Root Cause Analysis: Terms and Definitions, Accimaps, MES, SOL and WBA

Peter Bernard Ladkin
01 June 2012, modified 20 January 2013, 21 February 2013

Introduction

From late 2011 until January 2013 I have been involved in the attempted international standardisation of an engineering technique known as Root Cause Analysis, or Root-Causal Analysis, RCA. When an event has occurred which it is desired to explain causally, the process by which engineers try to do so is known as RCA.

There are two main reasons for performing an RCA.

The first comes from engineering quality control. Say you have a production line which is producing items, only 80% of which pass quality-control inspection and you wish to determine why it is only 80% (4 in 5), and to increase the pass rate to 99.9% (999 in 1,000). Then you would probably like to try to find out why things are coming out substandard so often, in other words to determine the causes of the substandard assembly, and fix them. That involves an RCA.

Second, major accidents are usually investigated as to their causes. Sometimes they are investigated by appointed commission headed by a judge (examples in the UK include the Piper Alpha oil-rig accident, the Kings Cross underground-station fire, and the Ladbroke Grove railway collision, all investigated by commissions headed by the judge Lord Cullen, and in Australia the Waterfall and Glenbrook rail accidents in New South Wales , which were investigated by commissions led by Justice Peter McInerney). In other industrial cases, there are agreements or laws in place which require accidents to be investigated (accident-investigation procedures may be part of so-called "*safety management systems*"). For example, international agreements in civil aviation require that transport-aircraft accidents be investigated. The UN agency responsible for managing such agreements is the International Civil Aviation Organisation, ICAO. All ICAO members (those who have signed the relevant agreements, which include most countries in the world) must investigate major accidents with a view to identifying factors which might lead to further accidents, and produce a report in a format mandated by ICAO. That also involves an RCA, but the process involves more than an RCA because

- *any* hazards identified in the course of investigation, including those which might be peripherally related or completely unrelated to the causes of the accident which is being investigated, must be identified and appropriate recommendations for mitigation suggested; and
- the investigation agencies are also required to make recommendations for mitigation or avoidance of any of the identified hazards and other danger-related phenomena

The use and maintenance of ,as well as practice with, complex modern military equipment is also an activity involving significant risk, and there are accidents. Major western militaries run accident investigations when one occurs.

The material in this note does not provide anywhere near a complete guide to RCA. It derives largely from my contributions to a standardisation effort which it appears as of writing will not be used. I hope some people seaching for some details on RCA may find it useful.

Inter alia I survey some techniques for RCA for accident analysis (the techniques used for quality control are largely simpler, less resource-intensive, but equally less appropriate for complex or sensitive analyses). Techniques widely used for accident analysis which do not appear here, but which are thoroughly treated elsewhere in the literature, are

- Events and Causal Factors Analysis (ECF. See for example Chapter 10 of Chris Johnson's Handbook of Incident and Accident Reporting at http://www.dcs.gla.ac.uk/~johnson/book/);
- STAMP (strictly speaking, a model) from Nancy Leveson at MIT (see Nancy's home page, especially her recent book, at http://sunnyday.mit.edu/);
- for analysis of human factors, often but sometimes inappropriately fingered as the primary set of factors in accident occurrences, the "Reason Model" based on Jim Reason's analysis of human error, may be found in his book Human Error, Cambridge University Press, 1990. The Reason model is highly influential and was used by the Australian Transport Safety Board from the early 1990's until at least 2005;
- Fault Tree Analysis (FTA) is in fact a technique for risk analysis of complex engineered systems at design time, but its results may be invaluable in determining causes after accidents happen. Nancy Leveson (private communication) told me that FTA was widely used in the RCA of the Deepwater Horizon drilling-rig accident. The locus classicus for FTA is the Fault Tree Handbook, NUREG-0492 from the US Nuclear Regulatory Commission, available on-line at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/ Examples and exercises in the FTH are somewhat sparse. Textbooks containing useful explanations and exercises on FTA for risk analysis (but not necessarily for accident analysis) are:
  - Probabilistic Risk Assessment for Engineers and Scientists, Second Edition, Hiromitsu Kumamoto and Ernest J. Henley, IEEE Press 1996;
  - Probabilistic Risk Assessment, Tim Bedford and Roger Cooke, Cambridge University Press, 2001
- for human factors, Hollnagel's CREAM and FRAM. See for example http://www.erikhollnagel.com/Books.html ;
- for human factors, Sträter's CAHR. See http://www.cahr.de/tools/tools.htm .

Organisation of this Note

First, I introduce and comment terms and definitions. Second comes a short synposis of the Accimaps technique, followed third by MES, fourth by SOL, and fifth by WBA.

Material from others, notably diagrams, are included here. I thank especially Mike Walker of the Australian Transport Safety Board for guidance on the use of ATSB materials, Babette Fahlbruch of TüV Nord and the people at SOL-VE GmbH for their diagrams and extensive background materials, likewise Ludi Benner apropos MES, and Chris Goeker of my university group RVS for his renderings of other diagrams.

1. Terms and Definitions

In 2012 I attempted to define the concepts used in Root Cause Analysis for a standardisation activity. Here is what resulted, with my annotations where the definitions come from the International Electrotechnical Vocabulary (see below).

It is required in standardisation activity that terms be taken as far as possible from the International Electrotechnical Vocabulary (IEV), available online at www.electropedia.org , the vocabulary defined for electrotechnology by the International Electrotechnical Commission, IEC, in the standard IEC 60050. Additional terms necessary for the explanation of root cause analysis techniques are included.

The quality of some of the IEV definitions may be questioned, as I do in notes appended to them below. I suggest that the definitions here be compared with those in the rationalised set

of system-safety definitions which I wrote in 2008, available at
www.causalis.com/90-downloads/90-publications/DefinitionsForSafetyEngineering.pdf

Items appearing in the IEV are annotated underneath with "[IEC 60050-zzz, definition zzz-xx-yy]". Here, "zzz" is most commonly "191". My annotations are appended as "PBL Note [x] <date>". Items without annotation are my proposed definitions for RCA concepts not already in the IEV.

causal predecessor (of an event or state)

item which occurs in some path of causal factors leading to (and maybe beyond) the given event or state. Mathematically, defined as the ancestor of the given event or state in the transitive closure of the binary relation of being a necessary causal factor.

contributory factor
a necessary causal factor regarded as secondary, according to an explicitly-given prioritisation of necessary causal factors

event
change of state

failure (of an item)
loss of ability to perform as required

NOTE 1 When the loss of ability is caused by a pre-existing latent fault, the failure occurs when a particular set of circumstances is encountered.

NOTE 2 A failure of an item is an event that results in a fault state of that item.

NOTE 3 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 4 Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

[IEC 60050-191, definition 191-43-01]

PBL Note 1 20120601: This definition concerns failure of an item, not more generally failure as it applies to behaviour. Say an engineer attempts to open a valve, and can't. An action has been attempted and cannot be executed. That is a failure, of behavior. It is not an error – the engineer's attempt was appropriate behavior. But that behavior failed. The engineer, however, did not "lose the ability to perform as required".

PBL Note 2 20120120. This definition of failure is particularly problematic for, say, software. SW may fail to perform as required (either in the sense of performing as expected/wishe/anticipated, or in the sense of performing according to the explicit requirements specification. However, the software doesn't "lose the ability" to perform as required, unless an explicit change has been effected in the code. It just doesn't

perform as it should. I see nothing amiss with describing such a failure to perform as desired a "failure" of the SW. But this definition rules this out.

failure cause
set of circumstances that leads to failure

NOTE A failure cause may originate during specification, design, manufacture, installation, operation or maintenance.

[IEC 60050-191, definition 191-43-11]

PBL Note 1 20130120: I don't see why a "cause" should be restricted to a "set of circumstances". A set of circumstances is close to what is known technically as a state. Events, which are changes of state, that is, changes in sets of circumstances, are more usually regarded as causes in both the philosophical and in the vernacular engineering literature.

PBL Note 2 20130120: I don't know what "leads to" means. It is not defined. Suppose I see smoke arising from the neighborhood of my house. I get rapidly back on my bicycle and pedal off, ignoring the nails on the road in front. A puncture ensues. The smoke arising from the neighborhood certain led to the failure of my bicycle tire; had the smoke not been there, I would have paid far more attention to the state of the road, and not even ridden in that direction. So according to this definition the smoke is a cause of the failure of my bicycle tire. Which is completely counter-intuitive.

PBL Note 3 20130120: There are lots of such problems as that in PBL Note 2 with the IEV's definitions in the area of failure and safety. I have been advised that fixing them is a lost cause. But I hope not.

failure effect
consequence of a failure, within or beyond the boundary of the item

NOTE For some analyses it may be necessary to consider individual failure modes and their effects.

[IEC 60050-191, definition 191-43-08]

PBL Note 20120120: It should rather read: "causal consequence of a failure...."

failure mechanism
process that leads to failure

NOTE The process may be physical, chemical, logical or a combination thereof.

[IEC 60050-191, definition 191-43-12]

PBL Note 20130120: Problem again with "leads to". How about "process that causes failure"?

failure mode
manner in which failure occurs

NOTE A failure mode may be defined by the function lost or the state transition that occurred.

[IEC 60050-191, definition 191-43-17]

PBL Note 20130120: "Manner" is vague. What is usually meant by "failure mode" is the following. In a specific engineering domain, classification of the common types of failures will have been derived through experience. Each category in such a classification is termed a "failure mode".

fault (of an item)
state of inability to perform as required, for internal reason

NOTE 1 A fault of an item results from, either a failure of the item itself, or a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance.

NOTE 2 Qualifiers, such as specification, design, manufacture, maintenance or misuse, may be used to indicate the cause of a fault.

NOTE 3 The type of fault may be associated with the type of associated failure, e.g. wear-out fault and wear-out failure.

NOTE 4 The adjective, "faulty" designates an item having one or more faults.

[IEC 60050-191, definition 191-44-01]

PBL NOTE 20120601: A fault of an item which is a component of a system does not necessarily result in the inability of a larger item of which it is a component to perform as required. So-called "fault-tolerant techniques" enable items to be designed and fabricated which continue to perform as required upon the occurrence of faults in their components.

focus event or focus state
the event or state which the RCA is intended to explain causally

functional failure
inability of an item to fulfil or to execute one or more of its required and defined functions

immediate 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, and without any other identified causal factor of the focus event being an effect of this factor.

PBL Note 20130120: This is not entirely satisfactory, because it is relative to the analysis activity. A root cause analysis is constructed out of a collection of events and states deemed to be significant by the analysts. It is relative to this collection that an "immediate..factor" is defined. In a different collection, this factor might no longer be immediate according to the definition, for another factor might be interpolated between it and the focus event. However, I don't see any way of eliminating this dependence on a specific collection of factors. I do, however, see some coherence conditions on collections of factors for them to be adequate for a causal explanation. These

conditions cannot be captured at present in definitions without explanation, and I do not know whether they are complete.

item
subject being considered

NOTE 1 The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

NOTE 2 The item may consist of hardware, software, people or any combination thereof.

NOTE 3 The item is often comprised of elements that may each be individually considered.

[IEC 60050-191, definition 191-41-01]

PBL Note 20130120: An item is a "subject"? What is a subject? Moving on, say the mechanic is repairing your car. You car is certainly being "considered" in some sense, so it's an item. But then you drive it home, put it in the garage and go to sleep. Now, no one is considering your car, so it cannot be an item. It seems things drift in and out of itemhood. Is an item really not an item when there isn't a human around to consider it? Bishop Berkeley asked that question a few hundred years ago. It is known as the "tree in the quad" example. Engineers might do well to read a little more widely.

necessary causal factor (of an event or state)
event or partial state that is antecedent in the relation "immediate necessary causal factor" to the given event or state

partial state (of a collection of objects)
An instantaneous collection of some properties and relations instantiated by the objects

root cause

a necessary causal factor which has no causal predecessor (under the application of the stopping rule)

Root Cause Analysis

systematic process to identify the causes of a focus event

PBL Note 20120601: IEC 60050-191, definition 191-52-05 provides the following more restrictive definition: "systematic process to identify the cause of a fault, failure or undesired event, so it can be removed by design, process or procedure changes". Reference to a purpose, namely "so it can be removed....." is inappropriate. Accident analysis attempts to determine the causes of an accident. Something that has happened cannot be "removed". If a car accident is caused (in part) by a car travelling too fast to negotiate a curve in the road, you cannot "remove" that cause. It is simply a part of history. Some accident investigations, particularly those in civil aviation, do attempt to identify causes which may also manifest themselves in other circumstances, or again in the future. It is said to be a purpose of ICAO-mandated

accident analyses to eliminate such factors. However, other accident investigations are pursued for the main purpose of distributing responsibility for the causes (to manufacturers, to operator companies, to individuals). Legal and moral philosophers (as well, of course, as lawyers, accident victims and relatives of victims) consider attribution of responsibility as equally important. Indeed, such attributions are pervasive in most human societies for thousands of years.

stakeholder
a person, group or organisation who is affected or could be affected by the focus event

PBL Note 2013-01-20: I understand that IEC 60030-1, definition 3.1.17 is "person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity". I think it is a mistake to leave out "group"; there are many collections of people, say all those people living on the street where an aircraft crashes, who can well be said to be stakeholders, but whose collection is more than "a person" and does not form "an organisation". Second, all kinds of people may perceive themselves to be affected by a root-causal analysis activity – consider for example those who have devised root cause analysis methods which they are vying to have used. I wouldn't consider such people "stakeholders".

state (of a collection of objects)
An instantaneous, complete collection of the properties and relations instantiated by the objects

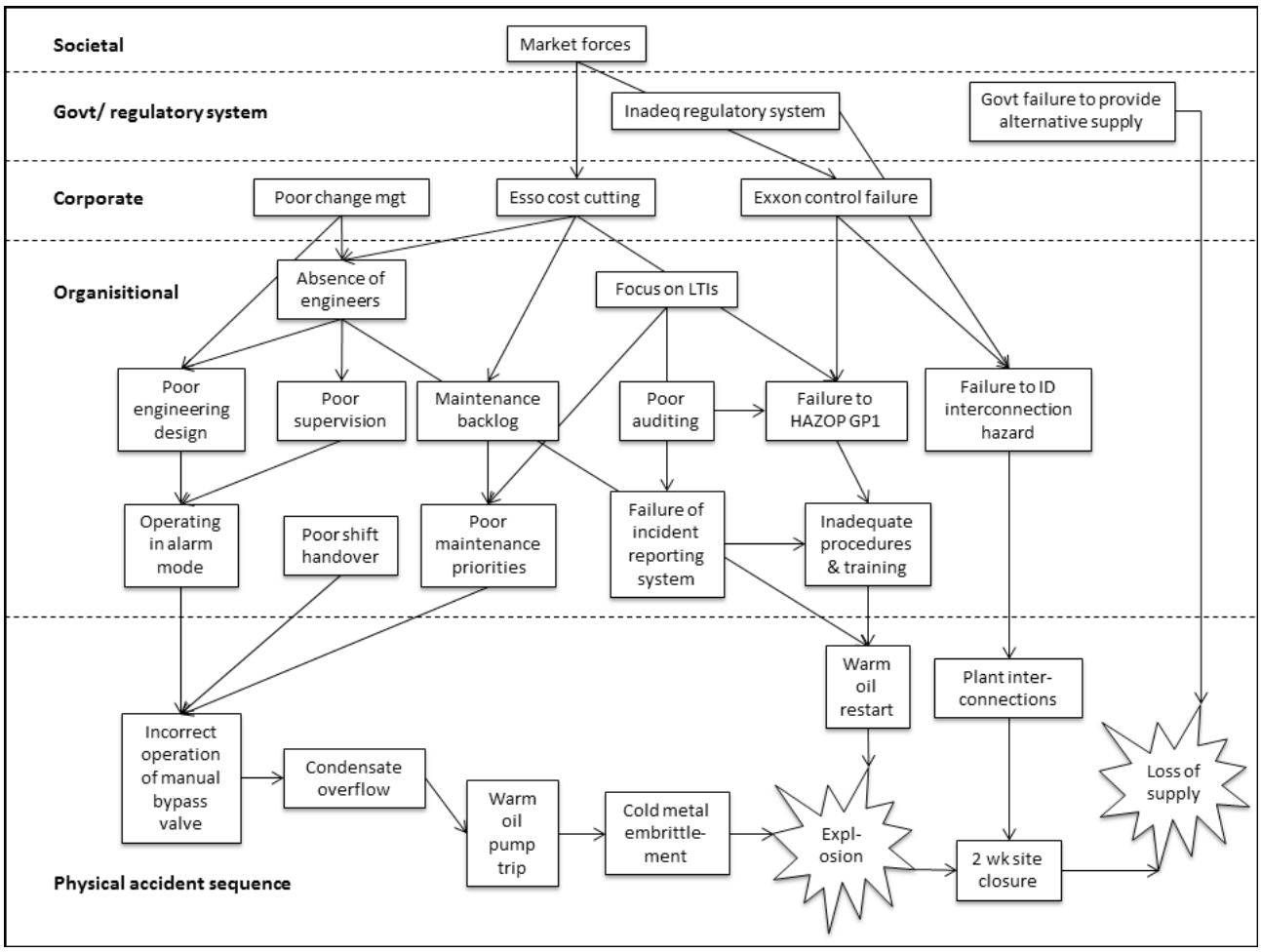
stopping rule
A reasoned and explicit means of determining when a necessary causal factor is defined as being a root cause

2. Accimaps

Overview

Accimaps show the causal relations obtaining between different technical, psychological, organisational, cultural, regulatory, legal and other factors, each of which domains typically have their own methods of explanation (for example, psychology does not follow physical laws; organisational behavior is explained using largely different concepts from those of individual psychology, and regulatory principles are often different from all those).

The causal relations are determined by using the counterfactual condition, an informal version of what is called in WBA the Counterfactual Test. The results are displayed in a (discrete-mathematics-type) graph, with "nodes" (boxes) representing the factors, and "directed edges" (arrows) representing the causal influence. The factors are separated into layers corresponding to the domains under which they occur.



Accimap of an Explosion Accident at a Gas Plant (courtesy C. Goeker, after Hopkins, *op. cit.*)

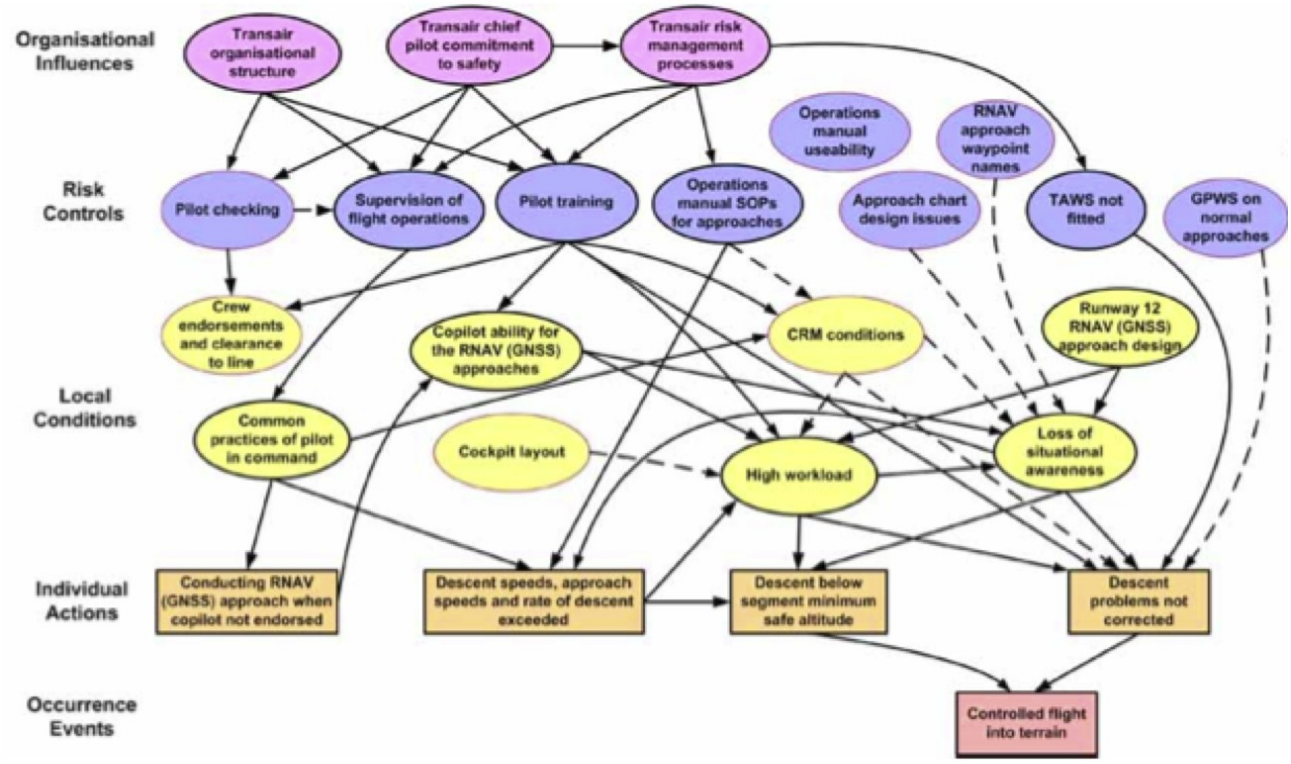
Relatively few factors appear in a typical Accimap. The Accimap itself is the result of the investigation, and is driven by the domains, the "model", into which factors are to be classified. A typical Accimap has of the order of twenty to forty nodes.

The level of abstraction of the nodes varies considerably between applications. In the Longford accident Accimap (see Figure), very general phenomena may be seen, such as a "*maintenance backlog*", or "*poor auditing"* as well as very specific phenomena such as: "*warm oil pump trip*" and "*condensate overflow*". It is up to the analyst to determine at what level of abstraction the factors are considered. It is also expected that the Accimap serves as an illustration to a textual, narrative explanation of the findings of the investigation; it is not intended as a stand-alone result.

The domains or "*levels*" in an Accimap are set by an organisational model. For example, the Australian Transport Safety Bureau (ATSB) organisational model used in the Lockhart River controlled-flight-into-terrain accident (CFIT; ATSB *op.cit.*) uses the following levels (explanation in paratheses by the authors of this note):

- Occurrence Events (what happened timewise proximate to the accident)
- Individual Actions (human actions over time which increased pertinent risk)
- Local conditions (environment, immediate organisational conditions and constraints which influenced individual actions)
- Risk Controls (organisational characteristics – or the lack of them – which could have influenced local conditions or individual actions to reduce risk)
- Organisational Influences (what was in place, resp. lack of such, to inhibit problems with the

risk controls)



Accimap of the Lockhart River CFIT accident (ATSB, *op.cit.*)

The resulting Accimap for the Lockhart River investigation contains 3 factors falling under Organisational Influences, 9 factors under Risk Controls, 8 factors under Local Conditions, 4 factors under Individual Actions and 1 factor, the CFIT event, under Occurrence Events, for a total of 25 nodes.

Factors to be included in an Accimap are determined by investigation. It is presumed that the investigators understand how to determine possible factors for consideration, at whatever level of generality they consider appropriate. This level of generality is not set by the Accimap format itself. Neither do Accimaps give guidance to investigators on identifying possible factors. The possible factors are determined to be causally relevant through the informal application of the counterfactual condition.

Process

After factors have been identified, the following process is used to construct the causal explanation in an Accimap:

- The factors are assigned to their respective domains

- The counterfactual condition is used to determine the causal influence between the factors
- The Accimap is constructed: domains are represented as horizontal layers; nodes for each causally-relevant factor are arrayed with their domain; arrows are drawn between nodes, representing that the node at the tail of an arrow is a causal factor of the node at the point of the arrow.

Strengths and Limitations

Strengths.

- An Accimap is intuitively easy to understand.
- An Accimap representation requires the analyst to consider all factors in various levels in the organisational model, and explicitly to check to see what the causal relations between any factors in different levels of the model might be. Causal connections are thus observed which might be missed if the domains in the organisational model are considered separately.

Limitations

- The counterfactual condition used to determine causality is informal; it is not provided with a formal semantics. Thus it is dependent on the intuition and personal judgement of the investigator.
- There is no criterion to determine whether an organisational model is adequate; the model comes from outside the analysis.
- The level of generality of the factors expressed in the nodes is high; they can be very abstract. An attempt to derive countermeasures is correspondingly vague.
- The Accimaps method provides only a weakly analytical approach to physical failures or identifying inappropriate features of the physical part of the system.
- An Accimap does not represent the results of a causal analysis by itself. It requires a textual expression of the results and serves to illustrate or summarise that text.
- The result of an Accimap analysis is relatively lightly constrained; it is thus possible to derive different Accimaps of the same incident showing different sets of causes, depending on the analyst's focus.

Literature

- Andrew Hopkins, Safety, Culture and Risk: The Organisational Causes of Disasters, CCH Australia, Sydney 2005.

- Andrew Hopkins, An Accimap of the Esso Australia Gas Plant Explosion, available at http://www.qrc.org.au/conference/_dbase_upl/03_spk003_Hopkins.pdf , accessed 2012.05.17

- Jens Rasmussen, Risk Management in a Dynamic Society: A Modelling Problem, Safety Science 27(2/3), 1997.

- ATSB, Australian Transport Safety Bureau, Collision with Terrain 11km Northwest Lockhart River Aerodrome, VH-TFU, SA227-DC (Metro 23), 7 May 2005, Aviation Occurence Final Report 200501977, ATSB, Canberra, April 2007. Available from http://www.atsb.gov.au/publications/investigation_reports/2005/aair/aair200501977.aspx ,

accessed 2012.05.15.

3. Multilinear Events Sequencing (MES) and Sequentially Timed Events Plotting (STEP)

Overview

Multilinear Events Sequencing (MES) and Sequentially Timed Events Plotting (STEP) are methods for analysis of accidents to complex systems. STEP is a successor to MES. We enumerate features common to both. MES/STEP conceives of an accident process as an interlinked succession of events involving people, objects and energy and their interactions over time. An event (or action) has an instigator, called an actor (which may be human or machine, or even a property), is partially triggered by other events, along with conditions enabling it to occur, and in turn helps to trigger further events.

The basic elements of an MES/STEP analysis are Event Building Blocks and a Time-Actor Matrix. The analysis method SOL also uses these basic structures, derived from MES. Events are represented as event building blocks (BBs). BBs consist of (partial or full) data records as described in Figure 1. BBs are arranged during the analysis in a Time-Actor Matrix. These matrices have a vertical axis representing the different actors, and a horizontal axis representing time, as in the SOL Time-Actor Diagram. Time Actor Matrices also contain Conditions, necessary for enabling an event along with precursor events, and various annotations for further tasks in an investigation, such as a note indicating a deficit of information, or an incomplete explanation of an event. Incompleteness in the sequence of events is identified, hypotheses generated to fill a “gap”, and requirements determined for data that would be sufficient to substantiate a given hypothesis. MES/STEP makes use of logic trees as a hypothesis-exploration technique.

Process

The first step is to gather available information for the initial series of BBs, and identify and track missing information. These initial BBs are arranged in an initial Time-Actor Matrix. Specific techniques are then used to identify incompleteness and “gaps”, generate hypotheses to “fill” the gaps with events (in the form of further BBs). The process terminates when an analyst considers that sufficient information is available in the Time-Actor Matrix.

Strengths and Limitations

Strengths

- The method has evolved over decades of practical use analysing commercial-aircraft accidents according to the terms of the ICAO treaty.
- Data formatting is relatively 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 has explicit notation for recording the state of an ongoing 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.

Limitations

- An MES/STEP investigation is heavily dependent on the MES/STEP-defined ontology.
- There is no explicit notion of cause, in particular of events being causes or partial causes of other events. The notion of cause is supplanted by a notion of "input/output relationship" between BBs, said to come from Cybernetics.
- The theoretical underpinnings of the specific event-based model do not appear to be as rigorous as those of methods such as Accimaps, SOL or WBA.

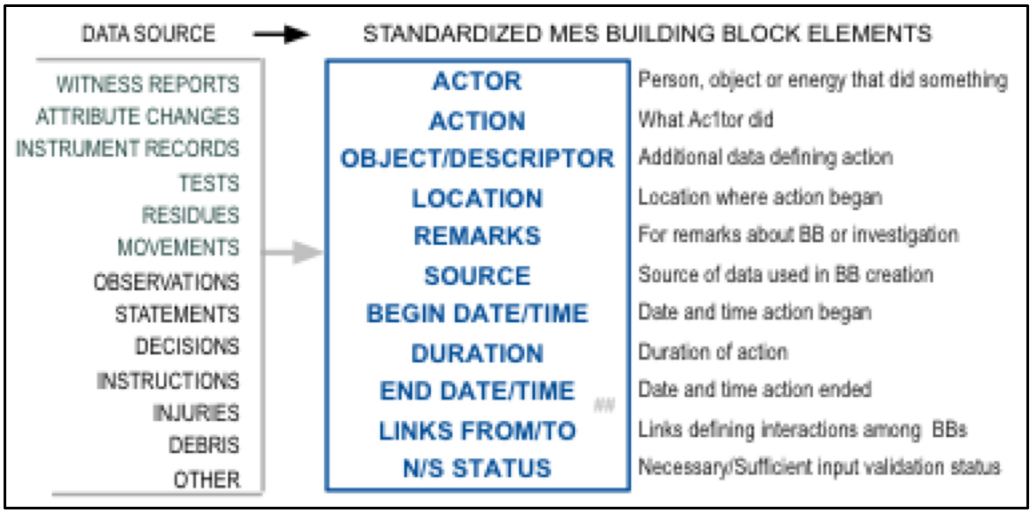


Figure 1: Data comprising an Event Building Block

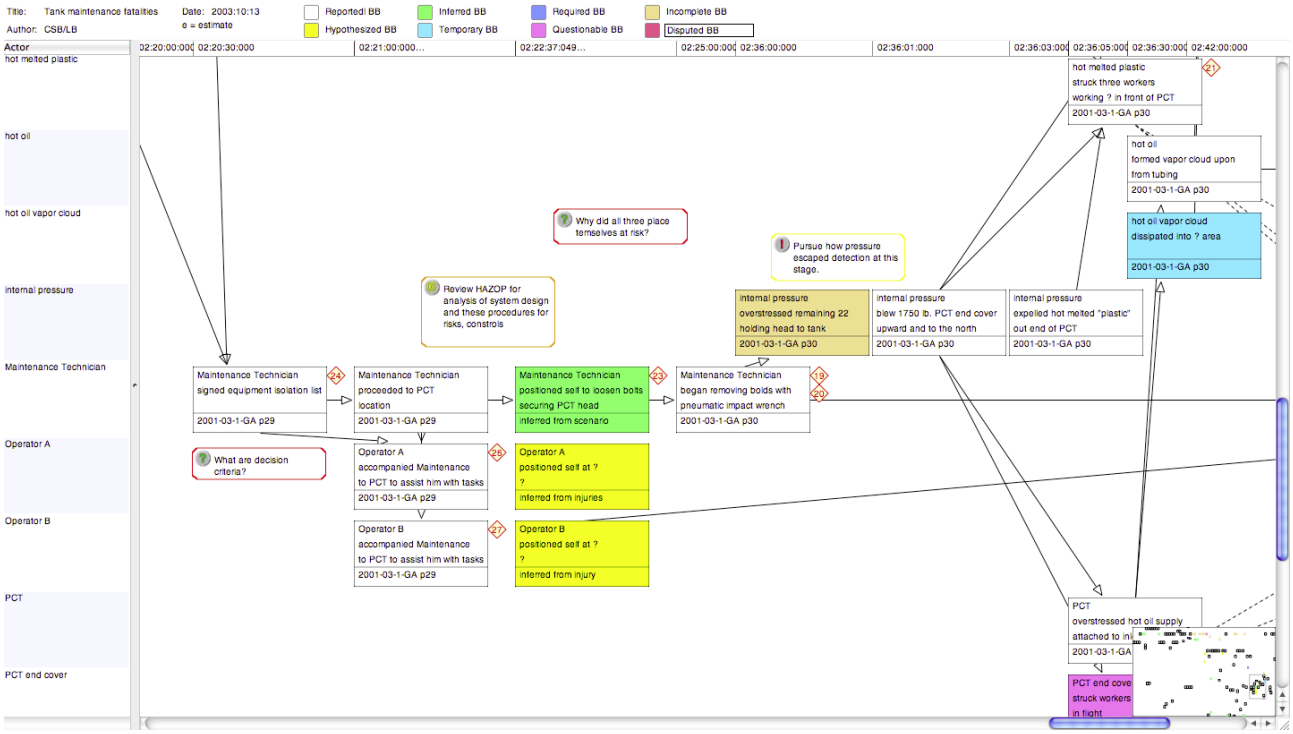


Figure 2: A Screen Shot of a Time-Actor Matrix.

Notes to Figure 2: BB colors represent "status" of BBs at this stage in the investigation. Lines represent so-called "input/output" relationships between BBs. Notes show investigation tasks still to be performed. The lower right corner is a computer-screen-navigation tool

Literature

K. Hendrick, K. and L. Benner, Jr., Investigating Accidents with STEP, Marcel Dekker, Inc., New York, NY 1986.

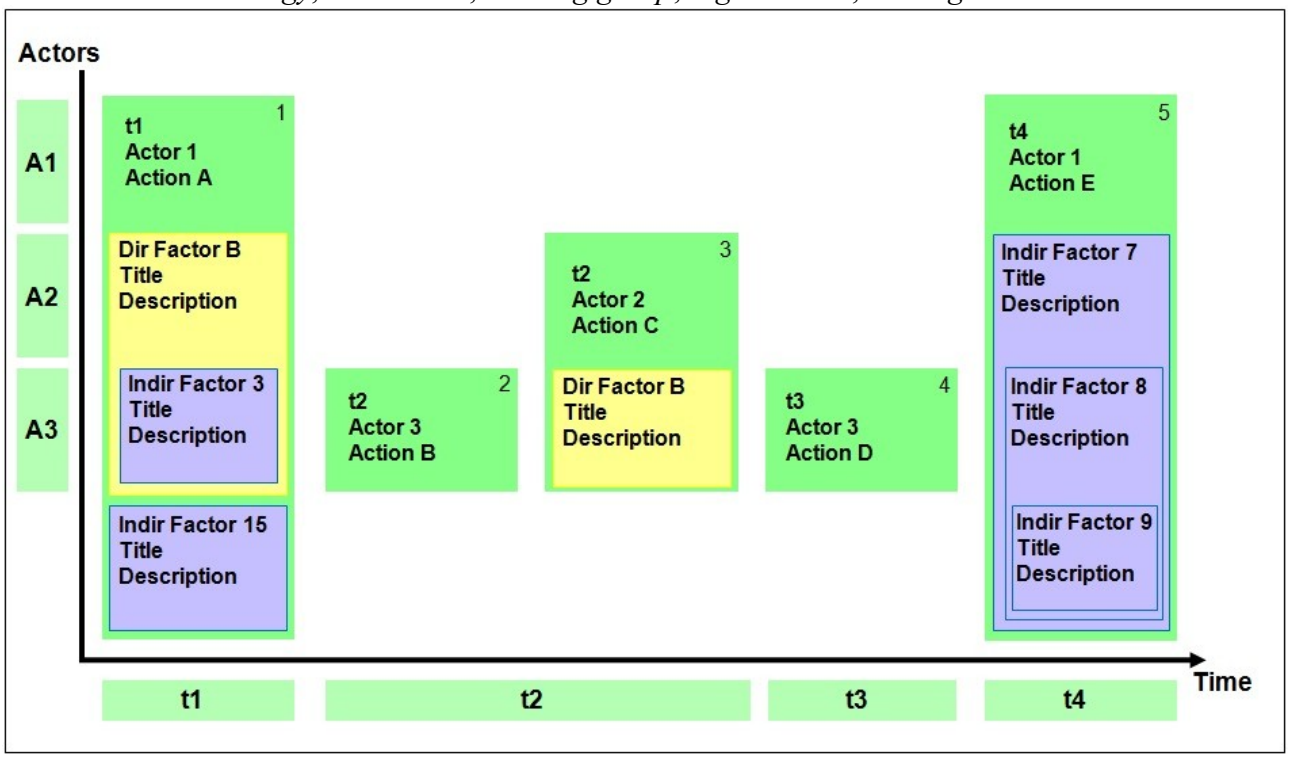
Ludwig. Benner, Jr. Accident Investigations: Multilinear Event Sequencing Methods, Journal of Safety Research 7(2):67-73, June 1975.

Ludwig Benner, Jr., Investigation Programs, in Handbook of Industrial Automation, ed. Richard L. Shell and Ernest L. Hall, Marcel Dekker, Inc., New York 2000.

4. Safety Through Organisational Learning (SOL)

Overview

SOL is an event analysis technique, which relinquishes the notion of *cause* (seen as problematic in the sociotechnical systems in which SOL is applied, largely in the nuclear-power industry) for that of *contributing factor.* The purpose of event analyses is seen to be systematic modelling of the system, identification of systemic weaknesses and improvement, and recurrence prevention. A side benefit is taken to be a deeper understanding of the system. Qualitative analysis is emphasised. Factors are classified into *technology*, *individuals*, *working group*, *organisation*, and *organisational environment*.



A Time-Actor Diagram (courtesy of SOL-VE GmbH, Berlin)

SOL proceeds first by constructing a situational description through *event building blocks* which consist of specific information concerning events constituting the situational description. The completed blocks are arranged in a *Time-Actor Diagram,* a form of graph with time along the horizontal axis and the actors along the others

Directly contributing factors are classified into i*nformation*, *communication*, *working conditions*, *personal performance*, *violations* and *technical components.* Indirectly contributing factors are classified additionally into twenty classes, which include four of these five (*technical components* is

always direct) such as *operation scheduling*, *control and supervision*, *training*, *safety principles*, *quality management*, r*egulatory bodies* and *environmental influence*.

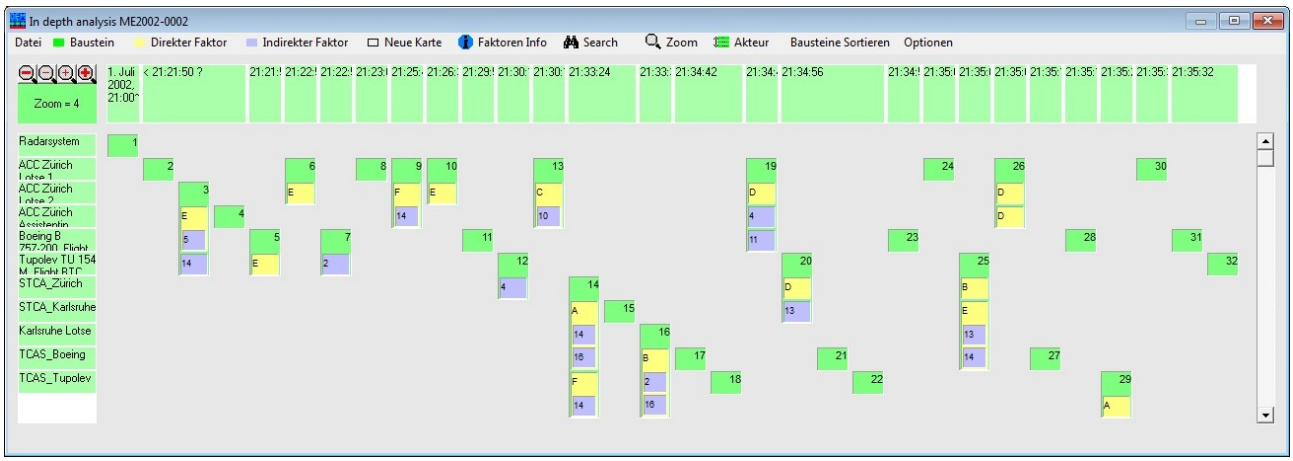
The emphasis in a SOL analysis is on organisational learning. The specific causes of a particular event are taken to be less important than the inquiry into system operations and its weaknesses, and the important conclusions are those which improve the system concerning safety.

A Information	1. Information
B Communication	2. Communication
C Working conditions	3. Working conditions
D Personal performance	4. Personal performance
E Violation	5. Violation
F Technical components	6. Operation scheduling
	7. Responsibility
	8. Control and supervision
	9. Group influence
	10. Rules, procedures and documents
	11. Qualification
	12. Training
	13. Organization and management
	14. Feedback of experience
	15. Safety principles
	16. Quality management
	17. Maintenance
	18. Regulatory and consulting bodies
	19. Environmental influence

SOL categories (from Fahlbruch and Miller, *op.cit*. Note: here only nineteen indirect contributing factors are shown; one has subsequently been added)

Directly contributing factor	points to	Indirectly contributing factor
E. Violations *"Have there been conscious violations?"*	1 3	8. Control and supervision *"Was the operators' performance not controlled or supervised sufficiently?"*
Examples are: • inappropriate transfer of processes from other situations • work performance that violates at least partly prescribed rules • inadmissible reductions during work performance • non-compliance with the safety regulations • evading of control principles ("4-eyes-principle") • ...	5 6 8 9 10 11 12 13 18	*Examples are:* • missing "4-eyes-principle" • missing protection against violations of the "4-eyes-principle" • missing control of the work by supervisors or co-workers • inadequate supervision • missing self-control of work results • attaching too much importance to work results in comparison to safe performance • ...

An Example of the Use of Leading Questions (Fahlbruch and Miller, *op.cit)*



A SOL-VE screenshot showing a question checklist (from Fahlbruch and Miller, *op.cit.*)

SOL is supported by a software tool, SOL-VE, which provides checklist-style forms for gathering information, displaying the event building blocks, and displaying the Time-Actor Diagram. The checklists consist of a series of questions which have been devised through the experience and research of the SOL authors, and the experience of the target industry, nuclear power.

Experience with SOL is that it is very helpful at generating many more factors in the course of analysis than were conceived at the start, SOL analyses generally identify many classes of contributing factors (avoiding "*mono-causal thinking*"), and generally broadens the focus on factors away from the actions of individual actors and towards more general systemic organisational and operational characteristics, which is felt to be of more help in improving the sociotechnical system.

Process

SOL has two main steps:

1. Situational description: the collection of information and the construction of "*event building blocks"*
   Situations are described through asking *When*? *Where*? *Who*? *What*? and *How*? The answers to each of these queries are guided by the use of specific formats for the information.
   Event building blocks have an identification number, and contain information on *time*, *location*, *actor*, *action* and also contain free-form additional *remarks*. The event building blocks are arranged visually on a *Time-Actor Diagram,* a two dimensional graph with time along the horizontal axis and discrete actors on the vertical axis.

2. The identification of directly and indirectly contributing factors are guided by checklists of questions, such as may be found say in lists of "frequently-asked questions" in internet-based informational material. The questions are derived from the experience of SOL's authors, who are largely organisational psychologists and organisational theorists, evolved through in-use experience in nuclear power plants.

Strengths and Limitations

Strengths.

- The checklist-question-based format of a SOL inquiry allows users who are not specialist organisational theorists or organisational psychologists to produce analyses of focus events which are useful in improving the system.

- The accuracy of SOL analyses has been improved through refinement of the checklist questions through use in the target industry.
- The emphasis on contributing factors rather than causes of a focus event allow more factors to be brought into consideration that a purely narrowly-causal analysis of the focus event might do, and thereby offer more chance of identifying possible improvements
- The format of the event building blocks gives less leeway to the judgement of individual analysts and helps to give a 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.

Limitations

- There is no specific notion of what is a cause. Similarly, what is a contributing factor is implicit in answers to the checklist-questions
- Because the analysis is driven by checklist-questions, the level of detail of an analysis is determined in advance, and cannot vary with the perceived level of explanatory need.
- The refinement of the checklist-questions has taken place in one specific industry, indeed largely in one general culture (German-speaking nuclear power operators), and may be therefore presumed culturally narrowly-focused, and less suitable for use in, say, commercial aviation accidents, which take place in a different organisational culture.

Literature

- Babette Fahlbruch, Vom Unfall zu den Ursachen, Mensch & Buch Verlag, Berlin 2000.

- B. Fahlbruch & M. Schöbel, SOL - Safety through organizational learning: A method for event analysis. Safety Science 49(1), p. 27–31, 2011.

- Stanislovas Ziedelis, Marc Noel, Comparative Analysis of Nuclear Event Investigation Methods, Tools and Techniques, Interim Technical Report EUR 24757 EN, European Commission Joint Research Center, 2011.

- Energy Institute, London, Guidance on Investigating and Analysing Human Factors and Organisational Aspects of Incidents and Accidents , London, May 2008

- Babette Fahlbruch, Rainer Miller, Safety Through Organisational Learning (SOL): an in-depth event analysis methodology, in Proceedings of the First Bieleschweig Workshop on Root Cause Analysis and Risk Analysis, http://www.rvs.uni-bielefeld.de/Bieleschweig/first/Fahlbruch_Miller_SOL-Handout.pdf , RVS Group, University of Bielefeld, 2002. Accessed on 2012.05.14.

- SOL-VE GmbH, SOL-VE OEM (Operating Experience Management). CD-Rom. Edition 05/2012. Berlin.

5. Why-Because Analysis (WBA)

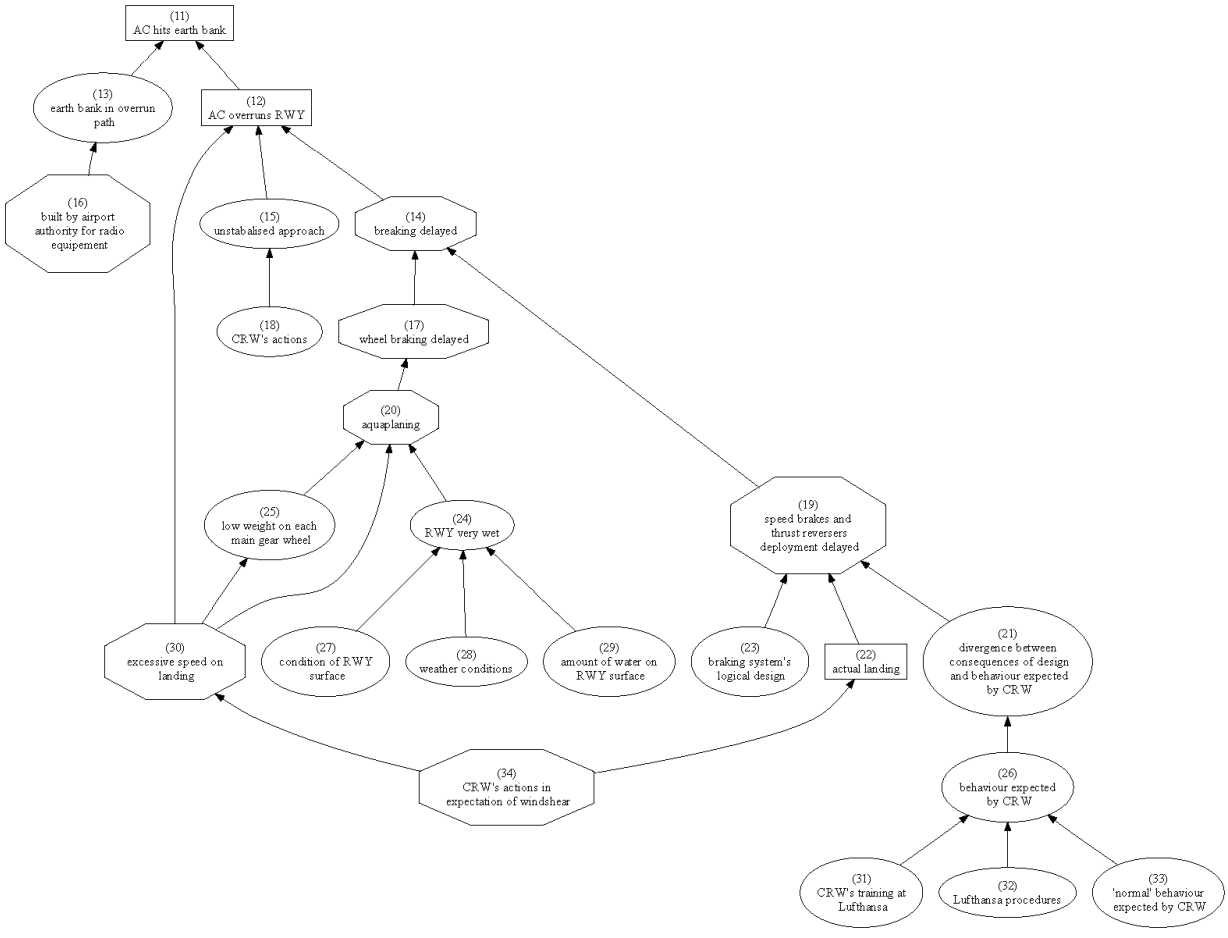
Overview

Why-Because Analysis is a causal-analytical technique for establishing which of a given collection of events and situations are (necessary) causal factors of which others. Given two events or situations in

this collection, A and B say, a condition called the Counterfactual Test is used to establish whether A is a necessary causal factor of B. The Counterfactual Test (CT) derives from the philosopher David Lewis, who himself derived it from the eighteenth-century philosopher David Hume. Lewis's causality concept is the subject of considerable contemporary academic research.

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".) When considering how the situation would have been had A not occurred, the world is taken to remain as similar as possible to the way it was, but without A occurring. If the answer is yes: B would not have occurred in this envisaged situation, then the CT succeeds and A is a necessary causal factor of B. If the answer is no: B could have happened anyway even had A not happened, then the CT fails: A is not a necessary causal factor of B. The Counterfactual Test is a precise semantic formulation of a condition used implicitly in many accident analyses.

The network of causal-factors is displayed as a Why-Because Graph (WBG), a "*directed graph*" in the language of discrete mathematics: 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.



Part of a Why-Because Graph (WBG) of a commercial-aviation runway-overrun accident

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

In order to determine whether sufficiently many 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 A and its collection of necessary causal factors as determined by the Counterfactual Test. If the CCT is not passed, then the collection of events and situations must be extended by further factors (which may not be to hand) 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 or more of A_1, A_2,...,A_n would not have occurred either.

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

WBA is supported by software, the SERAS® Analyst.

WBA is currently used primarily for the analysis of accidents in public transportation (rail and commercial air) but has also been applied in research to the analysis of process-industry accidents, in particular nuclear-reactor core-melt accidents, and computer-security incidents. WBGs for quality control within companies typically contain 10-25 nodes. WBGs displaying the results of commercial aviation accidents typically contain 30-120 nodes.

Process

The process of performing a WBA is largely as described above:

1. 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, situations.
2. Select the focus event (called in WBA the Accident Event) F.
3. Determine intuitively the immediate necessary causal factors of F from amongst the collection C; check using the Counterfactual Test. (An "immediate" factor is one for which no other factor in C lies between it and F). Display the results visually as a partial WBG.
4. Determine intuitively the necessary causal factors of those immediate factors; check using the Counterfactual Test. Extend the WBG with these factors.
5. Proceed to fill out the analysis (to extend the WBG) by testing each fact in C against the factors already in the WBG.
6. Apply the CCT to determine whether the WBG is complete, or whether factors are missing from the collection C.
7. Extend C if necessary; incorporate the new facts into the WBG using the Counterfactual Test. If insufficient information is available, assumptions may be included, providing they are clearly so labelled.
8. Finish when the CCT shows sufficient causal factors for each factor, under cognisance of the stopping rule. If insufficient facts are available, assumptions must be included in order to allow the CCT to succeed. Assumptions must, however, be clearly labelled as such.
9. If required, the WBG may be shown relatively complete through use of the causal-explanatory formal logic EL (this is rarely done except in research).

The SERAS® Analyst software supports solicitation and determination of facts, annotation of facts with sources and extended descriptions, classification into different types of facts (event, state, process, situation, assumption, etc). To be useful in industrial or legal analyses, a WBA must incorporate such "bookkeeping" functions, even if performed without help of the Analyst.

Strengths and Limitations

Strengths.

- A WBA may be performed with a minimum of training. A neophyte user of SERAS® Analyst,

which gives help on extracting facts from narrative descriptions, can typically perform a first, passable, WBA inside two hours.
- The WBG format of analysis results is easily understandable by third parties, with a few minutes of explanation
- The conceptual background required to perform a WBA is limited. An analyst must be able to apply the Counterfactual Test, and then the Causal Completeness Test.
- WBA is general; 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, EL. This renders analyses demonstrably objective (relative to the stopping rule).
- WBA can be used together with other methods; say, those providing more structure to the collection of facts.

Limitations

- It has been found to be hard for neophyte analysts to extract appropriate facts from narrative descriptions of phenomena surrounding a focus event, without guidance.
- There is only one constraint on the selection of facts, or the selection of a stopping rule, namely application of the CCT.
- There is no structuring of facts into categories, for example technical, procedural, human-factors, organisational, legal.
- Because facts are not structured, WBA provides limited guidance on countermeasures, in the case recurrence is to be prevented. Countermeasure selection usually stems from a structural evaluation of the phenomena surrounding the focus event, and WBA does not offer such a structure.

Literature

- The Why-Because Analysis Home Page http://www.rvs.uni-bielefeld.de/research/WBA accessed 2012.05.15.
- Bernd M. Sieker, The Spanair Accident at Madrid, Technical Report, Causalis Limited 2008. http://www.causalis.com/90-downloads/90-publications/SpanAir.pdf Accessed 2012.05.15. _
- Jan Sanders, Introduction to Why-Because Analysis, manuscript, 2012. http://www.rvs.uni-bielefeld.de/research/WBA/WBA_Introduction.pdf Accessed 2012.05.15.

- Peter Bernard Ladkin, Causal System Analysis, RVS e-book, University of Bielefeld 2001. http://www.rvs.uni-bielefeld.de/publications/books/CausalSystemAnalysis/index.html Accessed 2012.05.15..

- Peter Bernard Ladkin, Causal Reasoning About Aircraft Accidents, in Koornneef and van de Meulen, eds., Computer Safety, Reliability and Security, Proceedings of the 19th International Conference, SAFECOMP 2000, Lecture Notes in Computer Science No. 1943, Springer-Verlag, 2000. Also available from http://www.rvs.uni-bielefeld.de/publications/Papers/SAFECOMP2000.ps Accessed 2012.05.15.