BS EN 62740:2015

BSI Standards Publication

Root cause analysis (RCA)

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62740:2015. It is identical to IEC 62740:2015.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 79741 5

ICS 03.120.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62740

April 2015

ICS 03.120.01

English Version

Root cause analysis (RCA)
(IEC 62740:2015)

Analyse de cause initiale (RCA)
(IEC 62740:2015)

Ursachenanalyse
(IEC 62740:2015)

This European Standard was approved by CENELEC on 2015-03-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62740:2015 E

Foreword

The text of document 56/1590/FDIS, future edition 1 of IEC 62740, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62740:2015.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-12-20
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2018-03-20

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62740:2015 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-1	NOTE	Harmonized as EN 60300-1.
IEC 61025	NOTE	Harmonized as EN 61025.
IEC 61649	NOTE	Harmonized as EN 61649.
IEC 61163-1	NOTE	Harmonized as EN 61163-1.
IEC 62508:2010	NOTE	Harmonized as EN 62508:2010 (not modified).
ISO/IEC 31010:2009	NOTE	Harmonized as EN 31010:2010 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60050 Series	-	International Electrotechnical Vocabulary (IEV)	-	-

CONTENTS

INTRODUCTION

Root cause analysis (RCA) refers to any systematic process that identifies factors that contributed to a particular event of interest (focus event). RCA is performed with the understanding that events are addressed by understanding the root causes, rather than the immediately obvious symptoms. RCA aims to reveal root causes so that either the likelihood of them occurring, or their impact if they do occur, can be changed.

An important distinction to make is that RCA is used to analyse a focus event that has occurred and therefore analyses the past (a posteriori). However, knowledge of the root causes of past events can lead to actions that generate improvements in the future.

This International Standard is intended to reflect current good practices in the conduct of RCA. This standard is general in nature, so that it may give guidance across many industries and situations. There may be industry specific standards in existence that establish preferred methodologies for particular applications. If these standards are in harmony with this publication, the industry standards will generally be sufficient.

This standard is a generic standard and does not explicitly address safety or accident investigation although the methods described in this standard may be used for this purpose.

ROOT CAUSE ANALYSIS (RCA)

1 Scope

This International Standard describes the basic principles of root cause analysis (RCA) and specifies the steps that a process for RCA should include.

This standard identifies a number of attributes for RCA techniques which assist with the selection of an appropriate technique. It describes each RCA technique and its relative strengths and weaknesses.

RCA is used to analyse the root causes of focus events with both positive and negative outcomes, but it is most commonly used for the analysis of failures and incidents. Causes for such events can be varied in nature, including design processes and techniques, organizational characteristics, human aspects and external events. RCA can be used for investigating the causes of non-conformances in quality (and other) management systems as well as for failure analysis, for example in maintenance or equipment testing.

RCA is used to analyse focus events that have occurred, therefore this standard only covers a posteriori analyses. It is recognized that some of the RCA techniques with adaptation can be used proactively in the design and development of items and for causal analysis during risk assessment; however, this standard focuses on the analysis of events which have occurred.

The intent of this standard is to describe a process for performing RCA and to explain the techniques for identifying root causes. These techniques are not designed to assign responsibility or liability, which is outside the scope of this standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050 (all parts), *International Electrotechnical Vocabulary*

3 Terms, definitions and abbreviations

For the purposes of this document, the definitions given in IEC 60050-192, as well as the following, apply.

3.1 Terms and definitions

3.1.1
cause
circumstance or set of circumstances that leads to failure or success

Note 1 to entry: A cause may originate during specification, design, manufacture, installation, operation or maintenance.

[SOURCE: IEC 60050-192:2014, 192-03-11 modified – addition of the words “circumstance or” and "or success" in the term]

3.1.2
causal factor
condition, action, event or state that was necessary or contributed to the occurrence of the focus event

3.1.3
contributory factor
condition, action, event or state regarded as secondary, according to the occurrence of the focus event

3.1.4
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified – Deletion of Note 4 [1]][1]

3.1.5
failure <of an item>
loss of ability to perform as required

Note 1 to entry: A failure of an item is an event that results in a fault of that item.

Note 2 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 3 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

Note 4 to entry: This is failure of an item, not more generally of behaviour.

[SOURCE: IEC 60050-192:2014, 192-03-01, modified – Introduction of new Note 4]

3.1.6
failure mechanism
process that leads to failure

Note 1 to entry: The process may be physical, chemical, logical, psychological or a combination thereof.

[SOURCE: IEC 60050-192:2014, 192-03-12, modified – the word "psychological" has been added]

3.1.7
focus event
event which is intended to be explained causally

3.1.8
immediate causal factor
condition, action, event or state where there is no other causal factor between this causal factor and the focus event

---

1 Numbers in square brackets refer to the Bibliography.

Note 1 to entry: There may be more than one immediate causal factor.

3.1.9
necessary causal factor <of an event or state>
condition, action, event or state, that resulted in the given event or state, without which the given event or state would not have occurred

3.1.10
human error
discrepancy between the human action taken or omitted, and that intended or required

Note 1 to entry: The first edition of IEC 60050-191:1990 identified “mistake” as a synonym for "human error", but a mistake is a type of human error.

Note 2 to entry: The term human error applies to any situation where the outcome is not as intended whether the intent of the person was correct or not.

[SOURCE: IEC 60050-192: 2014 192-03-14, modified – Omission of the example, addition of Note 1 and 2]

3.1.11
item
subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item is often comprised of elements that may each be individually considered.

[SOURCE: IEC 60050-192: 2014, 192-01-01, modified – omission of internal references and Notes 4 and 5]

3.1.12
root cause
causal factor with no predecessor that is relevant for the purpose of the analysis

Note 1 to entry: A focus event normally has more than one root cause.

Note 2 to entry: In some languages, the term root cause refers to the combination of causal factors which have no causal predecessor (a cut set of causal factors).

3.1.13
root cause analysis
RCA
systematic process to identify the causes of a focus event

Note 1 to entry: IEC 60050-192:2014, definition 192-12-05 provides the following more restrictive definition “systematic process to identify the cause of a fault, failure or undesired event, so that it can be removed by design, process or procedure changes”. This standard uses an extended definition to allow a wider applicability of the process.

Note 2 to entry: This note applies to the French language only.

3.1.14
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: IEC 60300-1:2014, 3.1.15] [2]

3.1.15
stopping rule
reasoned and explicit means of determining when a causal factor is defined as being a root cause

3.2 Abbreviations

BGA	Ball grid array
CAST	Causal analysis using STAMP
CCT	Causal completeness test
CT	Counterfactual test
CTM	Causes tree method
ECF	Events and causal factors
EEM	External error mode
FTA	Fault tree analysis
GEMS	Generic error modelling system
HFACS	Human factor analysis and classification scheme
IEM	Internal error mode
MES	Multilinear events sequencing
MORT	Management oversight and risk tree
PEM	Psychological error mechanism
PSF	Performance shaping factors
RCA	Root cause analysis
SOL	Safety through organizational learning
STAMP	Systems theoretic accident model and processes
STEP	Sequentially timed events plotting
TRACEr	Technique for restrospective and predictive analysis of cognitive errors
WBA	Why-because analysis

4 RCA – Overview

RCA refers to any systematic process that identifies the cause or causes that contribute to a focus event. The immediate or obvious cause of a focus event is often a symptom of underlying causes and may not truly identify the root cause or causes that should be identified and addressed. RCA provides a greater understanding about why events have occurred. RCA may identify the following:

a) a single root cause;

b) multiple root causes in which the elimination of any cause will prevent the focus event from occurring;

c) root causes which are contributory factors where elimination will change the likelihood of the focus event occurring but may not directly prevent it;

d) root causes of successes.

By addressing the root cause or causes it is possible to make decisions regarding appropriate actions that will generate better outcomes in the future; implementing appropriate actions based on RCA are more effective at preventing the same or similar events with negative

outcomes occurring or increasing the probability of repeating events with positive outcomes, when compared with just addressing the immediately obvious symptoms.

RCA can be applied to any focus event whether success or failure, for example:

1) investigation for technological, medical and occupational focus events;
2) failure analysis of technological systems, to determine why an item failed to perform as and when required;
3) analysis of quality control and business processes;
4) analysis of successful outcomes.

RCA can be carried out at various levels of decomposition, for example, from system to component level or by selecting different events or outcomes as a starting point. The level appropriate to conduct the analysis will be dependent on the focus event.

RCA is used to analyse focus events which have actually occurred and is therefore applicable during the testing and operational phases of a project or product life cycle. RCA can identify problems of process including design, quality control, dependability management and project management.

The benefits of performing RCA include:

- obtaining a greater understanding into what has happened;
- finding the source of problems so corrective action can prevent future events;
- identifying the causes of events with beneficial outcomes so they can be repeated;
- identifying more effective actions to address the causes of focus events;
- achieving the objectives of focus event investigations more effectively;
- supporting traceability between focus event investigation evidence and conclusions;
- increasing consistency between investigations of similar focus events;
- increasing objectivity of focus event analysis.

5 The RCA process

5.1 Overview

To be effective, RCA should be performed systematically as an investigation, with the root causes and conclusions backed up by documented evidence. To achieve this, RCA should include the five steps shown in Table 1 and illustrated in Figure 1.

Table 1 – Steps to RCA

Step	Concepts and tasks to be performed
Initiation	Based on the knowledge available on the focus event, determine the need to carry out RCA and define the purpose and scope
Establishing facts	Collect data and establish the facts of what happened, where, when and by whom
Analysis	Use RCA tools and techniques to ascertain how and why the focus event occurred
Validation	Distinguish and resolve the different possibilities as to how and why the focus event was caused
Presentation of results	Present the results of the focus event analysis

RCA is iterative in nature, especially for data collection and analysis, in that data is collected on ‘what’ happened, which is then analysed in order to determine what other data needs to be collected. Once gathered, further analysis is conducted and any gaps identified, for which

further data is collected. This process is repeated until the purpose of the analysis is fulfilled and the root causes identified. The outputs of the RCA will be dependent on its purpose and scope.

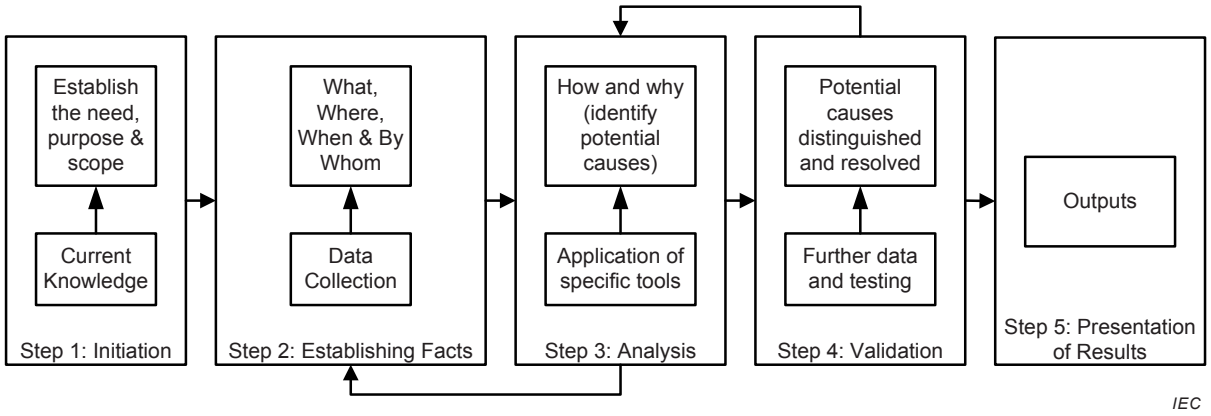


Figure 1 – RCA process

5.2 Initiation

The first step initiates the RCA process by evaluating the need to carry out RCA. It defines the purpose and scope of the analysis, in response to the focus event, and establishes a team and resources to carry out the RCA.

There is usually some criterion which is used to determine when an RCA is required, which may include:

- any single event with a large effect;
- multiple similar undesirable events;
- a parameter moving out of a defined tolerance level;
- failures or successes (whatever the level of effect) that involve critical items of equipment or activities.

When defining the type of events that require the conduct of RCA, it is important to consider that an event with a large effect may have common root causes to events with minor effects. Analysing and addressing root causes for events with minor effects may prevent a large effect event occurring. Examples of events where RCA may be required include: completion of a project (successes and failures), failures that result in unaccepfigure costs, injury or fatality, unacceptable performance or delays, large contractual consequences and equipment breakdown.

If a RCA is required, the focus event(s) to be analysed is/are described and an appropriate team appointed for the analysis. The description should include the background and context in which the focus event(s) occurred. A good description of a focus event is short, simple and easy to understand and should not be biased towards a specific solution. This description is used to identify appropriate members of the analysis team and ascertain where to start collecting data.

The purpose and scope of the RCA should be determined, taking into account knowledge of system, functions, interfaces etc. In some cases, the purpose of the analysis is to identify the causes of the focus event. In others, the purpose may be broader, for example, to also identify matters of concern outside those that led to the focus event.

There are in general two different types of RCA that have different objectives and should not be mixed up. These two types can be described as follows:

1) analysing a focus event using only verifiable factual information;
2) analysing a focus event to obtain hypotheses of sequences of events and cause.

The first version focuses on observed facts only. It may be an analysis "per se" according to the purpose of the study and no hypothesis about event occurrence is acceptable for this analysis. The second can be implemented when sufficient factual information is not available and hypotheses of potential causes are acceptable for the purpose of the analysis.

The outputs required of the RCA should also be identified. Examples are as follows:

- provide a description of each root cause along with sufficient background information to allow the identification of suitable actions;
- recommend actions that, taken together, prevent further occurrences of similar events with adverse consequences and improve the likelihood of successes;
- identify, implement and review actions to address root causes.

RCA can include the analysis of systems in which the boundaries continually evolve and interact with their environment; this interaction can take the form of information, energy, or material transfer. Therefore, the scope should specify the boundary of the analysis (what is included and what is excluded).

The scope of the analysis should where possible include a definition of the ‘stopping rule’, which is the point at which action can be defined or additional proof of cause is no longer necessary for the purpose of the analysis. For example, the last point where corrective action can be identified, before factors that cannot be influenced e.g. weather. It may however be more appropriate to ascertain the stopping rule at review points that determine whether further analysis is required.

RCA can be effectively carried out by one person provided that person is experienced with the causal analysis technique, is a domain expert (or has immediate access to domain experts) and has access to all the data required. However, it is more common to conduct RCA as a team. The team members for the analysis should be selected based on the specific expertise needed to analyse the focus event. The team should include:

- a person or persons who among them can provide a complete systems overview and knowledge of the programme or project and focus event;
- a facilitator skilled in the causal analysis technique, desirably trained or experienced in the facilitation of the causal analysis technique.

Team members can change depending on the activity being conducted, e.g. team members responsible for data collection will not necessarily be the same as those conducting the analysis. Team members can include engineers, technicians, operators, sales representatives and managers. The use of external parties should be considered to provide an independent perspective and avoid blind spots that may exist in the organization. Additional team members should be included for specific activities during the investigation to either bring expertise into the team or to increase the influence of the team. The role of these additional team members is to support the investigation so that it is not halted for technical or organizational boundary reasons. It is not appropriate for persons who may have had a role in causation of the focus event to be part of the team. Their input should be collected during the first two steps.

5.3 Establishing facts

This step includes all the activities necessary to prepare for the analysis. Establishing the facts is usually the largest part of the RCA. Facts should be determined on ‘what’ happened, ‘where’, ‘when’ and ‘by whom’.

Data should be collected, before it is lost (e.g. before evidence is disturbed or removed, or memories fade). In general data collected would include:

a) the context in which the focus event occurred;

b) the conditions before, during and after the focus event;

c) personnel involvement including actions taken (or not taken) and decisions made;

d) context data about the surroundings, including environmental data;

e) how the organization operates including organization charts, processes and procedures, training and skills;

f) historical data relating to similar events or precursors;

g) deviations from the expected;

h) interactions with other items and personnel;

i) equipment involved, its operating state and compliance with requirements.

The following lists examples of data that may be relevant:

1) Inspection of physical evidence such as failed components and failure reports. Generally, it is experience that will determine what physical evidence is required. If there is doubt, the evidence should be retained. It is also important to preserve the evidence.

2) Photographs and videos taken by monitoring cameras. Photographing the area of the occurrence from several views will also be useful in the analysis phase.

3) Operational data, recorded by monitoring systems, control systems, alarm and event loggers etc. Operator logs can be critical to understanding the operating conditions at the time of failure and since they are typically dated (or clocked), they are ideal for generating a timeline of events.

4) Personal testimony gathered by conducting interviews. Interviews should concentrate on data collection, e.g. building a consistent timeline etc; any premature discussion of the causes of the failure may adversely impact the interview process. Questions should be prepared before the interview to ensure that all necessary information is obtained. Interviews should be conducted with those people, who are the most familiar with the focus event, however, consider interviewing other personnel e.g. people who have performed the job in the past. All interviews should be documented.

5) Documentary evidence of relevant procedures, operating environment and regulatory environment.

This step can include failure analysis which examines failed components using a wide array of methods including microscopy, spectroscopy and non-destructive testing or models on the development of failure such as fire modelling or crash modelling.

Once all the data associated with the focus event has been collected, the data should be reviewed for correctness and suitability, missing data should be obtained and any inconsistencies should be resolved to ensure a clear and consistent picture of the focus event is determined.

The outcome of this step is information and understanding, supported by physical evidence and witness statements, concerning

- what happened including the circumstances that lead to the focus event,
- the time sequence of events which lead to the focus event,
- the location of the focus event,
- actions of people associated with the focus event,
- any necessary conditions for the focus event,
- the consequences of the focus event.

5.4 Analysis

5.4.1 Description

Having determined ‘what’ happened, ‘where’, ‘when’ and ‘by whom’, this step establishes ‘how’ and ‘why’ the focus event occurred. The objective of this step is to understand the focus event and its causes by structuring the data that has been collected into a form that allows root causes to be systematically derived.

RCA normally analyses facts to identify the causes that were necessary for the focus event to occur, referred to as “necessary causal factors”. However, in some cases, for example where sufficient facts are not available, the analysis may propose one or more hypotheses for cause and may also identify contributory factors and prevailing conditions which were possibly associated with the focus event, but cannot be proven to be necessary causal factors.

Analysis involves the following:

- organizing the physical evidence and witness statements concerning actions, events, conditions and outcomes;
- seeking how and why the focus event occurred using the data collected to justify conclusions. Models of causation, laboratory testing, check lists and taxonomies or statistical analysis of data may be used to assist this process;
- looking beyond the immediate causal factors to why they occurred. The aim is to seek all causal factors that contributed, not only the obvious causes;
- continuing this process until the stopping rule is invoked and root causes identified. There may be multiple root causes which can be independent or correlated.

In general, causal factors may involve technical issues, human aspects and factors relating to the physical or psycho-social environment in which the focus event occurred. All of these should be considered in seeking root causes. People with expertise in these areas should therefore be involved in the analysis.

Causal factors should be described clearly and unambiguously. Where a human action, omission or decision is identified as a causal factor, the nature of the act or decision should be specified, e.g. "the operator switched off the wrong power switch" and not just "human error".

The analysis of the causes (depending on the purpose and scope of the analysis) can consider:

- how the focus event occurred, i.e. the physical, chemical, psychological or logical process that was involved;
- preceding events or conditions that were necessary for the focus event to occur;
- relationships between causal factors including how they combined to cause the focus event and how a root cause leads to the focus event;
- organizational and management influences and human factors that were involved in the focus event or in the events and conditions leading up to it;
- prevailing conditions that may have contributed to the event occurring but were not necessary causal factors;
- matters of concern that could lead to other focus events (these are not strictly causal factors but may be an outcome of the analysis).

A structured analysis technique should be used to perform the analysis. Several formal techniques exist ranging from those that are based on a checklist of causes to techniques that guide the analyst through consideration of causes and graphically present the results. The techniques range from simple to complex and require suitably skilled practitioners or facilitators to conduct the analysis. Some techniques are based on particular models of how a

focus event occurs and hence give a particular emphasis to the results. The different models are based on different hypotheses with regard to the causation therefore they tend to lead the investigator to identify different contributory factors.

In some cases it is appropriate to use more than one technique or to take into account considerations of more than one model to identify all root causes.

Models of causation are described in Annex B and analysis techniques are described in Annex C. The most appropriate technique will be dependent on the focus event and the purpose and scope of the analysis (see Clause 6).

The analysis may indicate that further data is required. Requests for such data should be expected to occur throughout the analysis to resolve inconsistencies or complete gaps in the analysis. The analysis should continue until a ‘stopping rule’ is invoked.

5.4.2 The analysis team

A leader should be appointed for the analysis step, who is responsible for the following preparatory work:

a) obtaining copies of the agreed role and responsibilities of the team, and purpose and scope of the analysis;

b) obtaining copies of the focus event description and the facts established;

c) deciding the analysis technique(s) to be used;

d) converting the focus event description and facts established into a suitable format for use in the analysis technique selected;

e) developing an analysis plan;

f) forming the analysis team;

g) facilitating or arranging for training of team members in the analysis technique selected;

h) selecting software tools or other templates for use during the analysis;

i) arranging for a search to be made of databases, media, legal proceedings, etc. to identify focus events of a similar nature, or which may have occurred with the same or similar technologies.

The leader should review the information available to determine what analysis technique(s) should be applied and what skills are required. Expert advice in the field of RCA may need to be obtained regarding the selection of the analysis technique. The leader may also require an expert RCA facilitator for all or part of the analysis, depending on the complexity of the focus event, the complexity or volume of evidence and data or analysis technique selected.

The analysis is usually carried out by a team, with each team member being chosen for their experience and skills. The analysis team should be as small as possible, consistent with the relevant technical and operating skills and experience being available. Where input will be required from multiple parties, stakeholders or entities, the analysis team should contain representatives of each. It is the leader's responsibility to ensure the relevant stakeholders are informed, so that adequate stakeholder representation is available during the analysis.

The role and responsibilities of the analysis team members should be determined and milestones established at the outset of the analysis. A programme of meetings should be developed which reflects the objectives and milestones provided to the analysis team. This will ultimately enable any recommendations to be carried out in a timely fashion.

The leader should develop an analysis plan, which should contain the following:

1) focus event description;

2) agreed roles and responsibilities of the team, and the purpose and scope of the analysis;

3) a list of team members and the stakeholders to be represented;
4) time, date and location of the analysis meetings;
5) a summary of the data available;
6) analysis technique(s) to be used;
7) arrangements for training the analysis team in the selected analysis technique (if required);
8) the form of recording of the analysis and the analysis results, including reference to any templates or software tools to be used.

Adequate room facilities with visual and recording aids should be arranged by the leader for the efficient conduct of the analysis meetings. A briefing package consisting of the analysis plan and any essential pre-meeting reading or references should be sent to the analysis team members in advance of the first meeting, to allow them to familiarize themselves with the information available and the selected analysis technique.

The leader should ensure that an appropriate communication system is in place for informing and transferring the results of the analysis to those responsible for the next step of the RCA process (see 5.5).

5.5 Validation

A number of review activities are conducted throughout the RCA process to determine whether data collected is relevant and the analysis is representative of the data collected. This step tests whether the causes identified in the analysis can be substantiated and may be interleaved with the analysis or conducted as a separate activity.

An independent review can be carried out to assess whether the analysis is complete and correct and to determine whether the purpose of the analysis has been fulfilled. The review method will be dependent on the analysis technique used and on the focus event. In some cases experiments can be performed to repeat the occurrence of the focus event; where appropriate, statistical methods should be used to assess the degree of confirmation of the hypothesis of cause. If the causes are validated with the help of simulation, care should be taken to ensure the simulation is representative.

During the analysis there may be several alternative hypotheses of how the event could have happened. If the objective is to produce a factual report of the causes then at the completion of the analysis the causes should be validated and only a single conclusion should remain.

This step may require further data collection to seek direct evidence to support or refute the causes identified. Evidence may not always be available to fully validate all potential causes.

5.6 Presentation of results

The results of the analysis will depend on the purpose of the analysis. For example, if the purpose of the analysis is to identify the actions that, taken together, prevent further occurrences of similar events, the analysis results should identify corrective actions which break the causal network and prevent the focus event occurring again. If the purpose of the analysis is to repeat successes, then actions that enhance the likelihood or the consequences of the focus event should be proposed. The effectiveness of the analysis results is dependent on the quality of the analysis.

An agreed format for presenting the results of the RCA should be developed that summarizes the analysis and captures the required outcomes from the analysis, e.g. recommended actions. If the expected outcome of the RCA is to produce recommended actions, the summary should include the following as a minimum:

a) a general description of each cause requiring action along with sufficient background information and detail, to ensure the need to address each cause is understood and actions to be taken can be identified;

b) a set of options for treatment actions and, where practicable, and within the scope, a summary of the benefits and costs of each;

c) recommended actions to address each of the causes identified.

Recommended corrective actions should be evaluated for effectiveness and realism. In general, corrective actions aim to achieve the following:

- change the likelihood of the focus event and/or its consequences (i.e. reduce the likelihood or consequence of undesirable events or increase the likelihood or consequence of successful events);
- not to introduce new unacceptable risks, e.g. the safety of other systems must not be degraded by the proposed corrective action.

Where actions are identified they should be reviewed prior to implementation to determine whether they have not only addressed the root causes, but also not introduced new unexpected consequences and will therefore function as intended. Also reoccurrence of the same or a similar event should be monitored in order to evaluate the effectiveness of actions taken.

6 Selection of techniques for analysing causes

6.1 General

Formal techniques have been devised to help analysts identify causal factors and eventually root causes. Analysis techniques may perform one or more of the following functions:

- organize data and provide structure to the analysis and identify where further evidence is needed;
- provide a visual display of the evidence relating to the focus event, for example the time sequence of events or causal chains;
- conduct statistical analysis of the data, particularly from multiple similar events, to identify common causal factors;
- provide guidance to identify possible causal factors for further investigation and comparison with data (such methods include check lists and methods based on models of causation);
- guide the analysts through the causal chain to a set of root causes.

6.2 Selection of analysis techniques

RCA is undertaken in varying degrees of depth and may use one or several analysis techniques ranging from simple to complex. The depth of the analysis and technique(s) used should exhibit the following characteristics:

- be justifiable and appropriate to the focus event under analysis and the scope and the purpose of the analysis;
- provide results that enhance the understanding of the root causes of the focus event;
- be capable of use in a manner that is traceable, repeatable and verifiable.

The analysis techniques to be used are selected based on the applicable factors such as

- characteristics of the analysis technique,
- characteristics of the focus event e.g. severity or potential severity or complexity,

- characteristics of the organization, e.g. industry/sector approved techniques or cost benefit evaluation,
- purpose of the analysis e.g. outputs required or stakeholder expectations,
- the causation model or models most appropriate to the objectives of the analysis.

The attributes of the most commonly used analysis techniques are described at Annex A. The criteria used to characterize the techniques, described in Annex A, are as follows:

- expertise required;
- tool support;
- scalability;
- graphical representation;
- modularity;
- reproducibility;
- plausibility checks;
- intellectual rigour;
- time sequence;
- specificity.

Detailed descriptions of the RCA techniques are described in Annex C, which includes the methods and process used for each technique along with their strengths and weaknesses.

6.3 Useful tools to assist RCA

Modern data mining techniques enable a search for specific properties and conditions. Clustering analysis selects data that are closely related, and thereby identify deviating data (outliers). Modern cluster analysis can detect data that are closely related in one, two or more dimensions and thereby analyse products or processes that are closely related and identify deviating data points (outliers). An overview of these techniques is provided in Annex D.

Many focus events and analysis techniques involve human factors and several taxonomies have been developed to assist in finding root causes where human behaviour is involved. Two examples are given in Annex E.

Annex A
(informative)

Summary and criteria of commonly used RCA techniques

A.1 General

Annex A lists the most commonly used RCA techniques, with a brief description, and provides a reference list of criteria which can be used to compare different RCA techniques. The list is not comprehensive but covers examples of the different types of techniques used.

A.2 RCA techniques

Table A.1 provides a list and brief description of the most commonly used RCA techniques.

Table A.1 – Brief description of RCA techniques

Technique	Description
Events and causal factors (ECF) charting	ECF analysis identifies the time sequence of a series of tasks and/or actions and the surrounding conditions leading to a focus event. These are displayed in a cause-effects diagram
Multilinear events sequencing (MES) and sequentially timed events plotting (STEP)	MES and STEP are methods of data-gathering and tracking for the analysis of complex focus events. The results are displayed as a time-actor matrix of events
The ‘why’ method	The ‘why’ method guides the analysis through the causal chain by asking the question why a number of times.
Causes tree method (CTM)	CTM is a systematic technique for analysing and graphically depicting the events and conditions that contributed to a focus event. CTM is similar to the 'why' method in concept, but builds a more complex tree and explicitly considers technical, organizational, human and environmental causes
Why-because analysis (WBA)	WBA establishes the network of causal factors responsible for a focus event using a two-factor comparison, the counterfactual test. The network of factors is displayed in a "why-because" graph
Fault tree and success tree method	Fault or success tree is a graphic display of information to aid the user in conducting a deductive analysis to determine critical paths to success or failure, which are displayed graphically in a logic tree diagram
Fishbone or Ishikawa diagram	The Fishbone or Ishikawa diagram is a technique that helps identify, analyse and present the possible causes of a focus event. The technique illustrates the relationship between the focus event and all the factors that may influence it
Safety through organizational learning (SOL)	SOL is a checklist-driven analysis tool, oriented towards focus events in nuclear power stations. Results are in the visual form of a time-actor diagram, derived from the MES/STEP method
Management oversight and risk tree (MORT)	The MORT chart is a pre-populated fault tree with events, usually faults or oversights, expressed in generic terms. The MORT tree contains two main branches and many sub-branches giving a high level of detail. One main branch identifies about 130 specific control factors while the other main branch identifies over 100 management system factors. The chart also contains a further 30 information system factors common to both main branches of the tree
AcciMaps	AcciMaps is primarily a technique for displaying the results of a causal analysis. It requires an organizational model to separate factors into layers and to elicit factors in the layers; applies a version of the counterfactual test (see WBA) to determine the causal relations amongst the factors
Tripod Beta	Tripod Beta is a tree diagram representation of the causal network, focusing on human factors and looking for failures in the organization that can cause human errors

Technique	Description
Causal analysis for systems theoretic accident model and process (STAMP) (CAST)	CAST is a technique that examines the entire socio-technical process involved in a focus event. CAST documents the dynamic process leading to the focus event including the socio-technical control structure as well as the constraints that were violated at each level of the control structure

A.3 Criteria

Table A.2 provides a list and describes the criteria used to characterize the RCA techniques listed in Table A.1. Each criterion has three levels indicated by a (+), (o) or a (–), where the different levels indicate the range.

The attributes for each RCA technique using the criteria in Table A.2 are shown in Table A.3.

Table A.2 – Summary of RCA technique criteria

Criteria	Description	Levels
Expertise required	Is the method targeted towards the "sophisticated user" (does it require use of techniques such as theorem proving which requires specific expertise)? Is it suitable for use by domain experts only?	• Intuitive, little training necessary (+) • Limited training required e.g. one day (o) • Considerable training effort necessary, e.g. one week (–)
Tool support	Is tool support necessary?	• Can be well applied without dedicated tool support (+) • Tool support not required but usually needed for effective application (o) • Tool support necessary, can be applied only with dedicated tool support (–)
Scalability	Is the method scalable? Can the method be used cost effectively for simple as well as complex focus events? Can a subset of the method be applied to small, or to less-significant focus events and the full capability applied to large, or to significant focus events? So the question of scalability asks whether the complexity of analysis using the method scales with the complexity of the focus event	• Scales well with complexity (+) • Limited scalability, considerable overhead with every application (o) • Not scalable, the full method has to be applied (–)
Graphical representation	What is the nature of the method's graphical representation? The motivating principle is that a picture is better than a thousand words. It is often more comprehensible to display results of an analysis method as an image, a graph, or other form of illustration, than as purely written text. The desirable properties of a graphical representation are • to display clearly the semantics of causality (including denotation of causal factors, and taxonomy of factors), • to be cognitively (relatively) easily evaluated by a single person, • ideally, a graphical representation could also display the history of the analysis	• Graphical representation with clearly defined semantics and cognitively easy to understand (+) • Graphical representation, but without semantics (o) • No graphical representation defined (–)

Criteria	Description	Levels
Reproducibility	Are the results of the method reproducible? Would different analysts obtain similar results for the same focus event?	• The results can be reproduced, differences are only observed on the representation of the results, wording etc. (+) • A significant amount of the results can be reproduced, but some differences will be observed (o) • The results will depend on the analyst's expertise (–)
Plausibility checks	Are there reasonable, quick plausibility checks on the results obtained which are independent of the tool? What ways are there of checking the "correctness" of the results? One example would be checklists	• There are plausibility checks for almost all aspects (+) • There are plausibility checks, e.g. checklists, but they do not necessarily cover all aspects (o) • There exist only limited means supporting plausibility checks (–)
Intellectual rigour	How rigorous is the method? Rigour has two relevant aspects: • Does the method have a rigorous meaning, formal semantics, for the key notions of causal factor and root cause? Are the semantics easy to apply? • Are the results of the method amenable to formal (mathematical) verification? To what extent is an application of the method so amenable?	• Formally defined and can be formally verified (+) • Semi-formal definition (o) • Informal definition (–)
Time sequence	Does the method contain a representation of time sequence of events?	• Yes (+) • Only indirectly (o) • No (–)
Specificity	The extent to which the method limits analysis to necessary causal factors of the focus event rather than exploring a range of general problems with the system that existed at the time of the focus event and may have contributed	• Method only analyses necessary causal factors of the focus event (+) • Method can be used to analyse contributory factors as well as necessary causal factors of the focus event (o) • Method seeks problems in general whether or not they were necessary causal factors of the focus event (–)

Table A.3 – Attributes of the generic RCA techniques

	Expertise required	Tool support	Scalability	Graphical representation	Reproducibility	Plausibility checks	Intellectual rigour	Time sequence	Specificity
ECF	o	o	o	+	o	o	o	+	+
MES and STEP	–	o	o	+	+	o	o	+	+
The 'Why' Method	+	+	–	o	–	–	–	–	+
CTM	o	o	+	+	o	o	o	–	+
WBA	o	+	o	+	+	+	+	o	+
Fault tree and success tree method	o	o	o	+	o	o	o	–	o
Fishbone or Ishikawa Diagram	+	+	–	o	–	o	–	–	o
SOL	o	–	+	o	+	+	o	+	o
MORT	+	–	–	o	+	o	o	–	–
AcciMaps	o	o	o	+	–	o	–	–	o
Tripod Beta	–	+	o	+	o	o	o	o	o
CAST	+	+	+	o	o	o	o	+	+

NOTE The criteria for each attribute are described in Table A.2.

Annex B
(informative)

RCA models

B.1 General

This annex describes the most commonly used RCA models which provide different ways of thinking about focus events. The different models are based on certain hypothesis with regard to the focus event, e.g. barrier analysis assumes the focus event has occurred as a result of missing, failed or ineffective barriers. Therefore, the different models tend to lead the investigator to identify different causal factors. Models are used to direct thinking in conjunction with the techniques of Annex C, or simply to identify a set of causal factors.

B.2 Barrier analysis

B.2.1 Overview

Barrier analysis is based on the hypothesis that a focus event occurs as a result of the interaction of a source of harm on a target and that this can be prevented by the use of barriers [3]. An undesirable event occurs when the barriers are missing, failed or ineffective (see Figure B.1).

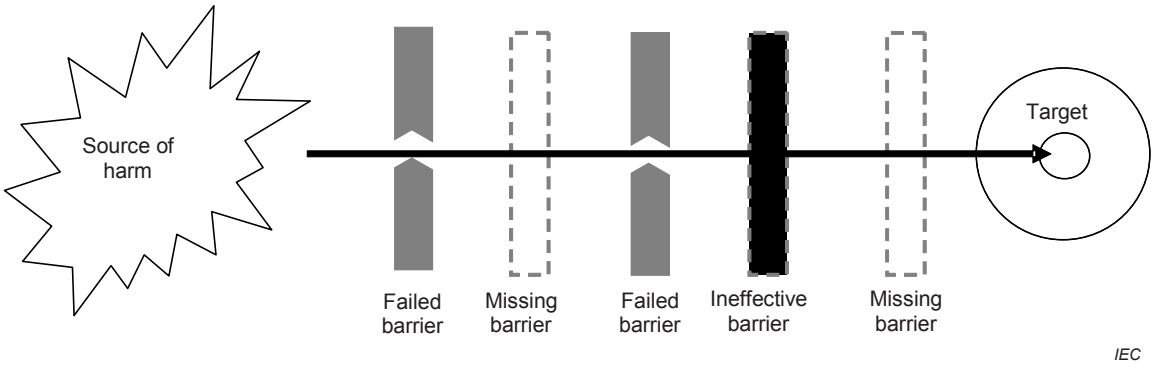


Figure B.1 – Broken, ineffective and missing barriers causing the focus event

Haddon [3] considered focus events where the source of harm is physical energy and barriers relate to how the energy can be modified or prevented from impinging on the target. The model has been extended in various ways [4], for example barriers are often divided into physical barriers and administrative barriers (see Table B.1 for some examples). Barriers may also be considered in terms of prevention, protection and detection (for example in the context where the focus event is a fire, these would be using non-flammable materials, providing fire extinguishers and installing smoke alarms).

The output of the analysis generally includes a barrier analysis worksheet (see Table B.2), which identifies those barriers that either were available but ineffective or were not in place during the occurrence of the focus event.

Table B.1 – Examples of barriers

Physical or energy barriers	Administrative barriers
Engineered safety features	Plant operating and maintenance procedures
Safety and relief devices	Regulations, policies and practices
Conservative design allowances	Training and education
Redundant equipment	Work protection
Locked doors and valves	Work permits
Ground fault protection devices	Skilled people
Shielding and guards	Methods of communication (3-way communication)
Alarms	Supervisory practices
Automatic fire containment systems	

Table B.2 – Example of the barrier analysis worksheet

Undesired outcome (what happened?) List one at a time, need not be in sequential order	**Source of harm**	**Barrier(s) that should have precluded the undesired event** List all physical and administrative barriers for each undesired outcome	**Barrier failure mechanism (how the barrier failed)**	**Barrier assessment (why the barrier(s) failed)** Identify if the barrier was missing, weak or ineffective; and why
Maintenance worker loosened nuts on flange of the pipe line that was pressurized	Pressurized liquid	Procedure to switch off pump and release pressure before commencing work	Pressure released on wrong system	Unclear labelling

B.2.2 Strengths and limitations

The strengths of barrier analysis are as follows:

- identifies what corrective actions are required to ensure adequate barriers (number and effectiveness) are in place.

The limitations of barrier analysis are as follows:

- may not recognize all failed or missing barriers, or the effect of the rate or frequency with which the barriers are challenged;
- addresses immediate causal factors rather than root causes, i.e. it seeks what barrier failed and how, but does not explore why in any depth.

B.3 Reason's model (Swiss cheese model)

B.3.1 Overview

Reason's model [5] is based on the premise that the basic required elements of any productive system are

- appropriate decisions from plant and corporate management,
- line management activities, operations-maintenance training, etc.,
- reliable and fit for use equipment,
- motivated workforce,

- integration of human and mechanical elements,
- safeguards against foreseeable risks.

There are inevitably weaknesses in these elements that can be considered to be latent failures. If these come together to form a triggering event, which may be unimportant in other circumstances, this results in failure.

The weaknesses in the elements of the productive system are pictured as holes in slices of Swiss cheese. An event will result when all individual weaknesses align. Reason's model is not strictly a barrier model as the layers are normal operating systems with weaknesses rather than failed barriers or controls.

Human error taxonomies based on Reason's model have been developed for a number of different industries.

B.3.2 Strengths and limitations

The strengths of Reason's model are as follows:

- encourages the analyst to explore causal factors of operator error and hence possible means of reducing it.

The limitations of Reason's model are as follows:

- superficial analysis of technical or environmental causal factors which considers technical aspects only in terms of failed barriers;
- assumes the core problem is operator error (errors at other levels and organizational failures are explored primarily in terms of how they influence operator error);
- does not supply a taxonomy to assist with the identification of motivations and psychological precursors of human error or in identification of latent failures and hence requires expertise in individual and organizational psychology to use properly.

B.4 Systems models

Systems theory [6] was developed in the 1940s and 1950s to handle the increase in complexity of systems after WWII and to consider the social and technical aspects of systems together as a whole.

In system models it is assumed that human interaction with technology in complex social structures is influenced by the organization's goals, policy and culture and by internal and external economic, legal, political and environmental elements. This system is stressed by the fast pace of technological change, by an increasingly aggressive, competitive environment, and by factors such as changing regulatory practices and public pressure. In this context focus events are due to multiple factors and are typically 'waiting for release' and not due to any one act or event.

Failures arise due to the complex interactions between system components that may lead to degradation of system performance. Two or more discrete events within system elements can interact in unexpected ways which designers could not have predicted and operators cannot comprehend or control without exhaustive modelling or test. Factors contributing to the focus event may include effects of decisions which are normal in the circumstances in which they were made, but produce an unwanted outcome.

Methods based on a systems model do not seek a causal chain or look for individual error or technical failures but consider the system as a whole, its interactions and its weaknesses. Individual human or hardware failures may be recognized but the focus is on interactions and systemic issues.

B.5 Systems theoretic accident model and processes (STAMP)

B.5.1 Overview

STAMP [7] is a causality model based on systems theory [6] that extends the traditional model (chains of directly related failure events) to include both the technical and social contributors to focus events and their relationships. It also captures focus events involving interactions among non-failing system components and processes, indirect and systemic causal mechanisms, complex operator and managerial decision making, advanced technology such as digital systems and software and system design flaws.

STAMP assumes incidents arise from interactions among humans, machines and the environment; it treats systems as dynamic control problems in which the controls aim to manage the interactions among the system components and its environment. The goal of the control is to enforce constraints on the behaviour of the system components, for example, aircraft in an air traffic control system have to always maintain a minimum separation distance. Focus events result from inadequate control or enforcement of constraints on the development, design and operation of the system. In the space shuttle "Challenger" loss, for example, the O-rings did not control propellant gas release through the field joint of the space shuttle. In STAMP, the cause of a focus event is a flawed control structure.

STAMP also incorporates the concept that incidents often arise from a slow migration of the whole system toward a state of high risk [8] so that financial and other pressures that lead to changing behaviour over time can be accounted for in the causal analysis process.

B.5.2 Strengths and limitations

The strengths of STAMP are as follows:

- considers the role of the entire socio-technical system in causation;
- includes indirect and systemic factors in the causal explanation;
- provides a model to explain accidents in very complex systems;
- identifies the causes back to the process with which a system was developed.

The limitations of STAMP are as follows:

- requires focus events to be analysed in a way that is often unfamiliar to engineers, therefore may take more time to learn how to analyse focus events using causal analysis processes based on STAMP.

Annex C
(informative)

Detailed description of RCA techniques

C.1 General

Annex C describes a range of techniques used during a RCA. The list is not comprehensive but covers examples of the different types of techniques used. Many of these techniques are supported by software tools. Some of the methodologies and software tools have elements that are proprietary, which may impact on the cost of implementing the technique.

Some techniques aim to identify causal factors that can be shown to be necessary if the focus event is to occur. Other methods seek general weaknesses of the system as a whole that probably contributed to the focus event but where the focus event could have occurred in their absence. In some terminologies a “causal factor” cannot be so described unless it is necessary to the focus event. In this annex such causal factors are referred to as “necessary causal factors”. Identified weaknesses that may have played a part in the focus event but may not be necessary to it are referred to as “contributory factors”.

In general, identification of necessary causal factors will be repeatable and based on evidence. There may be a higher level of subjectivity in identifying contributory factors and different analysis techniques with a different focus may identify different factors.

C.2 Events and causal factors (ECF) charting

C.2.1 Overview

The ECF chart [9] records events in chronological order from left to right in rectangles, with events characterized by single subjects and active verbs. Each event is derived strictly from the one before. Conditions necessary for the events are displayed in ovals above and below the sequence of events (conditions are states or circumstances rather than happenings). Events are connected by solid lines and conditions by dashed lines. Events and conditions based on evidence have a solid outline, whereas those that are presumptive have a dashed outline. There may be multiple or branching sequences of events, each with their own conditions.

Figure C.1 illustrates an example of an ECF chart in which a maintenance activity was incorrectly carried out due to the maintainer turning up late, resulting in an emergency landing carried out by an aircraft.

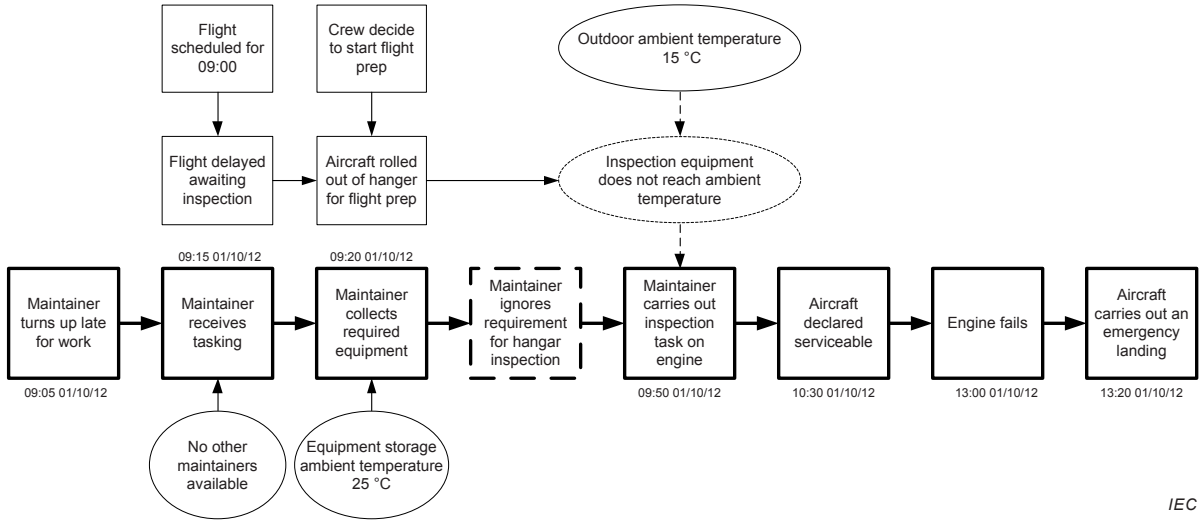


Figure C.1 – Example of an ECF chart

C.2.2 Process

The following describes the process for developing an ECF chart:

a) Identify the focus event and record it in a box on the right hand side.

b) Record the primary chain of events that led to the focus event where each event in the chain is both immediate and necessary to the event on the right hand side. Therefore, the consequence is recorded on the right hand side of each event (causal factor). Also, the consequence of a previous event may be the causal factor of the next event. The events are displayed in rectangles linked by arrows to the right of the focus event.

c) Determine what conditions led to these events. State each of them in an oval above the relevant event.

d) Add any secondary chains of events that may be relevant to the focus event and their conditions.

e) Check the validity of the causal factors by obtaining evidence that determines whether the conditions and events are true.

f) Develop the ECF chart until the event at the start of the sequence is identified and all conditions which can be verified by evidence are added.

In general, the exact chronology of events is not known at the beginning of the investigation but becomes clearer as the investigation proceeds. A method should therefore be used that allows investigators to easily change the sequence of events and conditions as more information is gained.

C.2.3 Strengths and limitations

The strengths of ECF are as follows:

- assists the verification of causal chains and event sequences;
- provides a structure for collecting, organizing and integrating evidence;
- identifies information gaps;
- assists communication by providing an effective visual aid that summarizes key information regarding the focus event and its causes.

The limitations of ECF are as follows:

- identifies some causal factors but may not necessarily determine the root causes;

- can be overcomplicated for simple problems.

C.3 Multilinear events sequencing (MES) and sequentially timed events plotting (STEP)

C.3.1 Overview

MES [10] and STEP [11] are methods developed to analyse focus events in complex systems, where STEP is a successor to MES.

As with ECF charting, MES/STEP conceives a focus event as arising from an interlinked succession of events with events characterized by a single subject and an active verb. In MES and STEP, the subject is called an actor (which may be a human, a machine or even a property).

Events are represented as event building blocks (BBs), which consist of (partial or full) data records as described in Figure C.2. These are arranged during the analysis in a time-actor matrix where the vertical axis of the matrix represents the different actors, and the horizontal axis represents time.

The time-actor matrix also contains:

- conditions necessary for enabling an event along with precursor events;
- annotations for further tasks in an investigation, such as a note indicating a deficit of information, or an incomplete explanation of an event.

An example showing part of the representation of a tank maintenance event is given in Figure C.3.

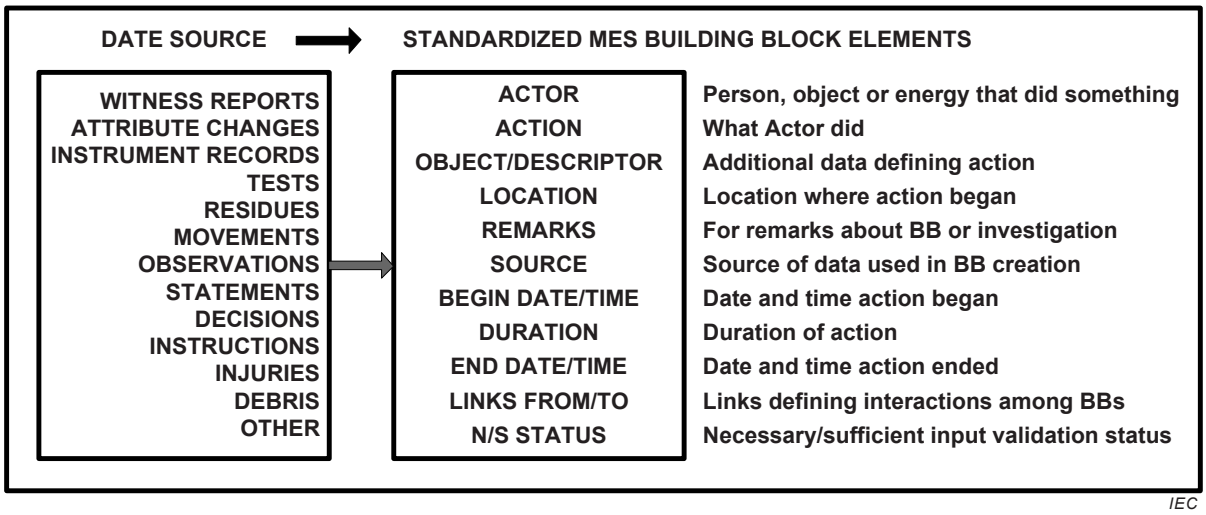


Figure C.2 – Data in an event building block

C.3.2 Process

MES/STEP has the following steps:

a) Gather information for the initial series of building blocks, and identify and track missing information.

b) Arrange the initial building blocks in an initial time-actor matrix.

c) Identify and generate hypotheses to "fill" the gaps with events (in the form of further building blocks).

d) Terminate the process when an analyst considers that sufficient information is available in the time-actor matrix.

C.3.3 Strengths and limitations

MES/STEP has the same strengths and limitations as ECF. Data formatting is relatively more elaborate, and there are explicit mechanisms for determining and tracking missing data and attempts to determine those data. Some such “bookkeeping” mechanisms are necessary for managing complex investigations with multiple investigators. The time-actor matrix also has explicit notation for recording the state of an on-going inquiry along with data-acquisition and explanatory tasks yet to be performed. This means that a comprehensible visual representation of the state of an investigation is available at all points in an investigation.

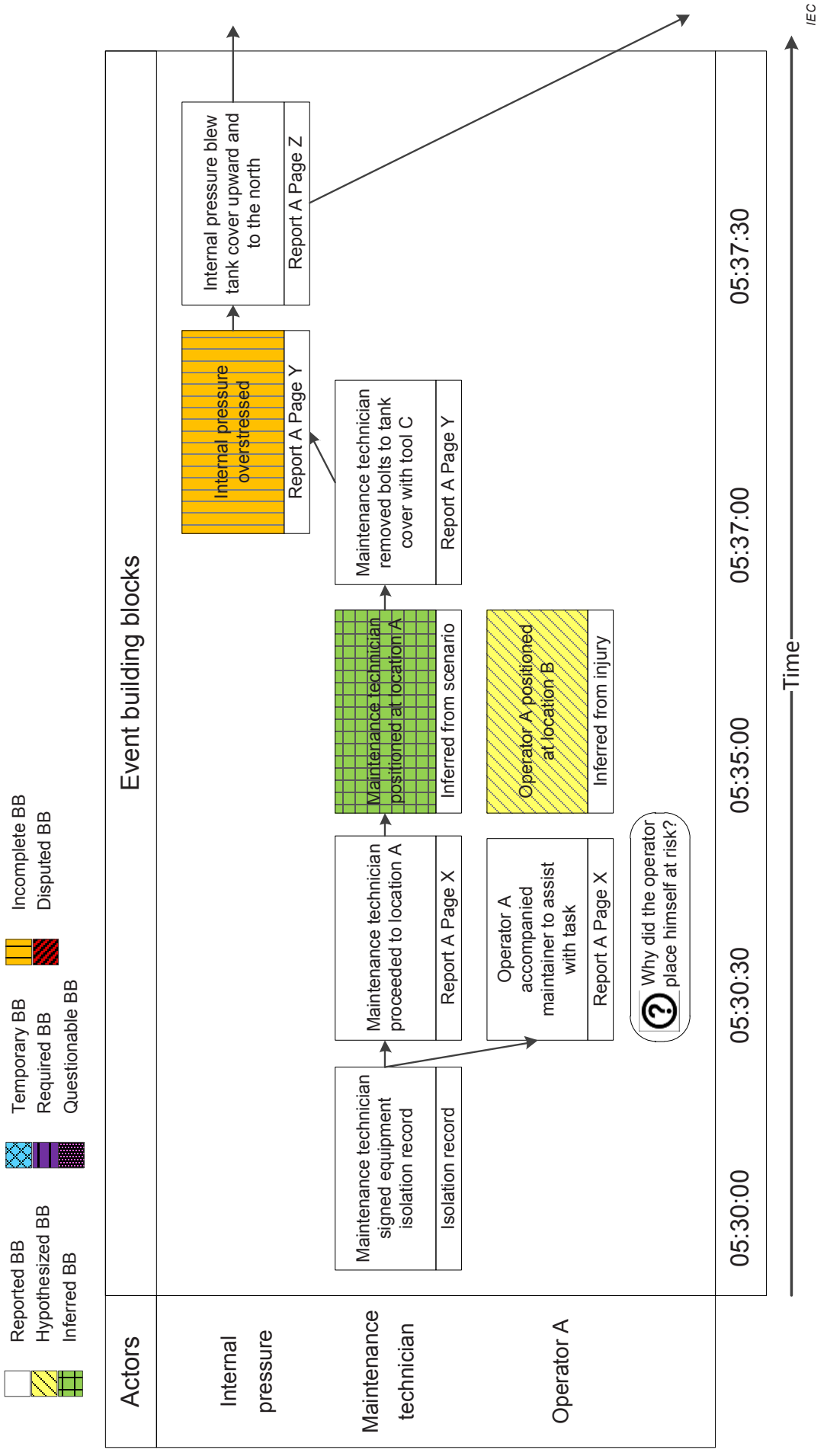


Figure C.3 – Example of a time-actor matrix

C.4 The ‘why’ method

C.4.1 Overview

The ‘why’ method uses a straightforward questioning process to arrive at the root causes.

Questioning starts with a statement of the situation and asks why it occurred. The answer to this question is turned into a second why question and the answer to this into a third question. Questioning ceases when the stopping rule is reached. Generally this requires approximately 5 levels of questions hence the method is sometimes known as the 5 whys.

Where a why question provides several causal factors, each is explored and the method produces a why tree.

The why method is used alone for simple situations but is also inherent in more complex tree methods such as the causes tree method (CTM) (see Clause C.5). It can be useful for eliciting information from witnesses on how and why an event occurred because the simple question ‘why’ does not make assumptions about cause or lead the witness.

Figure C.4 illustrates an example of a compressor that has experienced an unscheduled shutdown. In the example the fourth why suggested a number of potential causal factors for lack of lubrication and evidence was sought to define which in fact occurred. Although a human error was involved in that a person did not follow specified start up procedures, the recommendation is to improve the design so the compressor and pump motors are linked. Further analysis of why the error occurred, in this case, is not useful.

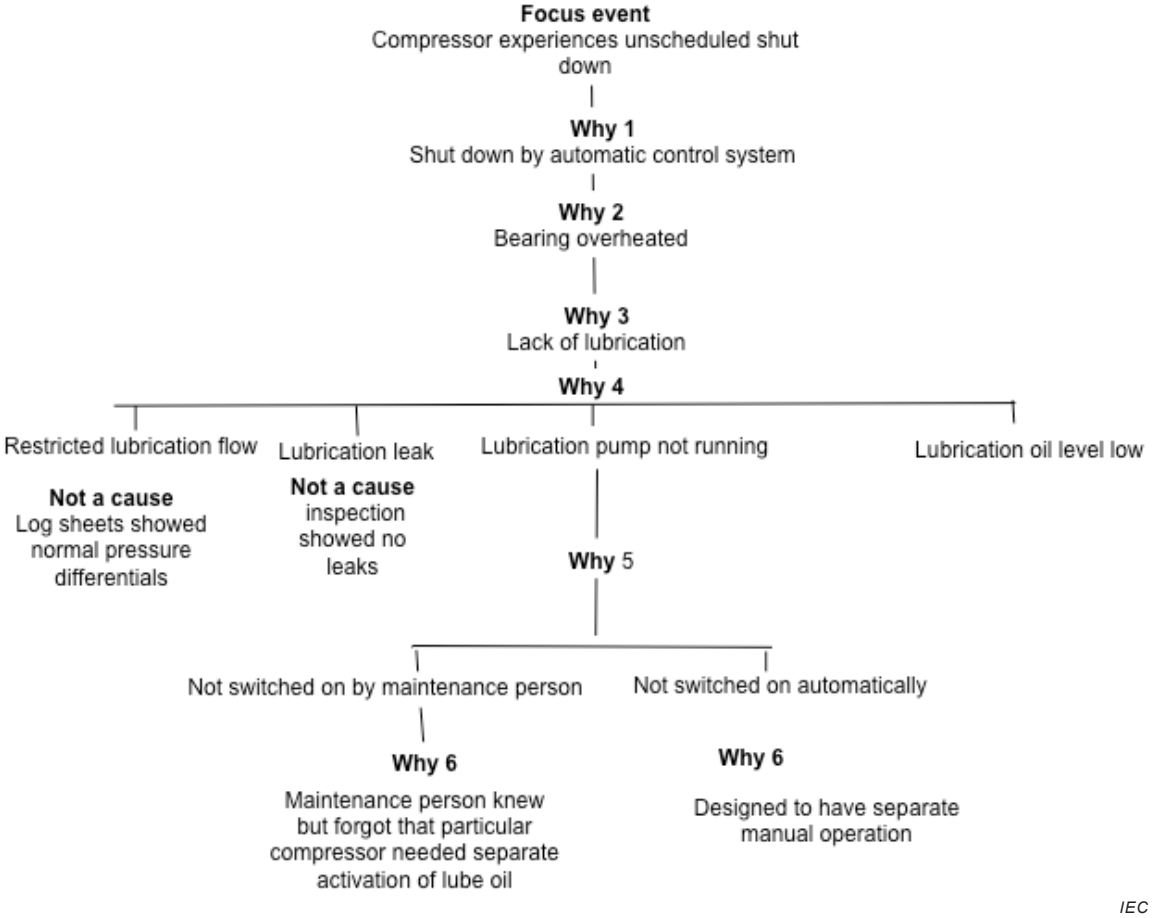


Figure C.4 – Example of a why tree

C.4.2 Process

The ‘why’ method has the following steps:

- Identify and record the focus event as the start of a 'why' diagram.
- Ask why the focus event occurred, seeking only the immediate causal factors.
- Ask “why” successively with respect to the previous answer. In each case the answer to the question "why" should be an immediate causal factor of the previous answer.

The question ‘why’ is asked as many times as is needed to lead to a root cause, which is normally five questions but this is only a guideline. Each time the question is asked, there may be multiple answers and some analysis will be needed to eliminate those possible answers that are not applicable. It may be more effective to ask ‘why did the process fail?’ instead of just asking ‘why’?

It can be useful to consider a set of categories of cause such as from the Ishakawa method and to involve a team of people. This will help ensure that all relevant areas are considered by the investigators.

C.4.3 Strengths and limitations

The strengths of the ‘why’ method are as follows:

- simple to apply by those involved in the problem;
- easy to understand by others;
- quick process to achieve results for simple problems;
- does not require extensive knowledge from the person asking the questions;
- does not require a lot of training from the person asking the questions.

The limitations of the ‘why’ method are as follows:

- only suitable for simple situations;
- heavily dependent on the knowledge and expertise of the people answering the questions, with expertise in both technical failure modes and human error often required to reach the root causes;
- root causes are likely to be missed if outside the knowledge base of those involved;
- possible uncertainty about when the appropriate root causes have been identified;
- can be developed to the level where reasons for people’s actions are being considered, where evidence is often not available and results are therefore not always repeatable.

C.5 Causes tree method (CTM)

C.5.1 Overview

CTM [12] is a systematic technique for analysing and graphically depicting the events and conditions that contributed to a focus event.

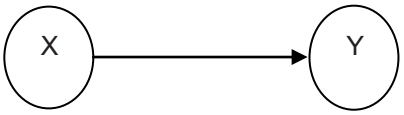
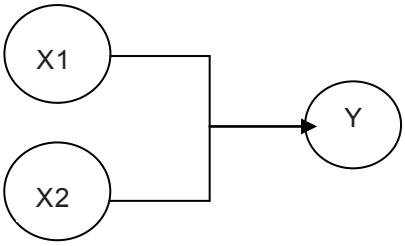
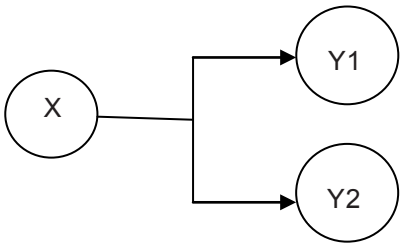
The method examines all the system components associated with the focus event. The investigation starts by establishing the tangible facts, taking care, in this phase, not to interpret them or to express an opinion about them.

CTM is similar to the why method in concept but builds a more complex tree and explicitly considers technical, organizational, human and environmental causal factors. Each antecedent (identified causal factor) is tested to check it is an immediate and necessary causal factor of the previous one, whereas the why method is less rigorous. Therefore, CTM is suitable for more complex situations.

CTM is also similar to a fault tree but, whereas a fault tree is used prior to an event to explore all possible causal factors and strict logic relationship(s) between faults are specified, the cause tree includes only those causal factors which apply to a specific event that has already occurred and does not develop the logical relationships in detail.

A cause tree may be used to explore successes as well as failures.

The cause tree forms a network of the causes which have directly or indirectly caused the focus event, using the three logical relations shown in Figure C.5.

Sequence: A cause (Y) has a single direct origin (X). i.e. (X) was necessary and sufficient for (Y) to occur	
Conjunction: A cause (Y) has several direct origins (X1) and (X2). That means, each of the direct origins (X1) and (X2) was necessary for (Y) to occur	
Disjunction or separation: Two or more causes (Y1;Y2, ...) have a single and identical direct origin (X). That means (X) was necessary for (Y1) and (Y2) to be produced.	

IEC

Figure C.5 – Symbols and links used in CTM

Figure C.6 shows an example tree, in which Mr L (the victim) and Mr A are working nights, as an exception, to store a surplus of stock. In accordance with the handbook, Mr L and Mr A were required to load the crusher with "flour" which is then bagged and stored. Normally this activity is under the responsibility of a head of team whose presence had not been considered essential by the management for this night. Of his own initiative to save time, Mr L took a forklift truck (the ignition key had remained on the dashboard as usual) to store the bags. At the end of the task, Mr L set about returning the forklift truck. Mr L carried out a sharp bend in reverse, forks raised, and while seeking to avoid a hole on the ground the forklift tipped over, crushing Mr L between the ground and the right safety upright of the truck.

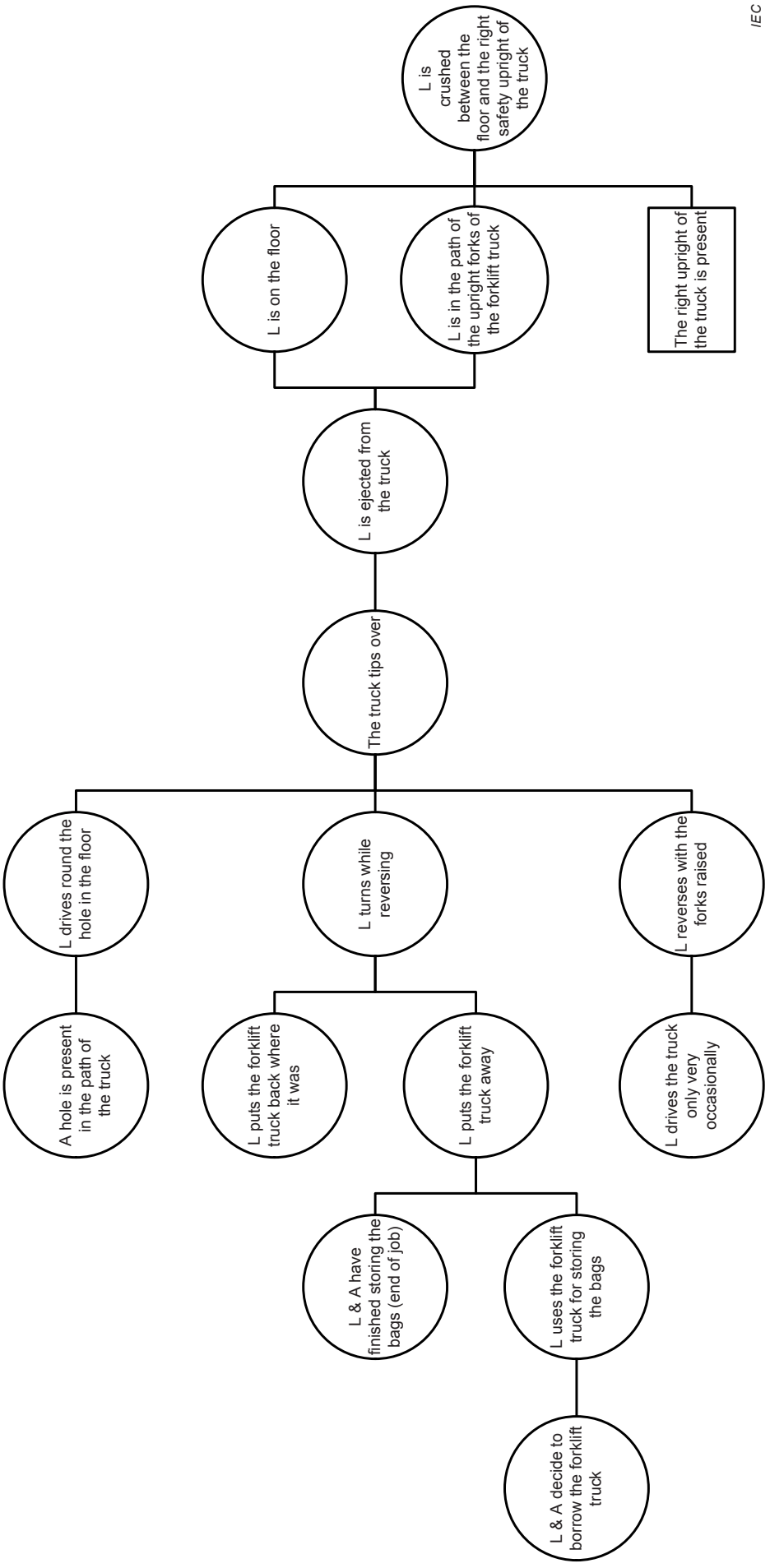


Figure C.6 – Example of a cause tree

C.5.2 Process

CTM has the following steps:

a) Identify the focus event to be analysed and record it as the starting point for the tree.

b) Collect and record all relevant data including people, their activities and actions, materials and equipment and factors relating to the physical and psychosocial environment.

c) Make a list of the causal factors to the focus event. These should be supported by evidence and be expressed as precisely as possible. Subjective opinions and judgements are not included. Causal factors include those which are unusual or change the normal course of events and those which are normal but played an active part in the occurrence of the event.

d) Work backwards towards the root causes by asking the following questions systematically for each antecedent that has been gathered:

   1) what antecedent X has directly caused the antecedent Y?;

   2) was X in itself necessary to give rise to Y?;

   3) If not, what are the other antecedents (X1, X2...) that were equally necessary in order to give rise directly to Y?

e) Display these immediate necessary causal factors in a box linked by an arrow to the focus event. The tree may be drawn horizontally or vertically but is normally drawn horizontally starting from the right, so that left to right corresponds to the chronology of events.

f) Continue asking the same questions with respect to each necessary causal factor found until the team agrees that there is no value in continuing further.

g) Check the validity of the tree by obtaining further evidence that determines whether it is true.

C.5.3 Strengths and limitations

The strengths of CTM are as follows:

- provides a method for structuring investigation of complex events;
- facilitates easy to read format;
- can be used to encourage group participation;
- identifies areas for collecting data as the investigation proceeds;
- can be used to analyse success or failure events;
- can be used for technical and non-technical events.

The limitations of CTM are as follows:

- many human and organizational factors may contribute to the occurrence of the focus event and it is often difficult to establish which in a particular instance were the necessary causal factors;
- there is no guidance on how to seek causal factors; therefore, expertise in human error and organizational systems is needed when the tree involves human and organizational failures, where evidence is often difficult to obtain;
- it is difficult to apply when an event occurs as a result in a change of quality in several areas, where no single causal factor is a necessary causal factor.

C.6 Why-because analysis (WBA)

C.6.1 Overview

WBA [13] is a causal-analytical technique for establishing which of a given collection of events and situations are necessary causal factors. Given two events or situations, A and B

say, a condition called the counterfactual test (CT) is used to establish whether A is a necessary causal factor of B. Suppose two events or situations A and B have been observed. The CT asks whether, had A not occurred, B would also not have occurred. (Since A did occur, a supposition that A had not occurred is contrary to fact, hence the word "counterfactual".) In asking this question, all other conditions are assumed to have remained the same. If the answer is yes: B would not have occurred then A is a necessary causal factor of B. If the answer is no: B could have happened anyway even if A had not happened (the CT fails) then A is not a necessary causal factor of B.

The network of causal factors is displayed as a Why-because graph (WBG), a collection of "nodes", boxes, diamonds and other shapes, containing a brief description of the fact, joined by "edges", or arrows, where the node at the tail of an arrow is a necessary causal factor of the node at its head, as determined by the CT.

A WBA is acyclic (contains no loops), so is usually drawn with arrows pointing in the generally upwards direction, as shown in Figure C.7, or horizontally with arrows pointing generally left-to-right, or right-to-left.

In order to determine whether sufficient causal factors are present in the collection of events and situations presented, the causal completeness test (CCT) is used. The CCT is applied to a given event or situation and its collection of necessary causal factors as determined by the CT. If the CCT is not passed, then the collection of events and situations has to be extended by further factors until it is passed. Suppose A_1, A_2,...,A_n have been determined to be necessary causal factors of B by the CT. Then the CCT is deemed to be passed if, had B not occurred, one of A_1, A_2,...,A_n would not have occurred either (formally, NOT-B is a necessary causal factor of NOT(A_1 AND A_2 AND...AND A_n) as determined by the CT).

When a WBG has been constructed and the CCT is passed for all the events and situations therein, then the WBG is complete and is deemed to represent a sufficient causal explanation of the focus event.

Figure C.7 illustrates an example of a WBG for a commercial-aviation runway-overrun accident.

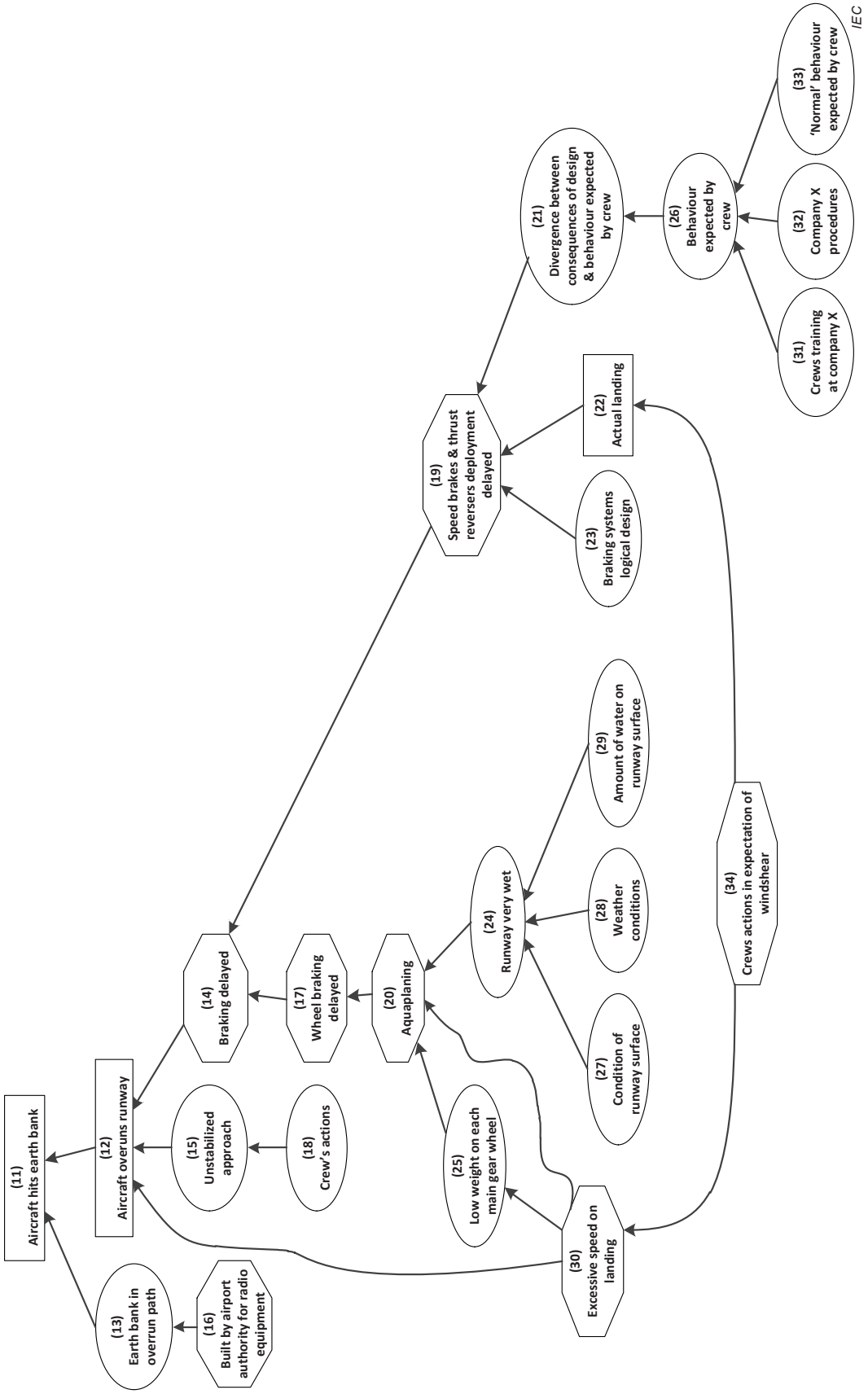


Figure C.7 – Example of a WBG

C.6.2 Process

WBA has the following steps:

a) Determine a collection of facts deemed to be relevant, under guidance of a stopping rule. This gives an initial collection C of facts, divided into events, states and situations.

b) Select the focus event (called in WBA the accident event).

c) Determine intuitively the immediate necessary causal factors of the focus event from amongst the collection C; check using the CT. Display the results visually as a partial WBG.

d) Determine intuitively the necessary causal factors of those immediate factors; check using the CT. Extend the WBG with these factors.

e) Proceed to fill out the analysis (to extend the WBG) by testing each fact in C against the factors already in the WBG.

f) Apply the CCT to determine whether the WBG is complete, or whether factors are missing from the collection C.

g) Extend C if necessary; incorporate the new facts into the WBG using the CT. If insufficient information is available, assumptions may be included, providing they are clearly labelled as such.

h) Finish when the CCT shows sufficient causal factors for each fact, in conformity with the stopping rule. If insufficient facts are available, assumptions have to be included in order to allow the CCT to succeed, but clearly labelled as such.

C.6.3 Strengths and limitations

The strengths of WBA are as follows:

- may be performed with a minimum of training (with the use of suitable tools that provide help on extracting facts from narrative descriptions, an inexperienced analyst can typically perform a first pass WBA inside two hours);
- the analysis results are easily understandable by third parties;
- the conceptual background required to perform a WBA is limited (an analyst must be able to apply the CT, and then the CCT);
- any network of causally-related phenomena may be analysed with a WBA;
- the reasoning behind a WBA may be formally checked using a formal logic;
- can be used together with other methods, e.g. those providing more structure to the collection of facts.

The limitations of WBA are as follows:

- the method provides no guidance on the collection of facts to which the tests are applied e.g. there is no structuring of facts into categories such as technical, procedural, human-factors, organizational and legal;
- because facts are not structured, WBA provides limited guidance on corrective action in the case where recurrence needs to be prevented.

C.7 Fault tree and success tree method

C.7.1 Overview

A fault tree [14] displays the immediate necessary causal factors of a focus event, their causal predecessors and the logic relationships between them. Fault tree analysis (FTA) [15] is normally used as a priori method of identifying and analysing potential failure modes, particularly of equipment. The fault tree diagram can be used in RCA by building a tree following the same logic but including in the tree only those events which actually occurred.

OR gates may be used during the analysis to describe alternative causal factors that need to be evaluated, but when all facts are clearly established only AND gates should remain, unless the purpose of the investigation is to prevent other related events. Therefore, as the investigation proceeds, potential causal factors that do not fit the evidence are gradually ruled out and removed from the tree. By closing out each branch of the tree, the causal factors of the focus event become apparent.

Strictly a fault tree represents binary events where a statement is true or false, e.g. a component failed or not. In RCA, the fault tree structure is often applied to a tree of causal factors where the logic rules are not strictly obeyed and changes in quality are included as well as binary events.

A similar logic can be applied where the focus event is a success. In this case the tree is referred to as a success tree.

Figure C.8 shows an example of a fault tree.

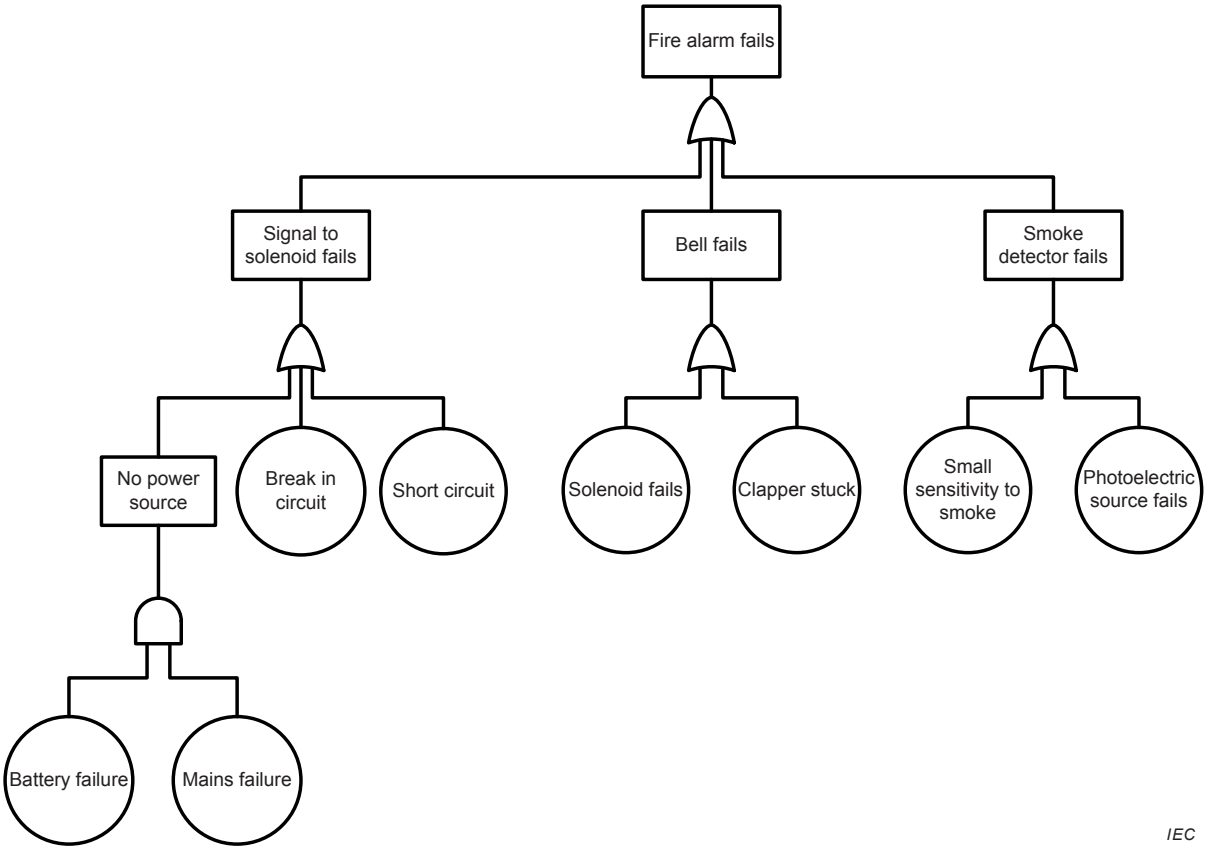


Figure C.8 – Example of a fault tree during the analysis

C.7.2 Process

The process for developing a fault/success tree is as follows:

a) Define the focus event to be analysed and record it as the starting point for the tree.

b) Establish the immediate necessary causal factors of the focus event and display them in a box linked by an arrow to the focus event. The tree may be drawn horizontally or vertically. These are the first level causal factors of the focus event.

c) Establish the logic relationships between the immediate causal factors using AND and OR Gates. The events at inputs of an AND gate have to be both necessary and sufficient to

cause the event above. OR gates may be used during the analysis to describe potential causal factors that require investigation.

d) Examine each causal factor to decide whether it is a root cause or the result of underlying causal factors.

e) Validate potential causal factors and update the tree accordingly.

f) Continue down the tree until the stopping rule is reached.

When the tree is developed, the possibility of causal factors relating to people, equipment and the environment is considered for each causal factor at each level. These should not be separated out at the top of the tree.

C.7.3 Strengths and limitations

The strengths of the fault/success tree method are as follows:

- provides a method for dividing up the analysis for large complex focus events;
- supported by many commercial software packages which assist in the development of the fault tree structure;
- encourages group participation;
- uses an orderly, easy-to-read format;
- identifies areas for collecting data.

The limitations of the fault/success tree method are as following:

- requires an experienced practitioner;
- has no underlying model of causation and provides no guidance on how to seek causal factors;
- does not easily represent situations where an event occurs as a result of a general changing of quality that affects for example adherence to procedures or tolerances of physical components.

C.8 Fishbone or Ishikawa diagram

C.8.1 Overview

The Fishbone or Ishikawa diagram [16] is a technique that helps identify, analyse and present the possible causes of a focus event. It may be used to structure a brainstorming session and to suggest ideas where further evidence may be sought. The technique was invented by Kaoru Ishikawa and graphically illustrates the relationship between an event and all the factors that influence it. This technique is also referred to as a "fishbone diagram" because of its appearance.

Figure C.9 shows an example of a Fishbone or Ishikawa diagram.

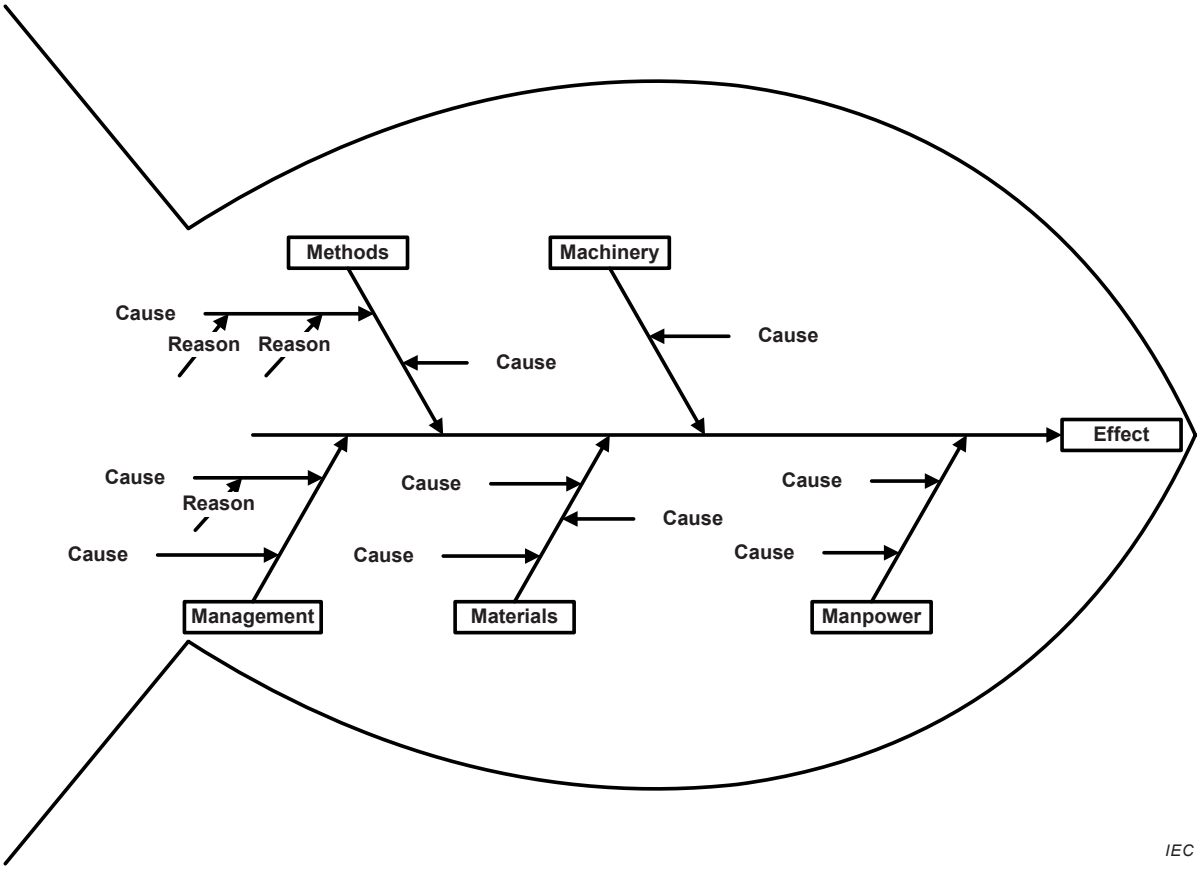


Figure C.9 – Example of a Fishbone diagram

C.8.2 Process

The process for developing a Fishbone or Ishikawa diagram is as follows:

a) Identify the focus event and record it on the right hand side and draw a line horizontally from it. This forms the head and spine of a fish.

b) Establish the main categories of causes to be considered and draw lines off the spine to represent each category. Categories commonly used include:

   1) 5Ms: methods, machinery, management, materials, manpower;

   2) 4Ps: place, procedures, people, policies;

   3) 4Ss: surroundings, suppliers, systems, skills.

c) For each category identify the possible causal factors of the focus event. These are presented as smaller lines coming off the 'bones' of the fish. Increasingly more detailed levels of causal factors can be shown as sub-branches coming off each cause line. It may be necessary to break the diagram into smaller diagrams if one branch has too many sub-branches.

d) Analyse the diagram: The diagram now shows all the possible causal factors of the focus event. The final step is to investigate the most likely causal factors which tests whether the analysis is correct. Analysis includes:

   1) reviewing the “balance” of the diagram, checking for comparable levels of detail to identify the need for further identification of causal factors;

   2) identifying causal factors that appear repeatedly as these may represent root causes;

   3) assessing what can be measured in each cause in order to quantify the effects of any changes made;

   4) highlighting the causal factors whose action can be taken.

C.8.3 Strengths and limitations

The strengths of the Fishbone or Ishikawa diagram are as follows:

- encourages group participation to identify people's perceptions of causal factors;
- seeks causal factors under a set of categories, so will identify a range of causal factors relating to human and organizational factors as well as hardware and procedural factors;
- uses an orderly, easy-to-read format;
- indicates possible causal factors of variation;
- can be used for simple investigations or as part of a more complex investigation.

The limitations of the Fishbone or Ishikawa diagram are as follows:

- there is no underlying model or theory of causation, so the causal factors identified are based on the team's perceptions.

C.9 Safety through organizational learning (SOL)

C.9.1 Overview

SOL [17] is an event analysis technique, which seeks weaknesses in the complex socio-technical system in which the event occurred. The purpose of SOL is to provide a model of the system and identify its weaknesses so it can be improved and recurrence of the focus event prevented. The emphasis is on organizational learning.

C.9.2 Process

SOL has the following steps:

1) Describe the situation using a time-actor matrix produced by MES/STEP (see Clause C.3).
2) Identify causal factors (which may be direct or indirect see Table C.1) for each event in the time-actor matrix, guided by checklists of questions derived from the experience and research of SOL authors. Direct causal factors are those that immediately resulted in the focus event, indirect causal factors appear further down the causal chain but may involve the same issues.
3) Classify causal factors into technology, individuals, working group, organization, and organizational environment.

Table C.1 – Direct and indirect causal factors

Direct causal factors	Indirect causal factors
Information	Information
Communication	Communication
Working conditions	Working conditions
Personal performance	Personal performance
Violations	Violations
Technical components	Scheduling
	Responsibility
	Control and supervision
	Group influence
	Rules, procedures and documents
	Qualifications
	Training
	Organization and management
	Safety principles
	Quality management
	Maintenance
	Regulatory and consulting bodies
	Environmental influences

C.9.3 Strengths and limitations

The strengths of SOL are as follows:

- the check list format allows users who are not specialists in organizational systems or organizational psychology to produce useful analyses;
- the emphasis on causal factors rather than necessary causal factors allows more factors to be brought into consideration than a narrowly causal analysis might do, and thereby offers more chance of identifying possible improvements;
- the format of the event building blocks gives less scope to the judgement of individual analysts and helps to give uniformity to SOL analyses;
- the stopping rule is implicitly defined by the checklist questions: when these have been answered, the information is deemed to be adequate.

The limitations of SOL are as follows:

- there is no specific notion of what is a causal factor other than what is implicit in the checklist questions;
- the level of detail is driven by the predetermined checklist of questions rather than the perceived need;
- the check list of questions was derived from research in the nuclear power industry and may be less suitable for other industries.

C.10 Management oversight and risk tree (MORT)

C.10.1 Overview

MORT [18] was first developed for analysing the root causes and causal factors for incidents in the nuclear power and aviation industries in the USA, but now has been applied in many industries.

MORT is a pre-populated tree based on a model of an organization's management system, which effectively provides a detailed check list for reviewing which parts of management and control systems were less than adequate when the focus event occurred. The basic structure of the tree is shown in Figure C.10.

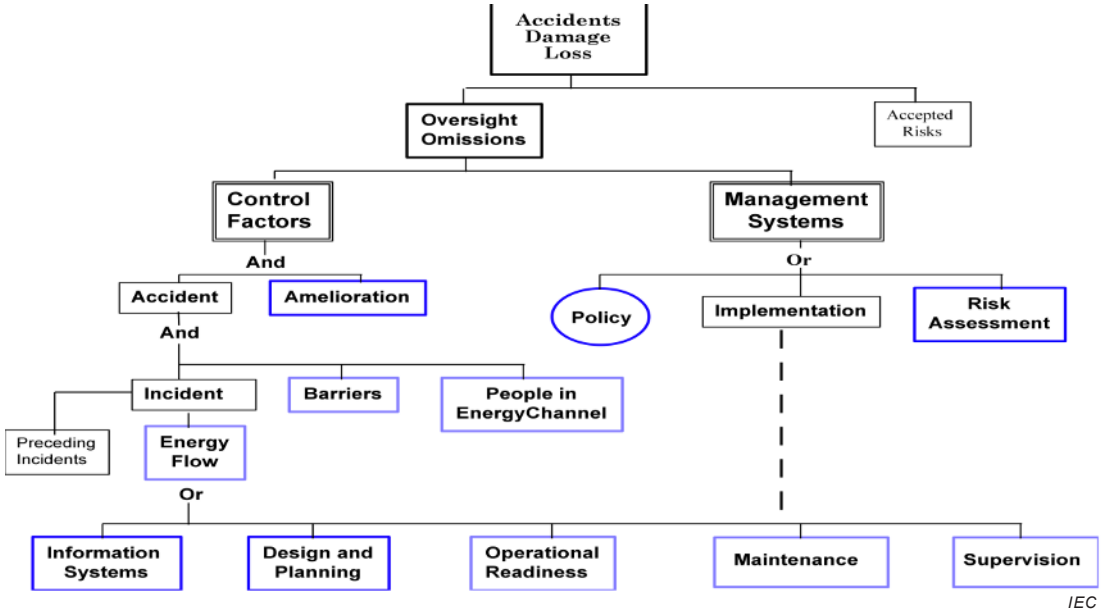


Figure C.10 – Example of a MORT diagram

MORT assumes that a failure occurs as a result of oversights or omissions in either management systems or the specific control factors which should have prevented the focus event from occurring.

Ultimately, failures in either branch in the tree occur because something within the general management systems (information systems, design and planning, operational readiness, maintenance or supervision) was less than adequate. Each box in Figure C.10 is developed into a detailed tree structure showing factors that might have been less than adequate.

C.10.2 Process

Start with the focus event and then work down the MORT tree in a logical manner asking and responding to pre-questions in the MORT manual. Symbols on the MORT chart are colour coded to indicate:

- there is no problem with an element (adequate);
- the element is giving rise to a problem (less than adequate);
- there is need for further enquiries.

C.10.3 Strengths and limitations

The strengths of MORT are as follows:

- provides comprehensive guidance for seeking all possible aspects of the system that were not adequate at the time of the focus event;
- less specialist expertise is needed than in some techniques because detailed guidance is provided on possible causal factors;
- identifies weaknesses in the system which might apply across a wide range of failure scenarios.

The limitations of MORT are as follows:

- explores weaknesses in the system in general that might have played a role in the focus event rather than seeking immediate or necessary causal factors;
- a very large number of questions (around 1 500) are asked, so the method is time consuming and hence most appropriate for serious events;
- unless the organization to which it is applied is a high reliability organization a very large number of weaknesses are found which make it difficult to implement changes;
- tedious when first learning or applying the method.

C.11 AcciMaps

C.11.1 Overview

AcciMaps [19] is based on concepts of causation published by Rasmussen and Svedung [20] and the organizational systems model (see Clause B.4).

AcciMaps is a graphical representation used to structure the analysis of a focus event and to identify the interactions in the socio-technical system in which the focus event occurred. It is a method designed to reveal the system wide failures, decisions and actions involved in a focus event. These are arranged in layers representing the different levels in a socio-technical system from government down to the equipment and surroundings involved. It also looks at the individual actors at each level and their decision-making routines and competence.

An example AcciMap for a gas explosion, showing typical system levels, is given in Figure C.11. The bottom level represents the physical arrangement of the scene of the focus event (buildings, equipment, surroundings, etc.). The next level up is the sequence of events leading to the focus event, including the failures, actions and decisions (including normal actions and decisions) that played a part. The higher levels show decisions and actions at each level that influenced, or could have influenced, the sequence of events at the lower levels.

C.11.2 Process

An AcciMaps is developed as follows:

a) Define a model of the system with different organizational levels.
b) Populate the levels (using boxes (nodes)) with the decisions and actions relevant to the focus event, the conditions that lead to them and their consequences.
c) Draw arrows that show all linkages and influences.
d) A process such as WBA may be added to ascertain which of the identified issues were necessary causal factors of the focus event.

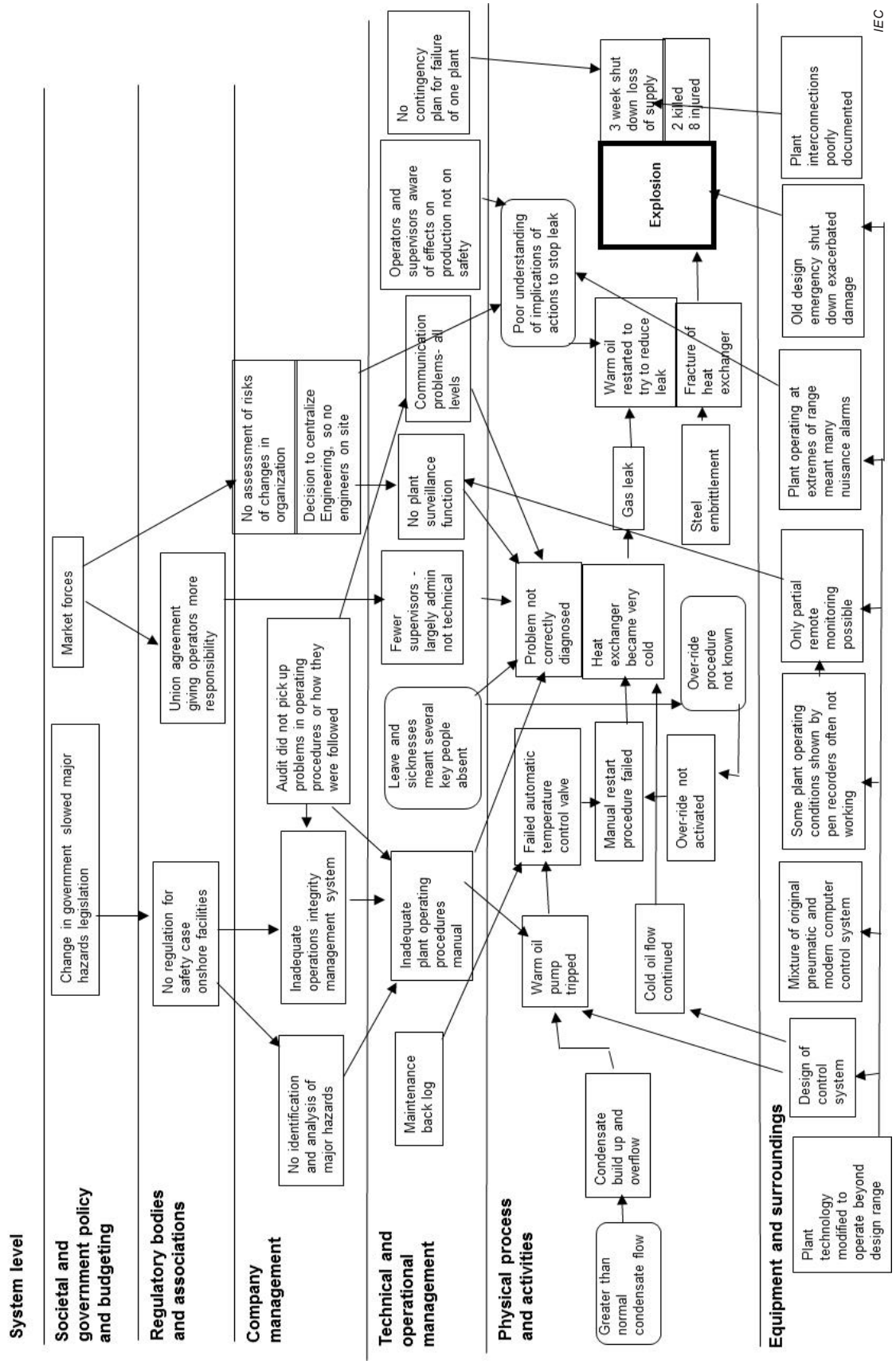


Figure C.11 – Example of an AcciMap

C.11.3 Strengths and limitations

The strengths of AcciMaps are as follows:

- as there is no taxonomy or guidance, AcciMaps has the potential to be highly comprehensive in identifying causal factors across all levels of the system;
- the linkages within and between levels helps ensure that failures are considered in the context of the things that influenced them;
- human error has equal focus with equipment and higher level organizational factors;
- personal factors which influence decisions, particularly at the lower levels, are not included.

The limitations of AcciMaps are as follows:

- the lack of a taxonomy means that the factors identified are based on the team's perception;
- the organizational model comes from outside the analysis and there is no criterion to ensure it is adequate;
- the result of the AcciMaps analysis is lightly constrained, therefore it is possible to derive different AcciMaps for the same focus event;
- with no specific taxonomy it is difficult to aggregate multiple analyses to find common factors;
- the generality of factors in the nodes is often high and can be very abstract. This makes it difficult to derive precise actions;
- it has a weak analytical approach to physical and equipment failures;
- it does not represent the results of a causal analysis by itself.

C.12 Tripod Beta

C.12.1 Overview

Tripod Beta [21] is an incident investigation and analysis methodology which combines the ideas from Reason's model (see Clause B.3) and Barrier Analysis (see Clause B.2), along with Rasmussen's generic error modelling system (GEMS) and Wagenaar's Tripod causation path. It describes incidents in terms of 'objects', e.g. people, equipment, etc. being changed by 'agents of change', e.g. anything with the potential to change an object. It also models 'barriers', showing them, for example, as effective, failed or inadequate.

Tripod Beta provides a format and rules for modelling the events (focus event and the events leading up to, and after, the focus event) and linking each element together, working back ultimately to the underlying causes. A number of software packages have been developed based on these rules, but it can be used with or without software. The software–based techniques contain checklists derived from the models and from analysis of past events mostly in the off shore oil industry.

The core of a Tripod analysis is a 'tree' diagram representation of the causal network (see Figure C.12) which describes the focus event as a network of events and their relationships.

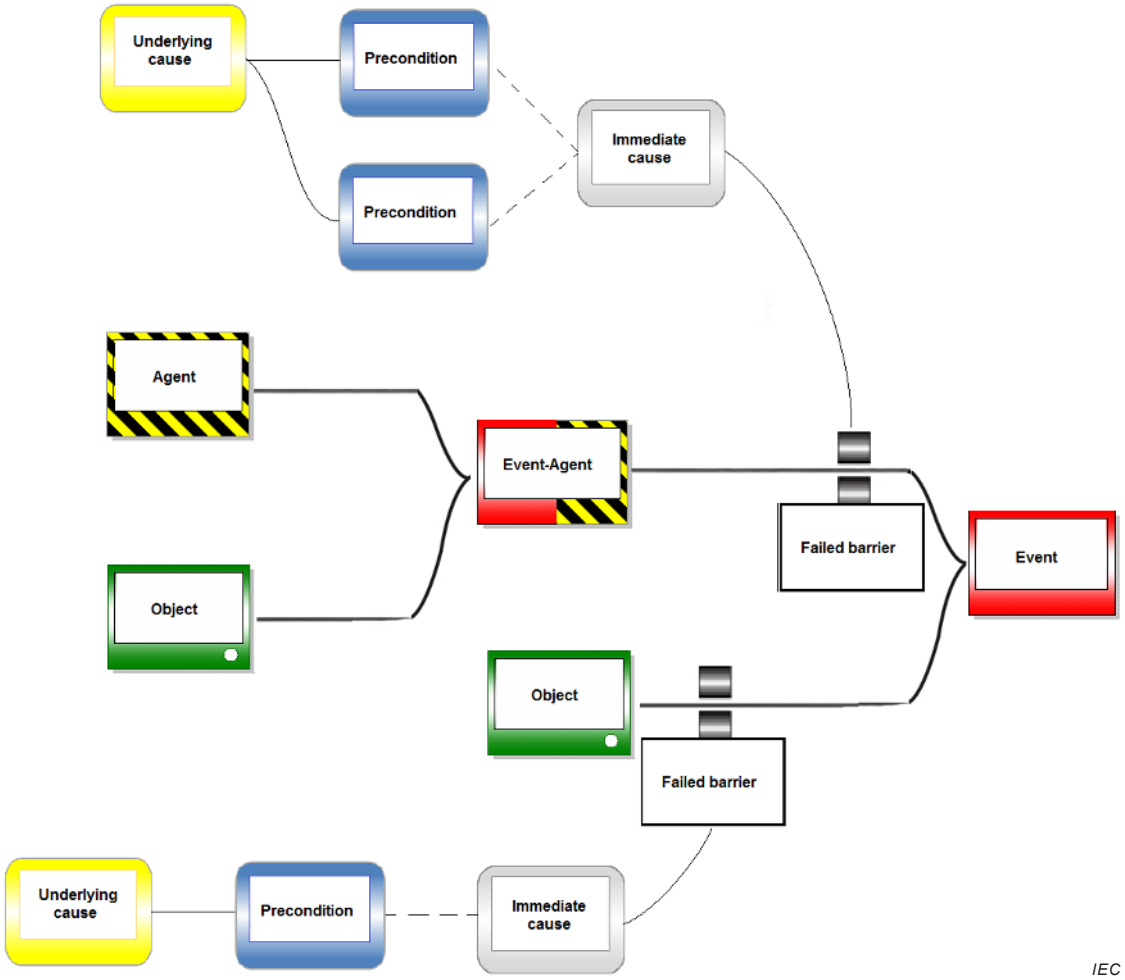


Figure C.12 – Example of a Tripod Beta tree diagram

C.12.2 Process

The process for developing the Tripod Beta tree diagram is to identify the following:

a) The agent (hazard or hazards) that lead to the focus event and the target that was harmed.

b) Controls or barriers, that were missing or failed, that could have prevented the event or protected the target.

c) Immediate causes – the human act, which resulted in the failed barrier. These are failures or errors that have immediate effect and occur at the point of contact between a human and a system (e.g. pushing an incorrect button, ignoring a warning light).

d) Preconditions – psychological and situational precursors e.g. the type of human failure (slip, lapse, violation, etc.).

e) Underlying causes (latent failures) in the organization, i.e. inadequacies in the management system, culture, etc. These can be categorized into pre-defined ‘basic risk factors’, derived from brainstorming and research into results of audits and accident investigations in the off shore oil industry.

C.12.3 Strengths and limitations

The strengths of the Tripod methodology are as follows:

- provides a map of the focus event and its causal factors;
- can help direct the investigation and define its scope;

- defines the barriers in the system;
- based on scientific research including a model of human behaviour to uncover what is behind the observed behaviour;
- leads the investigator to consider the reasons behind the immediate causes and human error;
- menu driven software is available.

The limitations of the Tripod methodology are as follows:

- can be resource intensive;
- leads to system level underlying causes which an organization might not be able to accept;
- use of the basic risk factors to categorize underlying causes can be too generic and simplistic;
- conclusions do not lead to simple remedial actions;
- extensive training is generally required.

C.13 Causal analysis using STAMP (CAST)

C.13.1 Overview

CAST [7] is a technique that examines the entire socio-technical process involved in a focus event. CAST is based on STAMP (see Clause B.5), which is used to guide the causal analysis. CAST documents the dynamic process leading to the focus event, including the socio-technical control structure as well as the constraints that were violated at each level of the control structure and why. The analysis results in multiple views of the focus event, depending on the perspective and level from which the focus event is being viewed.

To illustrate CAST, consider a focus event involving the contamination of a public water supply with E. coli in a small town in Canada. Figure C.13 shows the safety control structure for the water supply of the town. There are three physical systems being controlled: the well system, the water supply and public health. Each component in the structure controlling these processes has specific safety-related responsibilities. For example, the Ministry of the Environment provides oversight and control of the local water systems. Each component of the control structure gets feedback about the state of the process it is controlling. One common cause is that the controller gets incorrect feedback and thinks the state of the controlled process is different than it is. For example, budgets were cut and the Ministry of the Interior reduced the number of inspections and inspectors.

Figure C.14 shows the analysis of the role of the local health department in the focus event, including the roles and responsibilities, the unsafe control actions, the context in which the unsafe control actions were provided, and the flaws in the process (mental) model that contributed to the behaviour. Figure C.15 shows the same thing for another component of the control structure, the water system operations management.

In a full analysis, each component of the control structure would be considered with respect to their contribution to the focus event. In most focus events, contributions can be found from every component of the control structure.

Other features of the analysis (not shown) include examining the dynamic changes over time in the system that contributed to the focus event and the role of flawed communication and coordination.

System hazard: Public is exposed to E. coli or other health-related contaminants through drinking water.
System safety constraints: The safety control structure must prevent exposure of the public to contaminated water.
1) Water quality must not be compromised.
2) Public health measures must reduce risk of exposure if water quality is compromised (e.g. notification and procedures to follow)

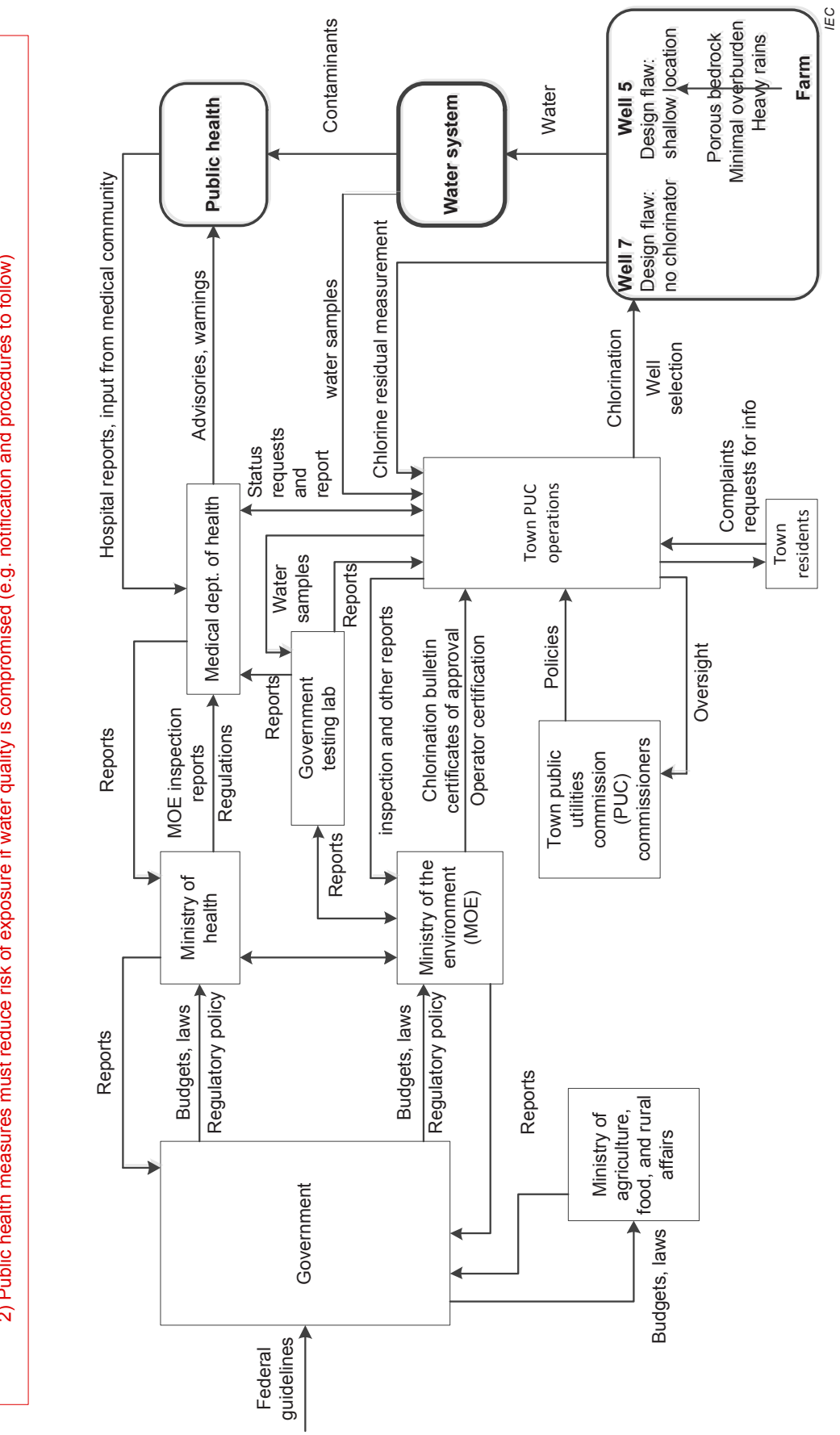


Figure C.13 – Control structure for the water supply in a small town in Canada

Medical department of health

Safety requirements and constraints:

- Provide oversight of drinking water quality
- Follow up on adverse drinking water quality reports
- Issue boil water and other advisories if public health at risk

Context in which decision made:

- Most recent water quality reports over 2 years old
- Illness surfacing in communities outside the town
- E. coli most commonly spread through meat

Inadequate control actions:

- Advisory delayed
- Advisory should have been more widely disseminated
- Public health inspector did not follow up on 1998 inspection report

Mental model flaws:

- Thought adverse water quality reports were being received
- Unaware of reports of E. coli linked to treated water
- Thought Mr K was relaying the truth
- Unaware of poor state of local water operations

Coordination

- Assumed the ministry of environment was ensuring inspection report problems were resolved

Figure C.14 – Example CAST causal analysis for the local Department of health

Town PUC operations management

Safety requirements and constraints:

- Monitor operations to ensure that sample taking and reporting is carried out
- Keep accurate records
- Update knowledge as required

Context in which decision made:

- Complaints by citizens about chlorine taste in drinking water
- Improper activities were an established practice for 20 years
- Lacked adequate training and expertise

Inadequate control actions:

- Inadequate monitoring and supervision of operations
- Adverse test results not reported when asked
- Problems discovered during inspections not rectified
- Inadequate response after first symptoms in community
- Did not maintain proper training or operations records

Mental model flaws:

- Believed sources for water system were generally safe
- Thought untreated water was safe to drink
- Did not understand health risks posed by under chlorinated water
- Did not understand risks of bacterial contaminants like E. coli
- Did not believe guidelines were a high priority

Figure C.15 – Example CAST causal analysis for the local public utility operations management

C.13.2 Process

CAST has the following steps:

a) Identify the system(s) involved in the focus event.

b) Identify the system constraints associated with the focus event.

c) Document the control structure in place. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback (if any) provided to help them do this.

d) Determine the proximate events leading to the focus event.

e) Analyse the focus event at the physical system level. Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective.

f) Moving up the levels of the control structure, determine, as follows, how and why each successive higher level allowed or contributed to the inadequate control at the current level.

   1) For each system constraint, either the responsibility for enforcing it was never assigned to a component in the control structure or a component(s) did not exercise adequate control to ensure their assigned responsibilities were enforced in the components below them.

   2) Identify unsafe decisions or control actions, including actions provided by software, operators, managers, regulators, etc.

   3) Any human decisions or flawed control actions need to be understood in terms of the information available to the decision maker as well as any information that was not available, the behaviour shaping mechanisms (the context and influences on the decision making process), the value structures underlying the decision, and any flaws in the process models (mental models) of those making the decisions and why those flaws existed.

g) Examine the overall coordination and communication (including missing feedback) that contributed to the focus event.

Although the process is described in terms of steps, the process need not be linear nor does one step need to be completed before the next one is started.

C.13.3 Strengths and limitations

The strengths of CAST are as follows:

- looks back through time to determine how the system evolved to a state of high risk;
- identifies the social and managerial factors and not just the human operations or technical system failures;
- does not impose any particular social theory on the analysis, any model of social behaviour could be used to generate the analysis results.

The limitations of CAST are as follows:

- it is not possible to graphically present the analysis, as the inclusion of indirect relationships between causal factors means that circles and arrows (which depict direct relationships) are not adequate to describe all the causal factors;
- may require more resources and time to fully understand the focus event than other methods with a more limited focus.

Annex D
(informative)

Useful tools to assist root cause analysis (RCA)

D.1 General

Annex D describes tools and techniques that can support the conduct of RCA.

D.2 Data mining and clustering techniques

D.2.1 Overview

Modern data mining techniques enable a search for specific properties and conditions. Clustering analysis selects data that are closely related, and thereby identify deviating data (outliers). Modern cluster analysis can detect data that are closely related in one, two or more dimensions and thereby analyse products or processes that are closely related and identify deviating data points (outliers).

In RCA, data mining and clustering analysis can give valuable clues and help to confirm or reject potential root causes. In some cases, e.g. aerospace and medical equipment, it is required to store batch numbers for the finished products and the associated component batch numbers and raw material batch numbers. This information can provide a useful structure for identifying correlations which hint at possible causal relations.

D.2.2 Example 1

A company observes 12 % failures of stocked items. Analysis shows that a plastic part is broken. The start of the 12 % failure pattern is identified as a batch number and a manufacturing date. This date is correlated with delivered batches of the plastic parts. There is no correlation. There is no correlation either with the batches of plastic raw materials. However, there is a correlation with the batches of a spring that load the plastic part. The problem started 3 days after a new batch of springs was received. The changes that were made between the two batches of springs is investigated. The difference is a new surface treatment against corrosion. This surface treatment process is investigated and contains a note that this treatment may interfere with certain plastic materials. Further analysis shows that the corrosion protection accelerates crack propagation in this plastic. Analysis of the data sheet for the plastic material shows a warning against local overload that may cause cracks. The conclusion therefore is that a causal hypothesis can be formulated: that a plastic part is continuously overloaded and undergoes fracture through local overload, and the fractures propagate in a manner accelerated by the new anti-corrosion treatment of the springs. These cracks then propagate in an accelerated manner due to the new anti-corrosion treatment of the springs. A failure analysis has previously shown a pattern on the fracture surface consisting of crack propagation lines originating in the points of contact with the spring and a brittle surface from the final fracture. The causal-explanatory hypothesis may be confirmed at a given level of confidence by experiment: setting up a number of plastic parts with and without the new treatment. If it is observed that plastic parts with the new treatment predominantly fail, one may conclude that the causal hypothesis is confirmed to the appropriate degree of confidence using standard methods of statistical inference.

D.2.3 Example 2

A number of soldering failures is observed in the field. The manufacturing weeks for the failed products are plotted in calendar time. It is observed that the manufacturing dates of the products with soldering failures are clustering in certain weeks. A causal hypothesis may be formulated on the basis of the initial observation, which is then confirmed to a given degree of confidence using standard statistical inference on the process-control data from

manufacturing, which indicate that the soldering process in these weeks was likely not performed under appropriate control. The conclusion is, to a high level of confidence, that a root cause of the soldering failures is insufficient process control of the solder process.

D.2.4 Example 3

A component is tested on a test board by twisting the board. The number of twists to failure is plotted on a Weibull plot (see IEC 61649 [22]). The analysis identifies a ”weak” and a ”strong” population (see IEC 61163-1 [23]). One component from the weak and one component from the strong population is analysed by cross-sectioning of the micro ball grid array (BGA) solder balls. It is noted that the component from the weak population has a large number of large voids in the solder balls, while the solder balls from the strong population have no or few small voids. It is concluded that a root-causal hypothesis is formulated, that voids in the solder balls of the micro BGA are a root cause of the incident events. The root-causal hypothesis is confirmed by collecting data on operational use and observing through analysis of the data that the reduction in voids correlates with successful use of the component.

Annex E
(informative)

Analysis of human performance

E.1 General

People at any level in an organization make decisions or perform or omit actions which may play a part in the events leading to a focus event. Human performance may be above or below expectation and the impact may be positive or negative. Decisions can be correct in the circumstances in which they were made but turn out to have unintended results.

People may make errors, be misguided or misinformed, be inappropriately motivated, may be trying to perform correctly or may knowingly violate rules. Analysis of human aspects of causation is complex and generally requires specialist expertise if it is required to go beyond identifying what occurred to seeking why and hence making recommendations.

E.2 Analysis of human failure

Analysis of human failures starts by identifying the error mode. This is the external manifestation of the error, i.e. what is observed to have been done (or not done). Examples of error modes are as follows:

- omitted;
- too early;
- too late;
- too much;
- too little;
- wrong direction;
- wrong object;
- wrong action;
- wrong sequence.

There are then a number of different taxonomies for categorizing and analysing causes of these errors. They differ in the number and types of classifications they consider and in the models of human behaviour on which the taxonomies are based and on where the most emphasis is placed. The following are generally considered:

a) The internal error mode and error mechanism. This is the reason behind the error in psychological meaningful terms e.g. for an error mode of “took a wrong turn in car”, the internal error mode and mechanism might be incorrect decision due to habit intrusion.

b) Inherent problems of the task, e.g. conflicting goals, planning problems, constraints, cognitive demands etc.

c) Performance shaping factors (PSF). These are the conditions of the technical or organizational environment or internal to a person which affect how well a task will be performed (see IEC 62508 [24]).

Some models also include an analysis of the flow of information and feedback without which correct judgements are unlikely to be made. The importance of these methods is that they first identify the psychological error mechanism before identifying why the error was made. For example if the error mechanism is not due to a lack of knowledge or skill, then further training is unlikely to be useful. If a decision is made to violate a procedure, then the reasons why this occurred should be investigated rather than assuming increased supervision is the solution.

Two examples of methods which can be used to analyse the causes of human failure which illustrate these principles are:

- Technique for retrospective and predictive analysis of cognitive errors (TRACEr);
- Human factors analysis and classification scheme (HFACS).

E.3 Technique for retrospective and predictive analysis of cognitive errors (TRACEr)

E.3.1 Overview

TRACEr [25] was developed for use in air traffic control. TRACEr, has eight modules as shown in Figure E.1, which can be divided into the following three categories:

- the context in which the error occurred, i.e. the nature of the task, the environment and the PSFs;
- the production of the error, i.e. the external error modes (EEM), internal error modes (IEM), the psychological error mechanisms (PEM) and the information on which the individuals based their actions;
- the detection and correction of the error.

The error production modules are based on the cognitive processes involved when a person perceives something needs to be done and takes action, e.g. perception, memory, decision-making and action (see Figure E.2).

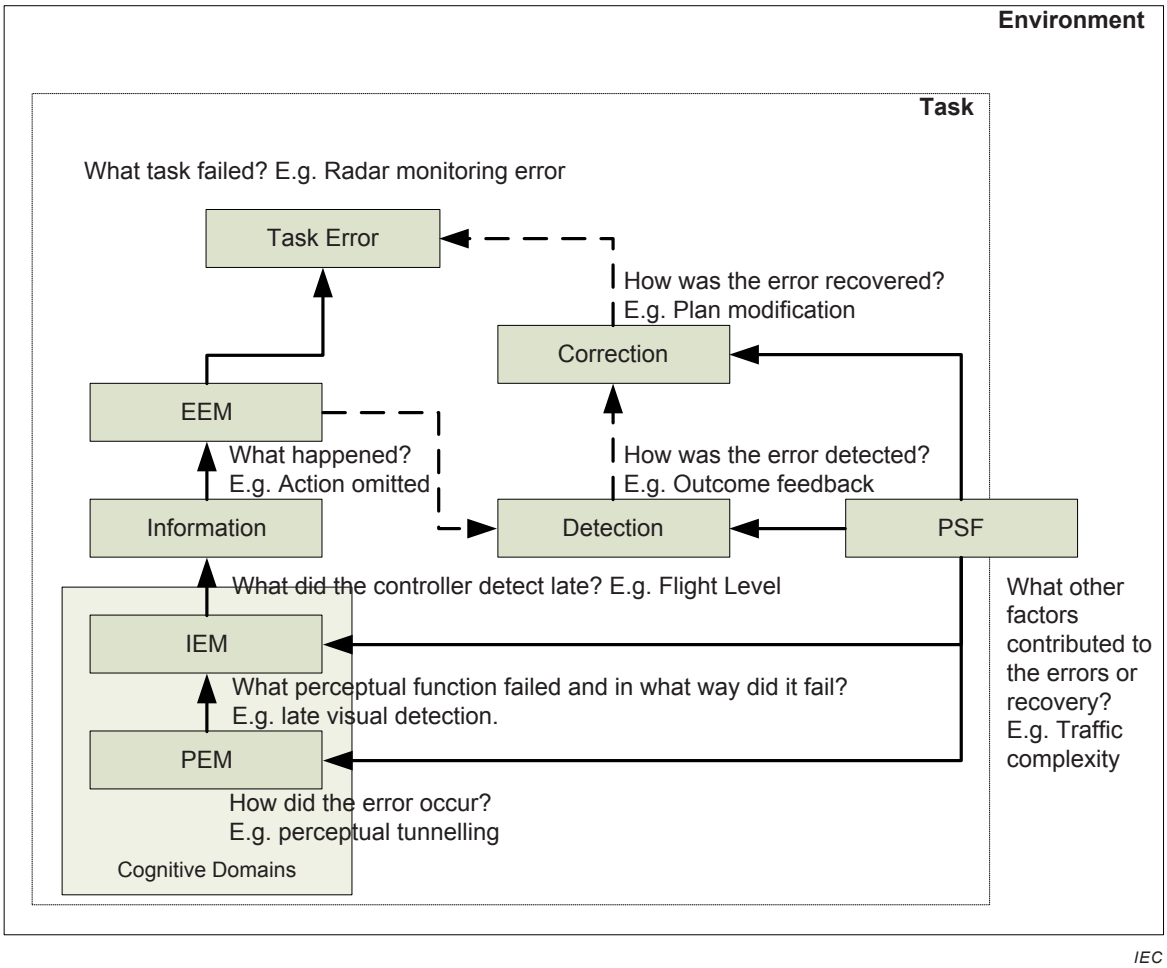


Figure E.1 – Example of an TRACEr model [25]

Cognitive domain	Cognitive function	Relevant keywords	Example IEM
Perception	Vision – Detection	None, late, incorrect	Late detection
	Vision – Identification	None, late, incorrect	Misidentification
	Hearing – Recognition/comparison	None, late, incorrect	Hearback error
Memory	Recall perceptual information	None, incorrect	Forget temporary information
	Previous action	None, incorrect	Forget previous actions
	Immediate/current action	None, incorrect	Forget to perform action
	Prospective memory	None, incorrect	Prospective memory failure
	Stored information (procedural and declarative knowledge)	None, incorrect	Mis-recall stored information
Judgement, planning and decision-making	Judgement	Incorrect	Misprojection
	Planning	None, too little, incorrect	Underplan
	Decision making	None, late, incorrect	Incorrect decision
Action Execution	Timing	Early, late, long, short	Action too early
	Positioning	Too much, too little, incorrect, wrong direction	Positioning error, overshoot
	Selection	Incorrect	Typing error
	Communication	None, unclear, incorrect	Unclear information transmitted

IEC

Figure E.2 – Generation of internal error modes

E.3.2 Process

A TRACEr model is created using the following steps:

a) Analyse the task being carried out and identify any environmental or situational factors that might affect human performance (PSF), which includes task complexity, knowledge and experience of the person, the ambient environment, etc.

b) Identify EEMs, which are classified in terms of selection and quality, timing and sequence, and communication (see Table E.1).

c) Identify the IEMs, which describe what cognitive function failed and in what way, the taxonomy for which is shown in Figure E.2.

d) Identify the information issues associated with the IEM, i.e. what information was misperceived, forgotten, misjudged or mis-communicated.

e) Identify the PEMs, which are the cognitive biases known to affect performance within each cognitive domain (see Table E.2).

f) Review the error detection process, which is how the person became aware of the error, what medium informed them of the error and what external factors improved or degraded detection.

g) Consider correction, i.e. what was done to correct the error, did other factors internal or external improve or degrade the error correction.

Table E.1 – External error modes

Selection and quality	Timing and sequence	Communication
Omission	Action too long	Unclear information transmitted
Action too little	Action too short	Unclear information received
Action too much	Action too early	Information not sought/obtained
Action in wrong direction	Action too late	Information not transmitted
Right action on wrong object	Action repeated	Information not recorded
Wrong action on right object	Mis-ordering	Incomplete information transmitted
Wrong action on wrong object		Incomplete information received
Extraneous act		Incomplete information recorded
		Incorrect information recorded

Table E.2 – Psychological error mechanisms

Perception	Memory	Decision making	Action
Expectation bias	Similarity interference	Incorrect knowledge	Manual variability
Spatial confusion	Memory capacity overload	Lack of knowledge	Spatial confusion
Perceptual confusion	Negative transfer	Failure to consider side effects	Habit intrusion
Perceptual discrimination failure	Mis-learning	Integration failure	Perceptual confusion
Perceptual tunnelling	Insufficient learning	Misunderstanding	Mis-articulation
Stimulus overload	Infrequency bias (memory failure due to knowledge not being used sufficiently frequently)	Cognitive fixation	Environmental intrusion
Vigilance failure	Memory block	False assumption	Other slip
Distraction	Distraction/ preoccupation	Prioritization failure	Distraction preoccupation
		Risk negation or tolerance	
		Risk recognition failure	
		Decision freeze	

E.4 Human factors analysis and classification scheme (HFACS)

E.4.1 Overview

HFACS [26] was developed by behavioural scientists in the Unites States Navy and analyses the causes of human error based on Reason's model (see Clause B.3). There are four levels of consideration based on Reason's model of slices of Swiss cheese:

- organizational influences;
- supervision;
- preconditions for unsafe acts;
- unsafe acts.

Some applications add a fifth level above organizational influences relating to legislation and government.

E.4.2 Process

Each level is subdivided into categories; examples are given of possible causal factors within the category. Different applications use the same categories (shown in the boxes below) but

may have different examples depending on the industry, and may provide a few examples or a more detailed check list. Examples of the four levels are shown in Figure E.3 to E.6.

Consideration of cause starts with Level 1 so that precursors for the act in question take account of the type of error involved then continues up through the levels seeking weaknesses that contributed to the focus event.

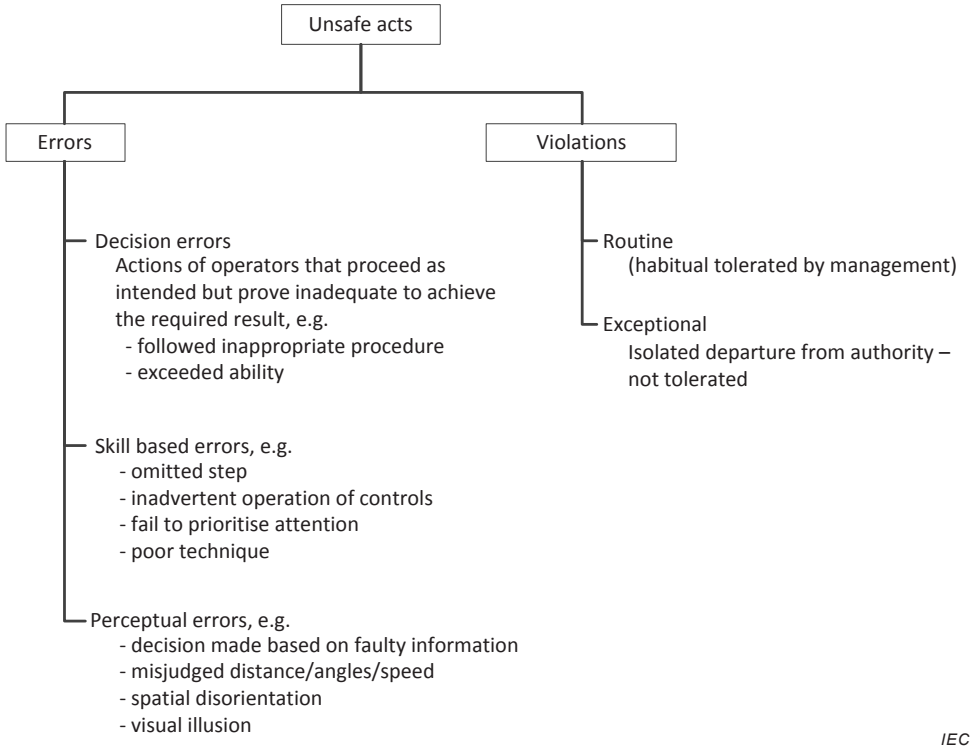


Figure E.3 – Level 1: Unsafe acts

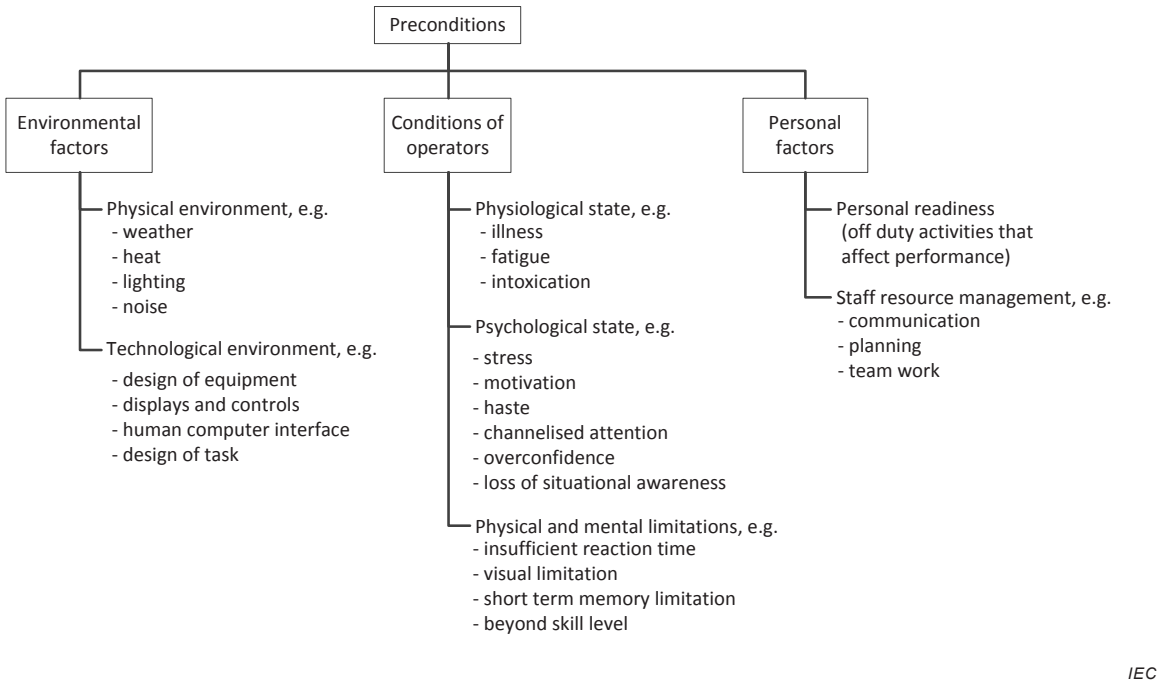


Figure E.4 – Level 2: Preconditions

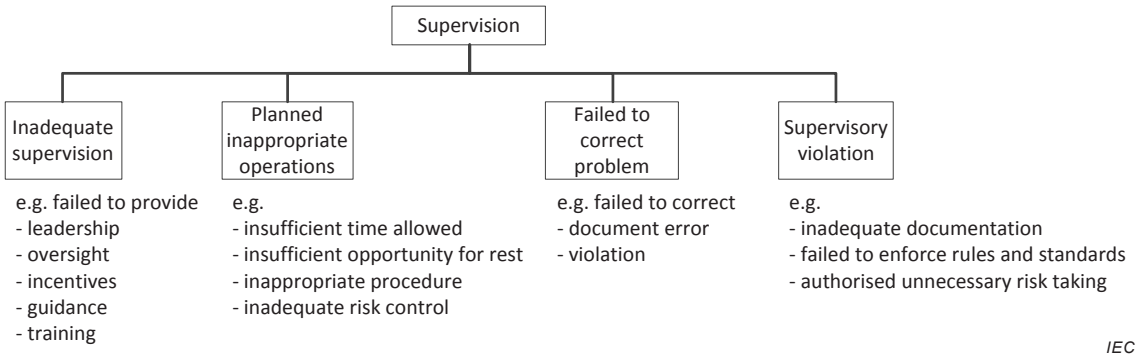


Figure E.5 – Level 3: Supervision Issues

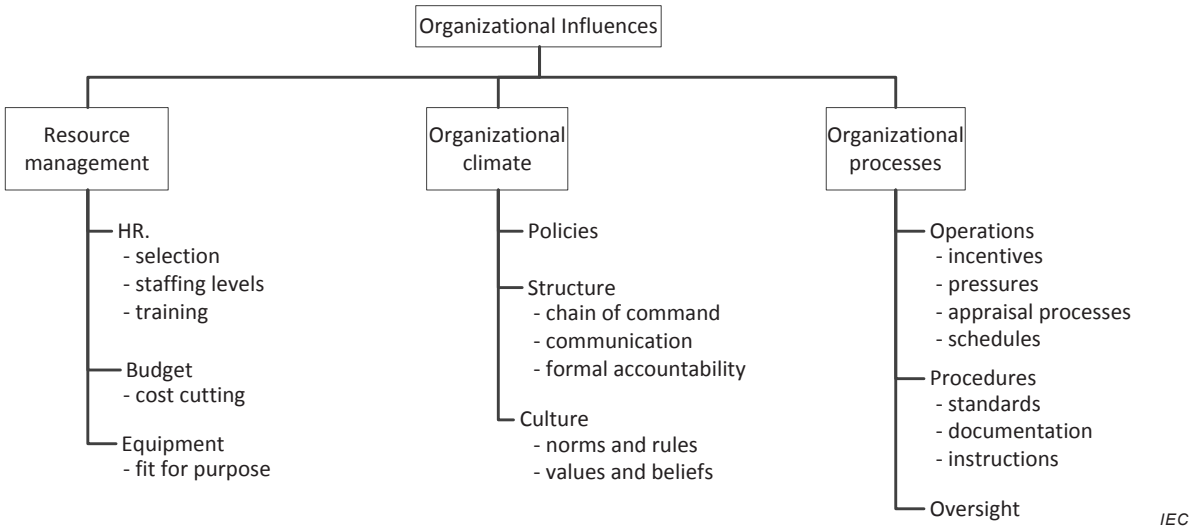


Figure E.6 – Level 4: Organizational Issues

Bibliography

[1] ISO Guide 73: 2009, *Risk management – Vocabulary*

[2] IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

[3] HADDON, W Jr., *Energy Damage and the Ten Counter-Measure Strategies,* The Journal of the Human Factors and Ergonomics Society, 1973

[4] HOLLNAGEL, E., *Barriers and Accident Prevention,* Ashgate Publishing Limited, 2004

[5] REASON, J., *Human Error,* Cambridge University Press, 1990

[6] CHECKLAND, P., *Systems Thinking, Systems Practice: Includes A 30-Year Retrospective,* Wiley Pages: 416, 1999

[7] LEVESON, N., *Engineering a Safer World,* MIT Press, 2012

[8] RASMUSSEN, J., *Risk Management in a Dynamic Society: A Modelling Problem*, Safety Science Volume 27, Issue 2-3, Pages: 183-213, 1997

[9] Technical Research and Analysis Center: Events and Causal Factors Analysis, SCIE-DOE-01-TRAC-14-95, 1995

[10] BENNER, L. Jr., *Accident Investigations: Multilinear Event Sequencing Methods*, Journal of Safety Research 7, 67-73, 1975

[11] HENDRICK, K. and BENNER, L. Jr., *Investigating Accidents with STEP*, Marcel Dekker Inc, 1986

[12] MONTEAU, M., *Analysis and reporting: accident investigation,* Encyclopaedia of Occupational Health and Safety, 57-22:26, ISBN 1:92-2-1-103290-6, 1982

[13] SANDERS, J., *Introduction to Why-Because Analysis*, 2012

[14] US Nuclear Regulatory Commission: NUREG 0492, Fault Tree Handbook, January, 1981

[15] IEC 61025, *Fault tree analysis (FTA)*

[16] ISHIKAWA, K., *Guide to Quality Control,* Asia Productivity Organization, 1986

[17] FAHLBRUCH, B. and SCHÖBEL, M., SOL – *Safety through organizational learning: A method for event analysis.* Safety Science, Volume 49, Pages 27–31, 2011

[18] JOHNSON, W. and DEKKER, M.,:*MORT Safety Assurance Systems*, 1980

[19] SVEDUNG, J. and RASMUSSEN, J.,:*Graphic representation of Accident Scenarios: Mapping System Structure and the Causation of Accidents,* Safety Science, Volume 40, Pages 397-417, 2002

[20] SVEDUNG, J. and RASMUSSEN, J., *Risk Management in a Dynamic Society: A Modelling Problem*, Safety Science, Volume 27, Pages 183-213, 1997

[21] Energy Institute, *Tripod Beta: Guidance on the use of Tripod Beta in the investigation and analysis of incidents, accidents and business losses,* 2013 http:www.tripodfoundation.com

[22] IEC 61649, *Weibull analysis*

[23] IEC 61163-1, *Reliability stress screening – Part 1: Repairable assemblies manufactured in lots*

[24] IEC 62508:2010, *Guidance on human aspects of dependability*

[25] SHORROCK, S. and KIRWAN, B., *Development and application of a human error identification tool for air traffic control,* Applied Ergonomics, Volume 33, Pages 319–336, 2002

[26] SHAPPELL, S. and WIEGMANN, D., *Applying Reason: The Human Factors Analysis and Classification System (HFACS), Human Factors and Aerospace Safety,* Volume 1, Pages 59-86 , 2001

[27] ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*

[28] ISO 31000: 2009, *Risk management – Principles and guidelines*

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™