis);

14. Other RCA related methods.

HPES is a comprehensive RCA method designed specifically for investigation of events in nuclear facilities involving human factor related problems, and is widely distributed within the nuclear industry. Due to numerous advantages confirmed by practice many other methods similar to HPES have been developed and adapted as necessary by different individual organisations for their specific needs and requirements, for example: HPIP (HPEP) by the USNRC, MTO by the Swedish NPP operators, K-HPES by the Korean NPP operators, J-HPES by the Japanese NPP operators, and UK-HPES by the United Kingdom NPP operators. Such methods as MTO, AEB, PRCAP, CERCA, CAS-HPES can also be attributed to this group. Therefore, for the purposes of a strengths and limitations review, these methods can be considered to generally fall into one 'school' of approach.

The common objective of all these methods is to determine: a) what was expected; b) what has happened (real consequences); c) what could have happened (potential consequences); d) cause-effect relations; e) faulty/failed technical elements (structures, systems or components); f) failed or missing barriers; g) inadequate procedures; h) inappropriate actions (human, management, organisational); and subsequently to identify: direct causes, contributing factors, root causes, common causes, lost opportunities, and recurrent causes from previous events.

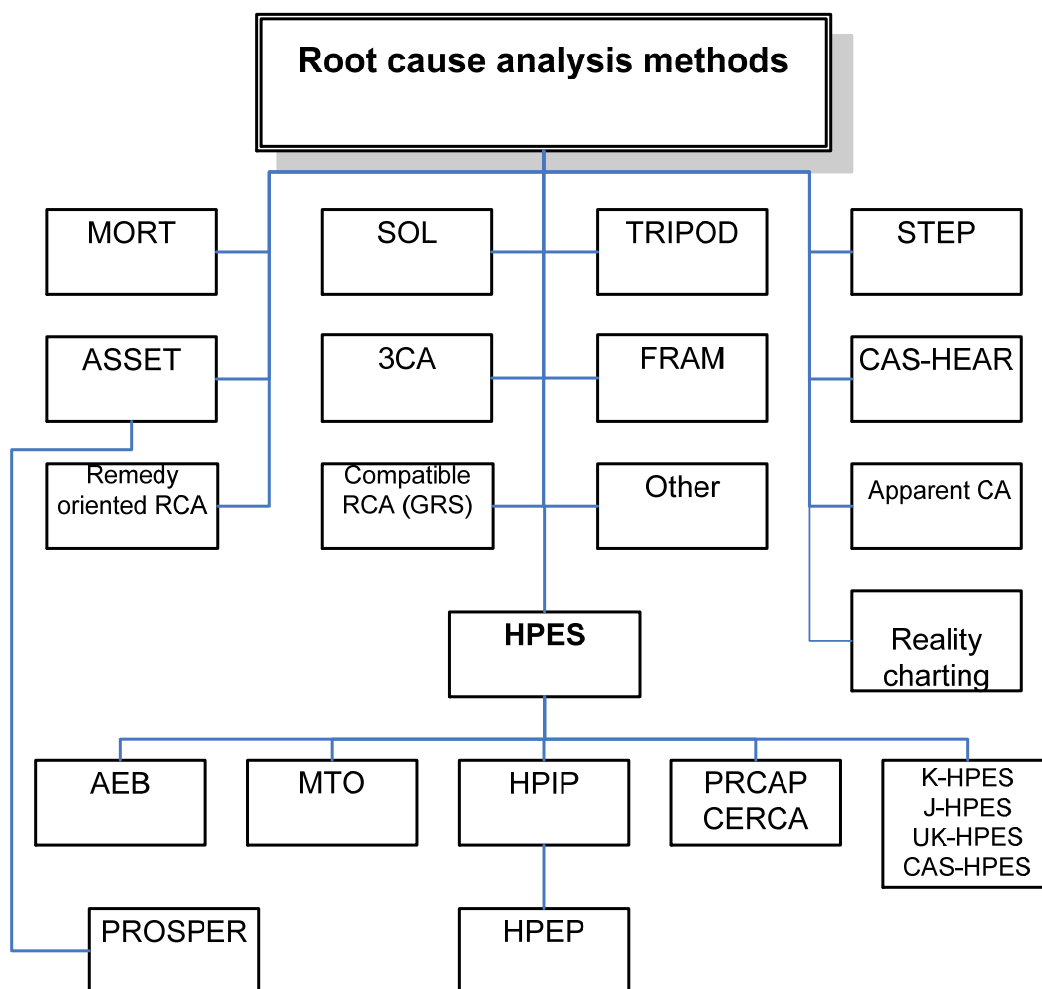


Figure2.1.1. Some most popular and commonly used RCA methods in the nuclear industry, supplemented by some relatively new but potentially useful methods employed in other industries

In parallel with the RCA methods listed above, the method named Apparent Cause Analysis should be considered. This method, prevailing in some utilities, is based on limited investigation, trying to quickly and simply determine the most immediate, or apparent cause of a less significant event or sub-standard

condition, without recourse to full root cause analysis, by considering the readily-available facts with little or no detailed investigation [1].

There are some instruments for regulatory oversight or peer review of OEF process based on event investigation methods. Such instruments, indirectly coherent with RCA methodology, are HPEP (human performance evaluation process) and PROSPER (Peer Review of the effectiveness of the Operational Safety Performance Experience Review process). Since, practically, HPEP and PROSPER are not designed for nuclear events investigation purposes, they are very important and useful for learning and understanding how the event investigation should be performed, and for further increasing the reliability of nuclear installations, because effective working methods, based on practical experience, are presented for evaluation of investigations of human performance problems, root cause analyses and corrective actions.

Conducting a Root Cause Analysis requires resources, so it is typically performed on events of high significance. According to IAEA documents [1, 111], events are classified in three categories: significant events, near misses and low level events. In the case of a significant event, a full root cause investigation can be conducted by an experienced individual trained in appropriate root cause analysis techniques, or for more complex issues by a multidisciplinary team containing a trained root cause analyst. In the case of near misses and low level events, an Apparent Cause Analysis or simple investigation may be conducted to determine the apparent cause of the event. All events (including near misses and low level events) are used for to establish trends. Consideration of trends in events over a period of time may identify common cause events that warrant a root cause analysis.

The criteria to determine the level of an event are taken from the organisation's technical specifications and supporting procedures. All incidents are screened against some pre-defined categorisation system to determine the level of investigation necessary. While management may be able to use their discretion not to perform a root cause analysis on some events, these exceptions need to be carefully monitored to ensure that systemic programme weaknesses are not developed.

2.1.1. HPES - Human Performance Enhancement System

HPES is a method developed by Institute of Nuclear Power Operations (INPO) in 1990 [1, 2, 18]. It is designed specifically for investigation of events in nuclear facilities involving human factor related problems and is widely distributed within the nuclear industry. It is user friendly and makes extensive use of graphic representation.

HPES method utilises event and causal factor charting, in which the tools of barrier analysis, change analysis and cause and effect analysis have been graphically incorporated into the same chart. The integrated chart shows the direct causes, the root causes, the contributing causes, and the failed barriers, with their interconnections and dependencies. Although valid for all types of issues (technical, procedural, etc), the methodology is oriented to enhancing the identification of human performance issues. A human performance specialist is recommended to be part of the team. Nevertheless, due to its systematic approach, the methodology can be used effectively by non specialists after a short practical training. The event investigation team members' proficiency in the technique is maintained by training, using the method frequently and participating in investigation teams.

The HPES method is a systematic process to guide the event investigator first to understand **what** happened before attempting to understand the causes. To understand the mechanism of human performance (or the individual's behaviour) during the event it is necessary to find out **how** the event happened. To find the causes, it is determined **why** the behaviour occurred and what additional factors contributed to the event. This is achieved by the coherent performance of several steps.

1. Task analysis. One of the first priorities when beginning an event investigation is to determine as much as possible about the activity that was being performed. This requires a review of work documents, logs, technical manuals and other documents, in an effort to determine what the task was about and how it was performed. Task analysis can be carried out using paper and pencil, when the task is broken down into sub-tasks identifying the sequence of actions, instructions, conditions, tools and materials associated with the performance of a particular task. Otherwise, in walk-through task analysis,

personnel conduct a step-by-step walk-through of the actions required for the performance of a task for an investigator, without actually performing the task. In both variants of the analysis, the investigator records each step of the task and notes any discrepancies or problem areas.

2. Change analysis. The purpose of this step is to explore the potential affective changes which might be contributory to the event. The analysis process consists of six sub-steps in which the situations before and after the event are compared and the differences are set down:

- Analyse the situation containing the inappropriate action.
- Analyse a comparable situation that did not have an inappropriate action.
- Compare the situation containing the inappropriate action with the reference situation.
- List all differences whether they appear to be relevant or not (seemingly insignificant differences can work together to cause events).
- Analyse the differences for effect on causing the event.
- Integrate the information relative to causes into the investigation process.

3. Barrier analysis. During an HPES investigation, the investigator should think in terms of barriers and identify all applicable physical and administrative barriers (controls) which are in place to protect the equipment and personnel, and determine what barriers (e.g. procedure) failed, allowing the event to progress. It should then be determined how (e.g. procedure not used) and why (e.g. procedure not considered necessary) the barriers failed.

4. Events and causal factor analysis. An event and causal factor chart (ECFC) is a graphically displayed flow chart of an entire event illustrating barriers, changes, causes and effects; it shows how these were involved in a human performance problem. The structure of the ECFC is illustrated below (Figure 2.3). The basis of an ECFC is the sequence of events plotted on a time line. The actions or happenings, **primary events**, directly leading up to or following the inappropriate action are shown in rectangles on the primary event line. Events not directly involved in the situation, **secondary events**, are shown below or above the primary event line. Each primary or secondary event must describe a single action or happening which can be described by a short sentence with one active noun and one active verb. Undesirable primary events which were critical for the situation being analysed are called **primary effects** and are shown as diamonds. The ECFC is completed by integrating the results of the change analysis and the barrier analysis on the graph.

For each primary event and primary effect the conditions are examined which allowed or forced it to occur. Conditions are circumstances pertinent to the situations that may have influenced the course of events. The conditions (causes) are placed on the chart (in ovals) showing their relationship to the effect. For each identified condition, the question is asked, why that condition existed, i.e. the condition is treated as an effect and the causes are determined. This cause-and-effect process is repeated until:

- the cause is outside the control of the plant staff;
- the cause is determined to be cost prohibitive;
- the primary effect is fully explained;
- there are no other causes that can be found that explain the effect being investigated;
- further cause and effect analysis will not provide further benefit in correcting the initial problem.

The HPES Causal Factor Work Sheets provide guidance for performing the cause-and-effect process and for determining the actual causal factors and root causes of the event. The identified root and contributing causes should meet the criteria that correction or elimination of the causes will prevent recurrence of similar conditions.

Based on each root cause and failed barrier, the corrective actions are identified. The corrective actions must meet the adequacy and feasibility criteria and should be checked by answering questions:

- Will the corrective actions prevent recurrence of the event?
- Is the corrective action within the capability of the utility to implement?

This method is used mostly for significant events. The HPES system is useful to help question potential contributing causes that may initially be outside the mindset of the investigator. A full analysis typically

requires 200-300 human resource hours on average. Lower level events can be investigated in a simplified format with fewer resources [3, 18].

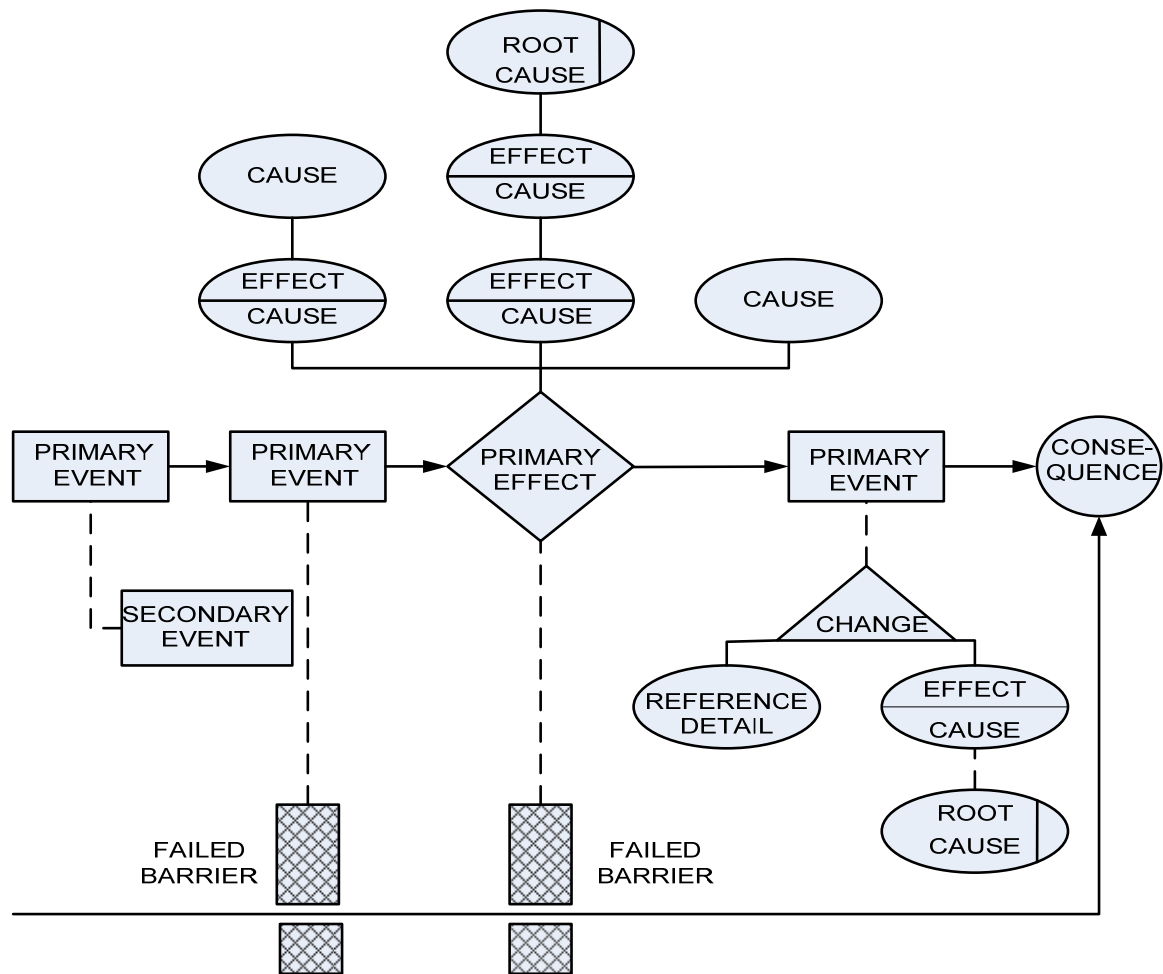


Figure 2.1.2. Structure of an event and causal factor chart (ECFC)

Strengths

- While the main focus is on human factors, it has been demonstrated that it can be applied equally to equipment and design related issues.
- It is a systematic approach which can be used by non-human factors specialists to give consistent results following a limited period of training and practice in the methodology.
- The event and causal factors charting is a powerful tool for presenting the event genesis, root cause development, and failed barriers in a concise and easily understood format.
- Corrective actions which address the root causes can be easily developed from the event and causal factors chart.
- Involvement of NPP line management in corrective action identification has proved effective in improving 'ownership' by line managers for corrective actions in their area.
- It is an effective instrument for the investigation of individual events, with a proven track record at many NPPs.
- It can be used flexibly or in a shortened format if required. This is particularly useful for 'apparent cause' analysis of near miss or low level events for subsequent use in significant event precursor trending.
- It has proved effective in identifying training and knowledge weaknesses whenever they are contributing factors to events.

- It can be used proactively to identify and correct ‘error-likely’ conditions and situations before they result in events.
- Identification of specific root causes and causal factors by coding allows for easy identification of trends in event contributing factors.

Limitations

- Organisational and managerial factors are not strongly supported by the method. It can be difficult to target management weaknesses from a single event investigation.
- The application of the whole process can be time consuming, particularly in the area of interviews of personnel. Such interviews can be difficult, especially if there is no ‘blame tolerant’ culture in place. However, it has been shown that continued use of HPES in some plants has promoted development of a healthy blame-tolerant environment.
- To maintain effectiveness, trained investigators need to practise investigation skills routinely. Corrective actions depend on the experience of the analyst (as for many other methodologies).

The HPES and associated methods have now been adopted by many countries and organisations. The approach has been proven to be practicable and successful across a broad spectrum of NPP operators and cultures, having been adapted where necessary to meet local needs. Its limitations in the managerial and organisational areas have been addressed by those organisations which are increasing their focus on these issues. A more comprehensive description of HPES methodology is presented in the document [18].

2.1.2. MORT - Management Oversight and Risk Tree

The Management Oversight and Risk Tree (MORT) method is an analytical procedure for inquiring into causes and contributing factors of accidents and incidents [21, 24, 149, 150]. The MORT method reflects the key ideas of a 34-year programme run by the US Department of Energy to ensure high levels of safety and quality assurance in its energy industry. The MORT programme started with a project documented in SAN 821-2, W.G. Johnson, February 1973.

MORT is a method originally developed for analysing events of nuclear safety significance for which organisation and management issues are apparent, and was later adapted for more general accident investigation and safety assessment. The MORT method is a logical expression of the functions needed by an organisation to manage its risks effectively. These functions have been described generically; the emphasis is on ‘what’ rather than ‘how’, and this allows MORT to be applied to different industries. MORT reflects a philosophy which holds that the most effective way of managing safety is to make it an integral part of business management and operational control.

According to the philosophy of the MORT system, an accident is caused by an energy flux which is not controlled in the right way by adequate barriers and/or control upon the unwanted energy transfer. It is based on developing the analysis through several interconnected fault trees, each one representing a domain of investigation, and filling in the fault trees using a predetermined check list. A predetermined checklist of around 100 generic problems and 200 basic causes is utilised. The implementation of this method presents a certain complexity, which requires expert users, with relatively high expenditure on human resource hours and other resources for the investigation. Some versions of this technique have been registered as a commercial product and are supported by software to expedite the diagnosis.

The MORT method is realised using the three steps procedure:

Step 1: define the events to be analysed;

Step 2: characterise each event in terms of unwanted transfers of energy;

Step 3: evaluate the hypothesis that the unwanted transfers of energy were the result of how risks were being managed in the activity in which the accident occurred.

Step 1 is supported using a procedure called Energy Trace and Barrier Analysis. In this step the analyst tries to identify a complete set of events comprising the incident or accident, and to define each event

clearly. It is very difficult to use MORT, even in a superficial way, without first performing an Energy Trace and Barrier Analysis.

In Step 2, the analyst looks at how the energy was exchanged with the person or asset. This way of characterising accidents – as a series of ‘energy exchanges’ – was proposed as a means of analysing accidents scientifically. There may be several different energy transfers that need to be considered in the same investigation. In this step, the analyst aims to understand how the harm, damage or danger occurred.

In Step 3, the analyst considers how the activity was managed. This step involves the analyst looking at the ‘local’ management specific to the activity and resources. The analyst also looks ‘upstream’ to find management and design decisions about people, equipment, processes and procedures that are relevant to the accident. To help make this analysis systematic, the analyst uses the MORT chart (Figure 2.1.3); this lists the topics and allows an analyst to keep track of their progress.

Each topic on the MORT chart has a corresponding question in the set of questions provided in advance [21, 24]. The questions in MORT are asked in a particular sequence, one that is designed to help the user clarify the facts surrounding an incident (Figure 2.1.4). The analyst, focused on the context of the accident, identifies which topics are relevant and uses the questions in the manual as a resource to frame their own inquiries.

Like most forms of analysis applied in investigations, MORT helps the analyst structure what they know and identify what they need to find out, mostly the latter. The accent in MORT analysis is on inquiry and reflection by the analyst [11, 21, 24].

Strengths

MORT is a proven method, and free to use. It looks to the whole management structure, uses a detailed fault tree and gives up to 1 500 potential causal factors. MORT uses barrier analysis and identifies the assumed risks taken by management. Computerised versions are available.

Limitations

- It is perceived by some to be complex, costly and time consuming due to extensive task analysis.
- As with other event investigation methods, MORT requires more training and experience for proficient use.
- Some versions of MORT and appropriate software are a commercial product that is only available for a fee.
- It is not appropriate for use by NPP staff in routine investigations.

A detailed description of the MORT methodology is provided in the document [21].

A simplified modification of MORT Safety management organisation review technique (SMORT) has been developed in Scandinavia [21, 45]. This technique is structured by means of analysis levels with associated checklists, while MORT is based on a comprehensive tree structure. Owing to its structured analytical process, SMORT is classified as one of the tree based methods.

The SMORT analysis includes data collection based on the checklists and their associated questions, in addition to evaluation of results. The information can be collected from interviews, studies of documents and investigations. This technique can be used to perform detailed investigation of accidents and near misses. It also serves well as a method for safety audits and planning of safety measures.

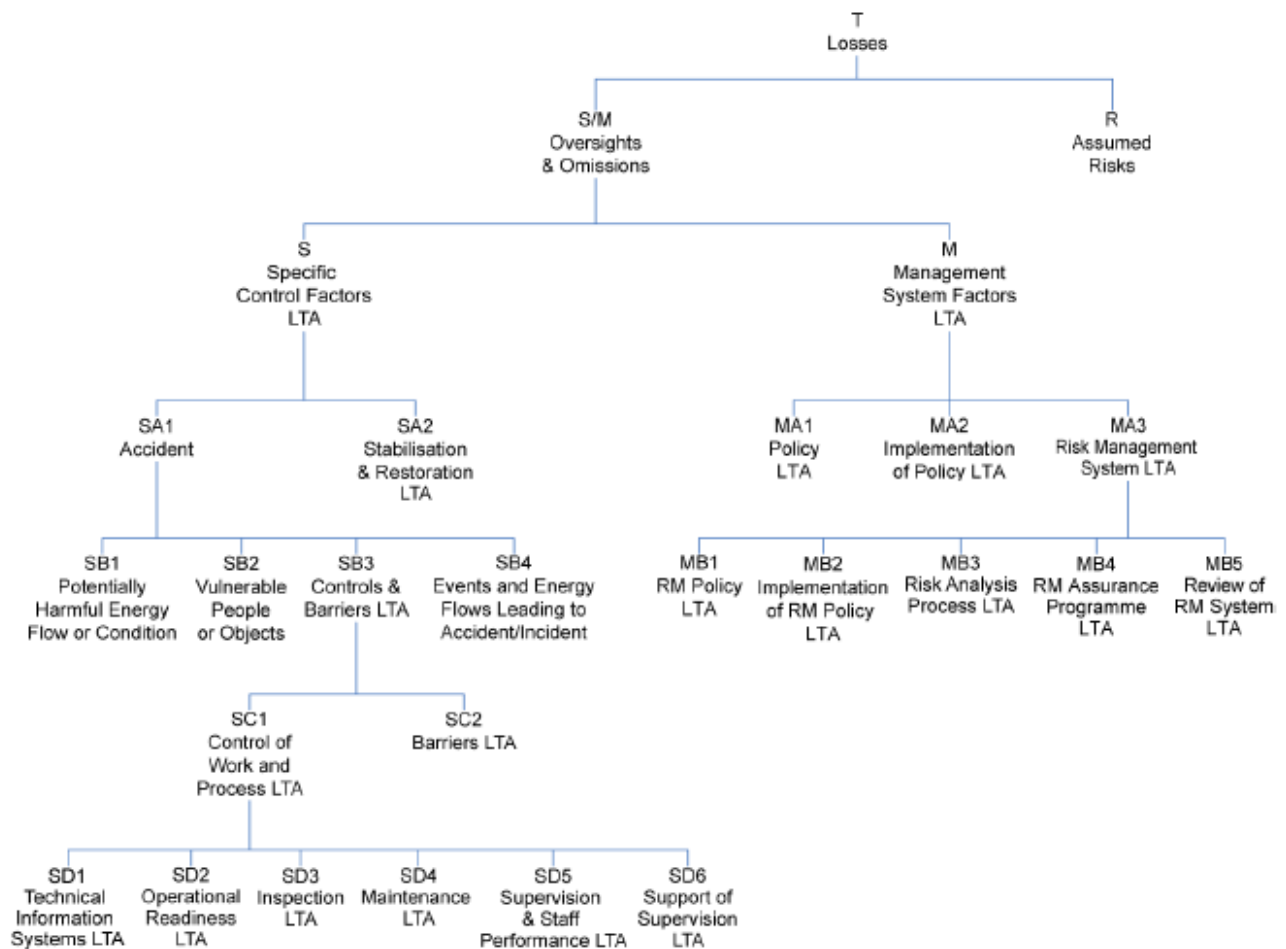


Figure2.1.3. Main Branches of the MORT Tree

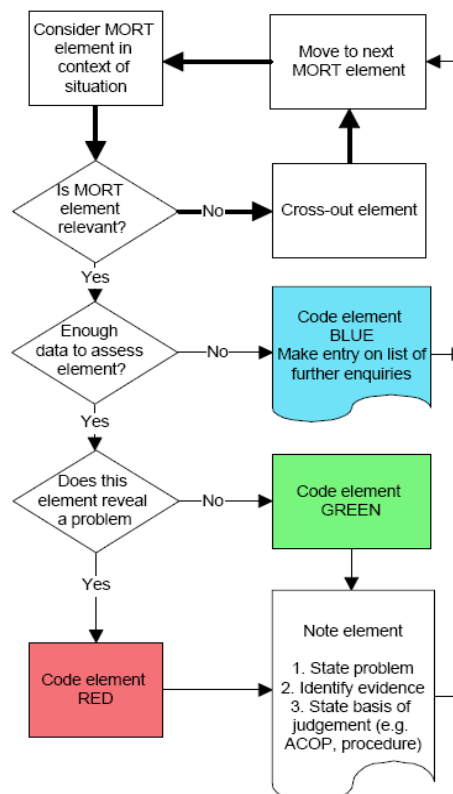


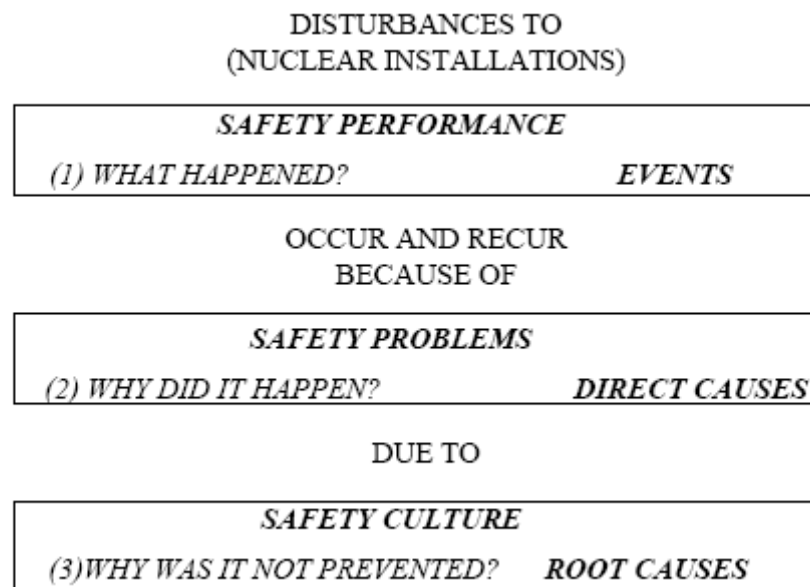
Figure2.1.4. Sequence for work through the MORT Chart

2.1.3. ASSET - Assessment of Safety Significant Event Team

ASSET is an IAEA method developed in 1991 for investigating events of high significance with related managerial and organisational issues. Issues and corrective actions identified by ASSET are often at a high level, more applicable to management policy and philosophy, and of a generalised nature [1, 2].

According to the ASSET method, the work process at a nuclear power plant has three basic elements: people, procedures and equipment. The reason for an error in the performance of the work process must be a deficiency in one, or several of these basic elements. The ASSET approach is based on the logic that events always occur because of a failure (of people, procedures or equipment) to perform as expected, due to a latent weakness (direct cause) which was not eliminated at the appropriate time due to deficiencies in the plant surveillance programme (root cause). In ASSET analysis, the event is broken up into logically connected occurrences which can be attributed to a single failure of either people, procedures or equipment, and the direct cause and root causes of each occurrence are identified to determine the corrective actions which will eliminate the direct cause and root causes.

The basis of the ASSET root cause analysis of an event is the following philosophy [3, 28]. Events result from preceding occurrences due to latent weaknesses that were not prevented by quality control, nor by preventive maintenance, and that were not discovered by plant surveillance and/or not covered by a feedback programme. An occurrence exists when any element of equipment, personnel or procedure fails to perform as expected. The root cause analysis is applied to an event, defined as a reportable failure. In this context, the term 'reportable' may be used for events reported which are internal or external to the plant and its headquarters, and for mandatory reporting of significant events to the supervisory authorities. Most events are preceded by one or more occurrences, in each of which a single element (of equipment, personnel or procedure) failed to perform as expected. The fundamental approach to the ASSET method is shown in the following diagram [3]:



According to ASSET, the objective of the root cause analysis is to establish exactly what happened and why, so as to contribute to the prevention of repetitious events. The root cause analysis is a process with three phases, namely:

- Investigation: the determination of what exactly happened, the identification of all the occurrences making up the event and their temporal and logical relationships;
- Analysis: the analysis of selected (or all of the) occurrences;
- Formulation of recommendations: the identification of corrective actions on which to base recommendations.

INVESTIGATION

The purpose of the investigation phase is to obtain a clear, logical picture of what happened in the period leading up to, as well as during, the event. The information required to build up this logical picture is derived from a range of sources, some of which are listed below:

- station operating log;
- plant control log;
- workshop logs and journals;
- fire team logs (for fire events);
- fire team incident reports (for fire events);
- event reports (may be several at different times of origin);
- investigation reports (may be several, each concerning specific areas of plant or activity);
- interviews with plant personnel involved, either directly by the analysts or from transcripts taken during other parts of the investigations/inquiries;
- plant inspections;
- plant safety analysis report and technical specifications;
- construction, installation, maintenance records, etc.

The prime source of information is the discussion between the investigation team members and their plant counterparts. It is thus very important to establish the rules of engagement. The investigation team members should stress the importance of establishing a blame-free culture in the context of promoting a good safety culture. It should be pointed out that there is no interest in blaming individuals or groups of individuals. There must be an open flow of information in order to establish exactly what happened.

The outputs of the investigation phase are:

1. A title for the event, indicating the nuclear safety implications of the event as well as the apparent lack, failure or deficiency that was involved.
2. A descriptive narrative a structured record of the event as derived from the investigation. From the narrative the reader should be able to understand how the event unfolded in time and in logic. Short sentences or statements increase clarity. It should be easy to identify the individual occurrences, to find out what element failed and the nature of the failure. The occurrences should be identified on the basis of narrative. ASSET uses the term ‘occurrence’ to describe the situation in which an element of equipment, personnel or procedure failed to perform as expected. The standard for what is expected is derived from the relevant specifications, e.g. design specifications and acceptance criteria for equipment and systems, work specifications and procedures for operational and maintenance work, training specifications and acceptance criteria for personnel and scope, and style and quality specifications for procedures. The narrative is complete when it does not leave questions unanswered and when it gives a complete picture of the event in terms of the time sequence of the occurrences and of the equipment, procedures and personnel involved.
3. A chronological list of occurrences, based on the narrative. It is important to identify quite closely which person or group of persons failed to perform as expected. This is because later in the analysis corrective actions in the shape of training and refresher courses will be discussed, and it will be necessary to know to which category the person(s) who failed to perform as expected belonged. Also, part of the corrective measures will be directed towards the individual(s) who failed which makes it necessary to identify the person concerned. Personal names, however, should not be included in a root cause analysis report. The chronological order of occurrences is just another aid, like the title of an event and the narrative, to make sure that the correct picture of the event has been established. If it is difficult to put the identified occurrences in the right order, there might still be some information missing in the narrative.
4. A logic tree of the occurrences which make up the event. This is a schematic diagram, illustrating the logical sequence in which the event unfolded and the logical relationships

between the individual occurrences which make up the event. An example of a logic tree of occurrences is shown in Figure 2.1.5. Constructing the logic tree the following are noted:

- The earliest occurrence is shown at the bottom of the tree and the 'event' is at the top.
- Two or more occurrences are shown in parallel if the succeeding occurrence depends on the existence of all of them, i.e. the event would not have progressed further if one of the parallel failures had not happened.
- Single occurrences, or groups of parallel occurrences, are shown in series if the upper is a logical consequence of the lower. To make it obvious why occurrences in series logically follow one another, it is sometimes helpful to indicate the situation or state which exists between them. The occurrences are shown in solid boxes, while the situation or state is indicated in a dotted box.
- Arrowed lines are used to indicate the logical connection between occurrences (and conditions).
- The occurrences in the logic tree are numbered for identification purposes.
- The nature of the occurrences is preferably indicated in the right hand margin of the page presenting the logic tree. This can be only one of three possibilities: equipment, procedure or personnel. The only purpose of identifying the nature of an occurrence is to make sure that the right picture of the event has been created. If the nature of the event is not quite clear, some information is still missing and must be obtained.

ANALYSIS

The analysis is applied to some or all of the occurrences identified in previous phases. If only a selection of occurrences is to be analysed then a brief note regarding the reasons for selection should be made. Occurrences chosen for analysis should be those judged to have the most significance for nuclear safety or those which offer the best insights into the safety culture at the plant.

The ASSET analysis is in fact the process of completing the event root cause analysis form (ERCAF) shown in Figure 2.1.6. The essential elements are the identification of the direct cause and the root cause. The direct cause is the latent weakness in the element which failed. The root cause is either the reason why the latent weakness was not discovered before an in-service failure, i.e. a failure of the surveillance programme OR it stems from the inadequate restoration of a previously recognised latent weakness. The direct cause has contributors stemming from deficiencies in quality control and/or preventive maintenance programmes. The root cause has contributors which can only be deficiencies in the management of, or the policy for, surveillance and/or experience feedback.

FORMULATION OF RECOMMENDATIONS

For each occurrence analysed, corrective actions are suggested to eliminate the latent weakness identified, bearing in mind that prevention of repeated failures is paramount. For example, if a failed piece of equipment has, for some compelling reason, to be replaced by an identical piece of equipment, the corrective action should also address the frequency of maintenance and/or surveillance testing to prevent further failures. Similarly, if the occurrence involves personnel and the corrective action proposed concerns training or refresher training, attention should also be given to the frequency of refresher training and to end of training testing (pre-service qualification).

The recommended corrective actions relating to the contributor to the latent weakness should specifically address the quality issues identified in the analysis. The aim is that future quality control and maintenance activities will ensure that further failures are avoided. The corrective actions offered to address the root cause identified in the analysis should be specific enough to ensure that the latent weakness will in future be identified before an in-service failure and/or that restoration activities are of sufficient quality to reduce the probability of possible in-series failures in the future.

The contributors to the root cause lie in the formulation of policies and their execution. The outcomes of event investigation should include focused suggestions for improving policy and/or its implementation to ensure future effectiveness of surveillance.

The corrective actions to be entered in the right-hand boxes of the root cause analysis form should be both practically and economically feasible measures which support the organisation, its staff and management in the enhancement of the prevention of incidents. Because different levels in the organisation are addressed, it is important to include the appropriate levels of responsibility in defining these corrective actions.

Quality control, typically, is performed prior to operation, which means quality control after manufacturing of components and before they are stored for future use, examination of personnel after training and before they are allowed to perform their job, and validation of procedures before release for use at the plant. Effective quality control, preventive maintenance and surveillance require the availability of clear and comprehensive acceptance criteria as a reference point. Preventive maintenance is necessary to mitigate the degradation of the quality of equipment, procedures and personnel. Based on experience, on information from the manufacturers, and taking into account the acceptance criteria, structured programmes can be designed for periodic overhaul, cleaning and exchange of components and equipment, periodic checks of procedures, refresher courses of personnel, etc.

Quality control and preventive maintenance programmes deal with expected degradation. Unexpected weaknesses and unexpected degradation are guarded against by the deployment of surveillance programmes. If an event has occurred, it means that the surveillance programme has been deficient. The analyst must identify the specific deficiency and enter it in the appropriate box on the form.

As mentioned above, each occurrence relates to one latent weakness. However, the deficiencies in quality control, preventive maintenance, acceptance criteria and surveillance, and their corrective actions, usually have broader implications. In particular, policy and management aspects influence other areas in the prevention of incidents. This means that plant personnel, performing ASSET root cause analysis of many events, should produce corrective actions for each one of the identified latent weaknesses, but should combine the results of analysis of related events to create a comprehensive recommendation for corrective action in connection with quality control, preventive maintenance, acceptance criteria and surveillance. A similar course should be followed in formulating corrective actions regarding management and policy aspects.

Strengths

- Useful for investigation of generic events which are applicable to a large number of NPPs.
- Can be useful for investigating a single event of high safety significance which has related managerial and organisational aspects.
- Useful for retrospective review of a population of events where a trend of recurring problems has been identified.

Limitations

- Uses a different terminology and definition of root cause compared with other techniques.
- Because the method identifies deficiencies in management, organisation and higher policy issues, knowledgeable senior staff with practical experience is needed to perform the analysis.
- Issues and corrective actions identified by ASSET method are often at high level, more pertinent to management policy and philosophy, and of a generalised nature. This makes development of concise, measurable, and achievable corrective actions difficult.
- ASSET services are no longer supported by the IAEA, and hence training and further improvements for the ASSET method may no longer be available through IAEA [1, 2]

The ASSET method, when applied to discrete events of limited safety significance, develops root causes which are at the higher managerial levels, and as a result generate more global corrective actions. Such actions have been found to be difficult to implement due to issues relating to high cost and insufficient focus of ownership and accountability. Additionally, in such cases, the potential exists to reduce the impact and opportunity for learning from experience, if such global actions are transferred to other

utilities in the international event reporting forum. Existing experience indicates that the application of other available methods in this respect can be more effective than the ASSET method for discrete events.

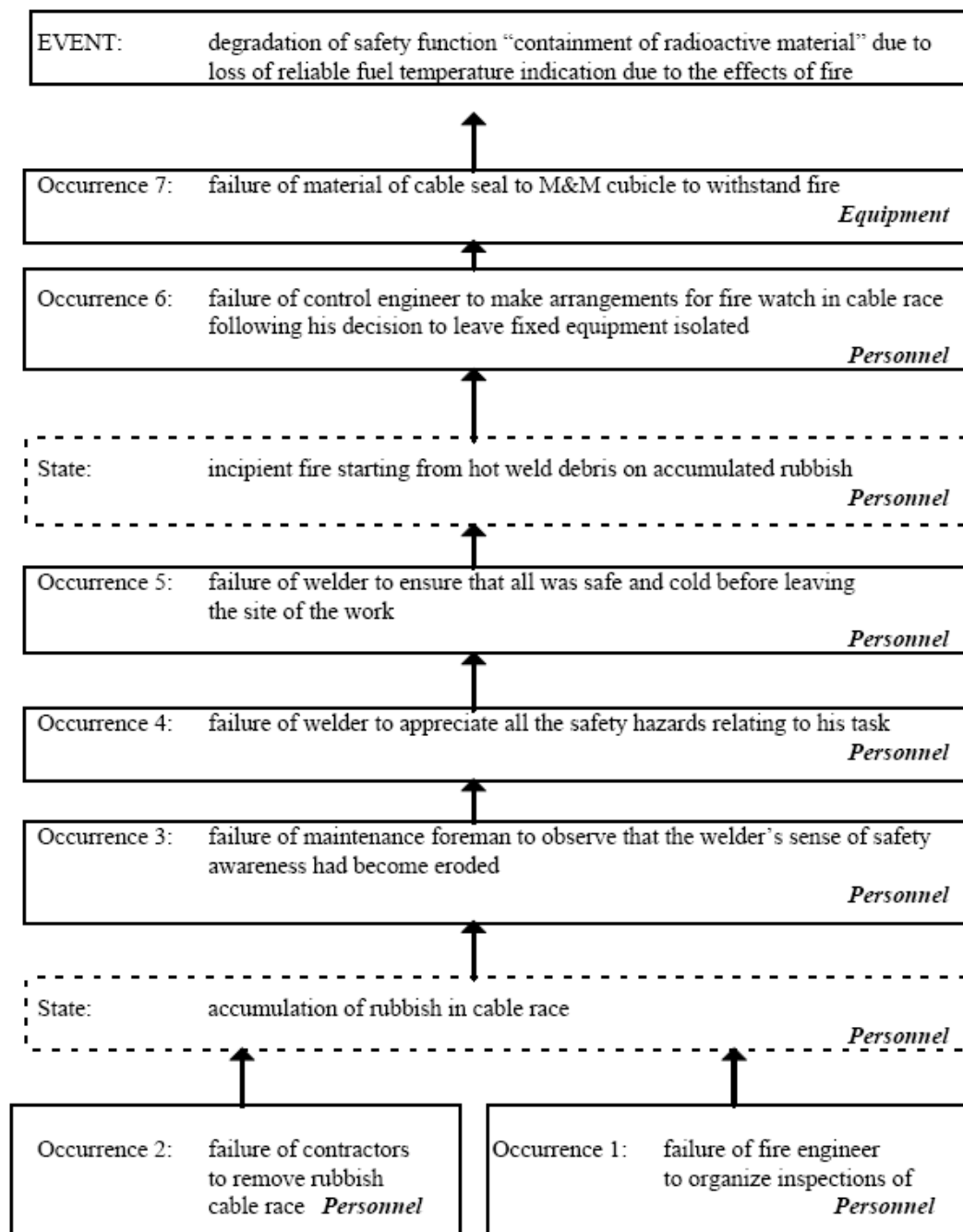


Figure 2.1.5. Example of logic tree of occurrences used in ASSET analysis [3]

IAEA		EVENT ROOT CAUSE ANALYSIS FORM		ASSET					
Event title:				Safety consequences due to initiating failure					
SAFETY PERFORMANCE: OCCURRENCE: What failed to perform as expected?				Corrective actions by plant					
Occurrence title:									
Nature of the failure		Personnel failure	Occurrence results from a failure during operation	Appropriate		Comprehensive		Implemented	
		Equipment failure	Occurrence results from a deficiency discovered by periodic testing						
		Procedure failure							
SAFETY PROBLEMS: DIRECT CAUSE: Why did it happen?			How to eliminate the problem? (Corrective actions by ASSET method)	Y e s	N o	Y e s	N o	Y e s	N o
Latent weakness of the element that failed to perform as expected				I					
Contributor to the existence of the latent weakness:				II					
Not qualified prior to operation. Poor quality control									
Qualification degraded during operation. Poor preventive maintenance									
SAFETY CULTURE: ROOT CAUSE: Why was it not prevented?			How to prevent recurrence? (Corrective actions by ASSET method)						
Deficiency in timely eliminating the latent weakness:				III					
Detection									
Restoration									
Contributor to the existence of the deficiency				IV					
Inadequate policy for:									
Surveillance									
Feedback									

Figure 2.1.6. Event root cause analysis form (blank) to be filled in result of ASSET analysis

2.1.4. RCA methods derived from HPES

To this group can be attributed the following RCA methods: HPIP, K-HPES, J-HPES, UK-HPES, HPIP; MTO, AEB, PRCAP, CERCA, CAS-HPES.

K-HPES is a Korean-version HPES developed on the basis of INPO-HPES in 1993. The development of K-HPES was an effort by KEPRI (Korea Electric Power Research Institute) to reduce human errors and to enhance human performance in nuclear power plants (NPPs), and the programme is currently being operated at all NPPs in Korea. KEPRI is now developing a computerised support system, tentatively named CAS-HPES (computer-aided system for HPES), which facilitates the K-HPES analyser in performing K-HPES analysis tasks [14].

2.1.4.1. HPIP - Human Performance Investigation Process

This process, called the Human Performance Investigation Process or HPIP, was developed to meet the particular needs of US NRC personnel for the identification of root causes of human performance problems [19]. HPIP leads the investigator through the technique to perform an in-depth investigation of human contributions to an event. HPIP combines current procedures and field practices, expert experience, human performance research, and the best applicable investigation techniques. This blending of experience and proven techniques results in a system that is intuitive, easy to learn and to use, and that helps event analysts to perform better field investigations of human performance problems. The Human Performance Investigation Process is a systematic method for investigations of nuclear power plant events that involve human performance issues. HPIP can be flexibly applied by the investigator, by choosing to use only the investigation techniques, forms, etc. that are needed.

The HPIP method is based on a simplified fault tree, and provides six investigative modules (procedures, training, verbal communications, organisational factors, human engineering, and supervision) for determining the root causes of human performance related events. There are six tools (techniques) that comprise a flexible HPIP procedure for identifying the root causes of human performance problems. These six tools are:

- Events and Causal Factors Charting
- SORTM (Stimulus, Operation, Response, Team performance, Management) a guide to HPIP Modules
- Barrier Analysis
- HPIP Modules
- Change Analysis
- CHAP - Critical Human Actions Profile.

The HPIP Flow Chart (Figure 2.1.7) portrays the process graphically and consists of three parts:

- The NRC HPIP Flow, which displays the steps used to investigate an event (centre column of the diagram);
- The Purpose of each major section of the process (left column of the diagram);
- The Tools which are the investigation techniques required to perform each major section of the process (right column of the diagram).

Some of the HPIP tools (Events and Causal Factors Charting, Barrier Analysis and Change Analysis) are universal; they are briefly outlined in chapter 3 of this report.

SORTM is a simple paper-and-pencil expert system that provides basic questions, similar to those that an expert human performance investigator would be expected to ask during an event investigation. These questions are presented as a Yes/No logic tree. SORTM ensures consistency in the breadth of contributors that are considered during an investigation. The answers to SORTM's questions lead the investigator to those human performance areas most likely to have contributed to human error during the accident / incident. SORTM, therefore, helps the investigator allocate investigation effort to those areas where the causes of human error are most likely to be identified.

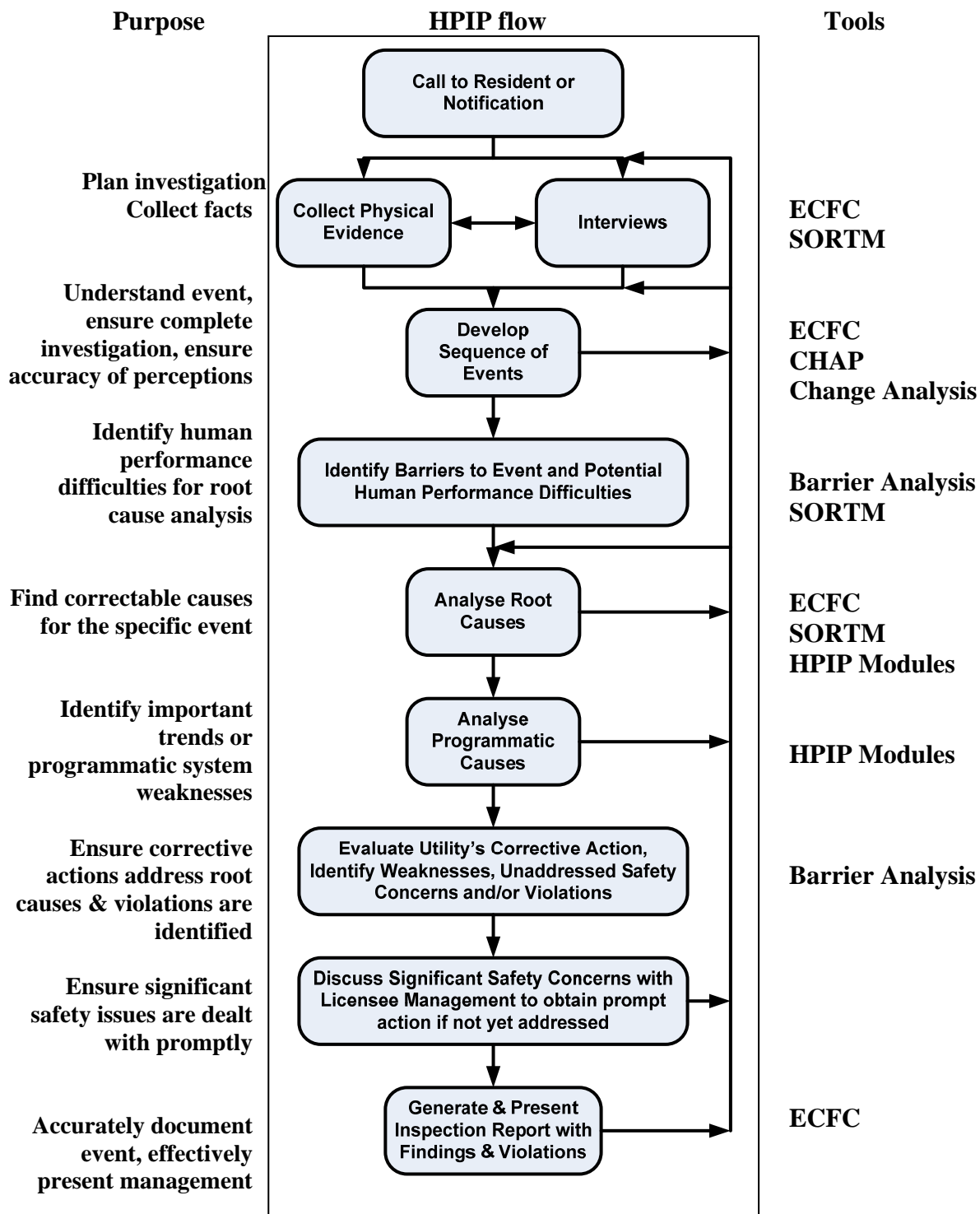


Figure 2.1.7. The HPIP flow chart [19]

The Critical Human Action Profile (CHAP) is an operationally oriented investigation technique, roughly based on the human factors technique of task analysis. An investigator using CHAP identifies and records all the critical human actions. A critical human action is one that, if performed correctly, could have prevented the event from occurring or could have significantly reduced the event's consequences. CHAP provides several techniques to help an investigator identify the critical human actions. The list of critical human actions can then be analysed using SORTM or, if special expertise is needed, the list can provide a starting point for investigation assistance by a human performance expert. CHAP does not

have to be used for every investigation, but should be used when identification of the causes of the event is difficult or controversial, when extremely complete documentation of the event is required, or when assistance from human performance experts is needed. HPIP offers the following **advantages** [22]:

- It is especially designed to meet regulatory needs;
- The methods of analysis of root causes are enhanced with the experience in human performance gathered by experts;
- It enables resident inspectors to make a preliminary assessment immediately after the occurrence of an event;
- Consequently, it strengthens communication with the support team, improving the systematisation of the investigation conducted and the evaluation to be made by the group;
- It allows the employment of different techniques of root causes analysis;
- Regulatory actions can be focused on safety conditions during operation and maintenance; therefore, the impact of human performance on the development of events can be more easily identified;
- It contributes to the identification of programmatic causes, which will be used to assess the corrective actions taken by the utility at the organisational level;
- As a result of the analysis, deterioration in the Quality/Safety Culture can be detected.

With respect to its application, this method presents the following **limitations**:

- Specific training of inspectors is needed. This aspect becomes significant in the trial applications of the method that will be carried out as part of this project, since it involves an additional effort on the part of the staff not included in the project;
- It can only be applied to aspects related to human performance; hence, to make a complete analysis of an event, other techniques have to be applied beforehand in order to detect its direct causes.

A more comprehensive description of HPIP methodology can be found in the document [19].

2.1.4.2. MTO - Man-Technology-Organisation Investigation

MTO (Man-Technology-Organisation Investigation) is a systemic theory with a focus on the interactions between people, technology and organisations. It is a modified version of the HPES method adopted by the Swedish nuclear industry. This method leads to the identification of root causes related to human and organisational factors. The MTO method uses three basic tools, relating to event and cause analysis, barrier analysis and change analysis. To structure the process events and causal factors flow-charts are used. MTO investigations are mostly used for significant events related to human and organisational factors. Proper training in the application of MTO is required to conduct an MTO investigation.

The basis for the MTO-analysis is that human, organisational, and technical factors should be focused equally in an accident investigation [62]. The essence of the MTO method is illustrated in Figure 2.1.8.

The MTO-analysis is based on the employment of three commonly used tools:

1. Structured analysis by use of an event and cause diagram;
2. Change analysis by describing how events have deviated from earlier events or common practice;
3. Barrier analysis by identifying technological and administrative barriers which have failed or are missing.

The first step in an MTO-analysis is to develop the event sequence longitudinally and illustrate the event sequence in a block diagram (see Figure 2.1.8 - the MTO-analysis worksheet). Then, the analyst should identify possible technical and human causes of each event and draw these vertically to the events in the diagram.

The next step is to make a change analysis, i.e. to assess how events in the accident's progression deviated from the normal situation, or common practice. Normal situations and deviations are also illustrated in the diagram below.

Further, there is an analysis of which technical, human or organisational barriers failed or were missing during the accident's progression. All the missing or failed barriers are illustrated below the events in the diagram. The basic questions in the analysis are:

- What may have prevented the continuation of the accident sequence?
- What may the organisation have done in the past in order to prevent the accident?

The last important step in the MTO-analysis is to identify and present recommendations. The recommendations should be as realistic and specific as possible, and might be technical, human or organisational.

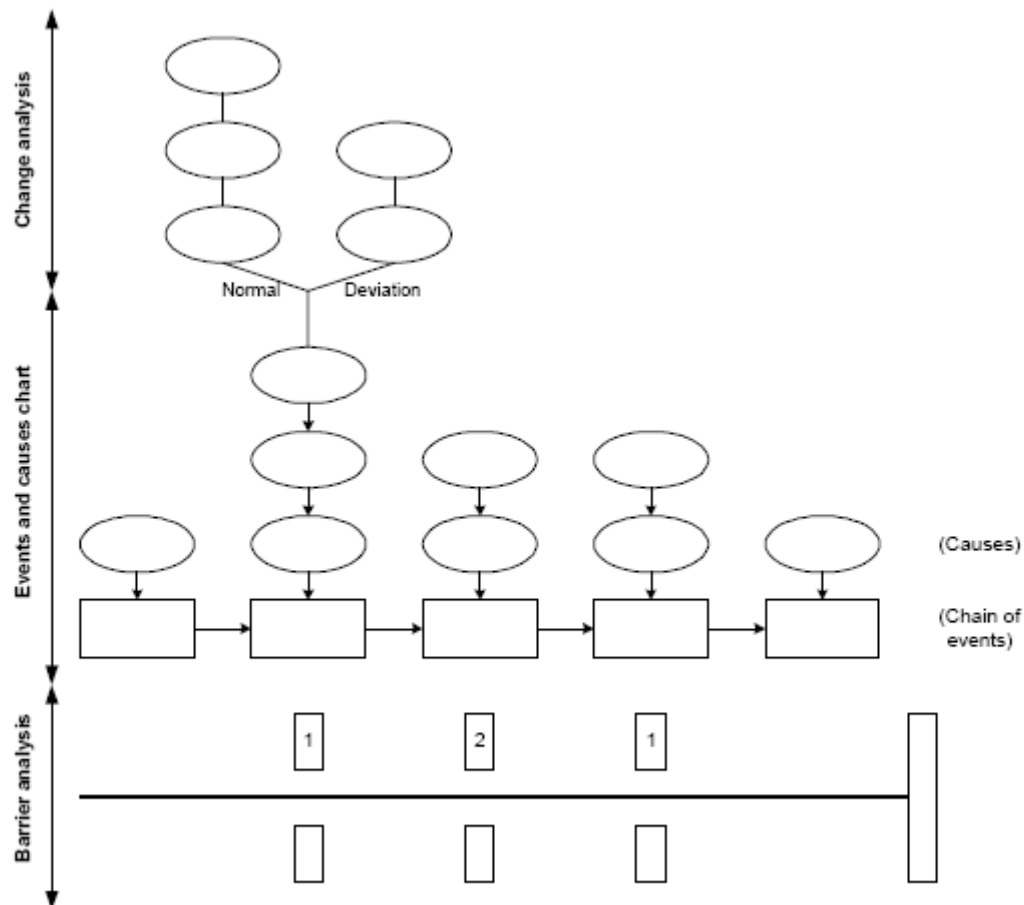


Figure 2.1.8. MTO-analysis worksheet [62, 68]

Strengths: Describes the context of event analysis in terms of necessary background knowledge and organisational structure. Has a strong connection to human factors.

Limitations: Limitations of specific techniques applied (i.e. barrier analysis, ECFC, change analysis) are apparent.

2.1.4.3. AEB - Accident evolution and barrier function

This method was developed by O. Svenson (1991) [114]. The AEB method models the interaction between human and technical systems. It consists of the narrative of the accident, the flow chart model of human and systems malfunctions, errors and failures, and barrier function analysis.

As a basic principle for classification in the AEB method, the evolution leading to an accident evolution is modelled as a chain or sequence of malfunctions, failures, and errors in human and technical systems [114]. With reference to this, a distinction is made between barrier functions and barrier systems. A barrier function represents a function (and not, e.g., an object) which can arrest the accident evolution so that the next event in the chain is never realised. Barrier systems are those maintaining the barrier

function. Such systems may be an operator, an instruction, a physical separation, an emergency control system, and other safety-related systems, components, and human factors organisational units [114]. More generally, a barrier function can be defined as the specific manner by which the barrier achieves its purpose, whereas a barrier system can be defined as the foundation or substratum (or embodiment) for the barrier function, i.e., the organisational and/or physical structure without which the barrier function could not be accomplished. The use of the barrier concept should be based on a systematic description of various types of barrier systems and barrier functions, for instance as a classification system. This will help to identify specific barrier systems and barrier functions and to understand the role of barriers, in either meaning, in the history of an accident [114].

The distinction between barrier systems and barrier functions was used as the basis for a general Accident Evolution and Barrier Function (AEB) model [114]. This model represented the development of an accident as a sequence of steps belonging to either the human factors / organisational system or the technical system (see Figure 2.1.9). Each step represents either (1) the failure or malfunction of a component or (2) an incorrectly performed function within each system, and the barrier functions are used to indicate how the development of the accident could be arrested. In Figure 2.1.9 barrier functions are shown as two parallel lines '//'.

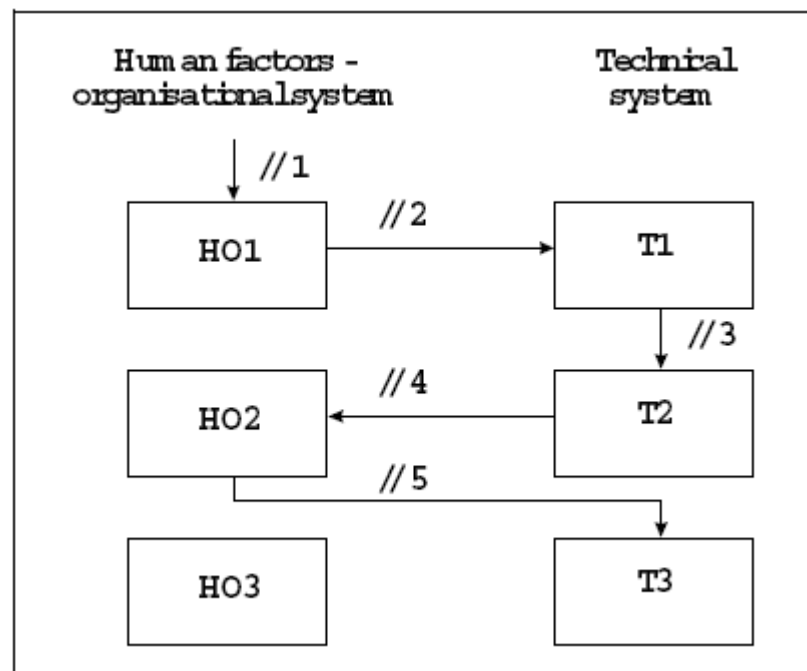


Figure 2.1.9. The Accident Evolution and Barrier (AEB) function model [114]

The AEB model proposed three different barrier systems, namely physical, technical, and human factors/organisational. Coupled with most links in this sequence of malfunctions, failures, and errors in human and technical systems there are opportunities to arrest the accident evolution through *barrier functions*, (e.g. a physical barrier function) controlled by *barrier function systems* (e.g. a computer-controlled lock). In contrast to a tree representation of the contributing factors to barrier function failures, this method implies that failures and failing barrier functions are analysed at successively more detailed levels.

Strengths: AEB method formalises the links between human performance and technology and uses the barrier function in a more graphical way. It is particularly focused on failures and errors and free to use.

Limitations: Does not present all the data in the AEB main flow chart and hence runs the risk of missing potential relevant contributory factors. Sometimes issues emerge while deciding when to stop going further back in the chain and barrier function analysis.

2.1.4.4. PRCAP - The Paks Root Cause Analysis Procedure

Developed in Hungary, PRCAP was originally an adaptation of HPES and MORT [1, 2]. Nevertheless, significant modifications and amendments of these methods were made to satisfy the specific interests and practices of safe and reliable operations at the Paks NPP. PRCAP represents a disciplined approach to systematic investigations and analysis of root causes of events that occur at operating NPPs. PRCAP includes a number of techniques such as change and barrier analysis, event and causal factor charting, event tree drawings, and causal factor searches.

CERCA: Developed in Hungary, CERCA is a computer based event investigation documentation method in use at the Paks NPP.

2.1.5. SOL - Safety through Organisational Learning

SOL (Sicherheit durch Organisationales Lernen - Safety through Organisational Learning) was initially developed by the research group in 1997 under the guidance of Bernhardt Wilpert at the Berlin University of Technology in collaboration with the TÜV [115-117]. It was initially developed for the nuclear power industry; however, a version for the chemical industry exists and a computer supported version was developed as well in 1999. The SOL method has been adopted by the Swiss and German nuclear industries as standard procedure for their in-depth event analyses. SOL aims at facilitating organisational learning from events by supporting the process of analysing events, ensuring its standardised conduct and mobilising expert knowledge and creativity in the analysis.

The SOL method covers the identification of human factors as well as technical, organisational and management factors. During the first phase of the analysis the event objective data is collected, without questioning its significance (see Figure 2.1.10). In the second phase the data is organised into elements of the event as individual actions performed by the personnel, organisational unit or systems. This is then classified chronologically by each person and represented in an actor-action-time illustration. The method uses a predetermined set of direct causes and contributing factors. On the basis of the selected direct causes, the method proposes questions to be addressed to help identify the contributing causes. These elements are successively added to the actor-action-time illustration, thus facilitating the progress of the investigation and the further collection of information.

Analysing events with SOL is conceptualised as a backward oriented problem-solving process [68, 115-117]. SOL operationalises the concept of event analysis in a set of two standardised process steps: (1) the description of the actual event situation, and (2) the identification of contributing factors. For both steps guidelines have been developed which support the event analyst. As the first step of the analysis, a situational description is constructed. The information needed for the description of the event is gathered by interviews and document analysis. A set of questions helps the analyst to ask the right questions in order to completely reconstruct the course of an event. Based on the STEP method [101] the information collected is broken down into a sequence of so-called event-building blocks, i.e. the event is broken down into a sequence of single micro-events to clarify and illustrate what happened [68, 115-117]. For each event-building block the information is categorised according to the actor (human and technical actors), the action, the point in time of the action, the location (where the action takes place) and additional remarks. Thus, an event is determined by a sequence of individual actions by different actors. The starting point of an event (i.e. the first event-building block) is defined as the first deviation from a warranted course of action. These deviations are identified by contrasting actions against formal procedures and technical system design, or against 'normal' system performance, based on the appraisal of an event analyst. The end point (i.e. the last event-building block) is defined as the recovery of a safe system state. The situational description illustrates only observable facts (what happened). Actions which were not shown, as well as hypotheses about potential causes, should not be incorporated into the situational description. Each event-building block is ordered graphically in a time-actor diagram, which provides an overview of the recomposed event and serves as an important information source for the subsequent identification of contributing factors.

The identification of contributing factors, i.e. the second step, is conducted in the following way: for each event-building block a separate analysis is conducted. A guideline with categories of possible contributing factors – the identification aid – supports this second step. The identification aid consists of categories of potential contributing factors which cover individual, technical, group, organisational and inter-organisational aspects to guarantee a sufficient scope of investigation.

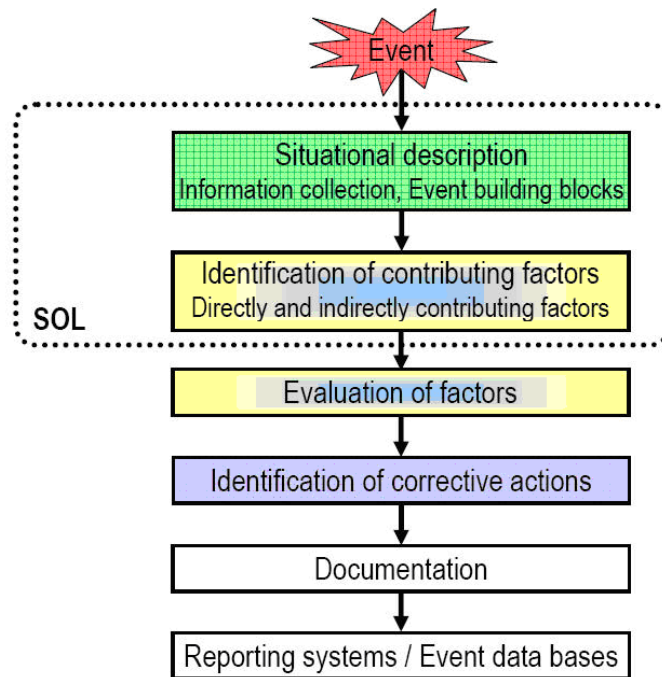


Figure 2.1.10. SOL and SOL-VE analysis procedure [116, 117]

In order to support the identification of contributing factors, each factor is assigned to a general question. For instance, the factor ‘working conditions’ is transferred into the question: ‘Could the working conditions have affected the operator’s performance?’ For each factor several specific examples are given to support the analysts, e.g. for ‘working conditions’ the examples are time pressure, noise, heat, lights or disturbances. Thus, the aid contains general questions related to possible contributing factors covering each of the five sub-systems in order to ensure the comprehensiveness of the analysis. Since it is assumed that an event analyst may not be exclusively a human factors specialist, the aid also gives illustrative examples of potential influences on contributing factors with the aim of stimulating creative problem solving processes. These examples are concrete enough to cover a broad range of potentially contributing factors, but they are not meant to be exhaustive. To guarantee the comprehensiveness of the analysis all general questions are linked to others. These so-called cross-references are theoretically and empirically based. If one question is answered in the affirmative, the team is guided to answer another set of questions in order to identify other potentially contributing factors. Contributing factors are roughly divided into direct and indirect factors. The analysis process starts with the identification of direct factors which are linked to a couple of indirect factors due to the cross-references. For instance, if the direct factor ‘personal performance’ is identified, a cross-reference to the indirect factor ‘training’ is given. By these cross-references mono-causal thinking and attaching too high a significance to active errors should be overcome. Finally, all identified contributing factors are added to the time-actor-matrix (see Figure 2.1.11), thus successfully completing the reconstruction of the event and its causes.

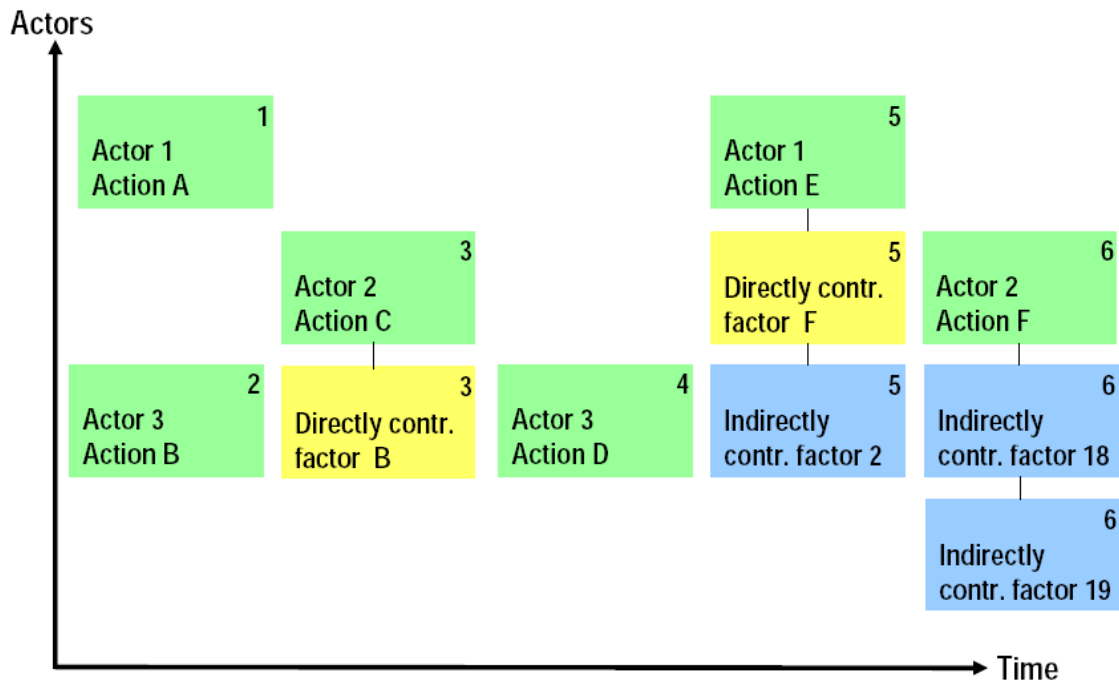


Figure 2.1.11. Example of the SOL time-actor diagram with contributing factors [116]

Overall, SOL is assumed to overcome the above mentioned problems in analysing events. The separation of information search and identification of contributing factors prevents premature hypotheses leading to a restricted information and causal search. The cross-references between potential contributing factors support the identification of factors remote in time and space (latent failures), prevent a focus on solely individual contributions and avoid mono-causal thinking by the analysts. The identification of contributing factors for each single event-building block prevents premature hypotheses and the identification of contributing factors due to past accidents. Finally, the questions and examples in the identification aid support the analysts in identifying ‘out of sight’ factors (e.g. factors that contribute by their absence).

In summary, SOL ensures sufficient scope of investigation by introducing 21 categories of possible contributing factors, with more than 160 specific and illustrative examples. SOL provides degrees of freedom for the analyst’s problem solving, but at the same time standardises the process of analysis. It requires a multidisciplinary team in order to ensure a broad approach.

SOL-VE (SOL –Versio Electronica) is an MS-Windows based software tool for event analysis, including the administration of events and associated corrective actions within a database. It covers the identification of human factors as well as technical factors, and supports the whole procedure of event analysis as a problem solving process. Tests and experience show that it fulfils the necessary criteria and that it is a useful and easy to handle method. The application includes database functions that allow trending of the various root causes across all event investigation results [2, 115-117].

SOL develops the concept of event analysis in a set of standardised process steps [62, 68, 69, 115-117]. A set of three specific instruments is aimed at supporting the process of event analysis, to ensure its standardised conduct while at the same time mobilising expert knowledge and creativity in the analysis, which can be compared to a backward oriented problem solving process:

1. Guideline for the description of the situation;
2. Guideline for the identification of contributing factors;
3. Guideline for the reporting of the event.

Guideline for Description of the Situation.

As soon as possible after an event occurred the whole event must be described, i.e. recording what happened between a starting point and an end point of the event. An accidental event is determined by a

sequence of individual actions by different actors (maybe a person or a technical component). The starting point is defined as the first alarm or the first perceived deviation from a warranted course of action. The end point is defined as the recovery of a safe system state. The description aims to separate the processes of information gathering and interpreting this information. Similarly to the STEP method (Sequential Timed Events Plotting) [68, 102], the event is broken down into a sequence of event-parts, i.e. single actions of different actors (person or machine), and event building blocks, and no contributing factors should be identified at this stage.

Guideline for the Identification of Contributing Factors (CFs).

This guideline takes the analysts through the individual steps of an event analysis in a certain sequence. It provides the standardisation of the analysis process. Every single action (representing an ‘event building block’) identified in the description of the situation should be analysed by asking the question ‘why’. Each event building block is located within a time-actor diagram. This graphic charting of the individual building blocks of the event is completed by identifying contributing factors. Every contributing factor is complemented by adding further contributing factors. The contributing factors are related to five subsystems shown in Figure 2.1.12. Thus, a graphic chart is developed which represents the event and all contributing factors in their whole complexity.

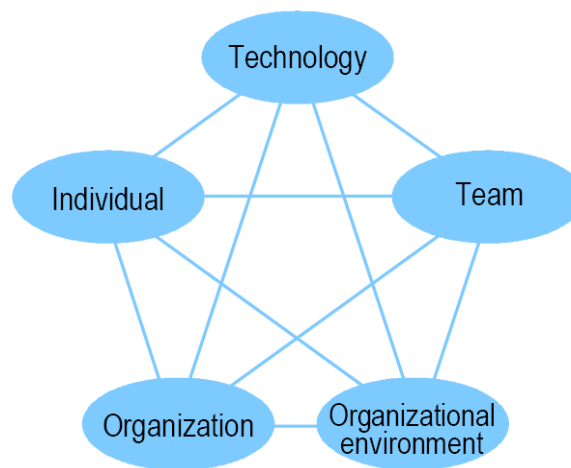


Figure 2.1.12. Socio-technical system model of event genesis [68, 118]

SOL differentiates directly contributing factors from indirectly contributing ones. Six factors are deemed to be directly contributing in terms of their direct and immediate contribution to the genesis of an event: a) information; b) communication; c) working conditions; d) personal performance; e) violation; f) technical components.

Indirectly contributing factors are seen to be those which are temporally and spatially somewhat more distant from the actual event evolution, but nevertheless often crucial for the event. A list of 19 categories of contributing factors (later extended to 21) was collated to assist the search for contributing factors : 1. Information; 2. Communication; 3. Working conditions; 4. Personal performance; 5. Violation; 6. Operation scheduling; 7. Responsibility; 8. Control and supervision; 9. Group influence; 10. Rules, procedures and documents; 11. Qualification; 12. Training; 13. Organisation and management; 14. Feedback of experience; 15. Safety principles; 16. Quality management; 17. Maintenance; 18. Regulatory and consulting bodies; 19. Environmental influence.

All possible contributing factors are transferred into general questions. Thus, the aid contains general questions related to possible contributing factors for each of the five subsystems and so ensures the comprehensiveness of the analysis. These questions serve as a support to the team’s problem solving process by giving them an idea of how certain factors could have contributed to the occurrence of the event.

Guideline for reporting of the event

This guideline is an aid for the composition of the event description, the event report, and the allocation of descriptors. The event description constitutes a comprehensive documentation of the process of

analysis and provides the main basis for the NPP's internal organisational learning. The guideline ensures the standardisation of reports in all NPPs; it contains information about the role, form and writing of the event report, and also information about the classification of contributing factors for statistical analysis.

The evaluation of SOL was conducted in two separate steps: (1) an empirical evaluation by conducting experiments with student samples and (2) expert judgments of actual use in the nuclear power and chemical industries. Overall, the results showed that the SOL methodology may help to overcome the above mentioned biases [116]. Specifically, the subjects exhibited broad causal search, multi-causal thinking, and consideration of factors beyond individual errors. SOL was also evaluated for its applicability by international scientists and practitioners in the field. Practitioners from nuclear power plants judged that SOL leads to at least as good, or even better, results than conventional methods which were used in the German industry. SOL was judged to be an analysis methodology which supports practitioners in NPPs and enhances systemic thinking and a questioning attitude. Meanwhile, the computerised version SOL-VE has been adopted by the Swiss and German nuclear power industries as the standard procedure for their in-depth event analyses.

2.1.6. TRIPOD

Research into the TRIPOD concept started in 1988, when a study by the Universities of Leiden and Manchester that was contained in the report 'TRIPOD, A principled basis for accident prevention' [152] was presented to Shell International Petroleum Exploration and Production Company. The idea behind TRIPOD is that organisational failures are the main factors in accident causation [62, 71, 152]. The Tripod theory uses an approach to safety aimed at the underlying problems that lead to incidents. It emphasises that the immediate causes (unsafe acts, people's errors), do not occur in isolation but are influenced by external factors – organisational or environmental preconditions. Many of these factors themselves originate from decisions or actions taken by planners, designers or managers who are far away from the scene of the accident – the latent failure. The nature of latent failures means that they usually have a broad impact. Hence, identifying and addressing them will bring wider benefit when compared to the immediate cause of the accident. These 'latent' factors, when contributing to an accident, are always followed by a number of technical and human errors. The complete TRIPOD-model 2 is illustrated in Figure 2.1.13.

Substandard acts and situations do not just occur – they are generated by mechanisms acting in organisations, regardless of whether or not there has been an accident. Often these mechanisms result from decisions taken at a high level in the organisation. These underlying mechanisms are called Basic Risk Factors (BRFs), and BRFs may generate various psychological precursors which may lead to substandard acts and situations. Examples of psychological precursors to slips, lapses and violations are time pressure, and being poorly motivated or depressed. According to this model, eliminating the latent failures categorised in BRFs, or reducing their impact, will prevent psychological precursors, substandard acts and operational disturbances. Furthermore, this will result in prevention of accidents. The identified BRFs cover human, organisational and technical problems.

The different Basic Risk Factors are defined in Table 2.1.1. Ten of these BRFs relate to 'operational disturbance' (the 'preventive' BRFs), and one BRF is aimed at controlling the consequences once the operational disturbance has occurred (the 'mitigation' BRF). There are five generic prevention BRFs (6-10 in Table 2.1.1.) and five specific BRFs (1-5 in Table 2.1.1.). The specific BRFs relate to latent failures that are specific for the operations to be investigated (e.g. the requirements for tools and equipment are quite different in an oil drilling environment compared to an intensive care ward in a hospital). These 11 BRFs have been identified as a result of brainstorming, a study of audit reports, accident scenarios, a theoretical study, and a study of offshore platforms.

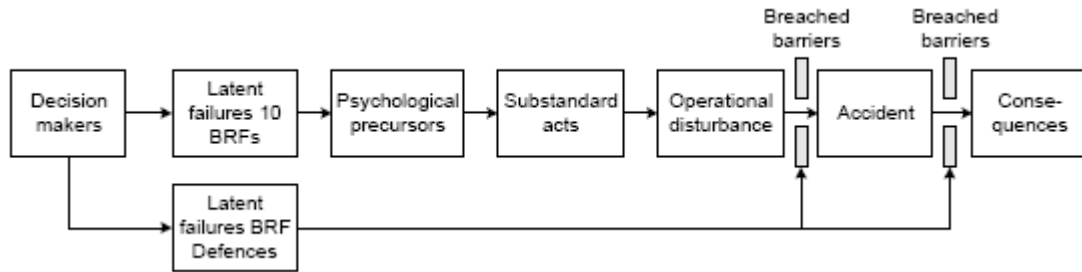


Figure 2.1.13. The complete TRIPOD model [62, 71]

Table 2.1.1. The definitions of the basic risk factors (BRFs) in TRIPOD [62, 71]

No	Basic Risk Factor	Abbr.	Definition
1	Design	DE	Ergonomically poor design of tools or equipment (user-unfriendly)
2	Tools and equipment	TE	Poor quality, condition, suitability or availability of materials, tools, equipment and components
3	Maintenance management	MM	No or inadequate performance of maintenance tasks and repairs
4	Housekeeping	HK	No or insufficient attention given to keeping the work floor clean or tidied up
5	Error enforcing conditions	EC	Unsuitable physical performance of maintenance tasks and repairs
6	Procedures	PR	Insufficient quality or availability of procedures, guidelines, instructions and manuals (specifications, “paperwork”, use in practice)
7	Training	TR	No or insufficient competence or experience among employees (not sufficiently suited/inadequately trained)
8	Communication	CO	No or ineffective communication between the various sites, departments or employees of a company or with the official bodies
9	Incompatible goals	IG	The situation in which employees must choose between optimal working methods according to the established rules on one hand, and the pursuit of production, financial, political, social or individual goals on the other
10	Organisation	OR	Shortcomings in the organisation’s structure, organisation’s philosophy, organisational processes or management strategies, resulting in inadequate or ineffective management of the company
11	Defences	DF	No or insufficient protection of people, material and environment against the consequences of the operational disturbances.

TRIPOD Beta

The TRIPOD Beta-tool is a computer-based instrument that provides the user with a tree-like overview of the accident that was investigated. It is a menu driven tool that guides the investigator through the process of making an electronic representation of the accident. TRIPOD Beta is distributed by Tripod Solutions (for more information, see [71]).

TRIPOD Beta-tool merges two different models, the HEMP (‘The Hazard and Effects Management Process’) model and the TRIPOD Beta accident causation model. This merging has resulted in an incident causation model that differs conceptually from the original TRIPOD model. The HEMP model is presented in Figure 2.1.14.

The TRIPOD Beta accident causation model is presented in Figure 2.1.15. This chain is used to identify the causes that lead to the breaching of the controls and defences presented in the HEMP model.

Although the model presented in Figure 2.1.15 looks like the original TRIPOD model, its components and assumptions are different. In the Beta-model the defences and controls are directly linked to unsafe acts, preconditions and latent failures. Unsafe acts include how the barriers were breached and the latent failures why the barriers were breached. An example of a TRIPOD Beta accident analysis is shown in Figure 2.1.16.

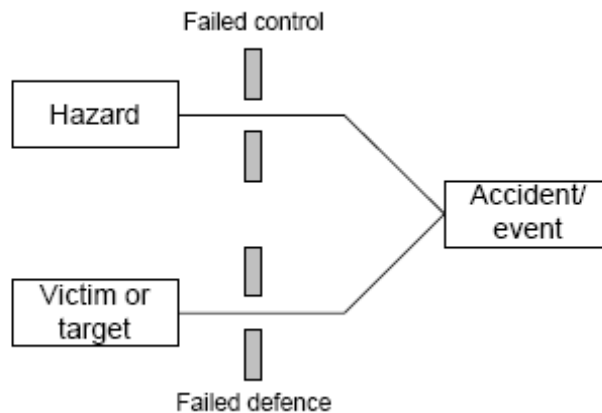


Figure 2.1.14. 'Accident mechanism' according to HEMP [62, 71]

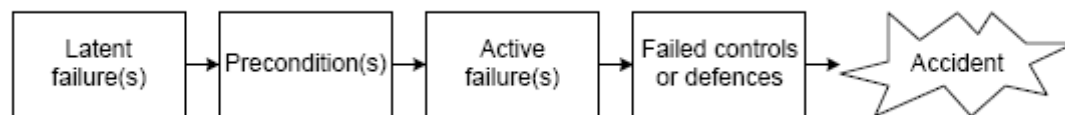


Figure 2.1.15. TRIPOD Beta Accident Causation Model [61, 70]

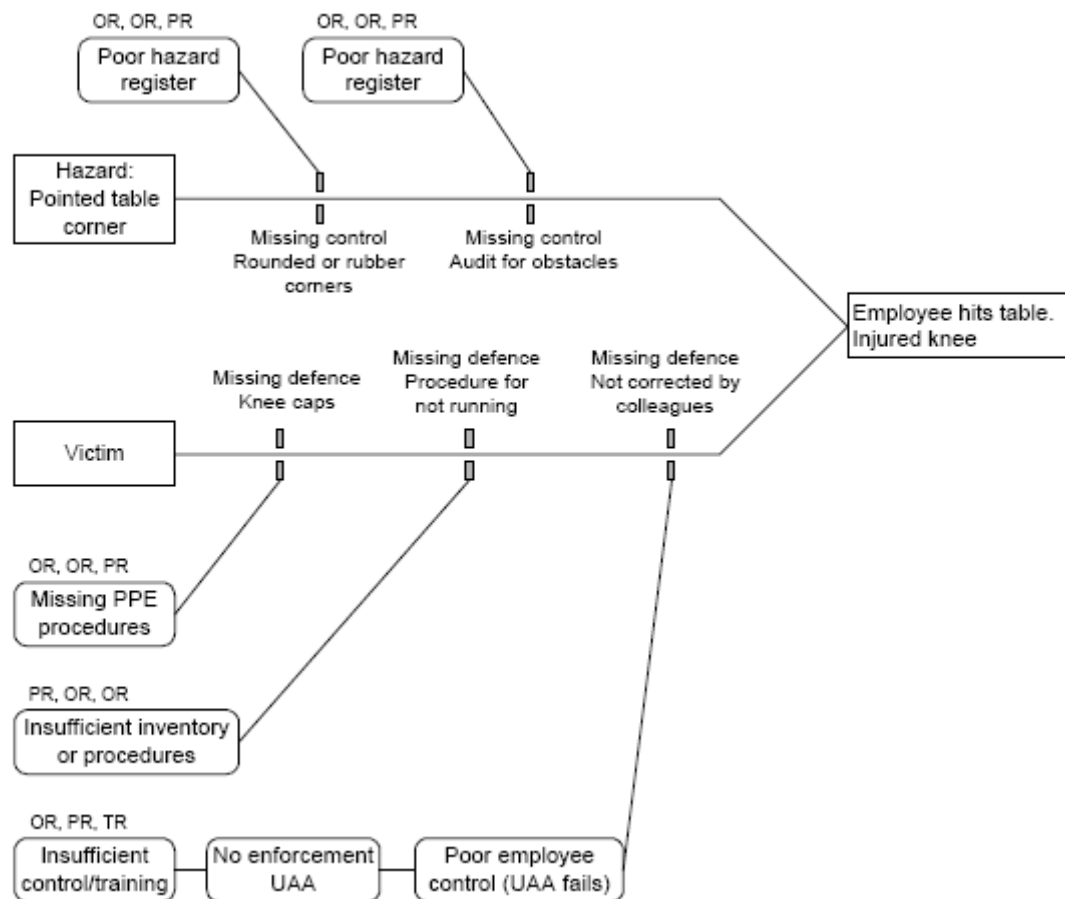


Figure 2.1.16. Example of a TRIPOD Beta analysis (abbreviations explained in table 2.1.1) [62, 71]

2.1.7. STEP - Sequential Timed Events Plotting

STEP (Sequential Timed Events Plotting) - a multi-linear method for accident analysis was developed by K. Hendrick and L. Benner in 1987 [68, 102, 118]. They proposed a systematic process for accident investigation based on multi-linear event sequences and a process view of the accident phenomena. In STEP, an accident is a special class of process, whereby a perturbation transforms a dynamically stable activity into unintended interacting changes of states with a harmful outcome. In this multi-linear approach, an accident is viewed as several sequences of events, and the system is broken down into a structure consisting of interacting events, in sequences or in parallel. STEP provides a comprehensive framework for accident investigation from the description of the accident process, through the identification of safety problems, to the development of safety recommendations.

STEP is built based on four key concepts:

1. Multi-linear event sequence, aimed at overcoming the limitations of the single linear description of events. Neither the accident nor its investigation is a single linear chain or sequence of events. Rather, several activities take place at the same time. This is implemented in a worksheet with a procedure to construct a flowchart to store and illustrate the accident process (see Figure 2.1.17).
2. The description of the accident is performed by universal events building blocks. A building block describes one event, i.e. an event is defined as one actor performing one action. To ensure that there is a clear description the events are broken down until it is possible to visualise the process and be able to understand its proper control. In addition, it is necessary to compare the actual accident events with what was expected to happen. The event Building Block format for data is used to develop the accident description in a worksheet.
3. Events flow logically during a process. Arrows in the STEP worksheet illustrate the flow. This concept is achieved by linking arrows to show proceed/ follow and logical relations between events. The result of the third concept is a cascading flow of events representing the accident process from the beginning of the first unplanned change event to the last connected harmful event on the STEP worksheet.
4. Both productive and accident processes are similar and can be understood using similar investigation procedures. They both involve actors and actions, and both are capable of being repeated once they are understood.

With such a process concept, a specific accident begins with the action that started the transformation from the described process to an accident process, and ends with the last connected harmful event of that accident process.

The STEP worksheet provides a systematic way to organise the building blocks into a comprehensive, multi-linear description of the accident process. The STEP worksheet is simply a matrix, with rows and columns. There is one row in the worksheet for each actor. The columns are labelled differently, with marks or numbers along a timeline across the top of the worksheet, as shown in Figure 2.1.18. The timescale does not need to be drawn on a linear scale; the main point of the timeline is to keep events in order, i.e., how they relate to each other in terms of time. An actor is a person or an item that directly influences the flow of events constituting the accident process. Actors can be involved in two types of changes, adaptive changes or initiating changes. They can either change reactively to sustain dynamic balance or introduce changes to which other actors must adapt. An action is something done by the actor. It may be physical and observable, or it may be mental if the actor is a person. An action is something that the actor does and must be stated in the active voice.

The organisation of the events is developed and visualised as a 'mental motion picture'. The completeness of the sequence is validated with three tests. The row test verifies that there is a complete picture of each actor's actions through the accident. The column test verifies that the events in the individual actor rows are placed correctly in relation to other actors' actions. The necessary and sufficient test verifies that the early action was indeed sufficient to produce the later event, otherwise more actions are necessary. The STEP worksheet is used to show a link between the recommended

actions and the accident. The events represented in STEP are related to normal work and help to predict future risks. The safety problems are identified by analysing the worksheet to find events sets that constitute the safety problem. The identified safety problems are marked as triangles in the worksheet (see Figure 2.1.18). These problems are evaluated in terms of severity. They are then assessed as candidates for recommendations. A STEP change analysis procedure is proposed to evaluate recommendations. Five activities constitute this procedure: the identification of countermeasures to safety problems, the ranking of the safety effects, assessment of the trade-off involved the selection of the best recommendations, and a quality check.

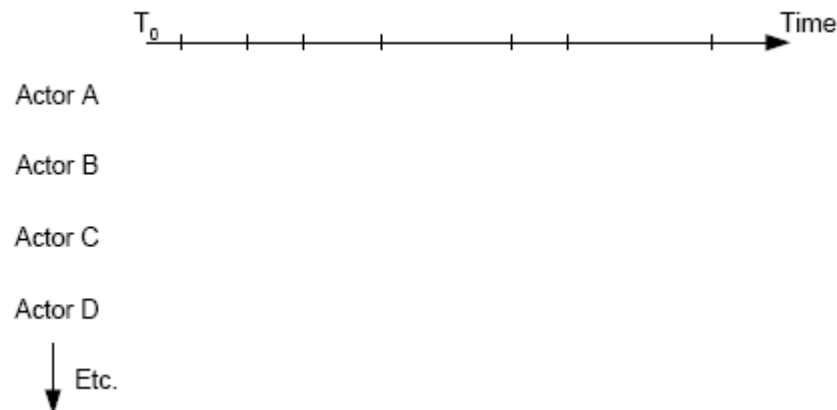


Figure 2.1.17. STEP worksheet [62, 68, 70, 102, 118]

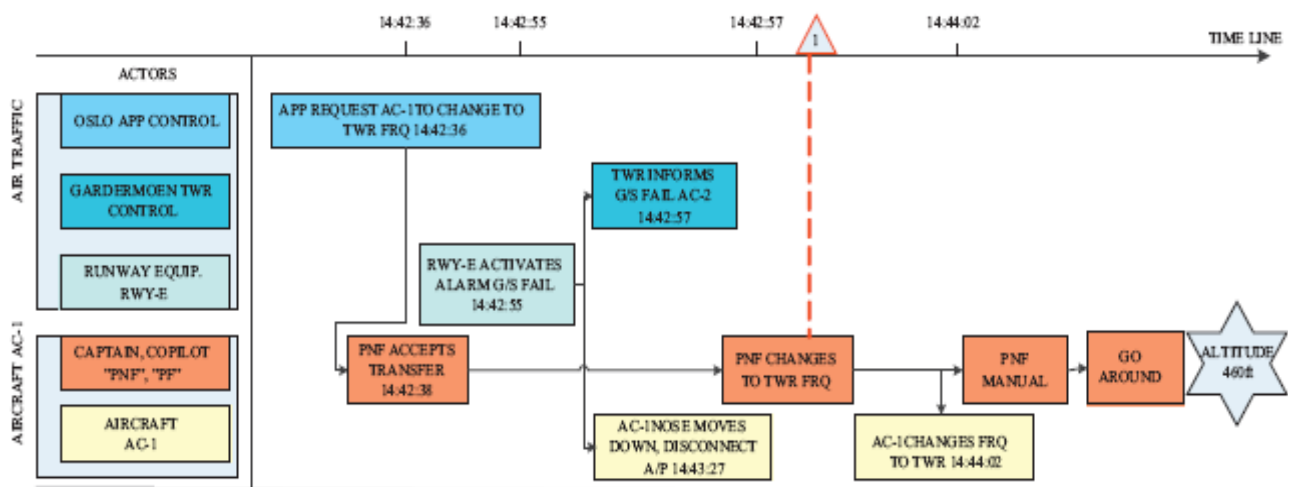


Figure 2.1.18. Simplified example of the STEP worksheet applied to air traffic incident NAX541 [118]

STEP is relatively simple to understand and provides a clear picture of the course of events. However, STEP only asks the question, which events happened in the specific sequence of events under analysis. This means that events mapped in STEP are separated from descriptions of the normal functioning of socio-technical systems and their contexts. For example (see Figure 2.1.18), the STEP diagram illustrates that the requested switch to another frequency was delayed, but not why. Instead, STEP only looks for failures and safety problems, and highlights sequence and interaction between events. STEP interpretation and analysis depend extensively on investigator experience. STEP is suited to describing tractable systems, where it is possible to describe the system in full, the principles of functioning are known, and there is sufficient knowledge of key parameters.

2.1.8. A remedy-oriented event investigation system

A remedy-oriented system for systematically analysing and evaluating human-related incidents occurring in nuclear power plants is proposed in Japan [38]. This system aims particularly at identifying causal factors and at deriving proposals for specific hierarchical countermeasures. Unlike conventional methods (e.g. HPES), which are based on a check-sheet format, are thus devoid of logical methodology for conducting the analysis, and which thus lack the means of searching for underlying causal factors, and which do not record factual information on the sequence of events, the system presented by Takano et al incorporates innovative techniques such as: (a) a modified fault tree method for searching the underlying causal factors, (b) compilation of related events into sequential charts, (c) a technique for devising proposed hierarchical redundant countermeasures, and (d) implementation procedures set out in a practical manual form for easy familiarisation and application.

Through several trial applications, this method has been shown to permit the identification of underlying causal factors, even down to those associated with the software aspects of human action and state of mind, and with the mode of management, organisation, operating rules and document forms, all of which are liable to be overlooked.

The overall structure of a remedy-oriented system is shown in Figure 2.1.19. The system comprises the three constituents of Implementation Procedure, Evaluation Forms and Evaluation Guides, which are individually detailed in what follows.

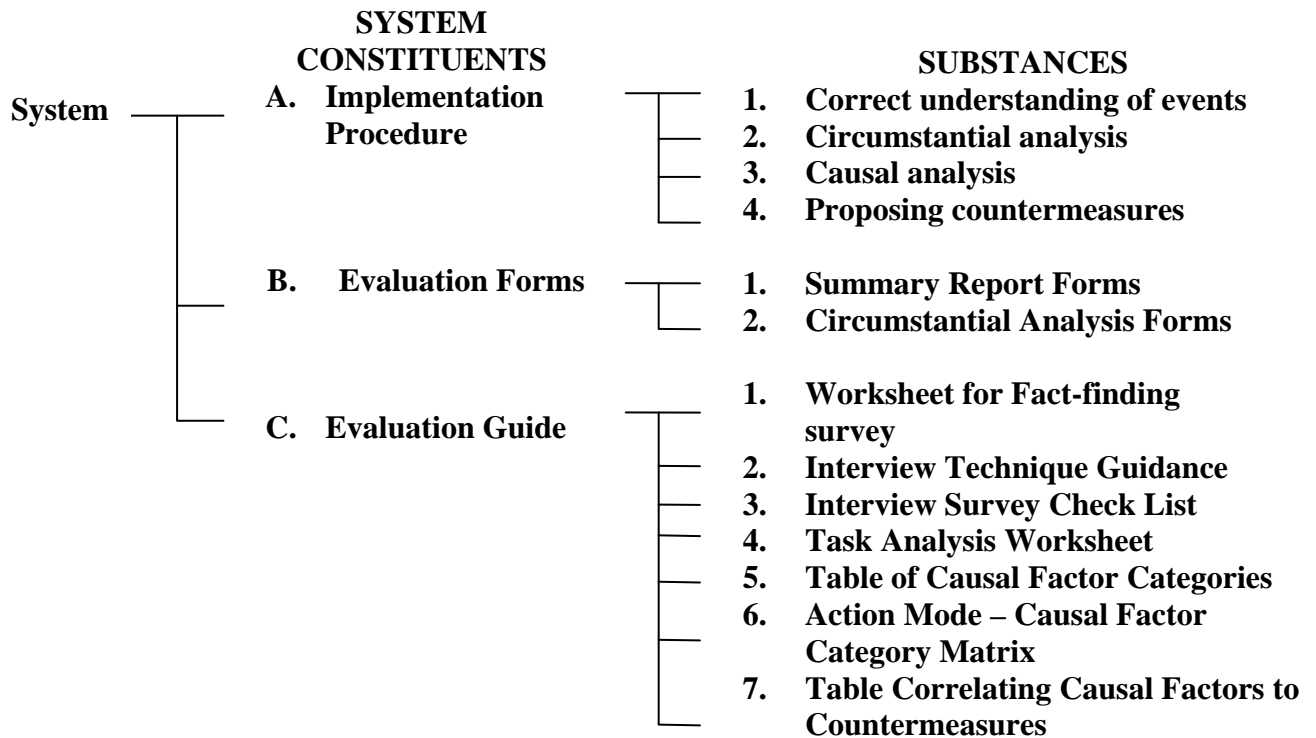


Figure 2.1.19. The overall structure of a remedy-oriented system [38]

The Implementation Procedure, originally developed through a three-fold trial application in Japanese nuclear plants, furnishes instructive advice on how to proceed on analysis and evaluation; the Evaluation Forms provide the format in which to record the results of analysis; and the Evaluation Guides are to aid personnel in efficiently performing their tasks in operations of analysis and evaluation. One part of the system constituents – covering records of circumstantial analysis – prescribes the use of check-sheets, similar to the HPES evaluation forms, and patterns of form presenting features that are common with the HPES have been adopted, so as to permit the carrying out of statistical analyses. The forms specified for

performing the circumstantial analyses, however, have been modified from those of the HPES, to be more suited to use in the Japanese nuclear industry. The Summary Reports describe originally devised forms in which to record the major results obtained by applying the newly developed techniques and method mentioned.

Of the foregoing three constituents, the Implementation Procedure plays the key role. It is divided into four stages, which are further subdivided into 15 steps in all (see Table 2.1.2). For each step, the Implementation Procedure Manual indicates concisely the sequence of procedures to be followed, the formats for recording the results of analysis (in generalised form and accompanied by illustrative diagrams), and the methods and items to be surveyed, together with an indication of the particular Evaluation Guide that contains the relevant reference material.

Evaluation Forms comprise two parts that complement each other, and which cover (a) Circumstantial Analysis, and (b) Summary Report. Both parts are stored in the database.

The seven Evaluation Guides have been devised applying the latest knowledge in human-factors engineering, to ensure efficient implementation free from oversight of the prescribed operations of survey, analysis and evaluation in proper sequence. The Guides, in the form of worksheets for easy use, have been prepared bearing in mind their application to case studies of the knowledge available in human-factors engineering.

The most notable features of the proposed system include the implementation of Procedure Manuals, which has significantly reduced the time required for personnel to become familiar with the system, and which has extended the range of application to all personnel wishing to use the system. Also, the modified fault tree method has made it possible to search for underlying causal factors, even down to those associated with the software aspects of human action and state of mind, which are highly liable to be overlooked. This modified fault tree method further serves usefully in proposing hierarchical redundant countermeasures that are more practically applicable and functionally effective than is possible with the current method. Another merit of our system is that the results obtained with it can be directly utilised for reporting to plant managers charged with implementing the countermeasures. The Summary Report Form contains a succinct description of the sequence of events, which can serve as useful material for subsequent activities aimed at promoting plant operation safety.

Table 2.1.2. Implementation procedure of 4 stages and 15 steps

Stage		Step	
1.	Correct understanding of events	1.	Correctly note sequence of states presented in equipment, and effects of change in state
		2.	Identify the relevant trigger action
		3.	Identify the sequence of tasks involving the trigger action
		4.	Draft sequential chart of related events
2.	Circumstantial analysis	5.	Fill in circumstantial analysis forms A, B, C
		6.	Complete sequential chart of related events
3.	Causal analysis	7.	List causal factors of trigger actions
		8.	Identify direct causal factors
		9.	Identify indirect/potential causal factors
		10.	Complete causal relation chart
4.	Proposal of countermeasures	11.	Propose level 1 countermeasures
		12.	Propose level 2 countermeasures
		13.	Propose level 3 and 4 countermeasures
		14.	Evaluate the proposed countermeasures
		15.	Complete the table of proposed countermeasures

2.1.9. HF- compatible RCA method

This method was presented by W. Preischl (GRS) [42]. Derived from behavioural science, task objectives (usefulness for in-depth analysis of notifiable events; fitness in established technical approaches for root-cause analysis, suitability for generation of recommendations for improvements, knowledge base for further HF-activities and OEF), and limitations of practical work, this method consists of Event description, Event model, M/M-system model and Performance shaping factors (PSF) modules. Structures of the Event model and the M/M-System Model are presented in Figs. 2.1.20 and 2.1.21. Interaction of Event / Man-Machine-Systems (A) / PSF Modules is illustrated in Figure 2.1.22.

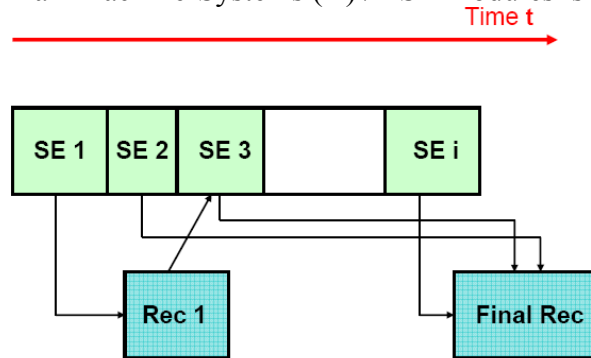


Figure 2.1.20. Structure of the event model (SE – sub-event, Rec – recovery actions) [42]

Some characteristics of the HF-System: it includes PSF-modules such as ‘Information’, ‘Action’, ‘Person’, ‘Environment’, ‘Organisation’ etc., and about 150 items (in total about 400 hierarchically structured items). Each module is provided by a system of pre-defined descriptors; additional coding for each item and grouping in accordance with PSF classification are possible. Special groups for the aspects ‘Safety culture’, and ‘Precautions for failure detection / failure compensation’ are established.

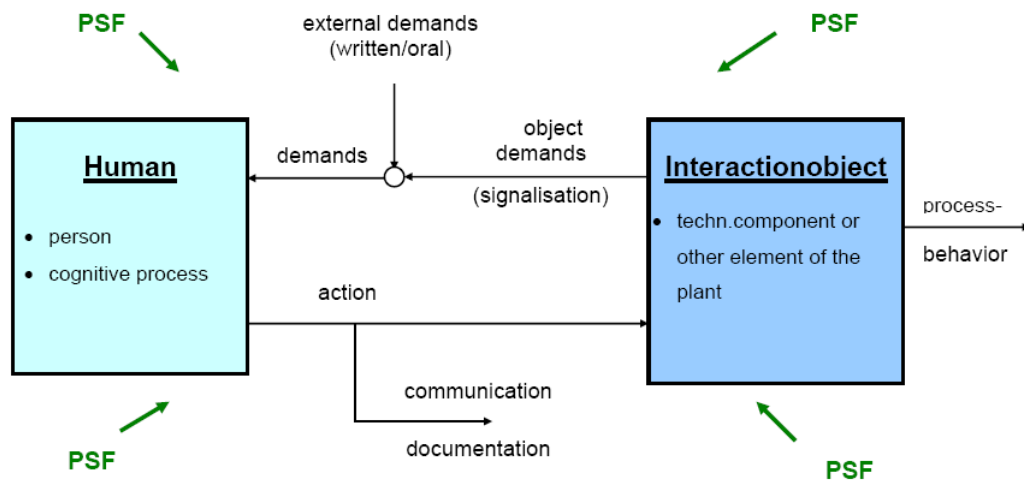


Figure 2.1.21. Structure of Structure of the M/M- System Model [42]

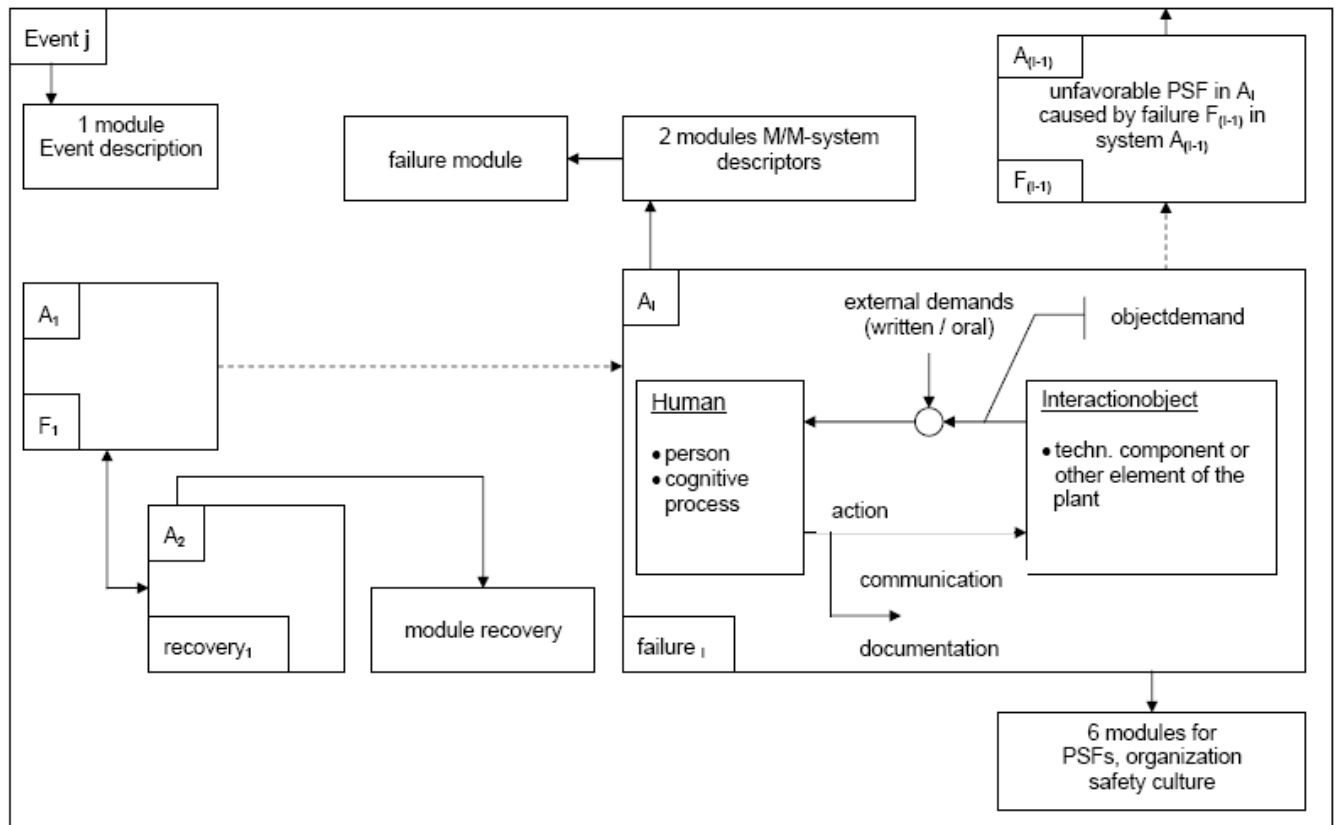


Figure 2.1.22. Interaction of Event / Man-Machine-Systems (A) / Modules [42]

2.1.10. 3CA - Control Change Cause Analysis

This method has its origins in a cooperative project run by Humber Chemical Focus and the UK Health & Safety Executive between May and November 2000 [73]. The venture was aimed at line managers of chemical sites in the Humber region and sought to develop their skills in identifying underlying causes of accidents and incidents. The project aimed to equip people with tools to help them investigate and identify lessons to be learned.

Most incidents contain more than one event that requires explanation, and often there are several. Identifying events for root cause analysis can be approached in a number of ways. One of the first methods considered was Energy Trace and Barrier Analysis (ETBA); this uses 'unwanted energy flows' as the defining characteristic. ETBA was evaluated and found not to interface adequately with the root cause method. What was needed was a different tool for identifying problematic events - a simpler root cause tool, one that structured the process of inquiring into underlying causes, but without burdening the user with long lists of prompts, and one that did not use the energy flow concept. This produced a generalised form of barrier analysis called 'Control Change Analysis' (or 2CA), still present as the first part of a new prototype - 3CA. In 2007-08, the NRI Foundation and HSE, working in partnership, produced the B-form of 3CA [73].

The results of trials of applying 3CA in a number of different companies and organisations suggested that 3CA:

- is quick to learn;
- provides a structured way of taking the specific events and outcomes of an incident through to the relevant areas of the safety management system, identifying ineffective ones;
- is systematic and reproducible;
- produces visible results that are easy to communicate;
- is recordable and can be audited.

Control Change Cause Analysis – 3CA – is designed to help investigators structure their inquiries into the underlying cause of incidents and to make it easy for others to review their reasoning. The manual [73] provides an explanation of the 3CA method and a description of the process.

An incident or accident happens as part of a continuous flow of changes. From this complex whole, the 3CA analyst selects facts by applying various tests of relevance to the incident or accident. The analyst sets out these facts in a worksheet to form explanations and sets of questions. The result of the analysis is a concise description of the incident – seen in terms of changes and limitations in the control of changes – and a set of questions that the investigator needs to fill gaps in the description.

The analyst can begin the 3CA process as soon as they have the basic facts about what happened. It is best to start early, because the analysis is likely to raise questions. In most investigations, the 3CA analysis will be revisited one or more times; as new facts emerge, the analyst can answer the questions posed earlier. These answers sometimes trigger new questions.

In 3CA, the analyst treats accidents and incidents as a sequence of events in which unwanted changes occur. This sequence begins with the moment that control is reduced and ends with the moment that control is restored. Some of the events in the sequence are ‘significant’ in the sense that they increase risks or reduce control in the situation, so allow further unwanted changes to occur. The first job for the 3CA analyst is to identify these significant events. With the set of significant events established, the analyst identifies what measures could have prevented them or limited their effects. To ensure the thoroughness of this identification, the analyst describes each significant event in terms that make explicit who/what is acting, the action and who/what is acted upon. In this way, the analyst scrutinises all the elements of unwanted change from the point of view of prevention. The analyst has to identify in what ways prevention was ineffective. In the first part of the analysis the focus is on tangible barriers and controls, those at the operational level. Next, the analyst restates the facts as differences between what was expected (based on norms such as standards and procedures) and what was true in the actual situation. The differences between the actual and expected situations provide the agenda for the rest of the analysis. The investigator seeks to account for these differences in terms of the reasoning used by people responsible for the barriers and controls, the organisational and cultural factors that influenced the situation and the systems and management arrangements that caused or allowed the difference to exist.






The analysis runs in parallel with other investigative efforts; after the initial 3CA analysis, it is likely that one or more revisions will be made as further enquiries yield new insights and, in some cases, new questions. The initial 3CA analysis is performed in two parts, as in the sequence described below and indicated in Table 2.1.3.

In the first part, you complete column 1 (the significant events) before completing column 2 (the barriers and controls). You finish the first part of the analysis by setting priorities in column 3; these priorities decide the sequence for the second part of the analysis. In the second part of the analysis, you complete columns 4 and 5 for one significant event at a time.

In 3CA, an event is defined as a moment of change. To be significant in 3CA terms, an event must significantly decrease the control over subsequent events and/or increase significantly the risk of subsequent unwanted events. The analysis begins by identifying a set of significant events from the wider collection of events that comprise the incident. The outcome of this part of the 3CA process is a list of the events marking important moments of unwanted change. It is important that you select items for analysis from a full, rather than a partial set of events. If the picture of what happened, and how, is incomplete, you may miss events that warrant inclusion in the analysis. To ensure completeness, you might consider using an ‘event sequencing’ method (such as Events and Conditional Factors Analysis – ECFA, ECFA+ or other).

The detailed step-by-step recommendations, aids and tips on how to perform the 3CA procedure, including an illustrated approach to 3CA (see Figure 2.1.23.) and a system prompt list, are presented in [73].

Table 2.1.3. Schematic showing sequence of the 3CA analysis [73]

(1) Significant EVENTS	(2) Safety Barriers & Work Controls	(3) Priority for analysis	(4) Difference between situation in incident and expectations in (2)	The difference between the observed and expected behaviour is because...		
				(5a) "Original logic"	(5b) Systems	(5c) Organisational & Cultural Factors
						
						

3CA Control Change Cause Analysis

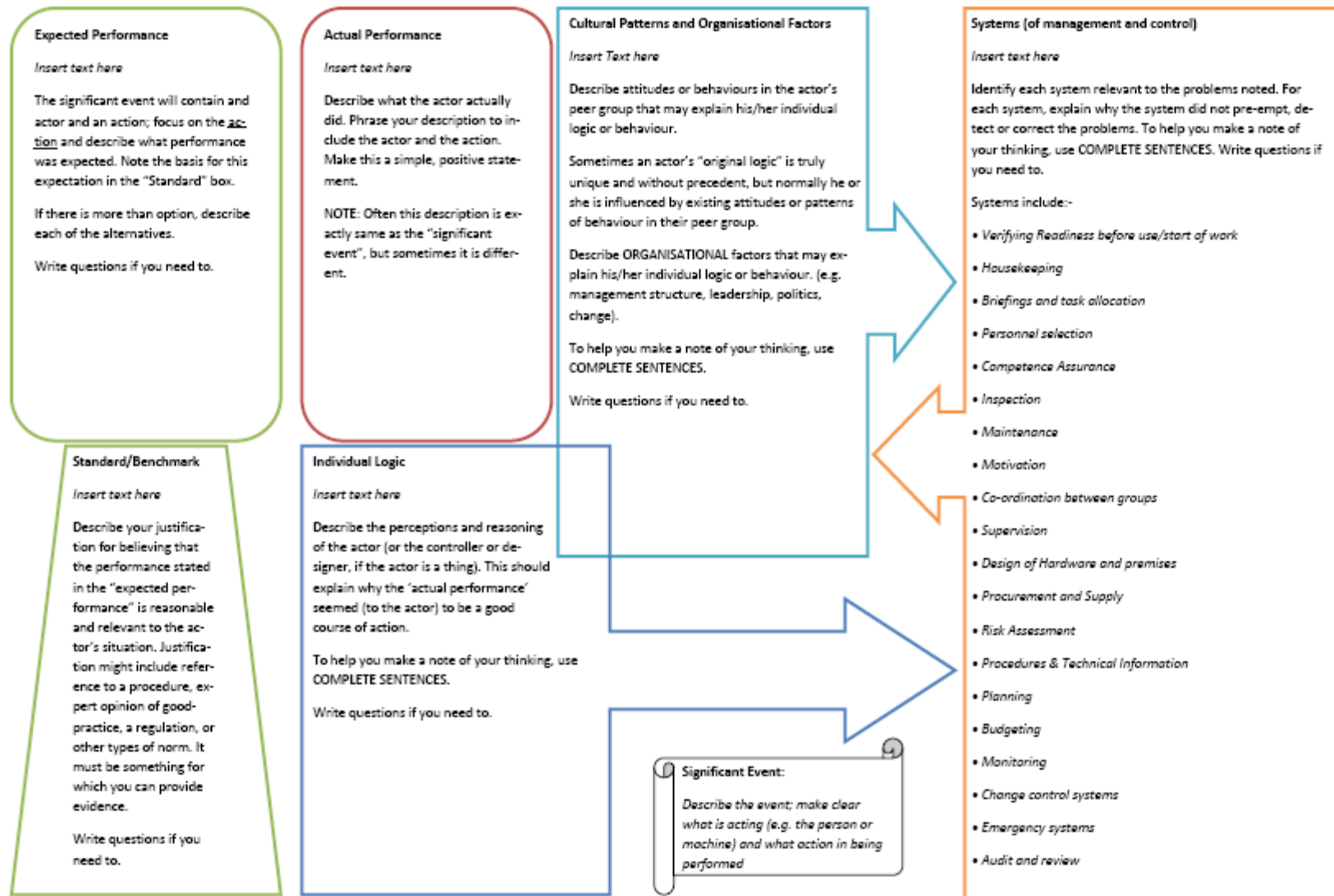


Figure 2.1.23. Diagram showing how to perform 3CA using a graphical approach [73]

2.1.11. FRAM - Functional Resonance Analysis Method

The Functional Resonance Accident Model, with its associated Functional Resonance Analysis Method (FRAM), considers safety as an emergent property of the socio-technical system as a whole [118]. Rather than physical components and sequences of events, functions and function performance are the units of analysis. A function may be defined as ‘a set of actions that a system performs or is used for, which are valuable for the achievement of a set of goals’. FRAM embodies a systemic approach for accident analysis and is based on four principles:

1. Both successes and failures result from the adaptations that organisations, groups, and individuals perform in order to cope with complexity. Success depends on their ability to anticipate, recognise, and manage risk. Failure is due to the absence of that ability (temporarily or permanently), rather than to the (organisational, human or technical) inability of a system component to function normally.
2. Complex socio-technical systems are by necessity underspecified and only partly predictable. Procedures and tools are adapted to the situation, to meet multiple, possibly conflicting goals, and hence, performance variability is both normal and necessary. The variability of one function is seldom large enough to result in an accident.
3. The variability of multiple functions may combine in unexpected ways, leading to disproportionately large consequences. Successes and failures are therefore emergent phenomena that cannot be explained by looking solely at the performance of (organisational, human or technical) system components.
4. The variability of a number of functions may resonate, causing the variability of some functions to exceed normal limits, the consequence of which may be an accident. FRAM as a model emphasises the dynamics and non-linearity of this functional resonance, but also its non-randomness. FRAM as a method therefore aims to support the analysis and prediction of functional resonance in order to understand and avoid accidents.

FRAM takes into account the non-linear propagation of events based on the concepts of normal performance variability and functional resonance. The analysis consists of four steps (that may be iterated):

Step 1: Identifying essential system functions and characterising each function by six basic parameters. A function is defined as an action of a component of the system. The nature of the functions may be technological, human, organisational, or a combination of human, technology and/or organisation. The functions are described in terms of six aspects: their input (I, that which the function uses or transforms), output (O, that which the function produces), preconditions (P, conditions that must be fulfilled to perform a function), resources (R, that which the function needs or consumes), time (T, that which affects time availability), and control (C, that which supervises or adjusts the function). They may be described in a table and subsequently visualised in a hexagonal representation (FRAM module, Figure 2.1.24). The main result from this step is a FRAM ‘model’, with all basic functions identified.

Step 2: Characterising the (context dependent) potential variability through common performance conditions. Eleven common performance conditions (CPCs) are identified in the FRAM method to be used to elicit the potential variability: (1) availability of personnel and equipment; (2) training, preparation, competence; (3) communication quality; (4) human–machine interaction, operational support; (5) availability of procedures; (6) work conditions; (7) goals, number, and conflicts; (8) available time; (9) circadian rhythm, stress; (10) team collaboration; (11) organisational quality. These CPCs address the combined human, technological, and organisational aspects of each function. After identifying the CPCs, the variability needs to be determined in a qualitative way in terms of stability, predictability, sufficiency, and boundaries of performance.

Step 3: Defining the functional resonance based on possible dependencies/couplings among functions and the potential for functional variability. The output of the functional description of step 1 is a list of functions, each with their six aspects. Step 3 identifies instantiations, which are sets of couplings among

functions for specified time intervals. The instantiations illustrate how different functions are active in a defined context (see Figure2.1.25). The description of the aspects defines the potential links among the functions. For example, the output of one function may be an input to another function, or produce a resource, fulfil a precondition, or enforce a control or time constraint. Depending on the conditions at a given point in time, potential links may become actual links; hence adjustment of the model for those conditions is recommended. The potential links among functions may be combined with the results of step 2, the characterisation of variability. That is, the links specify where the variability of one function may have an impact, or may propagate. This analysis thus determines how resonance can develop among functions in the system. For example, if the output of a function is unpredictably variable, another function that requires this output as a resource may be performed unpredictably as a consequence. Many such occurrences and propagations of variability may have the effect of resonance; the added variability under the normal detection threshold becomes a ‘signal’, a high risk or vulnerability.

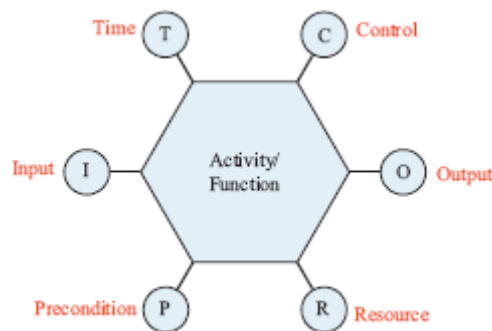


Figure2.1.24. Example of a FRAM module [118]

Step 4: Identifying barriers for variability (damping factors) and specifying required performance monitoring. Barriers are hindrances that may either prevent an unwanted event taking place, or protect against the consequences of an unwanted event. Variability is materialised due to trade-offs in face of multiple conflicting goals within available time. In this context, it is necessary to have barriers that both damp unwanted variability and facilitate desirable variability. Hence, barriers can be seen as both hindrances and enablers. On the one hand, barriers may either prevent an unwanted event from taking place, or protect against the consequences of an unwanted event. On the other hand, they may enhance the capabilities allowing the system to continue its operation. Barriers can be described in terms of barrier systems (the organisational and/or physical structure of the barrier) and barrier functions (the manner by which the barrier achieves its purpose). In FRAM, four categories of barrier systems are identified.

Compared with other accident analysis methods, for example STEP, FRAM refrains from looking for human errors and safety problems, but tries to understand why the incident happened. Since FRAM addresses both normal performance variability and the specifics of an adverse event, it broadens data collection of the analysis compared to a STEP-driven analysis: thus the development of the incident is contextualised in a normal socio-technical environment. Through asking questions based on the common performance conditions and linking functions in instantiations, FRAM identifies additional factors and the context of why performance varied becomes apparent.

In relation to the question of when each method should be used, the type of incident and system to be analysed needs to be taken into account. With respect to other methods, FRAM is better suited to describing tightly coupled, intractable systems of which the system described in [118] is an example. Because FRAM does not focus only on weaknesses but also on normal performance variability, this provides a more thorough understanding of the incident in relation to how work is normally performed. Therefore, FRAM may lead to a more accurate assessment of the impact of recommendations and the identification of factors left unexplored with other methods that may have a safety impact in the future.

While the chain of events is suited for failures of one or more components,, it is less adequate to satisfactorily explain system accidents.

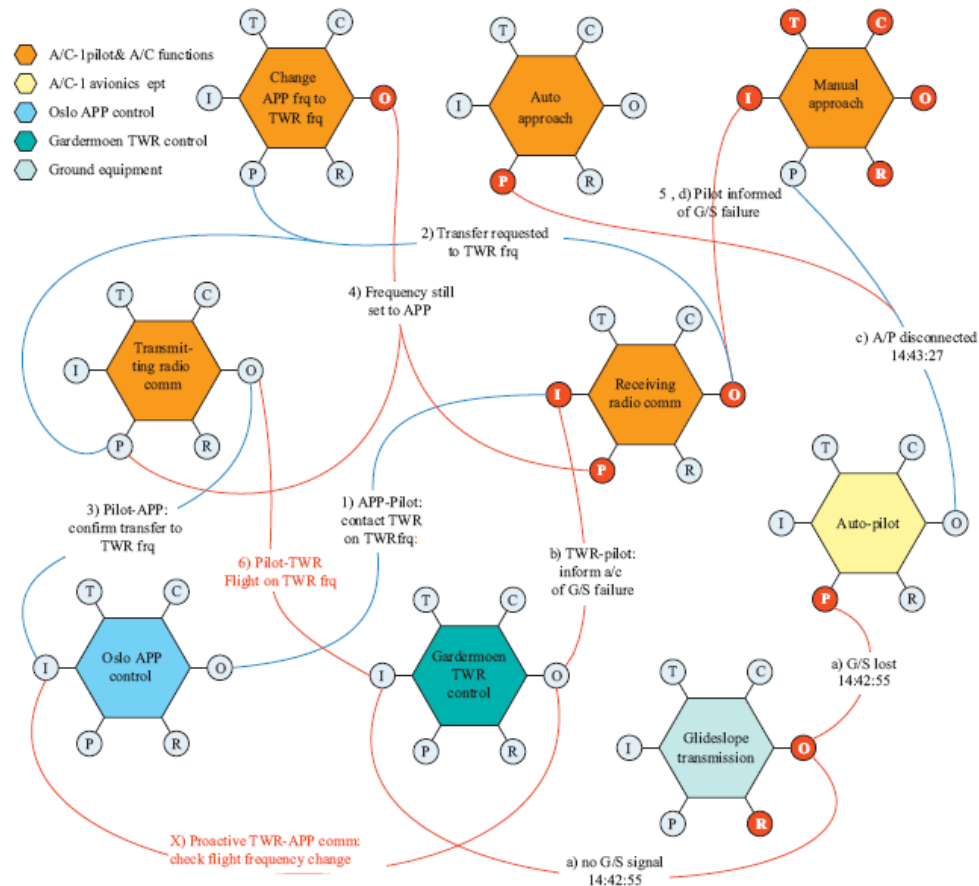


Figure 2.1.25. Example of a FRAM instantiation applied to air traffic incident NAX541 [118]

Three practical implications are found. The first is that FRAM provides new ways of understanding failures and successes, which encourages investigators to look beyond the specifics of the time sequence and failure under analysis, moving the analysis into the conditions of normal work. The second is that FRAM models and analyses an intractable socio-technical system within a specific context. Third, since other accident analysis methods, for example STEP, and FRAM are based on different understandings of the nature of accidents, their combined application during accident analysis provides complementary perspectives, and may contribute to a more comprehensive understanding of, and more effective learning from, an incident or accident.

While FRAM as a model has been accepted in the majority of discussions with practitioners and seems to fulfil a need for understanding intractable systems, as a method it is still young and needs further development.

2.1.12. CAS-HEAR - Computer-Aided System for Human Error Analysis & Reduction

2.1.12.1. Underlying model of CAS-HEAR

To conduct a systematic and thorough analysis of human error in an accident, it is essential to understand the process of accident causation. Of the aforementioned techniques, some are based on a model of accident causation. The models, however, do not include all elements related to the occurrence of an accident; hence, analyses using these techniques may be effective but are ultimately incomplete.

A managerial error analysis system, referred to as HEAR (Human Error Analysis & Reduction), was developed for use in the Korean railway industry [17]. HEAR, which includes a detailed procedure,

useful tools, and recording forms, was initially developed for human error analysis [65]. CAS-HEAR (Computer-Aided System for HEAR), a web-based system, was then designed to increase the quality and efficiency of human error analysis using the HEAR procedure. To develop HEAR and CAS-HEAR, the advantages and disadvantages of existing techniques for human error analysis were thoroughly reviewed, and a complete model of accident causation was developed, from which the main components of the analysis are derived (see Figure 2.1.26).

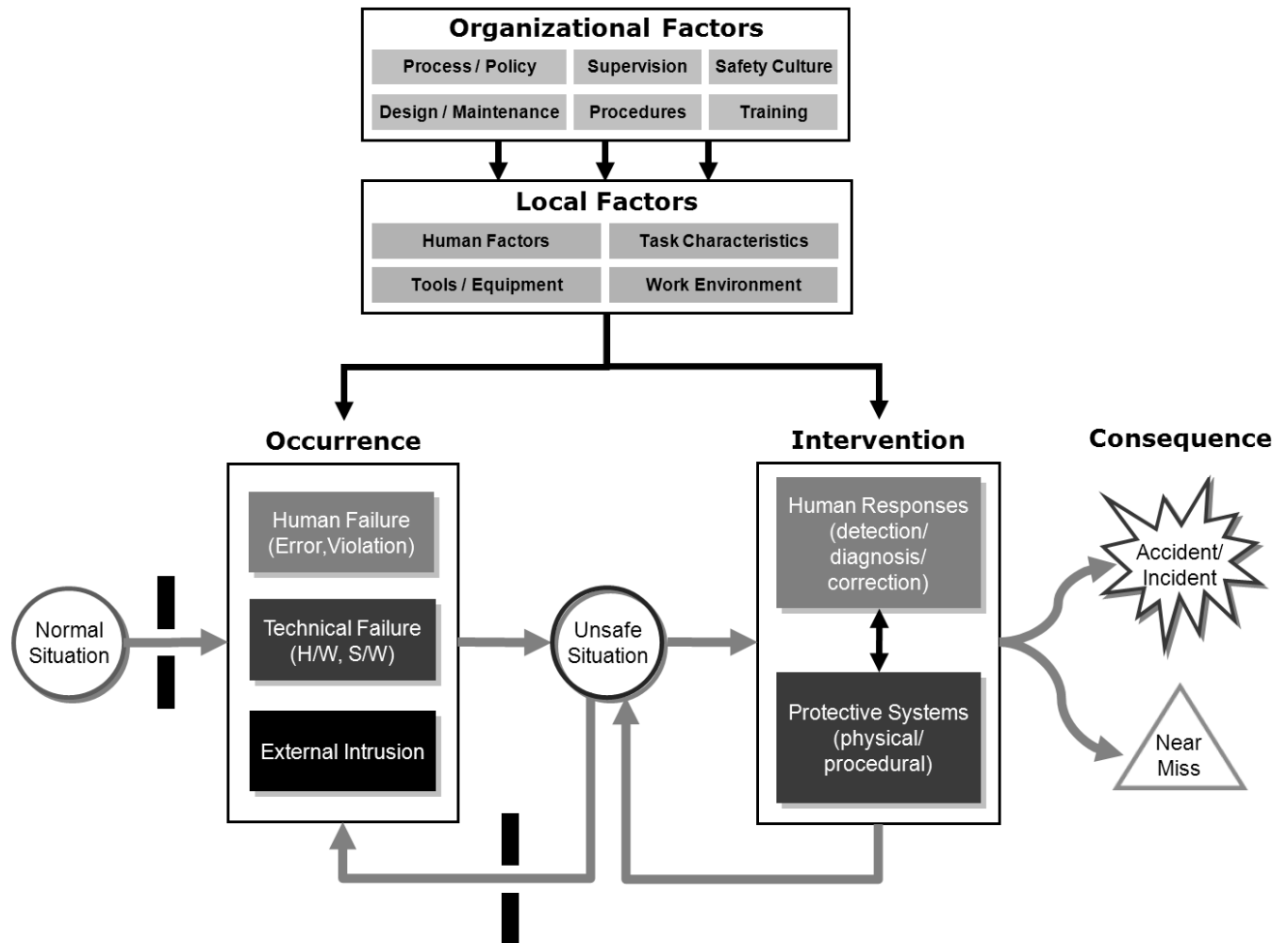


Figure 2.1.26. Accident causation model of CAS-HEAR [17]. H/W – hardware, S/W - software

The model explains how an accident or a near-miss occurs, what types of events can contribute to the accident, which factors can influence the events, and how to prevent an event or an accident. For an accident to occur, the initiating event must occur by penetrating barriers in a normal situation. There are three types of events: 1) human failure (error or violation by an operator); 2) technical failure (a fault in hardware or software); 3) external intrusion (e.g. a person on the railway tracks). When an event occurs, the entire system in operation enters into an unsafe situation. In this situation, another event occurs by breaking through the barriers, or humans or protective systems detect and recover from the event. In the latter case, if the intervention is implemented in a timely and accurate manner, or if luck is involved, a near miss results; otherwise, an accident/incident results, with loss of life and/or property, or the entire system continues in the risky and sometimes worsened situation. According to this model, human error can occur at two different stages: the ‘occurrence’ stage and the ‘intervention’ stage. In other words, human error can be not only a new event, but also a failure of human responses to events that have already occurred. A variety of factors can cause human error. Local factors which include human factors, task characteristics, tools/equipment, and the work environment influence human performance directly. Likewise, local factors are under the influence of organisational factors that include

organisational processes/policies, supervision, the safety culture, system design and maintenance, procedures, and training.

This model can help prevent analysts from missing any important aspects of human error analysis, which include event sequence analysis, context analysis, root cause analysis, barrier analysis, and the analysis of error detection and recovery processes.

2.1.12.2. Procedure of CAS-HEAR

The procedure of CAS-HEAR was developed based on the aforementioned model of accident causation. It also maximised the strengths and minimised the weaknesses of the earlier techniques, considering both the quality and efficiency of human error analysis. The analysis procedure and data flow of CAS-HEAR are depicted in Figure 2.1.27. The procedure consists of nine steps. It starts by selecting the human errors to be analysed in detail and ends after evaluating the corrective actions that are developed. This procedure is a 'Lite' version of the original HEAR [17, 65], which omits some parts judged to be inadequate for a computer-based analysis. It is assumed that all related information (e.g. physical evidence, documents, and the initial statements of people involved) has been collected and that the accident sequence analysis has already been completed. For each step, worksheets and guidelines are provided.

Full details of the separate steps of the CAS-HEAR procedure are as follows:

1. Select human errors to be analysed.

Human errors to be analysed are selected from the accident sequence. In other words, the analyst determines the critical human errors for each of which a detailed causal analysis is needed. Essentially, it is recommended that analysts select all human errors in the sequence. However, in cases that involve numerous human errors, it may be inefficient to perform a causal analysis (Step 3 - Step 6) of all human errors. For this reason, a number of elimination criteria (e.g. 'Human errors triggered by the preceding error, if there is no particular cause except the preceding human error, can be eliminated.') are given.

2. Analyse the context.

For each of the human subjects who committed the selected errors, the context is analysed. Four tables are provided for analysing, respectively, operator-related, task-related, environment-related, and organisation-related contexts. Each table consists of approximately 11 factors, with a total of 45 factors. For each factor, the content is recorded and the degree of influence on the accident is rated on a five-level scale, ranging from 'very low' to 'very high'. Each contextual factor has links to the causal factors analysed in Step 4, and causal factors related to the contextual factors rated as 'high' or 'very high' are highlighted, to support the task of identifying error causes. For each of the selected human errors, Steps 3 to 6 are iterated.

3. Identify error types.

First, the task types related to the error are selected. Second, the error types are determined. CAS-HEAR provides five error types. Four of these are based on a model of human decision making — perception error, situation assessment error, decision-making error, and execution error. The other type refers to violations. Each type is re-divided into several sub-types. More than two types can be selected.

4. Identify error causes.

All factors that influenced the occurrence of the error, often known as 'performance-shaping factors (PSFs)', are identified, by using a given classification scheme. The classification scheme has 13 categories: the mental states of the operators, the physical states of the operators, the knowledge/experiences/abilities of the operators, task characteristics, tools/equipment, the work environment, training/infrastructure, rules/procedures, human resource management, communications, team factors, supervision, and the organisational processes/policies/culture. Each category consists of approximately 10 factors, with a total of 138 causal factors. The classification scheme also includes causal links between the factors in order to reduce the complexity of finding the root causes. As mentioned above, causal factors linked to contextual factors rated as problematic in Step 2 are

considered as candidate causes. After a causal factor is selected as an error cause, other factors that influenced the factor are identified by following the causal links. This process is repeated until the root causes of the error are found. While finding error causes, a why-because tree, which depicts all causes of an error and their causal relationships, is automatically drawn.

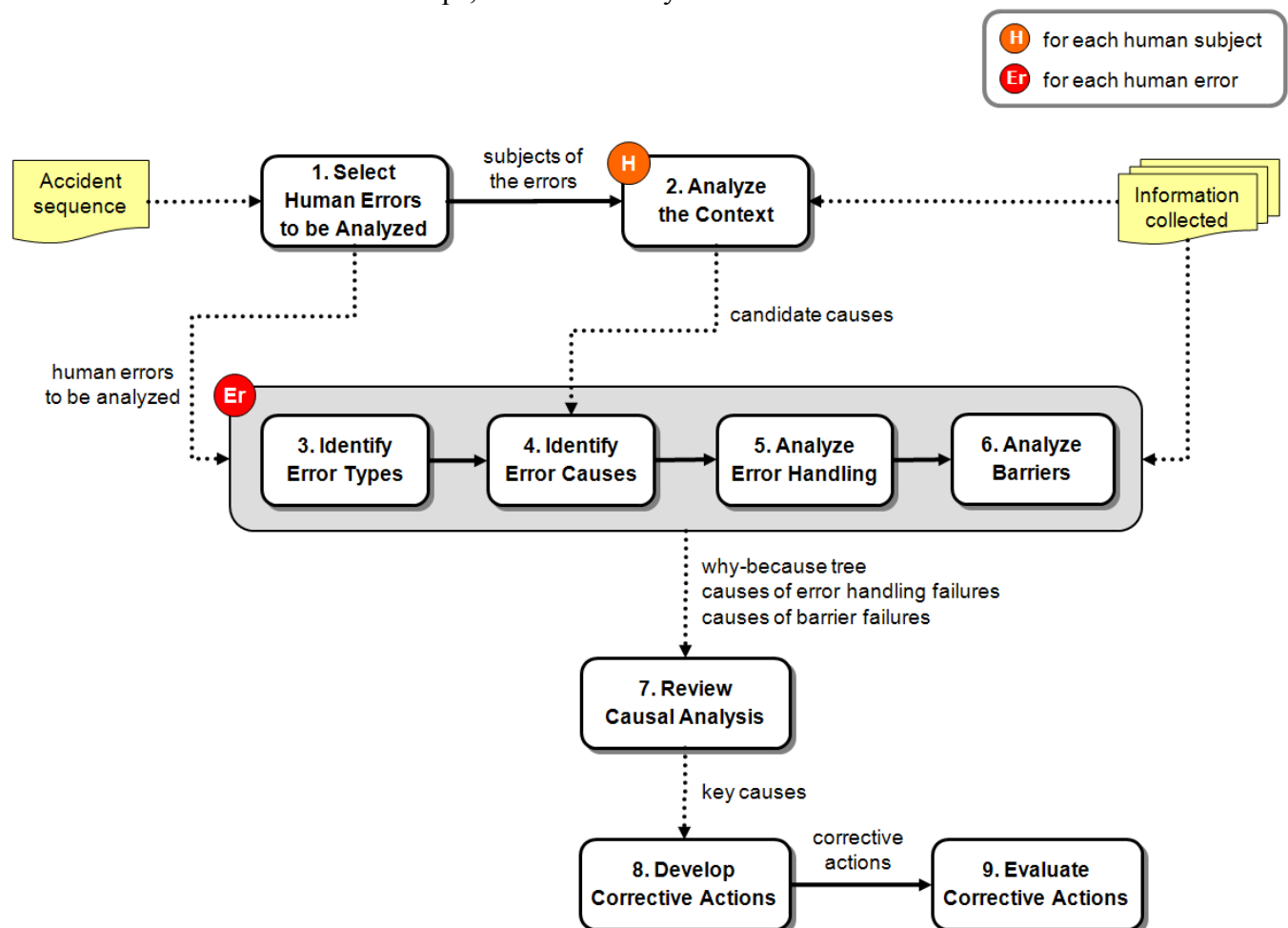


Figure 2.1.27. The CAS-HEAR procedure and data flow [17]

5. Analyse error handling.

Error handling processes, including error detection and recovery, are analysed. First, factors related to when, how and by whom the error was detected are analysed. Then, if the error was detected by someone, when, how and by whom the error was recovered from, are analysed. Lastly, the factors that had positive or negative influences on the detection and recovery processes are identified.

6. Analyse barriers.

First, there is an analysis of whether or not barriers existed that could have prevented the error from occurring. If they existed, the reason behind the failure of each barrier is analysed. Second, there is an analysis of whether or not barriers existed that could have prevented the error from proceeding to an accident. If they existed, the reasons for the failure of each of these barriers are analysed. A barrier can be of two types: the first is a physical barrier, such as an automatic train control (ATC) system; the second is an administrative or procedural barrier, such as standard operating procedures (SOPs).

7. Review causal analysis.

In this step, the analysis results of Steps 3 to 6 (i.e. the types and the why-because tree of each error, the factors that had negative effects on error detection and recovery, and the failed barriers and their causes) are put together. The key causes of the accident are then determined.

8. Develop corrective actions.

For the key causes, corrective actions are derived in two dimensions. The first of these focuses on improving physical systems, while the second focuses on improving administrative systems and procedures. For each category, several subcategories are provided, so that analysts can develop corrective actions from various viewpoints.

9. Evaluate corrective actions.

Each corrective action developed in the previous step is evaluated by four criteria, which are adapted from SMARTER (specific, measurable, accountable, reasonable, timely, effective, and reviewable) of TapRooT® [20].

Major Aiding Features of CAS-HEAR

There is no doubt that root cause analysis, which corresponds to Step 4 of the CAS-HEAR procedure, is the most important and demanding step in an accident analysis or human error analysis. Although many existing techniques provide a comprehensive taxonomy of causal factors, it is often cognitively demanding and time-consuming to find the causes of a certain error from among so many (sometimes over a hundred) possible causes. Furthermore, even if a list of causes was selected from a classification scheme, determining causal relationships between the causes so that the root causes can be found is another complicated task. There is a strong need to maximise the efficiency of this process without losing the quality of the result. Thus, CAS-HEAR focuses on aiding the task of finding the root causes of human errors. For this, Hollnagel's ideas [64], linking causal factors ('genotypes' in his words) with contextual factors ('common performance conditions' in his words) and making links between causal factors, were refined and extended for practical use in the railway industry. Figure 2.1.28 shows a schematic picture of the links between contextual and causal factors and the links between causal factors. The links are predefined; they are incomplete but plausible. Contextual factors marked as problematic send their related causal factors (1.1, 1.2, 2.3, 2.1, 3.1, and 3.4 in Figure 2.1.28) to the 'error cause analysis' step, where the causal factors are highlighted and used as candidate causes. Causal factors marked as error causes (1.1 and 2.3), from both the highlighted and non-highlighted causes, send their related causal factors (1.7, 3.8, 4.1, 4.4, 9.5, 3.1, 6.1, 6.2, and 7.13) to the analysis of the second-level causes. Likewise, causal factors marked as second-level causes (9.5, 3.1, and 7.13) send their related causal factors to the analysis of the third-level causes. This is the method by which the error cause analysis of CAS-HEAR proceeds. If a causal factor selected as an error cause has no further link (9.10 and 7.17), other factors that are not linked to it are searched, or the cause analysis of the error ends.

Linking contextual factors with causal factors

As an accident or a human error occurs in a specific context, it is unnecessary to examine all causal factors in a given taxonomy; it is often impractical in the field because there are a great many accident or incident cases to be analysed, while time and resources are limited. For any given context, there are a number of causal factors that are more likely to apply compared to others. Therefore, it is often helpful to use the result of assessing the context as the basis for determining the probable causes of an error. As a starting point for this approach, a simple matrix is proposed [64], indicating the relationship between the common performance conditions (CPCs) and the main genotype groups. However, this simple matrix is not very helpful in practice. Hollnagel also noted that developing a specific version of the matrix is necessary for use in practice for a given domain. In CAS-HEAR, probable links between 45 contextual factors and 138 causal factors are provided. In other words, each contextual factor has links to causal factors related to it.

Context Analysis

Error Cause Analysis

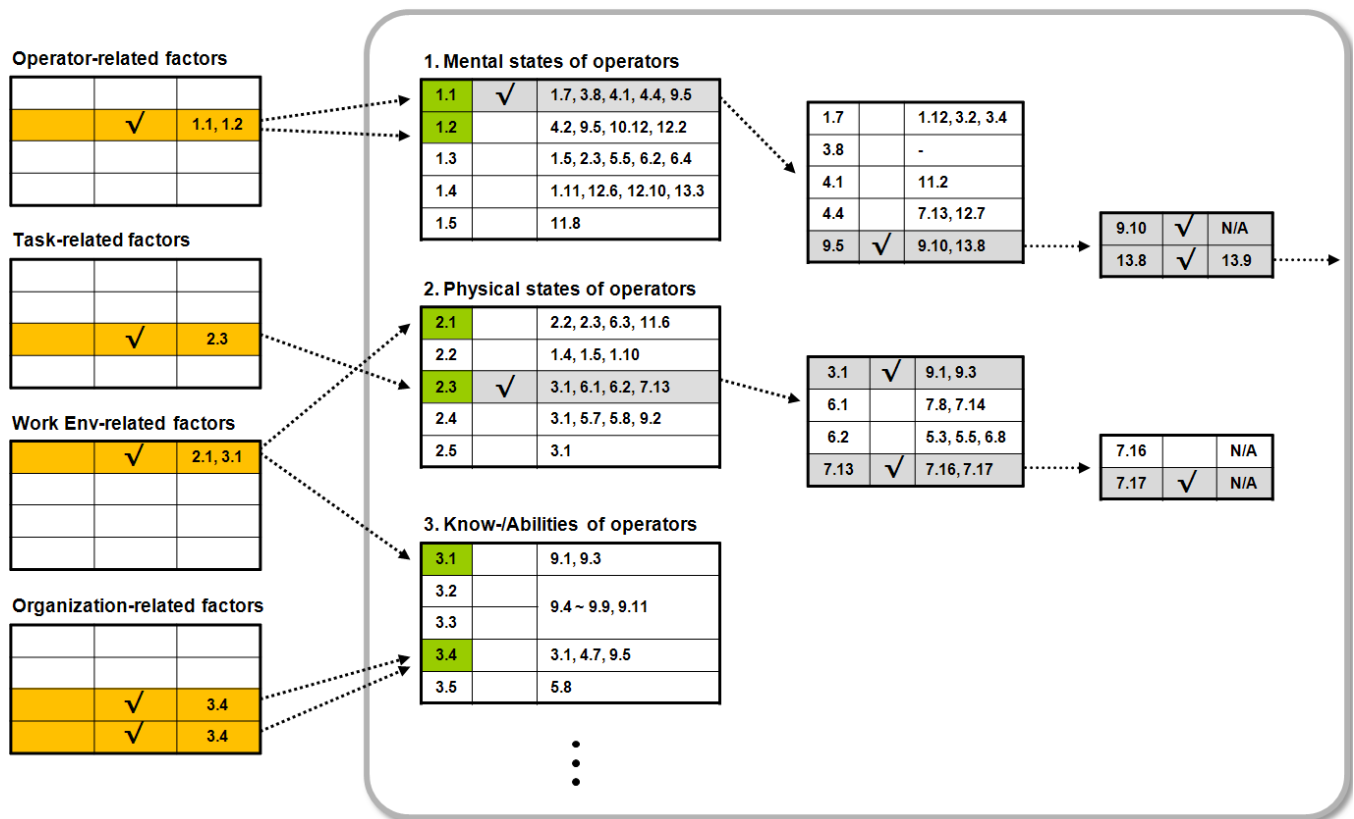


Figure 2.1.28. Links between factors of CAS-HEAR [17]

As mentioned in the description of the CAS-HEAR procedure, the analysis of the context is conducted as the second step of CAS-HEAR. Figure 2.1.29 displays part of the context analysis. For each human subject, four tables (operator-related, task-related, environment-related, and organisation-related) are recorded. While the content of a contextual factor is recorded, the corresponding contents of other subjects are shown on the left side of the display as a reference. This aiding feature will be particularly helpful when analysing the environment-related and organisation-related factors; in many cases, the subjects involved in an accident are in the same work environment and in the same organisation. If the influence on the accident of a contextual factor is rated as 'high' or 'very high', such as 'sleeping hours' in Figure 2.30, the causal factors (e.g. 'physical fatigue') related to it are highlighted in the 'error cause analysis' (Step 4) for human errors by the subject, as shown in Figure 2.31. The highlighted causal factors can be used as candidate causes of the errors. In addition, part of the results of the context analysis related to the highlighted causal factors is presented on the left side of the display for reference. The predefined links between contextual factors and causal factors are not complete, but they reduce the complexity of the analysis. The analysis of the context enables a prior sensitisation of the various causes, but it cannot lead to the exclusion of any of them. The highlighted causal factors should not be used as absolute criteria, but only as a reference.

Linking between causal factors

Accidents occur due to multiple layers of factors rather than one factor alone. Most human errors also occur due to several levels of causes. Therefore, for an effective error analysis, not only the immediate causes but also the root causes of the error should be determined. Although a large number of classification schemes for error causes have been used in various industries, it is not easy to find the root causes of an error using these schemes. They merely provide a list or a structured taxonomy of possible error causes, and do not produce information about relationships between the error causes. If possible relationships between various causes are provided, the root causes of an error will be found relatively

easily. To determine completely the causal links between causal factors is impossible, but it is possible to establish effective links based on theory and experience.

In contrast to other classification schemes, CREAM [65] provides possible links between the groups of error causes. However, the elements and links between them should be extended for practical use in a particular domain. Considering these limitations of existing schemes, CAS-HEAR selected 138 causal factors for the railway industry, classified them into 13 categories, and determined possible causal links between the 138 causal factors.

Driver (#2661) 2. Analyze the Context

Profile
Operator-related
Task-related
Environment-related
Organization-related

Results of Other Subjects

1. Driver (#303)

1) Day before accident : 4 hr
2) Avg. of the week before accident : 4 hr

Note:

1) For drivers, record their experiences on the kind of the train (e.g., years, mileage) in the remarks column.

2) In the remarks column, additional explanations of the factors are recorded.

Factor	Content	Influence on the accident					Remarks
		Very Low	Low	Med	High	Very High	
1. Length of work experience	0 yr 6 mo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
2. Physical check-up results	1) Last check-up date : 2007 yy 10 mm 2) Any special results : N/A	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
3. Aptitude test results	1) Last test date : 2007 yy 10 mm 2) Any special results : N/A	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
4. Awareness of task-related rules or procedures	<input type="radio"/> fully aware <input type="radio"/> partly not aware <input checked="" type="radio"/> wrongly aware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
5. Training	1) Last training date: 2007 yy 5 mm 10 dd 2) Training hours : 4 hr 3) Training content : operating procedures for emergency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
6. Disease/Alcohol use	1) Disease present at the time : ankle sprain 2) Intoxicated : <input type="radio"/> yes <input checked="" type="radio"/> no	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7. Sleeping hours	1) Day before accident : 3 hr 2) Avg. of the week before accident : 4 hr	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
8. Emotional state	<input checked="" type="radio"/> normal <input type="radio"/> nervous <input type="radio"/> depressed <input type="radio"/> excited <input type="radio"/> etc	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
9. Satisfaction with one's tasks/roles	<input type="radio"/> high <input checked="" type="radio"/> medium <input type="radio"/> low	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
10. Accident history	1) yy mm accident Causes : 2) yy mm accident Causes :	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Prev Next

Figure 2.1.29. CAS-HEAR display for context analysis [17]

In the analysis of the causes of an error (Figure 2.1.30), when the analysis of a category (e.g. ‘2. Physical states of operators’) was completed, and if more than one factor (e.g. ‘2.1. physical fatigue’) in the category were checked as error causes, the analyst clicks the button ‘why-because tree’. A new window displaying a why-because tree of the error then appears, as shown in Figure 2.1.31. A description of the error at hand is in the first column of the table; factors that have been checked as error causes, the first-level causes, are shown in the second column.

Why-Because Tree
Human error #1 ▾ 4. Identify Error Causes ▾

Profile of Human Error

Human error #1

1) Subject : driver(#2661)
2) Details :
The driver did not observe the red signal, so did not reduce the speed of the train(#2661)

Related Contextual Factors

1. Sleeping hours

1) Day before accident : 3 hr
2) Avg. of the week before accident : 4 hr

1. Mental states

2. Physical states

3. Know-/Exp-/Abilities

4. Task char.

5. Tools/Equipment

6. Work environment

7. Train/Infrastructure

8. Rules/Procedures

9. HRM

10. Communications

11. Team factors

12. Supervision

13. Org. processes/policies/culture

2. Did physical states of the operator affect the error?

(Describe the details)

Check all factors that were associated with the occurrence of the error.

Code	✓	Causal Factor	Description
2.1	<input checked="" type="checkbox"/>	Physical fatigue	Fatigue e.g. due to long shift or lack of rest
2.2	<input type="checkbox"/>	Physical illness	The symptoms of physical illness (e.g. fever, headache)
2.3	<input type="checkbox"/>	Alcohol or drug use	Use of alcohol or drugs prior to or during working hours
2.4	<input type="checkbox"/>	Temporary visual or hearing impairment	The sense of sight or hearing was impaired temporarily e.g. due to tunnel pass or noise.
2.5	<input type="checkbox"/>	Physical properties	Worker's physical properties (e.g. height, weight, hand size) were inadequate for the task or tools/equipment.
2.6	<input type="checkbox"/>	General motor ability	Lack of motor abilities to perform a task (e.g. muscular strength, agility)
2.7	<input type="checkbox"/>	Age/ gender	Worker performance was influenced by age- or gender-related factors
2.8	<input type="checkbox"/>	Etc. (description needed)	

Prev Next

Figure 2.1.30. CAS-HEAR display for error cause analysis: the main window

http://aig.kaist.ac.kr - Why-Because-Tree - Microsoft Internet Explorer

Human Error	1st Level Cause	2nd Level Cause	3rd Level Cause	4rd Level Cause
<div style="border: 1px solid black; padding: 5px; width: 100px; margin: 0 auto;"> The driver did not observe the red signal, so did not reduce the speed of the train (#303) </div>	1.4 Complacency/absent-mindedness			
	2.1 Physical fatigue			
	7.2 Inadequate location of signals or signs			

http://aig.kaist.ac.kr/cause_analysis/popRelateCauseTable.php?strCause=2.1&strLevel=2&strYP...

Related Contextual Factors

1. Working hours

1) Day before accident : 11 hours
2) Avg. of the week before accident : 10 hours

Search

Code	✓	Causal Factor	Description
2.2	<input type="checkbox"/>	Physical illness	The symptoms of physical illness (e.g. fever, headache)
2.3	<input type="checkbox"/>	Alcohol or drug use	Use of alcohol or drugs prior to or during working hours
6.3	<input checked="" type="checkbox"/>	Temperature/humidity	Effect of uncomfortably hot/cold or dry/humid conditions
11.6	<input type="checkbox"/>	Lack of staff	Adequate numbers of personnel were not available to perform the task.
12.3	<input checked="" type="checkbox"/>	Poor management of working hours	Long or irregular working hours

Confirm Cancel

Figure 2.1.31. CAS-HEAR display for error cause analysis: pop-up windows

For each first-level cause, the second-level causes should be found. When ‘find the next level of causes’ is selected from a context menu, which is created by pressing the right button of the mouse, a new smaller window appears. It shows a list of possible second-level causes from the predefined links between causal factors. The results of the context analysis are also used in this window. Among the causes in the list, causal factors that are related to contextual factors rated as problematic are highlighted (e.g. ‘inadequate management of working hours’ in Figure 2.1.31). In addition, part of the results of the context analysis, which is related to the highlighted causal factors, is presented on the top of the window

as a reference. If there is no appropriate factor in the list, searching for other factors by typing in keywords is possible. Factors that are selected as the second-level causes, whether highlighted or not, are placed in the third column of the table. The causal relationships between the first-level and the second-level causes are indicated using an arrow. In this way, the third-level, fourth-level, and fifth-level causes (and other causes, if they exist) can be found. This process is continued until the root causes of the error are found. If a causal factor is selected in the pop-up window and generated in the why-because tree, it is also checked automatically in the main window of the error cause analysis. According to the predefined links, causal factors included in the latter categories, in particular the 12th and 13th categories, are more likely to be the root causes of an error.

The why-because tree is automatically generated while an error cause analysis is conducted. Figure 2.1.32 shows an illustration of a completed why-because tree. Marking a box (i.e. a cause) as the key cause of the error (e.g. the shaded boxes in Figure 2.1.32), deleting a box, and moving the location of a box are allowed using the context menu.

A prototype of CAS-HEAR, a web-based support system, was developed to reduce the high cognitive load in the analysis of human error and to improve the quality of the analysis. This system helps the analyst to find multiple levels of the causes of an error and their causal relationships, using predefined links between contextual factors and causal factors, and links between causal factors. In addition, the support system is based on a complete accident model, which helps the analyst to conduct a thorough analysis without missing any significant part of the human error analysis.

The procedure of CAS-HEAR was subjectively evaluated by experienced field analysts at KORAIL (Korea Railroad Corporation). Its usefulness in human error analysis was confirmed; in particular, the links between contextual and causal factors, and the links between causal factors, were recognised as highly effective and efficient. However, field applications of CAS-HEAR that are more extensive in scope are clearly needed before its actual use in the field. These tests are expected to be conducted when the system is fully implemented and its use in field analyses is approved by the relevant regulatory authorities.

Although CAS-HEAR was developed specifically for the railway industry, it can be used in other industries with minor modifications. Some aspects of the contextual factors and causal factors may need to be customised for a particular industry. The examination of the transferability of CAS-HEAR to other domains represents another potential future task.

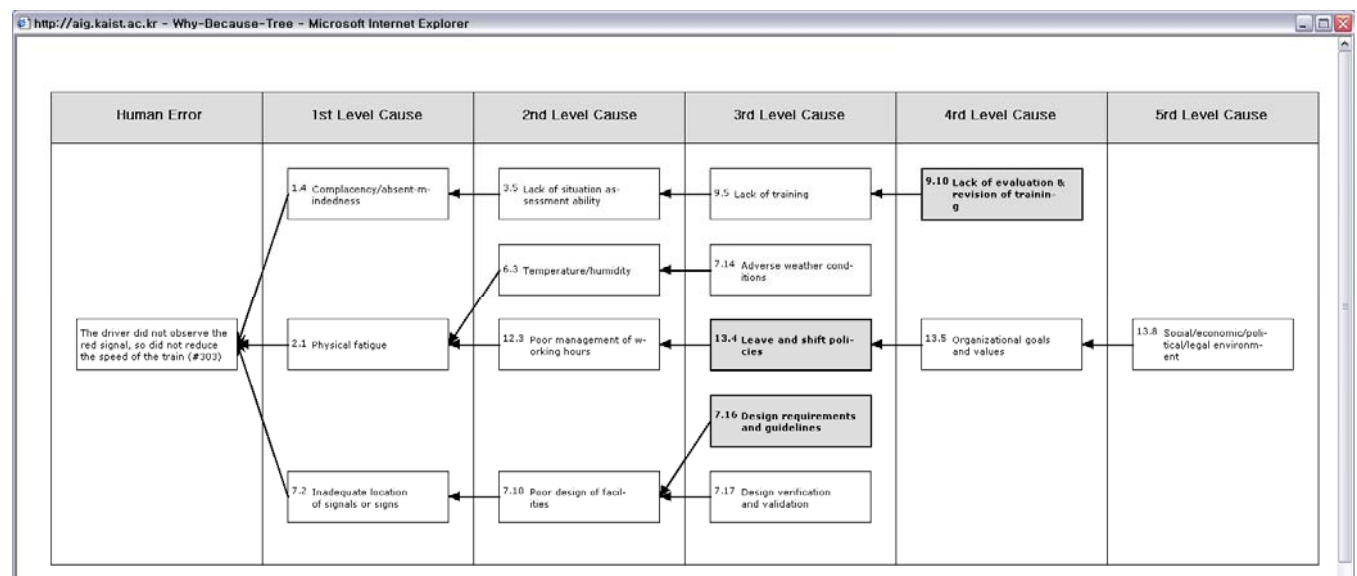


Figure 2.1.32. Why - because tree drawn by CAS-HEAR [17]

2.1.13. Apollo root cause analysis

Unlike the majority of previous root cause analysis methods, the Apollo Root Cause Analysis (ARCA) problem solving method does not use any pre-defined grouping or categorisation scheme or check list of possible causes or causal factors. The ARCA method is based on the assumption that the goal of the analysis is not to find the root cause, but to identify the most effective solution to prevent the primary effect. It is based on a Cause and Effect principle that holds true for everything that happens [25]. The Cause and Effect Principle provides four basic characteristics that allow us to understand reality in a simple, structured way. These four characteristics are as follows:

1. Cause and effect are the same thing;
2. Causes and effects are part of an infinite continuum.
3. Every effect has at least two causes in the form of actions and conditions;
4. An effect exists only if its causes exist at the same point in time and space.

Some specific terms and definitions are used in the ARCA process:

- Action causes – momentary causes that bring conditions together to cause and effect;
- Conditional causes – causes that exist over time prior to the companion action and create the relevant environment for event to occur;
- Elemental causal set – fundamental causal element of all that happens. It is made up of an effect and its immediate causes that represent a single causal relationship. The causes consist of an action and one or more conditions. Causal sets, like causes, cannot exist alone. They are part of a continuum of causes with no beginning or end.

The Apollo Root Cause Analysis method has four phases:

- Defining the problem;
- Creating a Realitychart;
- Identifying effective solutions;
- Implementing the best solutions.

The Apollo Root Cause Analysis (ARCA) starts with complete **problem definition**, which should include four elements, presenting answers to following questions: a) what is the problem (primary effect, recurrence of which should be prevented); b) when did it happen; c) where did it happen; d) what is the significance of the problem.

Creating a Realitychart has five elements or steps:

1. For each primary effect, ask ‘why’;
2. Look for causes of primary effect in actions and conditions;
3. Connect all causes with ‘Caused By’;
4. Support all causes with evidence;
5. End each cause path with a symbol ‘?’ or a reason for stopping.

Performing these five steps produces the elemental causal set, made up of an effect and its immediate causes – an action and one or more conditions. Then each cause is treated as effect, and the five-step procedure is repeated, generating the next elemental causal set. By continuing this process further, elemental causal sets are combined to form a reflection of common reality, just like a jigsaw puzzle – the Realitychart having no boundaries. If some elemental causal sets do not fit, they are probably part of another problem. Each causal path is ended with a symbol ‘?’ or when a valid reason for stopping is identified. A symbol ‘?’ indicates our point of ignorance, denoting our lack of knowledge and the need to get more information. There are four valid reasons for stopping the further expansion of the Realitychart: a) reaching the desired condition; b) reaching the situation without control; c) finding new primary effect when need to do a separate analysis is identified; d) finding other more productive cause paths.

Identifying effective solutions. Since an infinite number exists of causes of an event connected through causal relationships in many ways, an infinite number of possible solutions exist. The solution may affect one or several causes in a chain, such that the problem does not occur anymore, but the cause,

which could be fixed most effectively, does not have to be at the end of a cause and effect chain. The goal of the investigator is to find the best solution, which must meet the following criteria: a) prevent occurrence; b) be within our control; c) meet the set goals and objectives (not to cause other unacceptable problems and provide reasonable value for its cost). An effective solution is found by challenging each cause in the Realitychart and checking possible solutions against the best solution criteria.

Implementing the best solutions. Implementation of solutions should be based on the effective problem-solving programme, showing the inherent value of the identified most effective solutions and convincing all stakeholders about their effectiveness. This programme should be oriented to continuous improvement and institutionalisation of defined problems.

2.1.14. Other RCA related event investigation methods

Organisational accident theory and analysis.

Over the past decade a significant change has gradually occurred in how we perceive events—both accidents and incidents [98]. They are now understood not only as the immediate and direct consequence of adversely combined technical failures and/or human errors, but also as the result of a historical background and an unfavourable organisational context. A historical background, in as much as a number of decisions and unfavourable circumstances at safety level progressively generate a pre-accident situation, long before the occurrence of the initiating event and the triggering of the accident sequence. The historical context of the accident is analysed through the progression in time of the pre-accident situation (the ‘accident incubation period’). In addition, this situation of pre-accident safety deterioration may be worsened, speeded up, or even precipitated through specific conditions in the organisational context, such as increasingly heavy competition, new environmental and climatic conditions, etc. The analysis of these conditions and their impact on the organisation in charge of managing the hazardous system (aircraft fleet, nuclear power plants (NPP), chemical plant facilities, railway network, etc.) constitutes the second specific aspect of an organisational accident analysis.

The concept of organisational accidents refers to an accident examined from an organisational perspective. Here, organisation is taken in the broad sense of the term; it is the in-house organisation of the business directly implicated in the accident, but also, by extension, of other businesses or institutions indirectly implicated, including sub-contractors, safety control organisations, etc. It may extend to the organisation of an entire industrial sector. This point of view may be extended according to the requirements of the accident analysis and an effective curative or preventive action. The benefit of this concept is its capacity to escape the fatality of unforeseen accidents and repeated accidents or incidents, apparently all different, and to develop preventive action insofar as possible.

One of the most significant aspects of the theory of organisational accidents is that it considers the accident as resulting from concurrent local, technical and human causes, and broader organisational causes or factors, possibly generic, often pre-existing, which play an aggravating role in the case of a dysfunction, namely by reducing defences, or even by generating other dysfunctions which make it worse. Accident analysis, seen from this organisational angle, owes its richness to the construction (implicit or explicit) of what may be called an ‘organisational network’ of the accident. Little by little, the impact made by all those involved in various capacities in the accident, as well as by their institution and, within this institution, by their managers and senior managers responsible for the work organisation and work situations, leads to building empirically the actual accident network in time and space, and beyond the organisational theoretical structures. Acting in this way enables us to do something which is rarely done as a rule. That is, to highlight the consequences of the most recent decisions, taken in real time, at the moment of the accident or just before, as well as the most distant decisions, going back to the design stage of the technical installations or the setting up of the business organisation, the weaknesses of which were suspected, if not clearly identified, by their designers.

Standard accident analysis methods rely on ‘causal methods’; this approach demonstrates limitations with regard to taking into account interactions between events, temporal dependencies and non-causal

relations between events. In other words, these methods are insufficient to reveal the organisational factors at the origin of the occurrence and/or development of an accident. One way to progress in the field of accident analysis would be to carry out an analysis of the organisational type addressing three issues, as a complement to causal analysis:

- historical reconstitution of the event, going as far back as possible in order to ‘catch’ the first signs of situation deterioration;
- development of an organisational network of the event, or ‘laying bare’ the relations, dependencies and interactions of the actors involved and their entities, in order to locate the organisational dysfunctions;
- inspection of the organisation’s background in order, among other things, to identify decision making, and ‘re-question’ the role of managers and their level of implication in the occurrence of the event.

In conclusion, the approach recommended fits into a company policy of organisational vigilance concerning safety problems, contributing to a more effective prevention policy.

Methods for analysis of dynamic systems: GO method, digraph / fault graph, event sequence diagrams, Markov modelling, dynamic event logic analytical method and dynamic event tree analysis method [45].

The **GO method** is a success-oriented system analysis that uses 17 operators to aid in model construction [45]. It was developed by ‘Kaman Sciences Corporation’ during the 1960s for reliability analysis of electronics for the Department of Defense in U.S.

The GO model can be constructed from engineering drawings by replacing system elements with one or more GO operators. Such operators are of three basic types: (1) independent, (2) dependent, and (3) logic. Independent operators are used to model components requiring no input, and the dependent operators require at least one input in order to have an output. Logic operators, on the other hand, combine the operators into the success logic of the system being modelled. With the probability data for each independent and dependent operator, the probability of successful operation can then be calculated. The GO method is used in practical applications where the boundary conditions for the system to be modelled are well defined by a system schematic or other design documents. However, the failure modes are implicitly modelled, making it unsuitable for detailed analysis of failure modes beyond the level of component events shown in the system drawing. Furthermore, it does not treat common cause failures, nor provide structural information (i.e. the minimum cut sets) about the system.

The **fault graph method / digraph** matrix analysis uses the mathematics and language of graph theory such as ‘path set’ (a set of models travelled on a path) and ‘reachability’ (the complete set of all possible paths between any two nodes) [45]. Fault graphs are the natural evolutionary step over a traditional fault-tree model. A fault graph is a failure-oriented directed graph with logic connectives that allows cycles. For example, a system’s diagram could be constructed as a fault graph to trace the piping and instrumentation drawing (P&ID) of the system, but with logical AND and OR conditions added. Then the fault graph is analysed and evaluated with computer codes based on graph-theoretical methods [140].

This method is similar to a GO chart but uses AND and OR gates instead. The connectivity matrix, derived from the adjacency matrix for the system, shows whether a fault node will lead to the top event (see Figure 2.1.33).

The created matrices are then computer analysed to give singletons (single components that can cause system failure) or doubletons (pairs of components that can cause system failure). The Digraph method allows cycles and feedback loops, which make it attractive for a dynamic system. Figure 2.1.33 shows a success oriented system digraph of simplified emergency core cooling system.

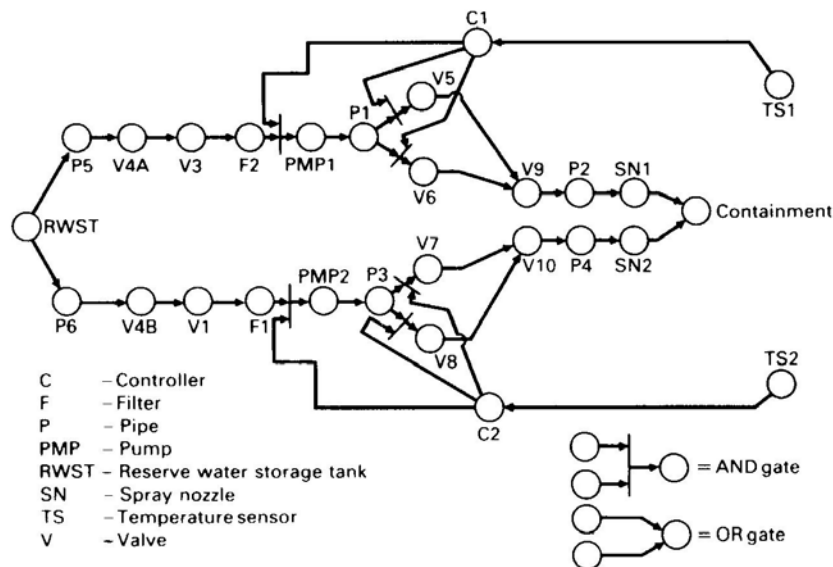


Figure 2.1.33. Success oriented system digraph of simplified emergency core cooling system in a nuclear power plant [45]

Markov modelling. Stochastic methods of system analysis, such as Markov Analysis, are also very useful types of quantitative analysis, in that multiple system states can be analysed using one system model. Markov modelling is a classical modelling method used for assessing the time-dependent behaviour of many dynamic systems. The Markov model depicts the system in all of its various possible failed states, and provides a method to determine the probability of being in any one state (see Figure 2.1.34) [29, 45]. The system is first modelled in all of its possible states. Then, the transition rates between operating states and failed states are determined. A set of differential equations is then solved, to determine the probability of being in any one given state. In ‘Markov chain’ processes, transitions between states are assumed to occur only at discrete points in time. On the other hand, in a ‘discrete Markov process’, transitions between states are allowed to occur at any point in time. For a process system, the discrete system states can be defined in terms of ranges of process variables as well as component status.

This method also incorporates time explicitly, and can be extended to cover situations where problem parameters are time independent. The state probabilities of the system $P(t)$ in a continuous Markov system analysis are obtained by the solution of a coupled set of first order, constant coefficient differential equations:

$$dP/dt = \mathbf{M} P(t),$$

where \mathbf{M} is the matrix of coefficients whose off-diagonal elements are the transition rate and whose diagonal elements are such that the matrix columns sum to zero.

One of the benefits of using Markov Analysis is that in addition to failure rates, the analysts can add ‘repair’ rates into the model, so that maintenance intervals can be established to provide adequate protection against the effects of significant latent failures in designs using fail-safe system architectures.

The dynamic event logic analytical methodology (DYLAM) provides an integrated framework to explicitly treat time, process variables and system behaviour [13, 45]. A DYLAM will usually comprise the following procedures: (a) component modelling; (b) system equation resolution algorithms; (c) setting of TOP conditions; (d) event sequence generation and analysis.

DYLAM is useful for the description of dynamic incident scenarios and for reliability assessment of systems whose mission is defined in terms of values of process variables to be kept within certain limits in time [19]. This technique can also be used for identification of system behaviour, and thus as a design tool for implementing protections and operator procedures.

It is important to note that a system specific DYLAM simulator must be created to analyse each particular problem. Furthermore, input data such as probabilities of a component being in a certain state

at transient initiation, independence of such probabilities, transition rates between different states, and conditional probability matrices for dependencies among states and process variables need to be provided to run the DYLAM package.

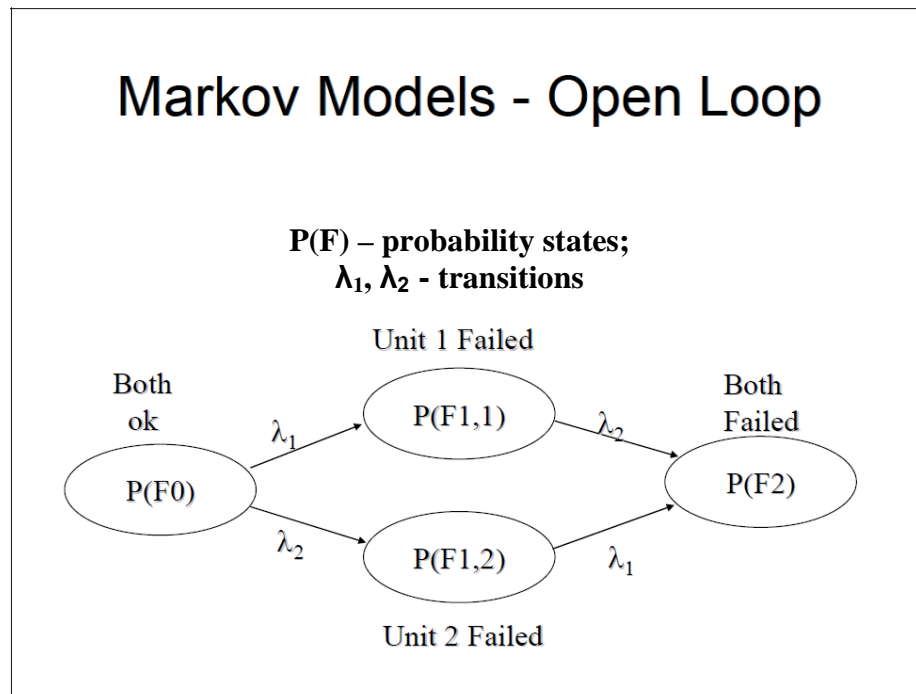


Figure 2.1.34. Example of an open loop Markov model [29, 45]

Dynamic event tree analysis method (DETAM) [45] is an approach that treats time-dependent evolution of plant hardware states, process variable values, and operator states over the course of a scenario. In general, a dynamic event tree is an event tree in which branching is allowed at different points in time. This approach is defined by five characteristics: (a) branching set; (b) set of variables defining the system state; (c) branching rules; (d) sequence expansion rule; (e) quantification tools. The branching set refers to the set of variables that determine the space of possible branches at any node in the tree. Branching rules, on the other hand, refer to rules used to determine when a branching should take place (a constant time step). The sequence expansion rules are used to limit the number of sequences.

This approach can be used to represent a wide variety of operator behaviours, to model the consequences of operator actions, and also serves as a framework for the analyst to employ a causal model for errors of commission. Thus it allows the testing of emergency procedures and identifies where and how changes can be made to improve their effectiveness.

The techniques discussed above address the deficiencies found in fault/event tree methodologies when analysing dynamic scenarios. However, there are also limitations to their usage. The digraph and GO techniques model the system behaviour and deal, to a limited extent, with changes in model structure over time. On the other hand, Markov modelling requires the explicit identification of possible system states and the transitions between these states. This is a problem, as it is difficult to envision the entire set of possible states prior to scenario development. DYLAM and DETAM can solve the problem through the use of implicit state-transition definition. The drawbacks to these implicit techniques are implementation-oriented. With the large tree-structure generated through the DYLAM and DETAM approaches, large computer resources are required. The second problem is that the implicit methodologies may require a considerable amount of analyst effort in data gathering and model construction.

2.1.15. Apparent Cause Analysis

When the number of available methods and tools for event investigation is permanently growing, the problem of RCA quality and its relation with so-called ‘shallow cause analysis -SCA’ (or ACA - ‘apparent cause analysis’) seem to be ever more important [56, 93]. Both SCA and ACA represent a less disciplined approach to operational reliability than true RCA.

According to event investigation hierarchy levels suggested by the IAEA [1], Apparent Cause/Specialist Investigation is a limited investigation to quickly and simply determine the most immediate, or apparent cause of a less significant event or sub-standard condition, without recourse to full root cause analysis, by considering the readily-available facts with little or no detailed investigation. One person may conduct this type of investigation, however this person needs to have an understanding of root cause techniques. SCA can be defined in an analogous way: it is a logical assumption of cause, based on the available facts and evaluator’s judgment, with minimum investigation, trying to save time and both financial and human resources. The typical tools of the ‘shallow cause analysis’ are 5-Why’s, a fishbone diagram and many form based RCA checklists [56].

Apparent Cause Analysis can be defined also as ‘Method to derive a cause with a minimum of investigation of the condition or event’ (one of definitions used in US nuclear plants) [93]. It is widely used in the nuclear industry, trying to save resources and to shorten the event investigation process. The real problem with Apparent Cause Analysis is the idea that one can skip some of the rigour of real root cause analysis, not ask as many questions, assume some facts, and even occasionally guess at the most likely cause, and that the results will be good enough to develop effective corrective actions and provide data to trend. However, RCA cannot be replaced by Apparent Cause Analysis, due to different approaches, rigorousness of analysis and capabilities to identify real root causes of an event. If actual root cause of an incident is not identified, even implemented corrective actions cannot be effective, and incidents or events will recur in the future.

A good illustration of such situations and comparison between Apparent CA (Symptom approach) and advanced RCA is given in [30]: ‘If we do a poor job of identifying the root causes of our problems, we will waste time and resources putting band-aids on the symptoms of the problem’.

Apparent CA - Symptom Approach:

- ‘Errors are often a result of worker carelessness.’
- ‘We need to train and motivate workers to be more careful.’
- ‘We don’t have the time or resources to really get to the bottom of this problem.’

Root Cause Approach

- ‘Errors are the result of defects in the system. People are only part of the process.’
- ‘We need to find out why this is happening, and implement mistake proofs so it won’t happen again.’
- ‘This is critical. We need to fix it for good, or it will come back and burn us.’

Some freedom in selection of event investigation methods also serves as a propensity to replace RCA, which requires a long time and a relatively large amount of resources, with the quickly performed, simple and cheap ACA. So, the criteria to determine the level of an event are not clearly defined: they are to be taken from organisation’s technical specifications and supporting procedures. To determine the level of investigation necessary, all incidents are screened against some pre-defined categorisation system. Here some sort of uncertainty always exists, because management may be able to use their discretion not to perform a root cause analysis on some events [1].

Conducting a Root Cause Analysis requires resources, so it is typically performed on events of high significance. A nuclear plant may in fact do five or maybe even ten good root cause analyses per year. In practice, despite the unquestionable deficiencies of ACA in comparison to RCA, sometimes NPPs do hundreds or even thousands of short-cut analyses, and try to implement thousands of ineffective corrective actions, based on guesses, and assumptions are driving their improvements.

2.1.16. HPEP - Human Performance Evaluation Process

The Human Performance Evaluation Process (HPEP) [4] is a resource for US Nuclear Regulatory Commission inspectors to use when reviewing licensee problem identification and resolution programmes with regard to human performance. Practically, HPEP is not designed for nuclear events investigation purposes. However, HPEP is very important and useful for learning and understanding how event investigation should be performed, and for further increasing the reliability of nuclear installations, because effectively working methods, based on practical experience, are presented for evaluation of investigations of human performance problems, root cause analyses and corrective actions. The HPEP review process consists of two parts. Part I provides a step-by-step process for reviewing licensee effectiveness in identifying, analysing and resolving human performance problems. The challenges in identifying and investigating human performance problems, available root cause analysis techniques, and characteristics of effective corrective action plans are also addressed in this part. The 1st part of the HPEP review process is organised as a series of tables that ask the inspector to answer evaluation questions in four areas. These areas are:

1. the licensee's identification and characterisation of human performance problems;
2. methods and information used to investigate human performance;
3. the analyses used to determine the causes of human performance problems;
4. the likely effectiveness of corrective action plans.

The first area to be checked is Problem Identification and Characterisation. For some problems human actions and decisions may not be important contributors to the problem. In others, human behaviour may have been central to creating the problem, and an understanding of the nature and causes of the behaviour was necessary to develop effective corrective actions. In the latter case, it is important that the human performance problem was characterised in sufficient detail to support problem resolution. The adequacy of human performance problems' identification and characterisation is verified, analysing answers to questions presented in the table.

The second area to be checked is related to methods and information used to investigate human performance. A thorough and systematic investigation is necessary to provide the information needed to perform causal analyses and develop effective corrective actions. The questions in the table may be used to guide the evaluation of an investigation of a human performance problem. In general, the extent of a human performance problem investigation depends upon the perceived significance of the problem.

The next area of the HPEP process is Causal Analyses. The review questions may be used in evaluating the causal analyses of human performance problems. The purpose of analysing the causes of human performance problems is to guide the development of effective corrective actions. Standard root cause analysis techniques, such as events and causal factors charting and analysis, change analysis and barrier analysis, are resource-intensive and time-consuming to apply, but yield reliable and useful results when performed properly.

The licensee's corrective actions for human performance problems are evaluated using the review questions presented in the last table. An effective corrective action for a human performance problem is one that will decrease the likelihood that it, and similar problems, will happen again. In an ideal world, an effective corrective action would prevent recurrence of the human performance problem. However, the causes of human behaviour are difficult to identify and, as a result, measures to improve human performance often yield inconsistent results. Developing effective corrective actions typically requires a thorough root cause analysis and an understanding of available methods for enhancing human performance. Depending upon the significance and scope of the cause(s) identified, corrective action plans may vary in scope from correcting a single cause, such as a missing tag on a valve, to a general organisational improvement plan. As a minimum, corrective actions must address each of the causal factors identified from the investigation.

The HPEP framework described in this section is illustrated in Figure 2.1.35. A hypothetical event sequence is shown across the bottom of the figure. Possible direct causes of the human error (barriers that failed or were missing) are shown above the event sequence. Possible programmatic causes that may have been responsible for the barrier failure are shown above the direct causes, demonstrating the loss of operational control that is evident from a human performance problem or significant event. In

this hypothetical event, a person who was not qualified to perform the task committed the error, and both the training and work control programmes were implicated as root causes.

Analysing answers are drawn to the questions in tables described above conclusions regarding the effectiveness of a problem identification and resolution programme for human performance. The HPEP, then, may be used when evaluating a problem identification and resolution programme to determine whether it (1) is effective in identifying the causes of human performance problems that play a causal or contributory role in significant events, and (2) results in corrective actions that target the causes of the problem(s) and result in effective problem resolution. On the basis of HPEP evaluation results human performance problems could be identified that should be evaluated for risk-significance.

Part II of the Human Performance Evaluation Process (HPEP) comprises the HPEP Cause Tree and Modules. The HPEP Cause Tree is a screening tool for identifying the range of possible causes for a human performance problem. The Cause Modules discuss typical causes of human performance problems in nuclear licensee facilities and provide examples of frequently identified direct and programmatic causes, based upon the research literature and industry experience. Each Cause Module is comprised of causal factors that have been found to affect human performance in the workplace as follows: Personnel (Fitness for Duty, Knowledge, Skills and Abilities, Attention and Motivation); Resources (Procedures and Reference Documentation, Tools and Equipment, Staffing, Supervision); Work Environment (Human-System Interface, Task Environment); Communication and Coordination (Communication, Coordination and Control).

The HPEP Cause Tree and Cause Modules may be used to verify the causes that were identified for human performance problems in order to complete the Causal Analyses process mentioned above. They also may be used as guidance in conducting an event investigation and to identify a human performance trend. Used as a checklist, the Cause Tree and Modules assist in overcoming the tendency to arrive at conclusions too early in an investigation, or to investigate only the possibilities that are initially suggested when an error is committed. Thus, the Cause Tree and Modules are intended to be used heuristically, but the possible causes that are investigated must be derived from the evidence.

Attributes: Similar to HPES. Simplified fault trees are easy to use. Minimal training is necessary if users are experienced in basic techniques.

A detailed description of the HPEP method is provided in the document NUREG/CR-6751 [4].

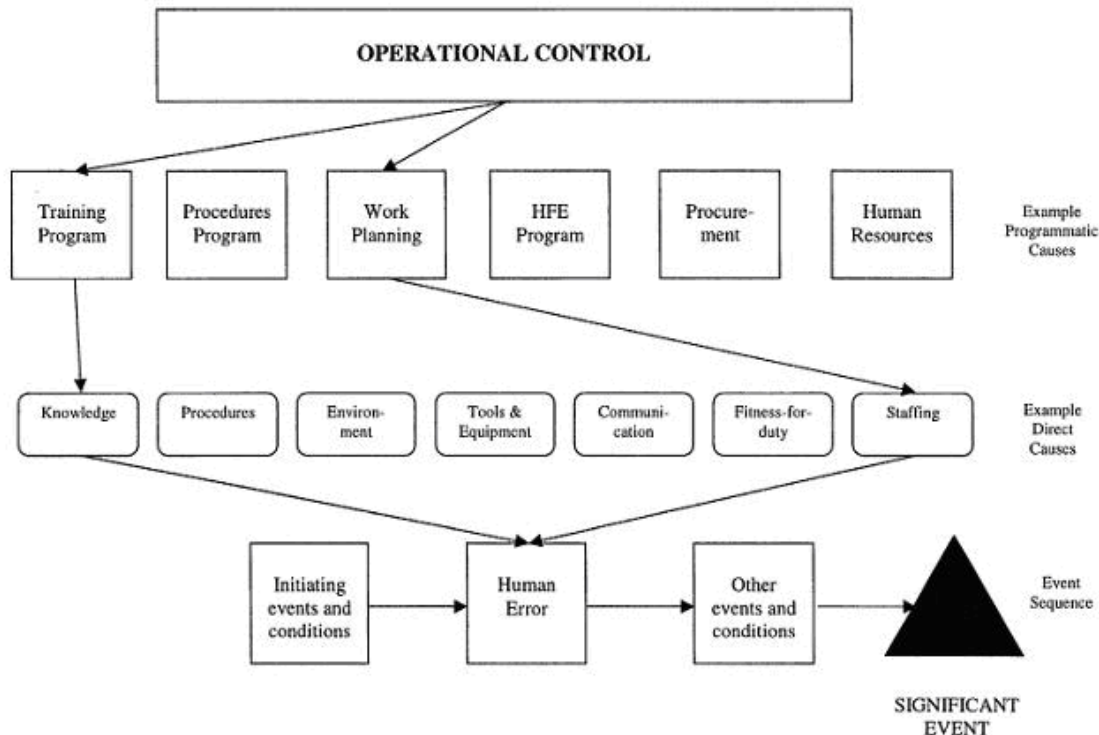


Figure 2.1.35. The HPEP framework [4]. HFE – human factors engineering

2.1.17. PROSPER - Peer Review of the effectiveness of the Operational Safety Performance Experience Review process

PROSPER is the next generation of the IAEA-led ASSET service, designed in 2000 to provide advice and assistance to utilities, or individual power plants, to strengthen and enhance the effectiveness of operational experience programmes in achieving fundamental safety objectives. The objectives and scope of the former ASSET methodology have been expanded and updated in PROSPER, with the aim of including an evaluation of the effective use of all operating performance information available to the plant (e.g. external operating experience, internal low-level and near miss event reports and other relevant operating performance information, such as performance indicators and Quality Assurance non-compliance reports). The typical input and output of PROSPER information is illustrated in Figure 2.1.36 [31].

According to the PROSPER method, evaluation of the effectiveness of the Operational Safety Performance Experience Review process should be performed in two stages. It is recommended that at the first stage utilities or NPPs conduct their own self-assessment of the effectiveness of their operational experience processes. At the second stage, the IAEA-led PROSPER team can then review the effectiveness and comprehensiveness of the plant self-assessment and offer comments and recommendations to further enhance the conclusions of the self-assessment. IAEA-led PROSPER missions compare, as far as possible, the operational experience processes for an NPP with guidance and equivalent good practices. These are based on guidance on safety practices produced by the IAEA and other international organisations, and the expertise of the PROSPER members themselves.

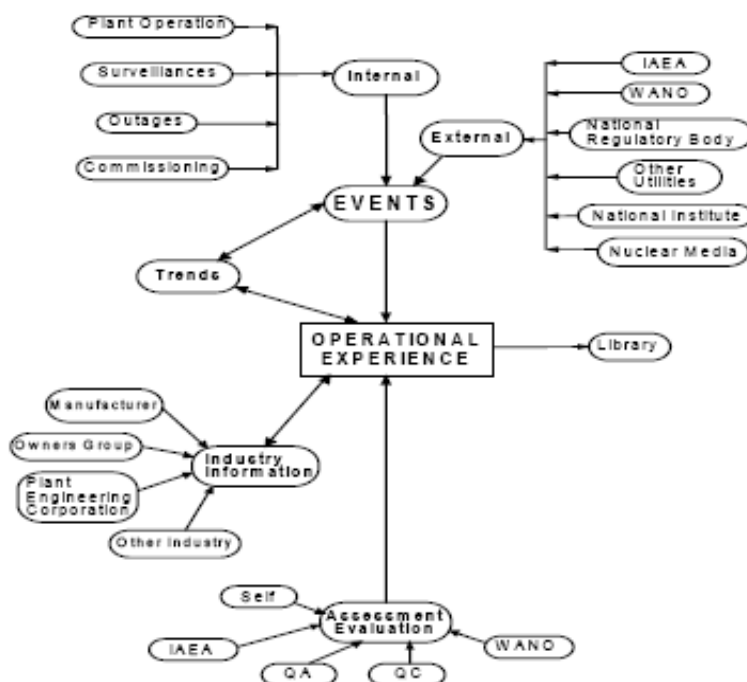


Figure 2.1.36. The typical input and output of PROSPER information

PROSPER missions perform a combination of two types of peer review (see Figure 2.1.37):

- a programmatic review of the overall effectiveness of the operational experience processes for the utility or NPP;
- a review focused on unresolved significant safety issues or individual events.

A PROSPER mission considers the effectiveness of the OE processes in enhancing operational safety performance. It is based on the review of the plant self-assessment report carried out in conjunction with

knowledgeable plant counterparts, together with observations made during plant walk-downs, discussions with plant staff in the field and consideration of relevant plant performance indicators.

Preparation for a PROSPER mission will be initiated only after the IAEA has been formally approached by a Member State and funding has been established. The scope of the mission is agreed between relevant organisations (e.g. a utility or NPP) and the IAEA at this stage.

The PROSPER methodology includes the following main elements:

- Preparation: establishing contacts with hosting organisation, team gathering, preparatory meeting, seminar or briefing, consideration of and agreement on the review type, scope and work plan;
- The review, using three methods to acquire the information needed to develop recommendations;
- Review of the self-assessment report, associated documents and written material;
- Interviews with personnel;
- Direct observation of the physical condition of the NPP and organisation, practices and activities associated with the operational experience process.

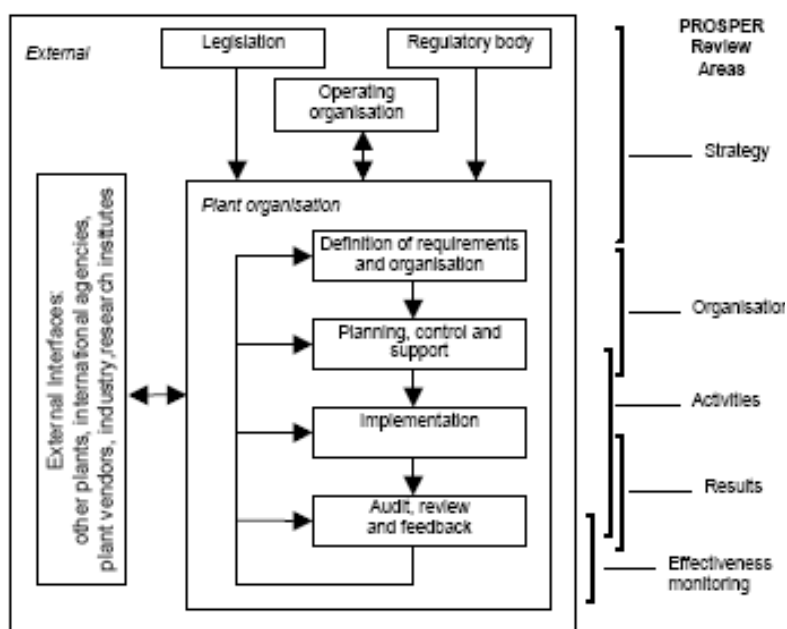


Figure 2.1.37. Management of the operational experience process to enhance safety and PROSPER review areas

Differences from IAEA Safety Standards and international practices which are identified are investigated, to document any concerns accurately in the PROSPER report, and in sufficient detail to be readily understandable. Recommendations and suggestions are formulated on the basis of weaknesses identified. Similarly, good practices encountered in the review are documented for the benefit of other utilities, and described in the report in sufficient detail to be readily understandable.

At the final stage of the review the PROSPER team report is prepared. It is the official team document that summarises the team's main findings and conclusions, from comparisons with the IAEA safety standards, proven international practices, including all recommendations, suggestions and good practices. Before the text is finalised the management of the NPP whose operational experience processes have been reviewed are given the opportunity to comment. The final report is submitted through official channels to the Member State and utility headquarters concerned. The IAEA restricts distribution to the utility concerned, the contributors to the report and responsible IAEA staff. Further distribution is at the discretion of the Member State or utility concerned.

2.2. PSA based event and precursor analysis methods

Probabilistic safety assessment (PSA) is a comprehensive, structured approach for identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk [37, 67, 74, 75, 76, 99, 122, 123, 125, 128, 133]. Methods based on this approach are designed for quantitative analysis of the risks in the operation of nuclear power plants and other installations. Safety functions for preventing or mitigating accidents, and the associated systems necessary to carry out the safety functions, are evaluated by the PSA analyses. PSA supports both the design of a nuclear power plant (NPP) and the safety management and control of a NPP right through its service life.

Three levels of probabilistic safety assessment are generally recognised. Level 1 comprises the assessment of plant failures leading to determination of the frequency of core damage. Level 2 includes the assessment of the containment response, leading, together with Level 1 results, to the determination of frequencies of failure of the containment and release to the environment of a given percentage of the reactor core's inventory of radionuclides. Level 3 includes the assessment of off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public risks.

PSA was first applied in the nuclear industry in 1975, when a study entitled WASH 1400 – Reactor Safety Study (also known as the Rasmussen Report) evaluated the probability of a number of accident sequences that might lead to fuel melting in the reactor (core damage) [125]. The application of the probabilistic safety analysis (PSA) in the risk follow-up of events started with pilot studies at the beginning of the 1990s. For example, a procedure for PSA based risk informed analysis of events at NPPs was developed by STUK (Finland) at that time [5]. The method was used to determine the safety significance of events and identify precursors. In PSA terms, precursors are infrequent initiating events and/or equipment failures that, when combined with one or more postulated events, would result in a plant condition leading to core damage. The analysis was based mainly on licensees' event reports. The calculated probability of core damage, given the failed equipment associated with the particular event, was termed a conditional core damage probability, and can be used as a measure of the safety significance of that event. The method was used mostly to evaluate events with failures in safety related systems or systems covered by Technical Specifications. Plant specific living PSA models were applied to the risk calculations of events. Conservative assumptions and model simplifications were often used in order to reduce the analysis burden. The conditional core damage probability was calculated based on the increased risk level due to the failure and the duration of the failure [2, 5, 26].

PSA-based approaches to event analysis, using plant-specific PSA models, became more attractive at the end of the 1990s. This was due to advances in computer hardware and software, and the growing availability of the plant-specific PSA models. This is now an increasingly common practice in many States and forms a routine part of operational feedback to complement the traditional deterministic analysis that is carried out to determine root causes, etc [123]. The purpose of event analysis is typically to determine the risk significance of possible events and the contributors to the risk, so that the events can be responded to according to their risk significance.

PSA based event analysis should be carried out for events at the plant (referred to as 'direct events') and events at other plants ('transposed events') with high potential safety significance. This necessitates the development of screening criteria that can be applied to screen out events with low safety significance and to rank events according to their significance. PSA based event analysis should include the analysis of initiating events (where an initiating event actually occurred and where failures occurred, but where an initiating event was prevented by prompt operator intervention) and of conditional events (where the likelihood of an initiating event was increased or the availability of the safety systems required to respond to initiating events was reduced).

PSA based event analysis should be carried out to complement deterministic analysis, by allowing multiple failure to be addressed, using an integrated model, and by providing a quantitative indication of the risk significance of operational events. It should also be used to provide an input into the

consideration of what changes could be made to reduce the likelihood of recurrence of such operating events.

Care should be taken in using the results of the PSA based event analysis for the identification of trends in the performance of a nuclear power plant or a set of nuclear power plants over a period of time. The results of such an application of PSA based event analysis could be misleading unless the analysis uses the same models, methods and assumptions throughout [123].

The fundamental purpose of PSA based analysis of operational events or of precursor analysis is to find answers to the following two basic questions [26, 123]:

- a) How could a precursor event have degenerated into an accident with more serious consequences?
- b) Is it possible to determine and measure what separates a precursor event from a potential accident with more serious consequences?

Thus, the analysis contains a qualitative and a quantitative element:

- Qualitative element of the precursor analysis. Finding the qualitative lessons to be learnt from the actual events considered as precursors for potentially more serious accidents. This gives an increased understanding of the vulnerabilities of the plant, given the event occurrence.
- Quantitative element of the precursor analysis - measuring the severity of the event. In this quantitative part of the analysis, the conditional probability that an operational event would progress to accidents with unacceptable consequences is calculated. Based on this information, events can be ranked according to their risk significance. Moreover it can be used to prioritise which weaknesses should be handled first, and to assess the level of safety of the plant.

Basically, in precursor analysis a re-analysis of the plant-specific PSA model is performed under the conditions in which the operational event occurred. Special attention is given to operating experience feedback information: by extrapolating precursor events to accident scenarios with serious consequences, valuable insights can be gained about serious incidents on the basis of minor events, without suffering their real consequences. The method thus makes it possible to learn from minor precursor events in the same way as we would learn from real accident experience.

Background and approach. Precursor events are operational events that may constitute important elements of accident sequences, potentially leading to unacceptable consequences. The most commonly used definitions of unacceptable consequences are core damage, beyond design conditions or unacceptable releases of radioactive material to the environment.

The PSA model used for precursor analysis should be sufficiently complete in scope to include the plant response to the operational event. It should be plant specific or at least plant type specific, to reflect the operational and design features of the plant with acceptable accuracy. It should include all relevant initiating events and all relevant operating conditions of the plant. For precursor analysis the PSA model sometimes has to be refined to a sufficient level of detail to reflect the precursor event analysis. This could involve modelling of missing accident sequences, missing component failure modes, or restoring accident sequences that were originally truncated or screened out. This could include changes in the fault tree model of the PSA or re-modelling or modelling of additional operator actions within the fault trees.

In precursor analysis a re-analysis of the PSA is performed under the conditions in which the operational event occurred. On this basis new conditional probabilities of accident sequences are calculated.

Analysis and quantification of conditional probabilities. As mentioned above, a re-analysis of the PSA needs to be performed under the conditions in which the operational event considered occurred. In performing this task, all the basic events in the PSA model should be checked to ascertain whether or not their reliability parameters are impacted by the operational event, and, if necessary, these parameters have to be re-assessed. Basic events representing failed components should be modelled as failed, for example with house events, i.e. these failed components should not be represented as a failure event with an associated failure probability in the modified PSA model.

For operational events involving component malfunctions or unavailabilities, but no initiating event, all initiating events have to be postulated, for which the degraded or failed components are demanded during accident sequences. The actual or estimated duration d of component unavailabilities (e.g. half

test interval) have to be taken into account. By multiplying this duration **d** with the frequency **f_i** of the initiating event **i** the conditional probability of the occurrence of the initiating event is calculated:

$$P_i = d f_i$$

and the conditional probability of the accident sequences is:

$$P \{ \text{accident precursor } j \} = \sum_i P_i \prod_i \{ \text{accident precursor } j \};$$

Where \prod_i - conditional probability of all accident sequences which have to be taken into account given the occurrence of the precursor event **j** and the initiating event **i**.

Results and interpretation. The main results of precursor investigations are the conditional probabilities. As a numerical threshold for judging the significance of operational events, based on a conservative estimate of the conditional core damage probability, a value of 10^{-6} is widely accepted and used. Multiplying the conditional probability of the precursor event **j** with the frequency, i.e. one event within the observation time in reactor years, and summing up all precursor events within the observation time yields:

$$\lambda = \frac{\sum_j P \{ \text{accident precursor } j \}}{\text{observation time}}$$

λ is an estimator for the unacceptable consequences, typically either core damage frequency or beyond design basis frequency. The estimator is called core damage index, beyond design basis index, or simply safety or risk index.

Figure 2.2.1 shows the task flow for PSA-based precursor analysis.

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

Several techniques can be used in performing a PSA. However, the usual approach is to use a combination of event trees and fault trees [123]. The relative size (complexity) of the event trees and fault trees is largely a matter of preference of the team carrying out the analysis, and also depends on the features of the software used. One widely practised approach is to use a combination of event trees and fault trees, often referred to as the fault tree linking approach. The event trees outline the broad characteristics of the accident sequences that start from the initiating event and, depending on the success or failure of the mitigating safety and safety related systems, lead to a successful outcome or to damage to the core, or to one of the plant damage states (required for the Level 2 PSA). The fault trees are used to model the failure of the safety systems and the support systems to carry out their safety functions. Another approach that is widely used is to carry out the analysis using large event trees and small fault trees. In this approach, failures of safety functions, safety systems and support systems are

modelled in the event trees. This approach is variously referred to as the large event tree approach, the linked event tree approach, or the event tree with boundary conditions approach. It is also possible to carry out the analysis using event trees only or fault trees only. However, in the latter case, the high level fault tree structure is usually derived from, or based on, an event tree or set of event trees.

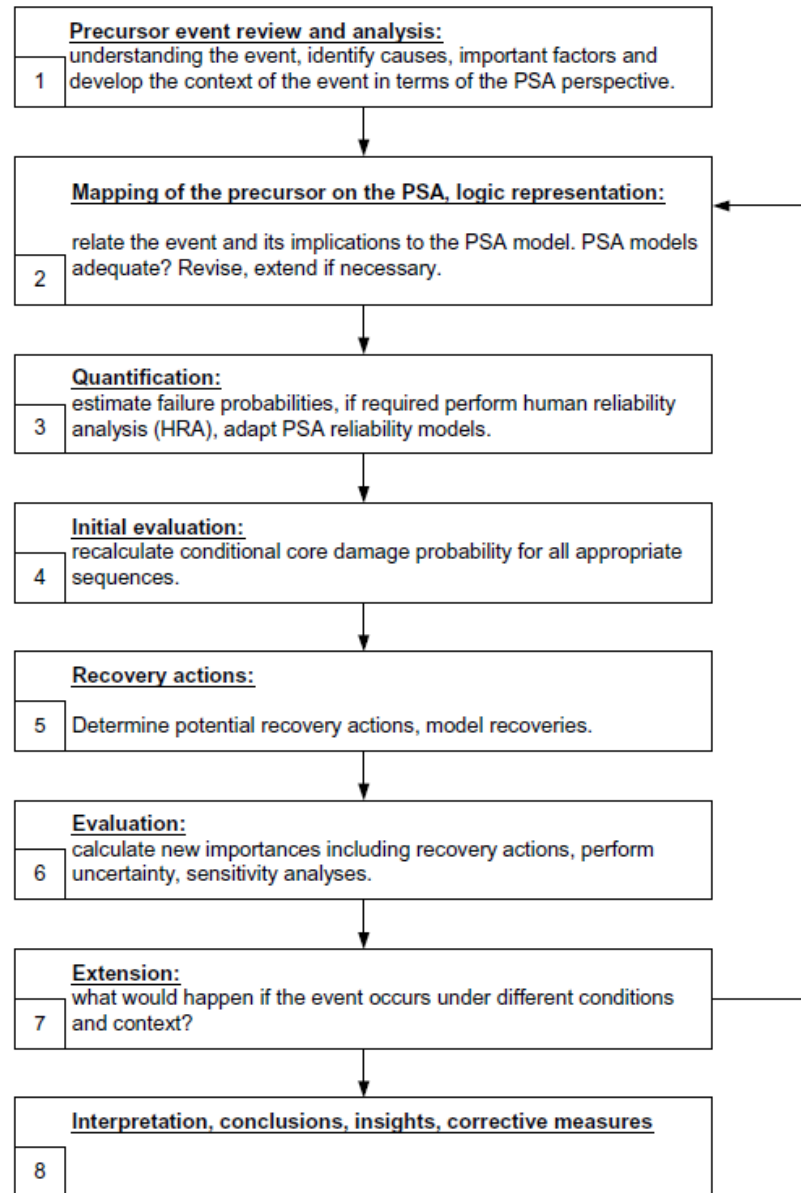


Figure 2.2.1. Procedural tasks in PSA-based precursor analysis [26, 41]

2.2.1. ATHEANA

One of the most recent versions of a second-generation human reliability analysis (HRA) is a method called ‘A Technique for Human Event Analysis,’ (ATHEANA) [43, NUREG-1624]. ATHEANA is the result of development efforts sponsored by the Probabilistic Risk Analysis Branch in the US Nuclear Regulatory Commission’s (NRC)’s Office of Nuclear Regulatory Research. ATHEANA was developed to address limitations identified in current HRA approaches by providing a structured search process for human failure events and unsafe acts, providing detailed search processes for an error-forcing context, addressing errors of commission and dependencies, more realistically representing the human-system interactions that have played important roles in accident response, and integrating advances in psychology with engineering, human factors, and PRA disciplines.

The ATHEANA method is an incremental extension of previous HRA methods, to provide the capability of analysing (both retrospectively and prospectively) kinds of human-performance problems. It is organised around a multidisciplinary framework that is directly applicable to the retrospective analysis of operational events and provides the foundation for a prospective analysis.

The fundamental concept of the multidisciplinary HRA framework is that many unsafe actions are the result of combinations of plant conditions and associated PSFs that trigger ‘error mechanisms’ in plant personnel. The framework provides a means for using the knowledge and understanding from the disciplines that are relevant to analysing risk-significant human performance in NPP accidents, including plant operations and engineering, PRAs, human factors, and the behavioural sciences. Existing HRA methods incorporate some but not all of these disciplines, which limits the kinds of insights any one method provides into human-performance issues. The HRA framework uses the relationships among these disciplines. In order to facilitate the use of these cross-disciplinary relationships, a limited amount of new terminology has been adopted to reduce some ambiguities due to the terms in one discipline being used differently in another discipline.

Figure 2.2.2 is the graphic description of the framework, which includes elements from plant operations and engineering PRA, human factors engineering, and behavioural sciences perspectives. All of these contribute to 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 following are the framework elements:

- error-forcing context (EFC)
- performance-shaping factors
- plant conditions
- human error
- error mechanisms
- unsafe actions (UAs)
- human failure events (HFEs)
- PRA model
- scenario definitions.

These combined elements create the minimum set necessary to describe the causes and contributions of human errors in major NPP events. Figure 2.2.2 illustrates the interrelationships of these elements.

The human performance-related elements of the framework (i.e. those based principally on the human factors, behavioural sciences, and plant engineering disciplines) are reflected by the boxes on the left side of the figure: namely, performance-shaping factors, plant conditions, and error mechanisms. These elements represent the information needed to describe the underlying influences on unsafe actions, and hence explain why a person may perform an unsafe action. The elements on the right side of the figure, namely, the HFEs and the scenario definition, represent the PRA model. The UA and HFE elements represent the point of integration between the HRA and PRA models. The PRA traditionally focuses on the consequences of the UA, 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 the model represents.

Error-Forcing Context. An EFC is the combined effect of PSFs and plant conditions that create a situation in which human error is likely. Analyses of NPP operating events reveal that the EFC typically involves an unanalysed plant condition that is beyond normal operator training and procedure-related PSFs. The unanalysed plant condition can activate a human error mechanism related to, for example, inappropriate situation assessment (i.e. a misunderstood regime). Consequently, when these plant conditions and associated PSFs trigger internal psychological factors (i.e. error mechanisms), they can lead to the refusal to believe evidence that runs counter to the initial misdiagnosis, or the failure to recognise that evidence, resulting in subsequent mistakes (e.g. errors of commission) and ultimately a catastrophic accident. PSFs represent the human-centred influences on human performance. Many of the PSFs used in this project are those identified in the human performance investigation process (HPIP)

(NUREG/CR-5455, [19]): procedures, training, communication, supervision, staffing, human-system interface, organisational factors, stress, and environmental conditions.

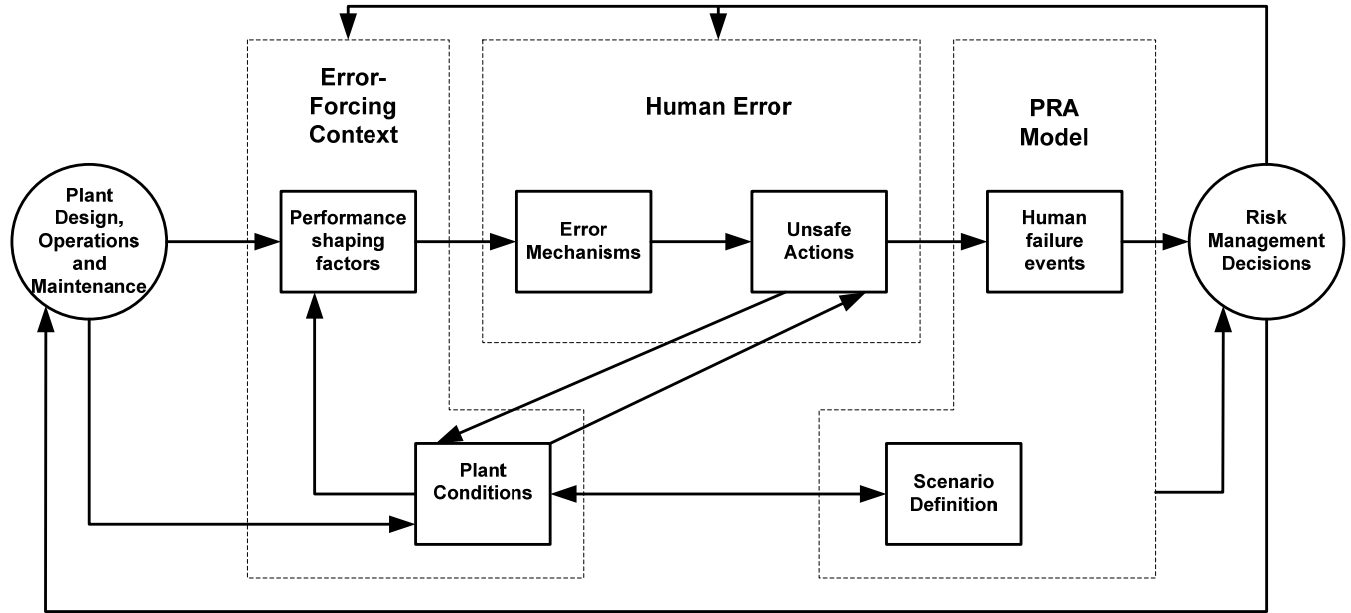


Figure 2.2.2. Multidisciplinary HRA Framework

An example of a PSF is a procedure whose content is incorrect (e.g. wrong sequence of steps), incomplete (e.g. situation not covered), or misleading (e.g. ambiguous directions) and that contributes to a failure in situation assessment or response planning.

Plant conditions include plant configuration; systems component and instrumentation and control availability and reliability; process parameters (e.g. core reactivity, power level, and reactor coolant system temperature, pressure and inventory); and other factors (e.g. non-nominal or dynamic conditions) that result in unusual plant configurations and behaviour. The following are some non-nominal plant conditions:

- history of false alarms and indications associated with a component or system involved in the response to an accident;
- shutdown operations with instrumentation and alarms out of normal operating range and many automatic controls and safety functions disabled;
- unusual or incorrect valve line-ups or other unusual configurations.

A ‘human error’ can be characterised as a divergence between an action performed and an action that should have been performed, which has an effect or consequence that is outside specific (safety) tolerances required by the particular system with which the human is interacting.

In the PRA community, the term ‘human error’ has usually been used to refer to human-caused failures of a system or function. The focus is on the consequence of the error. In the behavioural sciences, the focus is on the underlying causes of the error. For the purpose of developing ATHEANA, and to fully integrate it with the requirements of the PRA, the framework representation of human error encompasses both the underlying mechanisms of human error and the consequences of the error mechanism, which is the observable unsafe action (UA).

Error mechanisms are used to describe the psychological mechanisms contributing to human errors that can be ‘triggered’ by particular plant conditions and PSFs that lie within the PRA definitions of accident scenarios. Often these error mechanisms are not inherently ‘bad’ behaviours, but are mechanisms that generally allow humans to perform skilled and speedy operations. However, when applied in the wrong context, they can lead to inappropriate actions with unsafe consequences. Different error mechanisms are influenced by different combinations of PSFs and plant conditions. Therefore, by considering

specific error mechanisms, the analysis can be made more efficient because it can focus on specific PSFs and plant conditions relevant at the time.

Unsafe actions are those actions inappropriately taken by plant personnel, or not taken when needed, that result in a degraded plant safety condition. The term ‘unsafe action’ does not imply that the human was the cause of the problem. Consequently, this distinction avoids any inference of blame and accommodates the assessment on the basis of the analysis of operational events that people are often ‘set up’ by circumstances and conditions to take actions that were unsafe. In those circumstances, the person did not knowingly commit an error; they were performing the ‘correct’ action as it seemed to them at the time.

While not all UAs identified in the analysis of operational events correspond to HFEs as defined in PRAs, in some cases there is a direct correspondence. For example, operators terminating the operation of necessary engineered safety features would be performing a UA, and this action should be incorporated as an HFE in PRAs.

The *PRA model* identified in the ATHEANA framework is no different from those used in existing PRA methodologies. However, in ATHEANA prospective analyses, the PRA model is an ‘end user’ of the HRA process. The PRA model is a means of assessing the risk associated with the NPP operation. It has as its basis logic models which consist of event trees and fault trees constructed to identify the scenarios that lead to unacceptable plant accident conditions, such as core damage. The PRA model is used to estimate the frequencies of the scenarios by converting the logic model into a probability model. To achieve this aim, estimates must be obtained for the probabilities of each event in the model, including human failure events. When human-performance issues are analysed to support the PRA, it is in the context of HFEs applicable to a specific accident scenario defined by the plant state and represented by a PRA logic model.

ATHEANA consists of a retrospective process and a prospective process (including an HRA method).

The ATHEANA retrospective analysis process was devised initially to support the development of the prospective (or HRA) ATHEANA analysis process. 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. The ATHEANA approach was also used for retrospective analysis to train third-party users of ATHEANA in an earlier demonstration of the method. In this training, not only reviewing example event analyses, but actual experience in performing such analyses, helped new users develop the perspective required to apply the prospective ATHEANA process. Finally, event analyses using the ATHEANA approach are useful in themselves. Amongst other things, they can be used to help understand why specific events occurred and what could be done to prevent them from occurring again.

The key steps in performing a retrospective analysis are:

- identify the framework of safety and the key failures that occurred to challenge the safety barriers (including ‘near misses’ that may have reduced the margins of safety);
- identify the specific actions taken by people that caused the key failures and the contexts that led to the actions being taken.

The retrospective approach can be applied broadly, using the ATHEANA HRA framework mentioned above. Both nuclear and non-nuclear events can be easily analysed using this framework and its underlying concepts. A more detailed approach has been developed for nuclear power plant events, although it can be generalised for other technologies. This more detailed approach is more closely tied to the ATHEANA prospective analysis than general use of the framework.

The ATHEANA prospective process (or HRA) consists of several major steps (following preparatory tasks, such as assembling and training the analysis team). The basic steps in the prospective analysis are:

- integration of the issues of concern into the ATHEANA HRA/PRA methodology;

- performance and control of the structured processes for identifying human failure events and unsafe acts and determination of the reasons why such events occur (i.e. the elements of an error-forcing context - EFC-plant conditions and performance shaping factors);
- identification of how potential conditions can arise that may set up the operators to take inappropriate actions or fail to take necessary actions;
- quantification of the EFCs and the probability of each unsafe action, given its context;
- evaluation of the results of the analysis in terms of the issue for which the analysis was performed.

As noted earlier, ATHEANA's search for EFCs and its associated quantification approach (which some may term the 'HRA method') are especially unique. The ATHEANA search for EFCs has been structured to seek, among other things, plant conditions that could mislead operators so that they develop an incorrect situation assessment or response plan, and take an unsafe action. ATHEANA assumes that significant unsafe actions occur as a result of the combination of influences associated with such plant conditions, and specific human-centred factors that trigger error mechanisms in the plant personnel. In ATHEANA, EFCs are identified using four related search schemes:

- (1) A search with characteristics similar to a hazards and operability analysis ('HAZOP') for physical deviations from the expected plant response. This search also involves the identification of potential operator tendencies, given the physical deviation and the identification of error types and mechanisms that could become operative given the characteristics of the physical deviation. This search for human-centred factors is also conducted as integral parts of searches 2 and 3 described below.
- (2) A search of formal procedures that apply normally or that might apply under the deviation scenario identified in the first search.
- (3) A search for support system dependencies and dependent effects of pre-initiating event human actions.
- (4) A 'reverse' search for operator tendencies and error types. The first three searches identify plant conditions and rules that involve deviations from some base case. In this search, a catalogue of error types and operator tendencies is examined to identify those that could cause human failure events or unsafe actions of interest. Then plant conditions and rules associated with such inappropriate responses are identified. Consequently, this search serves as a catchall to see if any reasonable cases were missed in the earlier searches.

In order to address the elements of EFC (which go beyond the types and scope of context addressed in previous HRA methods), ATHEANA requires a new quantification model. In particular, quantification of the probabilities of corresponding HFEs is based upon estimates of how likely it is that the plant conditions and PSFs comprising the EFCs will occur, or how frequently they may do so, rather than upon assumptions of randomly occurring human failures. This approach blends systems analysis techniques with judgment by operators and experienced analysts to quantify the probability of a specific class of error-forcing context, and the probability of the unsafe act, given that context.

In the end, the overall approach must be an iterative one (i.e. define an error-forcing context and unsafe act, attempt quantification considering recovery, refine the context, etc.).

2.2.2. RASP

The Risk Assessment of Operational Events Handbook (sometimes known as the 'RASP Handbook') [74] is probably the most comprehensive source documenting methods and guidance that regulatory staff, plant analysts and other risk assessment specialists could use when performing risk assessments of operational events, developing and updating Standardised Plant Analysis Risk (SPAR) models and evaluating licensee performance issues. This handbook describes best practices, based on feedback and experience from the analyses of over 600 precursors of events dating back to 1969, and numerous Significance Determination Process (SDP) analyses (since 2000) performed in the US nuclear industry. The methods and processes described in the handbook [74] can be applied primarily to plant risk assessments and event assessments. The guidance is based on the use of SPAR models and Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software package and

can be applied in the risk analyses for other regulatory applications, such as special risk studies of operational experience.

Generic methods and processes to estimate the risk significance of initiating events (e.g. reactor trips, losses of offsite power) and degraded conditions (e.g. a failed high pressure injection pump, failed emergency power system) that have occurred at nuclear power plants are described in this document [74]. Specifically, guidance on the following analysis methods is provided:

- Exposure Time Determination and Modelling;
- Failure Determination and Modelling;
- Mission Time Modelling;
- Test and Maintenance Outage Modelling;
- Modelling Recovery and Repair Actions in Event Assessment;
- Multi-Unit Considerations Modelling.

In addition, further guidance is provided on the following analysis topics:

- Road Map – Risk Analysis of Operational Events;
- Quick Reference Guide – SAPHIRE Version.

Although the guidance in this volume of the handbook focuses on the analysis of internal events during at-power operations, the basic processes for the risk analysis of initiating events and degraded conditions can be applied to external events, as well as events occurring during low-power and shutdown operations.

The overall event analysis process involves the modification of a SPAR model to reflect attributes of an event, solution of the modified model to estimate the risk significance of the event, and documentation of the analysis and its results. The process is structured to ensure that the analysis is comprehensive and traceable. A detailed review by the analyst and a subsequent independent review(s) minimise the likelihood of errors, and enhance the quality of the risk analysis.

As a minimum, a risk analysis consists of the following (see Figure 2.2.3):

- Development of a risk-focused understanding of the event that occurred, relevant plant design, and operational features, as well as the status of the plant;
- Comparison of the event with the existing risk model to identify any changes that are necessary to support the analysis;
- Risk model elaboration, if necessary, to allow the risk-related features of the observed event to be properly represented in the model;
- Model modification to reflect event specifics;
- Initial model solution to estimate the risk significance of the event without consideration of crew activities to recover risk-significant failures;
- Recovery analysis to address potential crew actions to recover any failed components associated with risk-significant sequences;
- Analyst review of the results to ensure that the logic model and incident mapping process are correct. The focus of this review is to identify inconsistencies, errors, and incompleteness in the SPAR model. Then the SPAR model is modified and resolved;
- Final documentation of the inputs (facts), assumptions, results, and uncertainties;
- Independent review(s) of the completed analysis.

In addition, a supplemental effort that can improve analysis accuracy and confidence in the results should be performed for higher risk-significance or controversial events - sensitivity and uncertainty analyses to gain additional understanding of the impact of analysis assumptions and data variability on analysis results.

The event analysis process is iterative. Review of the model for applicability may highlight the need for additional detail related to the event. Review of the initial analysis results (significant sequences and cut sets) frequently identifies the need for additional detail concerning the event, plant design, operational information, or the need for greater model fidelity.

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

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

2.2.3. Attributes of PSA and correlation with other event investigation methods

PSA can provide useful insights and inputs for various interested parties, such as plant staff (management and engineering, operations and maintenance personnel), regulatory bodies, designers and vendors, for making decisions on a) design modifications and plant modifications; b) optimisation of plant operation and maintenance; c) safety analysis and research programs; d) regulatory issues.

The PSA should address the actual or, in the case of a plant under construction or when modifications are being undertaken, the intended design or operation of the plant, which should be clearly identified as the basis for the analysis. The status of the plant can be fixed as it was on a specific date, or as it will be when agreed modifications are completed. This needs to be done to provide a clear target for completion of the PSA. Later changes can be addressed in the framework of a living PSA program [123].

PSA-based event analysis provides a complement to the Root Cause Analysis approach by focusing on how an event might have developed adversely. Figure 2.2.4 shows the conceptual relation between root cause analysis and PSA-based event analysis. It depicts a flow chart for the overall event investigation process, which includes both the PSA based view and analysis, and the traditional deterministic practice used at many nuclear power plants (NPPs) for processing operating experience (OE) information arising from on- and off-site. It shows the basic elements of the process:

- screening and selection of events;
- in-depth analysis;
- implementation of actions.

Root cause analysis focuses on the real occurrences during the event and their causes. PSA-based event analysis uses this information as a starting point and looks at the potential occurrences during the event, leading to an estimate of the likelihood of the potential consequences of the event. The information developed by root cause analysts regarding causes is useful for the PSA-based event analysis since the failure causes affect the likelihood of the potential accident sequences [26].

The traditional event investigation process can be greatly enhanced by the introduction of supplementary information from PSA based analysis. According to Figure 2.2.5, in parallel with traditional qualitative event investigation performed by the operational experience group of the NPP, an additional PSA route is established. The precursor event analysis case is forwarded to the PSA group from the operational experience group after or during their in depth analysis of the operating event. All the information available or elaborated regarding the operational event and its implications should be provided to the group carrying out the PSA based evaluation.

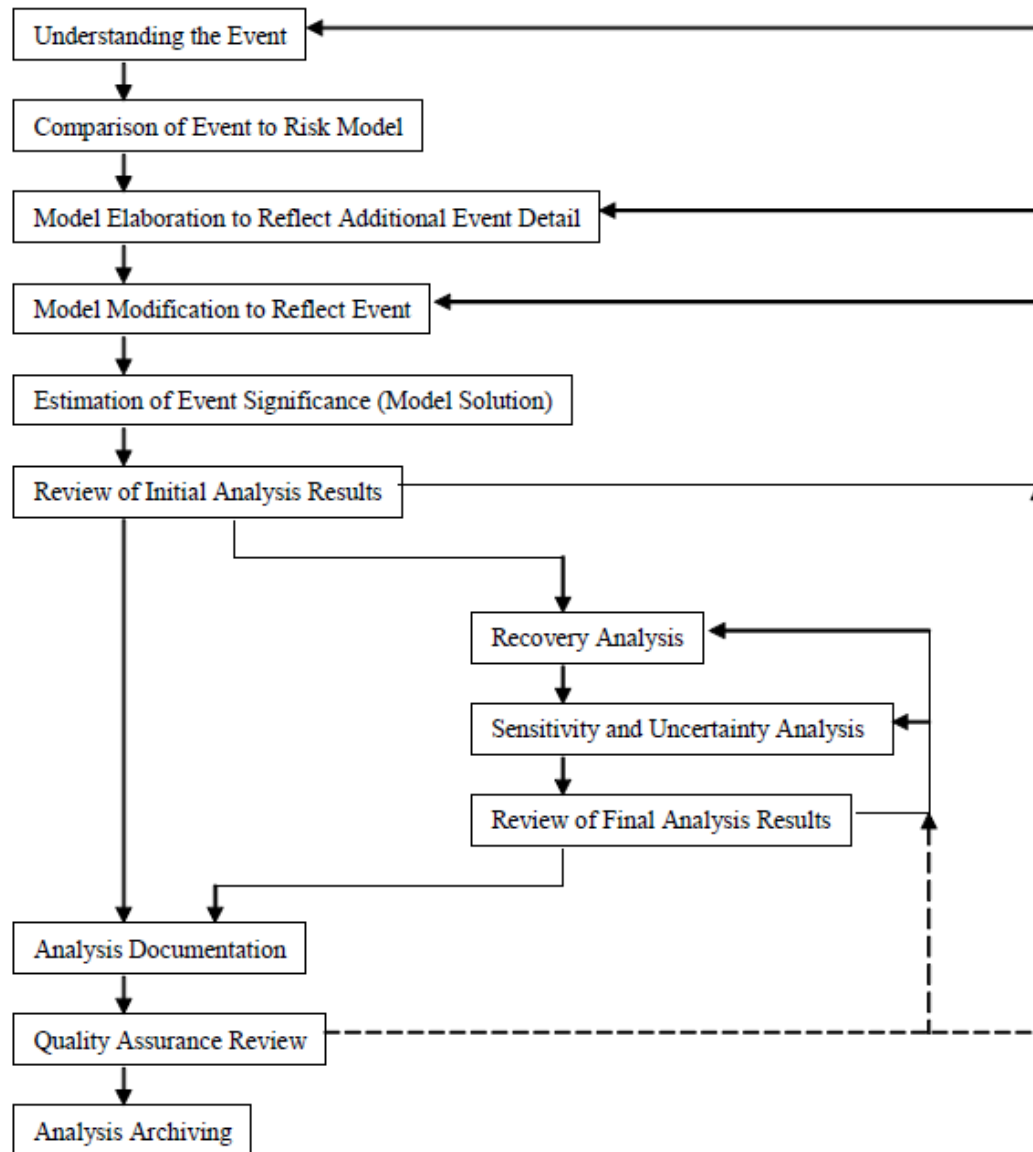


Figure 2.2.3. Risk Analysis of Operational Events – process flow with the main steps indicated

There are two main steps for detailed precursor analysis, as shown in the main flow diagram (see Figure 2.2.5):

- 1) Relating the operational event to the plant specific, or at least a plant type specific, PSA model, and finding out whether or not the event can be adequately analysed by PSA based models. Depending on the type of operational event, there are events which do not fall into the PSA perspective or cannot be treated in a useful way by this approach. If this is the case, it should be noted, with a short justification, an information notice sent to the operating experience group, and the process should be stopped. Otherwise, detailed analysis is carried out in the second step.
- 2) Precursor analysis, mapping of the precursor on the PSA model, qualitative and quantitative evaluation, interpretation of results and derivation of insights.

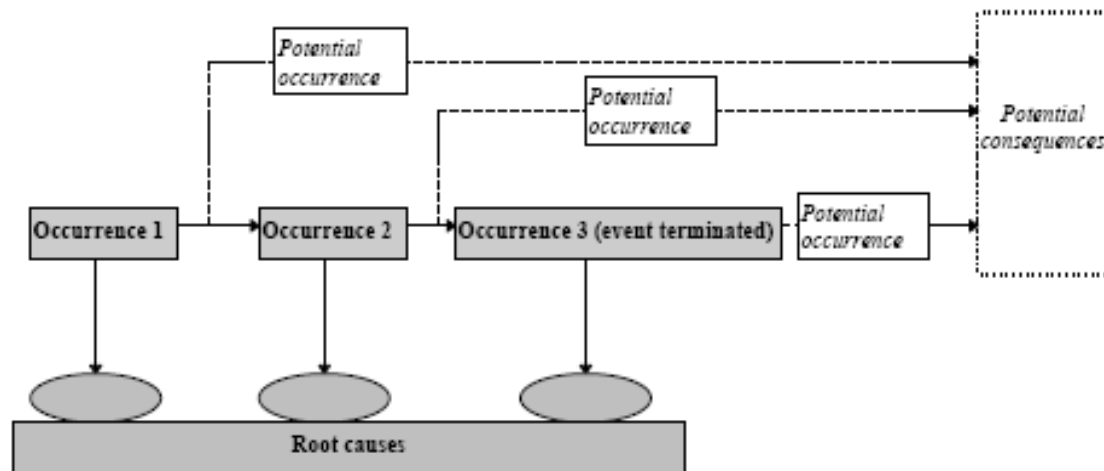


Figure 2.2.4. The relation between root-cause analysis and PSA-based event analysis

The PSA is an excellent technology, with many advantages for both the regulatory side and licensees, which can be effectively used in a wide range of areas, from design to maintenance management of nuclear power plants [126]. A major advantage of PSA is that it provides an explicit framework for the analysis of uncertainties in risk estimates. The identification of sources of uncertainty and an understanding of their implications on the PSA model and its results should be considered an inherent part of any PSA, so that, when the results of the PSA are used to support a decision, the impact of the uncertainties can be taken into account [123].

Moreover, PSA has been found useful [129] because it:

1. Considers thousands of scenarios that involve multiple failures, thus providing an in-depth understanding of system failure modes. Such an enormous number of possible accident scenarios are not investigated by traditional methods. The completeness of the analysis is significantly enhanced by PSA investigation.
2. Increases the probability that complex interactions between events/systems/operators will be identified.
3. Provides a common understanding of the problem, thus facilitating communication among various stakeholder groups.
4. Is an integrated approach, thus identifying the need for contributions from diverse disciplines such as the engineering, social and behavioural sciences.
5. Focuses on uncertainty quantification and creates a better picture of what the community of experts knows, or does not know, about a particular issue, thus providing valuable input to decisions regarding the research needed in diverse disciplines, e.g. physical phenomena and human errors.
6. Facilitates risk management by identifying the dominant accident scenarios so that resources are not wasted on items that are insignificant contributors to risk.

There are some other important strengths of the PSA [128]:

- integrative and quantitative approach allows ranking of issues and results;
- explicit consideration and treatment of all types of uncertainties, application of an optimisation process;
- cost-effectiveness: using PSA methods, it is possible to ensure that resources are focused on essential safety issues;
- probabilistic methods can be used both to enhance safety and to manage operability;
- results and decisions can be communicated on a clearly defined basis;
- due to the clearly structured approach to be followed, its use is beneficial even if the models generated are not quantified;

- even if the amount of available adequate probabilistic data is relatively small, the absolute accuracy of the result is not an issue if probabilistic approaches are used as comparative tools, allowing one to make decisions between different design or operation alternatives.

Like all event investigation methodologies, the probabilistic approach also has some limitations. These are due to the fact that the results of a PSA invariably contain uncertainties arising from three main sources [123]:

- Uncertainties due to a lack of comprehensive data regarding the area under consideration. It is impossible to demonstrate the exhaustiveness of a PSA, even when the scope of the analysis has been extended to as large a number of situations as possible -- notably in terms of various reactor operating states and potential initiating events.
- Uncertainties regarding data. Such uncertainties concern the reliability data for plant components, the frequency of initiating events, common-mode failures and failures resulting from human actions. The main uncertainties are those relating to the frequency of rare initiating events (for example, the combination of a steam piping break and a steam-generator tube break), as well as data relating to human factors.
- Uncertainties associated with modelling assumptions that cannot easily be quantified, such as the resistance of certain components under accident conditions, poorly understood physical phenomena or human actions.

In view of these uncertainties, the assumptions on which PSAs are based are designed to ensure sufficient safety margins. It is worth noting that the uncertainties are not intrinsic to PSAs, but may generally be attributed to lack of detailed knowledge. Indeed, one of the benefits of conducting PSAs is that they can identify areas about which we need to learn more.

Besides the above mentioned uncertainties, there are several more items that are not handled well, or not addressed at all by current PSA methodology [129]:

1. Human errors during accident conditions, including both errors of omission and errors of commission especially.
2. Digital software failures, which are the object of research aiming not to quantify the failure probabilities but, rather, to understand the kinds of failure modes that may be introduced.
3. Safety culture. When asked, managers of hazardous facilities say that they put safety first. Unfortunately, experience shows that it is not always the case. While it is relatively easy to ascribe an accident that has occurred to a bad safety culture, the fact is that defining indicators of a good or bad safety culture in a predictive way remains elusive: PSA certainly does not include the influence of culture on personnel behaviour.
4. Design and manufacturing errors, which are especially important for equipment that could be required to operate under unusual conditions, such as accident environments.

Despite substantial progress made with probabilistic risk analysis methods, some other problems encountered can also be mentioned [129]:

- Engineers and scientists often feel uncomfortable with methods that require considerable use of mixtures of 'subjective' (expert judgment) and 'objective' data (observations) and thus often have an overall feeling that the whole exercise lacks scientific rigour.
- Analysis and decision-making processes are more complex and time-consuming because more information and insights have to be collected, processed and considered for decisions. The relatively long duration of probabilistic studies (preparation, performing, interpreting) might be a fertile ground for endless debate between utility and regulator.
- Due to the more complex structure, the assumptions, methods and results are more difficult to understand, and require some mathematical knowledge. The fact that the results are characterised as prognostic estimations of what may, or may not, happen in the future makes understanding difficult and poses a still unresolved issue in many legal environments. A regulator's personnel has thus to be very well-informed scientifically and technologically in order to achieve consistent application of standards.

- An unduly high level of fascination with the approach as such and its tools, nowadays especially due to the ease of application by means of user friendly computer software tools. Often risk assessment becomes bogged down in the mechanics of performing risk analysis. While analysing risks is necessary, knowing what they are is far more important.
- It must not be thought that the numerical results from a PSA are ‘accurate’ in the same sense that a financial audit or a deterministic engineering analysis seems to be accurate. Really both probabilistic and deterministic models are full of uncertainties, and most risk analysts will not claim more than an ‘order-of-magnitude’ accuracy.

Despite these uncertainties, the probabilistic assessment of both the strengths and weaknesses of safety features can clearly suggest ways of improving both the design and operation of nuclear facilities. Probabilistic safety analysis has thus become an important supplement to deterministic analysis in checking the safety level of a facility, and improving it by identifying design weaknesses. In addition to assessing the safety of a plant at a given point in its lifetime, such applications have also demonstrated the usefulness of PSAs in other areas, and a certain number of programmes are already being developed which hint at future applications.

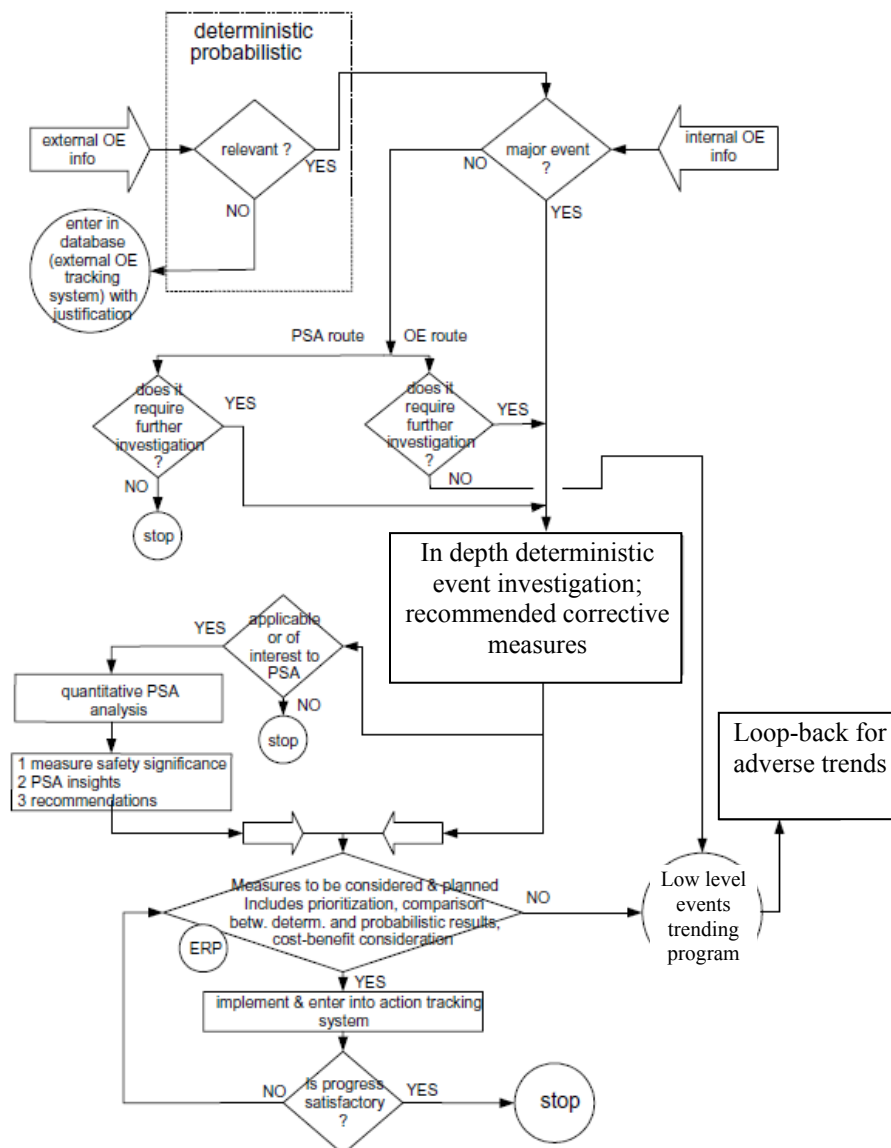


Figure 2.2.5. Process flow chart for operational event analysis [26]

2.3. Deterministic safety analyses

A major part of the process of designing and licensing a nuclear power plant is the safety analysis. IAEA Safety Standard [79] states that both deterministic methods and probabilistic methods are required to be applied. The objectives are to identify issues that are important to safety and to demonstrate that the plant is capable of meeting any authorised limits on the release of radioactive material and on the potential exposure to radiation for each plant state.

The deterministic evaluation of safety is typically bottom-up, i.e. it starts with postulated failures and proceeds to identify their consequences. If an event, such as failure of component, is judged to lead to unacceptable consequences, measures are taken either to make it less likely (without knowing quantitatively by how much) or to mitigate its potential consequences. Typically, these actions include introduction of redundant elements and additional safety margins, i.e. the difference between the failure point and the anticipated operating point is made larger. These actions are based on engineering judgment informed by analyses, tests, and operating experience. The result is frequently a complex set of requirements for the design and operation of the system. A facility that meets these requirements is judged 'acceptable' in the sense that there is no 'undue risk' to the public or the workforce. What 'undue risk' is remains unquantified. The presumption is that meeting the requirements guarantees adequate protection of public and personnel health and safety, i.e. the (unquantified) risk is acceptably low [129].

Deterministic safety analyses are analytical evaluations of physical phenomena occurring at nuclear power plants, made for the purpose of demonstrating that safety requirements, such as the requirement for ensuring the integrity of barriers against the release of radioactive material and various other acceptance criteria, are met for all postulated initiating events that could occur over a broad range of operational states, including different levels of availability of the safety systems [76].

The objective of deterministic safety analyses is to demonstrate that, in normal operational conditions and accident conditions, a sufficient number of barriers are retained.

Deterministic safety analyses for a nuclear power plant predict the response to postulated initiating events. A specific set of rules and acceptance criteria is applied. Typically, these should focus on neutronic, thermohydraulic, radiological, thermomechanical and structural aspects, which are often analysed with different computational tools. The computations are usually carried out for predetermined operating modes and operational states, and the events include anticipated transients, postulated accidents, selected beyond design basis accidents and severe accidents with core degradation. The results of computations are spatial and time dependencies of various physical variables (e.g. neutron flux; thermal power of the reactor; pressure, temperature, flow rate and velocity of the primary coolant; stresses in structural materials; physical and chemical compositions; concentrations of radionuclides) or, in the case of an assessment of radiological consequences, radiation doses to workers or the public.

Deterministic safety analyses should be carried out for the following areas:

- (a) Design of nuclear power plants. Such analyses require either a conservative approach or a best estimate analysis together with an evaluation of uncertainties.
- (b) Production of new or revised safety analysis reports for licensing purposes, including obtaining the approval of the regulatory body for modifications to a plant and to plant operation. For such applications, both conservative approaches and best estimate plus uncertainty methods may be used.
- (c) Assessment by the regulatory body of safety analysis reports. For such applications, both conservative approaches and best estimate plus uncertainty methods may be used.
- (d) Analysis of incidents that have occurred or of combinations of such incidents with other hypothetical faults. Such analyses would normally require best estimate methods, in particular for complex occurrences that require a realistic simulation.
- (e) Development and maintenance of emergency operating procedures and accident management procedures. Best estimate codes together with realistic assumptions should be used in these cases.

- (f) Refinement of previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid.

The demand for deterministic analyses of operational events is supported by the need to avoid recurrence of events by better understanding of the phenomena involved, and to validate the adequacy of corrective measures [126, 127]. For some operational events it is difficult to identify the particular reason for the event occurrence, or there are multiple possible reasons from which the major one needs to be identified. For such events, detailed deterministic analysis could be beneficial, as it can obtain the necessary insights and can help to find appropriate corrective measures. Typical operational events, which need deterministic analysis, are:

- Malfunction of valves, pumps or other components, resulting in complex response of the unit. To analyse these events, the same codes and similar models are used as for safety analysis reports. These events are typically used for code validation, but there is still a need to analyse such operational events for deeper understanding of plant behaviour and in order to prove the high quality of analytical predictions.
- Inadequate response of a control or safety system. Some reported events result in inadequate or unexpected response of a control or safety system. To explain such events detailed modelling of the relevant system is necessary. The typical integral plant model used for a safety analysis report does not credit control systems.
- Pipeline leakage, rupture or thermal fatigue. Events initiated by damage of pipelines can be caused by thermo-hydraulic phenomena - e.g. coolant stratification or frequent changes of coolant temperature or pressure, leading to increased thermal stresses and fatigue. Simulation of these events may require specific modelling of local phenomena. Significant uncertainties of initial and boundary conditions exist due to limitations of plant monitoring systems.
- Reactivity events. These events (e.g. control rod or cluster drop) should be analysed for assessment of effects and for proof of the similarity between design and measured changes in power profile.
- Other events. The list of other operational events, which should be analysed, depends on reactor type and the country specific practices.

In practice deterministic analysis is carried out only in a few cases, basically for two main purposes:

- to reveal the nature of the processes and phenomena which led to the failure by attempting to reconstruct the details of the process;
- to benchmark and validate an existing computer model by taking advantage of a well recorded and understood event.

The deterministic analysis of operational events involves four main steps:

- establish the sequence of events;
- evaluate the event as it happened;
- evaluate the event as it could happen ('what if' analysis);
- record the results of the event analysis in historical databases.

There are three ways of carrying out deterministic safety analyses of anticipated operational occurrences and design basis accidents to demonstrate that the safety requirements, which are currently used to support applications for licensing, are met:

- (1) Use of conservative computer codes with conservative initial and boundary conditions (conservative analysis).
- (2) Use of best estimate computer codes combined with conservative initial and boundary conditions (combined analysis).
- (3) Use of best estimate computer codes with conservative and/or realistic input data but coupled with an evaluation of the uncertainties in the calculation results, with account taken of both the uncertainties in the input data and the uncertainties associated with the models in the best estimate computer code (best estimate analysis). The result, which reflects conservative choice but has a quantified level of uncertainty, is used in the safety evaluation.

The deterministic analysis is performed using verified and validated operational plant models based on RELAP5, ATHLET, CATHARE, APROS, QUABBOX-CUBBOX, PARCS etc. codes.

Attributes of deterministic safety analysis and correlation with other event investigation methodologies

Some of the main strengths of deterministic risk analysis are [128]:

- Analysis and the subsequent decision-making process are relatively clear and simple. The systems analysis and the associated calculations are straightforward and the decision-making answer is 'safe' or 'not safe'.
- It can be carried out with comparatively little effort and is suitable for use by engineering-type personnel with a detailed knowledge of the plant design and operation, but not necessarily with expertise in risk analysis.
- Typical deterministic risk analysis schemes are often sufficient for a crude indication of internal safety management; however, they are not suitable for application for risk communication with regard to off-site consequences.

Progress in analytical tools, both software and hardware, allows for the performance of more detailed deterministic analysis of operational events, bringing several benefits:

- better understanding of the phenomena occurring during a specific event, and helping to identify the direct and contributing causes;
- identification of the impact of different contributing factors and conditions (operator and/or automated actions);
- evaluation of the plant safety margins during the event;
- operational safety enhancement; improvements in operator training and operating procedures;
- increase of the confidence in the code and code input models;
- sharing experience and utilising external experience;
- supporting designers by pinpointing weaknesses.

Some benefits of deterministic analysis for analysing operational events are illustrated in Figure 2.3.1.

Since a large number of operational events have occurred in nuclear power plants, only a few events were analysed by deterministic computer codes [128]. In most cases, the causes of the event and the phenomena involved were considered to be understood, and detailed analysis of the event was not found necessary. If the event remains within the range of the unit's technical specifications and the response of the unit is correlated to existing analytical predictions, then the event does not need deterministic analysis (although such analyses could be beneficial for code and model validation purposes).

Some of the main problems encountered in deterministic risk analysis are [129]:

- Deterministic risk analysis relies on a wealth of experience or 'common sense', which is often very specific for different companies and persons. Established practices are usually fine for dealing with high probability events, where cause and effect can easily be demonstrated. In many cases, however, decisions are required without this 'test of time' being available, because either the situation under consideration is complex or unusual, or the possible consequences are very severe.
- In deterministic risk analysis, there is no explicit consideration of the various types of uncertainties, and there is a lack of consistent information about which criteria or analysis results are more or less important with respect to the overall safety level. A strictly deterministic ranking procedure regarding the issues considered or the outcomes is not possible. Instead of this some sort of semi-quantitative 'weighting factor' approaches are used, whose assumptions are extremely difficult to justify.
- The real world cannot be modelled realistically by mainly using conservative assumptions. The worst case scenario selected for deterministic risk analysis represents only very rare single event

in the myriads of possible event sequences. Due to this there is a real danger that deterministically analysed systems are oversized in terms of their safety or protection equipment.

- Deterministic risk analysis results give the false impression that the results are ‘certain’ and the scenarios are ‘true’.

Since a deterministic safety analysis alone does not demonstrate the overall safety of the plant, it should be complemented by a probabilistic safety analysis. While deterministic analyses may be used to verify that acceptance criteria are met, probabilistic safety analyses may be used to determine the probability of damage for each barrier. Probabilistic safety analysis may thus be a suitable tool for evaluation of the risk that arises from low frequency sequences that lead to barrier damage, whereas a deterministic analysis is adequate for events of higher frequency, for which the acceptance criteria are set in terms of the damage allowed. To verify that defence in depth is adequate, certain very low frequency design basis accidents, such as large break loss of coolant accidents or rod ejection accidents, are evaluated deterministically, despite the low frequency of the initiating event. Thus deterministic analysis and probabilistic analysis provide a comprehensive view of the overall safety of the plant for the entire range of the frequency-consequence spectrum [76].

Deterministic safety analyses have an important part to play in the performance of a probabilistic safety analysis because they provide information on whether the accident scenario will result in the failure of a fission product barrier. Deterministic safety analysis should be used to identify challenges to the integrity of the physical barriers, to determine the failure mode of a barrier when challenged, and to determine whether an accident scenario may challenge several barriers. Best estimate codes and data should be used to be consistent with the objectives of probabilistic safety analysis, which include providing realistic results. It should be recognised that the results of the supporting analyses are usually bounded by the results of conservative deterministic analyses.

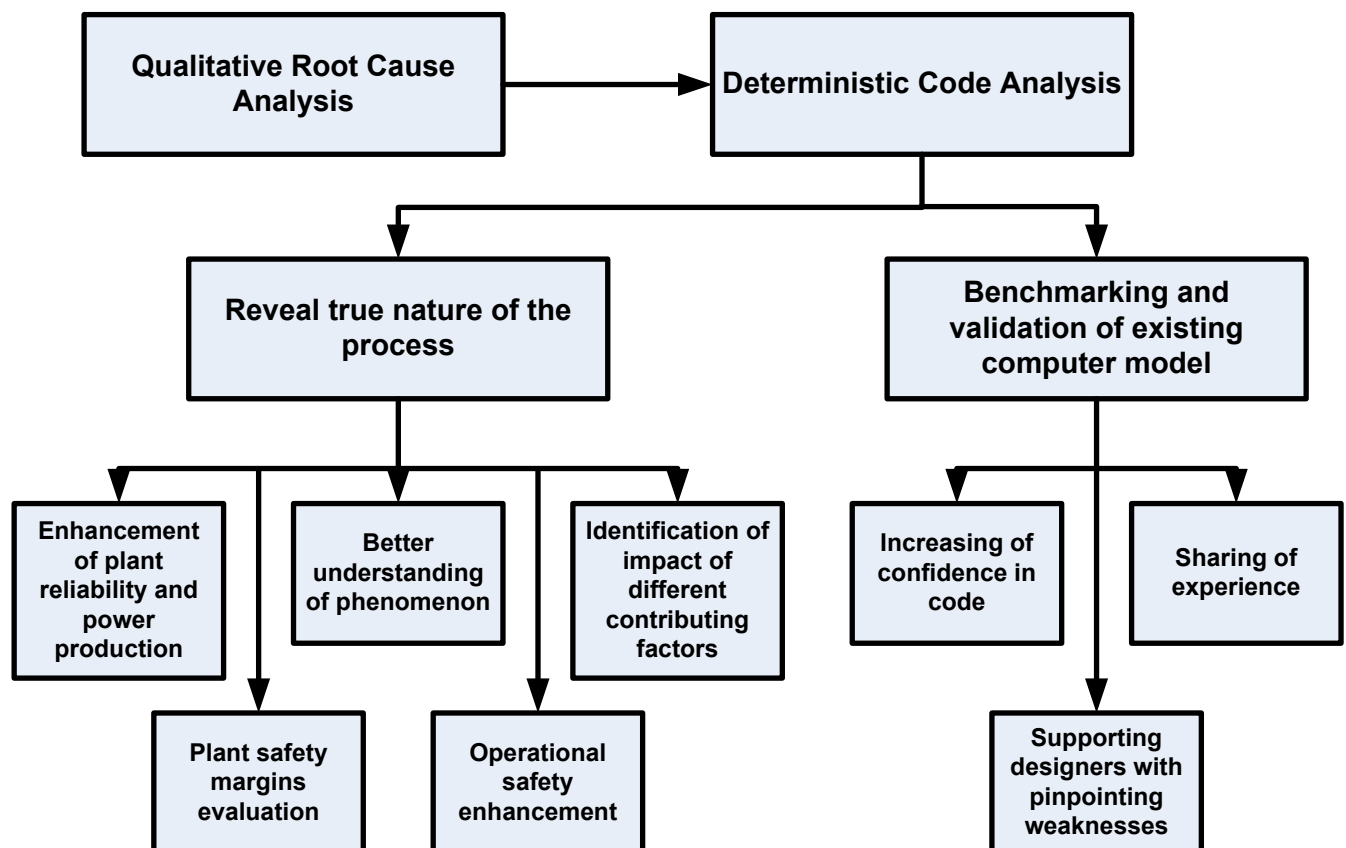


Figure 2.3.1. Benefits of the deterministic analysis of operational events

2.4. Safety Culture Impact Assessment

Safety culture has been recognised as one of the paramount factors in guaranteeing the safe operation of complex facilities. Indeed, analysis of many events in several industries including aviation, space exploration, the oil, railway, chemical and nuclear industries, has shown that - besides technical factors - organisational and human factors largely contribute to the prevention of incidents and accidents.

Safety culture is defined as the assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance [24, 37]. INPO defines safety culture as ‘an organisation’s values and behaviours – modelled by its leaders and internalised by its members – that serve to make nuclear safety the overriding priority’ [83].

At the same time, the organisational climate is defined as the way in which organisational members perceive and characterise their environment in an attitudinal and value-based manner [130, 131]. Lack of a common agreement on terms and definitions results in one more areas of confusion regarding the root cause analysis of events: most of licensees misunderstand that organisational factors are equivalent to safety culture.

The structure of safety culture can be explained using the Three Level model that was developed by Edgar Schein (see Figure 2.4.1) [78, 79, 81, 85, 86, 87].

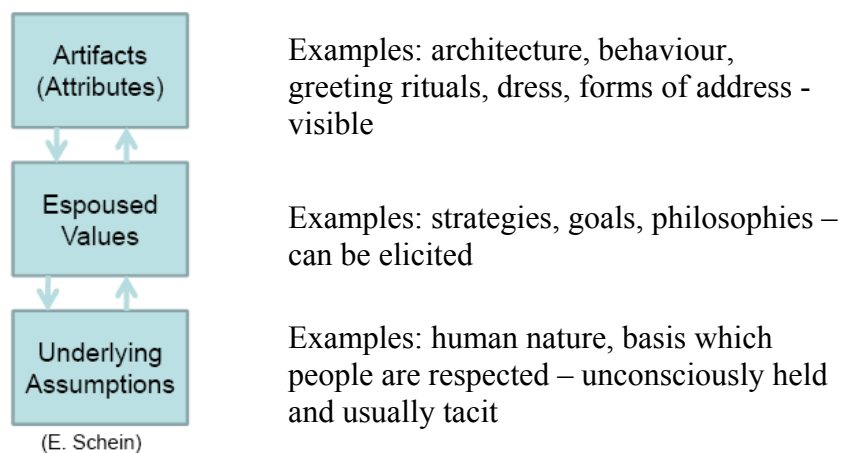


Figure 2.4.1. Three Level model of safety culture

Safety culture at a specific organisation can be defined by system of safety culture characteristics [78, 86-90]. Most of the characteristics can be assigned to the artefact level and/or the espoused level of the Three Level model, with only a small number more appropriately associated with the level of basic assumptions. Employee surveys (questionnaires, interviews) and different systems of performance indicators are used to obtain specific quantitative or qualitative information about the state of safety culture [78, 79, 82]. Some examples of performance indicators listed under the different levels of culture, in line with the Three Level model, that may be useful in measuring the overall state of safety culture, are shown below [79].

Artefacts

- (1) Percentage of corrective actions not completed within planned timescale (a measure of proper resource allocation, top management commitment to safety).
- (2) Safety audit scores (a measure of safety performance, self-assessment).
- (3) Safety attitude scores (a measure of employee involvement, motivation and job satisfaction).
- (4) Percentage of tasks having risk assessment in pre-work planning (a measure of a systematic approach to safety).

Espoused values

- (1) Frequency of senior manager plant tours (demonstrates high priority to safety).
- (2) Number of safety inspections (demonstrates high priority to safety).
- (3) Percentage of managers trained in root cause analysis (organisational learning).

Basic assumptions

- (1) Frequency of reporting of near misses (view of mistakes).
- (2) Number of safety improvement teams (view of people).
- (3) Percentage of employees who have a basic understanding of the safety culture concept and its importance (properly designed plant is inherently safe).

Other systems explaining structure of safety culture also exist. Most of them are based on different classification system of safety culture's attributes and characteristics (see Figure 2.4.2) [86]. For example, Conger [24] distinguishes 13 components of safety culture, separated into 4 groups:

- Human performance (Decision-Making, Resources, Work Control, Work Practices);
- Problem identification and resolution (Corrective Action Programme, Operating Experience, Self and Independent Assessments);
- Safety conscious work environment (Environment for Raising Concerns, Preventing, Detecting, and Mitigating Perceptions of Retaliation);
- Other components (Accountability, Continuous Learning Environment, Organisational Change Management, Safety Policies).



Figure 2.4.2. Structure of safety culture according to [86]

In practice, safety culture represents the ratio between priorities of importance attached by an organisation (especially by its management) to economic and production problems from the one side, and problems of safety assurance and improvement, from another side (see Figure 2.4.3) [24, 36, 78, 79, 82- 91].

Safety culture impact assessment is not an event investigation methodology. However, actual and often unidentified root causes of a considerable number of incidents at NPPs lie in deficiencies in safety culture. Root causes reside in the values and beliefs embedded in the organisation that are justified and reinforced by the behaviour of management. This would seem to be a suitable point to recall W. Edwards Deming's observation that 'most problems are management controllable - embedded in the manner in which management decides to operate the organisation' [94]. Until the analysis moves to this

level, an organisation has not begun to grapple with root causes. According to data from the Japan Functional Safety Laboratory [35], about 70 to 80% of accidents are caused by human factors. But in reality, often human factors are not the actual root cause of accidents. The actual root causes are generally made up of the following three elements: a) a lack of safety culture (overconfidence and self-satisfaction are the leading factors of this); b) organisational issues; c) a lack of relevant technology activities.

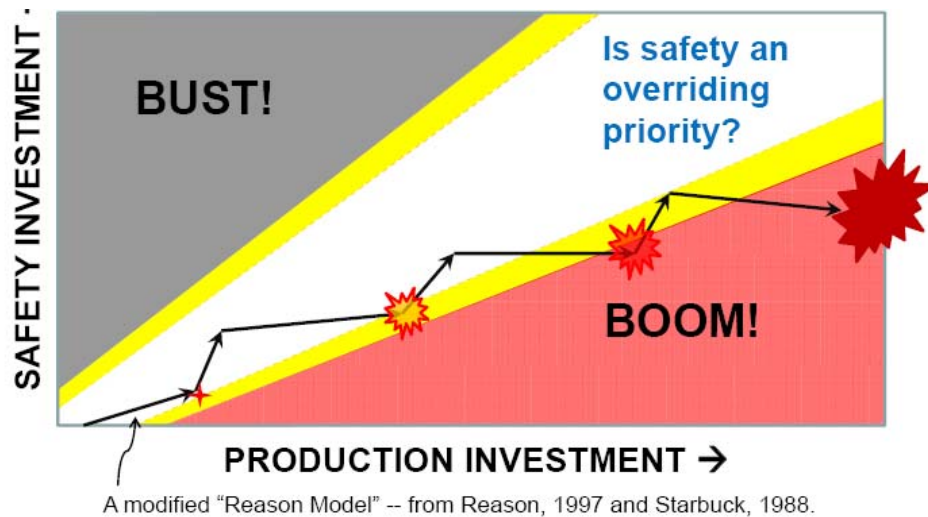


Figure 2.4.3. Role of safety culture as the balance between mission and safety [84]

Hence, assessment and improvement of safety culture should be considered as a promising and effective pro-active approach to precluding the different human factor related errors, initiating occurrences and incidents, leading to more serious safety related events. Assessment and improvement of safety culture, in combination with other event investigation methodologies, should be assumed to be an important means of increasing the reliability of NPP's operation [23, 24]. Assessment of safety culture is needed for establishing the safety level for benchmarking, for predicting the outcome of proposed safety interventions and for follow-up of improvements (see Figure 2.4.4).

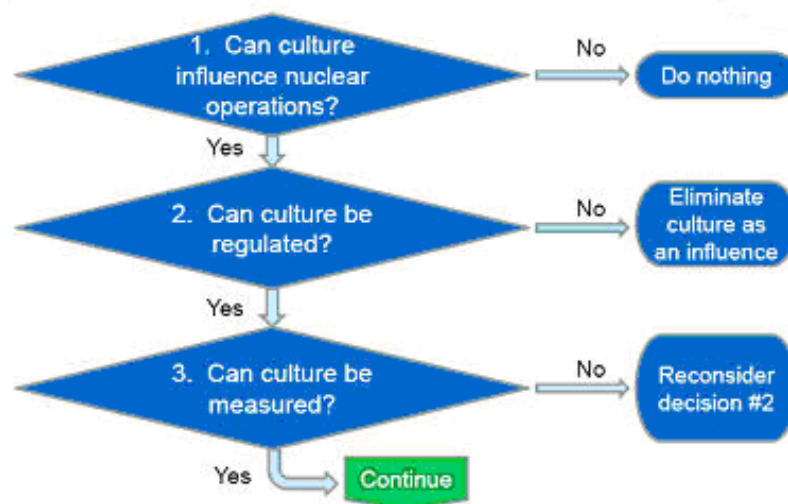


Figure 2.4.4. Main questions which should be answered before safety culture impact assessment [84]

Figure 2.4.5 shows the desired responses at the organisational levels of policy, management and the individual. The policy level establishes the necessary framework for the organisation. Management shapes the working environment and fosters attitudes conducive to achieving good safety performance. At the individual level, a questioning attitude, a rigorous and prudent approach, and good communication are emphasised.

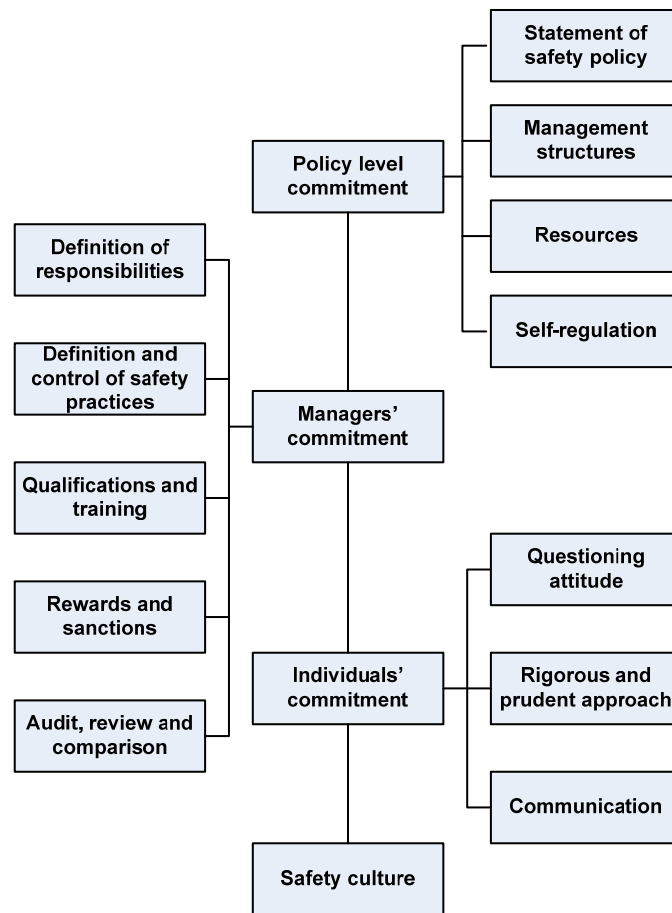


Figure 2.4.5. The desired responses at the organisational levels of policy, management and the individual conditioning of safety culture [82]

From the literature it emerged that management was the key influence of an organisation's safety culture [87]. A review of the safety climate literature revealed that employees' perceptions of management's attitudes and behaviours towards safety, production and issues such as planning, discipline etc. were the most useful measurement of an organisation's safety climate. The research indicated that different levels of management may influence safety in different ways, for example managers through communication, and supervisors by how fairly they interact with workers. Thus, the key area for any intervention regarding an organisation's safety policy should be management's commitment and actions towards safety. Ultimately management's attitudes and behaviour in terms of safety influence many aspects of safety behaviour including:

- the success of safety initiatives
- the reporting of near-miss occurrences, incidents and accidents
- employees working safely
- employees taking work related risks
- influencing production pressures
- implementing safety behaviour interventions
- health interventions
- the effectiveness and credibility of safety officers
- the effectiveness and credibility of safety committees.

Analysing results of investigations of several major accidents, such as the nuclear reactor accident at Chernobyl, the fire at King's Cross, the fire and explosion on Piper Alpha and the train crash at Clapham

Junction [87], it was recognised that a successful safety culture depends on leadership and, in practically all cases, needs to be improved.

The primary role of leaders in developing the organisational safety culture is also highlighted in [84, 90]. Corporate top managers influence safety through their decision-making on budgets and policies, but also through their daily actions and attitudes (see Figure 2.4.6). These channels of influence are important in forming the safety culture of the company. This is of particular interest in transport, chemical, oil, nuclear and other high-risk industries, where human errors are an important source of safety hazards, and safety culture is closely related to handling of risk. If the problems of administrative management cannot be prevented by improving daily management factors (that is, middle (junior) management cannot be improved), the top (senior) management factors and organisational climate should be analysed.

So, assessment and improvement of safety culture in combination with other event investigation methodologies should be assumed as important means of increasing reliability of NPP's operation. However, taking into account other on-going projects being performed by the IAEA, NEA WGOE, JRC IE SPNR and other organisations, methods and tools for measurement and assessment of safety culture are beyond the scope of this report. Some information about development, attributes and usage of these methods and tools can be found in [36, 78, 82, 84 - 90].

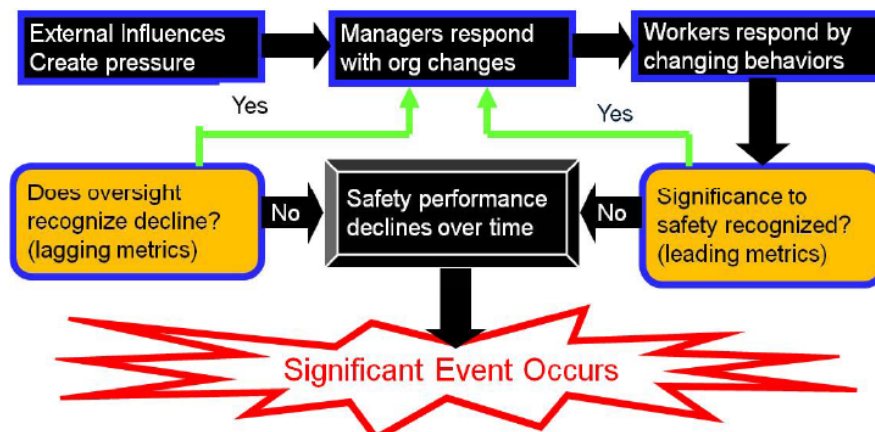


Figure 2.4.6. Possible scenario of changes preceding major accidents with emphasised role of leaders/managers creating safety culture [84]

3. Event investigation tools and techniques

The root cause analysis tool is a relatively simple event investigation instrument, developed through experience to assist groups and individuals in identifying root causes, providing detailed step-by-step working procedures for event analysis that can be recorded, repeated and verified. It is merely one of the vehicles to implement the method; it is distinguished by its limited use, relatively narrow scope and concretely defined inputs, procedures and outputs.

Usually root cause analysis relies to some extent on engineering, psychological etc. judgment. However, structured root cause analysis tools and techniques provide step-by-step procedures that can be repeated and verified. Clear documentation of the analysis allows a reviewer to check its accuracy and completeness, enhance rigour, traceability and credibility.

Practical experience has shown that different root cause analysis techniques provide different perspectives of an event, and the causes that are identified may differ [4]. This is because different root cause analysis techniques ask different questions about a human performance or hardware problem. As a result, best practices indicate that using a combination of tools ensures that a more complete set of causal factors is identified, increases confidence in findings and improves the quality of investigations. For example, events and causal factors charting and analysis, change analysis and barrier analysis work well together to ensure that all causal factors are identified. Techniques should generally be adopted early in the investigation for maximum effectiveness. To apply a technique at the end to 'illustrate' is to miss much of its benefit [24].

No matter which root cause analysis tools or techniques are used, the purpose of the analysis is to identify the causal factors that, if corrected, would minimise the likelihood that the same and similar 'significant conditions adverse to quality' will occur again. The effectiveness of a problem identification and resolution programme rests less on the root cause analysis tools or techniques used than on the thoroughness of the investigation conducted, assurance that the key causal factors have been identified, and the development and implementation of the corrective actions suggested by the analysis.

Analytical tools are only as good as their users. Used properly, any of these tools can be effective and produce good results. However, experience shows that the attractiveness of these tools is actually their drawback as well. Some of these tools are typically attractive because they are quick to produce a result, require few resources and are inexpensive. These are the very same reasons why they often lack breadth and depth [56].

There are many different root cause analysis tools, techniques and procedures of various complexity used in different industries. Depending on the authors concerned, some of them are called either tools or methods (or even methodologies). In 1982, there were 30 analytical techniques. Today, more than 100 have been identified. An adequate combination of methodologies, methods and tools should be selected, based on the nature of the event. The most frequently used universal root cause analysis tools are depicted in Figures 3.1 and 3.2. Some of them are widely used for solving different problems of other types. Many of the methods described in chapter 2 have been developed by combining the use of a certain number of basic tools, such as the following [4, 25, 30, 47]:

1. Event and causal factor charting and analysis
2. Cause and effect analysis
3. Interviewing
4. Task analysis
5. Change analysis
6. Barrier analysis
7. Fault tree analysis
8. Event tree analysis
9. Review of plant operating experience
10. Critical incident techniques
11. 5 Why's analysis

12. Pareto analysis
13. Storytelling
14. Failure modes and effect analysis
15. Interrelationship diagram
16. Current reality tree (CRT).

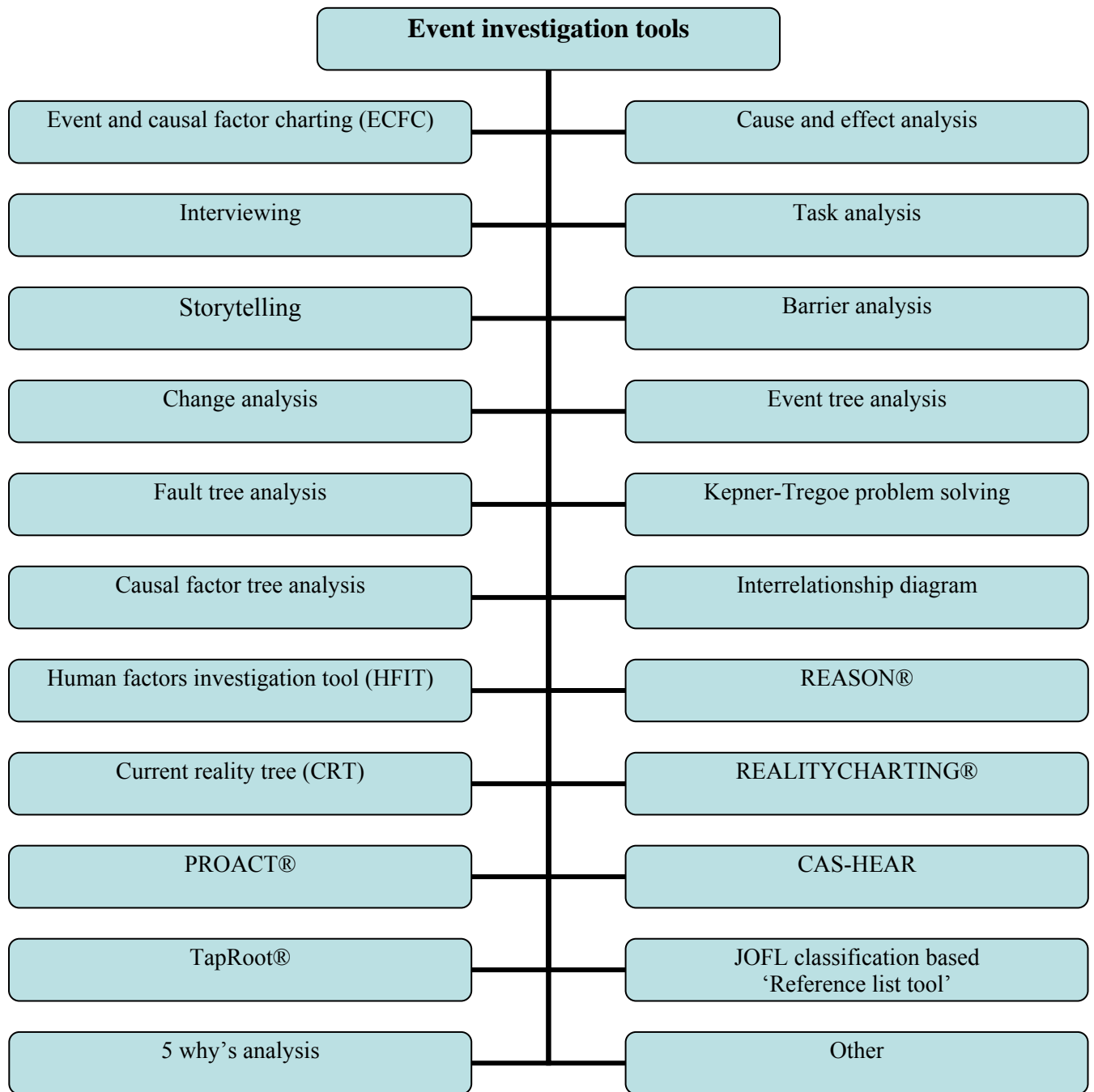


Figure 3.1. Some of most frequently used universal root cause analysis tools

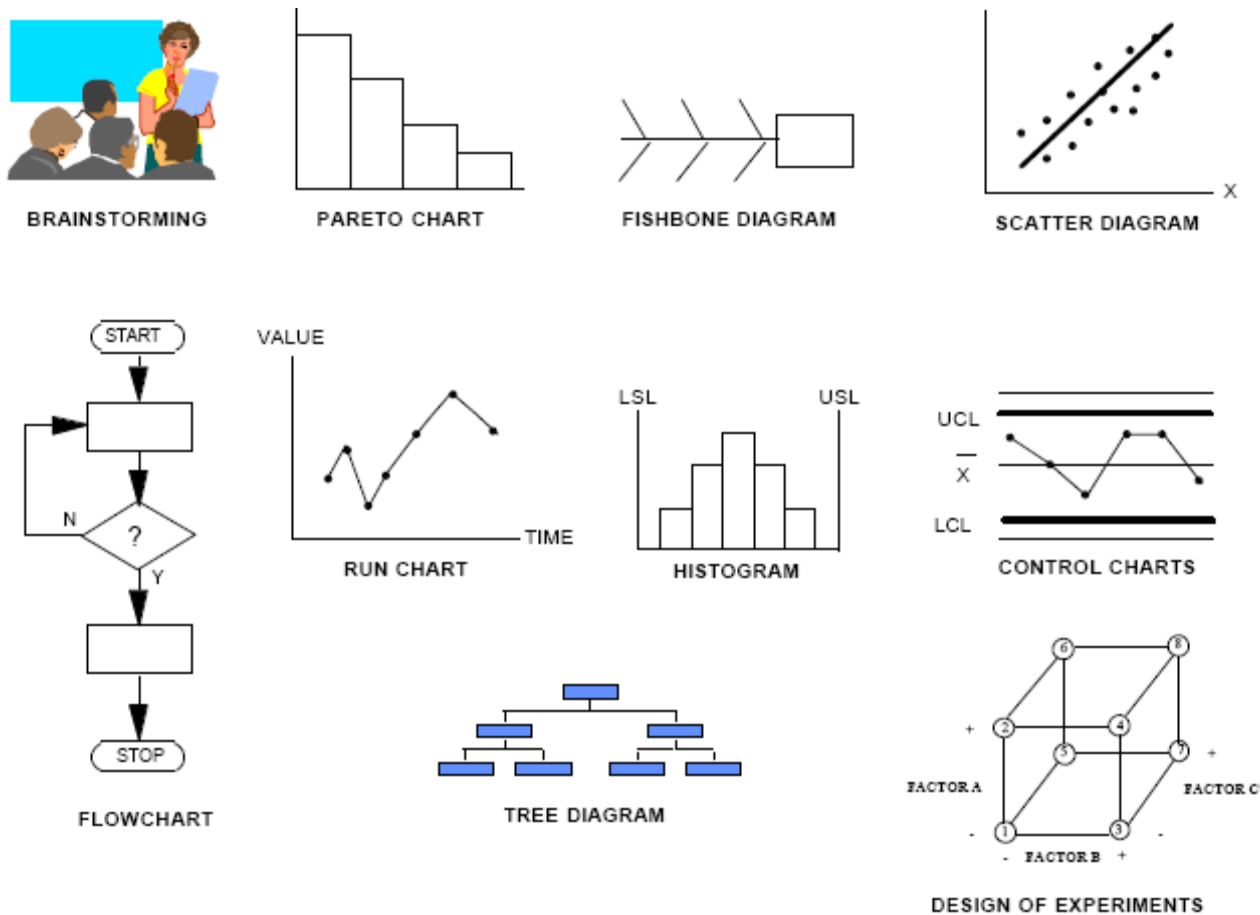


Figure 3.2. Examples of some of most frequently used universal root cause analysis tools

Brainstorming is a process in which a group quickly generates as many ideas as it can on a particular event, problem and/or subject [30, 56]. Usually such sessions are not structured in a manner that explores cause and effect relationships. Rather, people just express their opinions and come to a consensus on solutions. Brainstorming is useful because it can help a group of people utilise its collective brainpower to generate many ideas in a short period of time. It stimulates creativity and promotes involvement and participation. It should be used to help clarify mutual expectations and devise ground rules related to a team's way of operating. It is recommended that brainstorming be carried out using the following procedure:

- Identify a topic, problem or issue and make sure there is mutual understanding of the task and objective. Write the topic on a flip chart.
- Each person presents one idea, going round in sequence (Round Robin). If a person doesn't have an idea, pass and move on to the next person.
- All ideas are recorded on a flipchart.
- There is no evaluation or discussion during the session.
- Focus is on the quantity of ideas, not the quality.
- When all ideas are exhausted, take a break. When you come back, people may have more ideas to add to the list.
- Keep the idea generation separate from the evaluation or analysis of ideas.

Additional guidelines for brainstorming:

- Generate as many ideas as possible.
- Encourage free-wheeling.
- No criticism is allowed, either positive or negative.
- There is equal opportunity to participate.

- Record all ideas.
- Let the ideas incubate.

When comparing this approach to the essential criteria of RCA, brainstorming does not meet all the criteria, and therefore falls into the Shallow Cause Analysis category.

Pareto Analysis uses a failure database to trend the frequency of categorical failures. This process has many pitfalls, a few of which are discussed below.

1. The accuracy of a Pareto chart is limited by the accuracy of the data used to create it. If you use a failed approach like tree diagrams to determine the causes, the Pareto chart will only reflect causes from the pre-defined list provided.
2. The cause and effect principle shows that all causes and effects are part of the same continuum. In many cases, certain causes will be closely linked (i.e. close to each other). For example, the cause 'procedures not followed' is frequently caused by 'procedures not accurate.' In the Pareto analysis, this causal connection is lost. Instead, we see both 'procedures not followed' and 'procedures not accurate' in those top causes, so we end up working on solving both problems, when in reality we may only need to solve the 'procedures not accurate' problem. In this example, the incomplete view of reality provided by a Pareto analysis may have caused us to expend more resources than necessary.
3. Pareto analysis can mask larger, more systemic issues. For example, if quality management has transformed into a state of dysfunction, it can cause symptoms in many different areas, such as poor procedures, inadequate resources, outdated methods, high failure rates, low morale, etc. Pareto analysis has us capturing all these symptoms of a larger problem as causes, and wasting time solving the symptoms.

Storytelling. Perhaps the most common of all available tools for collection of information about the circumstances of an event is storytelling, also known as the 'fill-out-a-form method'. It is a primary form of communication between event investigator and event witnesses or participants [25]. The basis for any story is a sequence of events starting at some arbitrary point in the past, leading the reader to a significant undesirable consequence. Opinions, or consensus of a group, are then presented as corrective actions.

The primary purpose of this method is to collect initial data about the event under investigation and document the investigation and corrective actions, using special pre-defined forms. These forms usually do a good job of capturing the what, when, and where of the event, but little or no analysis occurs. Many companies do not even write the story down; they get together with the decision makers and tell stories to one another, then decide which category the problems fits into, and implement their favourite solution. Consequently, the corrective actions derived from storytelling fail to prevent recurrence 70% to 80% of the time [25].

The primary difficulty with this approach is that the investigator relies completely on the experience and judgment of the story-tellers or report authors in ensuring that the recommended solutions connect to the causes of the problems. Storytelling does not provide precise mapping between the problem and the recommended solutions. The issue of concern, however, is more than just poor reports; it is poor problem solving skills that are reinforced by poor report writing and rule-based thinking, like filling out a form. Forms subtly tell users to turn off their brains, fill in the blanks, write a good story, tick the boxes, and identify the right categories.

With such poor results, some might question why organisations continue to use this tool for development of the corrective actions programme. The answer is twofold. First, most organisations do not measure the effectiveness of their corrective actions, so they do not know they are ineffective. Second, there is a false belief that everyone is a good problem-solver, and that all they need to do is document their solution on a form. For those companies that recognise that they are experiencing repeat events, a more detailed form is often created, that forces the users to follow a specified line of questions with the belief that an effective solution will emerge.

This is a false promise, because the human thinking process cannot be reduced to a form. Attempting to standardise the thinking process, we restrict our thinking to a predefined set of causes and solutions. Because effective problem solving has been short circuited, the reports often are incomplete and the

problems keep occurring. It has been noted that ability to solve problems is conversely proportional to storytelling: the stronger the storytelling culture that exists within an organisation, the less effective people are at problem solving [25].

Troubleshooting is usually a ‘band-aid’ type of approach to fixing a situation quickly and restoring the status quo. Typically, troubleshooting is done by individuals, as opposed to teams, and requires no proof or evidence to back up assumptions. This off-the-cuff process is often referred to as RCA, but it clearly fails to meet the criteria to qualify as RCA [56].

Problem Solving comes the closest to meeting the RCA criteria. Problem Solving is usually team based and uses structured tools. Some of these tools may be cause-and-effect based, some may not be. Problem Solving often fails to meet the RCA criteria because it does not require evidence to back up what team members hypothesise. When assumption is permitted to be treated as fact in a process, it is not RCA [56].

The 5 Why’s technique was originally developed by Sakichi Toyoda and was later used within Toyota Motor Corporation during the evolution of their manufacturing methodologies. It is a critical component of problem solving training delivered as part of the induction into the Toyota Production System. However, the 5 Why’s approach itself has been around rather longer. The earliest known written version of the rhyme on the 5 Why’s (often taught to British children) is in John Gower’s *Confesio Amantis*, dated approximately AD 1390 [132].

The 5 Why’s is a questions-asking technique used to explore the cause/effect relationships underlying a particular problem. Ultimately, the goal of applying the 5 Why’s is to determine a root cause of a defect or problem [132]. The 5 Why’s procedure involves asking ‘Why?’ five times in succession. This can sound deceptively simple, but requires intelligent application in order to find the right Why? question to ask, and the discipline and persistence to follow the procedure. The answer to one question leads you to ask the next ‘Why?’ question, although it may not always be possible to answer the next question immediately. You may need to gather and analyse more information in order to answer it properly, or do more thinking and brainstorming. By the time you get to the fourth or fifth ‘Why?’ you are almost invariably looking straight at management practices as opposed to mere symptoms (see Figure 3.3). The 5 Why’s tool is valuable and powerful, but it does require practice. The more you use and practise it, the more you begin to find the real root causes of problems.

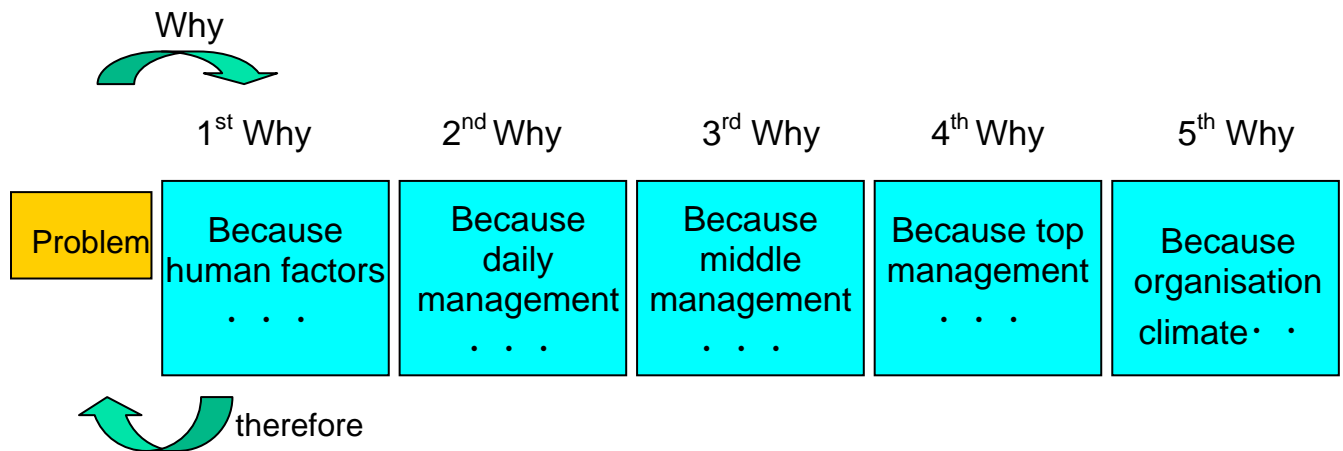


Figure 3.3. Example of using of 5 WHY’s tool [132]

The questioning ‘Why?’ could be continued further to a sixth, seventh, or even greater level. This would be legitimate, as the ‘five’ in 5 Whys is not gospel; rather, it is postulated that five iterations of asking why is generally sufficient to get to a root cause. The real key is to encourage the investigator to avoid assumptions and logic traps, and instead to trace the chain of causality in direct increments from the effect, through any layers of abstraction, to a root cause that still has some connection to the original problem. Note that in this example the fifth why suggests a broken process or an alterable behaviour, which is typical of reaching the root-cause level.

Advantages. If an investigator knows how to ask good, successive ‘why’ questions, and is able to ask them of the right people, they will find at least one root cause for a given problem. This approach takes little time to perform – as few as five minutes can be used to perform a 5Why analysis – and does not require the use of special software, flip chart paper or reading materials. If it is performed repeatedly with the same group of people in a sound manner, its use can lead to a new way of thinking amongst those people that have been exposed to the tool’s use [110].

Disadvantages. While the 5 Why’s is a powerful tool for engineers or technically knowledgeable individuals to help get to the true causes of problems, it has been criticised as being too basic a tool to analyse root causes to the depth that is needed to ensure that the causes are fixed. Reasons for this criticism include:

- tendency for investigators to stop at symptoms rather than going on to lower level root causes;
- inability to go beyond the investigator’s current knowledge - can’t find causes that they don’t already know;
- lack of support to help the investigator to ask the right ‘why’ questions;
- results aren’t repeatable - different people using 5 Why’s come up with different causes for the same problem;
- tendency to isolate a single root cause, whereas each question could elicit many different root causes.

In addition, the ‘5 Why’s’ approach normally leads to the identification of just one root cause for the problem concerned. You need to go through the ‘5 Why’s’ process several times for a given problem in order to ensure that all root causes are identified, and being able to do so effectively requires even more skill on the part of the question asker. Also, it does not necessarily point the problem solver towards the generic causes of similar problems.

This approach requires significant skill in order to ask the right ‘why’ questions – the ‘5 Why’ technique is not as simple as asking ‘why’ alone five times. While use of this tool leads to the definition of a root cause that is also a change that is needed (a corrective action), it does not often result in a corrective action that is well developed and defined. Most people fail to gain much success when using this tool, simply because they cannot develop the ability to ask good ‘why’ questions in succession [110].

These can be significant problems when the ‘5 Why’s’ is applied through deduction only. On-the-spot verification of the answer to the current ‘why’ question, before proceeding to the next, is recommended as a good practice to avoid these issues.

The ‘5 Why’s’ tool is inappropriate for any complicated event, but it is actually quite useful when used on minor problems that require nothing more than some basic discussion of the event. Unlike most of the other RCA tools, it identifies causal relationships, but still subscribes to the root cause myth of first finding the root cause and then assigning solutions. It should never be used for formal incident investigations, but is perfectly acceptable for informal discussions of cause. A popular graphical representation of the ‘5 Why’s’ approach is the ‘Why Staircase,’ which if used improperly leads to a linear set of causal relationships [25].

The root cause analysis tool called ‘**JOFL classification**’, using a viewpoint-oriented approach has been suggested in Japan [130, 131, 153]. This approach is based on the assumption that, if the problems of administrative management cannot be prevented by improving the daily management factors (that is, middle (junior) management cannot be improved), the top (senior) management factors and organisational climate and safety culture should be analysed, because usually management brings about the situations leading to the nonconformity or overlooks them until the nonconformity occurs [131]. In order to analyse deep-rooted causes contained in organisational factors, a new taxonomy was systematised as a ‘Reference List’ of the NISA Guideline [131]. ‘JOFL classification’ is composed of 6 key factors, structured by 63 intermediate classification categories and 137 viewpoints. The key factors include external environmental factor, organisational psychology factor, top management factor, middle management factor, group factor and individual psychological factor. Nuclear power reactor site inspectors and licensees in Japan use ‘JOFL classification’ as a checklist [131].

The majority of the above mentioned root cause analysis tools (excluding such simple tools as interviewing, task analysis) are currently supported with more or less sophisticated software, aiming to accelerate and make easy the event investigation process. Some of the modern RCA tools are designed to be implemented by means of specialised software. To this group could be attributed the following RCA tools [139]:

1. REASON Root Cause Analysis Software is designed for organisations that have a commitment to operational excellence. It is an expert system software that guides you to uncover the root causes of your operational problems, enables you to manage and track your corrective action plans, and communicates the lessons learned from your problem solving activities. It aims to preserve and communicate the knowledge learned from identifying and correcting the root causes of problems.
2. TapRooT Software was once just a very good root cause analysis tool and is now an Investigation Management System. It provides tools to manage the process from reporting an incident to validating the effectiveness of corrective actions. You can use one piece of software to report incidents, analyse root causes, develop corrective actions, write and approve reports, track fixes, validate the effectiveness of the fixes, and trend performance in a secure, password protected environment. TapRooT Software is unique, advanced, and has been patented.
3. NASA Root Cause Analysis Tool (RCAT) Software is designed to facilitate the analysis of anomalies, close calls, and accidents and the identification of appropriate corrective actions to prevent recurrence. The RCAT software provides a quick, easy, accurate, and repeatable method to perform and document root cause analysis, identify corrective actions, identify trends, and generate data usable in precursor analysis and probabilistic risk assessment.
4. ReliaSoft's XFRACAS software tool is a Web-based, closed-loop, enterprise-wide incident reporting/failure reporting, data analysis and corrective action software system. The XFRACAS software provides all the tools that any organisation needs to troubleshoot issues as they occur in the laboratory or in the field, capture the data required for important reliability, quality, safety and other analyses, work as a team to resolve underlying problems, and build a 'knowledge base' of lessons learned that will be instrumental in future troubleshooting and development efforts.
5. PathMaker helps you to systematically improve quality, solve problems, execute projects, and design innovative products and services. It has tools to brainstorm, create flowcharts,, charts and graphs together, analyse problems, track progress and indicators, think of solutions and accelerate your projects.
6. RealityCharting is a powerful, user-friendly software solution, created to help people better understand their problems and identify effective solutions that prevent recurrence. Whether you are a professional incident investigator, facilitator or an interested party, RealityCharting helps you to understand and document your problem better than you have done previously. A Wizard window guides the new or occasional user through the rules of the Apollo method and leads them towards completion of a Realitychart. Creating a Realitychart is accomplished in an iterative five-step process, integrally connected to implementation of the Apollo RCA process.
7. Solve makes root cause analysis very simple, as the software is designed to be extremely easy to use. The software helps you to build the Root Cause Tree directly on the screen and analyse all elements in a Path to Failure in one simple view. It lets you examine the entire Root Cause Tree in the Overview screen and instantly see the big picture, to come up with relevant actions to address the cause.
8. Tripod Beta is a systematic and structured process of incident investigation and analysis. It makes unknowns and uncertainties visible during the investigation, provides insights into the effectiveness of control mechanisms and latent failures, and lists the remedial actions to achieve sustainable improvement. It generates a Tripod Beta tree that is a graphical representation of the investigated incident (see chapter 1.1.6). The tree is easy to interpret and is a powerful tool for presenting and communicating the investigation results.
9. The PROACT® RCA Enterprise Suite gives your organisation the ability to collaborate on, and share root cause analysis data with, your investigation team and management personnel within your facilities worldwide. You can build fact driven logic trees, import/export numerous file types, organise analysis data, and customise automatically generated analysis reports, then print and share.

10. Investigation Catalyst is a new genre of self-directing, collaborative investigation support software for documenting, understanding, analysing and improving phenomena and processes of all kinds of problems faster and better. It is process design, investigation and improvement support software, developed to support the management and conduct of process development, hazard analyses, accident and incident investigations and analyses, investigation report quality assurance, and change management tasks.

It should be noted that the list of tools for event investigation mentioned above, and presented in Figs. 3.1 and 3.2, is not comprehensive. New tools are invariably being developed and appearing in the market (especially in the form of software), and only some of them are described in more detail below.

3.1. Event and causal factor charting and analysis

Events and causal factors charting and analysis is a tool for organising and analysing the evidence gathered during an investigation [2, 4, 13, 18, 47, 53]. This tool is the first that can be used for all investigations. An events and causal factors (ECF) chart displays graphically the events and conditions associated with an occurrence on a time line, highlighting occurrences and contributors (e.g. an error, a significant event, a human performance problem). It is developed by asking successively ‘what?’, ‘how?’ and ‘why?’ and presenting the information gained from answers graphically. This tool helps to identify what is known and what needs to be known chronologically, thus helping to set the direction of further investigation. As more information is discovered, the chart is updated, thus providing a continuous graphical indication of the progress of the investigation. In an ECF analysis, the chart is used to identify the causal factors associated with the hardware failure or human performance problem.

Events and causal factors analysis is an effective mean of integrating other analytical techniques into a concise and complete investigative summary. Events and causal factors analysis depicts, in logical sequence, the events and conditions which are necessary and sufficient for an accident to occur. It provides a systematic accident analysis tool to help in collecting, organising, and depicting accident information; validating information from other analytical techniques; writing and illustrating the accident investigation report; and briefing management on the results of the investigation [142, 143].

An ECF chart comprises symbols that represent the important events and conditions that led up to the hardware failure or human performance problem under investigation. **An event** in an ECF chart is any action or occurrence that happened at a specific point in time relative to the hardware failure or human performance problem under investigation. **A condition** is a state or circumstance that affected the sequence of events in the ECF chart. The symbols used for charting are unimportant. Any symbol set or other method to differentiate between events, conditions, causes and their inter-relationship, such as colour-coding, may be used in the chart.

Suggested Criteria for Event Descriptions and Conditions:

- Each event should describe an occurrence or happening and not a condition, state, circumstance, issue, conclusion, or result; i.e., ‘pipe wall ruptured’, not ‘the pipe wall had a crack in it’.
- Each event should be described by a short sentence with one subject and one active verb; i.e., ‘mechanic checked front end alignment’, not ‘mechanic checked front end alignment and adjusted camber on both front wheels’.
- Each event should be precisely described; i.e., ‘operator pulled headlight switch to “on” position’, not ‘operator turned lights on’.
- Each event should describe a single, discrete occurrence; i.e., ‘pipe wall ruptured’, not ‘internal pressure rose and pipe wall ruptured’.
- Each event should be quantified when possible; i.e., ‘plane descended 350 feet’, not ‘plane lost altitude’.
- Each event should be derived directly from the event (or events in the case of a branched chain) and conditions preceding it; i.e., ‘mechanic adjusted camber on both front wheels’ is preceded by ‘mechanic found incorrect camber’ which is preceded by ‘mechanic checked front end alignment’ -

each event deriving logically from the one preceding it. When this is not the case, it usually indicates that one or more steps in the sequence have been left out.

- Conditions differ from events insofar as they (a) describe states or circumstances rather than happenings or occurrences; (b) are passive rather than active. As far as practical, conditions should be precisely described, quantified when possible, posted with time and date when possible, and be derived directly from the conditions immediately preceding them.

Some specific symbols are used when creating ECF Charts. For example, a rectangle is typically used to indicate an event. A brief description of the event is written within the symbol, as well as the date and time at which the event occurred. Events are arranged in a line in chronological order, from left to right. Dashed rectangle is used to indicate events that are assumed to have occurred, but for which no validated evidence exists or has yet been collected. An oval is typically used to indicate a condition. A brief description of the condition is written within the oval, and the condition is placed above the event it affected on the chart. Dashed oval shows a condition that is assumed to have existed, but for which no validated evidence exists or has yet been collected. A diamond is used to indicate the occurrence of interest, such as a significant event. Arrows are used to connect events, and to connect conditions to events. An octagon may be used to indicate a causal factor, and is placed above the events or conditions it caused, and triangles are used to connect event lines that must be broken when, for example, the entire sequence of events will not fit on a page.

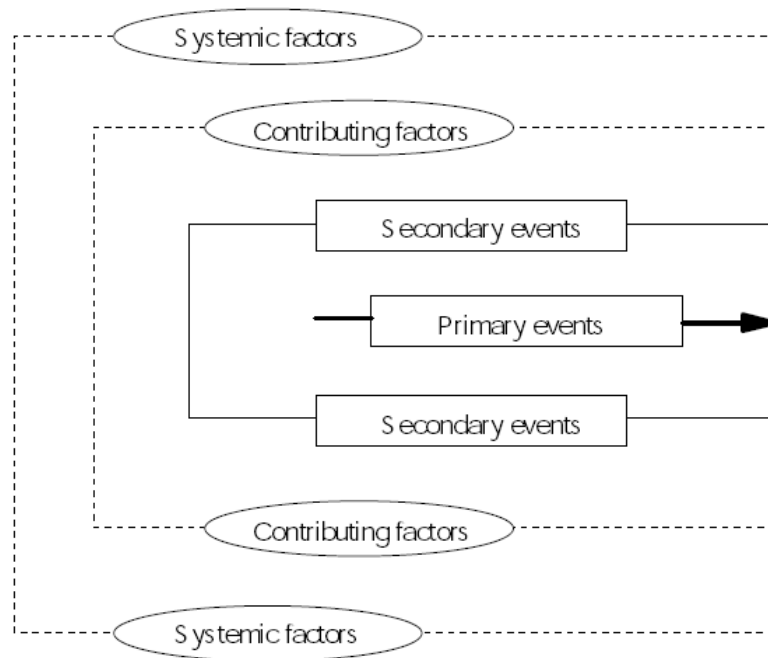


Figure 3.1.1. General Format for ECF Charts

Guidelines for practical application. The experience of many people participating in numerous accident investigations has led to the identification of seven key elements in the practical application of ECFA to achieve high quality accident investigations.

(1) Begin early. As soon as you start to accumulate factual information on events and conditions related to the accident, begin construction of a ‘working chart’ of events and causal factors. It is often helpful also to rough out a fault tree of the occurrence, to establish how the accident could have happened. This can prevent false starts and ‘wild goose chases’ but must be done with caution so that you don’t lock yourself into a preconceived model of the accident occurrence.

(2) Use the guidelines, as these will assist you in getting started and staying on track as you reconstruct the sequences of events and conditions that influenced accident causation and rectification. Remember to keep the proper perspective in applying these guidelines; they are intended to guide you in simple

application of a valuable investigative tool. They are not hard and fast rules that must be applied without question or reason. They have grown out of experience and fit well into most applications, but if you have a truly unique situation and feel that you must deviate from the guidelines for clarity and simplicity, do it. Analytical techniques should be servants, not masters.

(3) Proceed logically with available data. Events and causal factors do not usually emerge during the investigation in the sequential order in which they occurred. Initially, there will be many holes and deficiencies in the chart. Efforts to fill these holes, and to get accurate tracking of the event sequences and their derivation from contributing conditions, will lead to deeper probing by investigators, that will uncover the true facts involved. In proceeding logically, using available information to direct the search for more, it is usually easiest to use the accident or loss event as the starting point, and reconstruct the pre-accident and post-accident sequences from that vantage point.

(4) Use an easily updated format. As additional facts are discovered, and analysis of those facts identifies causal factors, the working chart will need to be updated. Unless a format is selected which displays the emerging information in an easily modified form, construction of the chart can be very repetitious and time-consuming. Successive redrafts of the ECF chart on large sheets of paper have been done; magnetic display boards or chalkboards have been used; but the technique that has consistently proved to be most effective, and most easy to update, is the use of 'post-it' notes, on which brief event or condition statements are written. A single event or condition is written on each note. The notes are then stuck onto a wall, or a large roll of heavy paper, in the sequence of events as then understood. As more information is revealed, notes can be rearranged, added, or deleted to produce a more complete and accurate version of the working chart. Once the note-based working chart has been finalised, the ECF chart can be drawn for inclusion in the investigation report. Several investigators have testified to the value of this approach, commenting that it made their investigations more expeditious and thorough. They further stated that use of post-it notes for the working chart was not only useful in establishing the accident sequence and identifying key events and conditions, but also highlighted deficiencies in knowledge, pointed out areas for further inquiry, and finally made the report writing straightforward.

(5) Correlate use of ECFA with that of other MORT investigative tools. The optimum benefit from MORT-based investigations can be derived when such powerful tools as ECFA, MORT chart based analysis, change analysis, and energy trace and barrier analysis are used to provide supportive correlation.

(6) Select the appropriate level of detail and sequence length for the ECF chart. The accident itself, and the depth of investigation specified by the investigation commissioning authority, will often suggest the amount of detail desired. These, too, may dictate whether ending the ECF chart at the accident or loss-producing event is adequate, or whether the amelioration phase should be included. The way the amelioration was conducted will also influence whether this should be included, and in how much depth it should be discussed. Certainly, if second accidents occurred during rescue attempts or emergency action, or if other specific or systemic problems were revealed, the ECFA should cover this phase. However, the investigators and the commissioning authority involved will have to decide, on a case-by-case basis, what is the appropriate depth and sequence length for each accident investigated.

(7) Make a short executive summary chart when necessary. The ECF working chart will contain much detail, so it can be of greatest value in shaping and directing the investigation. In general, significantly less detail is required in the ECF chart presented in the investigation report, because the primary purpose is to provide a concise and easy-to-follow orientation to the accident sequence for the report reader. When a detailed ECF chart is felt to be necessary to show appropriate relationships in the analysis section of an appendix of the report, an executive summary chart of only one or two pages should be prepared and included in the report to meet the above stated purpose.

Examples of an ECF chart can be found in Figures 3.1.2 and 3.1.3. These examples depict a partially completed ECF chart for an operational event in which the residual heat removal (RHR) system was overpressurised during initial pressurisation of the reactor coolant system (RCS), following a refuelling outage (NUREG/CR-5953, 1992).

Events and causal factors charting was developed to support the investigation of a single event. It can also be used to identify human performance problems. Developing ECF charts for the different errors that may represent an adverse trend, and comparing them, allows the detection of patterns and similarities in the events, and conditions associated with the different errors.

Analysis of the ECF chart begins after the investigation is completed, although the analysis itself may raise additional questions that require further investigation. The analysis is performed to identify direct, contributing and root causes for the hardware failure or human performance problem of interest. The analysis consists of first identifying the significant events in the timeline, and then evaluating them by asking a number of questions about each one.

An ECF chart often contains events that did not play a causal role in the human performance problem under investigation, but which must be included to 'tell the story,' so that others can understand what happened. These other events may be retained in the chart, but only the significant events will be analysed.

Identifying the significant events in the ECF chart starts with the event that came immediately before the hardware failure or human performance problem of interest. To determine whether this event is significant or not, the question is asked, 'If this event had not occurred, would the failure have occurred?' If the answer to this question is, 'Yes,' then the question is asked whether the event represented a normal activity with the expected outcomes. If it was a normal activity with the expected outcomes (e.g. the maintenance technician arrived at work, control rods were inserted and the reactor scrammed), then it is not a significant event in the chart. If the event had unplanned or unwanted consequences, then it is a significant event in the chart, and should be further analysed by asking the following additional questions:

- What were the other events and conditions that led to the significant event?
- What went wrong that allowed the event to occur?
- Why did those conditions exist?
- Were other significant events necessary for the failure or problem to occur, or would the recurrence of this event alone lead to another failure or problem?
- Is the significant event linked to other events or conditions that may indicate a more general or larger deficiency, such as a programmatic weakness?

For example, in Figure 3.1.2, the event in the chart that precedes the overpressurisation was the control room crew initiating system pressurisation. Starting RCS pressurisation is a significant event in this timeline, because, obviously, RCS could not have overpressurised without it, and because initiating pressurisation had unplanned and unwanted consequences.

The significant events in an ECF chart, and the events and conditions that were responsible for them, are causal factors. A brief statement that summarises the relevant characteristics of the causal factor is added to the ECF chart, above the significant event to which it applies. Figure 3.1.4 shows the ECF chart for the overpressurisation event, with one causal factor added above the conditions and event in the chart to which it applies.

When each significant event in the chart has been analysed, relationships among the causal factors may be revealed. For example, in some situations, several examples of training weaknesses may be identified, or the failure of one piece of equipment or system is found to have caused several of the events in the chart. When common causes are found, they may indicate the root cause of the problem under investigation.

The attributes of the event and causal factor charting tool are:

- the graphic display concisely captures the entire event. Better than long narrative descriptions;
- breaks down the entire case into a sequence of occurrences;
- shows exact sequence of events from start to finish in a chronological order;
- allows addition of barriers, conditions, secondary events, presumptions;
- facilitates the integration of information gathered from different sources;
- useful for both simple and complex problem solutions;

- many causal factors become evident as the chart is developed;
- presents the information in a structured manner.

Benefits. Use of the ECF charting tool by the accident investigator provides benefits in: (1) meeting the general purposes of accident investigation and conducting the investigation; (2) writing the investigation report. Specifically, ECF analysis:

- provides a cause-oriented explanation of the accident;
- provides a basis for beneficial changes to prevent future accidents and operational errors;
- helps delineate areas of responsibility;
- helps assure objectivity in the conduct of the investigation; organises quantitative data (e.g. time, velocity, temperature, etc.) Related to loss-producing events and conditions;
- acts as an operational training tool; provides an effective aid to future systems design;
- provides a check for completion of investigative logic. Even the most elementary types of sequence charting can reveal gaps in logic and help prevent inaccurate conclusions;
- provides a method for identification of matters requiring further investigation or analysis. Significant event blocks with vague or non-existent causal factors can alert the investigator to the need for additional fact-finding and analysis;
- provides a logical display of facts from which valid conclusions can be drawn;
- provides appropriate and consistent subject titles for ‘discussion of facts’ and ‘analysis’ paragraphs;
- provides a method for determining if the general investigative purposes and specific objectives have been adequately met in terms of the conclusions reached;
- provides a method for differentiation between the analysis of the facts and the resultant conclusions and evaluation of the factual basis of possible recommendations;
- presents a simple method for clearly describing accident sequences and causes to a reading audience with divergent backgrounds. Without the use of sophisticated or exotic methodology, the accident causes can be easily communicated to readers with a wide variety of experience and technical expertise;
- provides a source for the identification of organisational needs and the formulation of recommendations to meet those needs. The charting technique provides the basis for a systematic trace of the logic from a statement of the facts through the analysis, conclusions, judgments of needs, and recommendations;
- finally, the technique has been shown to be useful in solving various unanticipated problems associated with preparing the final report for specific accident investigations. The clear and logical development of the accident events and causal factors facilitates agreement among report reviewers on accident causation and minimises negative reaction from those persons and organisations whose performance deficiencies contributed to accident occurrence. They may not like what the report says, but they will agree that it is fair and accurate.

Disadvantages. While ECF can provide the timeline to help discover the action causes, it is generally inefficient and ineffective because it mixes storytelling with conditional causes, thus it produces complicated relationships rather than clarity [25].

Application. This tool is widely used for any event investigation in which a timeline or sequence of events might apply, regardless of the initiating event being equipment failure or human performance. With the aim of distilling refinements of approach that have been collected over the last decade through the experiences of the authors, and by applying criteria and methods published by others, on the basis of ECFA ‘Events and Causal Factors Analysis’, a new tool, called ECFA+, Events and Conditional Factors Analysis, was developed in 2007 [72].

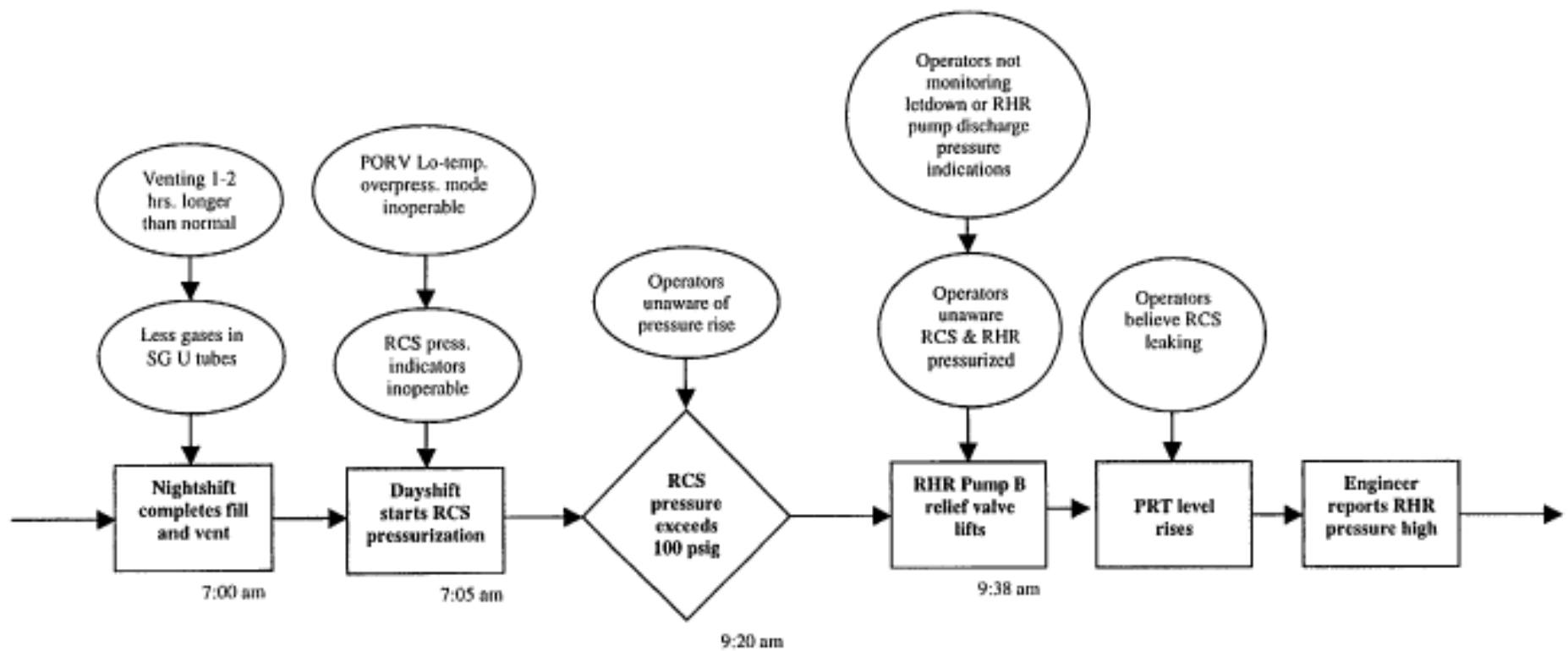


Figure 3.1.2. An example of an Events and causal factors (ECF) chart (RHR Overpressurisation Event, March, 1990) [4]. RHR - residual heat removal; RCS - reactor coolant system; SG – steam generator; PORV –pneumatically operated relief valve; PRT - pressurizer relief tank

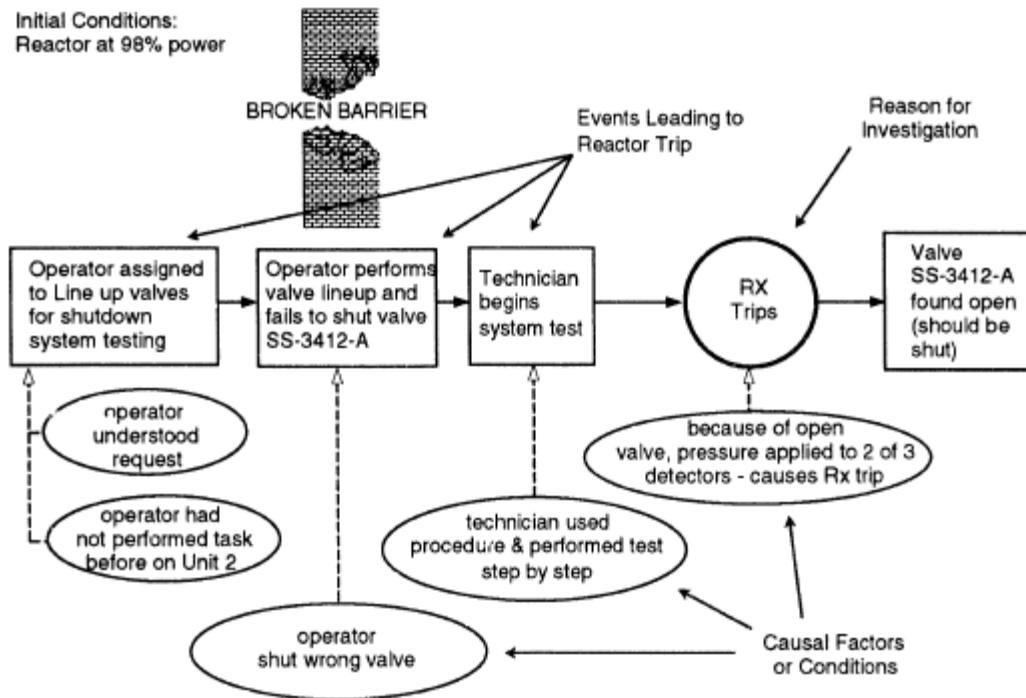


Figure 3.1.3. Example of an ECF chart for the reactor's RX trip event with broken barrier [19]

ECFA+ is a tool which produces a sequential description of an incident, which accounts for the logical relationships between the facts presented. Using witness narratives, logs and other sources of evidence, ECFA+ helps an investigator to build an account of the events that comprise an incident. Each event is stated using the present tense. These events are put into chronological order, and linked together by identifying logical relationships. These links are tested to ensure that each event is explained satisfactorily. When necessary, conditions are identified to ensure the completeness of these explanations. Every event, condition and logical relationship must be established to the standard of evidence required by the investigator. An example of an ECFA+, Events and Conditional Factors Analysis chart is shown in Figure 3.1.5 [72].

ECFA+ analysis is generally an iterative process, running in parallel with other investigative activities. New information is added to the evolving ECF chart, and this often raises new topics for further inquiries. If one were to add together the various iterations of work on an ECFA+ analysis, it would seldom take less than one hour; it would often take two hours, and sometimes more if the incident were complex. ECFA+ benefits from a team approach, and it adds to opportunity cost associated with using the tool.

The ergonomics of ECFA+ means that it is best approached as a paper and pencil method, but this assumes that there is a sufficient physical space in which to do the work: a blind wall, four metres wide, is adequate for most analyses. Experience suggests that a computer-based approach is not effective for performing ECFA+ in real time, especially when a team approach is used. If good-quality report is needed, it is normal practice to transcribe the ECFA+ chart using a flow-charting package or other vector graphics software application.

ECFA+ is generally approached as a team activity. The team needs to be selected to include the right mix of disciplines and experience relative to the incident to be investigated.

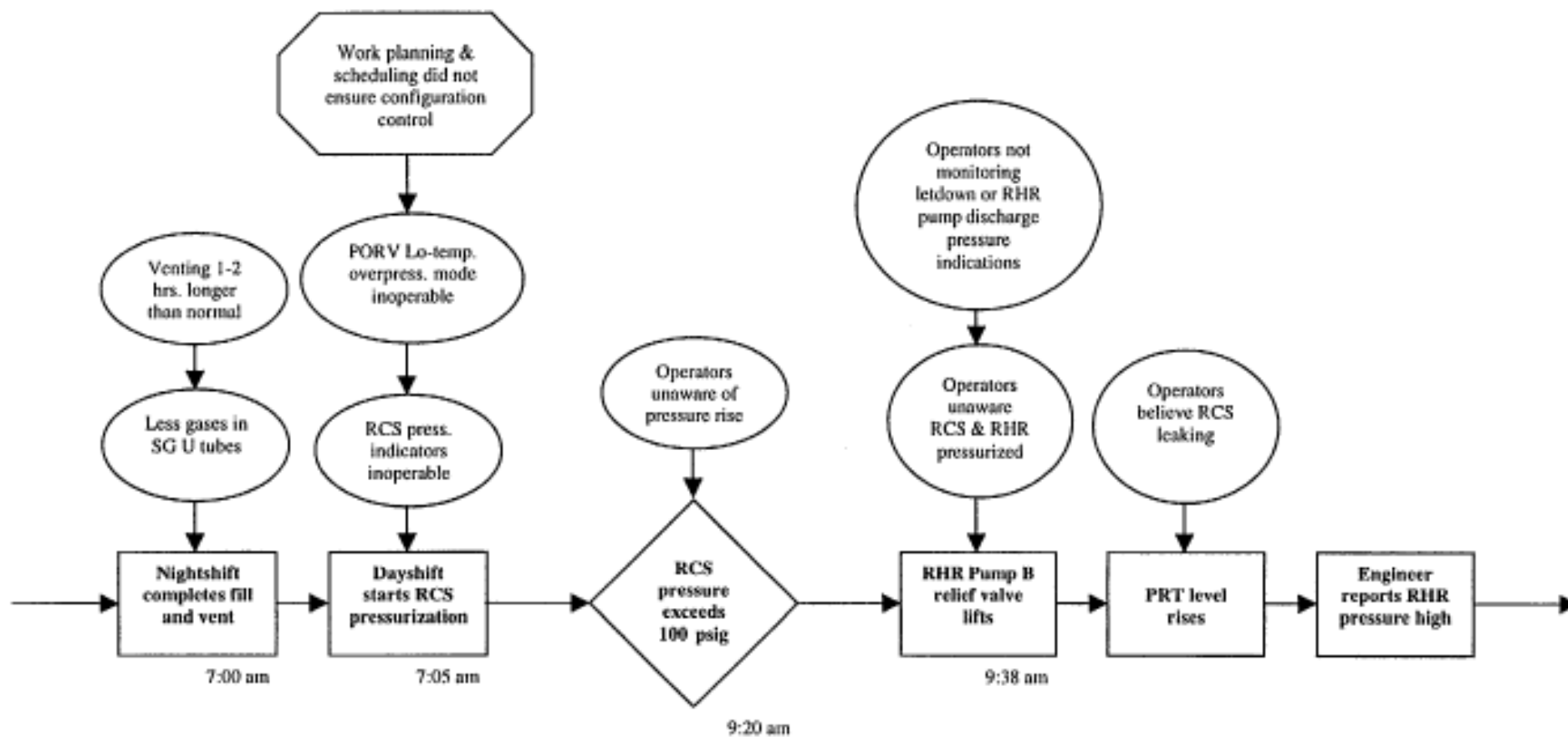


Figure 3.1.4. An example of an Events and causal factors (ECF) chart with one causal factor added (RHR Overpressurisation Event, March, 1990) [4]

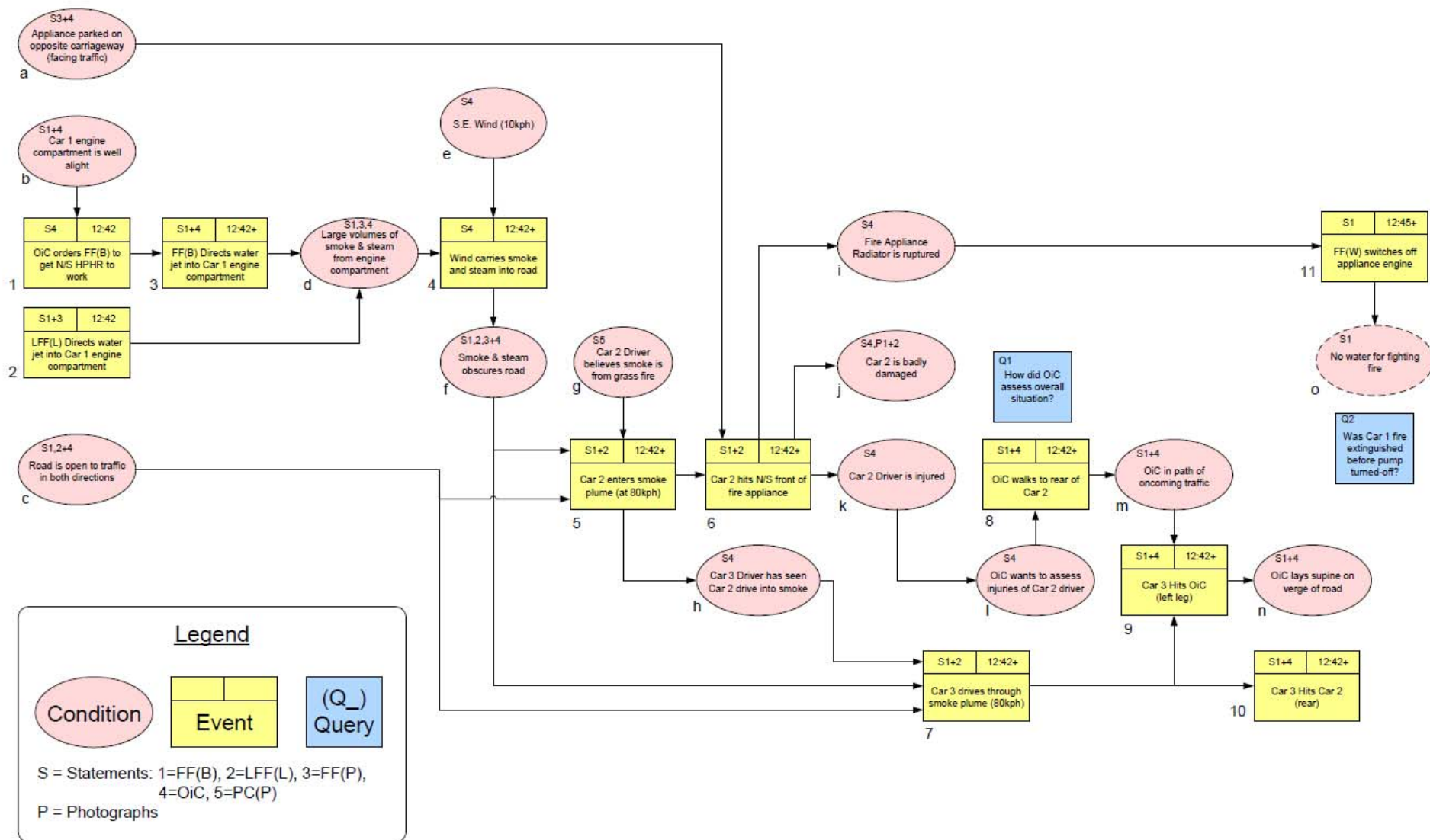


Figure 3.1.5. An example of an ECFA+, Events and Conditional Factors Analysis chart [72]

3.2. Cause and effect analysis

The purpose of this tool is to identify root causes by examining the relationship between cause and effect. It is performed by asking successively what effects have occurred and why, and proceeding from the last failure/deficiency backwards to find the cause. On the basis of information gathered the Cause & Effect Diagram (CED, also known as the Fishbone Diagram or Ishikawa Diagram) is created (Figure 3.2.1). It is a technique to identify graphically and organise many possible causes of a problem (effect). Professor Kaoru Ishikawa developed this tool in 1943 to explain to a group of engineers at Kawasaki Steel Works how various manufacturing factors could be sorted and interrelated. The original intent of the CED was to solve quality-related problems in products caused by statistical variation, but it was quickly realised that it could be used for solving other types of problems as well. The tool later came into widespread use for quality control throughout Japanese industry (Ishikawa 1982) and spread to other countries [1, 2, 6, 7, 9, 13, 25, 27].

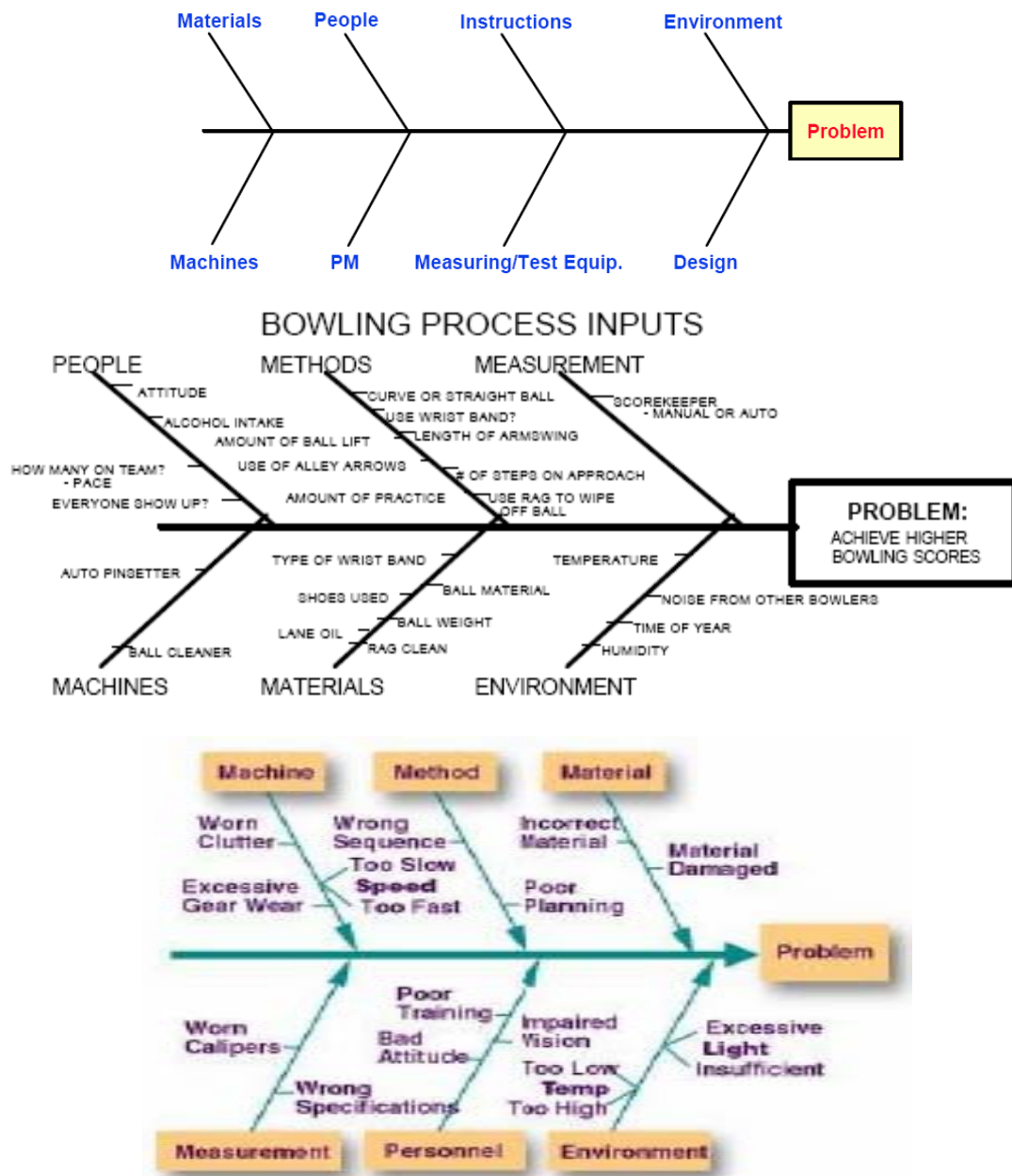


Figure 3.2.1. Examples of the Cause & Effect Diagram (Fishbone Diagram). PM – project management

The Ishikawa (Fishbone) Diagram is perhaps the oldest and most well known tool for conducting root cause analysis [20, 27, 56, 110]. In its most common form of use, the investigator attempts to define multiple possible causes for a given problem in the four areas of manpower, methods, materials, and machines (4-Ms). Other commonly used categories (Fish Bones) are: Place, Procedure, People and Policies (4-Ps) and Surroundings, Suppliers, Systems and Skills (4-Ss). The '5 Why' technique is often used with this tool to construct the bones of the chart, with the answer to each why resulting in a new branch being created off of the previous one, that the question originated from. It is currently one of seven basic quality control tools, and is commonly used to determine components needed for a desired outcome. The most important attributes of the Ishikawa (Fishbone) Diagram are:

1. does not use cause-and-effect;
2. modes are not dependent upon each other;
3. uses brainstorming primarily;
4. allows use of opinion as fact;
5. promotes belief that all causes are within categories used.

Cause and effect analysis determines root cause depending on only two items: the definition of a root cause, and a question: 'Why did this effect or event occur?' As such, this tool is very easy to use and is only limited by the knowledge and experience levels of the user [6].

The definition of a root cause is fundamentally important to the use of this technique, because it determines the criteria to be met by any root cause developed by the technique. For example: the root cause is defined as 'The most basic reasons for the event, which if corrected will prevent recurrence'. This definition tells that a root cause must be correctable; if it is not, it may be considered a cause but not a root cause, and the correction must be within our control: it must prevent event recurrence.

Using the cause and effect technique is simply starting with the most significant event and determining the cause(s) of it. The cause(s) for this event's cause(s) are then determined, and this chain of events and causes is continued until no other causes can be determined. These causes are then verified by determining if the root cause criteria have been met. Creating the CED, the main issue is written in a box that is typically in the centre of the right edge of the page. A line called the 'spine' or 'backbone' extends to the left, starting from the edge of the main box. Branches angle off of the spine, each representing a cause or effect of the main issue. Each of these branches may contain additional branches. Example. The most significant event is a reactor trip from the reactor protection system (RPS).

Therefore, why did the reactor trip from the RPS? Answer: due to actuation of the RPS low water level switches. Why did the RPS low water level switches actuate? Answer: due to a low reactor water level. Why was there a low reactor water level? etc.

Causes are not always as straightforward as those in this example. In most cases, the causes found for each event depend on the investigator's experience and knowledge levels. Therefore, when using this tool for determining root cause, it is strongly suggested that an expert team perform analysis. This broadens the experience and knowledge used in conducting the investigation and determination of root causes.

As the causes are being determined for each event, it is also suggested that corrective actions or solutions be prescribed for each cause. This gives the investigative team a benchmark for determining when the root cause has been reached. When a reasonable solution, which can be controlled or implemented by management, is reached, then the associated cause may be called a valid root cause.

The primary drawback to this technique is the implied suggestion that only one solution can correct a root cause. It also lays a significant burden on the investigative team, in that a 'reasonable' solution determined by them may not be an 'acceptable' solution for management to implement. In addition, extreme care needs to be taken to prevent 'short cuts' or predetermined assumptions from occurring when performing this technique. As can be seen in the example, each event must be listed as a single item, and only provable facts or qualified judgments are used for the associated causes.

An addendum to this technique strongly suggests that the investigative team provide at least two causes for each event/effect. This requirement ensures that all possible causes are considered for single event, and that no root causes are overlooked.

The attributes of the cause and effect analysis are:

- successively asks and answers the why question;
- stops at the farthest cause that can be corrected within the operating organisation;
- arrives at the underlying cause of an event in a very direct manner;
- similar to a fault tree analysis, but shows only the actual failed branches.

Advantages. This tool is better than nothing, and serves as a useful instrument for getting individual opinions onto a sheet of paper or screen [27, 110] so that everyone involved can talk about them and suggest additional possible causes.

Disadvantages. Cause and effect analysis is an opinion-based tool, and its design limits the user's ability to visually define multiple levels of 'why' answers, unless the paper that is being used is really large. Worse still, opinion (voting of some form) is normally used to select the most likely causes from those listed on the diagram. Teams are then encouraged to test different countermeasures for the selected causes to see if the problem goes away, which can be both time consuming and costly. Also, the tool does not focus on finding and eliminating generic causes.

Application. A cause and effect analysis is often used in addressing events initiated by both human performance and equipment failures. However, most root causes initiated by equipment failure usually require a more detailed variant of a cause and effect analysis, known as fault tree analysis (see cl. 3.7). For most events initiated by human performance issues, it is usually easier to use this tool later in the event investigation. Because of its logic and relationship aspects, a cause and effect analysis does not lend itself to use as one of the primary investigation tools for human performance issues. Such issues often have multiple influences on the event, and often cannot be clearly specified until late in the investigation.

3.3. Interviewing

Interviewing is a face-to-face communication between event investigator and witnesses, and questioning to obtain enhanced insight into facts. It is one of the key ways to find out what happened and provide context to the facts. In order to obtain accurate and factual information from the interviewees it is necessary to consider their sensibilities. The interviewer therefore requires special training. The initial questions are prepared in advance. Many questions are derived from other RCA tools (such as task analysis, change analysis, etc). The attributes of the interviewing are:

- interviewing is an important (sometimes most essential) tool for data gathering and is used practically for all investigations;
- focused on fact-finding, not fault-finding;
- need a non-blame environment;
- requires a degree of skill on the part of interviewer;
- is done as soon as possible: facts become less clear, memory is lost and opinions become established as time passes;
- some direct witnesses not always available: may have been injured; you will have to select others.

Due to the importance and nature of event investigations, interviews must be conducted in a professional manner. Interviewers must be capable of extracting factual information from interviewees, who may feel threatened, be hostile or emotional, or have trouble recalling the information in an unbiased way or expressing themselves clearly. For all of these reasons, interviewers must acquire a level of expertise in the various interviewing techniques through comprehensive training [1].

There are two main types of an interview: investigative and cognitive [44]. An investigative interview is designed to help interviewees retrieve from memory the events associated with a safety incident. A cognitive interview uses an interviewing technique based on psychological theory and research for examining the retrieval of information from memory.

The interview style recommended for Root Cause Analysis (RCA) investigations is a modified approach of the formal cognitive interview [44]. It involves actively listening to someone who recalls their first-

hand account of an event they have either witnessed, or been involved in, as soon as possible after it has happened.

Preparation

Listening to the first-hand accounts from those involved in an incident as soon as possible after it has happened will help the investigation team start to build a picture of what happened, and potentially highlight what other information will be required. The optimum time for holding an interview is between two and seventy-two hours after the incident. The interviewer needs to establish who they want to interview and make arrangements to do so as soon as possible. The identified staff should be invited to attend, and told the purpose of the interview, what to expect, and what preparation they need to do. It is essential that the interviewer and the room are prepared prior to the interview.

Inviting the member of staff to attend for an interview

Where appropriate, a written invitation to the interview can be provided and the details below included. Where this is not practical, due to the need to see staff as soon as possible after the incident, staff should be advised in advance, and be given the following information verbally:

- the purpose of the interview and details of the incident being investigated;
- the time, place and estimated length of the interview;
- who will be conducting the interview and their role;
- how the cognitive interview will be conducted and the first-hand account recorded (e.g. the interview will be informal, notes will be taken to inform the investigation, but these will not act as a formal witness statement and do not need the interviewee's signature);
- what documentary evidence will be available to them during the interview;
- the fact that they can bring a friend or colleague for support (explanations need to be given regarding the role of this friend/colleague, e.g. confidentiality, their involvement);
- advice on what will happen after the interview.

Interviewer preparation

- The interview should take place in a quiet, relaxed setting and, if possible, away from the interviewee's usual place of work, and not at the scene of the incident.
- The room should be set out informally, with refreshments available, and steps taken to ensure, where possible, that no interruptions occur (e.g. telephones, bleeps).
- Where possible, the interviewee should have the opportunity to attend the interview in work time, and arrangements may need to be made with their line manager to ensure this.
- Depending on the nature of the case, or the interviewee's personal involvement, they may find the process of recounting the events either upsetting or disturbing. The interviewer will need to have information available on staff support/counselling.
- The interviewer should ensure they have all the relevant documentation available at the interview. It is important to remember in the cognitive interview to only interview one staff member at a time.

Additional tips for preparation of the interview:

- schedule the appointments properly;
- choose an appropriate location;
- make sure you are interviewing the right people;
- have question areas or themes prepared in advance;
- have required reference documents to hand;
- be mentally prepared and focussed.

Conducting the interview

Introductions (where appropriate) should be made of those present in the room. Include details on roles and an explanation of the sequence of the interview and approximate length. The RCA process should be explained and an estimate given of how long it will take to complete. Recommendations concerning introduction:

- introduce yourself
- explain the purpose of the interview
- do not be confrontational
- control your body language.

It is important to emphasise that this is not part of a disciplinary process. The interviewer should explain that notes will be taken throughout, for the purpose of informing the investigation. It must be stressed that these notes will not act as a formal witness statement, and therefore do not need the interviewee's signature. If, following the interview, the interviewer feels that the individual staff member should write a formal statement, guidance and support should be given by a union representative or trust solicitor as applicable.

The interviewee should be asked to confirm that they have understood all of the above, and should be reminded that they should offer only factual information, but include everything, regardless of whether or not they think it is relevant. The interviewee should be discouraged from making 'off the record' comments. The interviewee should also be advised that the first-hand account and the final report will be written with due anonymity of staff.

Recommendations for interviewer concerning asking questions:

- seek to understand why, not just what;
- control the interview;
- keep questions simple and focused;
- use a funnel approach: broad leading to specific questions;
- anticipate unsatisfactory replies: have a means to deal with them;
- avoid jargon;
- avoid devious or trick questions;
- focus on facts;
- anticipate interviewee questions;
- be aware that interviewing is not interrogating.

Listening techniques:

- listen to answer before asking next question;
- be relaxed, friendly;
- maintain eye contact;
- use a neutral body language;
- do not let note taking interfere with listening.

Recording the information:

- take brief notes while listening;
- add more detail as soon as possible, from memory;
- if you do not understand, ask for clarification
 - do not wait until next day
 - discuss with counterparts
- request copies of documents for later study;
- use of electronic recording devices should be carefully considered.

Recommendations concerning cultural differences:

- try to recognise positive and negative aspects, and take them into account during the review;
- be alert for sensitive issues: treat them with care;
- treat plant staff with respect at all times;
- reinforce understanding through confirmatory discussions;
- don't assume, ask questions.

Completion of the interview

On completion, the interviewer should ensure the interviewee feels appropriately supported and that any further support required is organised. The interviewer should reconfirm what will happen with the information gained from the interview, and how this will be used in the RCA process.

3.4. Task analysis

Task analysis (TA) is a way of structuring procedures, actions and contextual information regarding human behaviour in a certain working environment. TA could be defined as the study of what a user is required to do in terms of actions and/or cognitive processes to achieve a certain task. The task analysis tool was first developed in the 1950s, with the aim of formally describing human behaviour by a series of simple and elementary components. It was originally applied to language learning, and was then extended to the wider context of operations and working processes. TA aims to provide a better understanding of exactly what is involved in carrying out an activity, so that a better fit between the person and the workplace (working environment) may be achieved [133].

TA involves not only collecting data about the operational procedures for performing a particular task, but in many cases the collection also of information about some properties of the tasks, such as job conditions, the required skills and knowledge, safety and environmental factors, references, equipment, job performance measures, etc.

Various techniques could be used to collect data when performing a task analysis. The selection of the method depends on the nature or characteristics of the task under consideration. The following major types of tasks have been identified:

- cognitive tasks, e.g., office job, control room job, etc.;
- accessible or non-accessible tasks, e.g., the task is highly dangerous, the field access is forbidden to the observer, etc.;
- manual or automatic tasks, e.g., a manual maintenance action, automatic distillation process, etc.

Techniques for collecting data – which are of particular relevance to the chemical process industry – for TA these include interviews, observations, analysing existing documents, etc. A single technique would not normally give sufficient results, thus a combination of several techniques is usually applied.

According to the application or case study for which a task analysis needs to be performed, a certain approach (or approaches) of TA can be used. Among the most well known approaches are:

- Initial Task analysis (ITA): involves a basic level of task analysis to provide at least a minimum level of understanding of the task.
- Hierarchical task analysis (HTA): involves exploring tasks through a hierarchy of goals indicating what a person is expected to do and plans indicating the conditions when subordinate goals should be carried out.
- Cognitive task analysis (CTA): involves analysing the interaction of mental procedures, factual knowledge and task objectives in the process of job performance.
- Goals, Operations, Methods and Selection Analysis (GOMS): involves identifying and analysing the rules for selecting methods for organising operators to achieve goals.
- Task Analysis for Knowledge Description (TAKD): involves identifying, analysing and utilising rules for knowledge elicitation against task descriptions.

Task analysis is usually performed in two steps:

- PAPER & PENCIL to study how the task SHOULD be done by reviewing the procedures and other documents, developing questions and identifying potential problems;
- WALK-THROUGH the area of the event, to learn how the task is done by simulating the task in the real environment of the plant, observing workers and re-enacting the task, to determine how the task was actually performed, and identifying potential problems;

The purpose of these steps is to become familiar with the task and to learn the potential difficulties.

The attributes of the task analysis paper and pencil tool are:

- provides investigators with a good insight into the task;
- identifies questions to use later for interviewing;

- useful for analyst not familiar with the task;
- may not identify how the task was actually done.

The attributes of the task analysis walk-through tool are:

- re-enacts the task with the persons involved with the event;
- if not available, can perform the task with another person who normally performs the task;
- limitations may exist to accessing the area after the event;
- can note differences between actual re-enactment and procedure steps;
- very helpful in identifying contributing factors that relate to physical environment and man-machine interface.

The first part of task analysis, how the task should have been performed, can be a complex and time consuming process if this technique is used thoroughly. Normally, subject matter expertise on the team, and documents such as written procedures, make it unnecessary to do a fully detailed task analysis. Often the work order process, pre-job brief, procedure and closing activities are used to create a very brief analysis of how the task should have been performed.

The second part of task analysis, how the task was actually performed, is almost always used as an investigation tool of human performance issues involved in events. It is absolutely critical to view the event from the standpoint of the individuals involved in the event. To accomplish this goal you must be able to stand in the shoes of the individuals involved. It is almost impossible to recognise many of the human factors and environmental issues without walking through the event, and these issues typically play a significant role in events in nuclear power plants.

Application: Task analysis compares how the task should have been performed with how the task was actually performed, the output which frequently becomes an input into a change analysis or other RCA tools.

3.5. Change analysis

Changes in the work environment often result in unanticipated and unwanted consequences. Change analysis involves systematically identifying and analysing any changes that may have affected the problem under investigation [4, 8, 11]. The change analysis tool for event investigation is designed to determine what changed, compared to previously successful occasions, if the change introduced was responsible for the consequences, and what was the effect of the change on the event.

Many types of changes may lead to unwanted consequences. These could include, e.g. changes in:

- the characteristics or number of workers involved in the task;
- other work activities going on concurrently with the work activity of interest;
- equipment condition or status;
- the work location or the environmental conditions in which the work was performed;
- supervision;
- management's expectations for the work.

Change analysis provides significant clues to help pinpoint inappropriate actions that may ultimately lead to the underlying root cause. However, not all changes found during an event investigation may necessarily play a role in the event.

Change analysis is an investigation technique that involves the precise specification of a single deviation, so that changes and/or differences leading to the deviation may be found by comparison to similar situations in which no deviation occurred.

As suggested by the name of the technique, change analysis is based on the concept that change (or difference) can lead to deviations in performance. This presupposes that a suitable basis for comparison exists. What is required, then, is to fully specify both the conditions which deviated and those which did not, and then compare the two so that changes or differences can be identified. Any change identified in this process thus becomes a candidate cause of the overall deviation.

What is a suitable basis for comparison? There are basically three types of situations that can be used. First, if the deviation occurred during performance of some task or operation that has been performed

before, then this past experience can be the basis. Second, if there is some other task or operation that is similar to the deviated situation, then that can be used. Finally, a detailed model or simulation of the task (including controlled event reconstruction) can be used, if feasible.

Once a suitable basis for comparison is identified, then the deviation can be specified. Various schemes exist for performing this specification. Perhaps the most useful scheme (attributed to Kepner and Tregoe, see cl. 3.10) involves four dimensions (WHAT, WHERE, WHEN, and EXTENT) and two aspects (IS and IS NOT). This technique consists of asking the questions: What? When? Where? Who? How? Answering these questions should provide direction towards answering the root cause determination question: Why? Primary and secondary questions included within each category will provide the prompting necessary to thoroughly answer the overall question. Some of the questions will not be applicable to any given condition. Some amount of redundancy exists in the questions, to ensure that all items are addressed.

Regardless of the scheme used, the end result should be a list of characteristics that fully describe the deviated condition. Given the full specification of the deviated condition, it becomes possible to perform a detailed comparison with the selected condition which did not deviate. Each difference between the deviated situations and those which did not deviate is marked for further investigation. In essence, each individual difference (or some combination of differences) is a potential cause of the overall deviation. After the potential causes are found, each is reviewed to determine if it could reasonably lead to the deviation, and under what circumstances. The most likely causes are those that require the fewest additional conditions or assumptions. In this way, a large list of potential causes can be whittled down to a short list of likely causes. Finally, given the likely causes, the actual or true cause(s) must be identified. Generally speaking, the only way to verify which likely cause is the true cause is by testing.

The purpose of change analysis is thus to discover likely causes of a deviation through comparison with a non-deviated condition, and then to verify true causes by testing. True causes found using change analysis are usually direct causes of a single deviation; change analysis will not usually yield root causes. However, change analysis may at times be the only method that can find important, direct causes that are obscure or hidden. Success in change analysis depends ultimately on the precision used to specify a deviation, and in verification of true cause through testing.

Change analysis for human performance problems is most effective when the same work activity has been performed successfully in the past, when the work activity and conditions under which it was performed were documented or can be reconstructed, and when procedures for performing the work are available. Change analysis can also be performed by comparing the work activity under investigation to how the work activity is successfully performed at other sites, or to 'ideal' situations as documented in standards and regulations.

Figure 3.5.1 shows the six main steps involved in Change Analysis. Figure 3.5.2 is the Change Analysis worksheet. The first step of a change analysis is to define the 'event-free situation' and compare it to the situation in which the 'event' under investigation occurred. The 'event' may be any hardware failure, human error or human performance problem. The 'event-free' situation is a comparable situation in which the hardware did not fail or the work activity was performed successfully.

Once the 'event' and 'event-free' situations have been identified, they are analysed to determine the specific differences between them. The impact of each difference on the event is then evaluated to determine whether the change was unimportant or was a direct, contributing, root and/or programmatic cause of the problem. Key elements of the Change Analysis procedure include the following:

- Consider the event containing the undesirable consequences.
- Consider a comparable activity that did not have the undesirable consequences.
- Compare the condition containing the undesirable consequences with the reference activity.
- Set down all known differences, whether they appear to be relevant or not.
- Analyse the differences for their effects in producing the undesirable consequences. This must be done with careful attention to detail, ensuring that obscure and indirect relationships are

identified (e.g. a change in colour or finish may change the heat transfer parameters and consequently affect system temperature).

- Integrate information into the investigative process relevant to the causes of, or the contributors to, the undesirable consequences.

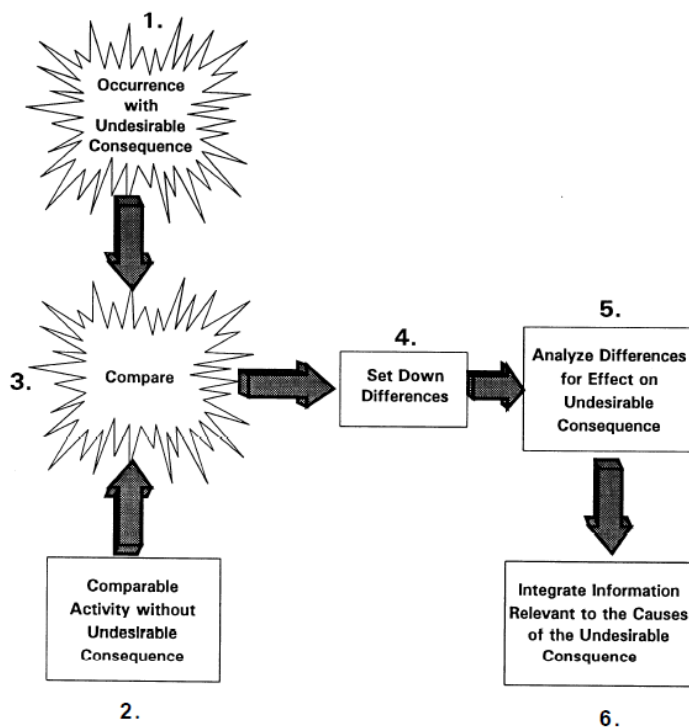


Figure 3.5.1. Six Steps Involved in Change Analysis [11]

Change Analysis Work Sheet

Change Factor	Difference/Change	Effect	Questions to Answer
What (Conditions, occurrence, activity, equipment)			
When (Occurred, identified, plant status, schedule)			
Where (Physical location, environmental conditions)			
How (Work practice, omission, extraneous action, out of sequence procedure)			
Who (Personnel involved, training, qualification, supervision)			

Figure 3.5.2. Change Analysis Worksheet

Figure 3.5.3 illustrates an example of a change analysis worksheet for the RHR overpressurisation event analysed in the chapter 3.2. The human error of interest is the operators' failure to detect and control the rapid rise in RCS pressure. As can be seen in Figure 3.5.3, four changes from previous occasions on which RCS pressurisation activities were performed successfully were identified.

Evaluating the causal roles of these changes involves asking, for each change, whether or not it meets the definition of a direct, contributing, root and/or programmatic cause, or did not play a causal role in the error. In this example, the inoperability of the RCS pressure transmitters was the direct cause of the error, because it was 'the action or condition immediately preceding the error in the event sequence that caused or allowed the error to occur.' If the RCS pressure transmitters were operable, the operators would have detected the rapid pressure increase in time to control it and prevent the transient. Evaluation of the roles of the other four changes, based on the evidence available, indicates that they were contributing causes. That is, each of the changes, alone, did not cause the error, but rather set the stage for it. It was the combination of these additional changes with the inoperability of the RCS pressure indications that allowed the event to occur.

Change Analysis is a good technique to use whenever the causes of the condition are obscure, you do not know where to start, or you suspect a change may have contributed to the condition. Not recognising the compounding of change (e.g. a change made five years previously combined with a change made recently) is a potential shortcoming of Change Analysis. Not recognising the introduction of gradual change, as compared with immediate change, is also possible. This technique may be adequate to determine the root cause of a relatively simple condition. In general, though, it is not thorough enough to determine all the causes of more complex conditions.

Event Situation	Event-Free Situation	Difference	Effect on Event
RCS pressure instrument transmitters isolated for maintenance	RCS pressure indicators operable	No accurate indications of RCS pressure were available	Operators were unable to monitor RCS pressure
Fill and venting of reactor head extended	Fill and vent evolution completed within normal time limits	Venting continued 1-2 hours longer than normally	The longer vent and fill evolution decreased the volume of gases in the steam generator (SG) U tubes
Reduced volume of gases in SG U tubes caused by longer vent time	Greater volume of gases in SG U tubes	Reduced amount of non-condensable gases caused RCS pressure to increase sooner than in previous refill operations	RCS pressure rose sooner than expected and approached 100 psig within 2.5 hours of initiating pressurization
Operators were monitoring the inoperable RCS pressure gauges, but not all available pressure indications (e.g., letdown and RHR discharge pump pressure gauges)	Operators monitored all available pressure indications	Operators did not detect indications of the rapid pressure increases on the letdown and RHR discharge pump pressure gauges	An opportunity to detect the pressure rise and prevent the overpressurization was missed

Figure 3.5.3. Example of Change Analysis Worksheet for an RCS Overpressurisation Event [11]

The attributes of the change analysis tool are:

- useful if you suspect some change has contributed to the event;
- does not lead directly to the root cause;
- it is a tool frequently used for quality audits;
- need follow-up with other methodologies.

Application: This tool of RCA analysis is used for almost all event investigations. In most cases, either the tasks or elements of the task will have been completed successfully before. Therefore, for most events, for failure to occur something must have changed. Change analysis is a technique used early in the investigation that provides input into the more thorough investigation tools.

Advantages. It is always useful to compare what should have happened with what did happen when analysing a problem. Change analysis is a conceptually simple, easy to grasp technique. This tool works well in combination with other methods. It is a very good tool to help determine specific causes or causal elements, and translate results naturally into corrective actions or recommendations. It can be used to find causes that are obscure, or that defy discovery using other methods.

Disadvantages. Change analysis effort alone will not lead the investigator to the root causes of, and corrective actions for, preventing the problem in the future. Application of tool requires some well defined basis for comparison. It does not provide a clear understanding of the causal relationships of a given event. Unfortunately, many people who use this tool simply ask why the change occurred and fail to complete a comprehensive analysis of the causal relationships [25]. Change analysis is intensive and requires exhaustive characterisation of deviation. It is applicable only for a single, specific deviation; it provides only direct causes for a deviation. Results may not be conclusive; testing is usually required.

3.6. Barrier analysis

The purpose of this tool is to identify the defence-in-depth failures, barriers that failed or the missing barriers. The barrier analysis technique can also be used to identify causes for human performance problems. In particular, it helps to determine what barriers should have been in place to prevent the undesirable outcome, which barriers were missing, failed, bypassed or circumvented, and what threat has, or has not, been prevented by a barrier (target-threat), and their causal roles. Barrier analysis also shows the barriers that succeeded, and prevented the problem from having more serious consequences [4, 8, 11, 20, 25].

Barrier analysis is based on the concept that hazards represent potentially harmful energy flows or environmental conditions, from which targets (i.e. personnel and equipment) must be protected. Hazards to personnel may include, for example, radiation, electrical energy, chemical and biological agents or adverse environmental conditions. Hazards to equipment may include human error, damage from wear and tear or natural phenomena.

Barrier analysis is an investigation tool that involves the tracing of pathways by which a target is adversely affected by a hazard, including the identification of any failed or missing countermeasures that could or should have prevented the undesired effect(s).

At the heart of barrier analysis is the concept of the target. The primary quality of a target is that it exists under a specified range or set of conditions, and that we require it to be maintained within that specified range or set of conditions. This very general quality means that almost anything can be a target -- a person, a piece of equipment, a collection of data, etc. Given the concept of the target, we then move to the means by which a target is adversely affected. By adverse effect, we mean that the target is somehow moved outside of its required range or set of conditions. Anything that does this is called a hazard. This is a very general quality -- almost anything can be a hazard. However, it is possible to uniquely define hazard/target pairs by the pathways through which hazards affects targets.

Having identified hazards, targets, and the pathways through which hazards affect targets, we arrive at the concepts of barriers and controls. A barrier is any means used to protect targets from hazards. There are two basic types: physical and management barriers (see Figure 3.6.1). Examples of typical physical barriers used in industrial settings to protect personnel are fences, guardrails around moving equipment, protective clothing and safety devices. Management barriers used to protect equipment in nuclear licensee facilities include preventative and corrective maintenance as well as supervision, training, the design of the human-system interface or procedures to reduce the likelihood of damage from human error. The barriers that could or should have been in place, and how they should have functioned, can be identified from subject matter expertise, knowledge of industry good practices, licensee policies and procedures, design basis documents and regulations.

Barriers are used to protect and/or maintain a target within its specified range or set of conditions, despite the presence of hazards. The primary quality of a barrier or control is that it cuts off a pathway by which a hazard can affect a target. Barriers and controls are often designed into systems, or planned into activities, to protect people, equipment, information, etc. The problem is that design and planning

are rarely perfect. Not all hazards may be identified beforehand, or unrecognised pathways to targets may surface. In both of these cases, appropriate barriers and controls may not be present. Even if they are present, they may not be as effective as originally intended. As a result, targets may lack adequate protection from change or damage. The purpose of barrier analysis is thus to identify pathways that were left unprotected, or barriers and controls that were present but not effective. All pathways relate to specific hazard/target pairs, and all barriers and controls relate to specific pathways. Success in barrier analysis depends on the complete and thorough identification of all pathways.

A barrier analysis is performed in five steps. The first step is to identify the hazard and target. The second step is to identify all of the barriers that could have protected the target from the hazard. The third step is to evaluate how each barrier performed. That is, did the barrier succeed or fail? For barriers that failed, the fourth step is to determine why they failed. Finally, the causal role of each barrier is evaluated to determine whether it was a direct, contributing, root and/or programmatic cause.

This technique is particularly useful in providing the basis for developing corrective actions to prevent the same or a similar problem from happening again. Corrective actions can strengthen existing barriers that failed or erect barriers where they are missing. Two examples of barrier analysis procedure are provided in figs. 3.6.1 and 3.6.2.

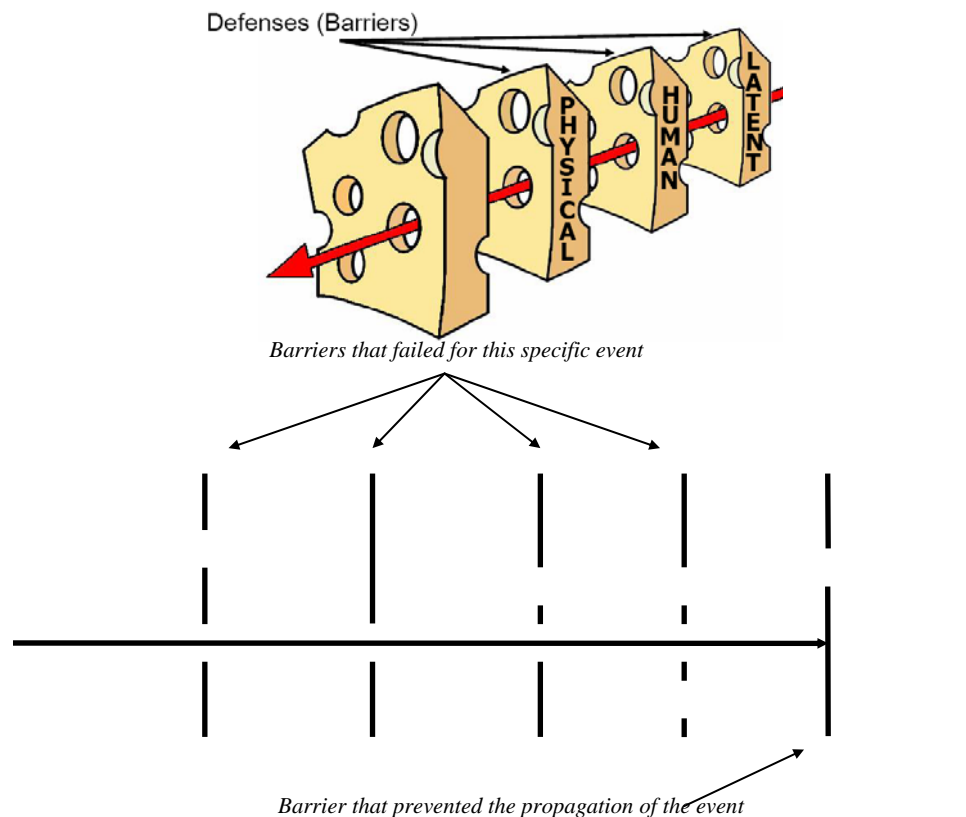


Figure 3.6.1. Illustrations of Reason's 'Swiss cheese' model [110] and defence-in-depth principle using several defence layers (barriers)

As can be seen from the example (Figure 3.6.2), analysis is an effective method to begin identifying programmatic causes as well as potential corrective actions. For example, had the RCS pressure indicators been labelled out-of-service, it is unlikely that the operators would have started RCS pressurisation activities until these indications were available. The station's policy of excluding control room instrumentation from the labelling programme indicates that the scope of the labelling programme may have been a programmatic weakness that, if corrected, could have prevented this event and other, similar events. However, responsibility for configuration control lies with the work management programme. Had the work planners (or an independent review) recognised that the RCS indicators were

not available for initial RCS pressurisation and ensured that they were, the rate of the pressure rise and the operators' focus on the three RCS indicators would not have mattered, because accurate pressure indications would have been available to detect and control pressure. Therefore, the start up procedure and the operators' status monitoring were contributing causes to the event, but not root causes. Further investigation of the work management programme would be necessary to identify the specific weaknesses that allowed this event to occur, as well as the corrective actions necessary to strengthen the programme. However, flaws in the work management programme appear to have been the root cause of the operators' error in this event.

Figure 3.6.3 shows an example of a barrier analysis worksheet for the RCS overpressurisation event which was analysed in chapter 3.2. In this example, the hazard would be pressure and the target would be the catastrophic failure of the reactor coolant or residual heat removal system piping.

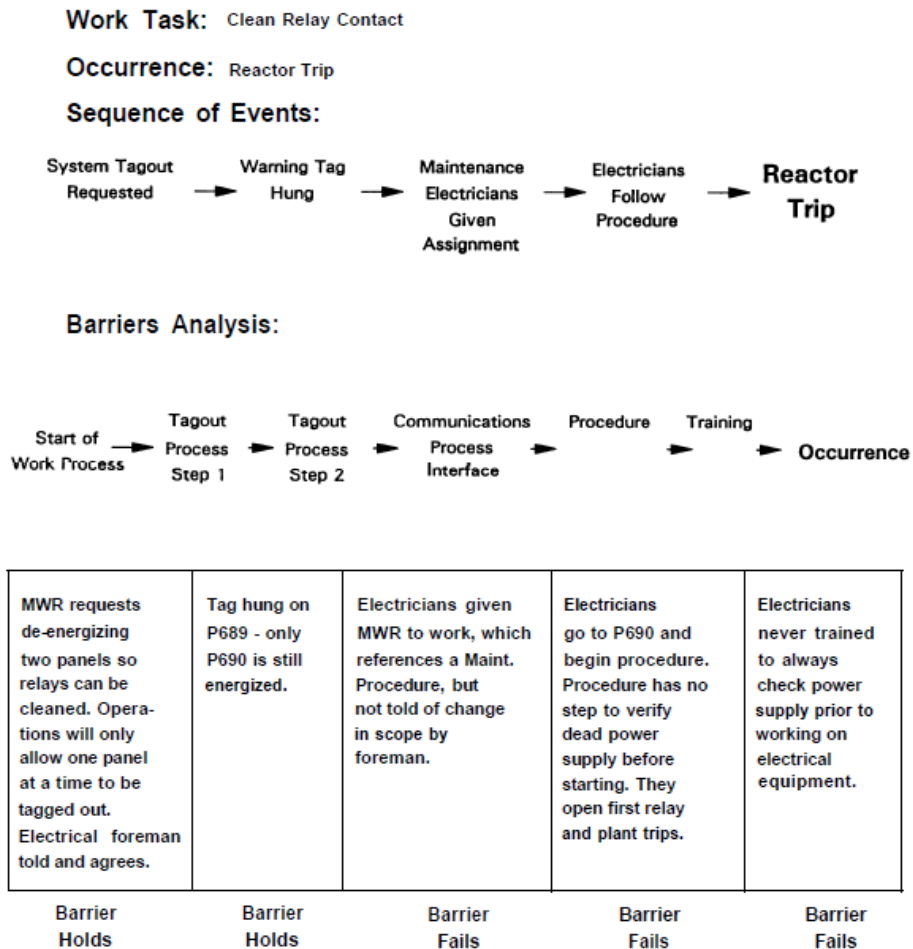


Figure 3.6.2. Example of a barrier analysis for reactor trip event due to panel de-energising by electricians [11]. MWR – maintenance work request

Evaluating the causal role of each failed barrier involves asking whether or not it meets the definition of a direct, contributing or root cause, or whether it did not play a causal role in the error. In this example, the inoperability of the RCS pressure transmitters again meets the criterion for the direct cause of the error, because it was ‘the action or condition immediately preceding the error in the event sequence that caused or allowed the error to occur.’ Further, if the RCS pressure transmitters were operable, two additional physical barriers would not have failed: the power-operated relief valves (PORVs) low-temperature overpressure protection and the computer alarm. Because the failure of these barriers was

dependent upon the RCS pressure transmitters being inoperable, they are contributing causes of this event.

Hazard: Pressure		Target: Catastrophic failure of system piping	
Physical Barriers	Performance	Why Did it Fail?	Effect on Event
RCS pressure instrument transmitters	Failed	Out of service for maintenance	RCS pressure indicators inoperable so operators could not detect rapid pressure rise
Power-operated relief valves (PORVs) low-temperature overpressure protection	Failed	The two wide-range RCS pressure instruments were the sensors for the PORV low-temperature over-pressure protection mode	PORV low-temperature over-pressure protection unavailable
RHR Pump B suction relief valve	Succeeded in stopping uncontrolled pressure rise		Maintained pressure below limits – prevented catastrophic failure of RHR piping
Pressurizer relief tank (PRT) level indication	PRT level increased when RHR suction relief valve opened		Succeeded in alerting operators to problem situation
Annunciators	Missing	RHR pressure did not reach alarm actuation setpoint and computer alarm came off the inoperable pressure transmitters	No audible indications of pressure rise
Management Barriers	Performance	Why Did it Fail?	Effect on Event
Startup procedures	Did not control RCS vent evolution	Fill and vent procedure did not specify a time limit for venting gases from reactor head	Night shift extended the RCS vent evolution 1-2 hours longer than normal, reducing the volume of gases remaining in the SG U tubes
Work management (planning and scheduling)	Failed	Work planners overlooked the need for the RCS pressure instruments to be operable before initial pressurization of the RCS	Pressurization was initiated without RCS pressure indications operable
Independent review	Missing	Not performed or required	Failed to identify the RCS pressure instrument isolation
Tagging out-of-service control room instruments	Missing	Tagging of out-of-service instruments in control room not required by tagout program	There was no visual cue that the three RCS pressure indicators were inoperable
Systems monitoring	Inadequate	Operators were focused on the RCS pressure indicators and were not monitoring all pressure indications available	Operators did not notice other indications of the pressure rise that indicated RHR, CVCS and RCS were pressurized

Figure 3.6.3. Example of Barrier Analysis Worksheet for Overpressurisation Event [11]

The attributes of the barrier analysis tool are:

- useful to evaluate defence-in-depth;
- need technically experienced people in the area being analysed;
- best used in conjunction with other tools.

Application: Barrier analysis is almost always used in event investigations. In most nuclear power plants, significant barriers have been installed to protect the plant and their employees. Barrier analysis

is a tool to help determine whether barriers failed, were circumvented, or should have been put in place but were not present.

Advantages. Barrier Analysis is a conceptually simple and easy to grasp tool, excellent for determining where to start root cause analysis. It is easy to use and apply, requires minimal resources, and works well in combination with other methods. It is then a straightforward process to translate results into corrective action recommendations.

Disadvantages. Barrier Analysis is not a perfect tool for finding effective solutions because it does not identify why a specific barrier failed or was missing. This is beyond the scope of the analysis. To determine root causes, the findings of the barrier analysis must be fed into another process to discover why the barrier failed [25]. Sometimes barrier analysis promotes linear thinking and is shown to be subjective in nature. Sometimes it can confuse causes and countermeasures. Reproducibility of results can be low for cases that are not obvious or simple.

The questions listed below are designed to assist in determining what barrier failed, thus resulting in the occurrence [11].

- What barriers existed between the second, third, etc. condition/situation and the second, third, etc. problems?
- If there were barriers, did they perform their functions? Why?
- Did the presence of any barriers mitigate or increase the occurrence severity? Why?
- Were any barriers not functioning as designed? Why?
- Was the barrier design adequate? Why?
- Were there any barriers in the condition/situation source(s)? Did they fail? Why?
- Were there any barriers on the affected component(s)? Did they fail? Why?
- Were the barriers adequately maintained?
- Were the barriers inspected prior to expected use?
- Why were any unwanted energies present?
- Is the affected system/component designed to withstand the condition/situation without the barriers? Why?
- What design changes could have prevented the unwanted flow of energy? Why?
- What operating changes could have prevented the unwanted flow of energy? Why?
- What maintenance changes could have prevented the unwanted flow of energy? Why?
- Could the unwanted energy have been deflected or evaded? Why?
- What other controls are the barriers subject to? Why?
- Was this event foreseen by the designers, operators, maintainers, anyone?
- Would it have been possible to have foreseen the occurrence? Why?
- Would it have been practical to have taken further steps to have reduced the risk of the occurrence?
- Can this reasoning be extended to other similar systems/components?
- Were adequate human factors considered in the design of the equipment?
- What additional human factors could be added? Should be added?
- Is the system/component user friendly?
- Is the system/component adequately labelled for ease of operation?
- Is there sufficient technical information for operating the component properly? How do you know?
- Is there sufficient technical information for maintaining the component properly? How do you know?
- Did the environment mitigate or increase the severity of the occurrence? Why?
- What changes were made to the system/component immediately after the occurrence?
- What changes are planned to be made? Which might be made?
- Have these changes been properly, adequately analysed for effect?
- What related changes to operations and maintenance have to be made now?
- Are expected changes cost effective? Why? How do you know?
- What would you have done differently to have prevented the occurrence, disregarding all economic considerations (as regards operation, maintenance, and design)?
- What would you have done differently to have prevented the occurrence, considering all economic concerns (as regards operation, maintenance and design)?

3.7. Fault tree analysis

The concept of fault tree analysis (FTA) was originated by 'Bell Telephone Laboratories' in 1962, as a technique with which to perform a safety evaluation of the Minutemen Intercontinental Ballistic Missile Launch Control System [45].

Fault tree analysis presents a top-down graphical representation of the possible explanations of a failure, and creates fault tree - an analytic diagram based on Boolean algebra. A fault tree is a logical diagram which shows the relation between system failure, i.e. a specific undesirable event in the system, and failures of the components of the system. It is a technique based on deductive logic. An undesirable event is first defined, and causal relationships of the failures leading to that event are then identified. Fault tree can be used in qualitative or quantitative risk analysis. The difference between these is that the qualitative fault tree is looser in structure and does not require use of the same rigorous logic as the formal fault tree.

This fault tree is designed to list all possible failure mechanisms and uses scientific research to verify or refute the possible causes until the true initiating mechanism can be determined. A fault tree analysis is recommended for equipment initiated events. It is implemented by reasoning from the general to the specific. There is no need to follow a chronological pattern. It helps to determine possible failure modes for the event to occur, which of these factors may have failed and what can be added or modified to reduce the probability of occurrence. It also provides a graphic display of the event rationale by using logic symbols (such as and/or) to chain the actions (Figure 3.7.1).

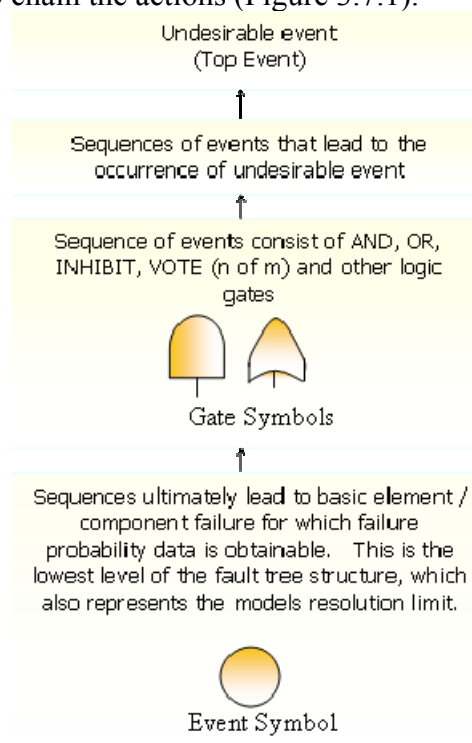


Figure 3.7.1. Simplified structure of a fault tree

Fault tree modelling is a structured technique that breaks down a complex problem into its simpler elements. An undesired system failure, such as a safety system failure, is selected for the top event [46]. The top event is related to more basic failure events by logic gates and/or more basic events. The process is continued, until the events can no longer be expanded. An example of a fault tree with top event 'Fire breaks out' is shown on Figure 3.7.2. Failure probabilities are assigned at the simplest elements of the model, and the model will compute the system level failure probabilities based on the interrelationship as constructed by the logic gates. The basic advantage of fault tree modelling versus

other modelling techniques like FMEA (Failure Mode and Effects Analysis) is that the analysis is focused on identification of causes that lead to a specific undesirable top event.

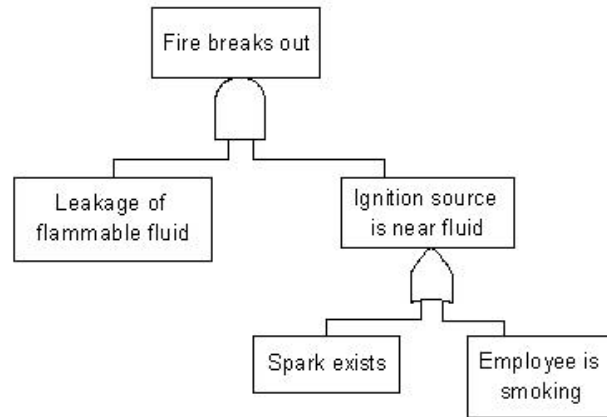


Figure 3.7.2. A fault tree with top event 'Fire'

Fault tree analysis results include top event failure probability and associated uncertainty, minimal cut sets, and importance analysis. Top event failure probability is further utilised in the overall risk assessment as an input to the event tree analysis. Minimal cut sets contain all the unique combinations of events that lead to occurrence of the top event. This result is utilised in identification of system weaknesses, and possible elimination of high probability combinations. Importance analyses are algorithms that prioritise single rudimentary events with respect to their impact on the top event, or system failure. These results are used to formulate recommendations for improvements and/or corrective actions.

If identified weaknesses or risks cannot be corrected by way of redesign (a redesign is either not feasible or not possible), the developed fault tree and event tree models should be used to assess the potential risk and consequences and to mitigate risk.

The attributes of the fault tree analysis tool are:

- top event is assumed as the major event;
- graphic tree shape representation provides a structured vision of the event;
- similar in approach to E&CF charting and to cause and effect analysis but with all branches;
- generally used to provide a graphic representation to a complex problem with many possible scenarios;
- good to conduct risk studies and improve/modify systems.

Among other fault tree analysis features, it should be mentioned that fault trees encourage the user to ask the 5 Why's multiple times for a given type of problem, and to evaluate several possible problem causes on one diagram (similar to the manpower, methods, materials, and machines boxes on a Fishbone Diagram). Like the other common root cause analysis approaches, fault trees tend to be a predominantly opinion-based tool, in that there are no predetermined questions that are used to help you to create the branches of a given tree.

Advantages. Fault trees may be preferred to Fishbone Diagrams because their design allows four to five levels of 'why' to be identified for a given problem, if the users are willing to exercise a high level of discipline as they draw their charts. Fault trees could be really useful for troubleshooting reoccurring problems, such as quality defects, because such problems tend to have a common set of causes and sub-causes. When used in this manner however, a fault tree essentially becomes analogous to the TapRooT® Equifactor® Troubleshooting technique, which is used in practice for equipment troubleshooting.

Disadvantages. Fault trees typically fail because a) people do not use them in a disciplined manner to develop multiple problem causes at each level; b) multiple levels of potential causes exist to be sorted through for each problem type; c) they are opinion driven. They often tend to be a blend of a cause-effect diagram and flow chart, but in such cases the user can easily get lost and not arrive at any

particular root cause. Also, a well-developed fault tree often leads the user to discover that the same management systems (such as poor training, employee turnover, weak communications, and poor procedure design) are at the root of their problems. In turn, a well designed fault tree will lead the investigator to the basic cause categories, but rarely to the comprehensive mix of real root causes [20, 110].

Application: Fault Tree Analysis is not normally used as a root cause analysis method, primarily because it does not work well when human actions are inserted as a cause. This is because the wide variance of possible human failure rates prevents accurate results [25]. But it works extremely well at defining engineered systems and can be used to supplement an RCA in the following ways:

- finding causes by reviewing the assumptions and design decisions made during the system's original design;
- determining if certain causal scenarios are probable;
- selecting the appropriate solution(s).

Fault tree analysis can be applied to identify critical paths and the relative importance of paths for achievement of the top event. This is typically done to help in assessing the safety significance of the event. This tool is broadly used for both RCA and PSA in a wide range of industries and has extensive support in the form of published literature and software packages.

Fault tree analysis can be used in combination with other tools (e.g. FMEA or FMECA) as part of a root cause analysis solution. Failure Mode and Effects Criticality Analysis (FMECA) and Failure Mode and Effects Analysis (FMEA) are processes by which potential weaknesses in design or a process are identified. FMECA as described in MIL-STD-1629A [148], and FMEA as described in ISO9000, involve reviewing schematics, engineering drawings, operational manuals, etc. to identify basic faults at the lowest (part) level and consequently determine their effects at subassembly (higher) level, or system level, with respect to safety and or operational requirements. This approach is also considered as an inductive analysis that methodically details, on an element-by-element basis, all possible failure modes, and identifies their resulting effects on surrounding elements and/or the overall system. FMEA is sometimes used to find the cause of a component failure. Like many of these other tools, it can be used to help find a causal element within a Realitychart. However, it does not work well on systems or complex problems because it cannot show evidence-based causal relationships beyond the specific failure mode being analysed.

Fault Tree Diagram Construction using FaultTree+ software [48]

FaultTree+ software provides an easy to use interface for constructing fault tree diagrams. The user simply adds gates and events by selecting an existing gate and dropping the new gate or event onto the selected gate. Once created, the new gate or event may be selected, and their parameters modified. Extensive copy and paste facilities make the re-use of existing fault tree sub-trees an easy task. In addition to the diagram construction area, a spreadsheet interface is available for the rapid access to and modification of gate and event parameters. The spreadsheet interface may also be used to construct the fault tree if desired. The screen shot below shows an example of the FaultTree+ diagram construction area (Figure 3.7.3).

FaultTree+ software features include:

- drag and drop add mode for fast tree construction;
- copy and paste for duplicating existing fault tree sub-trees;
- spreadsheet interface for rapid modification of gate and event parameters;
- automatic paging facilities - simply identify gates or branches with a new page tag and the program takes care of pagination;
- undo and automatic backup facilities;
- append existing FaultTree+ projects;
- descriptive text labels and bitmap images may be placed anywhere on a fault tree page;
- font selection for names, descriptions and labels;

- diagram scale and shift options including manual shifting of sub-trees and automatic alignment to the screen edit area;
- delete hidden data facility for tidying-up large projects.

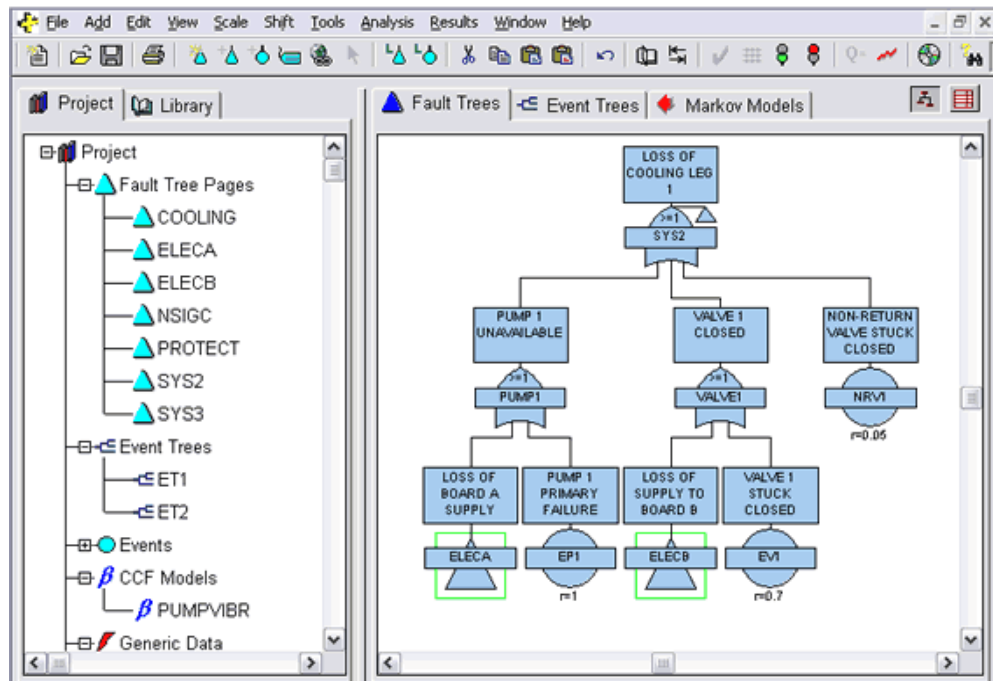


Figure 3.7.3. The FaultTree+ diagram construction area [48]

The FaultTree+ Edit Gate dialog allows the user to select the gate type, name and description. The user may also create the fault tree diagram using this dialog by selecting either the Add Gate Input or Add Event Input button. A spreadsheet interface is also available for rapid access to, and modification of, gate parameters. The FaultTree+ Edit Event dialog allows the user to select the event failure model (failure characteristic), name and description. A spreadsheet interface is also available for rapid access to and modification of event parameters.

FaultTree+ provides CCF analysis, importance analysis, uncertainty and sensitivity analysis facilities. It uses efficient minimal cut set generation algorithms to analyse large and complex fault and event trees. NOT logic may be included in the fault and event trees at any level and event success states retained in the analysis results as an option. After performing the analysis the Results Summary dialog (shown below) provides a detailed overview of the analysis results. The comprehensive reporting facilities are also included, allowing the user to report on their results using sophisticated text, graph and diagram reports.

Some other important the Fault Tree+ Analysis software facilities are [48]:

- range of event failure and repair models including fixed rates, dormant, sequential, standby, time at risk, binomial, Poisson and initiator failure models;
- basic events may be linked to Markov models created in the Markov analysis module;
- CCF analysis using the beta factor, MGL, alpha factor or beta BFR methods. Initiator-enabler analysis for sequence dependent analyses;
- sensitivity analysis allowing the automatic variation of event failure and repair data between specified limits;
- time dependent analysis providing intermediate values for time dependent system parameters. Verification checks providing diagnostic information before commencing an analysis. Checks are made for circular logic, undefined gates, invalid initiators etc.;

- fault tree house event analysis. Full minimal cut set analysis (including success states if required);
- post-processing facilities for accurate upper bound calculations. Importance analysis with Fussell-Vesely, Birnbaum, Barlow-Proshan and Sequential importance measures. Risk measures provided for event tree consequences;
- uncertainty analyses allowing confidence levels to be determined from event failure and repair data uncertainties. Status facility to indicate whether analysis results are out of date with respect to project data.

3.8. Event tree analysis

The purpose of the event tree analysis tool is to identify potential outcomes from an initial event. It helps to determine what happens when a line of defence is successful and what happens when it fails. Event tree modelling technique is a systematic approach to accident progression studies, and prevention [49]. It is constructed to investigate physical processes for accident sequence groups, before and after an incident, and to map out all possible progression paths. Accident progression scenarios are identified by including event tree branches with respect to events governing the circumstances of an accident. This analysis yields a listing of different outcomes for an accident progression, and the conditional probability of each accident progression scenario.

Further analysis may be necessary, that includes consequence determination for the most severe and less than desirable outcomes. Depending on the severity of an accident outcome, which may be determined by occurrence time, duration, and contributions to immediate and latent problems, a consequence is quantified using an event tree model. Event tree models can be developed as stand alone, and also in combination with event tree - fault tree models for more complex accident progression scenarios.

The event tree model is a first step in developing a 'Risk Graph'. A risk graph is then used in determining the safety integrity level (SIL) for a safety system. Determination of SIL is based on a probabilistic risk graph that is constructed using four parameters, 'Consequence - C', 'Exposure - F', 'Probability of avoiding hazard - P', and 'Likelihood of Event - W'.

Event Tree Construction and Analysis using the FaultTree+ software [48]

The FaultTree+ event tree analysis module is unique in its ability to handle large scale problems and to fully handle success logic. The event tree model may be created independently of the fault tree model or may use fault tree analysis gate results as the source of event tree probabilities. The event tree module handles both primary and secondary event trees, multiple branches and multiple consequence categories.

The screen shot below (Figure 3.8.2) shows the FaultTree+ event tree construction area.

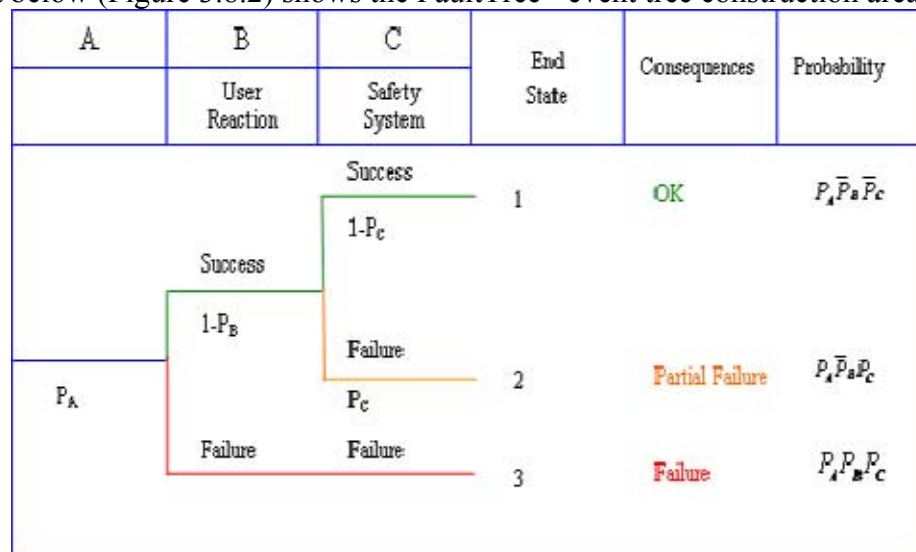


Figure 3.8.1. Simple event tree example

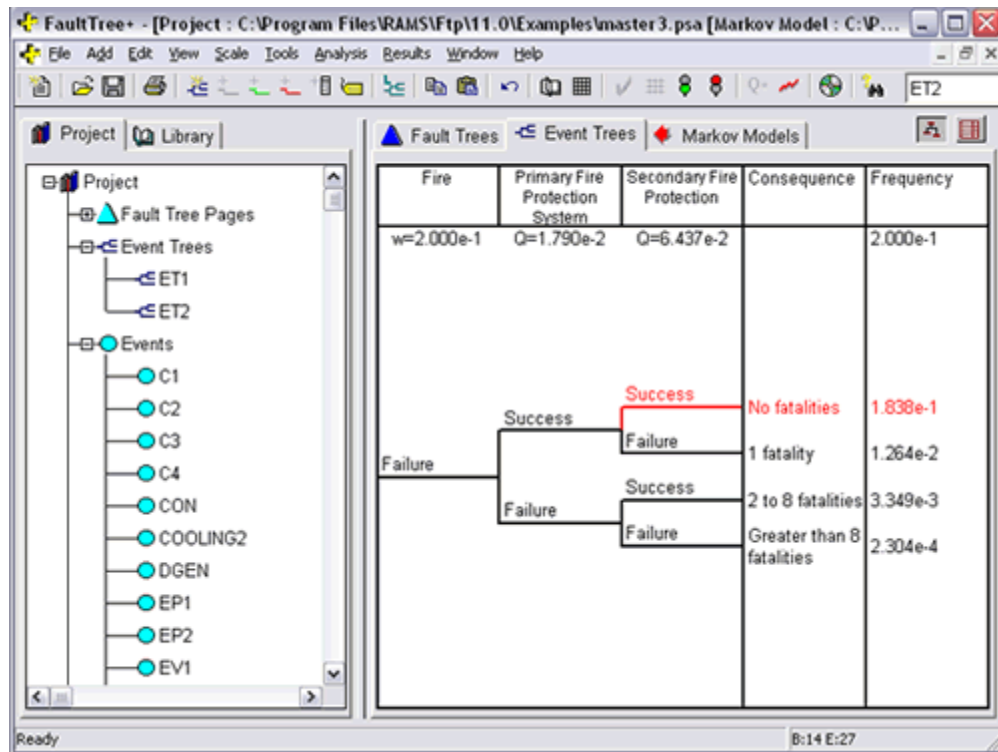


Figure 3.8.2. Event tree construction area using the FaultTree+ software [48]

Event Tree Construction Features

- primary and secondary event trees;
- multiple branching supported for event trees;
- multiple consequence categories for event trees;
- pruning of event trees;
- insert new columns retaining existing data;
- copy and paste event trees;
- descriptive text labels and bitmap images may be placed anywhere on an event tree page;
- font selection for names, descriptions and labels;
- undo and automatic backup facilities.

Event Tree Analysis Features

- full minimal cut set analysis. Success states are fully handled;
- range of event failure and repair models including fixed rates, dormant, sequential, standby, time at risk, binomial, Poisson and initiator failure models;
- basic events may be linked to Markov models created in the Markov analysis module;
- comprehensive risk calculation;
- risk importance analysis identifying the major contributors to risk;
- sensitivity analysis allowing the automatic variation of event failure and repair data between specified limits.

The attributes of the Event Tree Analysis Tool are:

- starts by an initiating event (not the final event);
- depicts what happens if the line of defence is successful (S) or fails (F);
- branching stops when a significant consequence or concern is identified;
- useful in quantitatively determining the probability of the different consequences when the probability of each line of defence is known;
- allows dependence and domino effects that are difficult to model in fault trees;

- allows for determining the effectiveness of possible corrective actions to prevent recurrence by quantitative analysis of possible future failures if proposed corrective actions were to be implemented.

Application: The event tree analysis is traditionally used to help in assessing the safety significance of the event, in both root cause analysis and probabilistic safety analysis.

A blend of fault tree and event tree analysis is sometimes treated as an autonomous event investigation tool, and called cause-consequence analysis (CCA) [45]. This technique was invented by 'RISO' Laboratories in Denmark to be used in risk analysis of nuclear power stations. However, it can also be adapted by the other industries in the estimation of the safety of a protective or other safety related systems.

This technique combines cause analysis (described by fault trees) and consequence analysis (described by event trees), and hence deductive and inductive analysis is used. The purpose of CCA is to identify chains of events that can result in undesirable consequences. With the probabilities of the various events in the CCA diagram, the probabilities of the various consequences can be calculated, thus establishing the risk level of the system. Figure 3.8.3 below shows a typical CCA chart.

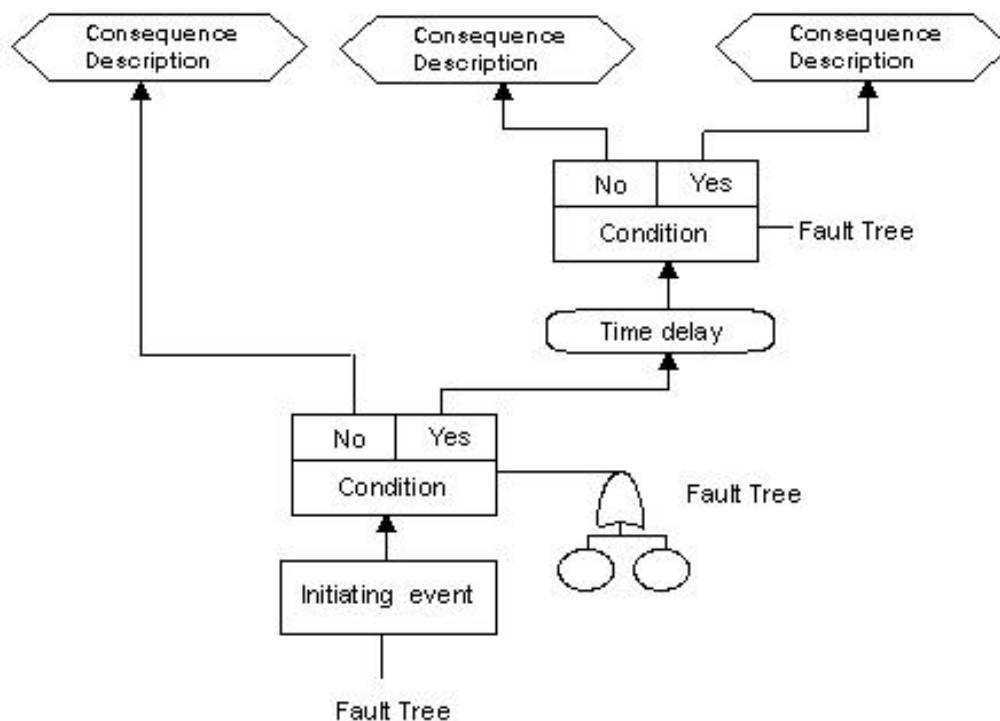


Figure 3.8.3. Example of a structure of a typical cause-consequence analysis (CCA) chart [45]

3.9. Causal factor tree analysis

Causal factor tree analysis is an investigation and analysis technique used to record and display, in a logical, tree-structured hierarchy, all the actions and conditions that were necessary and sufficient for a given consequence to have occurred [8].

Causal Factor tree analysis refers to what is sometimes called a Causal Analysis, or Causal Factor Analysis - a technique based on displaying causal factors in a tree-structure such that cause-effect dependencies are clearly identified. A Causal Factor is an event or condition that either caused the occurrence under investigation, or contributed to the unwanted result. If it were not for this event or condition, the unwanted result would not have occurred or would have been less severe [52].

The Causal Factor tree analysis approach is similar to Fault Tree Analysis, but the emphasis is placed on Actions and Conditions instead of faults, as in the technique marketed as Apollo Root Cause Analysis [25]. The idea is that specific conditions must be present for an action to result in an undesirable effect,

and that causes and effects form an infinite chain (e.g. 5 Why's), where the cause of the top-level effect is a 2nd level effect itself with a cause that is a 3rd level effect, etc. An example is fire. The conditions required are a source of oxygen and fuel. The action is initiation of heat. The action plus the conditions result in fire. The absence of any condition will not result in fire, regardless of the action.

Tree structures are often used to display information in an organised, hierarchical fashion: organisation charts, work breakdown structures, genealogical charts, disk directory listings, etc. The ability of tree structures to incorporate large amounts of data, while clearly displaying parent-child or other dependency relationships, also makes the tree a very good vehicle for incident investigation and analysis. Combination of the tree structure with cause-effect linking rules and appropriate stopping criteria yields the causal factor tree, one of the more popular event investigation and analysis tools in use today [8].

Typically, a causal factor tree is used to investigate a single adverse event or consequence, which is usually shown as the top item in the tree [52]. Factors that were immediate causes of this effect are then displayed below it, linked to the effect using branches. Note that the set of immediate causes must meet certain criteria for necessity, sufficiency, and existence. Proof of existence requires evidence.

Once the immediate causes for the top item in the tree are shown, then the immediate causes for each of these factors can be added, and so on. Every cause added to the tree must meet the same requirements for necessity, sufficiency, and existence. Eventually, the structure begins to resemble a tree's root system. Chains of cause and effect flow upwards from the bottom of the tree, ultimately reaching the top level. In this way, a complete description can be built of the factors that led to the adverse consequence. Often, an item in the tree will require explanation, but the immediate causes are not yet known. The causal factor tree process will only expose this knowledge gap; it does not provide any means to resolve it. This is when other methods, such as change analysis or barrier analysis, can be used to provide answers for the unknowns. Once the unknowns become known, they can then be added to the tree as immediate causes for the item in question.

Each new cause added to the tree should be evaluated as a potential endpoint. When can a cause be designated as an endpoint? This is an object of some debate. Several notable RCA practitioners use some version of the following criteria:

- The cause must be fundamental (i.e. not caused by something more important), AND
- The cause must be correctable by management (or does not require correction), AND
- If the cause is removed or corrected, the adverse consequence does not occur.

These three criteria, taken together, are basically just a statement of the most widely used definition for 'root cause'. An alternative set of criteria, preferred by the author [8], is presented below. Note that these are all referenced to the system being analysed.

- The cause is a system response to a requirement imposed from outside the system, OR
- The cause is a contradiction between requirements imposed from within the system, OR
- The cause is a lack of control over system response to a disturbance, OR
- The cause is a fundamental limit of the system design.

A causal factor tree will usually have many endpoints. The set of all endpoints is in fact a fundamental set of causes for the top consequence in the tree. This fundamental set includes endpoints that would be considered both beneficial and detrimental; every one of them had to exist, otherwise the consequence would have been different. Endpoints that require corrective action would typically be called root causes, or root and contributing causes if some scheme is being used to differentiate causes in terms of importance.

The structure of a causal factor tree is shown in Figure 3.9.1, and illustrations of a causal factor tree analysis are provided in Figures 3.9.2-3.9.4 [52].



Causal Analysis Tree

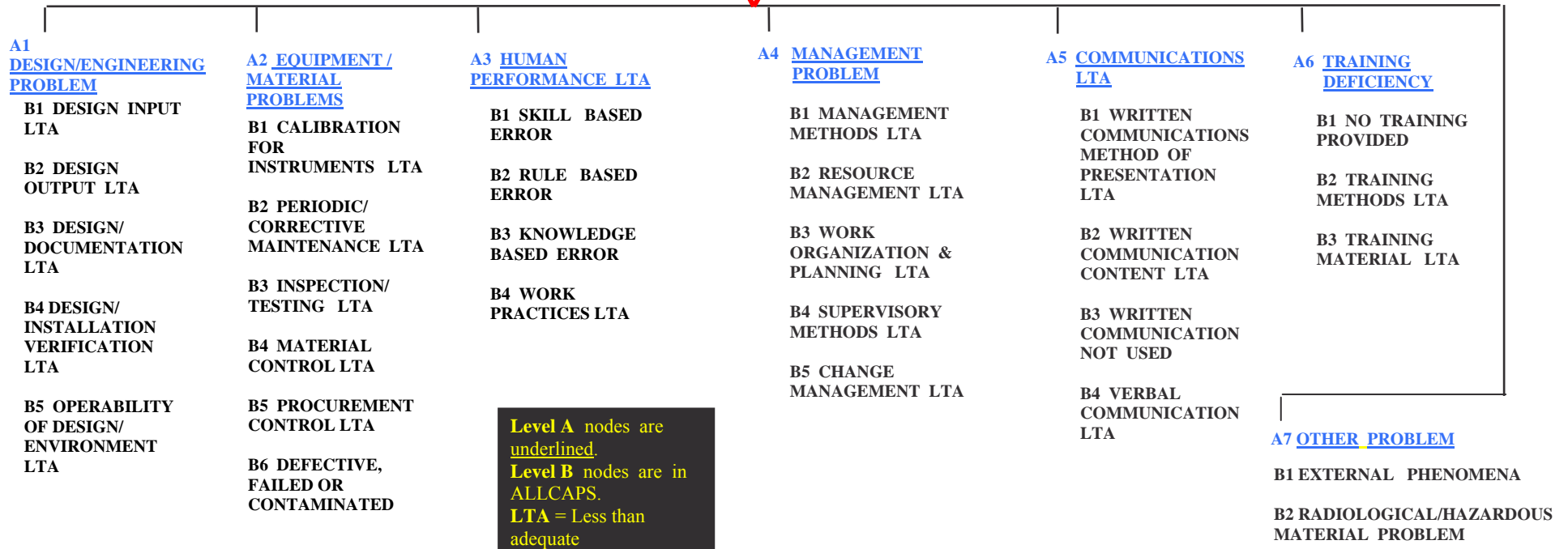


Figure 3.9.1. The structure of a causal factor tree

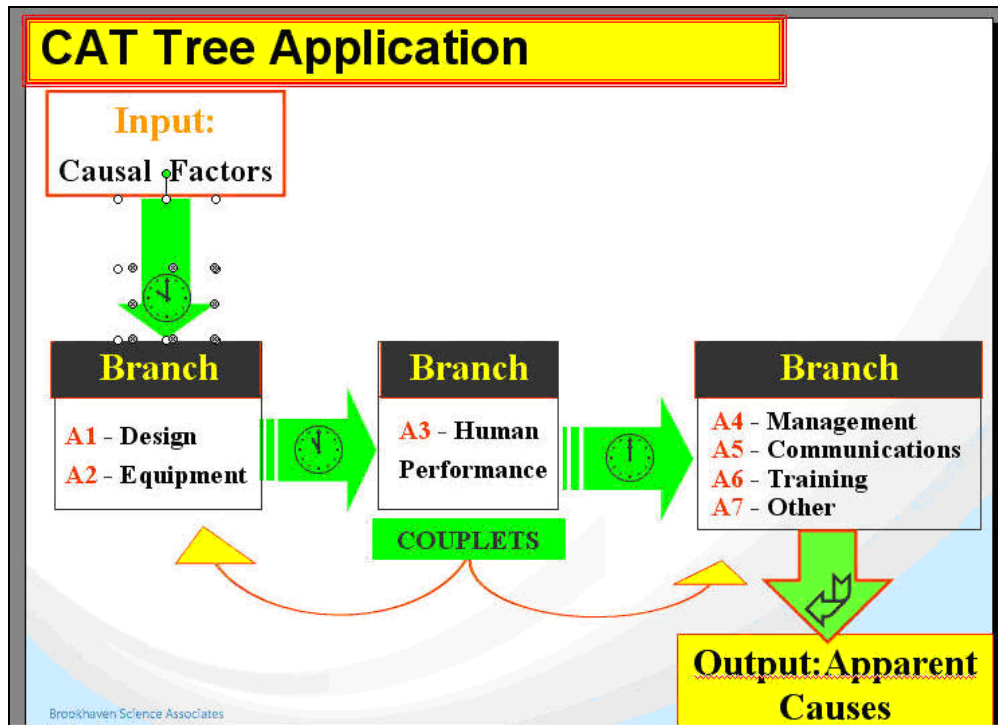


Figure 3.9.2. Apparent cause finding process using a causal factor tree

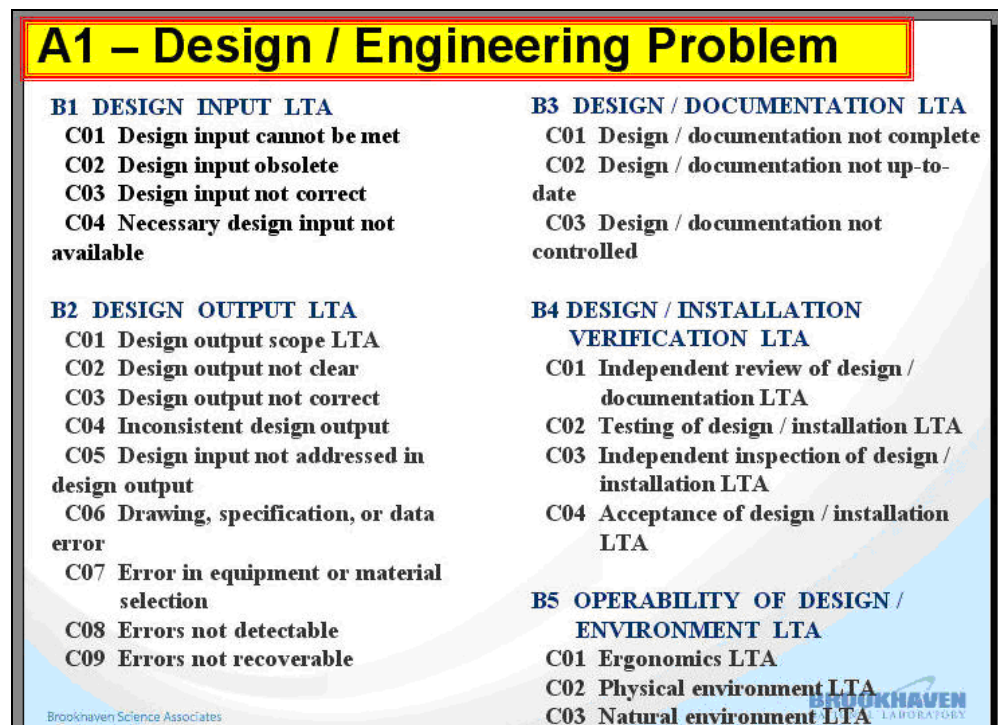


Figure 3.9.3. Further analysis of A1 – Design/engineering problem using a causal factor tree

In summary, the causal factor tree is an investigation/analysis tool that is used to display a logical hierarchy of all the causes leading to a given effect or consequence. When gaps in knowledge are encountered, the tree exposes the gap, but does not provide any means to resolve it; other tools are required. Once the required knowledge is available, it can be added to the tree. A completed causal

factor tree provides a complete picture of all the actions and conditions that were required for the consequence to have occurred. Success in causal factor tree analysis depends on the rigour used in adding causes to the tree (i.e. ensuring necessity, sufficiency, and existence), and in stopping any given cause-effect chain at an appropriate endpoint.

Advantages. Provides structure for the recording of evidence and display of what is known. Through application of logic checks, gaps in knowledge are exposed. Tree structure is familiar and easy to follow. Can easily be extended to handle multiple (potential) scenarios. Can incorporate results from the use of other tools. Works well as a master investigation/analysis technique.

Disadvantages. Cannot easily handle or display time dependence. Sequence dependencies can be treated, but difficulty increases significantly with added complexity. Shows where unknowns exist, but provides no means of resolving them. Stopping points can be somewhat arbitrary.

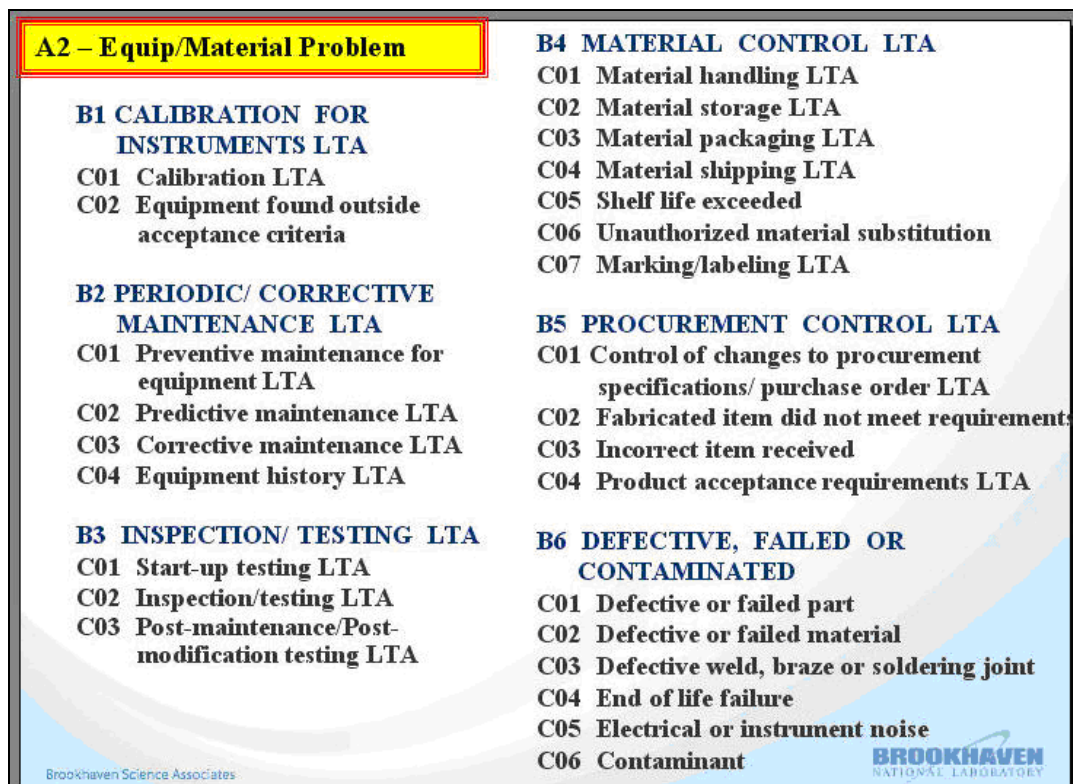


Figure 3.9.4. Further analysis of A2 – Equipment/materials problem using a causal factor tree

3.10. Kepner-Tregoe Problem Solving and Decision Making

The Kepner-Tregoe (KT) tool is a systematic, logical technique of resolving concerns. This process, or part of it, could be used by almost every event investigator, even those who have never received formal training in it. KT labels, and arranges in a logical sequence, the normal thought processes commonly used when making a decision or solving a problem [6, 11, 20, 109, 110]. The key components of the KT process include problem analysis, potential problem analysis, situation analysis, and decision analysis. Problem analysis is largely based on the 'IS/IS NOT' tool, so it is similar to the change analysis process. The decision analysis tool focuses on teaching people to evaluate possible improvement options in a systematic, fact-based manner, as opposed to finding root causes. Situation analysis is used to assess the risk associated with possible improvements, and Potential Problem Analysis looks at the possible repercussions of failing to make a change.

Kepner-Tregoe is used when a comprehensive analysis is needed for all phases of the occurrence investigation process. Its strength lies in providing an efficient, systematic framework for gathering, organising and evaluating information and consists of four basic steps:

- situation appraisal to identify concerns, set priorities, and plan the next steps;
- problem analysis to precisely describe the problem, identify and evaluate the causes and confirm the true cause (this step is similar to change analysis);
- decision analysis to clarify purpose, evaluate alternatives, assess the risks of each option and make a final decision;
- potential problem analysis to identify safety degradation that might be introduced by the corrective action, identify the likely causes of those problems, take preventive action and plan contingent action. This final step provides assurance that the safety of no other system is degraded by changes introduced by proposed corrective actions.

These four steps cover all phases of the occurrence investigation process, and thus Kepner-Tregoe can be used for more than causal factor analysis. Separate worksheets (provided by Kepner-Tregoe) provide a specific focus on each of the four basic steps, and consist of step by step procedures to assist in the analyses. This systems approach prevents any aspect of the concern being overlooked. A formal Kepner-Tregoe training is needed for those using this method.

The steps which make up the problem analysis process of the Kepner-Tregoe technique are implemented in the following way [6]:

1. Describe the Problem. The problem is described by clearly stating the deviation, or stating what should have occurred and what actually occurred. As an aid in clearly stating the deviation, information should be gathered to answer the following questions:
 - What is the deviation(s)?
 - Where is the deviation(s)?
 - When did the deviation(s) occur?
 - To what extent did the deviation(s) occur?

With this information in place, the next step in clearly understanding the deviation is to develop an IS and IS NOT comparison chart. This chart should contain information about what, where, when, and to what extent the deviation(s) IS along with what, where, when, and to what extent the deviation(s) IS NOT.

2. List the Possible Causes. This second basic step of the problem analysis process creates a list of possible causes for the specified deviation. This list is generated by listing the distinctions and/or changes that have occurred between the items of the IS and IS NOT lists. The causes of the distinctions or changes are then investigated.
3. Find the True Cause(s). The last basic step of the problem analysis process is finding the true cause of the deviation. This step tests the list of possible causes for the most probable causes. This is done by comparing all of the possible causes with the observed specifics (the IS/IS NOT chart) of the deviation. If the cause could produce all of the same observed specifics, it can be classified as a probable cause.

When all the probable causes have been determined, then the True Cause must be found and verified. This is done by further investigation, experimentation, observation, etc. of the most probable causes.

Advantages. As shown, the Kepner-Tregoe technique for performing a root cause analysis does provide the basic benefits of a good analysis tool. If the user has performed a good problem investigation and has collected a lot of information (especially data), it is possible to find the causes of the specific problem being analysed. Moreover, this technique acts as a structured guideline to an investigator in determining the information needed, the questions to ask, and when to stop; i.e., when the root causes have been identified. The Decision Analysis tool is one of the best for evaluating improvement options. This technique does provide a good base for the development of more specific analysis tools to find root causes of reactor plant events. Good information and a formal evaluation process help keep the user of KT tools from focusing too much on blaming people.

Disadvantages. The major drawback to this technique, when performing root cause analysis or determining corrective actions, is, as in any 'thought' process, that extensive training in the technique is required and constant practice in its use is necessary. Also, a significant amount of time, energy and

resources may be required for the verification of the true causes of the event. KT tools are not as functional as other RCA tools (e.g. TapRooT®) in terms of getting to generic causes.

3.11. Interrelationship diagram

The interrelationship diagram (ID), originally known as the relations diagram, was developed in 1976 by the Society of Quality Control Technique Development, in association with the Union of Japanese Scientists and Engineers (JUSE) [7, 51, 95]. The relations diagram was part of a toolset known as the seven new quality control (7 new QC) tools. It was designed to clarify the intertwined causal relationships of a complex problem in order to identify an appropriate solution. The relations diagram evolved into a problem-solving and decision-making technique from management indicator relational analysis, a method for economic planning and engineering.

The interrelationship diagram takes complex, multivariable problems and explores and displays all of the interrelated factors involved. It shows graphically the logical (and often causal) relationships between factors. The ID allows groups to identify, analyse, and classify the cause-and-effect relationships that exist among all critical issues, so that key factors can be part of an effective solution. The purpose of the ID is to encourage practitioners to think in multiple directions rather than linearly, so that critical issues can emerge naturally rather than follow personal agendas. The ID assists in systematically identifying basic assumptions and reasons for those assumptions. In summary, the ID helps identify root causes.

The ID uses arrows to show cause-and-effect relationships among a number of potential problem factors. Short sentences or phrases expressing the factor are enclosed in rectangles or ovals. Whether phrases or sentences are used is a group decision, but authors of ID tool recommend the use of at least a noun and a verb. Arrows drawn between the factors represent a relationship. As a rule, the arrow points from the cause to the effect or from the means to the objective. The arrow, however, may be reversed if it suits the purpose of the analysis.

The format of the ID is generally unrestricted, with several variants. The centrally converging ID places the major problem in the centre, with closely related factors arranged around it to indicate a close relationship. The directionally intense ID places the problem to one side of the diagram, and arranges the factors according to their cause-and-effect relationships on the other side. The applications format ID can be unrestricted, centrally converging, or directionally intense, but adds additional structure based on factors such as organisational configuration, processes, or systems.

The ID may use either quantitative or qualitative formats. In the qualitative format, the factors are simply connected to each other, and the root cause is identified based on intuitive understanding. In the quantitative format, numeric identifiers are used to determine the strength of relations between factors, and the root cause is identified based on the numeric value.

It is recommended to follow the procedure below when creating a relations diagram:

- Step 1: Collect information from a variety of sources.
- Step 2: Use concise phrases or sentences as opposed to isolated words.
- Step 3: Draw diagrams only after group consensus is reached.
- Step 4: Rewrite diagrams several times to identify and separate critical items.
- Step 5: Do not be distracted by intermediate factors that do not directly influence the root causes.

It is recommended to ask *why* questions to identify true cause-and-effect relationships, and to slow down the process so that participants can critically evaluate, revise, examine, or discard factors. The first step in using an ID is to determine and label the factors, then place them on an easel or whiteboard in a circular shape, and assess the relationship of each factor on other factors, using arrows. After all relationships have been assessed, count the number of arrows pointing into or out of each factor. A factor with more 'out' than 'in' arrows is a cause, while a factor with more 'in' than 'out' arrows is an effect. The causal factors form the starting point for analysis. Figure 3.11.1 shows an example of an unrestricted quantitative interrelationship diagram.

A variant of the ID is the ID matrix, which places all the factors in the first column and row of a matrix. This format creates a more orderly display and prevents the tool from becoming too chaotic when there are many factors. The strength and direction of the relationships can be represented through arrows, numbers, or other symbols placed in the cells of the matrix. It has been shown that users become careless with large, complicated diagrams, so the ID matrix is a good technique to force participants to pay attention to each factor in a more systematic fashion.

A particular concern relating to the ID is that it does not have a mechanism for evaluating the integrity of the selected root cause. In using the quantitative or qualitative method, practitioners must be able to assess the validity of their choices, and the strength of the factor relationships. Some users may simply count the number of arrows and select a root cause, without thoroughly analysing or testing their assumptions about the problem.

Overall, the ID's strength is that it is a structured approach that provides for the analysis of complex relationships, using a nonlinear approach. The disadvantages are that it may rely too heavily on subjective judgments about factor relationships and can become quite complex or hard to read.

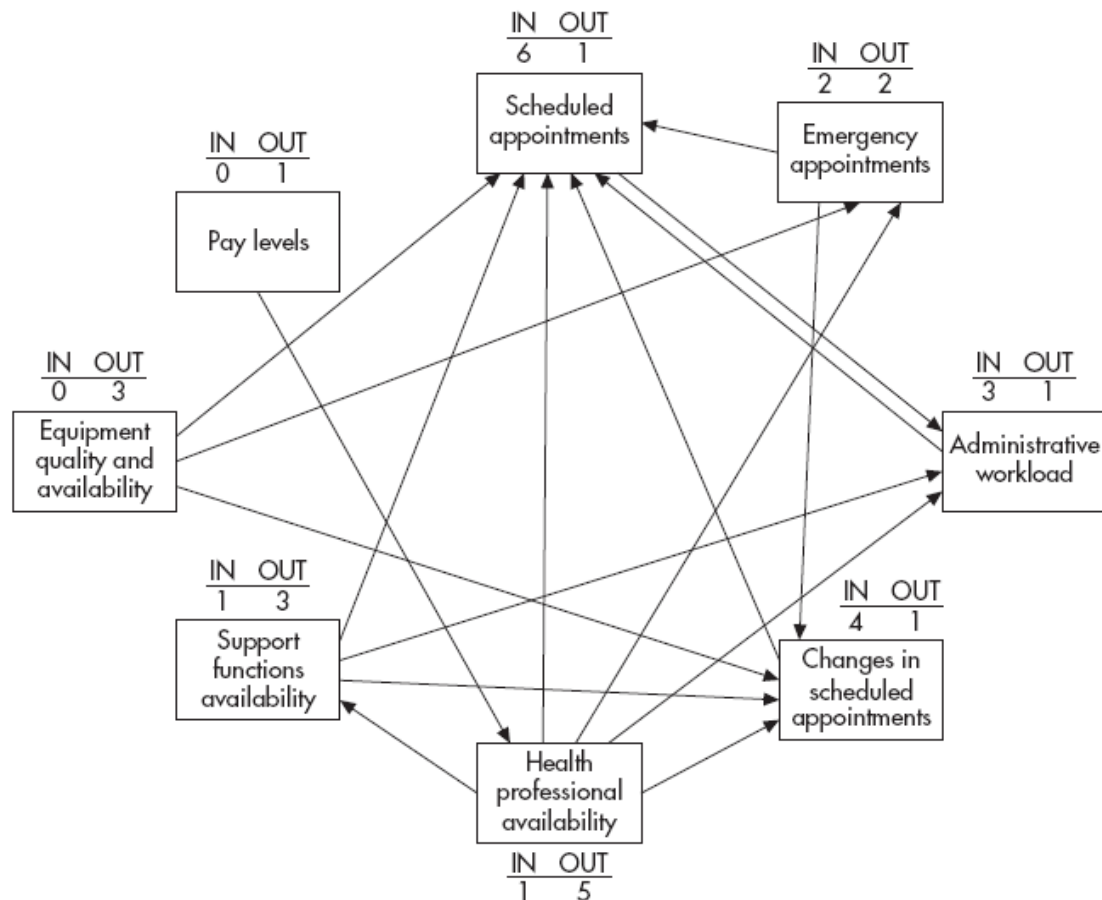


Figure 3.11.1. An example of an unrestricted quantitative interrelationship diagram [95]

3.12. Current Reality Tree (CRT)

The CRT addresses problems by relating multiple factors rather than isolated events. Its purpose is to help practitioners find the links between symptomatic factors, called undesirable effects (UDEs), of the core problem. The CRT was designed to show the current state of reality as it exists in a system. It reflects the most probable chain of cause-and-effect factors that contribute to a specific set of circumstances, and creates a basis for understanding complex systems [51].

The CRT assumes that all systems are subject to interdependencies among the factor components. Therefore, related causes must be identified and isolated before they can be addressed. Like the other tools, the CRT uses entities and arrows to describe a system. Entities are statements within some kind of geometric figure, usually a rectangle with smooth or sharp corners. An entity is expressed as a complete

statement that conveys an idea. An entity can be a cause, an effect, or both. Arrows in the CRT signify a sufficiency relationship between the entities. Sufficiency implies that the cause is, in fact, enough to create the effect. Entities that do not meet the sufficiency criteria are not connected. The relationship between two entities is read as an ‘if-then’ statement such as, ‘If [cause statement entity], then [effect statement entity]’.

In addition, the CRT uses a unique symbol, the oval or ellipse, to show relationships between interdependent causes. The literature distinguishes between interrelationship and interdependency, using sufficient cause logic so that effects due to interdependency are attributed to multiple and related causal factors. Because the CRT is based on sufficiency, there may be cases where one cause is not sufficient by itself to create the proposed effect. Thus, the ellipse shows that multiple causes are required for the produced effect. These causes are contributive in nature, so they must all be present for the effect to take place. If one of the interdependent causes is removed, the effect will disappear. Relationships that contain an ellipse are read as, ‘If [first contributing cause entity] and [second contributing cause entity], then [effect entity].’ Figure 3.11.2 shows an example of a current reality tree.

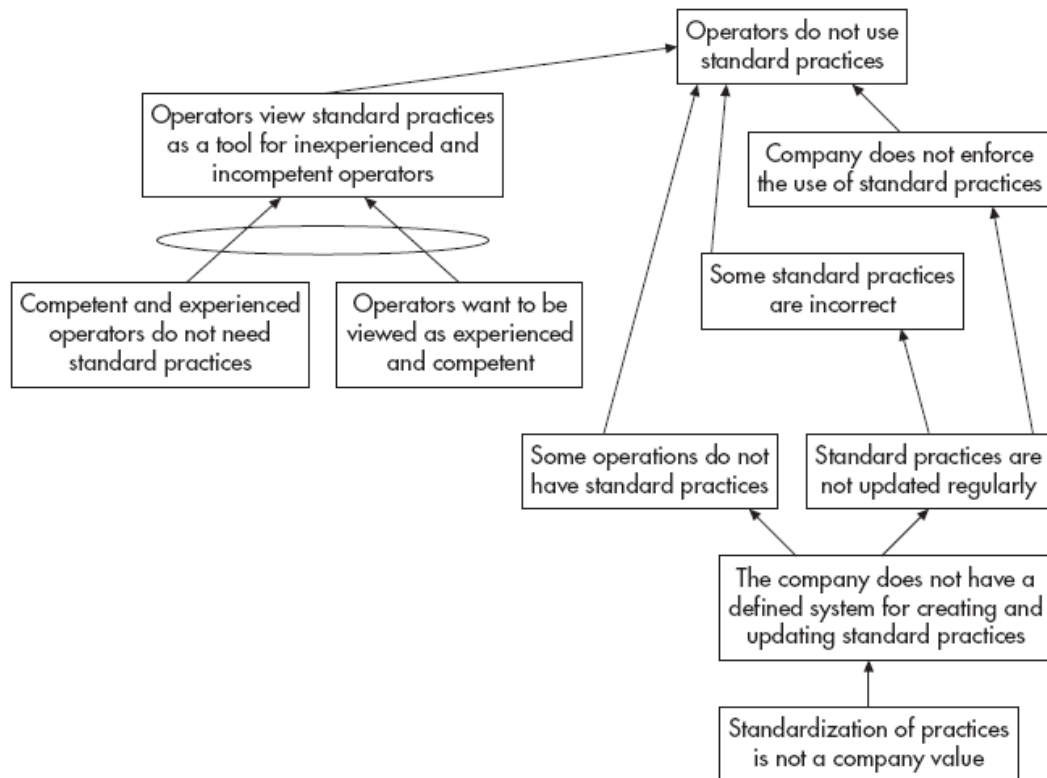


Figure 3.12.1. An example of a current reality tree [51]

The CRT also allows for looping conventions that either positively or negatively amplify the effect. In this situation, an arrow is drawn from the last entity back to one of the earlier causes. If the original core cause creates a negative reinforcing loop, but can be changed to a positive one, the entire system will be reinforced with a desirable effect. Although constructed from the top, starting with effects, then working down to causes, the CRT is read from bottom to top using ‘if-then’ statements. The arrows lead from the cause upward. The procedure for constructing a CRT is as follows:

1. List between five and ten problems or undesirable effects related to the situation.
2. Test each UDE for clarity and search for a causal relationship between any two undesirable effects.
3. Determine which UDE is the cause and which is the effect.
4. Test the relationship using categories of legitimate reservation.
5. Continue the process of connecting the UDEs using ‘if-then’ logic until all the UDEs are connected.
6. Sometimes the cause by itself may not seem to be enough to create the effect. Additional dependent causes can be shown using the ‘and’ connector.

7. Logical relationships can be strengthened using words like *some*, *few*, *many*, *frequently*, and *sometimes*.

This process continues as entities are added downward and chained together. At some point no other causes can be established or connected to the tree. The construction is complete when all UDEs are connected to very few root causes, which do not have preceding causal entities. The final step in the construction of the CRT is to review all the connections and test the logic of the diagram. Branches that do not connect to UDEs can be pruned or separated for later analysis.

The assumptions and logic of the CRT are evaluated using clarification rules called CLR. These rules ensure rigour in the CRT process and are the criteria for verifying, validating, and agreeing upon the connections between factors. They are also used to facilitate discussion, communicate disagreement, reduce animosity, and foster collaboration. The CLR consists of six tests or proofs: clarity, entity existence, causality existence, cause insufficiency, additional cause, and predicted effect.

Clarity, causality existence, and entity existence are the first level of reservation and are used to clarify meaning and question relationships, or the existence of entities. The second level of reservation includes cause insufficiency, additional cause, and predicted effect. They are secondary because they are used when questions remain after addressing first-level reservations. Second-level reservations look for missing or additional causes and additional or invalid effects.

Particular concerns relating to the CRT are its complexity of construction and rigorous logic system. Practitioners may find the application of the CRT too difficult or time consuming. Conversely, the strength of the CRT is the rigour of the CLR mechanism that encourages attention to detail, ongoing evaluation, and integrity of output.

3.13. Human Factors Investigation Tool (HFIT)

In an attempt to improve the investigation of the human factors causes of accidents in the UK offshore oil and gas industry, a Human Factors Investigation Tool (HFIT) was developed with the sponsorship of the UK Regulator, the Health and Safety Executive, and four exploration-related companies [61]. The tool was developed on a theoretical basis, with reference to existing tools and models, and it collects four types of human factors information including: (a) the action errors occurring immediately prior to the incident; (b) error recovery mechanisms, in the case of near misses; (c) the thought processes which lead to the action error; (d) the underlying causes. The investigation tool was evaluated on the basis of (i) an inter-rater reliability assessment; (ii) a usability assessment; (iii) case studies; (iv) an evaluation system developed by Benner [101].

The structure of HFIT is developed on a sequential model of the incident trajectory, where incidents (accidents and near misses) are seen as the product of a number of different causes, organised into four categories. As Figure 3.13.1 illustrates, the behaviours immediately prior to the incident are described as the first category, called 'Action Errors', which personnel at the sharp-end enact. These action errors are generally preceded and caused in part by a reduction in awareness of their situation, so Situation Awareness is the second category. The reduction in situation awareness is often related to 'Threats' to safety from the work environment; otherwise, there are conditions that may have been in the system for some time, but have not been identified nor rectified (third category). If the error or reduced situation awareness is detected and recovered from before an accident occurs (error recovery), a near miss results. So a fourth category, called 'Error Recovery', is included, that could occur during the action error or situation awareness stages. The four categories contain a total of 28 elements, listed in Figure 3.13.1. Each of these elements is further described in Figure 3.13.2, although only some examples are given at the 'sub-element' and 'item' levels. Action error elements are divided into 22 further 'items', situation awareness elements are described by 21 'items' and the error recovery elements contain 7 items. The 12 threat elements are divided into 'sub-elements' ($n = 43$) and 'items' ($n = 271$).

The Human Factors Investigation Tool, HFIT, was developed in a flowchart paper-based format, and after initial testing by potential users, it was developed as a computer-based tool. Figure 3.13.3 illustrates the process of investigating each category.

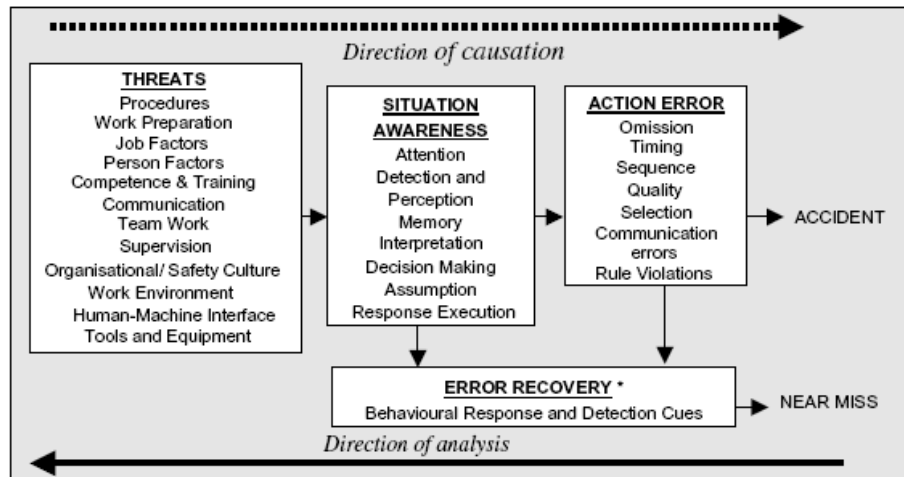


Figure 3.13.1. HFIT model of incident causation and direction of analysis

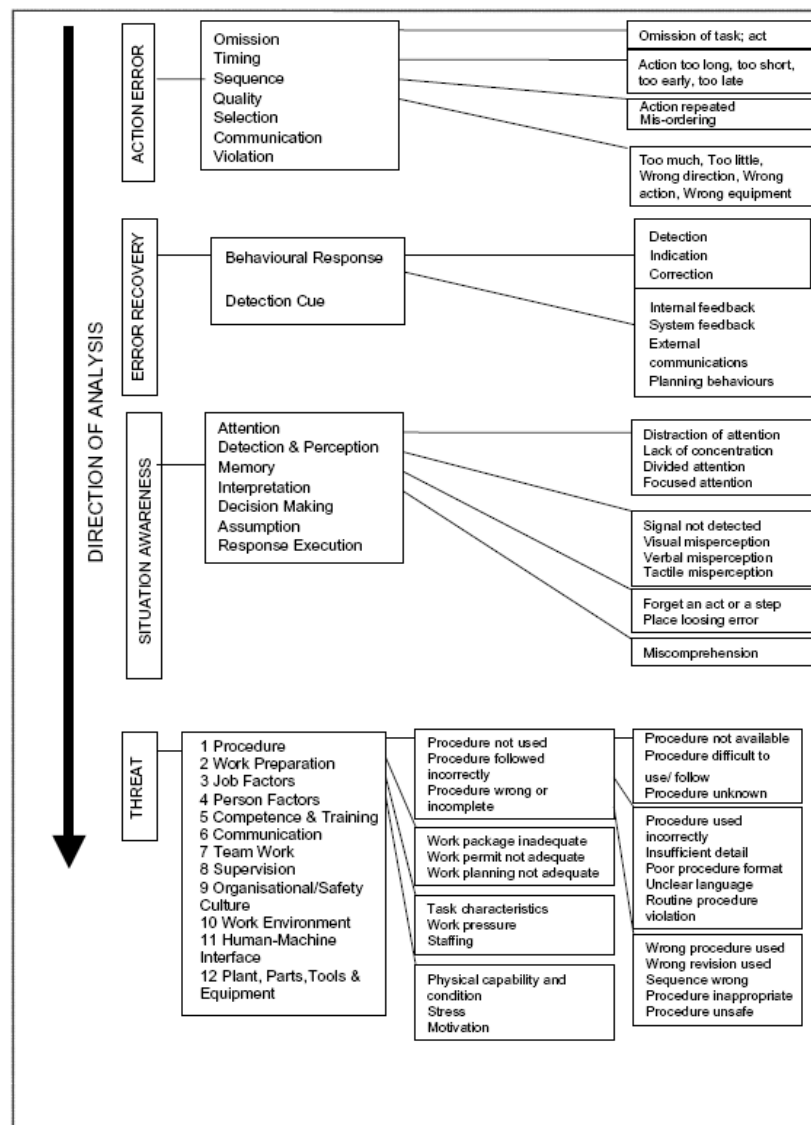


Figure 3.13.2. Structure of HFIT

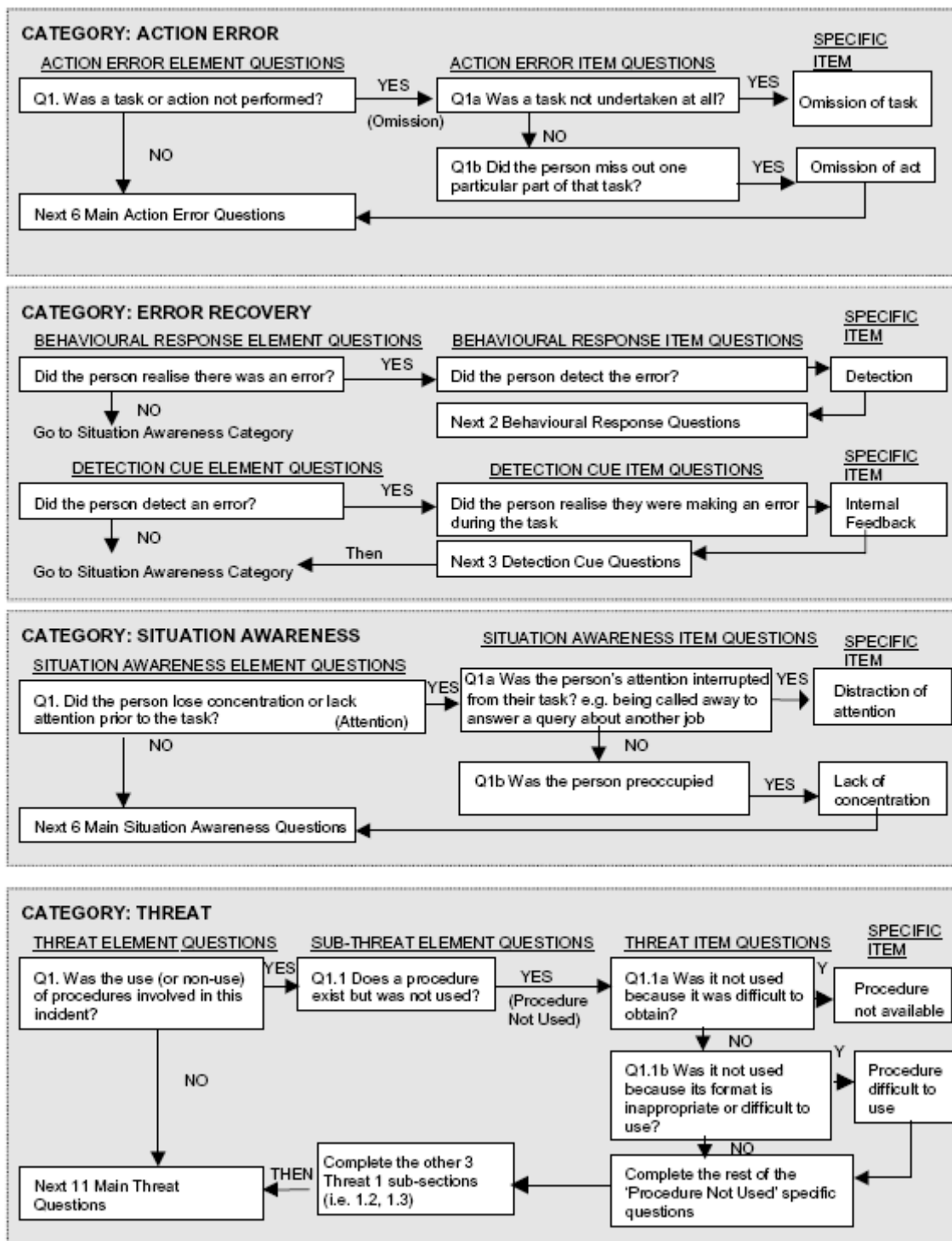


Figure 3.13.3. HFIT process

The HFIT tool can be used in a number of different ways: first, as an interview tool, where the investigator goes through the questions with each witness in turn. Secondly, the tool can be used after the witness interviews have taken place, and the investigator/s use the tool themselves, keeping in mind what they found from the interviews. Finally, it can be used retrospectively, on incidents that have been investigated previously, using other investigation tools.

The evaluation exercises performed have provided some initial evidence that HFIT improved the analysis of the incidents. HFIT was found to be useful for the development of remedial actions. However, some problems with the tool's reliability and with recording the results were identified. The implementation of HFIT into the incident investigation procedures of the participating companies indicated a very poor result, where only one out of the four participating companies collected data using HFIT. Lack of time and resources, and no incidents to report, were the reasons given for this poor response. In order for companies to implement HFIT, management support for the tool needs to be expressed to the potential users, encouraging them to make use of the tool, and presenting potential users with examples of how this tool can assist in their investigations. One of the main issues seems to be the cost and resources implications for implementing new tools, especially for large, international organisations.

3.14. Commercial all-purpose root cause analysis tools

3.14.1. REASON®

REASON is both a method and expert system software. The REASON method is a standard operating procedure that guides the investigator to ask the right questions at the right time to get the right answers. This dynamic, state-of-the-art method is programmed into the expert system of the software, which will then guide the investigator, step by step, through the root cause analysis process [9, 136, 137, 139, 158]. Professional REASON training focuses on the method, but includes abundant 'hands on' practice in applying the method with the use of the software tool.

REASON Root Cause Analysis is a multifaceted discipline that leads a user through the investigation of an event using a standard, repeatable inquiry process. This process guides the user to logically reconstruct an event from the causal facts. The method of inquiry is not based on predetermined questions found in a list or template, but is a process that dynamically creates a line of questioning, based on the very nature of the facts themselves. The REASON process ensures that the questions logically required by an event are indeed asked. It is a dynamic, systematic process that guides the investigator to discover the relevant facts, their causal relationship and potential solutions. Following this process creates a tree model of the event (see Figure 3.14.1.1). The tree represents visually the discrete facts of the event, and depicts graphically how these discrete facts networked to produce the overall event being investigated. The tree also indicates how solutions could have interrupted the causal network, thus achieving prevention of the unwanted event. When the model is finished, REASON® generates a series of reports and analyses automatically. Simply select the report elements desired, including cover sheet, report narrative and tree model, and REASON will automatically assemble a report for printing or editing.

REASON now offers three 'tiers' to its root cause analysis software. Each tier is a version of the REASON tool designed to provide the appropriate amount of guidance and rigour, depending on the criticality and risk involved with the problem being investigated. When beginning a REASON investigation, a case assessment is conducted to determine the criticality level of the problem to be investigated. The case assessment tool then recommends which tier in REASON is most appropriate. All three tools apply the same basic concepts, and cases generated with all three tools can be submitted and searched in the Lessons Learned system.

- **REASON Professional** offers the highest level of guidance and discipline in the process of eliciting and analysing relevant case facts.
- **REASON Express** offers flexibility in how much guidance and discipline the software provides in the process of eliciting and analysing relevant case facts.
- **REASON FrontLine** was designed to provide minimal guidance for situations in which an experienced worker already knows the solution, or perhaps several possible solutions; they just need a tool to get this information into the organisation's knowledge system.

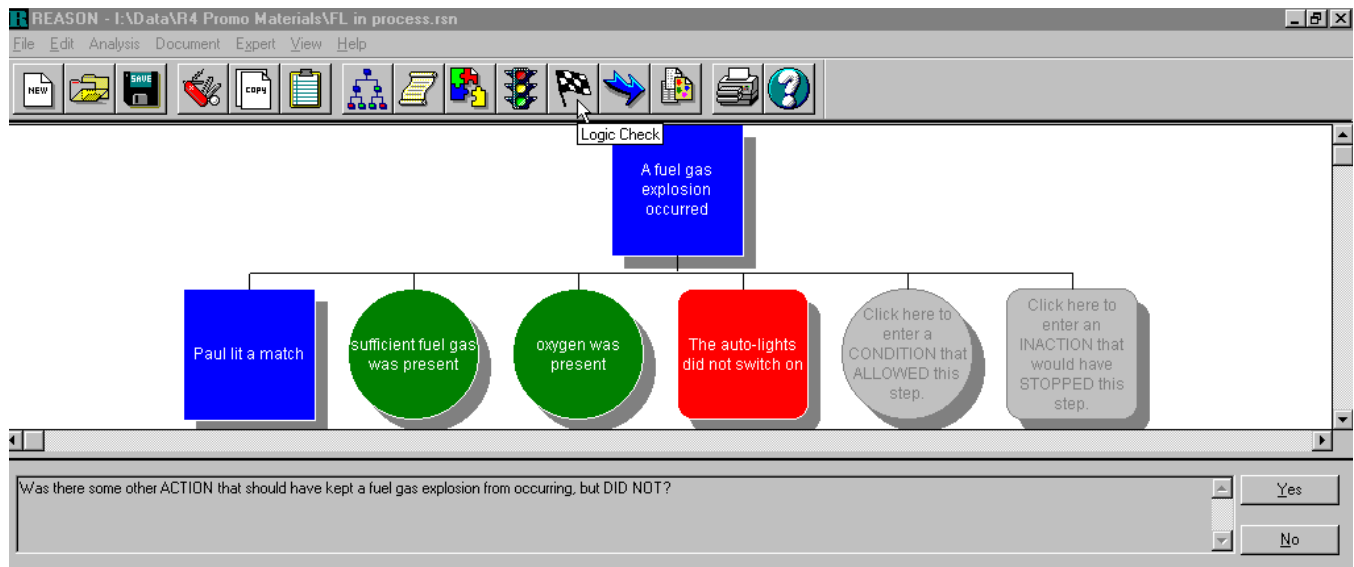


Figure 3.14.1.1. Example of a tree model of the event created using REASON® software [137]

The REASON Root Cause Analysis Process

Investigation starts at the final outcome of the event and works back through time. At each step in the investigation, the logic principles determine the next necessary piece of information, and REASON asks the appropriate question. In this way, the method guides the direction of the investigation by providing focused questions logically required by each new fact that is ascertained. The investigator must simply respond to the question by typing the answer into a box.

Step-by-Step Guidance

1. Identify Causal Relationships

The process assembles the facts into ‘sets’ of causal factors. These ‘sets’ provide a causal explanation for every factor in the event which networked to bring it about. For example, when lighting a match, leaking gas, and oxygen combine to produce an explosion, those factors form a ‘set,’ with the explosion as the outcome of their coming together.

2. Construct a Model of the Event

From these sets REASON builds a model of the event. The model depicts graphically the causal structure that brought about the event in a clear, easy-to-understand manner.

3. Verify Causal Relationships

After each set is built, the process then guides the investigator to validate each fact within the set. This process uses a simple validation process that applies the principles of causal reasoning known as ‘necessary and sufficient’ logic. This validation step ensures that no set within the investigation has facts causally irrelevant to the event being investigated.

4. Discover Root Causes or Corrective Opportunities

This process is continued until the investigator comes to factors which can be eliminated by applying some sort of ‘business process’ – that is, a policy, practice or procedure within the organisation. The absence of such a business process is a root cause of the event. A root cause may address a business process that already exists, or it may call for establishing a new business process to address the problem. REASON will guide the investigator, step by step, in determining what is needed.

5. Compare Solution Options

Each root cause represents a corrective opportunity, a solution option. The greatest advantage of the REASON method is that the process ensures that every causal factor is included in the event, thus ensuring that every possible avenue towards prevention is considered. This means that no

solution options will remain uncovered in the investigation. REASON provides an analysis feature that allows each solution option to be measured and compared to determine which provides the greatest benefit.

6. Reporting the Findings: Automatic Reporting Features

With just the click of a few buttons, REASON automatically generates a report on the investigation performed and assembles it into a report. The report can then be printed and saved as an MS WORD document file.

7. Lessons Learned Reports

REASON® investigations feed a Lessons Learned (LL) system that warehouses the knowledge from investigated cases. These cases are 'organisational experiences', recorded with both their pertinent facts and their solutions.

8. Broadcasting knowledge

The LL system provides an account-based (or push-based) system to automatically match up the cases submitted to LL with the people who need that knowledge.

9. Mining knowledge

REASON also provides a pull-based system in which users can actively search the LL system for knowledge that they need about the events happening in the organisation. The ability to search for trends and patterns across the organisation's problems provides a 'bird's-eye' view of the company. Having this ability allows organisation to measure improvement or loss of control in organisational processes throughout the company.

REASON's benefits. The Root Cause approach to incident /accident investigation using REASON's software offers an additional facet to the accident investigation. It may assist at looking at a systemic failure (organisationally) leading to an accident; it may also help to answer the systemic 'why' of an accident, complementing the 'how' and 'when.' Hopefully this approach will provide additional weight to recommendations following investigations. This tool, finally, pre-empts the old fashioned approach of 'remove the cause and the problem ceases to exist' [136].

3.14.2. PROACT®

PROACT® RCA provides the tools for the RCA analyst to easily document, validate, report and track findings and recommendations. The PROACT® RCA discipline involves: **P**Reserving Event Data, **O**rdering the Analysis Team, **A**nalyzing the Event Data, **C**ommunicating Findings and Recommendations, **T**racking for Bottom Line Results [10]. The PROACT® Suite not only identifies an organisation's most significant annual losses--it supplies the knowledge and tools to identify all the causes and then eliminate their recurrence in the future. This has been made possible by combining the PROACT® RCA software with the powerful LEAP Analysis software. LEAP - Basic FMEA Software & Opportunity Analysis - identifies what COULD go wrong or what HAS gone wrong, using Basic Failure Modes & Effects Analysis (FMEA) and Opportunity Analysis. The end result is that LEAP builds a business case for which events are the best candidates for Root Cause Analysis (RCA) based on the Return-On-Investment (ROI).

The building of a cross-functional RCA team is a critical step in the RCA process and has several strategic advantages, including providing a broader range of knowledge, viewpoints and programme ownership. However, the content of a root cause analysis effort on the item being investigated is limited by the cumulative experience and associated knowledge of the group.

The PROACT Logic Tree is representative of a tool specifically designed for use within RCA (see Figure 3.14.2.1). The logic tree is an expression of cause and effect relationship that built up in a particular time to cause an undesirable outcome to occur. These cause and effect relationships are validated with hard evidence as opposed to hearsay. The evidence leads the analysis, not the most vocal expert in the room. The strength of the tool is such that it can be used in court to support solid cases [56].

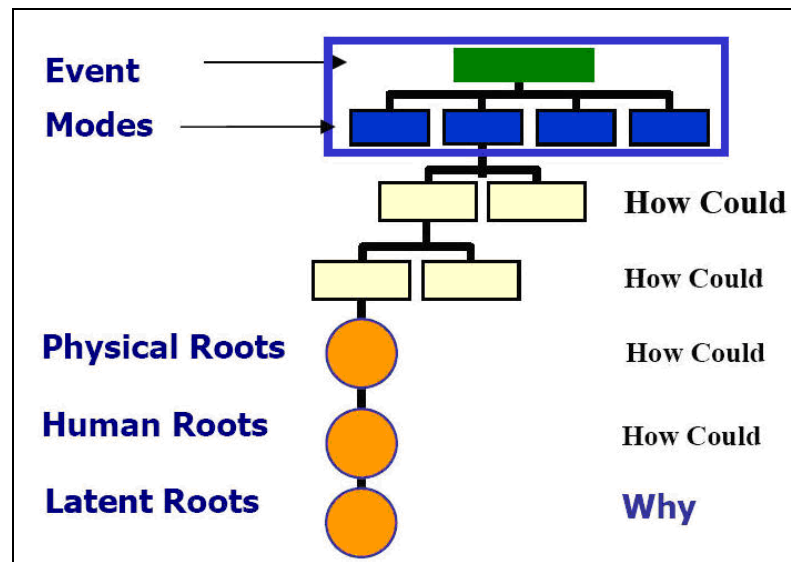


Figure 3.14.2.1. Structure of the PROACT Logic tree [10]

A logic tree starts off with a description of the facts associated with an event. These facts comprise what is called the Top Box (the Event and the Modes). Modes are the manifestations of the failure and the Event is ‘the least acceptable consequences’ that triggered the need for RCA. While we may know what the Modes are, we do not know how they were permitted to occur. So we proceed with the questioning of *how could* the Mode have occurred?

Usually investigators have been conditioned to ask the question *why* during such analyses. However, using this methodology the question used is *how could*? When looking at the differences between these two questions, we find that when simply asking *why* we are connoting a singular answer and to a point, an opinion. When asking *how could* we are seeking all the possibilities (not only the most likely), and evidence to back up what did and did not occur.

This questioning process is reiterative as we follow the cause-and-effect chain backwards. Simply ask questions, answer them with hypotheses, and use evidence to back them up. This holds true until we uncover the Human Roots or the points in which a human made a decision error. Human Roots represent errors of omission or commission by the human being. Either we did something we should not have done, or we did not do something we should have done. At this point we are exploring the reasoning of *why* someone made the decision they did.

This is an important point in the analysis, because we are seeking to understand why someone thought the decision they made was the correct one at the time. At this point in the analysis we do switch the questioning to *why*, because we are exploring a set of answers particular to an individual or group. Answers are what we call Latent Root Causes, or the organisational systems in place to help us make better decisions. The Latent Roots represent the rationale for the decision at the time that triggered the consequences to occur. These are called latent because they are always there, lying dormant. They require a human action to be triggered and when triggered, they start a sequence of Physical Root Causes to occur. This error-chain continues, if unbroken, to the point that it results in an adverse outcome that requires an immediate response.

The described logic tree approach is certainly cause-and-effect related, and requires evidence to back up what people say, and a depth of understanding of the flaws in the systems that contributed to poor decisions.

Conducting a Root Cause Analysis (RCA) can be a frustrating and time consuming task, yet it is invaluable to the cause of preventing recurrence of undesirable outcomes which potentially affect worker safety in an adverse way. Often the source of such frustration is the time pressure to complete a comprehensive RCA. The more time pressure to complete the RCA, the more short cuts analysts are likely to take to uncover all the root causes. Another issue companies are facing today is not effectively

capturing critical workforce knowledge and experience from older employees facing retirement, and few organisations are transferring that knowledge to newer and less experienced employees.

To meet these critical challenges, Reliability Center, Inc. (RCI) has developed a series of time saving industry related templates. This new product is the PROACT® Logic Tree Knowledge Management Templates™ that have been developed from completed analyses conducted in organisations worldwide. These unique one-of-a-kind PROACT® Logic Trees comprise events that have happened in numerous industrial settings across all departments, and include decades of researched industry experiences (see Fig 3.14.2.2).

The PROACT Logic Tree Knowledge Management Templates are an aggregation of experience associated with over 800 field investigations. The analyses have been thoroughly reviewed, and their results compiled to form this unique, single knowledge base. As analysts use RCI's PROACT Software and have exhausted their ideas for developing hypotheses, there are more opportunities available with the PROACT Logic Tree Knowledge Management Templates. These templates provide the analyst with the ability to see if there may be something they could have missed. While no knowledge base can ever cover all the potential variables of all potential events, analysts can learn from past experience to assist with preventing recurrences of similar events. The PROACT templates provide learning based on past experience and also a system of 'checks-and-balances' for the comprehensiveness of the analysis.

Some of the most successful RCA programmes are those which effectively capture and capitalise on workforce experience to determine the root cause of a problem. However, many organisations are failing to capture critical workforce knowledge and experience from older employees facing retirement, and few organisations are transferring that knowledge to newer employees. RCI's Logic Tree Knowledge Templates, now available within the PROACT Suite, are bridging the growing institutional knowledge gap, while helping users to hone their own logic skills, which are necessary to prevent equipment, process and human-related failures impacting on the safety, reliability and production of a company.

Significant features of PROACT® Software are:

- allows the user to quickly preview and select an appropriate template that most closely matches the conditions associated with any failure analysis;
- allows the user to quickly search the database, using either key words or the Table of Contents;
- allows the user to quickly drill down through the levels of detail that occur within any failure mechanism;
- provides multi-levels of detail to uncover related causes in the cause and effect relationship seen when analysing;
- allows for the deletion or modification of the graphic structure and text as new/ additional causes of the failure are identified and uncovered.

The templates database houses completed logic trees that are each drilled down to the REAL root causes of the undesirable events. While RCA templates alone cannot provide a list with all the answers (that is simply not possible), they do provide analysts with a number of different avenues to explore in order to broaden the scope of possibilities that could have caused the undesirable outcome.

The key to optimising the value of the templates is to use them as supplemental knowledge for the team. If the templates are used as the primary knowledge base for analyses, then there is the potential for the learning process to be cut short. The analysis team should always be encouraged first to conduct their own investigation, capitalising on their own knowledge and experience. After all hypotheses have been exhausted by the team, then the PROACT® Logic Tree Knowledge Management Templates™ do what they were designed to do: uncover more possible causes that the team may have overlooked.

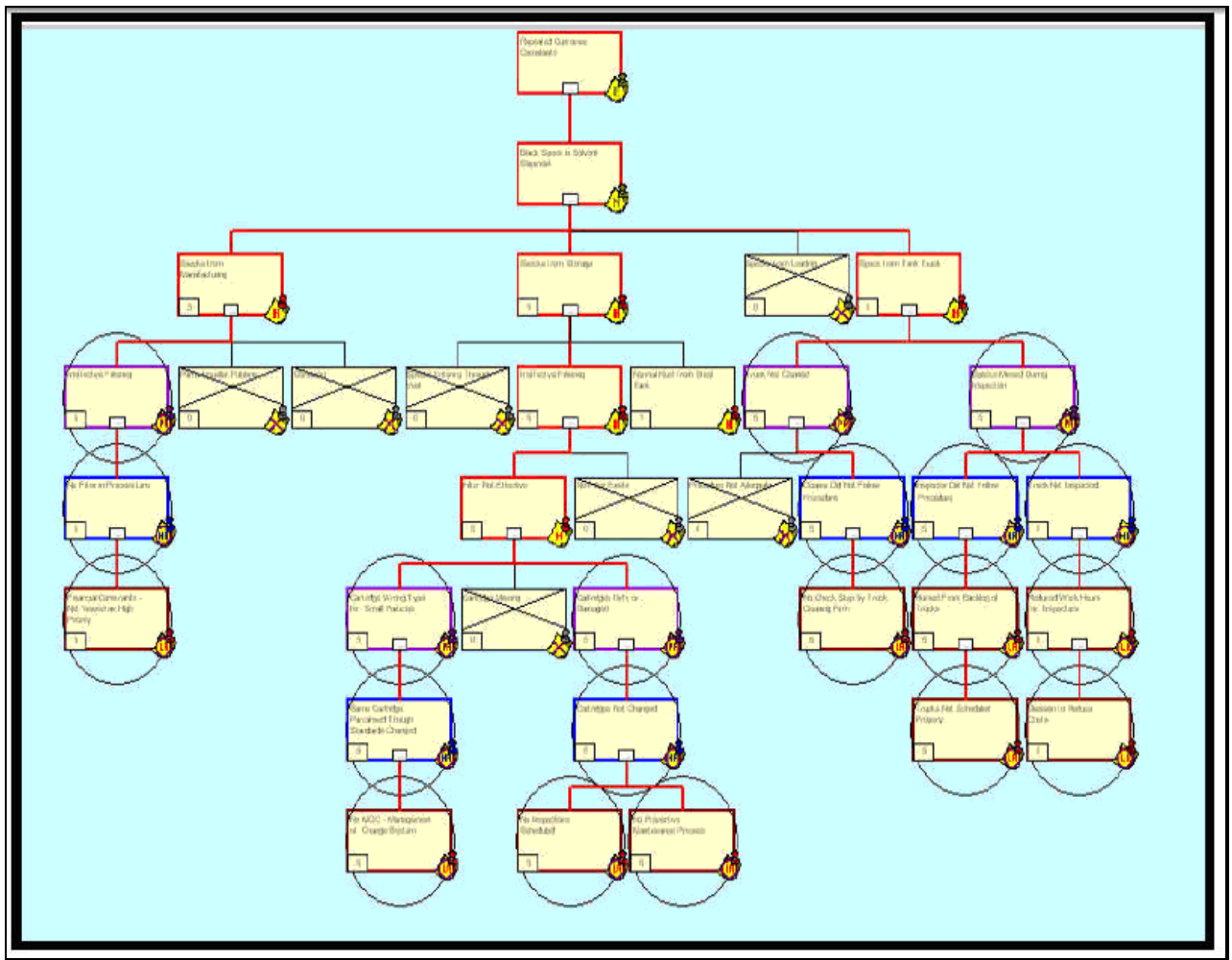


Figure 3.14.2.2. Example of the detailed PROACT® Logic tree

By using the PROACT® templates the analysis team can:

- validate team hypotheses;
- broaden considerations;
- identify team biases;
- illuminate frequently overlooked organisational factors (people, policy and management decisions);
- capitalise on past experience and use it in future analyses;
- quickly drill down through the levels of detail necessary to get to the REAL root cause;
- quickly search the RCA template database, using carefully developed key words, phrases and/or the table of contents;
- quickly reference multi-levels of detail to uncover the cause-and-effect relationships seen when analysing the undesirable outcomes.

The PROACT® Logic Tree Knowledge Management Templates™ are individual logic trees that can be searched and called upon for use in the PROACT RCA software program. Essentially these are experience templates aggregated from over 800 field investigations. The individual analyses have been combed through to remove redundancies, ensure accurate cause-and-effect logic, and to be developed in a way that makes them conducive to being searched in a very easy, disciplined and logical manner. The Templates are flexible enough to adapt to whichever RCA process the team is currently using (i.e. form-based, fishbone diagram, 5-whys, logic tree). RCI's PROACT® Templates can definitely help your organisation save time and reduce the RCA process uncertainties. The end result is that analyses can be

completed in a much more cost effective, efficient manner, while at the same time being as inclusive as possible in the results uncovered.

The analysis team is encouraged first to conduct their investigation utilising the knowledge of their team members. After all hypotheses from the team have been exhausted, then the Templates can be searched, using 'key word searches' to see if there are other suggestions from past analyses that the team may not have thought of. When such hypotheses are brought to the team's attention it often sparks new paths of thought (logic) and can lead to 'AHA!' moments because a paradigm might have been broken.

The Templates help to capitalise on past experience and use it in future analyses. When used properly, having access to such large volumes of specific past experience can increase the efficiency, effectiveness and accuracy of the analysis. Using the PROACT Templates also allows organisations to gain input from people outside of their organisation and industry. This is often not possible when trying to solve problems with team members alone, who are probably too close to the failure details to be objective. Having an injection of outside objectivity can certainly help any analysis. Some typical examples for which PROACT Templates available are shown in Figure 3.14.2.3.

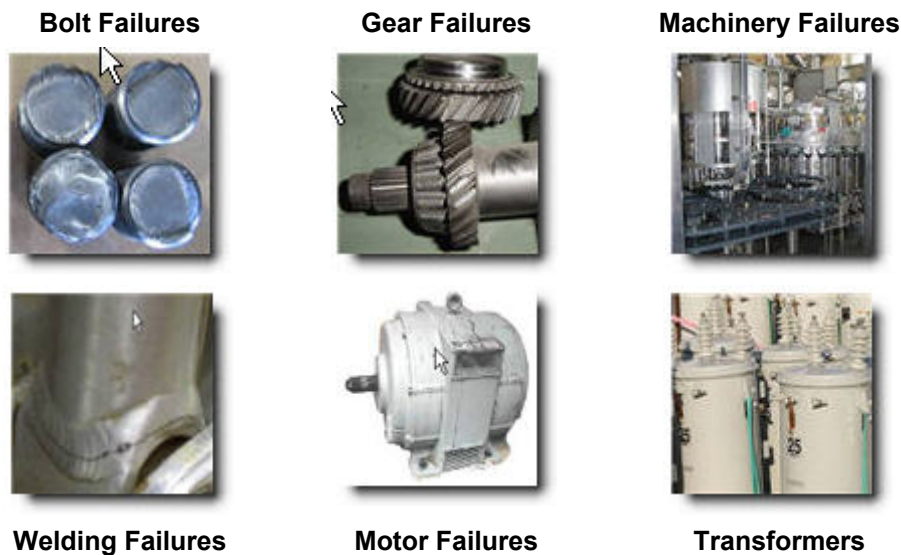


Figure 3.14.2.3. Examples of failures for which PROACT® Templates are available

3.14.3. RealityCharting®

RealityCharting® software is one of the best tools for event investigation developed for application of the Apollo Root Cause Analysis problem solving method [25, 57, 59, 60, 139]. The cause and effect diagramming process developed by Deen L. Gano in 1987 has historically been called Apollo Root Cause Analysis. The Apollo Root Cause Analysis problem solving method is based on the **Cause and Effect Principle**. This method seems to be unlike any causation model before it; its essence is described briefly in section 1.1.13. The principles of application of the RealityCharting® tool are explained in more detail below, with some examples.

The Cause and Effect Principle has four basic characteristics that allow us to understand reality in a simple, structured way. These four characteristics are as follows [25, 57]:

1. cause and effect are the same thing;
2. causes and effects are part of an infinite continuum;
3. every effect has at least two causes in the form of actions and conditions;
4. an effect exists only if its causes exist at the same point in time and space.

These are four rules that help define reality. Applying these rules means that every time we ask 'why' we must find at least two causes (third principle) and because cause and effect are the same thing (first principle), we must then ask 'why' again. Because each effect reveals at least two causes (usually many more), each of those two causes must reveal two more for a minimum of four more, and those four

become a minimum of eight and eight become 16, 32, 64, etc., on to infinity (second principle). Asking ‘why?’ leads to an ever-expanding set of causes, something like the branches of a tree, limited only by our knowledge of the subject or event. Some explanations of the **Cause and Effect Principle** are presented below.

Cause and effect are the same

Knowing that cause and effect are the same thing, only viewed from a different perspective in time, helps us understand one reason why people can look at the same situation and see different problems. They actually perceive different time segments of the same event. If we treat each perspective as a different piece of a jigsaw puzzle, we can stop the usual arguing and work on putting the different pieces together. For example, in Figure 3.14.3.1 below, we see that the primary effect is the ‘Injury’ and the first cause is a ‘Fall’. If we ask why ‘Fall,’ this cause has to be seen as an effect. That is, we cannot ask why of a cause, only of an effect, so ‘Fall’ changes from a cause to an effect. In a given event, we may each see the causes differently. You might see the ‘Fall’ as the problem effect, while the next person sees the ‘Leaky Valve’ as the problem effect. The reality is that cause and effect are the same thing, only viewed from a different point in time.

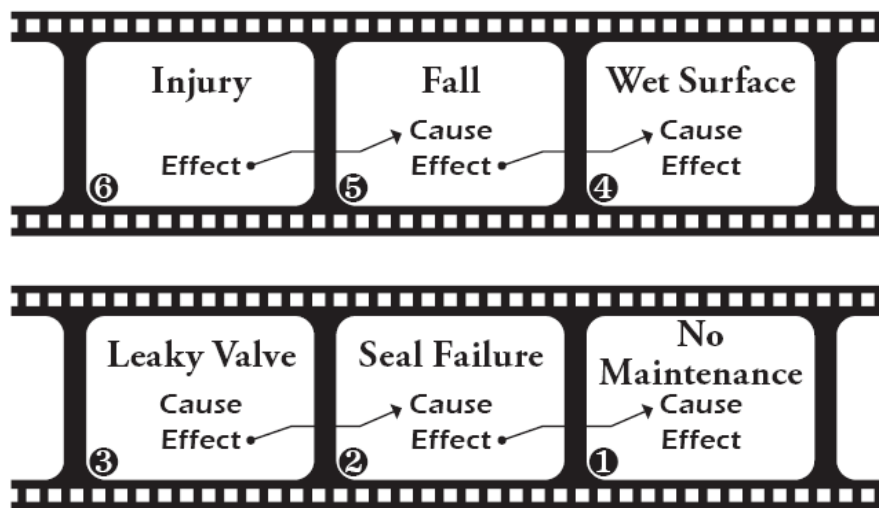


Figure 3.14.3.1. Example of a simple cause and effect chain [57]

Infinite continuum

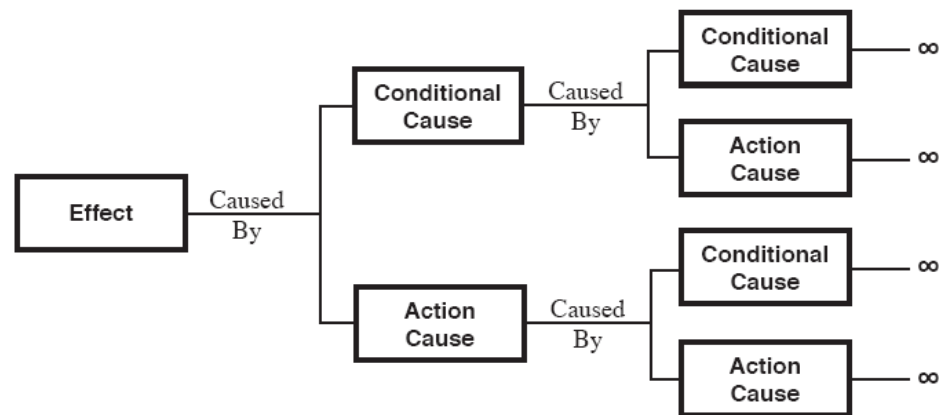
Knowing that causes and effects are part of an infinite continuum of causes helps us understand that, no matter where we start our problem analysis, we are always in the middle of a chain of causes. This helps us understand that there is no right place to start. Again, just as with a jigsaw puzzle, we can start the problem solving process anywhere and still end up with a complete picture. This avoids the usual arguments over who is right, and allows us to focus on finding causes. Again, in Figure 3.14.3.1, someone may be focused on the injury, while another is focused on the leaky valve. Instead of arguing over what the problem is, as we normally do, we can be aware that all causes are connected somehow in time, and we just need to work out what those connections are.

Each effect has at least two causes

Probably the most profound characteristic of the Cause and Effect Principle is that each effect has at least two causes, in the form of actions and conditions. This teaches us that every time we ask ‘why,’ we should find at least two causes, and because of the infinite continuum, for each of these causes we should find at least two more causes, resulting in four causes, and from each of these four causes we should find two causes, resulting in at least 8, and on to 16, 32, etc. See Figure 3.14.3.2.

With this understanding, we see that there is an infinite set of causes for each effect, limited primarily by our lack of knowledge. Presented with a reality that has a never-ending set of causes it is now easy to understand why we stop asking ‘why’ at an early age and pursue simpler strategies, like categorisation and storytelling. Designed to find the right answer, the human mind simply cannot deal with not

With this notion of the infinite set, it seems ridiculous to think we could just keep asking ‘why’ forever. In practice, however, the causal sets are rather short because we are not clever enough to know all the answers. Other natural limits come into play, and the process is very manageable as long as we are humble, and analyse the problem commensurately with its value.



Effects exist at the same point in time and space

From observation, we see that an effect exists only if its causes exist at the same point in time and space. For example, in Figure 3.14.3.3, an open fire exists because conditional causes came together with an action cause at a particular point in time and space. As we can see from this example, three conditional causes: oxygen, oily rags, a match, AND one action cause, a Match Strike, occurred at the same point. If these four causes did not exist at the same time and space, the fire would not exist. For example, if the oily rags were stored in a closed can, or if the match was struck at a different time, a fire could not exist. Understanding this characteristic helps us determine the validity of causal relationships.

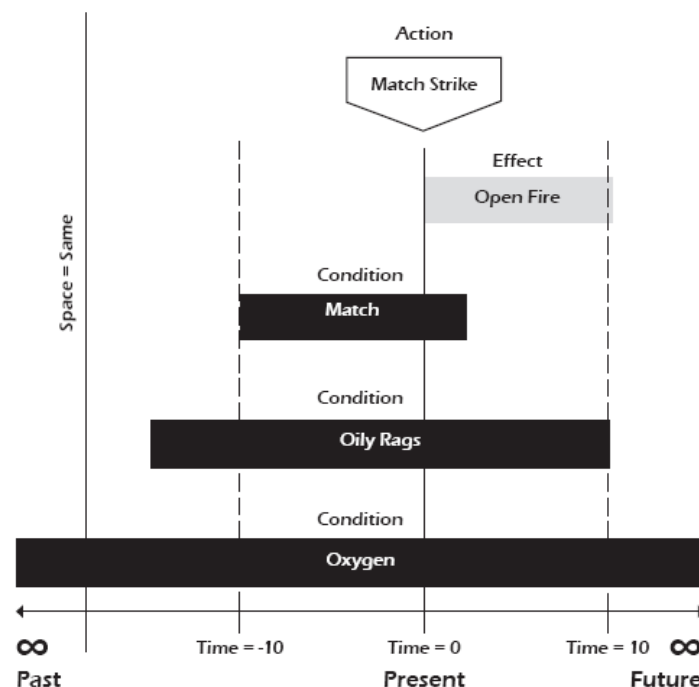


Figure 3.14.3.3. Example of time and space relationships

Using the cause and effect principle, the Apollo Root Cause Analysis (ARCA) method was developed. The four steps of the Apollo method are as follows:

Step 1: Define the problem by writing the:

- what: Primary Effect (Noun-Verb);
- when: Specific or Relative Time of the Primary Effect;
- where: Location in System, Facility, or Component;
- significance: Why you are working on this problem?

Step 2: Create a Realitychart:

- for each Primary Effect ask why;
- look for causes in Actions and Conditions;
- connect causes with 'Caused By';
- support causes with evidence or use a '?'
- end each cause path with a '?' or reason for stopping.

An example of the basic chart elements is shown on Figure 3.13.3.4.

Step 3: Identify effective solutions:

- challenge the causes and offer solutions;
- identify the best solutions — they must:
 - prevent recurrence
 - be within your control
 - meet your goals and objectives.

Step 4: Implement the best solutions.

Final Product. The product of steps 1 and 2 is a Realitychart, as in Figure 3.14.3.5. The iterative process of step 3 identifies effective solutions. And while obvious, step 4 is often not performed, so it is included as a reminder.

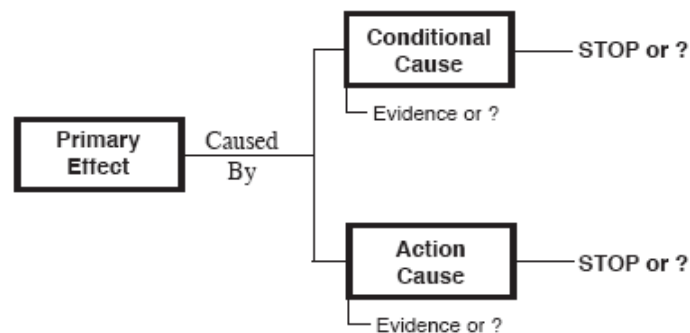


Figure 3.14.3.4. Example of the basic Realitychart elements

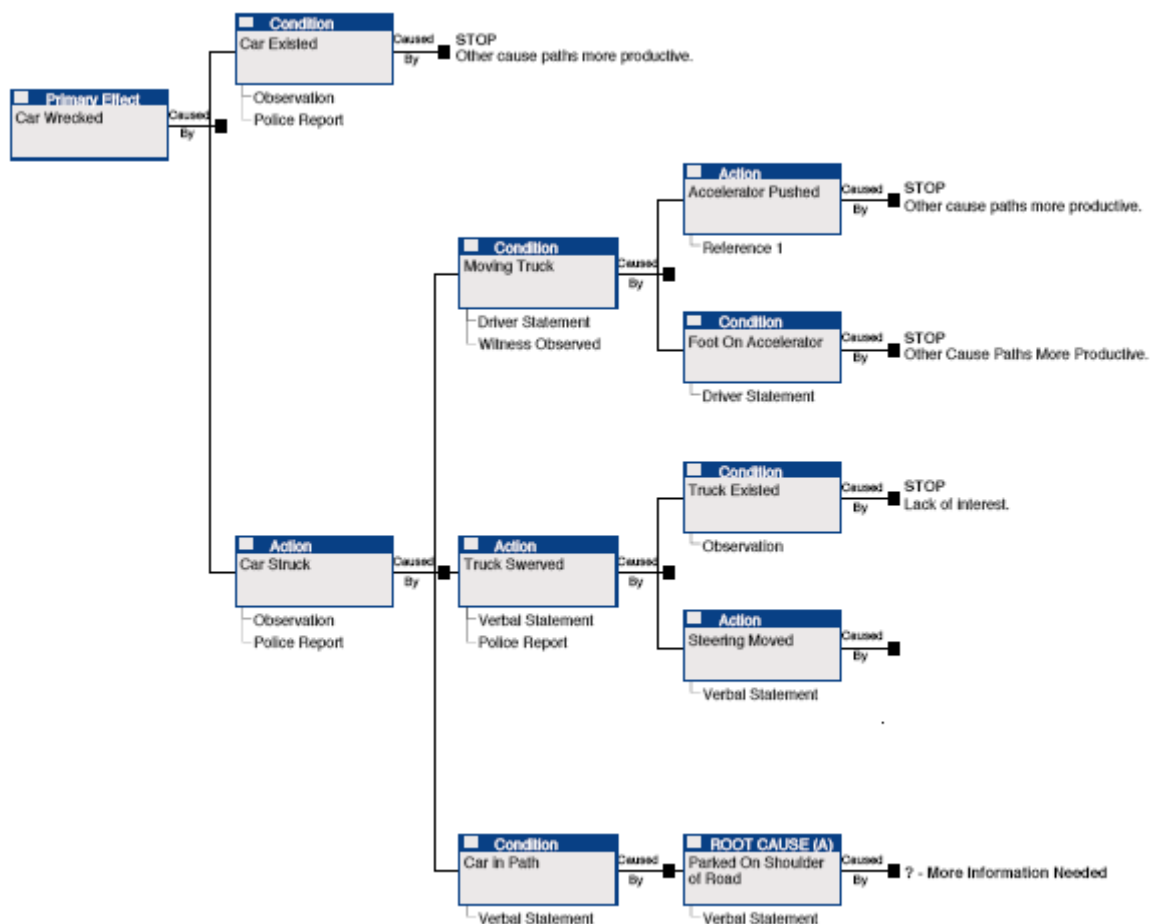


Figure 3.14.3.5. Example of a Realitychart for car wreck accident [57]

3.14.4. TapRoot®

TapRoot® System comprises a process and techniques for organising the facts of an event into a chronological order, investigation and analysis of these facts, identification of causal factors, determination of root causes and development of corrective actions to solve problems. The process and tools are described fully in the TapRoot® Book [20, 110].

The TapRoot® System has been used since 1991 for the investigation of chemical and petrochemical industry process safety incidents. A limited survey, conducted in 2001 by the Center for Chemical Process Safety, showed that it was the root cause analysis system most used by its members. The TapRoot® System also has broad use in a variety of other industries, including healthcare, transportation, aerospace, manufacturing, telecommunications, oil exploration and production, pulp and paper, and construction. These industries use TapRoot® to:

- improve process safety;
- improve industrial safety;
- improve product and service quality;
- reduce operations and maintenance errors;
- increase service and equipment reliability.

The TapRoot® System combines inductive and deductive techniques for systematic investigation of the fixable root causes of problems. The system can be used either reactively to prevent the recurrence of events, or proactively to find ways to improve performance before a major process safety accident occurs. It goes well beyond the simple technique of ‘asking why’ or the standard techniques of cause and effect (sometimes known as fishbone diagrams) or fault tree diagrams. The TapRoot® System has embedded intelligence, so that the system helps investigators find root causes that they may not have previously had the knowledge to identify. This allows the TapRoot® System to be simple enough for

application to everyday problems by people in the field, and yet robust enough for even the most complex major process safety accident investigation.

Unlike other common root cause techniques, the TapRoot® System is an investigation system. This means the tools and techniques in the TapRoot® System are used in all phases of an investigation - from initial planning, through the collection of information and root cause analysis, to the development of corrective actions and the presentation of an investigation to management or other interested parties. The system is supported by patented TapRoot® Software that makes presenting information easy and logical, and provides an incident/root cause database capable of showing trends and a corrective action management database.

The TapRoot® System is based strongly on the concept that each error could be categorised and learned from [110]. According to this system, the investigation of each incident should start by attributing each causal factor of an issue to one of the four initial categories: a) human performance difficulties; b) equipment difficulties; c) natural disaster/sabotage; d) other. Analysis then goes further, digging deeper by selecting or eliminating the appropriate more detailed subcategories to find root causes.

The TapRoot® categorisation system for human performance related problems was developed around proven human factors theories and models, combining these models with practical understanding of how work was accomplished, and how investigations were performed. As a background to the categorisation system, the proven core competencies (good practices) were selected, which can be used to prevent (or at least greatly reduce) human error. These best practices include: a) good procedures; b) good training; c) good quality control; d) good communications; e) good management systems; f) good human engineering; g) good work direction. These best practices are the basis of human performance technology that, when carefully applied, produce highly reliable human performance. In the TapRoot® System they are treated as basic cause categories. Weaknesses in these areas lead to increased human error. Thus, if one can identify the weakness in a particular core competency – or perhaps several of the core competencies listed above – one can find the missing best practice or knowledge that will lead to improvement of performance when the weakness is corrected.

To help the investigators (especially non-human factors experts) in selecting the appropriate Basic Cause Categories to analyse, the Human Performance Troubleshooting Guide, consisting of 15 Questions, was created and added to the front of the TapRoot® Root Cause Tree®. In an effort to improve the troubleshooting and Root Cause analysis of equipment, the Equifactor® Equipment Troubleshooting System (including 2 000 equipment troubleshooting tables) was developed and added to the TapRoot® System. So, TapRoot® became a powerful, highly tested and proven complete expert system for finding the root cause of human performance and equipment-related problems, fully supported with adequate software modules [110]. It could be used successfully in both a reactive and a proactive manner. The list of TapRoot® System techniques includes: SnapCharT®, Root Cause Tree®, Equifactor®, Safeguards Analysis, Change Analysis, and Critical Human Action Profile [20, 110].

Event investigation using the TapRoot® System is performed by applying a seven-step sequential procedure, where each step is realised by means of adequate software tools. These seven steps are (see Figure 3.13.4.1):

1. plan investigation – get started;
2. determine sequence of events;
3. define causal factors;
4. analyse each causal factor's root causes;
5. analyse each root cause's generic causes;
6. develop and evaluate corrective actions;
7. present/report and implement corrective actions.

The first step in the TapRoot® process requires the identification of an undesired event [63]. Usually this is an accident or incident, but in some cases it can be a particular process that may not be performing well. The choice of an undesired event may differ from the obvious, depending on the views or responsibilities of the investigator.

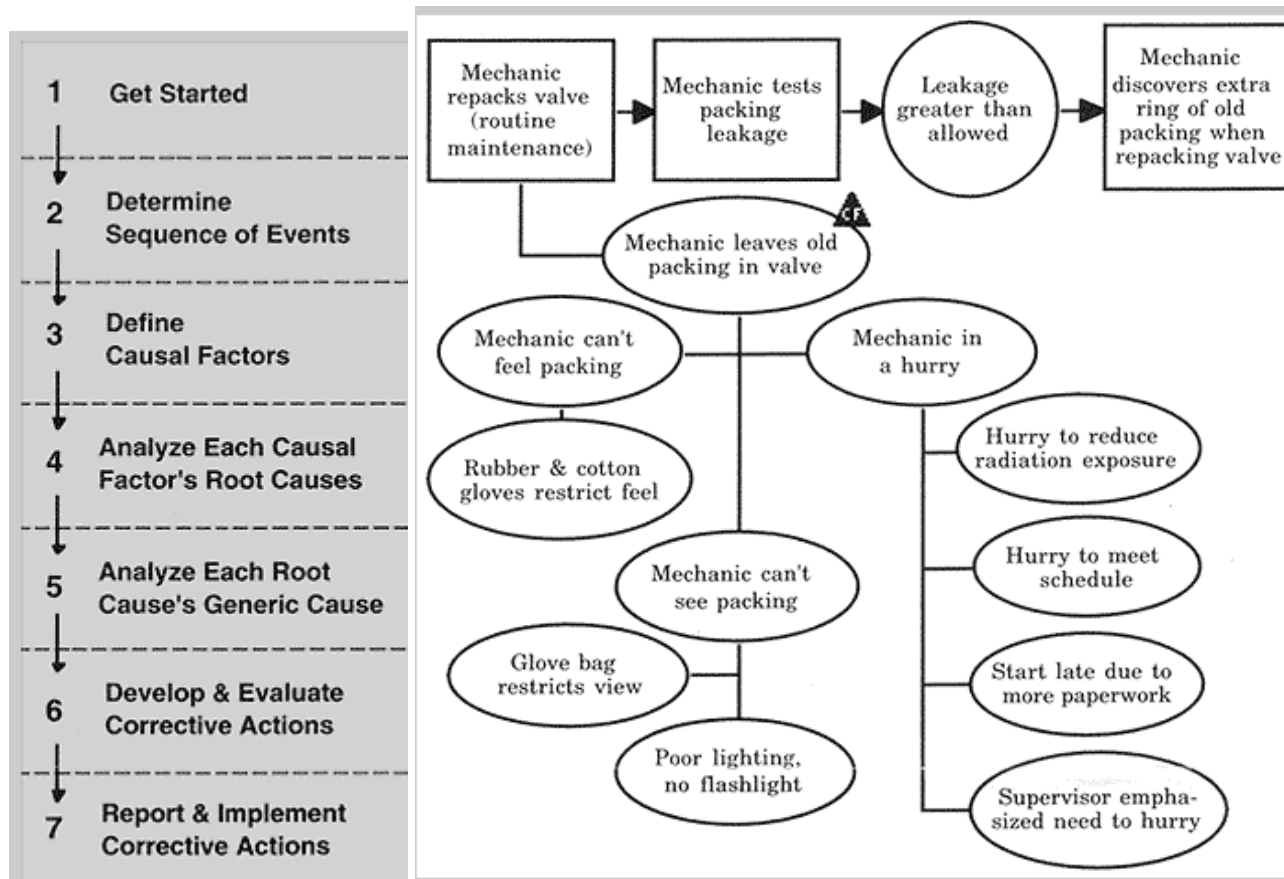


Figure 3.13.4.1. The seven-step sequential procedure of the TapRooT® System and an example of graphical representation of an event performed using SnapCharT® [145]

After determining the undesired event, the facts are arranged in chronological order, from the first relevant action to the undesired event, using a graphical representation known as a SnapCharT®. The SnapCharT® consists of actions, something that can be observed happening, and conditions, things that modify or explain an action. Once completed, SnapCharT provides a valuable visual display of the event, and helps ensure that all the pertinent information has been collected. Then each action or condition is subjected to the question: 'If the problem or condition were corrected, could that have prevented the event from occurring or significantly reduced the event's consequences?' Any items with answers 'yes' are considered as causal factors of the undesired event. Each one of these causal factors is analysed, using a TapRooT® Root Cause Tree®, which asks 15 yes-or-no questions. Depending on the answer to these questions, basic cause categories, and eventually root causes, are assigned to the causal factors. The software also offers assistance in developing corrective actions.

Since reactive improvement is the most common strategy to improve performance, the TapRooT® System is strongly recommended for use in a proactive manner. If a proactive improvement programme is implemented and TapRooT® process is used to analyse the causes for deviations and issues, that root causes can be corrected before an accident occurs.

For investigation of near-misses and low level incidents that does not provide enough return-on-investment to warrant a full seven-step root cause investigation, an investigator might apply a simplified TapRooT® process by skipping, simplifying or combining some steps in the seven-step sequence, and developing only easy-to-implement corrective actions, for only the most significant root causes [110].

TapRooT® Advantages. According to opinion of the TapRooT® authors, there are eight primary reasons why this process seems to be superior to most of the above listed tools [142]:

1. It is a closed loop process, in that it uses the Snapchart® for problem definition (define), the root cause tree and identification of trends for root cause identification (measure and analyse), and the corrective action process to define well-rounded problem solutions (improve).
2. The Snapchart® is time-based, in that it shows the sequence of events leading up to and following a given problem. This tool helps the user identify a more complete set of events and conditions that led to a given problem's occurrence.
3. The process is based on a set of well-developed operational definitions and questions, which are based on years of research and application, and which discourage the user from relying primarily on their opinions when selecting a root cause or causes.
4. The process encourages the identification of generic causes which, if corrected, will prevent similar problems from appearing in other parts of the organisation, or in other products or services in the product/service line.
5. The process software contains hundreds of possible corrective actions that have been used by hundreds of companies, to correct and prevent the problems that result from both individual and generic causes.
6. The process is grounded in human factors theory, which supports the fact that people are the key to organisational success, and most often the source of most problems, due to the design of the systems and processes they use, and the decisions they make as they do their jobs each day.
7. The software's design and content encourage and enable the individual problem solver, or a team of problem solvers, to keep their efforts focused and organised, due to the existence of the dictionary, corrective action helper, a highly visual problem definition (Snapchart) and root cause analysis process, and the linkages between the Snapchart causal factors, the root causes selected, the identified corrective actions, and the assortment of incidents analysed.
8. The results that event investigators could get from using this tool, versus the time invested to use it, will almost always outweigh the results they could get from the time invested using majority of the above tools – the time required per tool application is not much greater, if any, and the quality of results is far superior. In most cases, a couple of hours of use with most of the above tools would only give you a list of possible causes – in the same amount of time, the TapRooT® process will give you a clearly defined problem, a focused set of root causes, and a sound mix of corrective actions.

It has been clearly demonstrated from results of investigations that use of the Taproot® flowcharting process has been successful in helping to capture all relevant data, allowing for correct identification and management of causal factors [141]. This conclusion is based on the following premises, relating to the performance of participants in the process, bearing in mind that many of the incidents investigated are very stressful/traumatic for the persons involved. The Taproot flowcharting process:

- decreases the complexity of material, reduces the need to remember large amounts of information;
- tracks discussion, assists with the externalising of the incident and on problem focus;
- confirms and ensures a common perception of events.

Other observations which have been made about the outcomes of the process relate to the fact that in some ways the process of building the flowchart serves as a debriefing process. This is evidenced by the operation of the Taproot system in that it:

- minimises blame, normalises responses and concerns;
- allows people to express and talk about their perspective of the incident;
- adopts an exploratory rather than an investigative process (although it is an investigative tool);
- provides people with increased information about the event;
- builds supportive networks;
- helps people become problem focused rather than emotionally focused.

For significant and high risk issues, the recommended RCA method at Lawrence Berkeley National Laboratory (LBNL) is TapROOT®, which encompasses Barrier Analysis, Change Analysis, and Event and Causal Factors Analysis [143].

4. Comparative analysis of effectiveness and applicability of event investigation methodologies, methods and tools

4.1. General considerations

Different methodologies, numerous methods, tools and techniques for event investigation have been developed and implemented in high-risk industries such as construction, nuclear power generation, aviation, chemical, hydrocarbon processing etc., using complex technological systems, in recent decades. These activities have obviously been influenced by the ever greater focus on safety issues, the increasing potential consequences of accidents, the accumulation of operational experience and lessons learned. Some of the available methods and tools are based on original approaches; others, that were developed later, are derived from parts of the above mentioned techniques, or some combination of these.

In general, there are currently four main types of methodologies which can be used for nuclear event investigation: RCA, PSA, deterministic analysis and safety culture impact assessment [23]. The existing uses indicated for these types of methodologies can be briefly summarised as follows:

- Root Cause Analysis remains the most important methodology for incident investigation and qualitative evaluation; it serves for identifying, analysing, eliminating or mitigating the root causes and causal factors of an undesired outcome. It helps organisations to identify risk or weak points in processes, underlying or systemic causes and corrective actions. RCA enables people to understand, recognise and discuss the underlying beliefs and practices that result in poor quality/safety in an organisation. Information from RCA, shared between and among organisations, can help to prevent future events. RCA is moving beyond the field of nuclear operations into the general body of knowledge used for diagnosis and prevention of problems by quality management, environmental, health and safety professionals.
- Probabilistic Safety Analysis is a powerful methodology for quantitative risk assessment, analysis and evaluation of the safety significance of real or potential events with different scenarios of evolution, supporting both the design and the safety management and control of a NPP right through its service life.
- Deterministic analysis is based on the analytical evaluations of physical phenomena occurring at NPPs, and is best suited for events with rapid development of occurrences. Demonstrating that the plant is capable of meeting any authorised limits, it supports the designing and licensing of a nuclear power plant, and helps better understanding of the phenomena occurring during a specific event and identification of the direct and contributing causes.
- Safety Culture evaluation, impact assessment and the subsequent improvement, is an excellent approach for development of long term corrective actions. Moreover, it seems to be the most effective mechanism for proactive safety improvement, by means of removing or fixing the root causes of events (contained and hidden in so called the organisational climate– a system of behaviours, espoused values and underlying assumptions, which is equivalent to a safety culture) well before they happen.
- All four of the above mentioned methodologies complement each other, adding extra value to the thoroughness and comprehensiveness of analysis, the quality and reliability of results, the conclusions of event investigation, and the effectiveness of the corrective actions developed.
- Not all events are alike, and a careful consideration should be given to which methodology to use for evaluation of a particular event.

According to data from WANO [103], the most frequently used method at nuclear plants is the event investigation analysis (HPES), based on INPO's human performance enhancement system. Other methods often used are IAEA's ASSET teams, the management oversight and risk tree analysis (MORT) and, recently, safety through organisational learning (SOL), with a high emphasis on

organisational factors. Apart of the first few commonly accepted methods, application of others, presented in chapters 2 and 3 seems to be differentiated both territorially and by specific industries. For example (see Figure 3.1.1), in the US, besides HPES, HPIP and HPEP, commonly used in the nuclear industry, TapRoot®, Realitycharting®, Reason® and PROACT® are very popular [10, 20, 25, 110, 136, 139]; SOL-VE has been adopted as the standard procedure in Swiss and German nuclear power plants [115-117]; STEP and TRIPOD are widely used in Scandinavian countries [71, 102, 133]; HFIT is used in the UK offshore oil and gas industry [61]; K-HPES, KAIST and CAS-HEAR are used in South Korea [14, 17, 65]; and J-HPES and JOFL are used in Japan [130, 131], etc.

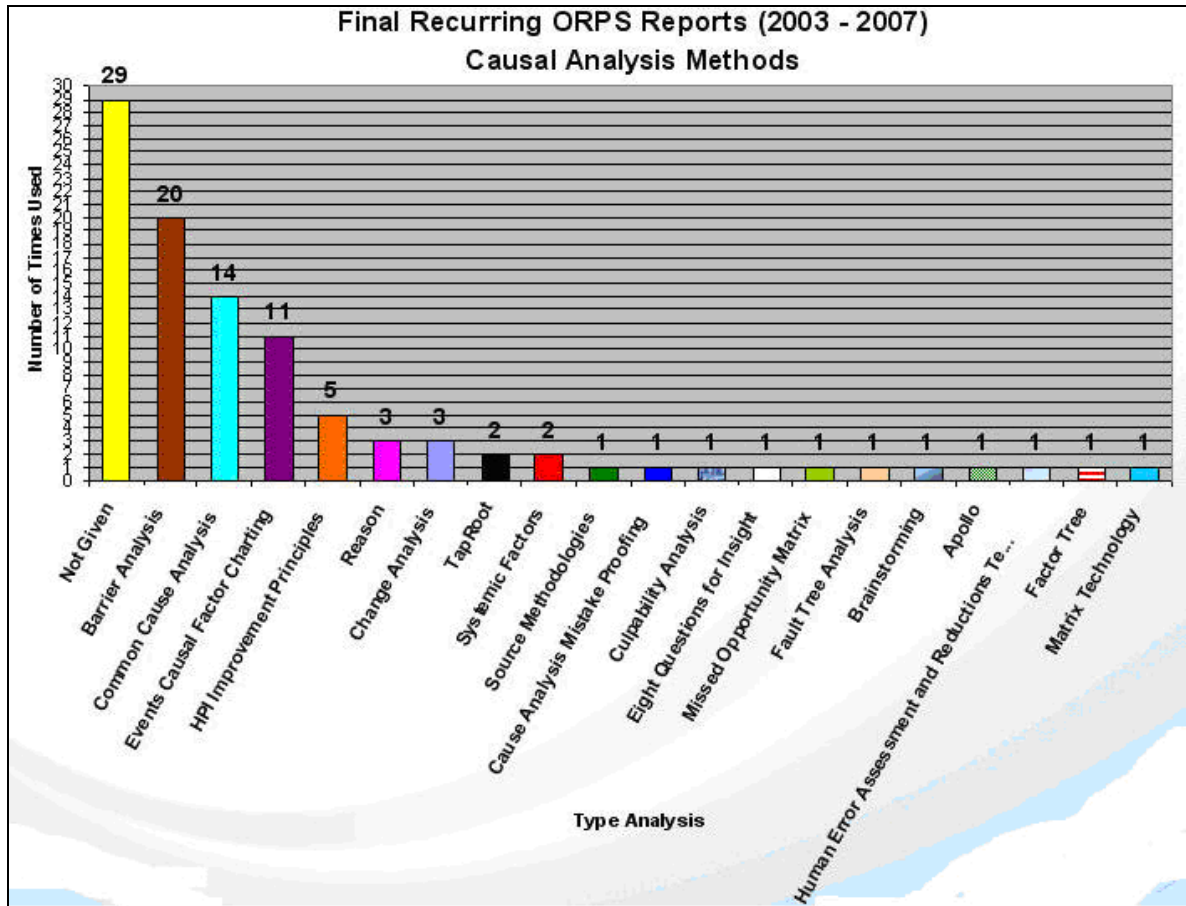


Figure 4.1.1. Preferred root cause analysis methods and tools in the Department of Energy complex of US [52]

The key similarity between all root cause analysis methods is a basic principle - recognition that controlling causes translates into controlling the problem. Apart from this, RCA methods vary greatly [29]. Due to the existing confusion regarding terms and definitions (free interpretation of the definitions of ‘method’ and ‘tool’) both of these groups are usually analysed together. However, the majority of instruments for event investigation could be attributed to at least one of the following groups: a) categorisation based; b) check list based; c) tree based; d) software based; e) the cause and effect principle based. Such grouping should facilitate the identification of some common advantages, disadvantages and particularities for employment, inherent in RCA methods and tools attributed to specific group.

Categorisation based RCA methods and tools.

Tree Diagrams and Categorisation Schemes based root cause analysis tools are very common and go by many names, such as Ishikawa Fishbone Diagram, Management Oversight and Risk Tree Analysis (MORT), Human Performance Evaluations System (HPES), and many other commercial brands. Most

RCA methods use some kind of categorisation scheme or checklist format (a predefined list of causal factors arranged like a fault tree) to help us find the root causes [25, 57, 59, 60]. For example, one of the main, basic, widely used RCA method, HPES, and typically other methods, have mainly envisaged classifying individual incidents into different patterns by reference to a check-sheet, on which previously selected items are listed in respect of the 5 W's and 1 H (When, Where, Who, What, Why, How). These methods thus involve no logical analysis, and sometimes do not require the provision of a procedural manual to guide personnel in practical application [25, 38]. These methods and tools postulate a prescribed set of potential causal factors, and this often leads to important underlying causal factors being overlooked. Another shortcoming of these methods and tools is that only scanty information is left on record concerning the concrete details of an incident, and this becomes a serious obstacle when, subsequently, the events that had occurred in the incident need to be traced in reviewing a previous incident. For this reason, the practical utility of such methods and tools is considered to be limited mainly to deducing, through statistical treatment, the salient characteristics common to a multiple number of incidents. Such treatment would only be effective for dealing collectively with incidents of analogous nature, occurring repetitively and relatively frequently.

Following the basic principle, that controlling causes directly transfers into controlling the problem, event investigators often mistakenly focus on finding root cause(s) prior to finding solutions. Conventional wisdom holds that causes are linear, and at some point in their linear progression (A caused B and B caused C, etc.) we will find a root cause, probably the fifth cause that, if removed, changed or otherwise controlled, will prevent recurrence. This common but misguided belief fails to take on board the cause and effect principle that dictates a non-linear branched set of conditional and action causes that branch and expand until we reach our collective point of ignorance. By applying the comprehensive categorisation scheme properly, it is easy to find the root cause of the event; but it is not the root cause we seek, it is effective solutions, and we can only know the root causes after we know which solutions will prevent recurrence. This misunderstanding is one of the main factors that cause the continuing succession of repeat events that we see each year.

The purpose of problem solving is to find effective solutions, not the root cause. Contrary to the approach of nearly every incident investigation method in use today, the problem solving methodology should focus first on the cause and effect relationships and then on effective solutions, and root causes are only identified after these solutions are committed to. Having clarified this, it can now be stated that the only value that categorisation methods provide is a mental reminder of the possible cause categories in which we may find causes. It is this memory jogging, and the specific knowledge of the investigators, that comes up with an effective solution, not any design of the categorisation scheme.

A sad consequence of categorical methodologies is that they lend themselves to being computerised. Once a categorical set is established it can easily be put on a computer that allows the user to turn off their brain and just follow the bouncing ball. Cause-tree software looks something like the following:

To identify the root cause, answer the following questions:

Failed Component Is?: Pump? Motor? Compressor?

Answer: Pump

Component Failure?: Bearing? Seal? Rotor?

Answer: Seal

Failure Mode?: Wear? Abrasion? Tear?

Answer: Tear

Cause of Failure?: Burr on shaft? Debris? Exterior Force?

Answer: Debris

Root Cause: Debris in fluid

Solution: Install a strainer on the flushing line.

By virtue of a documented logical set, as shown above, a great illusion is created by the fact that it makes sense to the reader — it has been observed before, and familiarity makes it 'right.' Being solution oriented and highly biased, we reason that it would be a waste of time to consider other possibilities when a favourite solution is to hand. Because this logic takes us to a favourite and seemingly successful

solution, the illusion is compelling. The expression ‘seemingly successful solution’ is used because we erroneously believe that past success will always guarantee future success. And it will, if we know all the cause and effect relationships. But when we only identify a few of the categorical causes, we delude ourselves into thinking we know what really happened. By fixing the causal chain together, as in the example above, the infinite set of possibilities, such as how the pump was maintained, operated or designed, is ignored.

According to the author of [25], Dean L. Gano, there are at least seven major weaknesses in the Categorisation Schemes and Tree Diagrams based model:

1. A Tree Diagram is clearly not a ‘Cause and Effect Chart’, as the proponents of these methods would have us believe. It simply does not show all the causal relationships between the primary effect and the root causes. The theory behind these Tree Diagrams is that, because all events have certain causal factors, we can find the root causes by looking for them in the pre-defined set provided. And while it can help jog the mind into certain lines of thinking, it fails to provide a causal understanding of the event.
2. No two categorisation schemes are the same, nor can they be, because we each have a different way of perceiving the world. Therefore, we have different categorical schemes, and hence the reason why there are so many different schemes being sold. When asked to categorise a given set of causes it is very difficult to find a consensus in any group. For example, what category does ‘Pushed Button’ fall into? Some will see this as hardware; some will see it as people; and some will see it as procedure. Using any of these categorisation methods to find a root cause is usually followed by some time wasted, debating which is the correct category.
3. The notion that anyone can create a list of causal factors that includes all the possible causes or causal factors of every human event insults our intelligence. Ask yourself if your behaviour can be categorised in a simple list, and then ask if it is identical to every other human on the planet. The very fact that a method uses the term causal ‘factor’ should be an indication that it does not provide a specific actionable cause but, rather, a broader categorical term, representing many possible specific causes. At best, it acts as a check list of possible causes for a given effect, but it does not provide any causal relationships. Since this error in logic is very contentious with those who use these methods, it begs the question as to why these methods seem to work for them. It was discovered, after talking with many people who claim success in using these methods that the approach works, in spite of itself, by providing some structure for the experienced investigator, whose mind provides the actual causal relationships. It is not the methodology that works, but the experience of the investigator, who is actually thinking causally. And while these methods seem to work for the experienced investigator, they are still incapable of communicating the reality of causal relationships. This inability to communicate effectively prevents the synergy among stakeholders which is necessary to fully understand the causes of the event, and which is required to get buy-in for the solutions.
4. These models do not provide a means of showing how we know that a cause exists. There is no evidence provided to support the causal factors in the list, so it is not uncommon for causal factors to be included that are politically inspired, with no basis in fact. With these methods, the best storytellers or the boss often get what they want, and the problem repeats. This may help explain why many managers and self-proclaimed leaders like this method.
5. Categorisation schemes restrict thinking by causing the investigator to stop at the categorical cause. Some methods reinforce this fallacy by providing a ‘root cause dictionary,’ implying that it is a well-defined and recognised cause.
6. Categorisation methods perpetuate the root cause myth, based on the belief that it is a root cause we seek, and solutions are secondary. Because these methods do not identify complete causal relationships, it is not obvious which causes can be controlled to prevent recurrence; therefore, you are asked to guess and vote on which causal factors are the root causes. Only after root causes are chosen are you asked to identify solutions, and without a clear understanding of all causal relationships between the solution and the primary effect, this method works by chance, not by design.

7. As mentioned earlier, some of these methods provide what is called an ‘expert system’, and include solutions for a given root cause. Expert systems can be quite useful for a very specific system, such as a car or production line, where 99% of the causal relationships are well known, and have a long history of repeatability. To presume that one could provide an expert system applicable to all event-based problems seems to be incredibly arrogant. In light of what is now known about the infinite set of causes that governs reality, how could anyone presume to know the causes for all systems, how they interrelate, and what constitutes the best solution for every organisation or individual? Beware the salesperson.

Check list based RCA methods and tools.

Many event investigators simply use check list or form-based RCA [56]. This is basically a ‘one size fits all’ mentality. It is root cause by the numbers, similar to painting by numbers. The same questions are asked, no matter what the incident, and opinions are input as acceptable evidence. Check lists are often provided which give people the false sense that the correct answer must be within the listed items. No ‘pick-up from a list’ RCA process can ever be comprehensive enough to consider all the possibilities that could exist in each working environment at all times. However, the innate human tendency to follow *the path of least resistance* makes using pick-up lists very attractive.

Many people choose to use form-based RCA systems because the regulatory authority seeking compliance provides them free of charge and *suggests* they be used. The paradigm is that ‘we are using their forms so we will have a better chance of complying if we use them’. This may indeed be true, but does not mean that the analysis was comprehensive enough to ensure that the undesirable outcome will not recur. Compliance with regulations does not necessarily ensure operational reliability!

The shortcomings of check-sheet based systems are:

- (1) The check-sheet system mainly indicates only superficial and direct causal factors, and is liable to overlook those that are of indirect or potential character, including underlying causal factors.
- (2) Only previously applied countermeasures are prescribed, since no provision is made for freshly incorporating preventive countermeasures that have not been practised before.
- (3) Insufficiency of recorded information on the sequence of events that took place in an incident, including the human activities that were involved, which prevents deriving the requisite information on what to learn from the incident from the analysed results, when the results of analysis are later reviewed.
- (4) Difficulty of plant personnel who are not knowledgeable about human factors, in conducting in-depth analysis and evaluation of incidents, in the absence of a practical technique of analysis and a manual to guide such operations.

Tree-based RCA methods and tools.

The tree-based methods are mainly used to find cut-sets leading to the undesired events. In fact, event tree and fault tree analysis have been widely used to quantify the probabilities of occurrence of accidents and other undesired events leading to the loss of life or economic losses in probabilistic risk assessment. However, the usage of fault tree and event tree analysis is confined to static, logic modelling of accident scenarios. In giving the same treatment to hardware failures and human errors in fault tree and event tree analysis, the conditions affecting human behaviour cannot be modelled explicitly. This affects the assessed level of dependency between events. No doubt, there exist techniques such as human cognitive reliability to reconcile such deficiencies in the fault tree analysis, and new methodologies that model such responses have emerged [45].

Practice shows that regulatory compliance with RCA guidelines does not ensure operational reliability. Since some organisations focus on improving safety from the formal administrative side and ignore real issues, passing the regulatory audit of event investigation practices does not ensure that the operation is any more reliable.

Software based RCA methods and tools.

RCA software – is it necessary for effective root cause analysis?

Some of the aforementioned tools and techniques can be applied manually, using a paper-based system; however, currently most are automated, using a form of software. A growing number of Root Cause Analysis processes are supported by RCA software. It should be emphasised that software IS NOT a

panacea for any analysis. If the analyst does not understand proper investigative methodology and technique, software will be of little value. We need to be careful not to oversell the benefits of software in effective problem solving – and in many cases, RCA software actually also has some disadvantages and drawbacks [55, 56].

Advantages and weaknesses of both approaches are well known. The paper-based approach leads to a double handling of data and a time lag for the re-input of data collected into the appropriate program before dissemination.

The primary value of the software-based approach is the enhanced process of documenting, receiving, storing, processing and disseminating information. Software can eliminate the double handling of data related to any analysis. Experience shows that, on average, this cuts analysis time by half (see Figure 4.1.2).

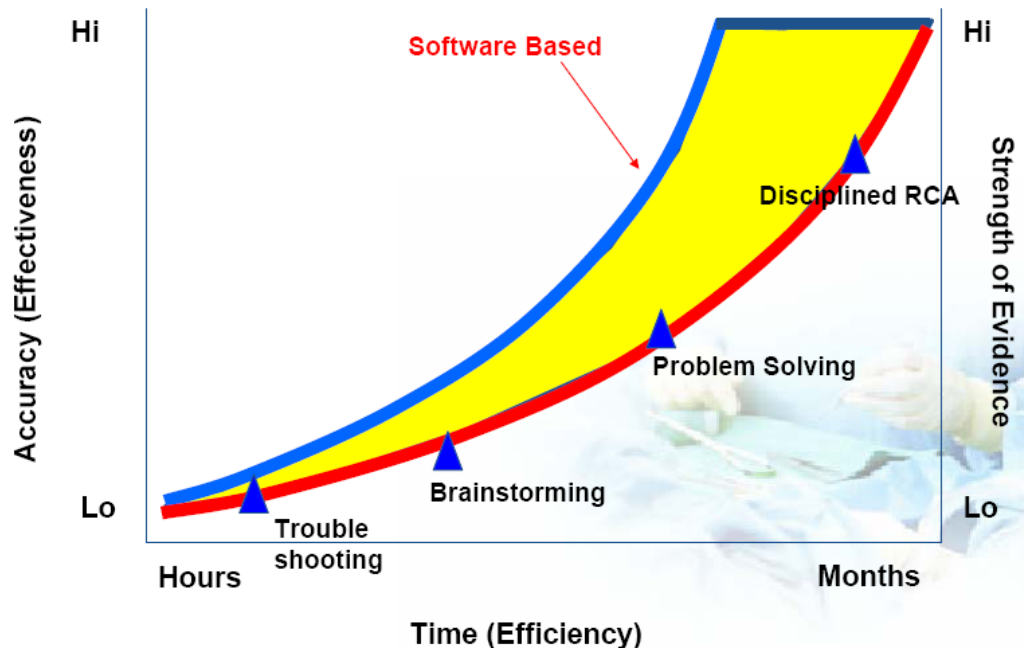


Figure 4.1.2. Accuracy and efficiency of different root cause analysis tools [52]

However, with all advantages there come some disadvantages. Technology itself can intimidate people and create a resistance to their using it. Regardless of the analytical process used, the tools employed in the execution or the technology used, if the analyst using the tool is not properly trained, the tool will not function to its fullest capability. Other drawbacks to the software-based RCA process are:

1. Implementation of effective problem-solving through Root Cause Analysis techniques represents, for most organisations, a significant change in their way of thinking, and a significant cultural shift. These fundamental changes cannot be effectively brought about simply by purchasing a software package, even though many technocratic organisations are tempted to believe that a technological solution (such as a piece of software) will solve their problems.
2. If conducting Root Cause Analysis requires the presence of software (and associated access to a PC or terminal), then you are probably missing out on a large number of opportunities for problem solving that could be applied by your tradesmen/technicians/mechanics and supervisors while they are in the field. There are generally many smaller problems that can be solved more or less immediately, simply through the use of a simple, but effective, Root Cause Analysis problem solving process and a pocket notebook. Shop-floor personnel are unlikely to use a process that requires them to log on to a terminal – and if they do use this process, it is likely to be some time after the event, rather than at the most appropriate time – when the problem has arisen.
3. Many software-based RCA tools involve some form of 'Categorisation' problem solving process. The software prompts the user to think about problem causes using some form of hierarchical outline or

‘pick-up list’, which users use to identify problem causes (and solutions). The problem here is that causes are not categories, and that there are an infinite number (and number of levels) of causes. A predefined hierarchy is likely to represent the biases of whoever created the categorisation scheme, and this may not reflect, or include, the causes that are relevant to the problem being solved. Even worse, these predefined hierarchies or ‘pick-up lists’ often focus almost exclusively on the Physical Causes of failures (because these are the easiest to categorise), yet as we discussed earlier, the most effective solutions are those which deal with Organisational or Latent Causes (which are much harder to categorise without being overly generic). Finally, because this categorisation scheme is contained in a computer program, it frequently carries a higher level of ‘authority’ than it deserves. Certainly, most of these computer programs provide the capability to add additional causes to their lists, but experience says that most people will restrict their thinking to those causes that are contained in the software. As a result, the solutions being developed will be suboptimal, while simultaneously giving the illusion of precision, as a result of having been developed using a computer.

Having said that, there is value in recording the results of past RCA analyses for future reference – but this can generally be achieved using readily available software tools, such as Microsoft Word, PowerPoint or Visio, without having to resort to specialist RCA software.

In short, Conventional Root Cause Analysis (RCA) methods work by chance, not by design [60]. Conventional incident reports do not communicate their findings effectively. Cause categorisation trees, and computer software based on them, create the illusion of finding solutions, but these solutions will not provide assurance of effectiveness, since they do not provide the branched causal relationships required by the cause and effect principle.

Categorisation methods are popular with rule-based people because they validate existing perceptions in a written format. If something is on a computer, it becomes even more trustworthy for them. In our search for an effective solution, we are often misguided by our existing strategies, and when solutions are presented as easy and painless we tend just to accept them.

For most situations which arise within an organisational context, there are multiple approaches to resolution. These different approaches generally require different levels of resource expenditure to execute. And, due to the immediacy which exists in most organisational situations, there is a tendency to opt for the solution which is the most expedient in terms of dealing with the situation. In doing this, the inclination is generally to treat the symptom, rather than the underlying fundamental problem that is actually responsible for the situation occurring. Yet, in taking the most expeditious approach, and dealing with the symptom rather than the cause, what is generally guaranteed is that the situation will, in time, return and need to be dealt with again.

The common processes of storytelling and categorisation are the product of thousands of years of evolution in human thinking. On the basis of reviews which have been performed, it can be shown that that, while conventional root cause analysis methods and tools provide some structure to the process of human event problem solving, they are significantly limited and often work by chance not by design.

The cause and effect principle based RCA methods and tools.

The typical representative of this group is RealityCharting® [25]. This is the only process that demonstrates an understanding of, and follows, the cause and effect principle, thus it is the only process that allows all stakeholders to create a clear and common reality to promote effective solutions every time. RealityCharting® (the previously used term was ‘Apollo Root Cause Analysis’) is unlike all other RCA tools and methods. It is the only one that actually provides a graphical representation, with evidence of all causes and their inter-relationships. With this clear understanding of reality, it can easily be communicated to anyone with a full appreciation of how the solutions will prevent the problem from recurring.

Apart from these general observations, some additional attributes and features of RCA methods and tools described in chapters 2 and 3 can be identified. So, ASSET, Change Analysis, HPES, MORT, STEP and TOR (Technique of Operations and Review) [147] are based on different accident causation models, e.g. Change Analysis and HPES have no explicit model, whereas MORT and STEP are based

on explicitly formulated models. The methods and tools vary in degree of standardisation, from general requirements for the process (Change Analysis), up to a set of attributes evaluated as adequate or less than adequate (MORT). Although ASSET, MORT and TOR explicitly consider organisational factors, inter-organisational factors are not included in any of the reviewed methods. None of the methods has explicit features for overcoming judgmental biases or shortcomings in causal reasoning [115].

A classic mistake in the use of RCA is to concentrate on the symptoms of a problem instead of the actual root cause, basically due to stopping to ask ‘WHY?’ too early [138]. Many accident investigations do not go far and deep enough. They identify the technical cause of the accident, and then connect it to a variant of ‘operator error’ – the line worker who forgot to insert the bolt, the engineer who miscalculated the stress, or the manager who made the wrong decision. But this is seldom the entire issue. When the determinations of the causal chain are limited to the technical flaw and individual failure, typically the actions taken to prevent a similar event in the future are also limited: fix the technical problem and replace or retrain the individual responsible. Putting these corrections in place leads to another mistake: to the belief that the problem is solved. So, many accident investigations remain at surface level — thus creating scope for the same type of events to recur. Furthermore, weaknesses in investigation could impede the capacity to find both generic characteristics from the analysis of the event and other characteristics of interconnected events [155].

4.2. Results of comparison of different event analysis methodologies, methods and tools

Despite a lot of existing detailed descriptions, recommendations and instructions for construction and use of different event investigation methods and tools provided in the literature, a fundamental problem exists: individuals and organisations have little information in order to compare them with each other. The perception is that one tool is as good as another. A further problem in making comparisons between different event investigation methods and tools is the existing anarchy when using terms and definitions. Due to the lack of standardisation of RCA, authors of some works do not differentiate between methodologies, methods and tools, and false RCA has become a diluted acronym that, essentially, has been rendered useless in terms of meaning. For example, a list of 39 different problem solving methodologies (starting with such ‘methodologies’ as ‘trial-and-error’ and ‘guess and check’, and ending with ARCA and TapRoot®) is presented in [146]. The major providers of RCA ‘methodologies’ cannot agree on a universally accepted definition of what RCA is, and this further confuses the market. This situation is reinforced by the competitive concerns of the RCA providers, because if such a definition is agreed upon, their respective ‘methodologies’ risk not being viewed as unique in the market, and this would possibly have a negative impact on business. Consequently, when trying to choose between RCA methods and tools, potential users are being denied the benefit of experience, expertise and information, even though providers are capable of providing this. For example, currently it is acceptable (although not possible to do it correctly) to compare, on the basis of equal status, the relatively primitive RCA instruments, such as 5-Why’s and Fishbone Diagrams, with such noted processes as PROACT, ARCA, REASON and TapRoot, because RCA is then being equated to troubleshooting, problem solving and brainstorming. This problem could be solved by RCA providers and users coming together, and producing an unbiased baseline standard that establishes the minimum requirements for what is to be considered RCA. So potential users would be provided with a baseline document, to evaluate the various RCA processes and select the one that is suitable for specific conditions [134].

Some results of a comparison of event investigation principles at the highest level – methodologies – are presented in table 4.2.1 [125]. Quantitative analysis methods (PSA), using such tools as fault tree analysis (FTA), event tree analysis and Markov analysis are often used to complement an RCA [29]. There are many causes that can be further analysed to better understand the quantitative contribution of a particular event under study. In summary, quantitative methods are similar to an RCA in that the tool allows for the determination of lower level causal events. However, a structured RCA is tailored more for qualitative determination of actionable causes; a PSA is tailored more to analysing the combinatorial

conditions that are required to occur, to lead to a certain system state, and hardware-related events, where the assumptions of primary event independence are more easily validated, or the dependence of such events can be more easily modelled.

Table 4.2.1. Comparison between features of the deterministic safety assessment and the probabilistic safety assessment [125]

	Deterministic safety assessment	Probabilistic safety assessment
Events to be covered	Small number of representative events considered to be severest among conceivable events	All accidents considered to be significant
Frequency	Simply assumed to occur (no discussion of its frequency)	Since the frequency has a probability distribution, it is assessed with a median value, or a mean value and uncertainty width
Method of an accident analysis	In accordance with the scenario defined by the Regulatory Guide it is analysed based on conservative assumptions (for example, a single failure is assumed for the most effective accident mitigation system)	Taking into account progresses of various conceivable accidents, all significant accidents (accident sequences) are analyzed under the realistic assumptions (multiple failures of mitigation systems are to be assumed)
Risk assessment	NA or qualitative analysis	Quantitative analysis
Treatment of uncertainties	Discussion on uncertainties is avoided by following ‘ the conservative methods for accident analysis’	Quantitative analysis including the propagation of uncertainties (in order to make a realistic assessment, the uncertainty will become large in addressing the areas with poor knowledge)
Interpretation of assessment results	Individual interpretation for each accident	Comprehensive interpretation based on all accident sequences
Examples of application	Documents of the Application for Reactor Establishment Licence	US NRC: An Assessment of Accident Risks in US Commercial NPPs; WASH-1400

Due to the lack of standardisation of Root Cause Analysis methods and tools, in order to compare RCA with anything, there is a need to somehow draw boundaries around what we mean by Root Cause Analysis. To establish these boundaries, some key characteristics of RCA should be established, and then used for evaluation of some commonly known RCA methods and concepts [29]. However, there are no commonly accepted key characteristics of, or criteria for, RCA methods and tools, and available results of comparisons of these instruments are mostly subjective, non-comprehensive and of limited use.

In order to establish what is Root Cause Analysis, and what is not (i.e. comes under Shallow Cause Analysis), 6 essential criteria are defined, which need to be met in order for a process and its tools to be called true Root Cause Analysis [56]:

1. Identification of the real problem to be analysed in the first place.
2. Identification of the cause-and-effect relationships that combined to cause the undesirable outcome.
3. Disciplined data collection and preservation of evidence to support cause-and-effect relationships.
4. Identification of all physical, human and latent root causes associated with undesirable outcome.
5. Development of corrective actions/countermeasures to prevent same and similar problems in the future.
6. Effective communication to others in the organisation of lessons learned from analysis conclusions.

Examination against these criteria shows (see Table 4.2.2), that techniques such as brainstorming, troubleshooting and problem solving should be attributed to SCA, but not to RCA [56].

Table 4.2.2. Differences between SCA and RCA tools [56]

Analytical process	Discipline data collection required?	Typically team (T) versus individual (I) based	Formal cause and effect structure	Requires validation of hypotheses using evidence	Identification of physical (P), Human (H), and Latent (L) root causes
Brainstorming	No	T	No	No	P or H
Troubleshooting	No	I	No	No	P
Problem solving	No	T	No	No	P or H
Root Cause Analysis	Yes	T	Yes	Yes	P, H, L

Another attempt to separate tools that should be categorised as SCA, rather than RCA [29] uses such key characteristics of RCA as degree of methodology, degree of causal information detail and level of automation. These three characteristics were chosen primarily to help illustrate the wide range of methods, tools and concepts that have been described as Root Cause Analysis (see tables 4.2.3-4.2.5). In writing the following characteristics and summarising the methods and tools below, there is no attempt to provide a level of subjective good or bad. Each RCA method or tool has its strengths and weaknesses. The particular needs of the situation and/or the organisation drive the selection of the most appropriate RCA method or tool [29]. Table 4.2.6 illustrates some results of comparison between the diverse range of instruments that are sometimes accurately called Root Cause Analysis methodologies, methods, tools and concepts. It is easy to see how there can be confusion regarding what constitutes a root cause analysis.

Another perspective on the relationship between root cause analysis and quantitative methods is provided Figure 4.2.1 [29]. This continuum concept illustrates some differences between RCA methods. There is no implied subjective assessment of good or bad in any of these areas. The approach used should be based on the needs of the organisation and the situation.

Table 4.2.3. Degree of Methodology of RCA methods

Degree of Methodology	Description
Well Defined	A clear methodology is provided which guides the user through the RCA Process with a focus on finding effective solutions. The most common process steps involve something like: 1) Define the Problem, 2) Analyze the problems and 3) Identify/Implement Solutions. Most of the commercial RCA products are based on a well defined methodology.
Loosely Defined	This means items such as brainstorming, multi-voting, or creating an Ishikawa fish bone diagrams. There are loosely defined methodologies for these.
No Methodology/ Collection of Concepts	Some courses and books fall into this category. In this approach, many concepts are presented to the user. Some concepts may be tools, while others may be ideas. In theory, the user finds what they want, and perhaps builds their own methodology to apply the knowledge.

Table 4.2.4. Degree of Causal Information Detail of RCA methods

DCID	Description	Examples	Effort Required
Very High	All possibilities that can cause the top level event	Similar to fault tree diagrams used in system safety assessments. Show what happened and also include every possible cause that can cause the same problem.	Very high. May not be practical for some event based problem solving.
Medium to High	High precision mapping of causes and effects, including actions and conditions.	Cause and Effect Diagrams used in Apollo Root Cause Analysis and Reason Root Cause Analysis. Note that some causal categorization trees are called cause and effect diagrams, which is somewhat misleading.	Low to moderate, depending on training, experience of practitioner. Can be higher effort for higher significance events based on need to understand causes in higher detail.
Low	Cause Grouping and/or low precision mapping of causes and effects	Ishakawa fish bone diagrams, timeline causal analysis, predefined causal categorization trees such as MORT, voting on causes	Low to moderate, depending on training, experience of practitioner.
Very Low	Text type narrative	Story or timeline of events. Commonly used in "Blue ribbon panel" type reports.	Same as above

Table 4.2.5. Level of Automation of RCA methods

Level of Automation	Description	Examples
High	Enterprise and/or stand alone software is available that automates the process, performs integrity checks, generates reports.	RealityCharting® software, based on Apollo Root Cause Analysis methodology. Reason® software based on the Reason RCA methodology
Some	Some elements of the process are automated	Database that automates the categorization and analysis of causes.
None	No software automation available (except for word processing, spreadsheets, etc.).	Completing a standard problem report form where you check off the pre-defined root cause categories, such as human error, equipment, procedures, etc.

The Data Dump + Recommendations: (lower left corner on Figure 4.2.1.) refers to a typical narrative report, possibly including a timeline, data, statements, etc. followed by expert recommendations based on expert judgment. The causal interconnections between the problems and solutions are not always clearly explained in these types of reports. We rely on the competence and experience of the experts to ensure the solutions match up with causes of the problem.

Timeline Analysis: is sometime used to identify causes. This involves a timeline that includes events (actions) and conditions that were present at each point in time. The timeline causal analysis is typically presented in a table, and does not provide detailed information on how each event or condition cause interconnect.

Pre Defined Cause Trees: These are typically an extensive list of cause categories, grouped in a hierarchical manner by similar categories, such as equipment problems or people problems. These can look similar to cause and effect charts, but they are vastly different. In Causal Categorisation Trees, the cause interconnections are based on grouping/categorising by arbitrarily chosen attributes, and do not reflect a cause and effect relationship. Sometimes, when the causes are categorised into groupings, the number of causes in each group is counted and a Pareto chart is created. This statistical approach, however, may be misleading if the true cause and effect relationship behind the cause groupings is not understood.

Table 4.2.6. Summary of selected RCA methods and tools

RCA Method or Concept	Degree of Methodology (Table 1)	Degree of Causal Info. Detail (Table 2)	Degree of Automation (Table 3)	Comments
Blue Ribbon Panels/ Expert Opinions	None (unless developed by group)	Very Low	None	Rely on the experts to ensure that solutions line up with causes.
Brainstorm & Vote	Loosely Defined	Low	None to Some	
Five Why's (Also called "Why-Why")	Loosely Defined	Low	None	Ask why five times, arrive at "root cause"
Ishikawa Fish Bone Diagram	Loosely Defined	Low	None to Some	Some charting software like MS Visio® includes templates for this
Management Oversight and Risk Tree (MORT)	Well Defined	Low	None to Some	Pre defined causal categorization tree originally developed by the DOE in the 1970's
RealityCharting® software (Based on Apollo RCA methodology)	Well Defined	Medium to High	High	Commercial Product
Wikipedia.com (search on "Root Cause Analysis")	Collection of Concepts	Depends on concept	None	Public web site

Describing the relationship between qualitative root cause analysis and quantitative methods shows how both can be used, in a complementary fashion, to find effective solutions to event based problems. Both RCA and quantitative methods are part of a larger whole, or continuum of approaches, used in finding solutions for event based problems.

Another standard against which the many so-called root cause analysis methods and tools can be compared and evaluated is suggested in [25]. For successful evaluation it should be generally agreed that the purpose of root cause analysis is to find effective solutions to our problems, such that they do not recur. Accordingly, an effective root cause analysis process should provide a clear understanding of exactly how the proposed solutions meet this goal. To provide this assurance, an effective process should meet the following six criteria (partially coincident with the six essential criteria presented above [56]):

1. Clear definition of the problem and its significance to the problem owners.
2. Clear delineation of the known causal relationships that combined to cause the problem.
3. Clear establishment of causal relationships between the root cause(s) and the defined problem.
4. Clear presentation of the evidence used to support the existence of identified causes.
5. Clear explanation of how the solutions will prevent recurrence of the defined problem.
6. Clear documenting of investigation results and how criteria 1-5 are met in a final RCA report so others can easily follow the logic of the analysis.

Using these comparison criteria, Table 4.2.7 provides a summary of how each selected method or tool meets the criteria. This comparison shows how poorly these conventional RCA tools and methods provide effective solutions. Since scores for specific tools and methods in Figure 4.2.3 do not look very convincing and could be the subject of discussion, it clearly demonstrates that RealityCharting seems to be one of the most universal and useful method for performing RCA.

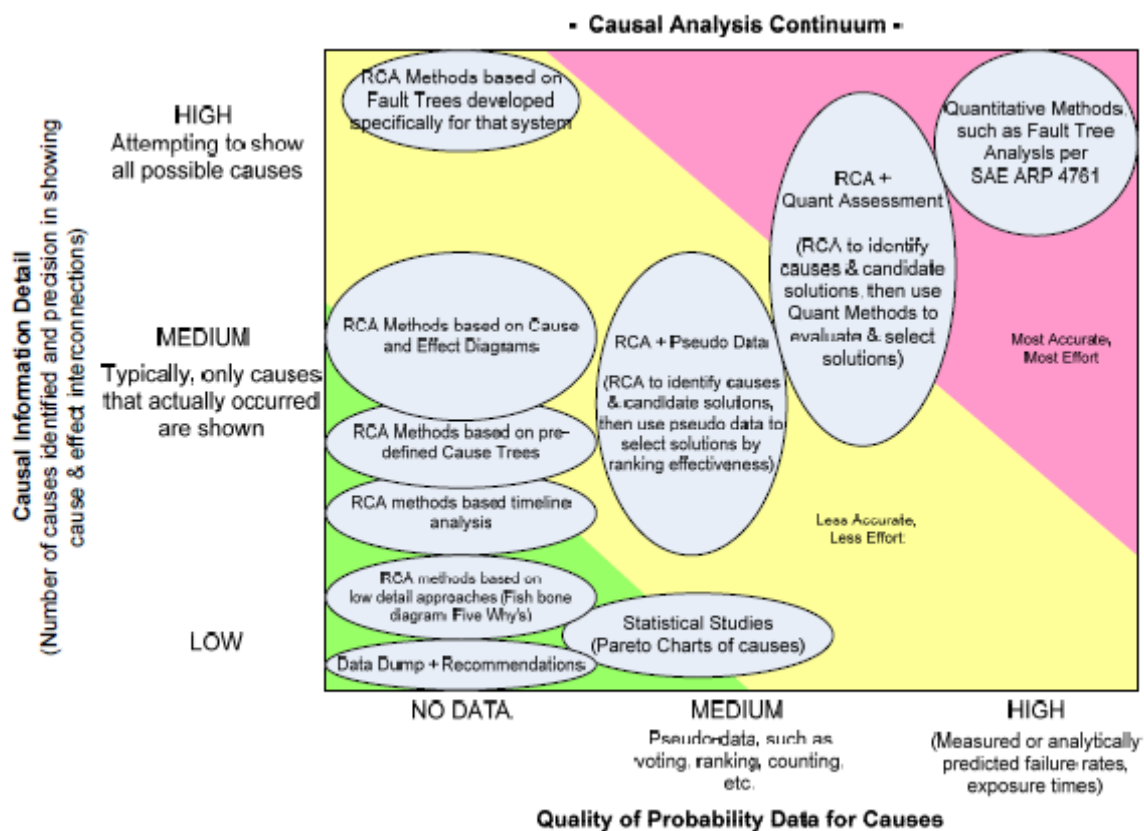


Figure 4.2.1. The Causal Analysis Continuum [29]

Table 4.2.7. Comparison of selected RCA methods and tools [25]. One point is scored for each criterion that is met, and 0.5 point is scored if criterion is met partially ('Limited')

Method/tool	Type	Defines problem	Defines all causal relationships	Provides a causal path to root causes	Deline-ates evidence	Explains how solutions prevent recurrence	Easy to follow report	Score
ECFC	Method	Yes	Limited	No	No	No	No	1.5
Change analysis	Tool	Yes	No	No	No	No	No	1
Barrier analysis	Tool	Yes	No	No	No	No	No	1
Tree diagrams	Method	Yes	No	No	No	No	No	1
Why-Why Chart	Method	Yes	No	Yes	No	No	No	2
Pareto	Tool	Yes	No	No	No	No	No	1
Storytelling	Method	Limited	No	No	No	No	No	0.5
Fault Tree	Method	Yes	Yes	Yes	No	Yes	No	4
FMEA	Tool	Yes	No	Limited	No	Limited	No	2
RealityCharting	Method	Yes	Yes	Yes	Yes	Yes	Yes	6

Results of comparison of the few representative current methods for analysing human-related incidents occurring in different industrial fields are presented in table 4.2.8 [38]. For the comparison, such characteristics were used as style of report, style of countermeasure presentation, survey performers, procedure and database availability, and level of human factors analysis. It was noted that, for HPES, ASRS, and the other current methods, such as those for evaluating the causes of ship collisions,

application in the field of equipment operation was mainly envisaged. After evaluation of selected features, it was concluded that the event investigation method developed by the author of [38] is superior to other compared analogous instruments.

Table 4.2.8. Comparison of the few representative event investigation methods used in different industrial fields [38]

Title, abbreviation	Industry	A	B	C	D	E	F
HPES	Nuclear	1	3	2	1	2	2
ASRS	Aircraft	1	1	2	1	2	2
Analytical sheets for chemical complexes	Chemical	1	1	3	1	2	2
Train trouble responsibility survey sheets	Railroad	1	1	2	1	1	1
Ships collision causes evaluation	Ship	1	1	1	1	2	1
Hazard evaluation	Automobile	1	1	2	1	2	2
Coded anti-safety behaviour matrix	Labour hazard	1	1	3	1	2	2
Error taxonomy	All fields	1	1	1	1	2	2
Takano method [38]	Nuclear	3	3	2	2	2	2

Note to table 4.2.6: characteristics of event investigation methods compared:

A: style of report (1 – check-sheet; 2 – descriptive; 3 – both);

B: style of countermeasure presentation (1 – common countermeasures based on statistics; 2 – detail description of countermeasures; 3 – both);

C: survey performed (1 – by specialist; 2 – by persons concerned; 3 – both);

D: procedure availability (1 – not provided; 2 – provided);

E: availability of database (1 – not provided; 2 – provided);

F: human factor s analysis (1 – on the same level as equipment; 2 – emphasis on human factors).

Fairly extensive comparison of some important, recognised, and commonly used methods for investigation of accidents is given in [68]. However, this study also cannot be treated as comprehensive, because some of the methods and tools which are well known and widely used in the nuclear energy sector (such as HPES, HPIP, HPEP, ASSET etc.) are not included in this survey. The author of [68] adopted the original classification of instruments for event investigation: they are all called ‘methods’, while ‘primary methods’ are stand-alone techniques, and ‘secondary methods’ are those which provide special input as a supplement to other methods. Moreover, root cause analysis is treated in this comparison as an ordinary secondary method together with different tools such as ECFC, barrier analysis, change analysis, fault tree analysis and so on.

The selected methods are compared according to the following characteristics (see Table 4.2.9):

- Whether the methods give a graphical description of the event sequence or not.
- To what degree the methods focus on safety barriers.
- The level of scope of the analysis. The selected methods are compared according to a classification of the socio-technical system involved in the control of safety, comprising the following levels: 1 - the work and technological system; 2 - the staff level; 3 - the management level; 4 - the company level; 5 - the regulator’s and association’s level; 6 - the government level.
- What kind of accident models have influenced the methods (A - causal-sequence; B - process; C - energy; D - logical tree; E - SHE-management models).
- Whether the different methods are inductive, deductive, morphological or non-system-oriented.

- Whether the different methods are primary or secondary methods.
- The need for education and training in order to use the methods.

Since the author of [68] did not present his own developed method of event investigation, his inquiry could be considered as independent and objective. Consequently, none of the selected methods was ranked above the others. It was only concluded that each of the methods compared has different areas of application, qualities and deficiencies, so that a combination of methods ought to be used in a comprehensive investigation of a complex accident. Another interesting conclusion was pertinent to the level of scope of the analysis. It was observed that most of the methods examined included an analysis of safety barriers, but it seems that most of the methods are limited to a focus on Level 1 (the work and technological system) and to Level 4 (the company level) of the socio-technical system involved in the control of safety (or hazardous processes). This means that investigators focusing on issues concerning the Government and the regulators in their accident investigation to a great extent need to base their analysis on experience and practical judgment, rather than on results from formal analytical methods. Since it was noted, that ‘like the technicians have to choose the right tool in order to repair a technical system, so an accident investigator has to choose proper methods to analyse different problem areas’, no recommendations for selection of proper methods and tools were suggested [68].

Table 4.2.9. Results of comparison of some methods and tools for investigation of accidents [68]

Method	Accident sequence	Focus on safety barriers	Levels of analysis	Accident model	Primary/secondary	Analytical approach	Training need
ECF charting	Yes	No	1-4	B	Primary	Non-system oriented	Novice
ECF analysis	Yes	Yes	1-4	B	Secondary	Non-system oriented	Specialist
Barrier analysis	No	Yes	1-2	C	Secondary	Non-system oriented	Novice
Change analysis	No	No	1-4		Secondary	Non-system oriented	Novice
Root cause analysis	No	No	1-4	B	Secondary	Non-system oriented	Specialist
Fault tree analysis	No	Yes	1-2	A	Primary/Secondary	Deductive	Expert
Influence diagram	No	Yes	1-6	D	Secondary	Non-system oriented	Specialist
Event tree analysis	No	Yes	1-3	B/E	Primary/Secondary	Inductive	Specialist
MORT	No	Yes	2-4	D	Secondary	Deductive	Expert
SCAT	No	No	1-4	D/E	Secondary	Non-system oriented	Specialist
STEP	Yes	No	1-6	A/E	Primary	Non-system oriented	Novice
MTO-analysis	Yes	Yes	1-4	B	Primary	Non-system oriented	Specialist/expert
AEB	No	Yes	1-3	B	Secondary	Morphological	Specialist
TRIPOD	Yes	Yes	1-4	A	Primary	Non-system oriented	Specialist
Acci-Map	No	Yes	1-6	A/B/D/E	Primary	Deductive/ Inductive	Expert

The results of another exercise to compare the most popular event investigation methods and tools (taking into account some of those developed in Japan) are presented in table 4.2.10 [131]. However, the selection of the methods and tools compared, the criteria used for comparison and the results of the evaluations are different. With a strong emphasis on the importance of such criteria as organisational factors and organisational climate, it was concluded that the most effective event investigation tool should be based on the JOFL Classification developed by the author of [131].

Table 4.2.10. Results of comparison of some methods and tools for event investigation (taking into account some of those developed in Japan) [131]

Method/tool	Type	Defines problem	Defines all causal relationships	Provides a causal path to root causes	Delineates evidence	Explains how solutions prevent recurrence	Easy to follow report	Defines organisational factors	Defines organisational climate
Cause-and Effect Diagram	Tool	Yes	Limited	No	No	No	No	No	No
Interrelationship Diagram	Tool	Yes	No	No	No	No	No	No	No
Current Reality Tree	Tool	Yes	No	Limited	No	Limited	No	No	No
Why-Why Analysis	Tool	Yes	No	Yes	No	No	No	No	No
Multi Vari Analysis	Tool	Limited	Limited	Yes	No	No	Yes	No	No
ECFA	Method	Yes	Limited	No	No	No	No	No	No
Change Analysis	Method	Yes	No	No	No	No	No	No	No
Barrier Analysis	Method	Yes	No	No	No	No	No	No	No
MORT	Method	Yes	Yes	Yes	No	Limited	Yes	No	No
HPES	Method	Yes	Yes	Yes	No	Limited	Yes	No	No
HINT/J-HPES	Method	Yes	Yes	Yes	No	Yes	Yes	No	No
SAFER	Method	Yes	Yes	Yes	No	Yes	Yes	No	No
ATOP	Method	Yes	Yes	Yes	No	No	Yes	No	No
Extended CREAM	Method	Yes	Yes	Yes	No	No	Yes	Limited	Limited
JOFL Classification	Tool	No	Yes	No	No	No	No	Yes	Yes

The results of one more attempt to compare the effectiveness of the three selected root cause analysis tools statistically are presented in [7, 51]. The cause-and-effect diagram (CED), the interrelationship diagram (ID), and the current reality tree (CRT) were selected for analysis. The purpose of study [7] was to compare the perceived differences between the tools listed above with regard to four independent variables: causality, factor relationships, usability, and participation. The first dependent variable was the perceived ability of the tool to find root causes and the interdependencies between causes. The second dependent variable was the perceived ability of the tool to find relationships between factors or categories of factors. Factors may include causes, effects, or both. The third dependent variable was the overall perception of the tool's usability to produce outputs that were logical, productive, and readable. The fourth dependent variable was the perception of participation resulting in constructive discussion or dialogue. In addition, the secondary interests of the study were to determine the average process times required to construct each tool, the types of questions or statements raised by participants during and after the process, and the nature of the tool outputs.

Guided by 3 trained facilitators, 72 participants in the study (first and second year undergraduate students) were randomly split into the three groups. A similarly formatted treatment work pack, with the steps for RCA tool construction, and a graphical example, based on published material, was provided for each group. The dependent variables were measured, using a twelve-question self-report questionnaire with a five-point Likert scale and semantic differential phrases. Having been given instructions, participants were asked to analyse, and to find the perceived root cause of the problem. The facilitators were available for help throughout the exercise. Upon completion of the exercise, the participants completed the self-report instrument. This process was repeated until all groups applied all three analysis tools to three randomised problems. Each subsequent exercise was carried out at seven days intervals.

Parametric statistical analysis of the data collected showed that the mean for the CED was either the same or higher on all dependent variables with standard deviations of less than one. No statistical difference was found between the three tools for causality or participation or regarding factor relationships. The CRT was deemed more difficult than the other tools. The other significant statistical finding was that the CED was perceived to be better at identifying cause categories than either the ID or the CRT. The type and amount of training needed for each tool varies. The CED and ID can be used with little formal training, but the CRT requires comprehensive instruction, because of its logic system and complexity. However, the CED and ID both appear to need some type of supplemental instruction in critical evaluation and decision making methods. The CRT incorporates the mechanism for testing the logic and evaluation system, but the CED and ID have no such mechanism and are highly dependent on the thoroughness of the group using them. In general, the author of [7] concluded that this study was not able to identify the best tool for root cause analysis. A synthesis of the comparison results of three selected root cause analysis tools (CED, ID, CRT) based on a review of the literature and the author's of [7] investigations is presented in Table 4.2.11.

Table 4.2.11. Comparison results of three selected root cause analysis tools (CED, ID, CRT) [7, 51]

	Performance criteria																
RCA tools	Ability to find a specific root cause	Ability to find a reasonable root cause	Ability to show systematic causes of effect	Shows causal interdependency	Identifies factor relationships	Shows intermediate factors	Identifies cause categories	Stimulates dialogue and discussion	Focuses activities	Has mechanism for testing logic	Construction process time	Construction accuracy required	Extent of subjective influence on output	Amount of problem knowledge required	Ease of use	Overall readability	Number of factors to analyse
CED	No	No	No	No	No	No	Yes	?	Yes	No	Low	High	High	High	High	Low	Many
ID	Yes	Mix	No	No	Yes	No	No	?	Yes	No	Low	Med	High	?	High	Low	?
CRT	Yes	Yes	Yes	Yes	Yes	Yes	?	Yes	Yes	Yes	High	Low	Low	?	Low	High	Few

A trial aiming to grade the different problem solving methods and tools according to a scale starting at 'very open' and ending with 'highly formal' is presented in [146]. Detailing the differences of a few selected event investigation methods and tools (see table 4.2.12), in the opinion of the author of [146], reinforces the point that a universally effective method (tool) does not exist. Data contained in table 4.2.13 illustrate not differences, but five common principles of selected problem solving methods and tools, similar to the well-known DMAIC principle [104, 110, 146].

One of the collective wide scale attempts to compare different event analysis methods and tools was a coordinated research project launched by the IAEA in 1998 [1, 2]. Its objective was exploration of root cause methods and techniques in use at that time in Member States, evaluating their strengths and limitations, and developing criteria for appropriate event investigation methods. This coordinated research project was performed over four years, and involved 15 national and international research organisations and 36 investigators.

The scope of analysis of this project was focused primarily on ASSET, HPES and MORT; the strengths and limitations of these different methods were identified, along with the extent of their use at that time. Only brief characteristics were provided for other available methods, such as SOL, PSA, AEB, PRCAP and CERCA. Important characteristics that event investigation and analysis methods should include were identified. However, no detailed comparison was performed of methods analysed against desirable characteristics. Only short recommendations for the selection of suitable methods, with very limited choice (from ASSET, HPES or MORT only), were provided (see table 4.3.2), and these cannot be considered to be comprehensive and practical.

Table 4.2.12. Grading of some event investigation tools against their level of formality [146]

Very open			Highly formal	
	Variable Analysis	TapRooT	DMAIC, DMADV, Apollo	High aptitude
	6M's; 8P's; 4S's	Simple Root Cause (SRC)		
	Ishikawa or Fishbone Diagrams			
Brainstorming, Experience	5 Whys		Work site risk assessment	Basic skill

Table 4.2.13. Common principles of selected problem solving methods and tools [146]

	DMAIC	5 Whys	Apollo	Brainstorming	Variable Analysis
Define the problem	Define	Write down the problem	Define the problem	Set the Problem	Define the problem
Understand the problem detail	Measure			Determine a set of leading questions	Describe the problem
Analyze the problem to understand the root cause	Analyze	Ask why until you have identified the root cause	Analyze cause and effect relationships	Generate ideas	Expand the analysis tree and eliminate the sub-variables
Develop a solution	Improve		Identify Solutions	Evaluation of ideas	
Implement and ensure successful elimination	Control	Develop and implement a solution	Implement the best solutions	Implementation	Implement a solution

An analysis and evaluation of event investigation methods applied by STUK, and the two Finnish nuclear power plant operators TVO and Fortum, was carried out by the Technical Research Centre (VTT) at the request of STUK at the end of the 1990s [5]. The study aimed to provide a broad overview of the whole organisational framework in place in Finland to support event investigation practices at the regulatory body and the utilities. The main objective of the research was quite comprehensive: to evaluate the adequacy and reliability of event investigation analysis methods and practices in the Finnish nuclear power industry and, based on the results, to suggest means for further improvement. However, no concrete information about the results of such an evaluation was provided; even methods and tools used for event investigation in the Finnish nuclear industry were not listed or mentioned (except the PSA-based method). It was only concluded that there were no indicators or measures used to evaluate the effectiveness of event investigation and operating experience feedback. Consequently, no suggestions concerning event investigation analysis methods and practices were made.

In recognition of the growing need for a unified problem solving methodology in order to improve the operational experience feedback process in the aerospace industry, a set of criteria was developed to study and evaluate root cause analysis methods, and concepts from lessons learned [137]. A hierarchical criteria structure was adopted, grouping the criteria into five categories, starting with those with the highest priority, and continuing in order of priority:

1. Technical accuracy of data (category 1):
 - 1.1. Technical accuracy of the data that were to be produced by the problem solving method, including the ability of the process itself to validate the accuracy and relevancy of the data;
 - 1.2. Utility of a built-in, procedural process that would require investigators to gather adequate data by driving them to systemic root causes;
 - 1.3. Capability to reliably filter out irrelevances through application of process;
 - 1.4. Capability to identify the need to acquire additional information when appropriate.
2. User friendly software (category 2):
 - 2.1. Ease of use – ease to understand and work through logic;
 - 2.2. Minimum time required to input data;
 - 2.3. Minimum time required to generate reports;
 - 2.4. Understandable cause code layout.
3. Analysis of data (category 3):
 - 3.1. Calling for some procedural way to objectively measure and compare available solution options and action plans, in order to assess their potential for immediate prevention benefit and their overall control impact upon the identified problem;
 - 3.2. Analysis capability to identify common causes;
 - 3.3. Ability to research results of similar undesired outcomes.
4. Archiving and communication of data (categories 4 and 5):
 - 4.1. Ability to view the data at all locations via Web;
 - 4.2. Integration with existing databases;
 - 4.3. Export/import capabilities;
 - 4.4. Incorporation of existing cause codes.

The set of criteria developed is focused upon the four essential task functions within problem-solving and communications activity; it seems to be appropriate to guide evaluation, research and study of available event investigation systems, and even for the eventual selection of an optimum system, depending on specific conditions. On the basis of results of the case studies performed, it was concluded that the REASON® RCA tool is the most efficient and accurate, and that it corresponds completely with the set of criteria developed [137, 138].

5. Recommendations

The effectiveness of learning from experience at NPPs could be maximised, if the best event investigation practices available from a series of methodologies, methods and tools, in the form of a ‘toolbox’ approach, were promoted. Since different instruments of analysis are the most suitable in different situations, recommendations for selection of the best instruments are necessary. Nevertheless, such recommendations should not be seen as prescriptive.

In line with the main goal of this study, recommendations concerning the selection and usage of different event investigation methods, tools and techniques described in the literature are presented and analysed in this chapter. Unfortunately, most of the available recommendations of this type are not exhaustive and user-friendly. They usually cover only a few instruments, of different levels, selected without adequate substantiation; event types for which some methods or tools are recommended for use are not adequately specified; some recommendations contradict others; and some clearly do not meet the principle of independence. So, most of the available recommendations are of little practical value, leaving current and future event investigators (including newcomers, who are not yet proficient) to make decisions regarding the selection of event investigation methods and tools, based on their own knowledge, or on providers’ promotional materials.

To start with, the general problem about the relationship between qualitative root cause analysis and quantitative methods should be considered. The majority of researchers who analysed this problem agree that both RCA and quantitative event investigation methods are part of a larger whole, or continuum of approaches, used in finding solutions for event based problems. The comparisons performed of their attributes [1, 2, 23, 26, 29, 32, 33, etc.] show that both can be used in a complementary fashion (see table 5.3.1). The flowchart (see Figure 5.3.1) illustrates an example of how the recommended interaction between RCA and quantitative methods could be realised in finding solutions (corrective actions) following an event based problem such as an incident or accident.

Table 5.3.1. Summary of Root Cause Analysis and Quantitative Methods [29]

	System design, certification	Operation – if failures or incidents occur
RCA	Not typically used in this stage, unless high significance failures occur in design, manufacture, test, etc.	To prevent or mitigate recurrence, effective solutions are required. Start with RCA, use it to determine causes, and then to find solutions. Use quantitative methods to help determine causes and/or to evaluate solutions for effectiveness.
Quantitative methods	Used for high consequence systems. In some industries and states, required by regulations.	Used in conjunction with RCA to develop effective solutions.

The literature, however, lacks a means for selecting the appropriate root cause analysis tool based upon objective performance criteria. Some of the important performance characteristics of root cause analysis tools include the ability to find root causes, causal interdependencies, factor relationships, and cause categories. Root cause analysis tools must also promote focus, stimulate discussion, be readable when complete, and have mechanisms for evaluating the integrity of group findings. Thus, problem solvers and decision makers are likely to select a tool based on convenience, rather than on its actual performance characteristics [94].

Lack of experience and absence of adequate recommendations sometimes lead to a situation, when users are looking for RCA tools, to their choosing what are called ‘Auto-RCA’ solutions - in other words, the easy way out. They are looking for something to give them the answer, so they do not have to think for themselves. Do such tools exist? Certainly. Do such tools have all the answers? No. Do the users think these tools have all the answers? Yes. Therein lies the danger. People do ‘RCA by the numbers’, by picking from a list and saying they have done a RCA. In reality, they may have missed some key contributing factors, which should cause a safety concern, as the risk of recurrence is greater.

The available recommendations for selection of the best problem solving tool vary from very simple to highly complicated. For example, in [146] it is recommended to consider the following few simply questions:

- What type of problem do I have?
- Who is going to be solving the problem?
- How much time do we have to solve the problem?
- What kind of solution is required?

At the same time, when evaluating which RCA processes are best for your organisation, it should be ensured that factors such as cost, minimum compliance, time and ease will not take priority over the important characteristics of value, comprehensiveness, operational reliability and efficiency [56].

A few recommendations for the selection of a suitable method, depending on the safety significance of an event, with very limited choice (from ASSET, HPES or MORT only), were formulated on the basis of CRP launched by IAEA [1, 2] (see table 5.3.2). It is noted, that the potential to develop (where

possible) some degree of integration of ASSET with HPES, and/or MORT, to form an integrated event investigation method ‘toolbox’ should be considered.

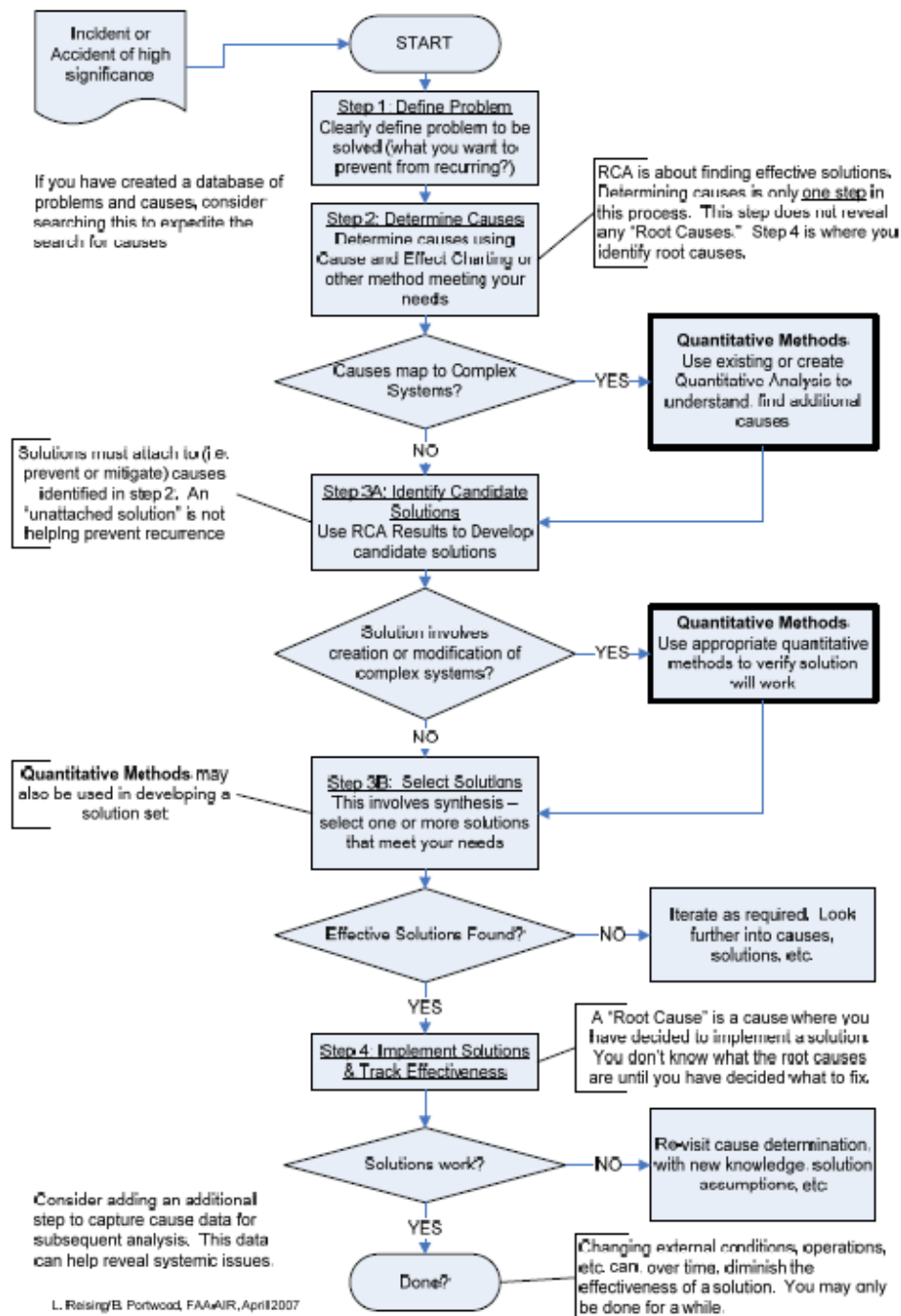


Figure 5.3.1. Recommended interaction of RCA and Quantitative Methods in resolving Event Based Problems [29]

The more comprehensive process of selection of the appropriate RCFA (root cause failure analysis) method for the needs of some organisations should consist of several steps and meet the following criteria [92]:

1. *Determine your Internal RCFA Needs:*

- Are you looking to set up an RCFA effort or to investigate a single incident only?
- Will your RCFA effort focus on ‘incidents’ only, chronic failures only, or both?

- Will management support be solicited?
- Will management systems be implemented?
- Will teams be dedicated to completion of RCFAs?
- Will hourly personnel participate in teams?
- Will additional technical resources be required?
- Will additional technical equipment be required?

2. *Determine Appropriate RCFA Method to Use for your Environment:*

- Evaluate simplicity of method.
- Evaluate analysis flexibility.
- Evaluate quality of materials and job aids.
- Evaluate training flexibility.
- Evaluate method comprehensiveness.
- Evaluate system to track for results.
- Evaluate overall value of method (cost-benefit analysis).

3. *Determine How to Implement: In-House or Outsource:*

- Does the facility possess the instructional technology skills and resources to develop in-house courses on evaluated and proven RCFA methods?
- Is it more economical and timely to develop courses in-house (cost-benefit)?
- Would utilising past vendor training be appropriate for in-house instructors?
- Are there any copyright infringement concerns utilising past vendor training in-house?
- Are qualified RCFA instructors with field experience available in-house?
- Would in-house instructors be dedicated to supporting and mentoring their students?
- Would management be willing to fund the RCFA method development in-house?
- Would management be willing to wait for completion of skill development and then implementation?

4. *Choose the Appropriate RCFA Vendor:*

- Does the vendor provide the RCFA method chosen by the facility?
- Does the vendor have training in RCFA for field personnel, engineers and management?
- Does the vendor possess various methods that complement each other and provide specifically designed training to the appropriate level of audience?
- Does the vendor's instructor(s) have field experience in implementing RCFA? How much?
- Does the vendor's instructor(s) have experience in instructional technology and applied learning to increase presentation retention rates?
- Can the vendor provide references of successful client field applications? In your industry?
- Does the vendor have products/services to support RCFA method (management system support models, software, on-site facilitation services, follow-up capabilities, etc.)?
- Is the vendor willing to customise instruction and materials to accommodate your needs?
- Is the vendor willing to work on specific, on-going in-house failures during training?
- Does the vendor possess the skills with staff to deal with managerial culture transformations?
- Is the vendor willing to partner? Share risk?
- Does the vendor possess the staff capacity to handle your requirements? Domestically? Internationally?

Obviously, this list of criteria is not as comprehensive as it possibly could be, however it is a good starting point. The key to starting is clearly defining what YOU want, and obtaining internal support for the vision. Then the task will be to identify the vendors qualified to help execute your vision.

The few recommendations for tool selection, depending on the nature of the problem, are presented in tables 5.3.3, 5.3.4 [143] and 5.3.5 [24]. In these publications a common opinion is maintained, which is that one method, or a combination of methods, may be used to determine the causal factors, contributing

causes, direct cause, and the root cause. However, the value of such recommendations is very low, because only a few basic RCA methods or tools are covered. Moreover, the suggestion to use TapRoot® in conjunction with each root cause analysis tool to assist with the determination of the root cause seems to be unsubstantiated, because TapRoot® is a high level RCA tool, and itself incorporates the principles of all three tools analysed in tables 5.3.3 and 5.3.4 [143].

Table 5.3.2. Recommendations for selection of root cause analysis tools [1, 2]

Situation No	Safety significance of an event	Event population	Event investigation methodology recommended (most appropriate)	Comment
1	Low	Single	HPES or MORT truncated ('apparent cause')	
2	High	Single	Combination of the ASSET, HPES, or MORT	
3	Low	Group or recurring	Combination of the ASSET, HPES, or MORT	
4	High	Group or recurring	ASSET	For NPPs already trained in ASSET

Table 5.3.3. Recommendations for RCA tool selection depending on problem nature [143]

Problem Nature	Barrier Analysis	Change Analysis	Event and Causal Factors Analysis
Organisational	Best	Good	--
Activity or Process	Best	Good	Good
Reorganisation	Good	Best	--
New or Changed Activity	Better	Best	Good
Personnel	Best	Good	Better
Accident or Incident	Better	Good	Best

Table 5.3.4. Areas of potential use of the three RCA tools [143]

Method	When to Use	Advantages	Disadvantages
Barrier Analysis	Use to identify barrier and equipment failures and procedural or administrative problems.	Provides a systematic approach	Requires familiarity with the process to be effective
Change Analysis	Use when cause is obscure. Useful in evaluating equipment failures.	Simple six-step process	Limited value because of the danger of accepting wrong 'obvious' answer(s).
Event and Causal Factors Analysis	Use for multifaceted problems with long or complex causal factor chain.	Provides visual display of analysis process. Identifies probable contributors to the condition.	Time-consuming and requires familiarity with the process to be effective

Table 5.3.5. Recommendations for use of few Root Cause Analysis Methods and tools [24]

	WHEN	WHERE	HOW
TREE (MORT)*	Investigation 1/3 through, parts OK early	Management or programmatic concerns, big events or potential	Label Color Note
E&CF**	ASAP, continuous	Where <u>facts</u> and story are needed, for large events	Story line events, then conditions
Fault Tree**	ASAP	Hardware failure	Start at top, use negative words and logic gates, show critical path
H-B-T**	Early	All accidents, where something is damaged or hurt, near hits	One hazard-target pair at a time, use <u>advertised</u> barriers
Change**	Early	When a <u>comparison</u> is needed	<u>Label</u> columns A & B, consider <u>potential</u> impact

(H-B-T – hazard, barrier, target)

Flow Chart for selection and summary of attributes with recommendations for use of 6 root cause methods and tools are given in Figure 5.3.2 and Table 5.3.6 [11].

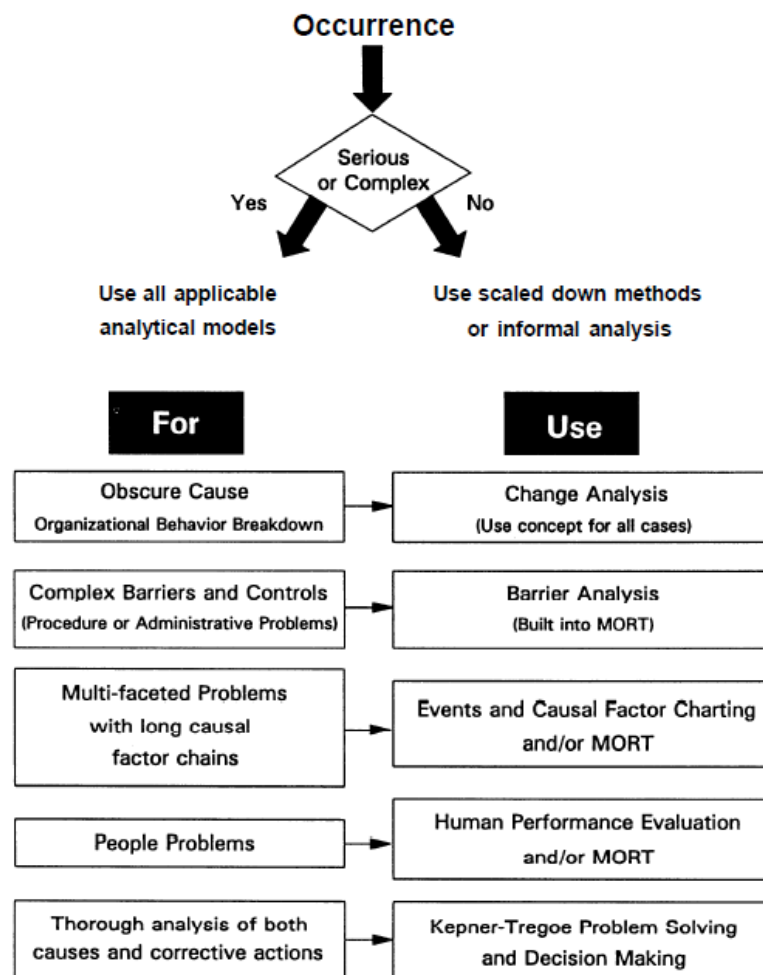


Figure 5.3.2. Flow Chart for selection of few root cause methods depending on significance of the occurrence [11]

The extent to which these methods are used, and the level of analytical effort spent on root cause analysis, should be commensurate with the significance of the occurrence. A high-level effort should be spent on most emergencies, an intermediate level on most unusual occurrences, and a relatively low level should be adequate for most occurrences caused by minor deviations from normal process. In any case, the depth of analysis should be adequate to explain why the occurrence happened, determine how to prevent recurrence, and assign responsibility for corrective actions. An inordinate amount of effort to pursue the causal path is not expected if the significance of the occurrence is minor.

A high-level effort includes use and documentation of formal root cause analysis to identify the factors leading up to the event and the programme deficiencies. Both Events and Causal Factor Analysis and MORT could be used together in an extensive investigation of the causal factor chain. An intermediate level might be a simple Barrier, Change, or Mini-MORT Analysis. A low-level effort may include only gathering information and drawing conclusions, without documenting the use of any formal analytical method. However, in most cases, a thorough knowledge and understanding of root cause analytical methods is essential to conducting an adequate investigation and drawing correct conclusions, regardless of the selected level of effort.

Table 5.3.6. Summary of attributes and recommendations for use of 6 root cause methods and tools [11]

Method	When to use	Advantages	Disadvantages	Remarks
Events and Causal Factor Analysis	Use for multi-faceted problems with long and complex causal factor chain	Provides visual display of analysis process. Identifies probable contributors to the condition	Time-consuming and requires familiarity with process to be effective	Requires a broad perspective of the event to identify unrelated problems. Helps to identify where deviations occurred from acceptable methods
Change Analysis	Use when cause is obscure. Especially useful in evaluating equipment failures	Simple 6-step process	Limited value because of the danger of accepting wrong 'obvious' answer	A singular technique that can be used in support of a larger investigation. All root causes may not be identified
Barrier Analysis	Use to identify barrier and equipment failures and procedural or administrative problems	Provides systematic approach	Requires familiarity with process to be effective	This process is based on the MORT Hazard/Target Concept
MORT	Use when there is a shortage of experts to ask the right questions and whenever the problem is a recurring one. Helpful in solving programmatic problems	Can be used with limited prior training. Provides a list of questions for specific control and management factors	May only identify area of cause, not specific causes	If this fails to identify problem areas, seek additional help or use cause-and-effect analysis
HPES	Use whenever people have been identified as being involved in the problem case	Thorough analysis	None if process is closely followed	Requires special training
Kepner-Tregoe	Use for major concerns where all aspects need thorough analysis	Highly structured approach focuses on all aspects of the occurrence and problem resolution	More comprehensive than may be needed	Requires special training

Probably the most comprehensive recommendations for selection of the most appropriate event investigation instrument are presented in [156]. Based on the results of research carried out, the attributes of 28 methods and tools are evaluated against a set of performance criteria, and adequate recommendations are developed. It is noted that many investigators do not use any specific methods to analyse human factors issues. They often rely only on their own extensive experience and expertise in either investigations or human factors/safety management. This equips them to ask the appropriate questions, develop a clear understanding of the factors that caused an incident, and identify the best approach to preventing further incidents with the same root cause. It appears that the methods used are to some extent secondary to the expertise – and particularly to the familiarity with human and organisational factors – of the team using them. However, two key areas for caution are identified, related to the expertise/competence of investigators in human factors and analytical methods.

The first problem is related to insufficient/lost skills or experience in using specific technical methods. This problem can be solved by means of honestly evaluating the level of expertise and appropriate selection of members in the investigation team, training (self-training or attending a training course provided by suppliers of methods), refresher training and periodic practice by investigators, keeping up to date with developments, seeking help from a professional investigator/analyst, if possible, and using their expertise as a learning opportunity for internal staff.

Another problem (already analysed in chapter 4.1 of this report) is related to check lists of factors or root causes, which may be incomplete, or can channel the analyst's thinking down certain tracks. Investigators should be aware of this problem, and use check lists as an initial prompt or aide-memoire. If necessary, a variety of check lists or expert help should be used, to provide guidance on the issues to explore.

Taking into account the areas for caution set out above, and the recommendations in tables 5.3.7 and 5.3.8 [156], it should be possible to decide on the type of method or tool that the event investigation team needs, and is able to use. It is noted that a simple method may be better during the early stages of investigation of a complex incident, moving to a more complex method when the investigation team has developed initial insights into the incident.

Since the Guidance [156] is designed mostly for petroleum and allied industry businesses, several event investigation methods and tools widely used in the nuclear industry are not included in the analysis. However, the recommendations in this study could be very useful, not only for selection of appropriate event investigation instruments, but also for their comparison and evaluation.

Table 5.3.7. Main features for selection of event investigation methods and tools (1)

		Training required	Paper-based or software		Retrospective analysis of incident reports	Used in petroleum industry	Generates graphical content (e.g. timeline)	Complete method for incident analysis	Provides solutions	Includes checklists or flow diagrams	Comments
			Paper	Software							
1.	ARCA - APOLLO Root Cause Analysis	✓	✓	✓	✓	✓	✓	✓	✓		Described as a general problem solving method
2.	Black Bow Ties		✓	✓		✓	✓				
3.	DORI – Defining Operational Readiness to Investigate		✓								Not an analysis method – describes how to conduct an investigation
4.	ECFA – Events and Causal Analysis (Charting) and ECFA+ - Events and Conditional Factors Analysis		✓				✓				Part of the MORT method but is often used as a charting method in an investigation/analysis to provide graphical depiction of incident
5.	Fishbone diagram		✓		✓		✓				Purely a method for graphically presenting results; software systems available to help draw
6.	HERA – Human Error Repository and Analysis System		✓	✓	✓						
7.	HERA-JANUS – Human Error Reduction In ATM (Air Traffic Management)	✓	✓		✓		✓	✓		✓	
8.	HFACS – The Human Factors Analysis and Classification System	✓			✓					✓	Classification system only – aviation based, would need to adapt
9.	HFAT – Human Factors Analysis Tools	✓	✓	✓	✓	✓	✓	✓	✓	✓	Can be applied to any type of behaviour and has been used as a proactive method in risk assessment
10.	HFIT – Human Factors Investigation Tool	✓	✓	✓			✓	✓		✓	
11.	HSYS - Human System Interactions	✓	✓	✓		✓				✓	Can be used for proactive analysis in risk assessment
12.	ICAM - Incident Cause Analysis Method	✓	✓	✓	✓	✓	✓	✓	✓	✓	
13.	MEDA – the Maintenance Error Decision Aid	✓	✓			✓	✓	✓	✓	✓	Maintenance error; contains basic solutions but relies on the user to identify definitive improvements. There are examples, however the user/interviewee needs to really come up with the definitive improvements; use other tools with MEDA e.g. timeline, police interview methods

Table 5.3.8. Main features for selection of event investigation methods and tools (2)

		Training required	Paper-based or software		Retrospective analysis of incident reports	Used in petroleum industry	Generates graphical content (e.g. timeline)	Complete method for incident analysis	Provides solutions	Includes checklists or flow diagrams	Comments
			Paper	Software							
14.	MORT – Management Oversight and Risk Tree	✓	✓	✓	✓	✓	✓	✓		✓	
15.	PEAT – the Procedural Event Analysis Tool	✓	✓	✓						✓	Flight crew error – can be adapted
16.	PRISMA – Prevention and Recovery Information System for Monitoring and Analysis	✓	✓		✓	✓	✓	✓	✓	✓	Was designed for retrospective analysis and to collect and structure data on incidents
17.	SCAT® – Systematic Cause Analysis Technique	✓	✓	✓		✓		✓	✓	✓	Provides an indication of 'areas for corrective action' rather than ready-made solutions
18.	SOL – Safety through Organisational Learning	✓	✓	✓			✓	✓	✓	✓	The software version, Sol-VE includes a module for identifying corrective actions
19.	SOURCE™ – Seeking Out the Underlying Root Causes of Events	✓	✓	✓		✓		✓		✓	Does not provide solutions but includes a checklist to help develop solutions. Does not generate graphical content, but recommends the use of fault trees or causal analysis charting
20.	Step	✓	✓				✓			✓	
21.	Storybuilder	✓		✓	✓		✓	✓			Training useful but not essential. Specifically for occupational incidents. Designed for use in all industries
22.	TapRoot®	✓	✓	✓	✓	✓	✓	✓	✓	✓	Solutions module available soon. Method includes advanced interviewing techniques for investigation
23.	Kelvin Top-Set®	✓	✓	✓		✓	✓	✓		✓	Forms part of the HFAT methodology
24.	TRACER – Technique for Retrospective and Predictive Analysis of Cognitive Errors		✓		✓	✓					
25.	Tripod Beta	✓	✓	✓	✓	✓	✓	✓			Does not provide ready-made solutions but leads the analysis back to basic risk factors that form the key elements of improvements
26.	WBA – Why Because Analysis		✓		✓		✓				
27.	5 Whys		✓								A simple method for exploring issues
28.	Why tree		✓				✓				

A quite assertive recommendation, concerning selection of the ratio between RCA and Shallow (Apparent) Cause Analysis approaches, is presented in [93]. It is based on the fact that a nuclear plant may actually carry out five, or perhaps even ten, good root cause analyses per year. But they undertake hundreds, or even thousands, of short-cut analyses (see Figure 5.3.3). The thousands of corrective actions based on guesses and assumptions drive their improvements. So time and resources are wasted on short-cut investigations and best-guess corrective actions, and some nuclear managers complain that improvement programmes are not cost effective. One of the most likely reasons for this seems to be the inefficiency and ineffectiveness of Shallow (Apparent) Cause Analysis.

M. Paradies recommends stopping Apparent Cause Analysis, and, wisely, allocating resources to establishing an improvement programme based on advanced root cause analysis, instead of continuing to use the inefficient Apparent Cause Analysis approach [93]. This includes using root cause analysis both reactively (for significant incidents) and proactively (by targeting audits, assessments, and observations to the highest potential risk areas and activities). The result of this change in emphasis, from thousands of short-cut analyses to fewer, better, more targeted, more proactive analyses, should be apparent to both nuclear plant management and regulators. Firstly, more potentially significant events will receive a more thorough root cause analysis, and more effective corrective actions, based on root cause analyses. Even though these investigations constitute only 10% of the previous number of total Root Cause and Apparent Cause investigations, the improvements should have greater impact because of their effectiveness. This impact includes fewer ‘repeat’ investigations, because of the effectiveness of a thorough investigation in preventing the recurrence of problems. Secondly, management’s attention, and perhaps even regulatory attention, can be focused more efficiently on the significant issues, rather than being spread across thousands of Apparent Cause Analyses. This becomes even more obvious when the number of significant issues decreases due to effective corrective actions. Thirdly, because proactive efforts are targeted by risk analysis, these efforts can provide even more efficient improvements, by eliminating the highest cost (in money, in plant down-time, in regulatory attention, and in bad publicity) incidents. Fourthly, because proactive efforts and root cause analysis yield data that are forward-looking, the data are much more useable by management when directing the company’s improvement efforts to avoid major problems.

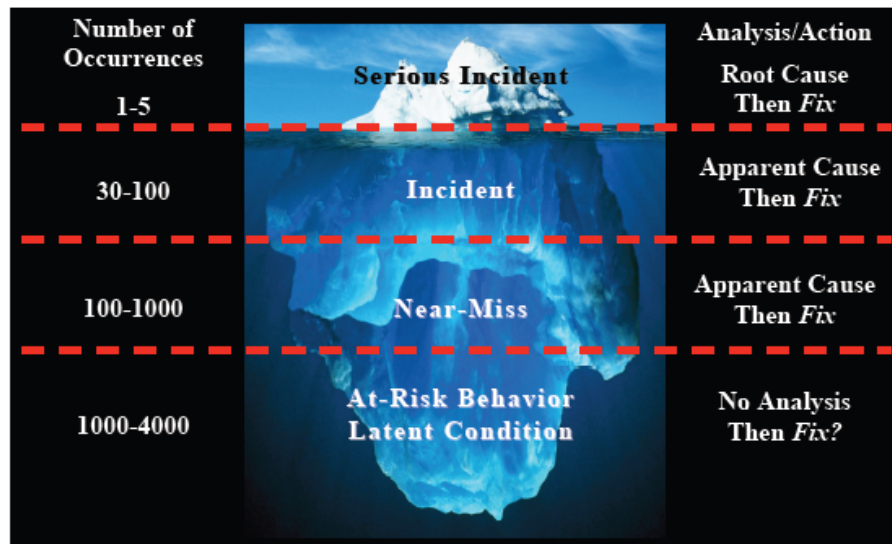


Figure 5.3.3. Numbers of occurrences at a nuclear power plant and types of analyses

The start of such change could be ‘effort neutral’ - no more effort is required for this new, more effective approach than is currently being used in [93].

1. Expand good root cause analysis to all significant incidents without taking shortcuts (see Figure 5.3.3). Defining the real root causes of these significant incidents enables the development of

well substantiated corrective actions, gaining valuable lessons learned, and effort expended is cost effective.

2. Stop doing Apparent Cause Analysis on near misses and instead, categorise the occurrence types and watch for adverse trends. This requires an adequate categorisation system and advanced methods for identifying trends (not the inadequate, arbitrary, goal driven ‘up is bad, down is good’ approach applied by so many companies). Stopping Apparent Cause Analysis saves significant investigatory effort. But even more significant is the effort saved by NOT implementing inadequate ‘best-guess’ solutions that do not work.
3. Take the effort saved from not doing thousands of short-cut analyses and not fixing the assumed problems, and put that effort into a targeted PROACTIVE improvement programme, based on good root cause analysis. This targeted programme can be managed so that the investment in improvement can be budgeted – even rationed if need be – and measured for effectiveness.

Taking into account the available operational experience, the recommendation to stop Apparent Cause Analysis seems to be too drastic and not realistic. However, the ratio between RCA and Apparent CA should be gradually changed in the direction of an increase in the use of root cause analysis, both reactively (for significant incidents) and proactively (by targeting audits, assessments, and observations of the highest potential risk areas and activities), especially when developing programmes of corrective actions, and allocating resources for their implementation.

Another radical way to improve the quality of root cause analysis is based on W. Edwards Deming’s observation that most problems are management controllable - embedded in the manner in which management decides to operate the organisation [104]. In recent years such an approach, based on the integrated solving of RCA, human and organisational factors, safety culture and quality management problems together, and promoting the crucial role of top management in safety improvement processes, has been widely supported by different specialists [24, 35, 36, 52, 53, 77, 78, 81- 90, 104, 130, 131]. The essence of this approach could be illustrated by a proposition such as: ‘Safety and quality are one and the same. Only a change in the management system will reduce the frequency of accidents. Companies with weak management systems have higher accident rates’ [151]. With reference to the experience of more than a hundred hearing meetings of licensee’s RCA audit, it is concluded that ‘an excellent RCA is not dependent on methodology, but on viewpoint-oriented approach to analyse deep-rooted cause in organisational factors’ [131].

Following the approach based on the integration of event investigation and improvements in safety culture and quality management systems controlled by top managers, the new root cause taxonomy was suggested by J. Dew [104] and approved by American Society of Quality (ASQ) and the 2002 Annual Quality Congress.

Taxonomy is a method for organising and classifying information. The immediate benefit of having taxonomy of root causes is that it helps identify the end point in the questioning process, and allows organisations to add up the number of times problems occur in a specific root cause area. If the taxonomy of root causes is organised around observations that are not truly root causes, then the questioning process may be ended prematurely and the organisation may continue to suffer from the unnamed root cause.

The purpose of this new taxonomy is to drive the process of critical thinking to deeper levels within organisations that purport to practice root cause analytical thinking. This taxonomy seeks to unearth the truly fundamental problems with management systems in any organisational setting. This new taxonomy categorises root causes into seven belief systems, any one of which can create extreme dysfunction in a management system. Until management recognises its belief system, understands how these beliefs create dysfunctional behaviours and then embarks on a journey to develop new beliefs and behaviours based on the quality body of knowledge, it cannot extract itself from its quandary.

This new root cause taxonomy includes [104]:

1. placing budgetary considerations ahead of quality;
2. placing schedule considerations ahead of quality;
3. placing political considerations ahead of quality;

4. being arrogant;
5. lacking fundamental knowledge, research or education;
6. pervasively believing in entitlement;
7. practising autocratic behaviours, resulting in 'endullment' of personnel.

Leaders who succumb to any of these seven fundamental root causes will not want to acknowledge their problem. This is why quality has been viewed as a fad in many organisations. People hear the quality message, and leaders embrace the quality lingo, but when quality principles and methods come up against the deeply entrenched, dysfunctional belief system in an organisation, quality is rejected and condemned. Managers denigrate quality concepts as a fad, and turn back to their focus on costs, schedule, political manipulation, arrogance, ignorance, entitlement or 'endullment'.

Another of the relevant, but clearly and unambiguously unanswered questions related to event investigation is: when to perform root cause analysis? The simple answer is: whenever the organisation encounters unacceptable consequences. Experience dictates that RCA is typically conducted in most cases reactively under such circumstances as [134]:

1. when someone is injured or died;
2. significant production loss;
3. when there is catastrophic damage to equipment or facility;
4. when there is a regulatory violation;
5. when an event adversely affects the community;
6. when there is recognised liability on the part of the company.

In every organisation an incident investigation policy and adequate programme should be established to determine when, and to what extent, analysis should be conducted. An incident investigation programme should be based on three basic elements: threshold criteria, evidence preservation policy and clearly defined responsibilities regarding incident investigation [25].

Every organisation needs to establish its own threshold criteria or sentinel events for defining the level of analysis, depending on the type of industry, organisation and potential risk of activities [1, 25, 111]. In line with the concept of continuous improvement, the threshold criteria should periodically be reviewed and revised: if no problems are meeting the threshold criteria, they should be tightened; if time and resources spent on investigation exceed the acceptable limits, they should be relaxed. An incident investigation programme should envisage the application of RCA in a proactive manner by addressing chronic repetitive events ('routine failures') and so reducing the risks associated with the emergence of more dramatic, sporadic events, which have much more serious consequences [134].

According to [154], the main criterion for choosing accident investigation methodologies is accordance with their context of use. The context is determined by the Terms of Reference of the accident investigation agreed upon between the parties, which define the scope of the investigation (direct and root causes), the requirements for the report and urgent recommendations, the timescales and the audience. Context therefore implies, according to the stakes involved in the accident and the expected results of the investigation, several levels of resources that are usually provided for the investigation. Constraints may be placed upon the investigation, as well. The choice of people and skills required in the investigation team ranges from those with general knowledge to specialist experts, all helping to understand and make sense of the phenomena (from physical to human, organisational and societal aspects). The choice of methodologies will depend upon the resources, time constraints and expertise needed to use the investigation tool.

To assist in these decisions, some basic '*do's and dont's*' are suggested [154]:

- Tools and methodologies are 'servants' and not 'masters'.
- Organisations that want to increase their potential to learn from opportunities such as incidents should already have trained some investigators beforehand to use a set of relevant tools.
- Apply the 'stop rule': this rule usually leads to stopping an investigation with a goal that can be managed. However, investigators have a tendency to limit themselves in their investigation, so it is not necessary to be too strict in the framing of an investigation.

6. Conclusions

1. The effectiveness of learning from experience at NPPs could be maximised, if the best event investigation practices available from a series of methodologies, methods and tools, in the form of a 'toolbox' approach, were promoted.
2. The literature provides a lot of information about the individual attributes of numerous event investigation methods, tools and techniques, including detailed descriptions, recommendations, and instructions for construction and use, supported by colourful and illustrative examples. However, there is little information regarding the performance of these instruments relative to each other.
3. Analysis of the available sources of information shows that only a limited number of studies designed to compare the different event investigation methods and tools are performed. These studies usually aim for specific goals, use different comparison criteria, which are not commonly accepted, are of limited scope, and cover only a small number of instruments from the available toolbox. Some of the results of such comparisons seem to be of a promotional type, one-sided and unfair.
4. There are no established threshold criteria for performing an event investigation of an appropriate level. Every organisation needs to establish its own threshold criteria for defining the level of analysis, depending on type of industry, organisation and potential risk of activities. The validity of such an approach could be questioned (especially for high risk industries like nuclear energy).
5. The literature lacks a means for selecting the appropriate root cause analysis methods and tools, based upon objective performance criteria. Most of the available recommendations concerning selection and usage of different event investigation methods, tools and techniques are not exhaustive and user-friendly: they usually cover only a few instruments of different levels, selected without adequate substantiation; event types for which some methods or tools are recommended for use are not adequately specified; and some recommendations contradict others. So, most of the available recommendations are of little practical value, leaving current and future event investigators (especially newcomers, who are not yet proficient) to make decisions about the selection of event investigation methods and tools, based on their own knowledge or providers' promotional materials.
6. Lack of standardisation in the area of event investigation methodologies was identified: there are no universally accepted systems of classification or standardisation of terms, definitions and criteria for evaluation of different event investigation methods, tools and techniques.
7. In pursuance of the suggested classification system, an inventory, review and brief comparative analysis of event investigation methods, tools and techniques, either recently developed or already used in the nuclear industry (with some examples from other high risk industry areas), was performed in this study. Some advantages and drawbacks of these different instruments were identified and analysed. It is demonstrated that the supposed advantages (sometimes actively promoted by providers) of simple, easy to use RCA tools, which require neither training nor qualification of the user (especially some software based RCA tools) should be not overestimated. These tools could be used effectively, taking into account their existing limitations.
8. Unstructured processes of root cause analysis put too much emphasis on opinions, take too long, and do not produce effective corrective measures or lasting results. For further improvement of operational reliability and better employment of operational experience feedback in the nuclear industry, it is necessary to establish baseline standards, setting out criteria and minimum requirements for what is to be considered RCA, policies for training, and best practice, using structured root cause analysis methods and tools. The alternative is to continue to assume that existing efforts will somehow produce different, better results.
9. For the generation of more concrete recommendations concerning the selection of the most effective and appropriate methods and tools for event investigation, new data, from experienced

practitioners in the nuclear industry and/or regulatory institutions, are needed. It is planned to collect such data, using the prepared questionnaire [155], and performing the undergoing survey.

7. References

1. IAEA-TECDOC-1600. Best Practices in the Organisation, Management and Conduct of an Effective Investigation of Events at Nuclear Power Plants. IAEA, Vienna, 2008. ISBN 978-92-0-109308-0.
2. IAEA-TECDOC-1278. Review of Methodologies for Analysis of Safety Incidents at NPPs. IAEA, Vienna, 2002. ISSN 1011-4289.
3. IAEA-TECDOC-632. Asset Guidelines Revised. IAEA, Vienna, 1991.
4. NUREG/CR-6751. The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems. U.S. Nuclear Regulatory Commission, 2001.
5. Suksi S. Methods and practices used in incident analysis in the Finnish nuclear power industry. Elsevier B.V., 2004.
6. Kluch J.H. Root Cause Analysis: Methods and Mindsets. Paper presented at the annual Nuclear Instructors' Workshop of the Midwest Nuclear Training Association. Columbus, OH, 1988. p.82 p.
7. Doggett M.A. A Statistical Comparison of Three Root Cause Analysis Tools. Journal of Industrial Technology. Volume 20, Number 2, 2004. p.9
8. Barrier Analysis. Root Cause Analysis: RCA Tools. <http://www.bill-wilson.net/b52.html>.
9. Root Cause Analysis: Reason. <http://www.rootcause.com/>
10. PROACT® RCA. Root Cause Analysis Software. http://www.reliability.com/industry/pdf/ProactRCA_v3.pdf.
11. DOE-NE-STD-1004-92. Root Cause Analysis Guidance Document. DOE Guideline, 1992.
12. Kalinauskas R. Developing a Root Cause Analysis Work Process. <http://maintenanceworld.com/Articles/kalinauskasR/Developing-Root-Cause-Analysis-Work-Process-3.html>.
13. Rooney J. J., Van den Heuvel L. N. Root Cause Analysis for Beginners. Quality Basics. <http://www.asq.org/pub/qualityprogress/past/0704/qp0704rooney.pdf>.
14. Joong Nam Kim. The development of K-HPES: a Korean-version human performance enhancement system [for nuclear power plant control]. Korea Electr. Power Res. Inst. Proceedings of the 1997 IEEE Sixth Conference on Human Factors and Power Plants, 'Global Perspectives of Human Factors in Power Generation'. 1997, pp. 1/16-1/20. ISBN: 0-7803-3769-7
15. Dhillon B.S., Liu Y. Human error in maintenance: a review. Journal of Quality in Maintenance Engineering, 2006, vol.12, Nr. 1, pp. 21-36.
16. Harrison M. J. Performance Evaluation Systems and Methods. US Patent application No 20080228549, 2008.
17. Kim D.S., Baek D.H., Yoon W.C. Developing a Computer-Aided System for Analyzing Human Error in Railway Operations. <http://koasas.kaist.ac.kr/bitstream/10203/7892/1/2008>
18. Human Performance Enhancement System, INPO 90-005, Atlanta: Institute of Nuclear Power Operations, (1990).
19. NUREG/CR-5455. Development of the NRC's Human Performance Investigation Process (HPIP). SI-92-01, Vol. 1, Washington, DC: US Nuclear Regulatory Commission, (1993).
20. Paradies M., Unger L. TapRooT®: The system for root cause analysis, problem investigation, and proactive improvement, System Improvements, Inc., (2000). (<http://www.taproot.com/>.)
21. NRI MORT User's Manual. For use with the Management Oversight & Risk Tree analytical logic diagram. NRI-1, Second Edition, 2009.
22. Pérez, S.S. Investigation of Methodologies for Incident Analysis: Regulatory Aspects. Final Report of the Coordinated Research Program on 'Investigation of Methodologies for Incident Analysis'. Research Contract / Agreement No: ARG 9960 / RO. Nuclear Regulatory Authority, Argentina.
23. Dusic M. Analysis of Operational Events in NPPs. Presentation at Joint IAEA/EC Regional Workshop on Operational Events, Transients and Precursor Analyses. EC - JRC IE, Petten, Netherlands, 24 – 28 August 2009.

24. Conger D. Root Cause Analysis Presentation Notes. Presentation at Regional Joint IAEA/EC-JRC Workshop on Operational Events, Transients and Precursor Analyses – RER/9/088. EC – JRC, Petten, Netherlands, 24-28 August 2009.
25. Gano D. L. Apollo Root Cause Analysis – A New Way of Thinking. Apollonian Publications, LLC. Third Edition, 2007, p.206
26. IAEA-TECDOC-1417. Precursor analyses - The use of deterministic and PSA based methods in the event investigation process at nuclear power plants. IAEA, Vienna, 2004. ISBN 92–0–111604–7.
27. Create Cause & Effect Diagrams in Minutes. <http://www.smartdraw.com/specials/cause-and-effect-diagrams.htm>
28. IAEA-TECDOC-1112. Root Cause Analysis for Fire Events at Nuclear Power Plants. IAEA, Vienna, 1999. ISSN 1011–4289.
29. Reising L., Portwood B. Root Cause Analysis and Quantitative Methods - Yin and Yang? Paper presented at the International System Safety Conference, 2007 (www.realitycharting.com).
30. Root Cause Analysis. <http://process.nasa.gov/documents/RootCauseAnalysis.pdf>
31. PROSPER Guidelines: Guidelines for Peer Review and for Plant Self Assessment of Operational Experience Feedback Process. IAEA, Vienna, 2003, p.45
32. SF-1. Fundamental safety principles: safety fundamentals. IAEA, Vienna, 2006. ISBN 92–0–110706–4.
33. IAEA Safety Standards Series No NS-R-2. Safety of Nuclear Power Plants: Operation. IAEA, Vienna, 2000.
34. INSAG-23. Improving the International System for Operating Experience Feedback: a Report by the International Nuclear Safety Group. IAEA, Vienna, 2008, p.31 ISBN 978-92-0-108008-0.
35. Ritsuo Yoshioka. Why do Accidents Happen? The Framework of Safety in Advanced Countries that Have Learned from Accidents. Presentation during visit of the 78th Safety Caravan at Tokai Power Station, The Japan Atomic Power Company (JAPC). Japan, 2005.
36. SCART Guidelines. Reference Report for IAEA Safety Culture Assessment Review Team (SCART). IAEA, VIENNA, 2008, ISSN 1816–9309.
37. IAEA safety glossary: terminology used in nuclear safety and radiation protection: 2007 edition. IAEA, Vienna, 2007. ISBN 92–0–100707–8.
38. Takano K., Sawayanagi K., Kabetani T. System for Analyzing and Evaluating Human-Related Nuclear Power Plant Incidents. Development of Remedy-Oriented Analysis and Evaluation Procedure. Journal of Nuclear Science and Technology, 31[9], pp. 894-913 (September 1994).
39. Tarrel R. J. Proc. 3rd Symposium on Aviation Psychology, Apr. 1985, Columbus, Ohio, USA.
40. Harkins B. Human Performance Improvement. Presentation at DOE Facility Representatives Workshop, 2007. http://www.hss.doe.gov/deprep/facrep/workshop2007/Presentations/May-15/7_Brian-Harkins.ppt
41. NUREG-1842. Evaluation of Human Reliability Analysis Methods against Good Practices. Final Report. US NRC, 2006.
42. Preischl W. Human Performance in the Context of Notifiable Events. RCA Method of GRS. Presentation at IAEA Regional Technical Workshop on Event Analysis and Root Causes, including Human and Organisational Factors (HOF). JRC IE, Petten, Netherlands, 9 – 13 November, 2009.
43. NUREG-1624. Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA). US NRC, 2000.
44. Guidance Undertaking an Investigative Interview. www.msnpsa.nhs.uk/rcatoolkit/resources/word_docs/Guidance/GuidanceUndertaking_an_Investigative_Interview.doc
45. Risk Analysis Methodologies. <http://www.cip.ukcentre.com/risk.htm#2.2%20Fault%20tree>
46. Delivering Advanced Engineering Solutions. Fault Tree. AESC, 2008. <http://www.2aesc.com/services/faulttree.html>
47. Events and Causal Factors Analysis. Technical Research and Analysis Center SCIENTECH, Inc. Idaho Falls, August 1995. SCIE-DOE-01-TRAC-14-95.

48. Fault Tree Diagram Construction. Isograph Ltd., 2010. <http://www.isograph-software.com/ftpoverdgc.htm>
49. Delivering Advanced Engineering Solutions. Event Tree. AESC, 2008. <http://www.2aesc.com/services/eventtree.html>
50. Kelly L. Lanier. Experiences in Root Cause Analysis and Defect Prevention Methods. Raytheon Network Centric Systems, 2003.
51. Doggett A.M. Root Cause Analysis: A Framework for Tool Selection. Quality Management Journal (QMJ), vol. 12, No 4/© 2005, ASQ. pp. 34-45.
52. Sierra E.A. Causal Analysis Tree Training. Presentation at DOE Facility Representative Workshop, Las Vegas, Nevada, May 13, 2009.
53. Chandler F. Using Root Cause Analysis to Understand Failures & Accidents. Presentation at 7th Military and Aerospace Programmable Logic Devices (MAPLD) Seminar. NASA, September 8, 2004.
54. Latino R. J. What is RCA? Separating the Tools from the Methodologies. Reliability Center, Inc. http://www.reliabilityweb.com/art04/what_is_rca.htm.
55. Dunn A. Getting Root Cause Analysis to Work for you. <http://www.plant-maintenance.com/>
56. Latino R. J. Root Cause Analysis versus Shallow Cause Analysis: What's the Difference? July 24, 2008, EVP – Reliability Center, Inc. <http://www.gha.org/telnet/2414RCA.pdf>; www.proactforhealthcare.com
57. Gano D.L. The Cause and Effect Principle. http://www.realitycharting.com/_public/site/files/pdf/CE-Principle.pdf
58. Jing G. Have You Found the 'Root Cause' yet? A New Spin to Root Cause Analysis. Entegris, 2006. <http://www.mnasq.org/files/summaries/rootcauseanalysis.pdf>
59. Gano D.L. A Brief History and Critique of Causation. Apollo Associated Services, LLC. 2008. http://www.realitycharting.com/_public/site/files/pdf/Paper-History-and-Critique-of-Causation.pdf
60. Gano D.L. Effective Solutions Versus the Root Cause Myth. Apollo Associated Services, LLC. http://www.apolloorca.com/_public/site/files/Effective%20Solutions%20vs%20Root%20Cause%20Myth.pdf.
61. Gordon R., Flin R., Mearns K. Designing and evaluating a human factors investigation tool (HFIT) for accident analysis. Safety Science, 43 (2005) p. 147–171. www.elsevier.com/locate/ssci.
62. Investigation methodology: Man – technology – organisation. Excerpt from the SINTEF-report. http://www.ptil.no/getfile.php/z%20Konvertert/Health.%20safety%20and%20environment/Safety%20and%20working%20environment/Dokumenter/mto_engl.pdf.
63. Cawby T. TapRooT® Root Cause Analysis Tool at Alaska Airlines. http://flightsafety.org/files/analysis_tools.pdf.
64. E. Hollnagel. Cognitive Reliability and Error Analysis Method, Oxford: Elsevier, (1998).
65. KAIST. A Manual for Human Error Analysis and Reduction (HEAR) System, Final Report, Korea Advanced Institute of Science and Technology, (2007).
66. NUREG-1792. Good Practices for Implementing Human Reliability Analysis. U.S. Nuclear Regulatory Commission, Washington, DC, April 2005.
67. GUIDE YVL 2.8. Probabilistic Safety Analysis in Safety Management of Nuclear Power Plants. STUK, Finland, 2003.
68. Sklet S. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials, v. 111, 2004, p. 29–37.
69. Wilpert B., Fahlbruch, B.: SOL – Safety through Organisational Learning. A Computer Assisted Event Analysis Methodology. The Bieleeschweig Workshops on System Engineering: http://www.rvs.uni-bielefeld.de/Bieleeschweig/Fahlbruch_Miller_SOLHandout.pdf (udatert).
70. Groeneweg J.: Controlling the controllable. The management of safety. Fourth edition. DSWO Press, Leiden University, the Netherlands, 1998.
71. Tripod Solutions: Tripod Brochure 2004. Organisational Risk Management. Controlling Human Error. Nederland, 2004. <http://www.tripodsolutions.net/>

72. Kingston J., Jager J., Koornneef F., Frei R., P. Schallier P. ECFA+. Events and Conditional Factors Analysis Manual. Noordwijk Risk Initiative Foundation, NRI-4 (2007).
73. Kingston J., Koornneef F., Frei R., P. Schallier P. 3CA - Control Change Cause Analysis. Form B. Investigator's Manual. Noordwijk Risk Initiative Foundation, NRI-5, October 2009.
74. Risk Assessment of Operational Events. Handbook. Volume 1 – Internal Events. Revision 1.03, US NRC, August 2009.
75. Vrbanic I. Introduction to PSA-based operational event analysis. Part I: Basic Concepts. Presentation at Joint IAEA/EC Regional Workshop on Operational Events, Transients and Precursor Analyses. EC - JRC IE, Petten, Netherlands, 24 – 28 August 2009.
76. IAEA Safety Standards Series No SSG-2. Deterministic safety analysis for nuclear power plants: safety guide. Vienna, International Atomic Energy Agency, 2009. ISBN 978-92-0-113309-0.
77. IAEA-TECDOC-860. ASCOT Guidelines. Revised 1996 Edition. IAEA, Vienna, 1996, ISSN 1011-4289.
78. IAEA-TECDOC-1329. Safety culture in nuclear installations. Guidance for use in the enhancement of safety culture. IAEA, Vienna, 2002. ISBN 92-0-119102-2.
79. IAEA Safety Standards Series No NS-R-1. Safety of Nuclear Power Plants: Design. IAEA, Vienna, 2000.
80. IAEA Safety Standards Series No GS-G-3.1. Application of the Management System for Facilities and Activities. IAEA, Vienna, 2006.
81. Key Practical Issues in Strengthening Safety Culture. INSAG Series No 15, IAEA, Vienna, 2002.
82. Verlini G. The Mindset of Nuclear Safety. http://www.iaea.org/Publications/Magazines/Bulletin/Bull501/NS_Mindset.html.
83. Hansen T. An Approach for Plants to Address INPO's Nuclear Safety Culture Expectations. <http://www.pennenergy.com/pennenergy-2/en-us/index/power/display.articles.power>.
84. Winokur P. S., Minnema D.M. Measuring Safety Culture. Presentation at ANS Annual Meeting 'Progress in Regulation of Safety Culture', June 16, 2009.
85. Lorrain O., Penington J. The Review of Safety Culture Research and of Measurement Methods. Presentation at Canadian Aviation Safety Seminar (CASS 2007), May 2, 2007. www.shumac.qc.ca.
86. Collins A.M., Gadd S. Safety Culture: A review of the literature. HSL/2002/25. http://www.hse.gov.uk/research/hsl_pdf/2002/hsl02-25.pdf.
87. Hay D. Safety Culture Assessment Tool. http://www.workplacepress.co.nz/assessment_tool.pdf.
88. The enhancement of safety culture. Book of Abstracts. SCK, CEN-BA-28. Mol, 15 October 2009. http://publications.sckcen.be/dspace/bitstream/10038/1325/1/book_of_abstracts_td.pdf
89. Fleming M. Developing safety culture measurement tools and techniques based on site audits rather than questionnaires. Final project report. Saint Mary's University, Halifax, Nova Scotia.
90. Räisänen P. Influence of corporate top management to safety culture. A literature survey. Turku University of Applied Sciences, Ship Laboratory, 2008. <http://www.merikotka.fi/metku/Raisanen%202008%20Influence%20of%20corporate%20top%20management%20to%20safety%20culture%20final%20v3.pdf>
91. Alwani A. Investigation of Accelerator Incidents – Regulatory Perspective. Canadian Nuclear Safety Commission, Ottawa, Ontario, Canada.
92. Latino R. J. How to Select the 'RIGHT' Root Cause Failure Analysis (RCFA) Methodology & Vendor. Reliability Center, Inc., 2005.
93. Paradies M. The Curse of Apparent Cause Analysis. System Improvements Inc., www.taproot.com.
94. Dew J.R. In Search of the Root Cause. Quality Progress, 24. 1991, No3, p. 97-107.
95. Reason J. Human Error. New York: Cambridge University Press, 1990.
96. Bastos S.M. The need for a European Union approach to accident investigations. Journal of Hazardous Materials, v. 111, 2004, p. 1-5.
97. Roed-Larsen S., Valvisto T., Harms-Ringdahl L., Kirchsteiger C. Accident investigation practices in Europe - main responses from a recent study of accidents in industry and transport. Journal of Hazardous Materials, v. 111, 2004, p. 7-12.

98. Yves Dien Y., Llory M., Montmayeul R. Organisational accidents investigation methodology and lessons learned. *Journal of Hazardous Materials*, v. 111, 2004, p. 147–153.
99. Hulsmans M., De Gelder P. Probabilistic analysis of accident precursors in the nuclear industry. *Journal of Hazardous Materials*, v. 111, 2004, p. 81–87.
100. Rollenhagen C., Westerlund J. Lundberg J., Hollnagel E. The context and habits of accident investigation practices: A study of 108 Swedish investigators. *Safety Science*, v. 48, 2010, p. 859–867.
101. Benner, L. Rating accident models and investigation methodologies. *Journal of Safety Research*, v. 16, 1985, p.105–126.
102. Hendrick K., Benner L. Jr. Investigating accidents with STEP. ISBN 0-8247-7510-4, Marcel Dekker, 1987.
103. Revuelta R. Operational experience feedback in the World Association of Nuclear Operators (WANO). *Journal of Hazardous Materials*, v. 111, 2004, p. 67–71.
104. Dew J. Root Cause Analysis. The Seven Deadly Sins of Quality Management. *Quality progress*, 2009, No3. <http://www.asq.org/pub/qualityprogress/past/0903/59theSeven0903.html>
105. IAEA Safety Guide No NS-G-2.11. A System for the Feedback of Experience from Events in Nuclear Installations. IAEA, Vienna, 2006.
106. INSAG-12. Basic Safety Principles for Nuclear Power Plants. 75-INSAG-3 Rev. 1. IAEA, Vienna, 1999.
107. Gross, M. M., Ayres T. J. Research initiative for human performance management of nuclear power. Presented to the IERE Workshop: R&D for Cost Reduction, Fukuoka, Japan, 1998.
108. Wildberger A. M., Gross M.M., Ayres T.J. Learning Lessons Intelligently in the Electric Power Industry. From AAAI Technical Report WS-00-03. 2000, AAAI. (www.aaai.org).
109. Sproull B. Process Problem Solving: A Guide for Maintenance and Operations Teams. Productivity Press, Portland, 2001.
110. Paradies M., Unger L. TapRooT®: Changing the Way the World Solves Problems. System Improvements, Inc., Copyright © 2008, 502 p. ISBN 978-1-893130-05-0.
111. IAEA TECDOC-1581. Best Practices in Identifying, Reporting and Screening Operating Experience at Nuclear Power Plants. IAEA, Vienna, 2007.
112. Aviation Safety Reporting System. Program overview. <http://asrs.arc.nasa.gov/overview/summary>.
113. Holnagel E. Accident Analysis and Barrier Functions. IFE (N), Version 1.0, February 1999. <http://www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf>.
114. Svenson O. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Anal.* 1991 September, 11(3), p. 499-507. <http://www.ncbi.nlm.nih.gov/pubmed/1947355>.
115. Fahlbruch B., Schöbel M. SOL – Safety through organisational learning: A method for event analysis. *Safety Science*, 49. 2011, p. 27–31.
116. SOL - Safety through Organisational Learning. A methodology for systematic event analysis. <http://mahbsrv.jrc.it/mars/TWG1/TWG1docs/meetings/4th-Meeting-31-Jan-2-Feb-2007/Presentations/09-DE-SOL-e.pdf>
117. Wilpert B. SOL – Safety through Organisational Learning. A Computer Assisted Event Analysis Methodology. http://erg.bme.hu/sol/SOL_Williamsburg5.pdf
118. Herrera I.A., Woltjer R. Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis. *Reliability Engineering and System Safety*, 95, 2010, p. 1269–1275.
119. Jørgensen K. A tool for safety officers investigating ‘simple’ accidents. *Safety Science*, 49, 2011, p. 32–38.
120. Hovden J., Albrechtsen E., Herrera I.A. Is there a need for new theories, models and approaches to occupational accident prevention? *Safety Science*, 48, 2010, p. 950–956.
121. Katsakiori P., Sakellariopoulos G., Manatakis E. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. *Safety Science*, 47, 2009, pp. 1007–1015.

122. IAEA Safety Standards Series No SSG-3. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. Specific Safety Guide. IAEA, Vienna, 2010.
123. Probabilistic Safety Assessment: An Analytical Tool for Assessing Nuclear Safety. <http://www.nuce.boun.edu.tr/psaover.html#6>.
124. Comparing Nuclear Accident Risks with Those from Other Energy Sources. OECD, 2010, Nuclear Energy Agency (NEA), No6861. ISBN 978-92-64-99122-4.
125. Probabilistic Safety Assessment (PSA). Japan Nuclear Energy Safety Organisation (JNES), 2007.
126. IAEA-TECDOC-1581. Best Practices in Identifying, Reporting and Screening Operating Experience at Nuclear Power Plants. IAEA, Vienna, 2008. ISBN 978-92-0-111507-2.
127. IAEA-TECDOC-1550. Deterministic Analysis of Operational Events in Nuclear Power Plants. Proceedings of a Technical Meeting held in Dubrovnik, Croatia, 23-26 May 2005. ISBN 92-0-101307-8.
128. Kirchsteiger Ch. On the use of probabilistic and deterministic methods in risk analysis. Journal of Loss Prevention in the Process Industries, Volume 12, Issue 5, September 1999, pp. 399-419.
129. Apostolakis G. E. How Useful Is Quantitative Risk Assessment? Risk Analysis, Vol. 24, No3, 2004, pp. 515-520.
130. Kubota R. Identifying and Overcoming Barriers to Effective Consideration of Human and Organisational Factors in Event Analysis and Root Cause Analysis. Proceedings of the Special Experts Meeting of the NEA Working Group on Human and Organisational Factors, Paris, France, September 21 – 22, 2009.
131. Kubota R. Viewpoint-Oriented Approach to Identify Organisational Factors in RCA. Presentation at Consultancy Meeting on Development of Root Cause Analysis Reference Manual. IAEA, Vienna, 2010.
132. The '5-Whys' Method. Intelligent Quality Management. <http://www.mapwright.com.au/newsletter/fivewhys.pdf>.
133. Salem W. An Integrated Method for Improving Risk Analysis Using Human Factors Methods and Virtual Reality. Dissertation. Otto-von-Guericke-Universität Magdeburg, 2009, p. 228. http://edoc.bibliothek.uni-halle.de/servlets/MCRFileNodeServlet/HALCoRe_derivate_00003254/Waleed_Salem.pdf.
134. Latino R. How Can Root Cause Analysis (RCA) Be Proactive? EVP Strategic Development, Reliability Center, Inc., 2010. <http://www.reliability.com/industry/articles/article33x.pdf>.
135. Latino R. Root Cause Analysis – Investment or Expenses? CEO, Reliability Center, Inc., 2010. <http://www.reliability.com/industry/articles/article33x.pdf>.
136. Dagon J.P. The practical use of Root Cause Analysis system (RCA) using REASON®: A building block, for accident/incident investigations. Presentation at the ISASI (International Society of Air Safety Investigators) seminar in Washington D.C., USA, August 2003.
137. Cook R., Jones S. A. Establishing Criteria for Evaluating a Problem Solving System. Presentation at the AIAA Space 2001 Conference and Exposition. American Institute of Aeronautics and Astronautics, 2001.
138. Vantine, W., Benfield, K., Pritts, D., & Ballard, K. Evaluating and Incorporating New Age Software Technology for Identifying Systemic Root Causes. Joint ESA-NASA Space-Flight Safety Conference. Edited by B. Battrick and C. Preyssi. European Space Agency, ESA SP-486, 2002. ISBN: 92-9092-785-2., p.369.
139. 10 Best Software Tools to Conduct Root Cause Analysis and Solve Complex Problems. <http://open-tube.com/10-best-software-tools-to-conduct-root-cause-analysis-and-solve-complex-problems>.
140. Alesso H.P., Prassinis P. and Smith C.F. Beyond fault trees to fault graphs. Reliability Engineering, Volume 12, Issue 2, 1985, pp. 79-92.
141. Shortus P. Using the Taproot Methodology in Accident/Incident Investigations. Presentation at 4th National Investigations Symposium, NSW, 7 & 8 November 2002. http://svc032.wic135dp.server-web.com/00_pdfs/phil_shortus.pdf

142. McManus K. How Do You Find Root Causes? <http://www.greatsystems.com/rootcause.htm#taproot#taproot>.
143. Root Cause Analysis Program Manual. LBNL/PUB-5519 (2), Rev. 1, July 18, 2008. <http://www.lbl.gov/DIR/OIA/assets/docs/OCA/IA/PUB%205519-2%20R1.pdf>
144. Sefton A. Taproot Methodology in Incident Investigation. Commentary on 4th National Investigations Symposium, NSW, 7 & 8 November 2002. http://svc032.wic135dp.server-web.com/00_pdfs/Anne_sefton.pdf
145. ESA Strategic Plan. Utility Advisory Council Presentation. Canada, May 2010. http://www.esaeds.info/pdf/3/A/2010/UAC_Presentation_May_27_2010.pdf
146. Milner T. Solving problems from first principles. Part one of a five part series. May, 2010. http://www.stroudconsulting.com/fileadmin/user_upload/pdf/solving_problems_first_principles_1_of_5.pdf
147. Weaver D.A. TOR analysis: a diagnostic tool. ASSE J., June 1973, pp. 24–29.
148. MIL-STD-1629A. Procedures for Performing a Failure Mode, Effects and Criticality Analysis. US Department of Defense, 1980.
149. Department of Energy (DOE). SSDC 76-45/27. Accident/incident investigation manual. 2nd ed., November 1985.
150. DOE Workbook. Conducting Accident Investigations. Revision 2, May 1, 1999. <http://www.hss.energy.gov/csa/csp/aip/workbook/aichapt2all.pdf>
151. Engblom-Bradley M. Quality Management Tools to Enhance Safety and Health. Petroleum Systems Integrity Office Division of Oil and Gas Department of Natural Resources. Presentation at the State of Alaska Governor's Safety and Health Conference, 2009. http://www.dog.dnr.state.ak.us/oil/programs/psio/quality_mgmt_pres_0309.pdf
152. Reason J. et al. TRIPOD, A principled basis for accident prevention. 1988.
153. Hata T., Makino M. Viewpoints to evaluate operator's' autonomous efforts to correct nonconformity corresponded to organisational factors analyzed by Root Cause Analysis. 2nd International Symposium on Symbiotic Nuclear Power Systems for 21st Century (ISSNP2008), Sep. 10, 2008.
154. Dechy N., et al. Results and Lessons Learned from the ESReDA's Accident Investigation Working Group. Safety Science, 2009.
155. Guidelines for Safety Investigation of Accidents. ESReDA, Working Group on Accident Investigation (Eds.). Oslo, 2009.
156. Ziedelis S. Survey on Existing Practices Related to Nuclear Event Investigation Methods, Tools and Techniques. European Clearinghouse on Operational Experience Feedback. SPNR/CLEAR/10 10001 Rev. 00, 2010.
157. Guidance on Investigating and Analyzing Human and Organisational Factors Aspects of Incidents and Accidents. Energy Institute, London, UK, May 2008, p.69
158. Effective Root Cause Analysis. Criteria for evaluating root cause analysis systems. http://www.root-cause-analysis.com/root_cause_analysis_detail.html

EUR 24757 EN – Joint Research Centre – Institute for Energy

Title: COMPARATIVE ANALYSIS OF NUCLEAR EVENT INVESTIGATION METHODS, TOOLS AND TECHNIQUES

Author(s): Stanislovas Ziedelis, Marc Noel

Luxembourg: Publications Office of the European Union

2011 – 204 pp. – 21 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1018-5593

ISBN 978-92-79-19712-3

doi:10.2790/3097

Abstract

Feedback from operating experience is one of the key means of enhancing nuclear safety and operational risk management. The effectiveness of learning from experience at NPPs could be maximised, if the best event investigation practices available from a series of methodologies, methods and tools in the form of a ‘toolbox’ approach were promoted.

Based on available sources of technical, scientific, normative and regulatory information, an inventory, review and brief comparative analysis of information concerning event investigation methods, tools and techniques, either indicated or already used in the nuclear industry (with some examples from other high risk industry areas), was performed in this study. Its results, including the advantages and drawbacks identified from the different instruments, preliminary recommendations and conclusions, are covered in this report.

The results of comparative analysis of nuclear event investigation methods, tools and techniques, presented in this interim report, are of a preliminary character. It is assumed that, for the generation of more concrete recommendations concerning the selection of the most effective and appropriate methods and tools for event investigation, new data, from experienced practitioners in the nuclear industry and/or regulatory institutions are needed. It is planned to collect such data, using the questionnaire prepared and performing the survey currently underway. This is the second step in carrying out an inventory of, reviewing, comparing and evaluating the most recent data on developments and systematic approaches in event investigation, used by organisations (mainly utilities) in the EU Member States. Once the data from this survey are collected and analysed, the final recommendations and conclusions will be developed and presented in the final report on this topic. This should help current and prospective investigators to choose the most suitable and efficient event investigation methods and tools for their particular needs.

How to obtain EU publications

Our priced publications are available from EU Bookshop (<http://bookshop.europa.eu>), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

