energy INSTITUTE

# Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents

# GUIDANCE ON INVESTIGATING AND ANALYSING HUMAN AND ORGANISATIONAL FACTORS ASPECTS OF INCIDENTS AND ACCIDENTS

May 2008

Published by
**ENERGY INSTITUTE, LONDON**
The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

The Energy Institute (EI) is the leading chartered professional membership body supporting individuals and organisations across the energy industry. With a combined membership of over 13 500 individuals and 300 companies in 100 countries, it provides an independent focal point for the energy community and a powerful voice to engage business and industry, government, academia and the public internationally.

As a Royal Charter organisation, the EI offers professional recognition and sustains personal career development through the accreditation and delivery of training courses, conferences and publications and networking opportunities. It also runs a highly valued technical work programme, comprising original independent research and investigations, and the provision of IP technical publications to provide the international industry with information and guidance on key current and future issues.

The EI promotes the safe, environmentally responsible and efficient supply and use of energy in all its forms and applications. In fulfilling this purpose the EI addresses the depth and breadth of energy and the energy system, from upstream and downstream hydrocarbons and other primary fuels and renewables, to power generation, transmission and distribution to sustainable development, demand side management and energy efficiency. Offering learning and networking opportunities to support career development, the EI provides a home to all those working in energy, and a scientific and technical reservoir of knowledge for industry.

This publication has been produced as a result of work carried out within the Technical Team of the Energy Institute (EI), funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit http://www.energyinst.org.uk

The EI gratefully acknowledges the financial contributions towards the scientific and technical programme from the following companies

BG Group
BHP Billiton Limited
BP Exploration Operating Co Ltd
BP Oil UK Ltd
Chevron
ConocoPhillips Ltd
ENI
E. ON UK
ExxonMobil International Ltd
Kuwait Petroleum International Ltd
Maersk Oil North Sea UK Limited
Murco Petroleum Ltd
Nexen
Saudi Aramco
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
Statoil (U.K.) Limited
Talisman Energy (UK) Ltd
Total E&P UK plc
Total UK Limited



ISBN 978 0 85293 521 7

Published by the Energy Institute

Further copies can be obtained from
Portland Customer Services, Commerce Way, Whitehall Industrial Estate, Colchester CO2 8HP, UK. Tel: +44 (0) 1206 796 351
email: sales@portland-services.com

Electronic access to EI and IP publications is available via our website, www.energyinstpubs.org.uk.
Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.
For more information, contact the EI Publications Team.
email: pubs@energyinst.org.uk

# CONTENTS

# FOREWORD

Simply attributing incidents/accidents to human error is not adequate; human factors aspects should be investigated such that lessons are learned to prevent recurrence. Each incident or accident is a learning opportunity, but one that can be wasted unless the effort put into investigating and analysing it focuses on discovering its true underlying causes rather than on the people directly involved and the immediate causes of their failure.

Whilst many petroleum and allied industry businesses investigate and analyse both incidents and accidents – whether with major hazards or occupational potential – human and organisational factors aspects are rarely addressed enough. This is particularly true for non-engineering aspects of HSE's priority human factors issues, such as supervision and organisational culture.

The problem is compounded by the volume of tools available to investigate and analyse incidents, many of which have some good points; however, none of them presents an ideal solution.

This guidance document has been developed following an extensive review of the literature on accident investigation, as well as from interviews and discussion with users and developers of these investigation and analysis methods. Some of the interviewees provided worked examples or case studies illustrating how the methods are used in practice.

This publication is aimed at anyone who is involved in an incident/accident investigation or analysis either as the lead investigator or part of the supporting team. The guidance has been devised for use by the experienced or novice user although it should be of most value to those who have experience in health and safety issues.

Further information and resources on accident investigation and human factors can be found on the Energy Institute's Human and Organisational Factors Working Group webpage:
www.energyinst.org.uk/humanfactors



Suggested revisions are invited and should be submitted to Technical Department, Energy Institute, 61 New Cavendish Street, London, W1G 7AR.

# ACKNOWLEDGEMENTS

This project was carried out by Bill Gall of Kingsley Management Services and was commissioned by the Energy Institute's Human and Organisational Factors Working Group, which comprised during the project:

| | |
|---|---|
| Fiona Brindley | Health and Safety Executive |
| Dr Robin Bryden | Shell International Exploration and Production B.V |
| Bill Gall | Kingsley Management Services |
| Kerry Hoad | EI |
| Pete Jefferies | ConocoPhillips |
| Rob Miles | Health and Safety Executive |
| Graham Reeves | BP plc |
| Dr Mark Scanlon | EI |
| Dr John Symonds | ExxonMobil Corporation |
| John Wilkinson | Hazardous Installations Directorate (HID) - HSE |
| Mark Williamson | Schlumberger Oilfield Services |

The Energy Institute gratefully acknowledges the valuable contributions that the following individuals and companies made to this project:

| | |
|---|---|
| Dr Kathryn Mearns | Aberdeen University |
| Prof Rhona Flin | Aberdeen University |
| Lee Vanden Heuvel | ABS Consulting |
| Denise McCafferty | American Bureau of Shipping |
| Andrew Livingston | Atkins Global |
| John McCollom | BAe Systems |
| Prof Graham Braithwaite | Cranfield University |
| Les Smith | DNV |
| Dominique van Damme | Eurocontrol |
| Dr Barry Kirwan | Eurocontrol |
| Rachael Gordon | Eurocontrol |
| Peter Ackroyd | Greenstreet Berman |
| John Chappelow | Human Factors Investigations |
| Dr Claire Blackett | Human Reliability |
| Euan Dyer | Kelvin Top-Set |
| Ronny Lardner | Keil Centre |
| Richard Scaife | Keil Centre |
| Prof Trevor Kletz | Loughborough University |
| Stuart Withington | Marine Accident Investigation Branch |
| Rainer Miller | Mensch-Technik Organisation |
| Louise Farrell | National Grid |
| Chris Mostyn | National Grid |
| Dr Steve Shorrock | NATS |
| Rudolf Frei Noordwijk | Risk Foundation |
| Prof Ann Mills | RSSB |
| Declan Kielty | Pfizer |
| Gerry Gibb | Safetywise Solutions |
| Mark Paradies | System Improvements Inc |

| | |
|---|---|
| Tjerk van der Schaaf | Technical University Eindhoven |
| Gerard van der Graaf | Tripod Foundation |
| Dr Linda Bellamy | White Queen BV |
| | Step Change in Safety Organisation |

The Energy Institute would also like to acknowledge the HSE for their financial contribution to the development and dissemination of this publication.

Project coordination and technical editing were carried out by Kerry Hoad and Mark Scanlon. Formatting by Joanna Stephen.

# 1 INTRODUCTION, SCOPE AND APPLICATION

This section introduces the key issues with current incident and accident investigation methods. It emphasises the importance of searching below the surface of an incident to identify root causes. It provides a case study and worked examples to illustrate the depth of analysis required in order to understand the human performance issues in an incident or accident.

*"To err is human, to forgive divine" – Alexander Pope, an Essay on Criticism (1711)* [1]

## 1.1 BACKGROUND

Many petroleum and allied industry businesses investigate both incidents and accidents whether these have process safety/major hazards potential or occupational safety potential only. However, in these investigations, human factors issues are typically not well addressed.

As an example, one company's accident report form includes a section for the investigator to describe the root causes of the accident. The section includes items such as 'lack of competence', 'inadequate procedures', 'inadequate tools or equipment'. To a human factors analyst, however, these are not **root causes**: the root cause in those cases would be the system deficiencies **that led** to poor competence, procedures and equipment.

In another company's report form, there is a blank space for entering root causes and example entries from real investigations include weather conditions, fatigue and even 'human error' as root causes identified by the analyst. Again, these are not **root causes**. These investigations should have probed further than this to explain the organisation's failure to deal with, for example, 'weather conditions' or 'fatigue'. These are, to a human factors analyst, **performance-shaping factors**, not **root causes** of error.

### 1.1.1 Making the most of incidents and accidents

*Experience has shown that accidents are rarely simple and almost never result from a single cause.* [2]

Each incident or accident is a learning opportunity, but one that could be wasted unless the effort put into analysing it focuses on discovering the true underlying causes of the incident rather than focusing on the people directly involved and the immediate causes of their failure.

Incident investigation is one of the tools for improving control over hazards in the working environment. It is a **retrospective** tool – applied once the flaws in our systems have drawn attention to themselves via an incident. Any modern organisation may also have in place proactive methods of observation, inspection and audit as complementary methods for improving hazard control. However, in using incident investigation methods, investigators should be aware that:

— Incidents often arise because of a highly unusual combination of underlying problems. The investigation may therefore deal with only that combination, and other factors that could have been identified in the investigation are left unchanged.

— High probability but low consequence (HPLC) incidents – 'everyday' mishaps that do not cause major harm – can become the main focus of an organisation's attention. HPLCs are very visible, typically less complex and thus easier to deal with than low probability high consequence (LPHC) events – disasters.

— Organisations can be deluded into believing that everything is under control but, in fact, the focus on these more easily managed problems can divert attention from more serious deficiencies. Organisations need to be sure that they are equally aware and in control of the factors that affect process safety and personal safety.

One possible cause of confusion between the types of incident is the concept of 'accident triangles' (or 'accident pyramids') developed from analysis of accident statistics. One of these, devised by HSE, is cited in Ref. [2]. It shows that, for every 189 non-injury accidents ('near-misses'), there should be around seven minor injuries and one major or over-three-day lost time injury. The key point made in Ref. [1], however, is that, 'not all near misses…should involve risks which might have caused fatal or serious injury.'

For example, a cleaner working in the accommodation block on an oil platform slipped on a mat that she had not noticed was wet underneath. She sustained bruising and minor cuts from impacting the edge of a doorframe.

This was purely an occupational accident with no major hazard implication. Any measures taken to prevent further similar incidents may not have any impact on major hazard incidents, for two reasons: first, HPLC incidents stem from different underlying causes – in the example, failure to use non-slip mats – and secondly, the remedies introduced are likely to focus on slips and trips in the accommodation block and on cleaning staff and not on operators or maintenance crew working more closely with very hazardous materials outside. The non-injury and minor injuries parts of the accident triangle may, however, diminish.

In effect, major hazard and occupational hazard incidents have separate 'triangles', though in some cases, these may overlap, for example, a dropped object, such as a heavy grinding tool, could strike a person, causing serious injury or death, or it could impact vulnerable pipework below causing a major leak of oil or gas with the potential for extensive plant damage, injury and loss of life. Protecting against the impact of dropped objects, then, may have an impact on both occupational and major hazard incidents. The key to understanding where the different triangles overlap and where they do not is, risk assessment – identifying hazards and the potential targets that could be affected by those hazards then devising suitable measures for controlling the specific hazards.

### 1.1.2 The importance of investigating incidents and accidents

*"It has been estimated that up to 90% of all workplace accidents have human error as a cause"* [3]

The above is one estimate of the contribution of human error to accidents (and refers to errors **and violations**). The term 'human failure' is used in this guide to refer to errors and violations: newspaper headlines tend to use 'human error' as a blanket term for both.

Whether the true figure is 90 % or some other higher or lower figure, it is clear from a wide range of sources of information that human failures make a significant contribution to incidents and accidents. An example of a recent study [4] for the maritime industry (which included UK data), found that:

*'…approximately 50% of maritime accidents are initiated by human error, while another 30% of maritime accidents occur due to failures of humans to avoid an accident. In other words, in 30% of maritime accidents, conditions that should have been adequately countered by humans were not.'* [4]

It should be noted that the remaining accidents causes were attributed to mechanical failures (up to 10 %) and it is almost certain that human error – for example in installing or servicing equipment – contributed to those failures.

### 1.1.3 Human failure in incidents and accidents

It is unfortunate that the phrase, 'human error' has become virtually meaningless through over-use and that it is usually interpreted to mean that the person 'at the sharp end' was at fault by committing some form of error or 'violation'.

It is easy to be misled and to believe that human errors arise because of carelessness, inattention, incompetence or reckless rule breaking by the workforce. However, the guidance in this publication should show that human errors occur because the systems for preventing them failed in some way. An incident, then, is not a **person** failure but a **system** failure and, to prevent further incidents, it is important to understand those systems: what they are, how they are intended to work and how, in specific cases, they have failed.

### 1.1.4 A human failure case study

The following case study and examples illustrate why it is important to seek out root causes of incidents and accidents. See Box 1.

**Human error caused blackout, says Transco**
(Headline, Daily Telegraph, 10/09/03; reproduced by permission)

National Grid Transco yesterday admitted "human error" had caused the London blackout of August 28, but denied suggestions it had been negligent or faced a fine.

An incorrectly installed fuse in a substation in Wimbledon, London, was cited as the cause of the power failure, which lasted just 37 minutes but left thousands of commuters stranded.

National Grid's official report on the failure said the fuse, installed by sub-contractors two years ago, had been too small to handle a power surge that occurred when another part of its transmission network failed. The power cut left 410,000 electricity customers without power.

Box 1

What should the company's reaction be to this event?

— Find the contractor responsible and take disciplinary action for negligence?
— Inform the contracting company that their staff are to be assessed and re-trained before they are allowed to work for the company again?

As indicated earlier, in order to identify the most effective course of action, the company should go deeper than this superficial reactive level to understand the true underlying human and organisational factors that caused the event. In this case, Transco took immediate action to examine all other similar relays in their system.

There were around 40 000 relays and none of them was found to be faulty. This suggests that, in replacing relays, there is a very low probability of error in performing the task.

Nevertheless, the error had significant consequences and without a full investigation, the company could not be certain that it has solved the underlying problem.

It is worth noting that, although the newspaper article highlighted 'human error' as the cause, this phrase was never used in the official report on the incident.

Detailed investigation of the above incident led to the conclusion that it was a contractor error. But since this was an error 'lying in wait' (a 'latent failure') for two years before it revealed itself, it was impossible to ascertain what sort of failure it was ('error' or 'violation', 'slip', 'lapse', 'mistake') let alone the underlying causes.

The company found that the engineers involved in the commissioning of the equipment had the appropriate training, authorisation, experience and skills to undertake the task. Competence, then, did not seem to be the issue. It would be possible, but not worthwhile so long after the event, to speculate on the range of influences on the task, but it should be noted that one finding from their detailed report indicated that:

'…the rating of the automatic protection equipment that is included on the documentation used for commissioning could have been more clearly visible to the commissioning engineers.'

In other words, there was a problem in the documentation/procedures used.

This simple problem surely then has a simple solution: correct the documentation to improve the information provided. It is not clear whether an independent check is done following the fitting of these critical components but, again, this would help. The independent check, though, should not use the same documentation used by the fitter.

However, to gain more from the investigation, investigators should understand **why** there was a problem with the documentation. What was the deficiency in the **system** for producing procedures that led to this incident and could the same deficiency have affected other procedures?

### 1.1.5 Incident causes and solutions

Table 1 describes three incidents alongside the investigation findings and solutions proposed. The last column of the table describes why the investigations and thus the solutions are inadequate.

**Table 1: Example incident investigations**

| Incident | Cause of human error | Proposed solution | Comment |
|---|---|---|---|
| 1. A road tanker driver refuelling their vehicle left it unattended; diesel spilled onto the forecourt of the refuelling bay, requiring clean-up and causing delay to other drivers | The driver did not comply with company procedures for refuelling; they had left their vehicle unattended to speak to a colleague | Discipline the driver and warn others. Consider removing the locking trigger mechanism on filler nozzles or add an automatic cut-off | The investigation did not explore underlying causes of the violation such as:<br>– the driver needed urgent information from his colleague<br>– they were under time pressure (real or imagined)<br>Regarding the proposed solutions:<br>– removing the locking trigger could encourage drivers to improvise a locking mechanism (though installing a cut-off mechanism would prevent spillage)<br>The issue of 'culture' is not explored - the role of his colleague and other observers in discouraging this behaviour |
| 2. A control room operator heated up a vessel too rapidly; liquid boiled off and ignited | Two pushbuttons- one to increase and one to decrease the flow in the heating coils were laid out in a non-standard and confusing arrangement - upper button = decrease, lower button = increase | Rearrange the controls; include a clear warning in procedures about the controls and regarding heating rates | The investigation did not explore why the controls were laid out that way. It could be due to system procurement procedures, culture (why not reported or if reported acted upon before it led to an incident?) A systematic review of other critical controls may be required<br><br>The existing layout is poor, but people are used to it. The change may lead to more errors.<br>For the immediate fix, a better solution would be to replace the buttons with a more appropriate slider, rotary knob or other device |
| 3. A maintenance fitter omitted to remove a blanking plate from a relief line: the line leaked inside the plant when it came under pressure | The fitter had worked on similar vent lines but using in-line block valves rather than blanking plates. A supervisor signed off the worksheet but did not query each of the completed 'tick boxes' | Issue a reminder notice to fitters regarding isolations; improve fitter’s training on the plant; brief all maintenance supervisors on the importance of closely monitoring critical tasks and to check work thoroughly | The cause for the error may be resourcing: for example, using less experienced personnel may be seen as a necessary short cut to get the job done. Lack of resource could also explain why supervisors are rushed and unable to properly supervise |

The more 'levels' of analysis that are applied to an investigation should produce better results in terms of the findings they generated regarding the underlying problem and thus the solutions required. This is essentially the process of continuing to ask, 'why?' and not stopping at the 'level 1 or 2' answers.

**Table 2: Levels of analysis of an investigation**

| Incident description: an operator using a new pipe cutting machine trapped and badly injured their hand whilst reaching in to retrieve the pipe | | | | |
|---|---|---|---|---|
| **Poor** | ← | **Analysis** | → | **Better** |
| Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
| Operator is to blame for reaching into the machine whilst still switched on | Operator believed that lifting the guard would disable the machine | Operator had already received training; the machine used in training is interlocked | The machine was not tested before being put to use | The machine was needed quickly; the procurement process did not identify that the machine purchased did not have a safety interlock |
| | | **Response** | | |
| Discipline the operator | Re-train the operator in all aspects of operating the machine | Train on same machine as used on site | Review and consider amending the procedure for introducing new equipment into the workplace | Review and consider amending the procurement procedure to include a more thorough risk assessment |

The investigation methods described in this publication (see Annex C) do no more than guide the user through a process of thinking through a problem to a root cause level. They do this by describing tested approaches and providing, in some cases, flowcharts and checklists to make the analysis easier to carry out and to try to ensure that the user reaches 'level 5' in their analysis of incidents.

## 1.2 PURPOSE AND SCOPE

This document has been prepared as a guide to good human and organisational factors analysis in incident and accident investigations and should:

- help the reader to learn more about the true system and organisational root causes of incidents and accidents;
- describe the elements of a good human and organisational factors investigation of an incident or accident, and
- describe available incident and accident investigation methods that can identify human and organisational elements of incidents whether occupational or major hazards.

## 1.3 APPLICATION

The publication has been derived partly from interviews with users and developers of the methods described. Interviewees have strongly suggested that, to succeed in finding the human and organisational root causes of an incident the analyst should have at least a basic level of competence in human and organisational factors. This competence can be acquired through formal training, focused background reading or through the experience of conducting accident investigations. For this reason, section 2 describes the basic concepts underlying many of the methods described. This on its own may not be sufficient to produce the level of competence required but should make it clear to readers whether or not they need further training or experience in order to carry out successful analyses.

The approach taken to incident investigation should be a holistic one rather than the human factors issues being investigated only as 'a last resort' once engineering-type immediate causes have been eliminated. To facilitate this, the investigation team should have human factors expertise from the outset.

This publication is aimed at anyone who is involved in an incident investigation or analysis either as the lead investigator or part of the supporting team. The guidance has been devised for use by the experienced or novice user although it should be of most value to those who have experience in health and safety issues.

# 2 HUMAN FACTORS, SAFETY MANAGEMENT AND SAFETY CULTURE

This section describes the basic concepts that have been used in developing the investigation and analysis methods reviewed. It is essential reading for anyone not familiar with human factors, safety management, safety culture or related issues. It is not a substitute for in-depth knowledge but should enable the reader to determine their level of knowledge and from that to judge whether they require further training or competent assistance.

## 2.1 AN OVERVIEW OF HUMAN PERFORMANCE MANAGEMENT

Human factors is concerned with optimising human performance in all tasks and, in major hazard organisations, the primary intention is to achieve **safe** performance. These organisations should have conducted risk assessments and put in place a range of controls to prevent major accidents but should also focus on human performance issues to eliminate or reduce human failures.

An organisation's safety management system (SMS) can be thought of as the organisation's integrated set of processes that support human performance. The SMS does this through implementing policies, organising resources and measuring performance. Safety culture affects the way management and workforce approach safety and has a direct influence on the success of the SMS.

A good starting point for developing an understanding of human factors, safety management and safety culture issues is the EI's Human factors briefing notes [5] and HSE Managing human performance briefing notes which are aimed at lower tier COMAH sites and covering the key issues [6].

A very brief overview of these topic areas is provided below in Table 3.

There is a clear link between the three topics listed in Table 3; all are concerned with optimising human performance. For example, a key influence on task performance is personnel competence. The SMS should include all of the selection, training, assessment and development processes necessary to ensure competence. The organisation's safety culture has a direct influence on the effective functioning of the SMS in that, if management regard training as simply a means for meeting legal requirements for competence, then the system would not work as well as if there were a more positive attitude to staff development.

## 2.2 HUMAN FAILURE TYPES

To make sense of the information gathered in an incident investigation and in particular, to develop appropriate recommendations for improvement, at least the basics of human error should be understood. This section provides an outline only of the principles involved. If more in-depth analysis of these issues is required, further information should be read or a human factors specialist consulted.

The basics are:

— there are different recognisable **types** of human error, and
— there are numerous factors that affect human error.

**Table 3: Key human factors topics**

| **Topic** | **Brief definition** | **Example issues** |
|---|---|---|
| Human factors [7] | Environmental, organisational and job factors, also human and individual factors that influence behaviour in a way that can affect safety | A drilling company reviewed working conditions for all its critical tasks including:<br>– Environmental – temperature, humidity, lighting, noise<br>– Job – task demands (physical and mental), provision and suitability of tools, equipment and procedures<br>– Individual/personnel – team selection and organisation, competence, personality |
| Safety management [2] | The HSE advocate the POPMAR framework for successful health and safety management. This means: set effective health and safety policy.<br>Put in place the organisation necessary to implement the policy; involve everyone in contributing to health and safety so as to foster a good safety culture.<br>Use hazard and risk assessment methods to plan and put in place controls against identified hazards.<br>Measure performance proactively through self monitoring systems against specific standards<br>Use independent audit and self monitoring Review findings to assess and continually improve performance. | Petroleum spirit is the main hazard at a depot. Management have made all arrangements for controlling the hazard by introducing various 'barriers'/safeguards. Some are physical engineered barriers, others are 'administrative' e.g. procedures/safe systems of work. There is also a near-miss reporting system for use by all staff. |
| Safety culture [8] | Organisational attitudes, beliefs and ways of working that place high emphasis on safety | In the example in the row above, although the reporting system is known to everyone and available, it is not used because the workforce fear management sanctions if they report incidents for which they could be blamed. |

These basic facts are important in making improvements. For example, if an incident occurred because someone took a reading from the wrong gauge and this resulted from confusion because the gauge was next to the one that he should have read, retraining the person in reading these devices would be less effective than re-designing or repositioning the gauge. This illustrates that different types of human failure require different responses to secure improvements and that solutions from higher up the 'hierarchy of control' need to be considered. This would entail asking:

- Can the hazard be removed?
- Can the human element be eliminated, e.g. by automation?
- Can the consequences of the human failure be prevented, e.g. by additional barriers in the system?
- Can human performance be assured by using interlocks or other engineered means?
- Can the performance shaping factors be changed to be more positive?

HSE's document, HSG 48: *Reducing error: Influencing behaviour* [7] describes the well-known categories of human error: 'slips', 'lapses' and 'mistakes'. A simplified version of this description is given in Table 4.

Note also that violations fall into several categories from deliberate sabotage (which is rare) to 'routine' everyday breaches of procedure. Further information on this can be found in the 'Hearts and Minds' material on the Energy Institute's website at: http://www.energyinst.org.uk/heartsandminds/rule.cfm

**Table 4: Definition and examples of human error types**

| Error type | Description | Examples | Potential error recovery mechanisms |
|---|---|---|---|
| Slip | When a person forgets to do something due to a failure of attention/concentration or memory | i) Plant operator pressed the start button for 'pump A' instead of 'pump B'<br><br>ii) Petroleum blender keyed in the wrong proportion of benzene to produce a batch of fuel<br><br>iii) Welder ground off too much material when finishing a weld | i) Alarms would sound in response to the wrong pump being started; other plant indications would alert the operator to the error, other plant operators might notice that the expected flow is absent<br><br>ii) In checking progress of the blending process, the blender may notice their error; laboratory samples taken at intervals should identify the error<br><br>iii) The welder should check the quality of the weld; for high integrity welds, a senior supervisor should check; final testing of the system before putting into service may show flaws in the weld |
| Lapse | When a person forgets to do something due to a failure of attention/concentration or memory | iv) A tanker driver forgets to set the blend indicator on their tanker and fills the compartment intended for LRP with unleaded<br><br>v) Control room operator misses a step in a plant start-up sequence after taking a phone call mid task | iv) The driver may check their docket before starting the delivery and realise their error: this is an example of an error where recovery may not occur<br><br>v) Normal alarms are likely to be disabled for start-up and the error may be unrecovered; plant indications or colleague/supervisor checks (if planned into the start-up) may act as a cue to the operator that they are at the wrong stage in the start-up process; interlocks may stop the process from proceeding further following the error |
| Mistake (also known as a 'cognitive' error) | When a person does what they meant to do, but should have done something else. This is not necessarily a 'violation' (see below) but part of the action taken could involve rule-breaking or similar non-compliances | vi) A busy fitter investigating a leaking water pipe 'nips up' the flange and notices that the leak stops. He thus diagnoses the problem as an incorrectly tightened flange but the real problem is a poorly fitting seal (the leak worsens later)<br><br>vii) A power operated relief valve has stuck open; the operator does not know this since the panel shows that power is off to that valve; believing the valve is closed leads to the conclusion that the pressure and level drop is due to a pipe break | vi) This may not be recovered before a more serious failure occurs as a result of damaging the seal further or over-tightening the flange studs<br><br>vii) Difficult to recover from quickly as people have a tendency to make evidence fit their existing conclusion; it may be recovered by plant operators noticing materials venting to atmosphere or monitoring other plant variables such as pressure controller valve opening |

**Table 4 continued.**

As well as errors, personnel can also commit violations:

| Error type | Description | Examples | Potential error recovery mechanisms |
|---|---|---|---|
| Violation | When a person decided to act without complying with a known rule, procedure or good practice | viii) The first mate of a tank barge crew reports for duty knowing that he has already exceeded his working hours for the day<br><br>ix) Plant operators open a by-pass valve to speed up filling of a tank but forget to close it again | viii) Violations are difficult to recover from; fitness for duty procedures (if in place and enforced) may pick up the mate's fatigued state<br><br>ix) Alarms fitted to the tank may indicate that the tank is unexpectedly filling (or emptying) |

It is important during the course of an investigation to establish whether the human failures in an incident were errors or violations: the remedies for errors may be quite different from those appropriate to violations and even between different sorts of errors – slips, lapses, mistakes – the solutions vary.

In general, errors of the above types result in either:

| | |
|---|---|
| An error of omission | Something is not done that needs to be done |
| An error of commission | Something is done but is done incorrectly |

In addition, it should be noted that an error of commission such as operating the **wrong** device would also involve an error of omission because the device that **should** have been operated is **not** operated.

A distinction is also often made between 'active' failures – those that have an immediate and usually visible effect; and 'latent' failures – those that 'lie in wait' in the system, as in the National Grid Transco example given in section 1.1.4, sometimes for many months before causing a problem.

Generally, any safety critical system* intended for human use should be designed to provide multiple defences. This is sometimes referred to as a 'forgiving' system. In such a system, a single human error should not lead to a serious incident. In the examples given in Table 2, several opportunities or 'mechanisms' for recovery from the error are given; in some cases, there would be no effective recovery.

* For the purposes of this guidance document, a safety-critical system is any part of an installation whose failure could contribute substantially to a major accident or whose purpose is to prevent or limit the effects of such accidents. This definition is adapted from that of 'safety critical elements' in the Offshore Installations (Safety Case) Regulations 2005 [9].

An important tool in proactively reducing human errors is risk assessment. According to HSE's document, 'Five Steps to Risk Assessment', "a risk assessment is nothing more than a careful examination of what, in your work, could cause harm to people, so that you can weigh up whether you have taken enough precautions or should do more to prevent harm." An effective risk assessment should determine which tasks are the most critical and require additional or more effective barriers. By contrast, incident investigation seeks to retrospectively identify where barriers have failed and make improvements based on the experience gained.

## 2.3 A USEFUL FAILURE MODEL

Table 5 is based on the work of James Reason [10]. It illustrates how a human-machine system can fail and introduces the main ideas about human errors that would be useful in understanding the origins of incidents and accidents. These ideas feature in a wide range of the methods described in this publication. In this context a human-machine system is one in which technology and human beings have specific functions but work together towards common goals.

Any accident can be thought of in terms of a 'hazard' having a harmful effect on a 'target'. Example hazards are: toxic chemicals, heavy objects, sparks or flames, high pressure in some form of containment. Example targets are: plant and equipment, people, products, the environment.

**Table 5: Origins of incidents and accidents**

| Organisational decisions | Latent failures | Psychological precursors | Unsafe/sub-standard act | Operational disturbance | barriers | Accident | barriers | Consequences |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

### Working from right to left in Table 5:

**Consequences:** the damage caused to the target by the hazard e.g. crude oil is accidentally spilled into the sea killing marine life. In the case of a near miss, the concern is for the potential consequence (e.g. a fitter working up a ladder drops a 2 kg hammer that narrowly misses a small bore fuel line).

**Barriers:** may be physical barriers: fences, guards, bunds, protective clothing, safety devices or 'administrative' barriers – checking procedures, permits-to-work, supervision. E.g. A pipe is depressurised and drained prior to removing a pump. A drip tray is placed under the pipe in case of leaks, also, the permit-to-work requires a second fitter to ensure that the pipe is isolated and drained and to sign the permit-to-work when he has completed the check. From the above, it is clear that there are two types of barriers: those designed to prevent incidents and accidents and those designed to counteract or reduce the consequences of an accident. See 2.4 for a further discussion of barriers.

**Accident:** the event itself.

**Operational disturbances:** these are events where an action (or inaction) by the person reduces the level of control over a task; such a disturbance **could** result in an incident or accident. E.g. a small pump was being lifted by a sling attached to an eyebolt on the pump. This was a 'blind lift' and the load snagged causing the eyebolt to fail and the pump to drop several feet. The decision to use the eyebolt to lift the pump and the decision to conduct a blind lift were both 'sub-standards acts' leading to the operational disturbance of lifting the load in this manner. An incident may not have occurred in this instance but did.

**Unsafe/sub-standard acts:** these are the human behaviours that lead to the operational disturbance. In the original human error model derived by Reason, there is no intermediary stage 'operational disturbance': an unsafe act can lead to a challenge to a barrier. If the barrier is ineffective, then an accident or incident ensues.

**Psychological precursors:** the state of mind of the person would determine the type of unsafe/sub-standard act carried out. It is not possible to know their state of mind at any given time but certain factors could affect a person's state of mind more than others: time pressure, lack of competence etc.

**Latent failures:** in contrast to active failures that lead to an immediate consequence, latent failures can remain dormant in a system until some later event reveals them. An example is the Transco incident cited earlier in which a faulty fuse was fitted into a system – this was a human failure – but this led to a consequence only when a demand was made on that fuse some months later. More deep-rooted latent failures are those that stem from faulty organisational decisions (see below). These can create the conditions from which errors later emerge. Such conditions include: poor selection or design of plant and equipment, inadequate training of personnel, ineffective supervisory practices, inaccurate communications, poor team structuring etc.

**Organisational decisions:** within this model, decisions made within the organisation about how to manage all the tasks carried out are the ultimate root cause of incident and accidents at the 'sharp end'. The **ultimate** root causes may thus be the factors that affect *those* management decisions, but this is a level of complexity that we do not need to touch on here.

## 2.4 BARRIERS

From 2.3, it follows that an incident can be thought of as the end result of a number of failures in various types of barrier ('risk control systems'). Those barriers – also referred to as safeguards or defences, could be physical barriers or procedures that act as a barrier against sub-standard human performance.

A popular model describing the failure of barriers, and one that is referred to in several incident analysis methods, is the 'Swiss cheese' model (see Figure 1) [10]. Swiss cheese is the type that has holes in it when sliced through. Similarly, any barrier can be thought of as having 'holes' in it that make it less than perfect. A guard, for example, might literally have a hole in it that swarf from a cutting tool could be ejected from; a permit-to-work may be poorly worded or laid out so that it is not used correctly, i.e. the permit-to-work system has 'holes' in it. Against most hazards, there should be several barriers. They can be imagined as slices of Swiss cheese between the hazard and a possible 'target'. The hazard could pass through all the barriers and hit the target if all the holes in barriers happen to line up.

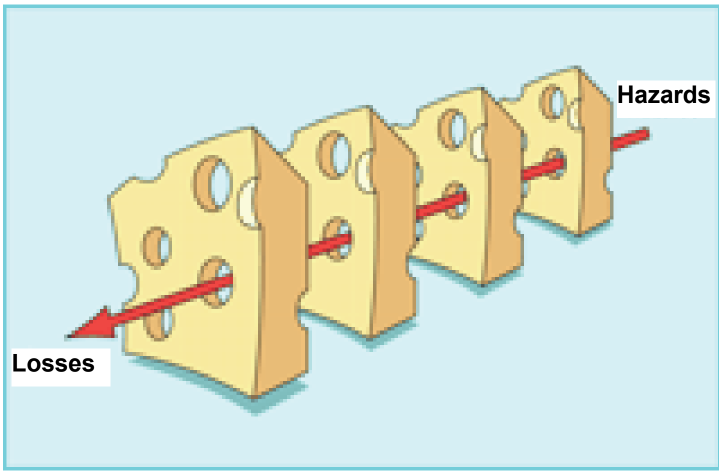


**Figure 1: 'Swiss cheese' model**

## 2.5 THE 'JUST' CULTURE – WORKFORCE AND MANAGEMENT

Aware that incidents and accidents are so rich a resource for identifying management and organisational problems, UK industry is maturing in its approach to 'blame' and no longer seeks to identify the person at fault in an incident. The idea of a 'no blame' culture, however, has been largely replaced by the idea of the 'just' culture; meaning that blame should be assigned only to those who have been reckless or clearly negligent in their work, i.e. the 'just' culture does not remove individuals' accountability.

It is almost inevitable that a thorough root cause analysis of an incident would very often lead back to management and organisational deficiencies, that is, it is likely that management decisions would be the underlying cause of most 'sharp end' error. A consequence of this that has been noted in some reviews of incident investigation systems is reluctance on the part of management to delve too deeply into incidents in case this reflects badly on the arrangements that they have put in place. However, the 'just' culture principle should be applied at all working levels in an organisation: pressures on management, similar to those of the workforce, should be recognised and accounted for. It is possible that safety management systems (SMS) need to be changed not only to reduce failures at the shopfloor level, but also at the management level.

## 2.6 INFORMATION PROCESSING

Several human factors-oriented incident investigation methods are based on models of human information processing – frameworks for describing 'how humans think'. On a basic level, the frameworks are similar:

**Input – Processing – Output**

The frameworks show the 'sub-processes' at each stage; that is, how information is input into the system (via our senses); how memory is involved in comparing stored information with new information or with storing new information; how information is processed and how this leads to the right or wrong output/action.

These are useful in investigations by pinpointing where the information processing system 'broke down'; the investigator could consider each element of the information processing model to determine, for example, if there was a breakdown at the input stage: what information was available, was it in the correct form, was it presented in the correct sequence, was it presented to the right person etc? This type of investigation would then provide useful pointers towards solutions that focus on the specific breakdown in the information processing task.

# 3 LIFECYCLE OF AN INCIDENT OR ACCIDENT INVESTIGATION

This section describes the key stages of an investigation and the elements at each stage required in order to ensure that human and organisational factors are appropriately addressed in the investigation.

The information that follows describes the various stages of incident investigation and should enable organisations to determine whether they have suitable arrangements in place at each stage to gain maximum value from their investigations.

The lifecycle of an incident investigation begins with detecting and reporting the incident and ends with the close-out of the remedial actions identified by the investigation and analysis process. The stages are described below with (in italics) a number of tips and cautions for each stage.

## 3.1 REPORTING

When an incident or accident is detected, it should be formally reported and recorded.

Organisations use various means of reporting incidents: this may be via a paper form or using an on-line system. Serious incidents should also be reported externally to regulators. Note that a system that includes near misses, plant damage incidents and other events short of actual accidents would be more valuable than one that deals only with accidents.

Reporting should be rapid to ensure that an investigation is begun as soon as possible after the incident: people have a tendency to forget things, 'reinvent' history or unduly influence each other by discussing an incident before it can be properly investigated. Care should be taken to preserve evidence at the scene.

*All employees should be familiar with the system and encouraged to use incident (near miss) reporting systems. A culture of mutual trust between workforce and management is required. The system should be a 'just' system (see section 2.5) where the blame for incidents is not automatically assigned to the person involved in the incident but is based on a fair system.*

*Confidential reporting may be considered where the culture of trust and fairness is not established. Employees and contractors are able to submit anonymous reports of incidents or unsafe acts. Management should decide whether to investigate based on the information provided.*

## 3.2 INVESTIGATION

Once an incident has been reported, the next logical step in the examination of the incident is typically the initiation of the investigation.

The 'level' of an investigation is usually determined by the severity or possible severity of the consequences of an incident. For the more serious incidents:

— the investigation is more likely to commence sooner;
— the investigation team should be better resourced (more extensive in numbers and competencies – both investigation and human factors/safety management and safety culture competencies) and include more senior members of the organisation, and
— there should be rapid feedback and remedial actions.

Various investigation methods may be deployed. HSE *Investigating Accidents and Incidents*[11] provides a good overview of the investigation stage and the need to establish:

- what happened;
- who or what was affected and to what extent;
- what were the conditions like;
- what was the chain of events (what happened just before the event and just before that);
- what was going on at the time, and
- was there anything unusual/different in the working conditions etc?

Investigators should look more widely than the immediate 'actors' in the incident and determine, for example, how other shifts conduct the task of interest, whether they have experienced problems such as near misses etc.

Many of the specific methods described in Annex B of this publication contain more detailed guidance but the HSE guide is a useful starting point. Chapter 5 of HSE guide [2] also contains some simple useful guidance on this and section 8.3.5 of the American Institute of Chemical Engineering's guide provides some specific guidelines on interviewing witnesses. (See Source materials after References (Annex C))

*Regarding team competencies – all investigation teams should have at least a basic level of competence in human factors. This should be sufficient to recognise where additional help is required on human factors issues. This is difficult on the basis that, 'you don't know what you don't know', but this publication should help investigation teams to determine if they have sufficient knowledge of human factors to make this decision.*

*Investigation processes should be clear, open and objective to avoid 'contaminating' the evidence or following false trails, for example by:*

- *making assumptions;*
- *asking leading questions;*
- *causing concern or suspicion among witnesses, and*
- *failing to use systematic methods or using checklists or aids that could be misleading.*

*It is to be expected that evidence may not be readily available or necessarily clear-cut and may be: incomplete, inconsistent/contradictory, ambiguous, misleading or false. A useful rule of thumb is to accept evidence as a conclusive finding if it is supported from at least two independent sources. This is not always possible and the analyst should have to decide whether to use a single finding as 'evidence'. This is usually based on the importance of the finding e.g. if it suggests a serious deficiency in an organisation's SMS; single findings can be 'tested' by asking those involved in the incident if they agree or disagree with it. In general, where any assumptions are made, these should be explicitly stated in the investigation report.*

*Management should be committed to the investigation process and the organisation as a whole should show a clear willingness to learn from incidents. This should entail supporting analysts in investigating to the level of management and organisational factors involved in an incident. Analysts must resist any perceived or actual pressure to restrict their investigation.*

## 3.3 MAKING RECOMMENDATIONS

Based on the evidence gathered from the investigation, the investigating team should make recommendations for improvement.

Recommendations should naturally follow from the findings of the investigation; that is, it should be clear what to do. If the findings go to the necessary depth, that is, to the real underlying causes, then the recommendations should be well focused.

*It should be ensured that the team making recommendations has an understanding of human factors, human error, safety management and safety culture concepts. Without this, it is possible that recommendations may not be correctly targeted. If the basic knowledge and skills in these topic areas is missing from the investigation team, make use of methods that contain appropriate checklists or guidance or seek assistance from an expert.*

*The investigation should lead to 'SMART' – (Specific measurable achievable relevant and timebound) – recommendations. Recommendations should aim, ultimately, to strengthen the safety management system.*

## 3.4 ASSIGNING, TRACKING AND CLOSING OUT ACTIONS

The recommendations generated in 3.3 should be turned into practical measurable actions.

Action should be based on what would be the most effective. Superficial to more deep-rooted issues e.g. fix an immediate problem, check on equivalent problems but also look at the meaning of the problem – what does the problem suggest might be wrong about how things are currently controlled and what needs to be done to fix these underlying problems. Consider the 'hierarchy of controls' that can be applied (see section 2.2).

*Actions should be very specific even if the recommendation is 'examine this further'. Terms of reference for any further investigation should be set out and clear objectives determined.*

*Actions would succeed best in an environment in which the systems available, the culture and management support are focused on supporting them; they may actually fail entirely without this support*

*Actions should be assigned to a specific person or group who should own the action until it is resolved. Even where groups are responsible for undertaking the action, one person should be ultimately accountable to make sure this happens.*

*Actions should be time-bound with a specific end-date for completion and for any interim stages.*

*It should be clear when an action is complete. Specific criteria may be set and evidence provided to demonstrate that the criteria have been met. Further criteria and measures should be set to demonstrate that actions have been effective. This is likely to be difficult and the measures may be long-term. Audits may be required to determine whether the remedial actions and recommendations continue to be followed.*

## 3.5 SHARING INFORMATION

An organisation should share lessons learned across sites on lessons learnt from incidents and accidents and may wish to share information with other organisations.

*Some systems have a facility for sharing information in the form of forums or alerts that can be posted on intranet or internet sites. Bulletins may be issued by email or on notice boards. Toolbox talks and safety meeting presentations may also be used to disseminate learning experiences.*

# 4 KEY FACTORS INFLUENCING HUMAN FAILURE

This section provides a brief checklist of factors that have been identified as having a significant effect on human performance. It can be used as a preliminary guide to help identify some of the underlying causes of incidents; however, there should be a more thorough analysis.

The list of factors in Table 6 below has been extracted and summarised from the investigation methods reviewed: these factors have the most significant effect on human performance. The table can be used as a high-level checklist in an investigation to ensure that key human and organisational factors are considered.

Some factors should be long-term conditions – for example, poor lighting in a work area that eventually contributes to an incident. Others should be short-term/short-lived factors that affected performance on the day of the incident – for example, the state of health of a team member on a particular shift.

The following factors set out below:

- workplace;
- task;
- personnel, and
- organisational,

can be combined with the usual six questions:

- where;
- when;
- what;
- how;
- why, and
- who,

to produce the initial lines of enquiry in an incident investigation/analysis. 'Where did the incident take place?', 'What features of the workplace contributed to the incident?' etc.

**Table 6: Factors affecting human performance**

| **Workplace factors** |
|---|
| – Workspace unsuitable for the job – too small, workstations widely spread out or in wrong place, excessive stretching or reaching required<br>– Housekeeping – untidy, hazardous conditions, poorly maintained<br>– Equipment/tools/materials unsuitable or used incorrectly<br>– Systems not resilient to failure – few or no recovery opportunities<br>– Interfaces sub-standard – displays unclear or confusing, too much information or too little, alarms inadequate<br>– Environment poor – temperature, lighting, noise, weather etc. |
| **Task factors** |
| – Tasks poorly designed – unstimulating, not matched to personnel competencies – rely unrealistically on sustained detailed attention to the task, perceptual skills, vigilance, memory, problem solving, judgement, decision making or timely correct action<br>– Workload too high/too low, time pressure, many interruptions/distractions<br>– Job hazard assessment not done or poorly communicated<br>– Emergency tasks – not well-prepared or practised<br>– Teamwork problems – poor communications/coordination, poor allocation of tasks, team decisions poorly supported<br>– Procedures or safe systems of work – not available, unclear, out of date, not used |

**Table 6 continued.**

| **Personnel factors** |
| --- |
| – Competence – lack of aptitudes, training, experience<br>– Health and fitness of personnel<br>– Fatigue<br>– Stress<br>– Motivation/job satisfaction low<br>– Use of prescription or recreational drugs including alcohol |
| **Organisational factors** |
| – Supervision inadequate, poor leadership<br>– SMS inadequate – procedures and processes, proactive and reactive systems, auditing and improvement<br>– Safety culture poor – attitudes, beliefs, behaviours<br>– Change management poor – new equipment, methods, training, organisational structures not introduced adequately |

# ANNEX A
# SELECTING AN APPROPRIATE METHOD

## GENERAL CAUTIONS AND GUIDANCE

Extracting useful information from incidents is done in two main stages:

- Investigation – gathering information that should allow time-lining, event sequencing or other means of reconstructing the incident.
- Analysis – thorough and systematic review of the structured information in order, ultimately, to identify the root causes of the incident.

From the research of methods included in this publication, it is clear that incident investigation and analysis is not as easy a process as it may appear. Many investigators do not use any specific methods to analyse human factors issues. They often rely only on their own extensive experience and expertise either in investigations or in 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 the familiarity with human and organisational factors – of the team using them.

If an investigation team is confident that it has sufficient expertise in human factors, then the most basic method – a wallchart and pens/yellow stick-on notes – should be adequate, perhaps supported by the checklists and flow diagrams contained in some of the methods set out in Annex B. Note, however, that certain methods with extensive supporting materials may still require a good level of human factors knowledge to understand and use them. Most of these are proprietary commercially available methods, however, and are provided on the basis that the buyer undertakes the necessary training.

The two key cautions to observe, then, are related to expertise/competence in human factors and in analytical methods (see Table A1):

**Table A1: Expertise/competence in human factors and analytical methods**

| Caution | Problem | Recommendation |
|---|---|---|
| Expertise | Insufficient skills or experience to use very simple or very technical methods.<br>Loss of skills/practice | Be honest about the level of expertise in the investigation team. This should include expertise in the human performance elements of the tasks being investigated (those being conducted when the incident occurred). Workforce representatives can bring valuable expertise in this respect.<br>Make time for self-training or<br>Attend training course provided by suppliers of methods<br>Use the methods and keep up to date with developments. Practice on 'old' incidents or on normal operations e.g. to explore barriers, possible human errors etc.<br>If all else fails, seek help from a professional investigator/analyst; if possible, use their expertise as a learning opportunity for internal staff. |
| Checklists | Checklists of factors or root causes can tunnel the analyst's thinking down certain tracks.<br>Checklists may be incomplete | Be aware of the problem. Use checklists as an initial prompt or *aide-memoire*. Seek additional help. Use a variety of checklists or expert help to provide guidance on issues to explore. |

Table A2 should be of help in the selection of the most appropriate method for an investigation. From reading the earlier sections of this publication and the cautions set out in Table A1, it should be possible to decide on the type of method that the team needs and is able to use. The criteria are not detailed but are intended to steer the reader towards finding out more about a particular method before making a final selection. Note that a simple method may be better during the early stages of investigating a complex incident, moving to a more complex method when the investigation team has developed initial insights into the incident.

Table A2 has been populated with the most accurate information made available during the course of this research on the methods described. The developers of the method described were all invited to provide their view of the features and most of them supplied information. The authors of this publication document have reviewed all ratings provided and determined whether they can be supported. Whilst that information should provide a good indication of the key attributes of each method, this cannot be guaranteed and the reader's attention is drawn to the last paragraph of the Foreword.

Table A2 should be used as an initial filter in selecting a suitable method. The reader should obtain further information on the methods. To assist with this, the method descriptions in Annex B include references to further useful information.

The features described are those that should be most useful to the user, but there are some notable omissions, for example, cost. Cost is a difficult feature to rate fairly and objectively in that some methods may be free but require expensive training; others appear expensive but make more efficient use of analysts' time. For this reason, cost as a feature of the methods has been excluded. Users should explore costs when researching methods further.

The attributes of the methods listed in Table A2 are defined as follows:

**Training required**: the method provider requires the user to undergo training in using the method or training would be required by a novice user in order to use the method effectively. In some cases, novice users would have to familiarise themselves thoroughly with the method before using it and may decide that they need more formal training or briefing from an expert in the method.

**Paper or software based:** the method is available as a document only or as a software tool only, some are available in both forms.

**Retrospective analysis of incident reports:** the method has been designed specifically in order to examine existing incident reports rather than assist in a new investigation or analysis: many of the methods could be used in this way. Moreover, most of the methods could be used proactively as a risk assessment method. This feature is highlighted where the method seems particularly useful in the retrospective analysis of past incidents.

**Used in the petroleum industry:** indicates where there is clear evidence that the method has been used in the petroleum or allied industries. Comments are provided in the table where a method has been devised specifically for another industry, for example, aviation.

**Generates graphical content:** the method requires the development of a timeline or similar pictorial representation of the incident and describes how to prepare this. The graphics may be paper or screen based (software systems).

**Forms a complete method for incident analysis:** some methods are 'stand alone', whereas others require the user to employ additional tools to complete the analysis. Several methods have been developed on this basis and include modules from other methods.

**Provides solutions**: the method provides 'ready-made' solutions in the form of notes or checklists of corrective actions against specific problems found from the analysis. Note that, since accident investigation is essentially the reverse of risk assessment, then the same 'hierarchy of controls' approach (see section 2.2) is applicable to solutions generated here i.e. can the hazard be removed, can the human element be eliminated? etc. The methods do not do this; users need to determine for themselves how these apply to **their** critical tasks at **their** sites).

**Includes checklists or flowcharts:** the method has decision making aids to guide the user through the analysis; some may be simple prompts or memory joggers to explore specific topics.

**Comments:** this column in the table is used to provide further explanation or detail as needed.

## Table A2: Analysis methods features

| | | 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 A2 continued.**

| | | 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® | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | |
| 24. | TRACEr – Technique for Retrospective and Predictive Analysis of Cognitive Errors | | ✓ | | ✓ | ✓ | | | | ✓ | Forms part of the HFAT methodology |
| 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 | | ✓ | | | | ✓ | | | | |

# ANNEX B
# BRIEF DESCRIPTIONS OF METHODS

All of the following methods can help an incident investigator/analyst to identify the human factors aspects of an incident. They have been chosen for inclusion in this Annex because they:

— were cited by interviewees who contributed to this guide as a method they had successfully used;
— feature prominently in incident investigation literature, or
— offer a sound approach to identifying human factors aspects in incident analyses.

**The methods are:**

B1. ARCA – APOLLO Root Cause Analysis
B2. Black Bow Ties
B3. DORI – Defining Operational Readiness To Investigate
B4. ECFA – Events and Causal Analysis (Charting) and ECFA+ - Events and Conditional Factors Analysis
B5. Fishbone diagram
B6. HERA – Human Error Repository and Analysis System
B7. HERA-JANUS – Human Error Reduction in ATM (Air Traffic Management)
B8. HFACS – The Human Factors Analysis and Classification System
B9. HFAT – Human Factors Analysis Tools
B10. HFIT – Human Factors Investigation Tool
B11. HSYS – Human System Interactions
B12. ICAM – Incident Cause Analysis Method
B13. MEDA – Maintenance Error Decision Aid
B14. MORT – Management Oversight and Risk Tree
B15. PEAT – Procedural Event Analysis Tool
B16. PRISMA – Prevention and Recovery Information System for Monitoring and Analysis
B17. SCAT® – Systematic Cause Analysis Technique
B18. SOL – Safety through Organisational Learning
B19. SOURCE™ – Seeking Out the Underlying Root Causes of Events
B20. STEP Sequentially Timed Events Plotting
B21. Storybuilder
B22. TapRooT®
B23. (Kelvin) Top-Set®
B24. TRACEr – Technique for Retrospective and Predictive Analysis of Cognitive Errors
B25. Tripod Beta
B26. WBA – Why-Because Analysis
B27. 5 Whys
B28. Why Tree

## B1. ARCA - APOLLO ROOT CAUSE ANALYSIS

Apollo is a general problem solving method that can be applied to accident investigation. It does this by helping the analyst to identify the relationships between causes and effects noting that an effect of one event can be the cause of another. One of Apollo's basic principles is that an 'effect' has at least two causes in the form of an 'action' and a 'condition'. The analyst uses the evidence gathered about an event to build a picture of causes and effects using the 'Realitychart'™ software.

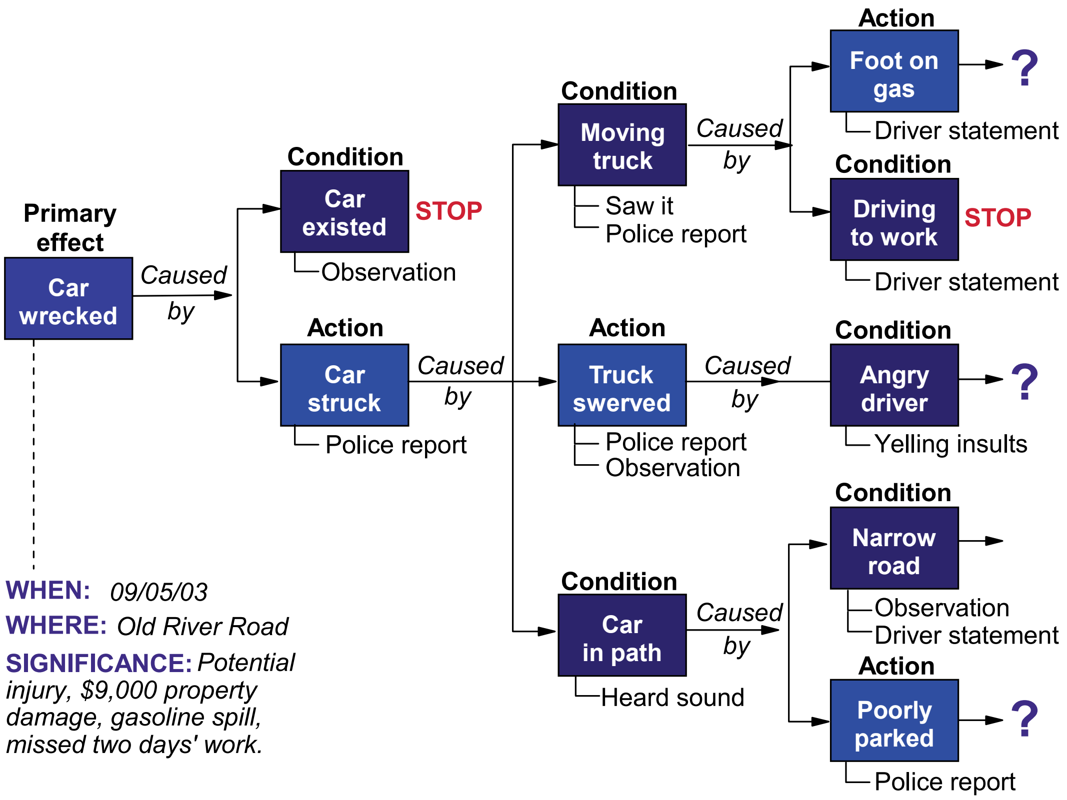


**Figure B1: Example Apollo cause and effect chart**

An example Apollo cause and effect chart is shown in Figure B1. This is an example of a car accident. Actions and conditions are described in boxes with the source of evidence for the condition or action described below each box. The chart forms a description of the incident leading to underlying causes that the analyst can use to identify solutions. The basic steps in the problem-solving process are:

- Define the problem – identify the event that you wish to prevent.
- Analyse cause and effect relationships – using the charting method to show causes and interactions between causes.
- Identify solutions – the method does not offer solutions; the analyst has to devise them based on the evidence.
- Implement solutions.

The developers provide a two-day seminar to train users in the method. Shorter introductory and manager focused seminars are also provided. Public courses are held regularly in the US and internationally.

**Useful reference information**

Gano, DL (1999) Apollo root cause analysis - A new way of thinking, Apollo Associated Service Inc., USA. ISBN: 1-883677-01-7
http://www.realitycharting.com/#start
http://www.apollorca.com/

## B2. BLACK BOW TIES

The method is not an investigation method in itself but a means of representing Tripod Beta models in the 'bow tie' format used in some risk assessments. Figure B2 shows the general format of a bow tie diagram. As an accident investigation tool i.e. ignoring its use in risk assessment, building the bow tie comprises seven steps:

1. Describe the hazardous event – what occurred and what hazard was released?
2. Identify the 'threats' – anything that could have led to or contributed to the hazardous event. Threats include design faults, possible human errors, corrosion etc.
3. Identify consequences – what happened as a result of the incident? This might be a chain of consequences with one event leading to another and can be complicated. The analyst may wish to record only the ultimate consequence or else split consequence descriptions across several bow tie diagrams.
4. Identify the threat barriers – what was in place to prevent this accident? What activities were needed to keep those barriers in place and who was responsible for those activities?
5. Identify recovery measures – contingency methods in place to recover from the accident and reduce consequences, including technical, operational and organisational measures.
6. Optional: identify 'escalation factors' – factors that could reduce the effectiveness of controls such as abnormal operating conditions or human errors.
7. Identify escalation factor controls - any additional controls specifically to manage these factors.

Tripod analyses can be mapped onto bow-tie diagrams to indicate possible active failures, preconditions and latent failures (see Tripod Beta description (No.B25)) that could have adversely affected control measures.

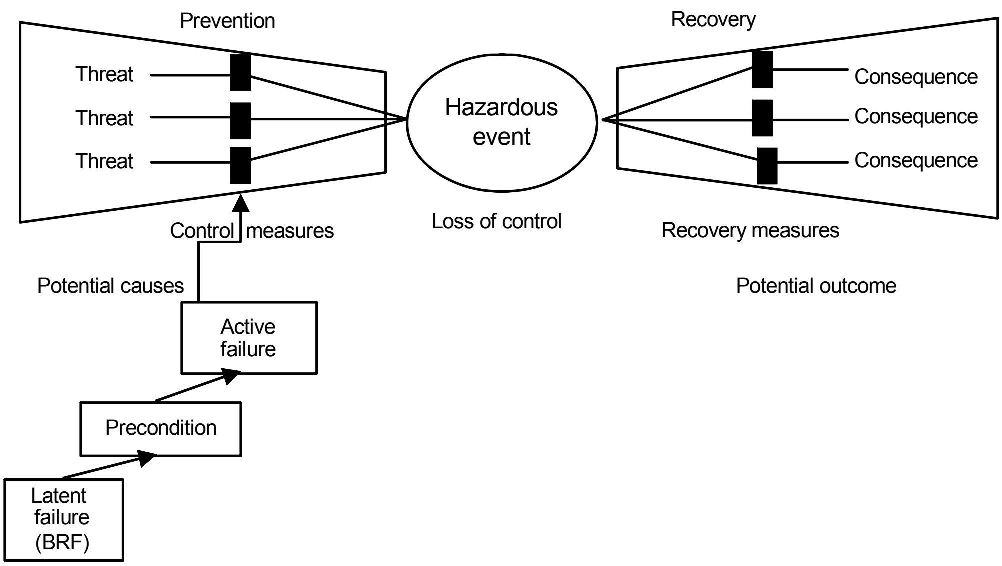


**Figure B2: Bow-tie diagram**

Multiple incidents can be mapped in a bow tie model and layered onto an existing risk assessment to build up a more complete picture of the underlying risk factors and potentially filling any gaps in the risk assessment.

Black Bow Ties is available as a software package – 'Black BowTie XP'. In addition, a software tool 'Black Box' is available that provides a complete investigation tool by linking the TopSet® methodology with the Black Bow Ties modelling method.

The developers of the method suggest that it is a sophisticated approach that may not be acceptable within organisations that have not reached a high level of maturity in their approach to risk.

**Useful reference information**
http://www.bowtiexp.com/

## B3. DORI – DEFINING OPERATIONAL READINESS TO INVESTIGATE

This is not an investigation method but sets out ideas about what an organisation needs in place in order to investigate incidents effectively. An interim 'white paper' was published in 2005 – available from the Noordwijk Risk Initiative Foundation website. This was prepared in collaboration with RoSPA (The Royal Society for the Prevention of Accidents) and provides ideas that organisations can use to develop their strategies for investigation; it encourages them to determine:

- The range or 'levels' of incidents that the organisation should be prepared for.
- The tasks that need to be done – the paper provides a checklist of 34 possible investigation tasks.
- How those tasks are to be carried out depending on the level of the incident.
- Resources required in order to carry out the tasks – people, plant and equipment, procedures and management controls.

**Useful reference information**
Kingston, J, Frei, R, Koomneef, F and Schallier, P (2005) Defining operational readiness to investigate – DORI. Noordwijk Risk Initiative Foundation, Netherlands.
http://nri.eu.com/toppage4.htm

## B4. ECFA – EVENTS AND CAUSAL ANALYSIS (CHARTING) AND ECFA+ - EVENTS AND CONDITIONAL FACTORS ANALYSIS

ECFA is part of the MORT method (See No.B14). ECFA+ is a later variation of the method. The description that follows encompasses both methods.

The core element of ECFA is the Events and Causal Factors (ECF) chart. This is the 'picture' that the investigator constructs from the information gathered in their investigation. The chart shows 'events' – what happened – in rectangles – and 'conditions' in ovals. Event boxes are linked by arrows showing the sequence of the incident. Conditions that affected the event are also linked to the boxes by arrows.

Analysts using ECFA should typically use a paper wall chart and draw on event boxes. They should start with the incident itself, then work backwards putting in further boxes to describe the sequence that led up to the event. They should also work forward describing what happened after the event. The main event sequence should be shown in the middle of the chart with any contributory or secondary events shown in separate sequences above or below this. Stick on notes are often used to allow the analysts to change the sequence or add elements quickly.

Various conventions are observed in using ECFA:
- Each event description should indicate:
  – the 'actor' – the person involved e.g. maintenance fitter;
  – their action – in the present tense e.g. drops;
  – the 'object' involved – e.g. 5lb hammer.
- Where the analyst is unsure about an event or a condition, for example, through lack of solid evidence, they depict the event or condition in a box or oval with a dotted borders.
- The analyst should check event logic – for example, that one event does necessarily follow from another.

The rules for structuring an ECFA chart should be followed to ensure that the analysis is clear and complete. Buys and Clarke set out the conventions clearly and provide examples.

The method does not identify root causes and should be used in conjunction with other methods that do so.

The method is not complex and a team should be able to construct ECF charts with minimal training although considerable resource may be needed to analyse complex incidents and some users have been reluctant to apply ECFA in these cases.

**Useful reference information**

Buys, R.J. and Clark, J.L. (1978). Events and Causal Factors Charting. DOE 76-45/14, (SSDC-14) Revision 1. Idaho Falls, ID: System Safety Development Center, Idaho National Engineering Laboratory.
ECFA+ - Noordwijk Risk Initiative Foundation http://www.nri.eu.com/

## B5. FISHBONE DIAGRAM

A fishbone diagram is a general problem-solving method that has been used to record and make sense of incident events. Using a large sheet of paper, the analyst writes down a brief description of the event. A horizontal line is then drawn from the description towards the left hand side of the paper. The analyst then adds 'ribs' to this 'backbone' where each rib is a factor thought to have influenced the incident. Further ribs can be added as the analysis proceeds. From that point, the method is similar to the 'five whys' method of asking why each factor is thought to have contributed to the incident.

In the example, a tanker driver has delivered the wrong product into a storage tank. Using the HSE's model of human and organisational factors: job, person, organisation, these factors form the main ribs of the diagram. Across the ribs, causal factors have been added in each category. For example, under, 'Job' the factors contributing to the incident are poor lighting in the delivery access chamber making it difficult to see the product labels. The torch carried as part of the driver's toolkit is missing. Under 'Person', they are rushing as it is close to the end of their shift.

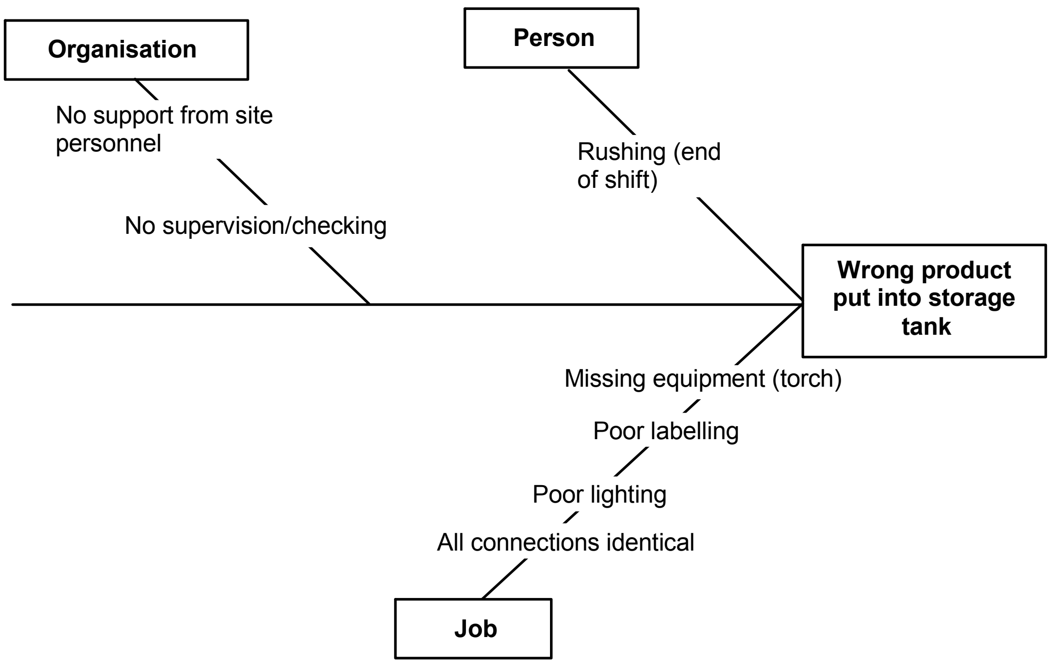


**Figure B3: Fishbone diagram**

Each of these causes can be explored down to their root causes using the 'why' process. The diagram (Figure B3) provides an overview of ideas and helps the analyst to identify any gaps and to focus on key issues.

**Useful reference information**
http://www.isixsigma.com/library/content/t000827.asp

## B6. HERA – HUMAN ERROR REPOSITORY AND ANALYSIS SYSTEM

Note that this method is not related to HERA-JANUS described in B7.

HERA was devised for the US nuclear industry as a method for collecting data on incidents in a systematic format for entry into a software database. Its value as an analysis tool is in the 'worksheets' it provides. These are used to examine and structure the information collected. Worksheet A has three sections:

1. Plant and event overview – sources of information used for the analysis, type of event, type of plant, overall event description.
2. Event summary and abstracts – brief summary of the event – may be copied from the original source material (e.g. an existing report).
3. Index of sub events – specific successes and failures of equipment and personnel actions.

Worksheet B has seven sections:

1. Personnel involved in sub event.
2. Contributory plant conditions – that contributed to the event or to personnel actions/decisions.
3. Positive Contributory Factors/PSFs - factors that assisted performance.
4. Negative Contributory Factors/PSFs – factors that contributed to the sub event.
5. PSFs - HERA describes 11 PSFs. The user can obtain information on PSFs from the source material

on the incident or infer what they were. Negative PSFs are based partly on the factors described in HSYS.
6. Error type – error or omission/error of commission; slip, lapse, mistake, circumvention or sabotage.
7. Sub event comments – for additional information.

The method is aimed at analysts with existing knowledge of probabilistic risk assessment or human reliability analysis. The novice user would find it useful as a checklist of items to consider in an analysis and as a useful tool for examining the human factors content of events that have already been reported. The user would have to become familiar with human reliability terminology and read the HERA reports thoroughly to develop their understanding of the method. HERA is not, however, a complete method.

It is not known whether the software tool is available publicly to those outside the nuclear industry and the US, but NUREG/CR-6903B is available to the public via US Nuclear Regulatory Commission's website.

**Useful reference information**

Hallbert, B et al (2006). Human Event Repository and Analysis (HERA) System, Overview, NUREG/CR-6903B. USNRC, Washington DC.
http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6903/

## B7. HERA-JANUS

The method is a combination of the Human Error Reduction in Air Traffic Management (HERA) method and HFACS. It was devised as a method for retrospective analysis of air traffic control incident reports but has proven useful as an investigation tool. It is intended to be used by safety specialists, accident investigators, human factors analysts and others. The method is oriented towards air traffic controllers and the terminology used reflects that application though it could prove useful to others by suitably altering the wording. It should be noted that information on air traffic incidents is generally plentiful since all controller actions and conversations with pilots are recorded – this has made it easier to develop a comprehensive method for that industry and to identify an exhaustive list of specific error causes.

The method is used in several stages each supported by checklists and flowcharts based on human factors research regarding human failure types and information processing models:

1. Describe the error - error type – e.g. timing errors, action errors, communication errors.
2. Describe error detail (ED) – based on the information processing stage that failed, whether a perception/vigilance; memory; planning/decision-making or response execution error.
3. For each ED, identify the error mechanism (EM) – e.g. for a memory error, EMs could include: forget to monitor the situation; mis-recall information.
4. For each EM, described how the information processing (IP) level failed – e.g. for EMs related to memory, associated IPs include: distraction, memory overload, failed learning. IPs are the most difficult to classify.

Each step above is supported by flowcharts and checklists to guide the user through the process of identifying errors/violations, defining types of task and equipment used at the time of the incident and identifying underlying causes of failure. There are flowcharts and extensive lists of 'contextual conditions' - factors that could have provoked the incident such as: training and experience, weather conditions, procedures, actions of others.

Error recovery or reduction strategies are developed by the analyst based on the information generated concerning the origin of the particular failure.

The method is described fully in the references below. Some customisation would be required for use in other industries.

**Useful reference information**

Isaac, A et al(2003) The human error in ATM technique (HERA-JANUS), EATMP Infocentre, Eurocontrol, Brussels.
http://www.eurocontrol.int/humanfactors/gallery/content/public/docs/DELIVERABLES/HF37-HRS-HSP-002-REP-04withsig.pdf

## B8. HFACS – THE HUMAN FACTORS ANALYSIS AND CLASSIFICATION SYSTEM

HFACS is based on James Reason's ideas of 'latent failures' and the 'Swiss cheese' model. Reason's model suggests that any incident is preceded by:

- An unsafe act – an error or violation, which is encouraged by…
- Preconditions for unsafe acts – substandard conditions or substandard practices. These in turn are not prevented or corrected due to…
- Unsafe supervision –planned (but) inappropriate operations; failure to correct known problems; supervisory violations; and underlying all of this are…
- Organisational influences - poor resource management; organisational climate; organisational processes.

The authors of HFACS believed that Reason's model was useful: it described the idea that there could be 'holes in the cheese' but did not describe what those holes might be. HFACS provides descriptions of preconditions, unsafe supervisory practices and organisational influences in the form of checklists. These have been derived from investigations of naval aviation accidents and supplemented by data from the army and the transport and civil aviation industries.

The available literature on HFACS is well written and clear. It is, however, a classification system, not an investigation method but could be used by experienced investigators as a tool to supplement their analysis. Other users with limited human factors or investigation experience may find it difficult to apply.

HFACS provides a set of checklists for incident analysis. It also includes descriptions of types of human error: skill based errors, decision and perceptual errors and two forms of violation: routine and exceptional. As with all checklist methods, it is not clear if every conceivable underlying factor has been captured, but the checklists are extensive and based on real events. Users in the petroleum and allied industries may need to adapt the checklists to their own use by, for example, changing some of the terminology, which is based on aviation ('aircrew', 'altitude' etc). It should produce reasonably consistent results across different analysts as the analysis should be based principally on the checklists provided. HFACS would have to be supplemented by another method such as ECFA (see No. B4) to provide input information.

HFACS provides examples of the types of deficiencies associated with the four levels of failure from Reason's model, and therefore lends itself to the identification of causes and recommendations, although they would be generated by the analyst.

HFACS has been available since 2003 and has been applied in a range of industries, including:

marine, military, commercial, and general aviation sectors. In the literature consulted for the present review, it is regarded as a successful and useful method and has been noted as a useful method for the petroleum industry.

HFACS can be used to examine the content of accident databases retrospectively to determine underlying causes that may not have been disclosed previously. The success of this is wholly dependent on the quality of the information contained in the database.

The method is described fully in Wiegmann and Shappell (2003). Some further training by those who have used it may be required.

**Useful reference information**

Wiegmann, DA, Shappell, SA (2003). Human error approach to aviation accident analysis: The human factors analysis and classification system. Ashgate, London, ISBN-13 978-0-7546-1873-7 http://www.ashgate.com/index.htm

## B9. HFAT – HUMAN FACTORS ANALYSIS TOOLS

HFAT was developed for a petroleum industry client but has been used in other industries. HFAT is applied when the incident investigator has collected information about the critical factors and causes of an incident and wishes to explore the human factors elements in more detail. HFAT supports the analyst in examining incident findings in order to identify the human behaviours of interest and to classify the behaviours as either errors or violations. Errors are then analysed using one module in the toolkit; whereas violations are analysed using another module.

The method is based on two existing methods:

1. 'ABC' analysis (Antecedents, Behaviours and Consequences) – Antecedents are prompts or triggers for 'behaviours' and 'consequences' are the result of the behaviours. ABC allows the analyst to explore the motivations for violation behaviour. (Komaki et al).
2. TRACEr – Technique for Retrospective Analysis of Cognitive Error which is in turn based on the information-processing model of Wickens. The model describes human behaviours as:
   - Perceiving information.
   - Using memory (to store and retrieve information).
   - Making decisions.
   - Taking actions.

TRACEr allows the analyst to establish where in this process the behaviour went wrong. Note that it was developed for air traffic control applications and has a strong bias towards information processing activities though it has been used recently for more industrial tasks.

HFAT can be used as a stand-alone method to analyse any human failure but in order to identify root causes, is best integrated with a root cause analysis method. Analysis begins by applying the 'behaviour extraction' module. This allows the investigator to identify the actions of interest in the incident being examined and to determine whether the behaviour was intentional (a violation) or unintentional (an error). ABC or the human error analysis module is then applied as appropriate.

A two-day training course is required in order to use HFAT. Candidate trainees should ideally be interested in human factors and have experience of incident investigation methods.

HFAT does not contain any ready-made incident-specific solutions but the HFAT analysis does:

identify specific deficiencies in the systems and conditions for controlling human performance; contain generic guidance on developing effective recommendations for shaping and influencing behaviour.

HFAT is relatively new and following feedback from trials and applications, the method continues to be developed.

**Useful reference information**

Komaki, J Coombs, T, Redding, Jr, TP and Schepman, S (2000) A rich and rigorous examination of applied behaviour analysis research in the world of work, International Review of Industrial and Organisational Psychology, 15: 265–367

Wickens, CD (1992). Engineering psychology and human performance 2nd Edition. New York: Harper Collins.

Shorrock, ST and Kirwan, B (1999). TRACEr: a technique for the retrospective analysis of cognitive errors in ATM. In D. Harris (Ed.) Engineering psychology and cognitive ergonomics: Volume 3 – Transportation systems, medical ergonomics and training. Aldershot, UK: Ashgate.

The Keil Centre Edinburgh http://www.keilcentre.co.uk/index.htm

## B10. HFIT – HUMAN FACTORS INVESTIGATION TOOL

HFIT is based on a model of how accidents are caused which is in turn derived from a wide range of different models derived from research. The model is shown in Figure B4.

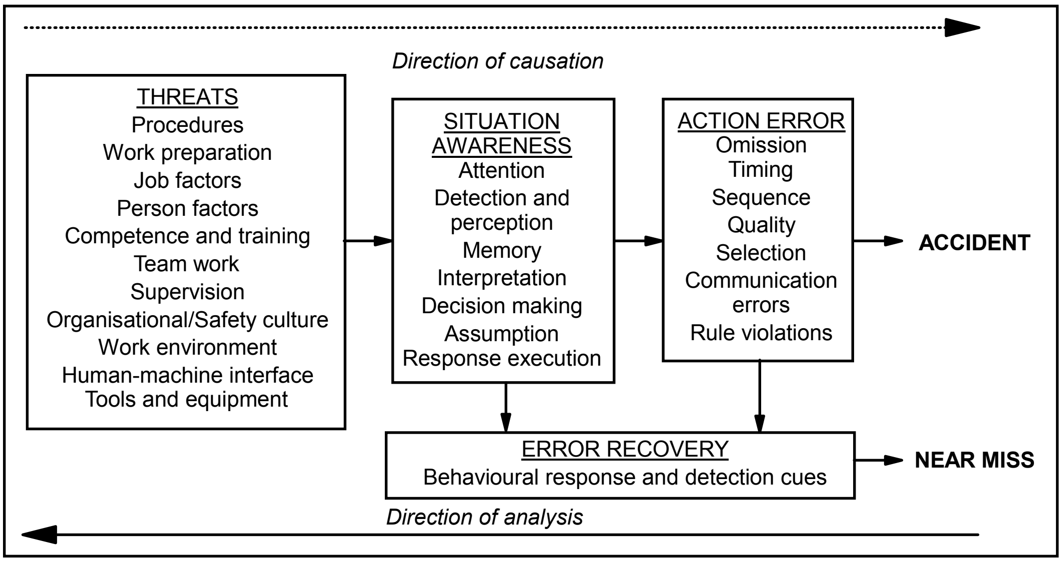


**Figure B4: HFIT model**

The model suggests that accidents occur when a person makes an 'action error', for example, omits to carry out a critical task. Action errors occur because of some fault in the person's information processing sequence – lack of attention, failure to detect information, failure of memory etc. There can be opportunities to recover situation awareness or the action error itself by detecting and correcting the problem. If this is successful, the outcome is a near miss rather than an accident.

Problems with situation awareness arise because of threats such as poor procedures, competence, communication, supervision, safety culture or other factors.

HFIT analysis is based then on a four-step process working through each of those four elements in an incident scenario. At each stage, the analysis is supported by checklists and flowcharts. The analysis is applied to information gathered from the incident investigation and recorded, for example, on a timeline. The checklists can be used also as interview prompts.

Paper and software-based versions of the tool are available. The four steps are:

1. Identify action errors.
2. Identify possible recovery mechanisms from those errors.
3. Identify the elements of the information processing sequence that failed.
4. Identify threats that contributed to the incident at any stage in its evolution.

Users without human factors experience would require some basic training to use HFIT. A one-day training course is available (overview of human factors concepts; how to use the HFIT tool and practical exercises).

HFIT does not generate ready-made solutions to the problems identified, but the information gathered should help the analyst to make improvements.

**Useful reference information**
The HFIT figure was published in Safety Science, Vol. 43, Gordon R, Flin R & Mearns K (2005). Designing and evaluating a human factors investigation tool (HFIT) for accident analysis. Pg.150. Copyright Elsevier (2005).
http://www.abdn.ac.uk/iprc/papers%20reports/Designing%20and%20Evaluating%20a%20human%20factors%20investigation%20tool.pdf

## B11. HSYS - HUMAN SYSTEM INTERACTIONS

The method was developed in the Idaho National Engineering Laboratories in the US in the early 1990s. It is no longer maintained by the developers but versions of the HSYS manual or software may still be available within some organisations

HSYS is based on a model of human performance devised by its developers called 'the Input Action model'. The model describes human performance in five stages:

1. Input detection
2. Input understanding
3. Action selection
4. Action planning and
5. Action execution

For each stage of the model, e.g. 'input detection', HSYS provides a 'tree' in a similar way to MORT (see No. B14). The trees are used to identify which aspects of human performance were 'less than adequate' (LTA) in the incident. For example, input detection may have been LTA because the person involved in the incident was not paying sufficient attention to their work ('attention LTA'). The tree then refers the analyst to a set of flowcharts to explore why attention may have been LTA. At the end of the flowchart is either a reference to another flowchart or the expression 'explain reasons why' which is the prompt for the analyst to ask about root causes.

HSYS is used by interviewing those involved in the incident. The interviews are structured around the flowcharts.

HSYS was made available in the form of a paper-based manual and a software tool. At the time of writing, it is to be superseded by a new method known as the Human Event Repository and Analysis System. HERA is not a direct replacement for HSYS and has different objectives (see No. B6)

The input action model is based on human performance models developed in the 1970s and 1980s. It is less sophisticated than currently available models but includes the main features of human information processing and action.

In trials, users of the method reported that the flowcharts and hierarchical trees were easy to use. It is not clear if these users had prior human factors knowledge or experience of investigating accidents. The review performed in developing this publication suggests that the flowcharts would be straightforward to use for an experienced human factors analyst or incident investigator, but some of the terminology might be difficult for a novice user.

As with all such methods, the use of flowcharts can introduce a high level of consistency. The underlying model should help to ensure that failures at key human performance stages are considered. There is a tree diagram for each stage each supported by flowcharts. The full range of flowcharts and questions were not available for review but it is clear that a large amount of information is provided suggesting that the method is capable of comprehensively analysing an incident.

The HSYS system does not generate recommendations but provides the basis for the analysts to develop solutions to the problems disclosed.

The approach has been validated by using HSYS to study accident reports but development of the system does not appear to have progressed since the early 1990s. It has been used to consider accidents in offshore drilling incidents and for human performance military aviation tactical command. The US Federal Aviation Administration lists the method on their website.

HSYS can be used as an investigation tool and as an analytical tool to determine, prior to an incident, whether systems in place to control human performance are 'adequate' or not.

**Useful reference information**

Hill, SG, Harbour, JL, Sullivan, C, Hallbert BP (1990), Examining human system interactions: the HSYS methodology. Proceedings of the Human Factors Society 34th Annual Meeting. 1990 http://www.osti.gov/bridge/servlets/purl/6307928-GUQW83/

US Federal Aviation Administration
http://www2.hf.faa.gov/workbenchtools/default.aspx?rPage=Tooldetails&toolID=122 but with a note that it has yet to be proven in practice.

## B12. ICAM - INCIDENT CAUSE ANALYSIS METHOD

ICAM is based on the research of James Reason. This is illustrated in Figure B5 where errors or violations occur as a result of poor organisational control over, for example selection, training, procedures and equipment selection and also due to adverse task and environmental conditions including time pressure, task complexity and workload. If the consequence of the error or violation is not trapped by any of the available defences, the result is an incident or accident.

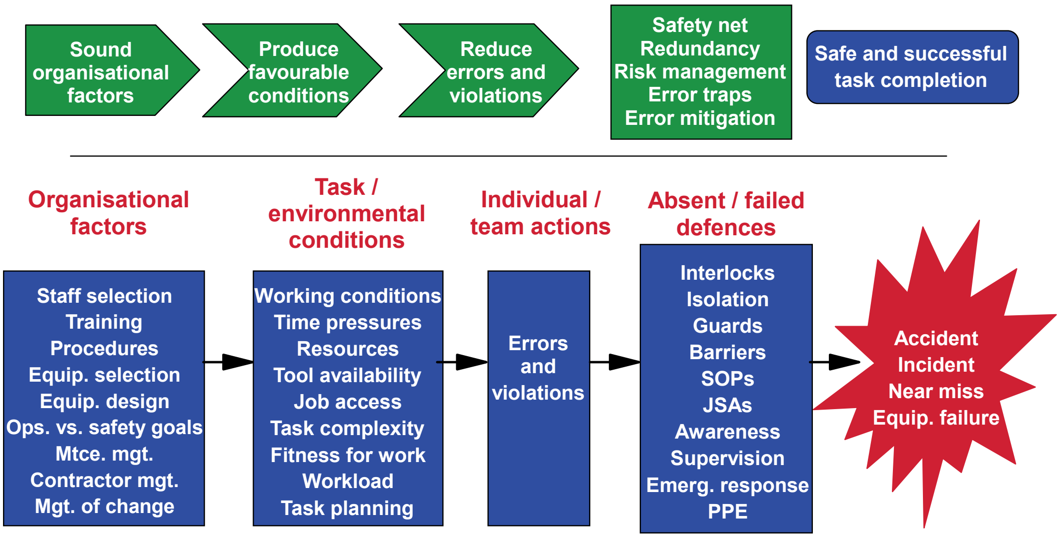


**Figure B5: ICAM diagram**

Figure reproduced with kind permission of Safety Wise Solutions Pty. Ltd

An incident investigation using ICAM seeks to identify the absent or failed defences, then the actions that led to the incident, the task and environmental conditions as they affected those actions and the underlying organisational factors that contributed to the incident.

ICAM can be used as a proactive tool for examining organisational factors. In this respect, it is similar to Tripod (see No. B25) and the organisational factors cited in ICAM are almost identical to Tripod basic risk factors.

**Useful reference information**

http://hsecreport.bhpbilliton.com/2006/
http://www.safetywisesolutions.com/productsicam.html

## B13. MEDA – THE MAINTENANCE ERROR DECISION AID

MEDA was developed by Boeing as a method for investigating maintenance errors. It is related to the PEAT method (see No. B15).

The method was developed taking into account human error research and the concepts of slips, lapses, mistakes, violations, PSF etc, but presents a simplified view of them. Errors are described in more specific terms than 'slips' etc, for example: 'tool left in housing'; part not installed'; 'part installed incorrectly'; 'failed to lubricate after servicing'.

The underlying philosophy of MEDA contends that no-one sets out to commit an error and that management have control over 80 to 90% of the factors that contribute to errors, with maintenance technicians or their supervisors having control over the remaining 10 to 20%.

The simple model of incident and accident 'events' is that various 'contributing factors' – akin to PSFs – increase the probability that an error should occur and an error increases the probability of an event. Contributing factors include: competence and other attributes of the mechanic, the working environment in the broadest sense including weather conditions and factors such as time pressure and team work, supervision, and 'organisational philosophy' – policies, procedures and processes.

Following an event that the organisation considers, from a preliminary assessment, may have originated from maintenance errors, a MEDA investigation is applied as mainly to investigate – mainly by interviewing the technician and any other involved in the event. The investigator should use the 'MEDA results form' as a prompt list and to record information. The form is divided into six sections:

1. General information – facts about the event including: aircraft type, where it occurred, interviewer name, reference to previous event number etc.
2. Event – short list of aviation-related events including: flight delay, in-flight shutdown, diversion, aircraft damage, personal injury.
3. Maintenance error - checklist of error types and specific errors including: installation error, repair error, isolation/test/inspection error, personal injury, servicing error with space for specific free-text description.
4. Contributing factor checklist – 11 factors with prompts as to what the problem may have been with that factor and space for a free text description of how specifically the factor contributed to the error, for example, 'information' could be – not understandable, unavailable/ inaccessible, incorrect, conflicting or not used. The remaining ten factors are:
   - equipment/tools/safety equipment;
   - aircraft design/configuration/parts;
   - job/task;
   - technical knowledge/skills;
   - individual factors – such as time constraints, peer pressure, distractions;
   - environment/facilities;
   - organisational factors such as quality of support, staffing/resources, procedures; leadership/supervision;
   - communication, and
   - other.

The Boeing MEDA User's guide elaborates on these checklists and provides specific examples of possible specific contributing factors e.g. equipment unsafe could mean sharp edges, lock out systems not working, electrical sources not labelled.

5. Error prevention strategies – asks the question 'what current existing organisational procedures, processes and/or policies are intended to prevent the incident but did not?' Suggestions are: policies or processes, inspection or functional check, documentation and 'other'. The section includes space for recording recommendations listed alongside the contributing factor it is intended to address. The person involved in the incident is asked to contribute to this section.

6. Summary of contributing factors, error, event – free text description summing up the basic findings

The User guide elaborates on all the sections of the form and provides advice on interviewing strategies and the use of precise language in filling out the form.

**Useful reference information**

Boeing (2001) Maintenance error decision aid (MEDA) user's guide

http://www.tc.gc.ca/CivilAviation/general/Flttrain/SMS/Toolkit/MEDA/MEDA.pdf

## B14. MORT – MANAGEMENT OVERSIGHT AND RISK TREE

MORT was developed in the early 1970s for the nuclear industry. Investigators used fault trees as a means of presenting information on major accidents. They noticed that the same causal factors appeared in many of the fault trees developed for different accidents and this led them to develop a number of generic trees describing system faults that can lead to incidents. The current form of the system, developed via funding from a petroleum industry company and presented in the MORT User Manual, has question sets instead of 'trees' to explore whether controls that should have been in place to prevent an incident were adequate or not.

There are eight ready-made 'trees' or question sets covering 98 generic problems and 200 basic causes of 'losses'. Figure B6 shows the overall logic of MORT. 'Losses' are caused by either oversights/omissions or 'assumed risks'. The latter are risks that have been assessed and accepted (in practice, losses could be due to a combination of both).

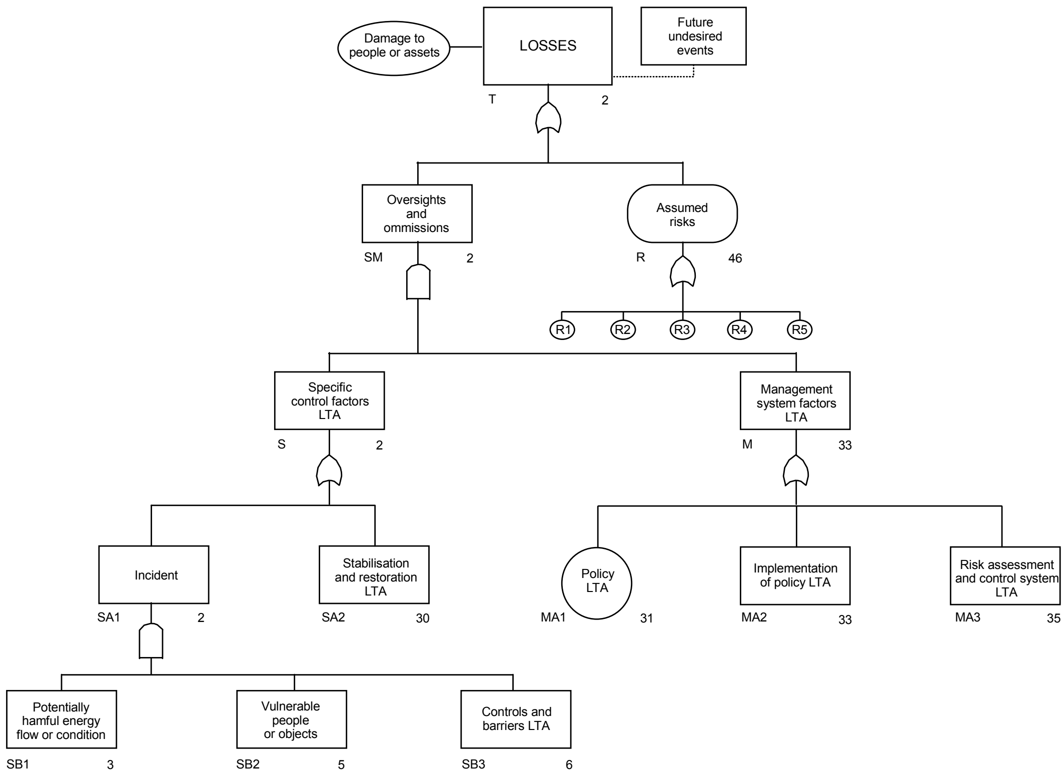


**Figure B6: MORT diagram**

Diagram reproduced with kind permission of Nordwijk Risk Initiative Foundation

Oversights and omissions occur because control factors or management system factors are 'less than adequate' (LTA). Control factors relate to the incident itself (failures that led to) or to events after the incident (that failed to control it and thus led to losses). The question sets are concerned with:

SA1 – describing the incident itself using barrier analysis
SA2 – stabilisation and restoration (following the incident)
SB1 – potentially harmful energy flows or environmental conditions

SB2 – vulnerable people or objects
SB3 – barriers and controls (broken down into sub-sections e.g. information systems, operational readiness, inspection, maintenance
MA1 – policy
MA2 – implementation of policy
MA3 – risk assessment and control system

There is also a question set for assessing assumed risk. Numbers in Figure B6 are the relevant page numbers in the MORT User's manual.

The questions are applied to specific 'episodes' of interest in an incident: these are identified using 'barrier analysis' – see below. The users (ideally in a team of two) work through the trees/question sets identifying whether any of the causes described in MORT are applicable to the incident. Usually, they should mark the trees with coloured pens to code problem areas; those that are well covered and those where there is insufficient information to judge.

Barrier analysis is an essential step prior to conducting a MORT analysis. There are three concepts in this analysis: energy; targets; and barriers. Energy is the harmful agent that can affect a target (person or thing) but not necessarily damage it (this would be a near miss). Barriers are any means for protecting the target from energies. The analysis consists of identifying: targets (people or things that were harmed or threatened in the incident), then energy flows that were directed at the target then the barriers or controls that should have prevented the energy flows from reaching the target.

No specific human factors model is mentioned in MORT. The barrier analysis concept is very similar to the 'Swiss cheese' model described in section 2.4. The technical language and specific terminology used in MORT may prove difficult for the novice user, but, with practice, it should be possible for anyone who wishes to use the system to do so from a thorough reading of the MORT User's manual and, if necessary, by obtaining supplementary advice from the Noordwijk Risk Initiative Foundation (NRI) – the present custodians of MORT.

MORT covers a wide range of root causes of incidents and should prompt the user to consider the majority of possible contributors to an incident. The method does not provide ready-made recommendations for improvement but these can be developed from the findings indicating which elements of the current system are less than adequate.

MORT is a well-established method and has been used in a wide range of industries. It is a comprehensive method and can be used with a minimal knowledge of human factors. Many of the questions are supported by text describing examples of 'adequacy'.

Koornneef and Hale at Delft University of Technology have developed a software version of MORT known as the Intelligent Safety Assistant (ISA). Little information is available on ISA – except in Koorneef (2000). Contact Delft University for further information.

**Useful reference information**

Frei, R et al (2002) NRI MORT User's Manual. ISBN 90-77284-01-X Available from:
http://www.nri.eu.com/serv01.htm
Koornneef, F. (2000). Organisational learning from small-scale incidents. Delft University Press, Netherlands. ISBN 90-407-2092-4

## B15. PEAT – THE PROCEDURAL EVENT ANALYSIS TOOL

PEAT was developed by Boeing and, as with MEDA (see No. B13), is a checklist-based tool for examining deviations from procedures by interviewing those involved. The focus of PEAT, however, is flight crew rather than maintenance.

The overall PEAT process is to identify deviations from procedures; identify the contributing factors that led to those deviations and make recommendations that should address those factors. The steps in a PEAT analysis are:

1. The investigator reviews any preliminary information gathered about the event and compiles a list of possible crew errors but does not speculate on contributory factors.
2. In an interview, they ask those involved in the event for their recommendations to reduce future similar events: what the company could do and what flight crew could do. Doing this at the start encourages the crew to think about how their recommendation would address a particular contributory factor.
3. Organise the list of contributory factors into groups according to the part of the decision-making process they affected.

PEAT prompts the user to consider possible contributory causes including:

— equipment factors;
— environmental factors;
— procedures;
— crew factors;
— situation awareness factors – vigilance, attention etc;
— factors affecting individual performance – fatigue, workload etc;
— personal and corporate stressors, management or peer pressure etc;
— crew coordination/communication, and
— technical knowledge/skills/experience.

PEAT is available as a training package. Boeing Flight Technical Services deliver the three-day course required to qualify for using the software.

**Useful reference information**
Moodi, M and Kimball, (2004) Example application of procedural event analysis tool. GAIN Working Group B, Analytical Methods and Tools. Boeing Company, Seattle, WA.
https://www.flightsafety.org/gain/PEAT_application.pdf

## B16. PRISMA – PREVENTION AND RECOVERY INFORMATION SYSTEM FOR MONITORING AND ANALYSIS

PRISMA comprises three steps:

1. Build a 'causal tree' – akin to a fault tree – describing the incident
2. Identify causes – using the 'Eindhoven Classification Model'
3. Identify solutions to the problems disclosed – using guidance provided within the method

Thus:
1. The analyst creates a causal tree to set out the events leading to an incident. Typically, the earlier events are placed on the left hand side of the tree and the later events to the right hand side.

Unlike conventional fault trees, the branches of the tree are linked by gates only.

2. The analyst then examines the tree using the classification model. The model is based on analysis of the causes of incident in the petrochemical industries. Different versions exist for different industries. For the petroleum and allied industries, the model is arranged such that the analyst should consider the cause of each event as either technical, organisational or human behaviour based.
   — Technical – engineering, construction or materials
   — Organisational – operating procedures or management priorities (some versions include safety culture in this category)
   — Behavioural – knowledge, rule or skill based, all of which are further broken down.

3. Using the PRISMA 'classification/action' matrix, the analyst should be able to identify specific solutions to the root cause problems identified in step 2. For example, if knowledge transfer is the problem, solutions are focused on training and coaching; if management priorities are the problem, solutions are concerned with bottom-up communications.

**Useful reference information**
van der Schaaf, TW (1996). PRISMA: A risk management tool based on incident analysis. In International Workshop on Process Safety Management and Inherently Safer Processes. Orlando, Florida, USA, 8-11October 1996.

## B17. SCAT® SYSTEMATIC CAUSE ANALYSIS TECHNIQUE

SCAT® was originally developed by the International Loss Control Institute (ILCI) and is currently a proprietary method of Det Norske Veritas. SCAT® is based on the International Safety Rating System (ISRS). ISRS is a method for assessing the adequacy of loss control management in an organisation by examining the organisation's approach to safety management system elements such as: leadership, risk evaluation, project management, training and competence, communication, emergency preparedness and risk monitoring. SCAT® allows the user to examine an incident and from that determine whether any of these elements are adequate or less than adequate. The method is available on paper or as a software package (ESCAT).

An analyst would use the software system as follows, to describe:

1. The accident (date, time, what happened).
2. The 'loss potential' which comprises the following factors:
   — loss severity potential - i.e. how bad could it have been?
   — probability of reoccurrence – e.g. 'moderate' - a similar problem could arise until measures are taken to remove the causes.
   — frequency of exposure – e.g. 'moderate' – the task being carried out when the incident occurred is a common task.
3. Type of contact - SCAT® provides various choices. In the example, the contact is, 'with heat' (other choices are with: cold; radiation; caustics; noise; electricity etc.).
   From lists, the user then selects the immediate causes (ICs) - substandard acts or substandard conditions. These include:
   'failure to follow procedure/policy/practice' and 'failure to check/monitor'. These were both causes of the fire in the example.
4. Basic causes (selected from options given by the software) – Basic underlying causes (BCs) are split into 'personal factors' and 'job factors'. The analyst may choose to see only the most probable BCs that apply to the ICs chosen in the last step. BCs include: 'abuse or misuse' which

can be described as 'improper conduct that is not condoned'. or, 'improper motivation' which leads to 'improper attempt to save time or effort'.

From the ICs and BCs identified, SCAT® should suggest a number of 'control actions needed' (CANs). These are based on ISRS elements and are aimed at removing or reducing the impact of the underlying causes of the accident. CANs include 'task observation' - the need for a scheme to carry out 'spot checks' on tasks; 'rules and work permits' - review of how compliance with rules is achieved; and 'general promotion' (of safety) - promotion of critical task safety and promotion of housekeeping systems.

**Useful reference information**

International Loss Control Institute (1990). SCAT® – Systematic Cause Analysis Technique, Loganville, GA.
Det Norske Veritas. Place House, Cathedral Street, London SE1 9DE

## B18. SOL – SAFETY THROUGH ORGANISATIONAL LEARNING

SOL was devised for the nuclear power industry and is based on the 'Swiss cheese' model idea of accident causes in which barriers in place to prevent incidents are breached because of various indirect and direct causes. An incident is the end point in a chain of other single events. The direct and indirect causes are concerned with: technology, the individual, the working group, the organisation and the organisational environment. The authors of the method are not concerned if the true root causes are disclosed but more interested in using incidents as a stimulus for discussing improvements to systems, focusing on these five elements. The method requires some creativity on the part of the analyst and is thus applicable to a wide range of industries. It includes two aids to help the incident analyst to:

1. Describe the event

The cues for describing the event are the five classic questions: when, where, who, what and how? Using these prompts, the analyst should identify: when the event started/finished, where it took place (and other locations involved), who was involved directly and indirectly, what type of work was being carried out at the time, what procedures were being used, how were teams organised and allocated their tasks, how did they communicate with each other, did environmental conditions have an effect? etc.

The overall event is graphically depicted as a series of 'event building blocks' showing what each 'actor' in the event was doing at a particular time.

2. Identify the contributing factors

The analyst should next consult a list of six possible directly contributing factors: information, communication, working conditions, personal performance, violation, or technical components. The list suggests up to 19 possible indirectly contributing factors for each of these six. For example, if violation is a possible direct cause, the indirect cause could be lack of supervision. Indirectly contributing causes include the first five of the six directly contributing causes and others such as: group influence:

- rules;
- procedures and documents;
- training;
- feedback of experience, and
- quality management and maintenance.

The method does not provide solutions but the information generated at step 2 provides the means for developing solutions. A software version of the method known as SOL-VE is also available and helps the analyst to conduct further steps for producing corrective actions, documenting the analysis and providing input to the company reporting system and event database.

**Useful reference information**
MTO (Mensch-Technik-Organisation) in Berlin. Website:
http://www.mensch-technik-organisation.de/e/mto_home.html

Safety through Organizational Learning (SOL)- an in-depth event analysis methodology
http://www.rvs.uni-bielefeld.de/Bieleschweig/first/Fahlbruch_Miller_SOL-Handout.pdf

## B19. SOURCE™ – SEEKING OUT THE UNDERLYING ROOT CAUSES OF EVENTS

SOURCE™ is based on a number of methods that are already available in industry supported by some of ABS Consulting's own methods. The methods it draws upon include: event and condition charging, cause and effect tree analysis, change analysis and 5 Whys and ABS's 'Root Cause Map'. SOURCE™ is taught in a workshop setting and those who attend the workshop are then able to use the SOURCE™ methodology licence-free. Most of the checklists and guides are contained in the handbook obtained by attending the course.

The method provides checklists and helpful guides for:
1. Preparing the investigation – securing the site, forming the team etc.
2. Data to gather and data gathering methods – photos, physical evidence, records, witnesses, via interview.
3. Data analysis – fault tree, timelines, causal factors charting.
4. Root cause identification – procedure for and a 'root cause map'.
5. Generating recommendations – checklist provided to assist.
6. Communicating results of the analysis – report writing.
7. Miscellaneous – e.g. entering information in data-tracking system.

**Useful reference information**
Vanden Heuvel, L et al (2005). Root Cause Analysis Handbook: A Guide to Effective Incident Investigation. Published by Rothstein Associates Inc.
ISBN 1-931332-30-4
SOURCE™ investigator's toolkit
http://www.absconsulting.com/resources/RCAresources.zip

## B20. STEP–SEQUENTIALLY TIMED EVENTS PLOTTING

STEP is similar in some respects to SOL (see No. B18); events that took place within an incident are shown graphically alongside each 'actor' involved in those events. The analysis should normally begin by completing a series of STEP cards for each event. The analyst should record the following information on those cards:
— the actor involved – this could be a person or a 'thing';
— the action they took – what the person or thing did;
— the time that the event started;
— the duration of the event;
— sources of information and evidence;

— the location of the event, and
— a description of the event.

The information is then plotted on a graph – see Figure B7.

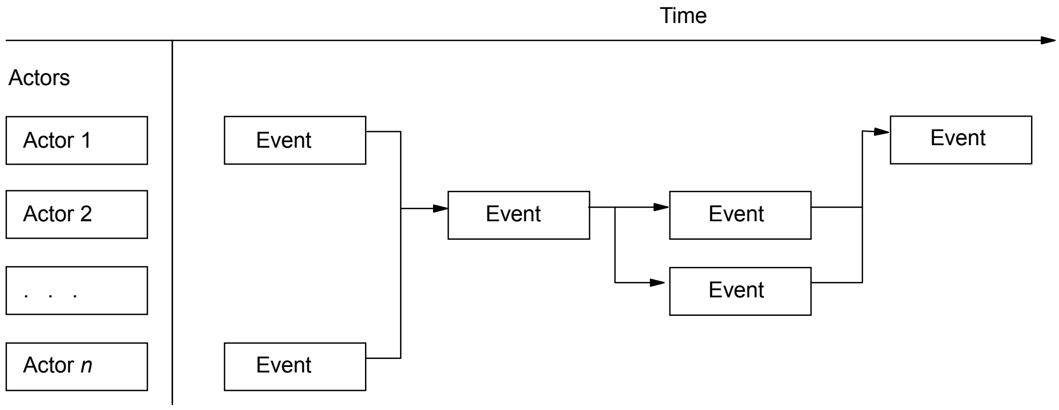


**Figure B7: STEP graph**

The analysts describe each actor on the left hand side of the graph and show all events in which they were involved, in their correct sequence along the time axis of the graph in line with the description of the actor. The analysts then determine links between events and show these links using arrowed lines joining different events. The logic used is that of assessing necessary and sufficient conditions: if one event was sufficient to cause the next event, then it is linked to that event. If an event is necessary (must occur) before the following event can logically occur, then the two events are linked. Several events may have to occur for a subsequent event to occur; all those events are shown as influencing the subsequent event by arrowed lines showing the direction of influence. Where a causal relationship cannot be established, but one event preceded another, the analyst can insert a broken arrow with a question mark to denote this.

Conditions that may influence events are deliberately excluded from STEP. They are considered to introduce information that can obscure the real reasons for events and, in any case, are usually outcomes from previous actions. STEP's supporters suggest that ignoring conditions allows them to focus purely on event relationships and avoid any confusion or ambiguity that could ensue from considering conditions. They also argue that conditions are often simply outcomes from events. As an example, an operator fails to input a set point on a fuel delivery system correctly. This – it could be said – was caused by poor environmental conditions: cold, bright weather affecting manual dexterity and the operator's view of the setting. STEP could include this in several ways; for example, by including the event of the operator entering that environment or the event of failing to adequately check the setting.

There are no specific rules in STEP for identifying root causes. Analysts should inspect the event information presented and determine from inspection which of these could be root cause.

**Useful reference information**

Hendrick, K and Benner, L. (1987). Investigating accidents with Sequentially Timed and Events Plotting (STEP). Marcel Decker, New York, USA.

## B21. STORYBUILDER

Storybuilder is a recently developed software tool for analysing existing industrial incident reports.

The method has been devised on behalf of the Dutch government and is intended to help in identifying the dominant causes of occupational accidents. Those causes should be tackled first.

The method is based on the bow-tie model of accidents (see No. B2).

Storybuilder is used to analyse specific classes of occupational accidents. As an example, 715 accidents involving falls from ladders were analysed. Of these, 482 failures were attributed to 'ladder stability' as the primary safety barrier that failed. 417 of these resulted from incorrect placement by the user. In turn, half of these failures were caused by the user selecting the wrong type of ladder.

Storybuilder contains a large number of ready-constructed bow-ties for different accident classes. These can be used to analyse further accidents by matching them to the appropriate story.

The method could be used by anyone wishing to examine existing occupational incidents in order to identify trends and underlying causes.

**Useful reference information**
Oh, J (2007). The use of Storybuilder as an incident analysis tool. Presented at OECD/CCA Workshop on Human Factors in Chemical Accidents and Incidents. 8-9 May 2007, Potsdam, Germany
http://www.storybuilder.eu/

## B22. TAPROOT®

An incident investigation using TapRooT® is conducted in the following steps, each supported by tools provided by the method:

1. Determine sequence of events – from evidence gathered in the incident investigation. TapRooT® provides a number of tools to help in this including: change analysis, barrier analysis and Critical Human Action Profile (CHAP – which helps to characterise critical tasks). The sequence of events is represented on a timeline akin to an ECFA chart known as a SnapCharT®.
2. Define causal factors – from further investigation, the analyst adds further sequences and causal factors to the chart. A causal factor may be the failure of a specific item of equipment. A causal factor is anything that, if absent from the sequence of events, would have prevented the event occurring or made its consequences less severe.
4. Analyse each causal factor’s root cause – TapRooT® provides a tool for the analyst to identify whether the root cause was either:
   — a 'human performance difficulty';
   — an 'equipment difficulty';
   — a natural disaster or sabotage, or
   — 'other'.
5. Analyse each root cause's generic cause – having determined in the previous step the root cause, the method provides a 'troubleshooting guide' in the form of question sets that direct the analyst to explore a deeper level of causes.

   For example, a fitter forgets to close a valve following a maintenance task. This is found, using the tools provided, to be a 'human performance difficulty'. The 'basic cause' of this is then found to be 'human engineering'. Exploring this category, the analyst determines that the cause of the 'human engineering' problem is that the system is too complex (this is a 'near root cause').

The root cause is found to be that the fitter was attending to too many items at once.

6. Develop and evaluate corrective actions – the method suggests corrective actions based on the causes found in the incident analysis.
7. Report and implement corrective actions – in the software version of the tool, the report is generated automatically.

**Useful reference information**

Paradies, M and Unger, L (2000). TapRooT® - The system for root cause analysis, problem investigation, and proactive improvement, Knoxville, TN: System Improvements, Inc.
www.taproot.com

## B23. KELVIN TOP-SET®

Kelvin Top-Set is a method for investigating and analysing incidents. The name is derived from the issues that the method developers believe should be investigated, namely: Time, Organisation, People, Similar Events, Environment and Technical.

The method is available as a paper-based or software tool. The information below is based on the 'Investigator' software. This is identical in function to the paper-based version of Top-Set. Using this, the analyst conducts an investigation in nine steps:

1. File an initial incident report – logs the incident and basic details about it.
2. Terms of reference – these are generated automatically following step 1 and can be edited.
3. Report introduction – free text area for the analyst to set out relevant details for the report.
4. Plan the investigation – shows the Top-Set 'indicator card' outlining the areas for investigation and sub-areas, for example, 'People' has sub-set areas 'activities and tasks' and 'skills and training'. Clicking on any sub-set topic produces a 'planning issues' pro-forma. This provides a prompt for taking action on a particular topic as part of the investigation.
5. Develop the storyboard – a timeline is already partially completed from the information provided already but can be edited and re-arranged. In appearance, the storyboard resembles a wallchart with 'yellow stick on notes' attached.
6. Identify immediate causes – in this section, the immediate and underlying causes are identified and explored via prompts from the system. The inputs made to this part of the method are shown in the 'root cause diagram' described in step 7.
7. Draw a root cause diagram – the input from the above produces an initial root-cause diagram that can be edited. The yellow boxes are shown with lines attached indicating why particular events or conditions occurred.
8. Make recommendations – the method does not provide ready-made solutions. In this section, the analyst should make recommendations for improvement. The method encourages the recommendations to be 'SMART'.
9. Generate a final report – automatically generates a report from the information provided up to this point.

The method providers offer various levels of training courses to support the use of the tool. It is unlikely that an untrained user would be able to generate appropriate information without training. Top-Set appears to have been based on the expertise of its developers. The topic areas covered are relevant to human factors.

**Useful reference information**

http://www.kelvintopset.com/

## B24. TRACEr – TECHNIQUE FOR RETROSPECTIVE AND PREDICTIVE ANALYSIS OF COGNITIVE ERRORS

TRACEr is an error identification and analysis tool developed for the aviation industry, in particular, air traffic control, but has been used in other industries. This usually entails no more than changing some of the terminology used, e.g. from 'aircraft' to 'ship' or 'locomotive'.

The model that forms the basis of TRACEr (see HFAT (see No. B9)), describes four elements of information processing. TRACEr describes the errors that could be associated with each of these elements, for example:

1. Perception – errors in seeing, hearing or otherwise detecting information.
2. Memory – forgetting information or recalling it incorrectly; forgetting an action just carried out or forgetting to perform an action in the future.
3. Judgement – errors in planning, decision-making and judgement .
4. Action execution – actions that do not achieve the intended aim (errors of commission).

TRACEr supports the analyst in examining incident data in order to establish:

- The 'external error modes' i.e. the type of error such as 'action omitted', 'action on wrong object', 'action too early/late', 'information not sought/obtained', 'wrong information transmitted' etc.
- The 'internal error modes' i.e. the underlying error with perception, memory etc. that could have contributed to the external error, such as: late detection (of information); forget information or forget to carry out an action; misjudge (e.g. distance) or make an incorrect decision; overshoot or overdo an action, give out incorrect information.
- The 'psychological error modes' influencing the internal error modes i.e. underlying failures in information processing such as: making assumptions; becoming confused or distracted; having a memory block etc.
- The PSF influencing the errors such as the working environment, procedures, training and experience.

As an example, a plant operator failed to close a valve to stop a leak. They had detected the leak and knew what to do, thus it was not a perception error but an action error – in this case, 'action too late' – since they closed the valve but could have done so more quickly. The internal error mode was a judgement error – they believed they had more time to react and carried out other actions first. Several psychological error modes drove the internal error, including 'prioritisation failure' and 'incorrect knowledge'. A key PSF was the stress of the incident.

The method is used as an aid to interviewing those involved in incidents although it may be possible to derive some useful information from written records of incidents depending on the detail in those records.

The concepts in TRACEr may be new to the untrained user and may require existing expertise in human reliability terminology. The flowcharts and checklists provided are easy to use. The analyst should need to interpret the material for their own industry, but the method provides the stimulus for exploring incidents.

### Useful reference information

Kirwan, B and Shorrock S (2002). Development and application of a human error identification tool for air traffic control. Applied Ergonomics 33 (2002) 319–336

## B25. TRIPOD BETA

Tripod Beta is based on the research work of James Reason, Jop Groeneweg and others. It describes incidents in terms of 'objects' e.g. people, equipment being changed by 'agents' (of change i.e. anything with the potential to change an object). Tripod Beta also models 'barriers' showing them as, for example, effective, failed or inadequate barriers.

Tripod Beta provides a format and rules for modeling the event and linking each element together and working back ultimately to the underlying causes.

In Tripod, the underlying causes - 'latent failures' - 'are known as Basic Risk Factors (BRFs). BRFs are associated with:
— design;
— hardware;
— maintenance management;
— error inducing conditions;
— housekeeping;
— incompatible goals;
— procedures;
— communication;
— training, and
— organisation.

A twelfth BRF, 'Defences' is equivalent to the idea of 'barriers'. The example below illustrates the method. The incident under investigation is a vehicle rollover seriously injuring a driver.

In Figure B8 (numbers added for purposes of illustration)

(1) The red box describes the event in terms of its outcome – permanent disability. The box above this (2) with the red and yellow/black border is a combination of an object (3 – the driver) undergoing change (back injury) as a result of another set of events and condition combinations leading to (4 – vehicle rollover). The driver would not have suffered permanent disability had he been moved expertly by his company's search team. Failed barriers (5 and 6) are shown as black blocks that allowed an agent (7 – incorrect extraction of driver) to make this change. Factors causing the barriers to fail are modelled as 'preconditions' (8, 9 and 10 – blue boxes) that in turn originated in several BRFs (yellow boxes), in this case, organisational failure (11) incompatible goals (12) and a failed defence (13).

Tripod Beta is a software-based tool and should be used only by trained analysts. The practitioner training takes four days; shorter courses for other types of user are also avaliable. The training introduces the philosophy underlying the method.

**Useful reference information**

Groeneweg, J. (2002). Controlling the controllable, the management of safety. Fifth edition. Global Safety Group, Leiden University ISBN 90 6695 140 0 / ISSN 0928 8058;29)
http://www.tripodsolutions.net/

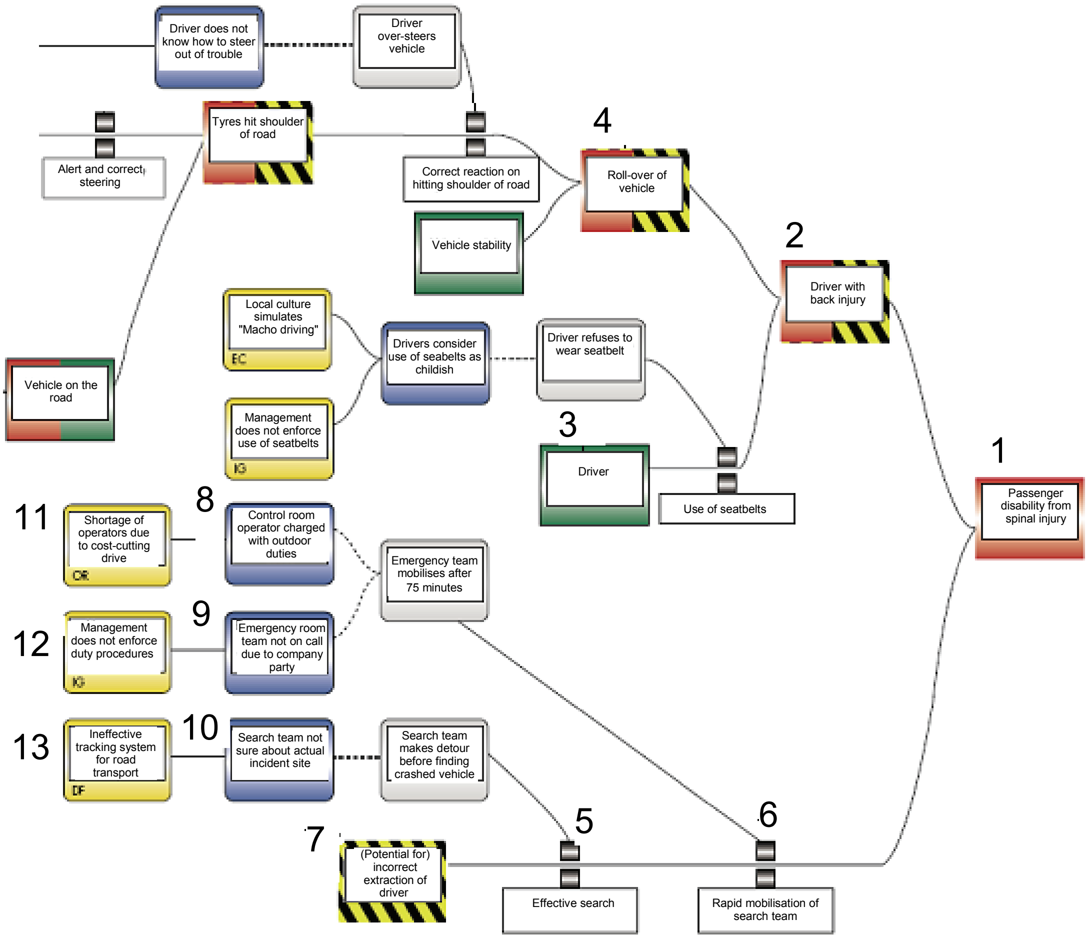


**Figure B8: Tripod Beta diagram**

## B26. WBA – WHY BECAUSE ANALYSIS

Why Because Analysis (see Figure B9) comprises the following key steps:

1. Gather and assess information about the incident – thoroughly review all witness and documentary evidence to determine the basic facts about the incident. Then, using this information, do either step 2 or 3.
2. Create a 'list of facts' – literally, a list of all items of information gathered. Give each fact a unique number, describe the fact briefly and note down where the fact came from (witness name, document reference, photograph etc.).
3. Construct a 'why-because list' – this is a list of pairs of effect-cause facts. E.g. Fact A = 'The Titanic's hull was holed below the waterline' [why? because] Fact B = 'the Titanic collided with an iceberg'.
4. (Optional step) Apply a 'counterfactual test' to the pairs of facts, and correct as necessary. This is purely a logic test; the analyst questions whether, if B had not occurred, A would have still have occurred? If the answer is yes, then the two facts are not logically linked.
5. (Optional step) Create an auxiliary list of facts – if the list of facts or 'why because list' fails to produce a clear picture of the events that took place, the facts can be re-arranged into groups according to, for example, the time they occurred or the person involved. (Using this classification can help produce a timeline or other supplementary model of the events and conditions that contributed to the incident.)
6. Construct a why-because graph as follows:
   - Determine the 'mishap' – the event that was most responsible for the incident. Make this the top node in the graph e.g. 1 500 people died [why?because] the Titanic sank.
   - Identify the 'necessary causal factors':
     - If why-because pairs have been used, these should already be paired logically.
     - If the list of facts is used, start with the 'mishap' and identify which facts in the list of facts pass the logic test in Step 4
   - Continue until a detailed breakdown of the facts is represented on the graph e.g. 'bow section divided from stern' [why?because] 'stern section lifted out of the water' [why?because] etc.
7. Quality check the analysis for completeness and accuracy – change the graph as necessary.

The graph itself can be produced using yellow 'stick on notes' and paper with the nodes joined by arrowed lines showing the logical relationships between facts.

**Useful reference information**
http://www.rvs.uni-bielefeld.de/research/WBA/

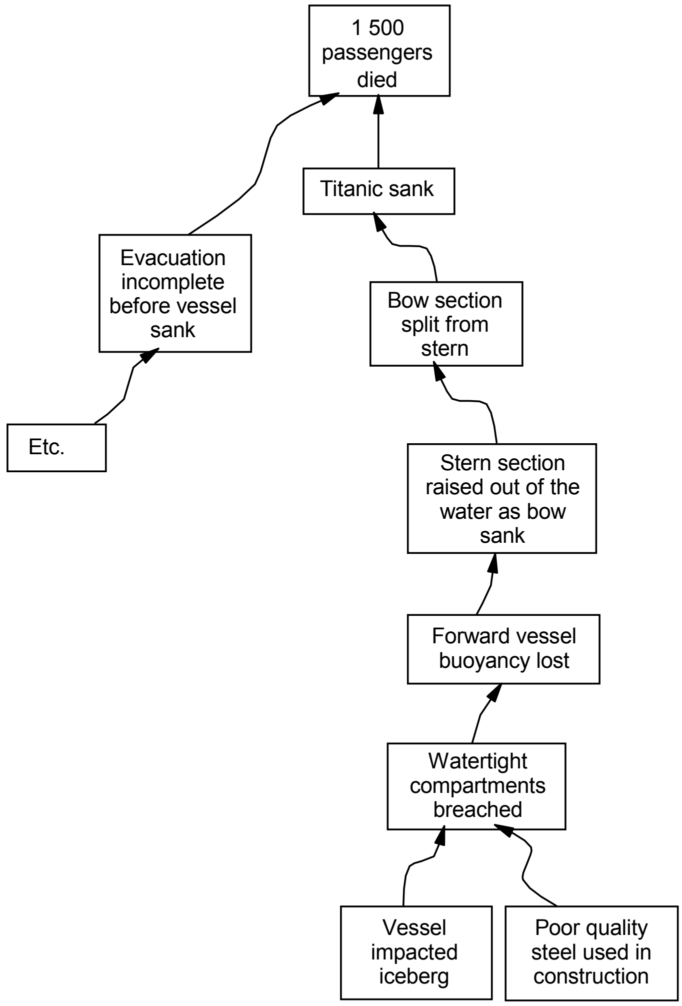


**Figure B9: WBA diagram**

## B27. 5 WHYS

The basic approach is to gather information on an incident and form a team. The team then asks why (the incident occurred), referring to the information available to answer the question. The team should reach a point when asking why no longer makes sense either because a root cause has been found or there is insufficient information to answer the question. This can take more or less than five 'whys'; questions may also be phrased in other ways, 'how is it that', 'what affected this'. It is a simple method for novice users, but they should need some knowledge of root causes in order to know whether they have reached the appropriate level of detail in their analysis.

The method is often used by drawing a timeline on a large sheet of paper stuck onto a meeting room wall. The team can then trace back the events leading up to the incident and write on the reasons that they believe each event occurred (or use yellow 'stick on notes' to make changes more easily).

**Useful reference information**
Information freely available on the Internet for example
http://www.isixsigma.com/library/content/c020610a.asp

## B28. WHY TREE

Why Tree analysis is a means of assembling information on an incident in a logic diagram. It is sometimes known as 'Causal Factors Tree Analysis'. The diagram looks like a fault tree but is a means of structuring information about a problem. A tree is illustrated in Figure B10 and shows how a person was injured at work. Below this event, the four main causes are shown. Each cause should be necessary or sufficient for the event to happen; otherwise they do not belong in the diagram. Below the events boxes, key factors are shown. Again, these should be necessary or sufficient to have caused the event above. Finally, corrective actions are determined and shown on the diagram against the factor they are intended to address. This is not, in this form, a root cause analysis method as there are unanswered questions as to why the conditions noted existed.

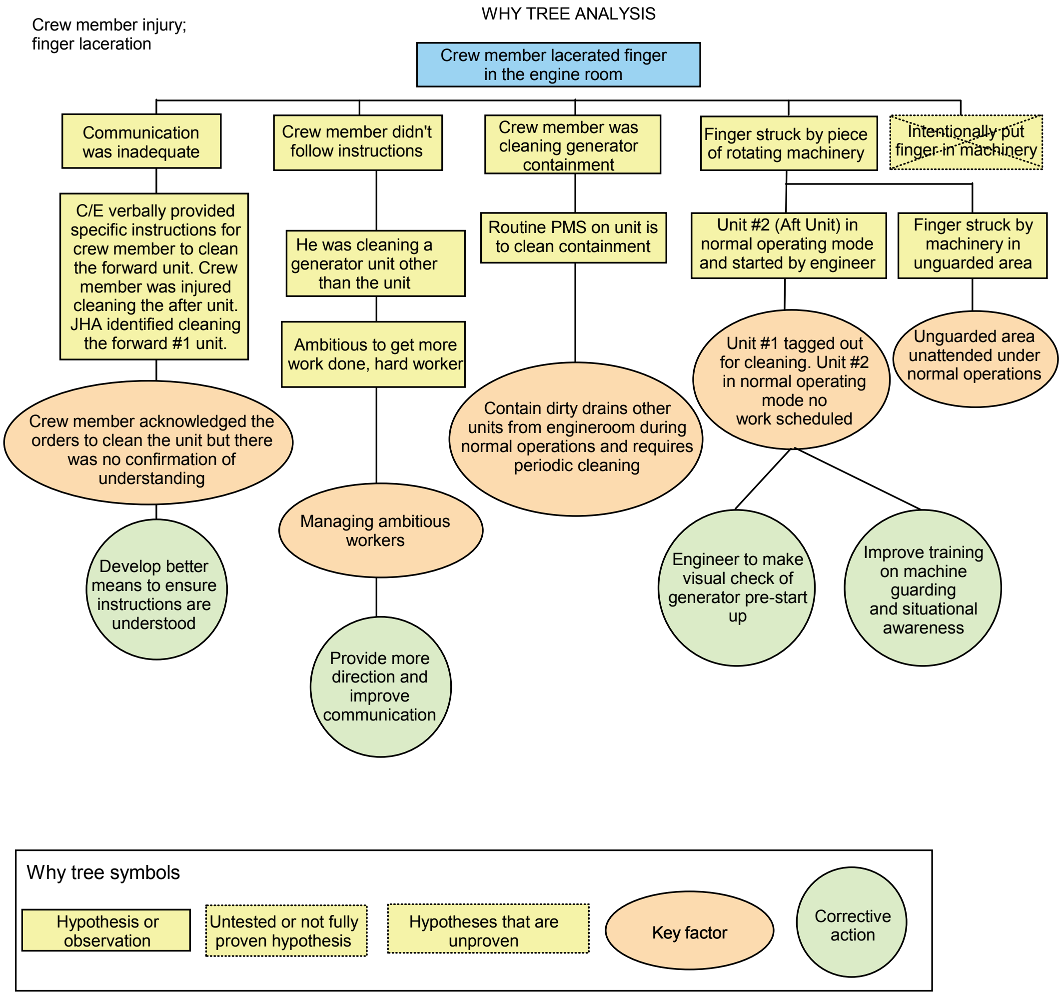


**Figure B10: Why tree diagram**

### Useful reference information

Nelms, RC (1996). The Go Book. ISBN 1886118205
http://www.failsafe-network.com/

**FURTHER METHODS:**

Some further methods cited in the literature are also briefly described. They are not in Annex B as they did not seem to be mainstream techniques used by petroleum or allied industry users. They do seem to have the potential for application in these industries however (see below):

**CALM – Combined Accident anaLysis Method**
A combination of SOL and simplified Why Because Analysis. The method helps the analyst to develop: a situational description; a list of facts – which are then organised into - Event Building Blocks (EBBs) and from those, it is possible to build a Time-Actor Diagram (TAD) – i.e. a timeline. A checklist of factors then helps the analyst to identify 'active failures' and 'latent conditions' and the analyst then builds the EBBs in to a Why-Because graph to determine causes.

**For further information see:**
Blackett, C. (2005). PhD Thesis, Combining accident analysis techniques for organisational safety. National University of Ireland, Faculty of Science, School of Computer Science and Informatics. Dublin http://www.claireblackett.com/papers/ISSC05.pdf

**ISIM Integrated Safety Investigation Method**
ISIM is the method that inspectors in the Transportation Safety Board of Canada use to investigate accidents. It is a software tool based on Reason's 'Swiss cheese' model and the 'SHELL' model. SHELL is an acronym to remind the user that incidents originate in the interaction between 'Liveware' (people), 'Software' (including manuals etc), 'Hardware' (tools and equipment), 'Environment' and other 'Liveware'.

**PROACT®**
PROACT® is a software package that allows the user to identify the root causes of incidents. It assists the user in building a logic tree (akin to a fault tree) to assemble and analyse the information collected. Causes of incidents are described in terms of '5Ps': parts - items that failed in the incident; position – taking photographs of the scene; paper – manuals, and other relevant material such as inspection reports, job safety analyses etc; people – those involved in the incident or present when it occurred; paradigms – 'mind-set' or false beliefs about any aspect of the job.

**SACA – Systematic Accident Cause Analysis**
Used to generate statistics on causes of incidents. Based on the UK Health and Safety at Work Act as a means of determining responsibility for remedial action. Includes checklists of causes:
— persons;
— equipment;
— place of work;
— systems of work, and
— outside local control.
Each of these is divided into sub-categories.

**For further information see:**
Waldram I, (1988), What really causes accidents?, The Safety Practitioner
Health and Safety Executive (2001). Root causes analysis: Literature review. Contract Research Report 325/2001. HSE Books. ISBN 0 7176 1966 4
http://www.hse.gov.uk/research/crr_pdf/2001/crr01325.pdf

**STAMP Systems Theoretic Accident Modelling and Process**
STAMP is a method that requires the analyst to model the system that people work within and then determine how various identified hazards affect the system. Incidents result from failings in the

system.

This method differs from the timeline-based methods: it could be difficult to use and to ensure that the model developed is complete. STAMP can be used proactively to analyse potential system weaknesses by examining how the system would react in various scenarios.

**For further information see:**

Blackett, C. (2005). PhD Thesis, Combining accident analysis techniques for organisational safety. National University of Ireland, Faculty of Science, School of Computer Science and Informatics. Dublin

**TOR – Technique of Operations Review**

A method that provides worksheets allowing a group or individual to investigate the root causes of accidents. The worksheets probe the following elements: training, responsibility, decision and direction, supervision, work groups, control, personality traits, and, management.

**For further information see:**

Waldram I, (1988), What really causes accidents?, The Safety Practitioner

Health and Safety Executive (2001). Root causes analysis: Literature review. Contract Research Report 325/2001. HSE Books. ISBN 0 7176 1966 4

http://www.hse.gov.uk/research/crr_pdf/2001/crr01325.pdf

# ANNEX C
# REFERENCES AND BIBLIOGRAPHY

## C1 REFERENCES


[1] Buys, R.J. and Clark, J.L. (1978). Events and causal factors charting. DOE 76-45/14, (SSDC-14) Revision 1. Idaho Falls, ID: System Safety Development Center, Idaho National Engineering Laboratory.
[2] Health and Safety Executive (1997). Successful health and safety management. HSG65. HSE Books, Sudbury, Suffolk. ISBN 0 7176 1276 7
[3] Parliamentary Office of Science and Technology (2001) POST Note 156 (www.parliament.uk/post/pn156.pdf) quoting Feyer, A.M. and Shouldiamson, A.M. (1998): Human factors in accident modelling. In: Stellman, J.M. (Ed.), Encyclopaedia of Occupational Health and Safety, Fourth Edition. Geneva: International Labour Organisation
[4] Baker, CC and Seah, AK(2004). Maritime accidents and human performance: the statistical trail. American Bureau of Shipping. Presented at MARTECH 2004, Singapore, 22-24 September, 2004
[5] Energy Institute (2003). Human factors briefing notes. http://www.energyinst.org.uk/humanfactors/bn
[6] Health and Safety Executive (2004). Managing human performance – briefing notes. http://www.hse.gov.uk/humanfactors/comah/briefingnotes.htm
[7] Health and Safety Executive (1999). Reducing error and influencing behaviour. HSG48. 2nd Edition. HSE Books, Sudbury, Suffolk. ISBN 0 7176 2452 8
[8] IAEA (1991). Safety Culture: A report by the international nuclear safety advisory group. Safety Series No 75-INSAG 41991. IAEA, Vienna.
[9] SI No. 205/3117 The Offshore Installations (safety case) Regulations 2005, ISBN 0110736109. The Stationery Office.
[10] Reason, J (1990). Human error. New York: Cambridge University Press.
[11] Health and Safety Executive (2005). Investigating accidents and incidents. HSG245. HSE Books. ISBN 0 7176 2827 2 (http://www.hsebooks.com)Health and Safety Executive (1997).
[12] Successful health and safety management. HSG65. HSE Books, Sudbury, Suffolk. ISBN 0 7176 1276 7


The key references used in order to develop this publication are cited below. Detailed information on most of the incident/accident investigation methods can be found in these references.

Source material for the methods described in Annex B may be found alongside each item in Annex B.


— American Institute of Chemical Engineers (2003). Investigating chemical process incidents. 2nd Edition. AIChemE, Park Avenue, New York 10016-5991. ISBN 0-8169-0897-4
— American Bureau of Shipping (2005). Guidance notes on the investigation of marine accidents. ABS, Houston.
— Blackett, C. (2005). PhD Thesis, Combining accident analysis techniques for organisational safety. National University of Ireland, Faculty of Science, School of Computer Science and Informatics. Dublin. http://www.claireblackett.com/papers/ISSC05.pdf
— Health and Safety Executive (2001). Root causes analysis: Literature review. Contract Research Report 325/2001. HSE Books. ISBN 0 7176 1966 4 http://www.hse.gov.uk/research/crr_pdf/2001/crr01325.pdf
— Johnson, CW (2003). Failure in safety-critical systems: a handbook of accident and incident reporting. University of Glasgow Press, Glasgow, Scotland. ISBN 0-85261-784-4 http://www.dcs.gla.ac.uk/johnson/book/

— Johnson, CW (2002) Ed.. Workshop on the investigation and reporting of incidents and accidents (IRIA 2002). Department of Computing Science. University of Glasgow.
— Rail Safety and Standards Board (2004). Technical Report 09/T122/ENGE/003/TRT. Data to be collected for investigations of railway accidents. RSSB, London.

## C2 BIBLIOGRAPHY

The following websites were also consulted in the preparation of this publication but are not specifically referenced:

— Australian Transport Safety Bureau. http://www.atsb.gov.au/
— Failsafe Network Inc. http://www.failsafe-network.com/index.htm
— Federal Aviation Administration. http://www.faa.gov/
— Major Accidents Hazards Bureau. http://mahbsrv.jrc.it/
— Marine Accident Investigation Branch. http://www.maib.dft.gov.uk/home/index.cfm
— National Transportation Safety Board. http://www.ntsb.gov/
— Rail Accident Investigation Branch. http://www.raib.gov.uk/home/index.cfm
— Root Cause Live. http://www.rootcauselive.com/

# ANNEX D
# GLOSSARY AND ABBREVIATIONS

**accident:** any unplanned event that results in injury or ill-health to people, or damages equipment, property or materials but where there was a risk of harm.

**active failure:** a human error or violation the effects of which become evident almost immediately.

**barrier:** any measure taken to protect people or property from hazards, including physical guards but also administrative measures such as rules and procedures. Sometimes referred to as safeguards, defences or risk control systems.

**circumvention:** see *violation*.

**cognitive error:** see *mistake*.

**hazard:** anything with the potential for human injury or adverse health, damage to assets or environmental impact. See *risk* and *risk assessment.*

**HPLC (event):** high probability, low consequence (event). Also see *LPHC*.

**human error:** system failures attributable to people but not including *violations*.

**human failure:** a term used to collectively refer to both errors and violations.

**human-machine system:** a system in which technology and human beings have specific functions but work together towards common goals.

**immediate cause (of an incident):** the most obvious reason why the incident occurred e.g. the guard is missing, the employee slips etc. There may be several immediate causes identified in one adverse event.

**incident:** an unplanned or uncontrolled event or sequence of events that has the potential to cause injury, ill-health or damage. Also referred to as a *near miss*.

**lapse:** when a person forgets to do something due to a failure of attention/concentration or memory.

**latent failure (or latent error):** a human error or violation whose effects can lie dormant in a system for a long time.

**LPHC (event):** low probability, high consequence (event).

**major accident hazard:** hazards with the potential for major accident consequences, e.g. ship collisions, dropped objects, helicopter crashes as well as *process safety hazards*. Major accidents are potentially catastrophic and can result in multiple injuries and fatalities, as well as substantial economic, property, and environmental damage.

**mistake (synonymous with 'cognitive error'):** when a person does what they meant to do, but should have done something else. This is not necessarily a *violation* but part of the action taken could involve rule-breaking or similar non-compliances.

**near miss:** see *incident*.

**non-compliance:** see *violation*.

**occupational safety hazard:** personal or occupational safety hazards give rise to incidents – such as slips, falls, and vehicle accidents – that primarily affect one individual worker for each occurrence (noting, of course, that they could affect many people). They contrast with *process safety hazards* and *major accident hazards* in that the latter have the potential to affect a very large number of people including those off-site.

**performance shaping factor (PSF):** any factor that can affect human performance; PSFs can exert a positive or negative influence.

**personal safety hazards:** see *occupational safety hazard*.

**POPMAR:** policy, organising planning measuring (performance) auditing and reviewing (performance) – the SMS model used in HSE's Successful health and safety management.

**process safety hazards:** hazards that can give rise to major accidents involving the unplanned release of potentially dangerous substances, pressure, energy (such as fires and explosions) etc.

**risk:** the level of risk is determined from a combination of the likelihood of a specific undesirable event occurring and the severity of the consequences (i.e. how often is it likely to happen, how many people could be affected and how bad would the likely injuries or ill health effects be?).

The likelihood of human injury or adverse health, damage to assets or environmental impact from a specified hazard. Note that other risk definitions include a reference to the severity of the consequences – injury, damage etc. See *hazard* and *risk assessment.*

**risk assessment:** the process of assessing the risk of exposure to a particular hazard in a specified activity. See *hazards* and *risk.*

**root cause (of an incident):** an initiating event or failing from which all other causes or failings spring. Root causes are generally management, planning or organisational failings.

**safety critical system:** any part of an installation whose failure could contribute substantially to a major accident or whose purpose is to prevent or limit the effects of such accidents.

**slip:** when a person does something but not what they meant to do.

**SMART:** specific, measurable, achievable (and assigned to someone), relevant and timebound (with a specific deadline for completion).

**SMS:** safety management system.

**underlying cause (of an incident):** the less obvious 'system' or 'organisational' reason for an incident e.g. pre-start-up machine checks are not carried out, the hazard has not been adequately considered via a suitable and sufficient risk assessment, production pressures too great etc.

**violation (synonymous with 'circumvention'):** a type of human failure when a person decided to act without complying with a known rule, procedure or good practice. The word may have connotations of wrongdoing and alternatives such as *non-compliance* or *circumvention* are also used.

Note: organisations differ widely in their use of some of the above terms, for example, the words 'incident' and 'accident' are often used to mean the same type of event. The above definitions are used in this publication.

**Note:** that for the purposes of brevity, where the word 'incident' is used on its own, unless otherwise stated, it should be taken to refer to an *incident* or an *accident*.

**Energy Institute**
61 New Cavendish Street
London W1G 7AR, UK

t: +44 (0) 20 7467 7157
f: +44 (0) 20 7255 1472
e: **pubs@energyinst.org.uk**
**www.energyinst.org.uk**

This publication has been produced as a result of work carried out within the Technical Team of the Energy Institute (EI), funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost effective, value adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and beyond.

ISBN 978 0 85293 521 7