The imperfections of accident analysis

Erik Hollnagel and Fiona Macleod

Summary

Determining the cause of an accident is a psychological (social) rather than logical (rational) process and can never be completely free of bias.

Keywords: Accident investigation, Safety–II, ETTO, resilience engineering, WAI-WAD, Work-as-imagined, Work-as-done, cognitive bias

Introduction

Most accident analyses assume that it is possible to reason backwards in time from effect(s) to cause(s) in order to implement specific remedial actions and learn the relevant lessons.

The simplicity of this way of thinking has made it attractive, but it leads to a false sense of comfort; the real world of work is too complex for such simple methods to work.

This paper presents four concepts that help us understand why simple solutions are insufficient, hence why accidents recur.

- WAI-WAD – Work As Imagined vs Work As Done
  The ideas about how work should take place may be far removed from how work actually takes place. Few tasks are performed in isolation and there is no giant rule book that covers all the interfaces and interactions.
- ETTO – Efficiency Thoroughness Trade Off
  People, individually as well as in groups, are required to balance the time and resources spent on preparing to do something against the time and resources spent on doing it. In order to carry out work, it is necessary continuously to make compromises based on the information, time and resources available in the real world.
- M&M – Methods-and-Models
  Accident analysis is usually based on pre-defined models — from falling dominos to slices of swiss cheese to the abstraction hierarchy behind STAMP (Systems – Theoretic Accident Model and Process). These models directly or indirectly provide the rationale for the methods, but are rarely visible or explicitly recognised. They are usually also linear and based on simple causality: one thing causes another. But modern process plants are complex, interlocking, intractable systems, designed and run by people — socio-technical rather than pure technical systems. Linear models are no longer adequate, nor is causal reasoning sufficient.
- WYLFIWYF – What You Look For Is What You Find
  Even though those in charge often promise "to leave no stone unturned" when accidents are investigated, there are many factors that may constrain an investigation. There may be significant time and public (political) pressure. The depth of analysis is often limited by available resources and by deadlines. And the investigation often looks for liabilities, people and organisations to blame and punish, and then accept these as causes.

  If your only tool is hammer, then everything looks like a nail[1].

Discussion

WAI (Work As Imagined) vs WAD (Work As Done)

The design, management, and analysis of work tacitly assumes that we know how things are done or should be done. The planning and management of work assumes that compliance with procedures, rules, and guidelines is sufficient to guarantee safety. The purpose of accident investigations is to understand why the outcome of a series of actions led to an unacceptable adverse event.

In reality, only in very special cases is real work completely regular or orderly and perfectly described by rules. In fact "Work to rule" has been used in the past as a form of industrial action, where employees precisely follow all written regulations to the letter in order to cause a slowdown and decrease in productivity.

Work-as-done (WAD) will always be different from work-as-imagined (WAI) because it is impossible to know in advance what the actual conditions of work will be, not least the demands and resources at the time. In general, it is inadvisable to assume that compliance guarantees safety.

In real work, people face a variety of difficulties, complexities, dilemmas and trade-offs and are called on to achieve multiple, often conflicting, goals. Safety is created at the sharp end as practitioners interact with the hazardous processes inherent in their field of activity in the face of the multiple demands and using the available tools and resources[2].It is practically impossible to provide guidelines or instructions that are detailed enough to be followed "mechanically". How work is actually done, how everyday performance is balanced and why things go right is a prerequisite for understanding what has or could go wrong.

Many things go well without being right in a more normative sense. There are degrees to "how well" something may go, and it is precisely this grey zone that is essential in the understanding of work.

The reason why everyday performance in most cases goes well is that people — and organisations — know or have learned to adjust what they do to match the actual conditions, resources, and constraints — for instance by trading off efficiency and thoroughness (ETTO)[3]. The adjustments are ubiquitous and generally useful. But the very reasons that make them necessary also means that they will be approximate rather than precise.

0260-9576/19/$17.63 + 0.00

Approximate adjustments are the reason why tasks usually go well, and things go right, but by the same token also the reason why tasks occasionally end badly and things go wrong

The conditions under which work takes place always are underspecified, hence with limited predictability. There will always be some variability in the environment, hence unexpected conditions and situations.

Things do not generally go wrong because of outright failures, mistakes, or violations. They rather go wrong because the variability of everyday performance aggregates in an unexpected manner.

WAI vs WAD – Victoria Hall

In 1883 190 children died in the Victoria Hall in Sunderland, England when the planned distribution of presents at the end of a show led to a stampede and the crushing and trampling of children by others.

Lessons from disaster – How organisations have no memory and accidents recur p137 – Trevor Kletz

WAI vs WAD – Piper Alpha No1

The permit to work procedure for Occidental North Sea Oil Rig, Piper Alpha, in Scotland had many flaws which made it impossible to follow as written. In 1988 the recommissioning of a pump still under maintenance caused a fire and explosion which led to the death of 165 men.

The failure in the operation of the permit to work system was not an isolated mistake. There were a number of respects in which the laid down procedure was not adhered to and unsafe practices were followed. One particular danger, which was relevant to the disaster, was the need to prevent the inadvertent or unauthorised recommissioning of equipment which was still under maintenance and not in a state in which it could safely be put into service. The evidence also indicated dissatisfaction with the standard of information which was communicated at shift handover.

The Public enquiry into the Piper Alpha Disaster – Lord Cullen

ETTO — Efficiency Thoroughness Trade Off

People — from regulators to financiers to designers to operators — and the organisations they work for, must make regular trade-offs between the resources they spend on preparing to do something and the resources they spend on doing it. The trade-off may favour thoroughness over efficiency if safety and quality are the dominant concerns, or efficiency over thoroughness if throughput and output are the dominant concerns. The ETTO principle states that while no activity can expect to succeed without a minimum of either, it is not possible to maximise both efficiency and thoroughness at the same time.

Efficiency here is defined as keeping the resources used to achieve a stated objective as low as possible. The resources may be expressed in terms of time, materials, money, psychological effort (workload), physical effort (fatigue), manpower (number of people), etc. For individuals, the decision about how much effort to spend is usually not conscious, but rather a result of habit, social norms, experience and established practice. For organisations, it is more likely to be the result of a direct consideration — although this choice in itself will also be subject to the ETTO principle.

Thoroughness here is defined as planning the activity to the point that it is carried out only if the necessary and sufficient conditions exist so that it will achieve its objective and not create any unwanted side-effects. These conditions comprise time, information, materials, energy, competence, tools, etc.

A perfect operation for one system (extended shift handover) often conflicts with what is safe for another (worker fatigue).

In Blink[4], Malcolm Gladwell praises "thin-slicing": the human ability to use limited information from a very narrow period of experience to reach a conclusion. He contends that sometimes having too much information can interfere with the accuracy of a judgment (analysis paralysis). Intuitive judgment is developed by experience, training, and knowledge. This "efficient" mode of operation is not without risk.

In Thinking Fast and Slow[5], Daniel Kahneman contrasts two modes of thought: "System 1" is fast, instinctive and emotional; "System 2" is slower, more deliberative, and more logical. From framing choices to people's tendency to replace a difficult question with one which is easy to answer, the book highlights the pitfalls of associating new information with existing patterns and demonstrates the need for rational, statistical analysis or "thoroughness".

In everyday life, individuals switch effortlessly between different modes of thinking: System 1-Efficient-Fast and System 2-Thorough-Slow. We all know that the perfect decision made too late is worse than an adequate decision made on time. It is only with hindsight that we tend to point the finger of blame.

The ETTO fallacy is that people are required to be both efficient and thorough at the same time — or rather to be thorough when with hindsight it was wrong to be efficient.

ETTO – a clash of priorities

A supervisor issued a permit for hot work to construct a new pipeline in a trench. Busy on a plant some distance away, a request came for a second permit to remove a slip plate to complete the emptying of the connecting line, he judged the distance between jobs to be safe and did not visit the construction site again before issuing the second permit.

Rain had left pools of water in the trench. Removal of the slip plate released a few litres of liquid hydrocarbon into the trench, which spread over the surface of the water and was ignited by the hot work 20m away, killing the man splitting the pipe.

Lessons from disaster – How organisations have no memory and accidents recur p131 – Trevor Kletz

Everyone makes daily compromises based on the information, time and resources available in the real world. The supervisor may have made the wrong judgment in prioritising the process over the inspection of the job site, but in the real world we constantly ask people to juggle multiple priorities. Adding more people is not always a solution as we still need an overall co-ordinator who understands linked activities.

0260-9576/19/$17.63 + 0.00

ETTO – Piper Alpha No 2

On Piper Alpha, maintenance supervisors were supposed to visit open jobs and discuss status face-to-face with operations at the end of the shift. However, this meeting clashed with shift handover between operating crews which took priority.

When Performing Authorities returned permits to the Control Room shortly before the end of the day-shift they would sign off all copies of the permit and leave them on the desk of the lead production operator for his subsequent attention. This was contrary to Occidental procedure which required the Performing Authority and the Designated Authority to meet. This deficient practice had developed because the lead production operators were engaged in their handover at this time.

The Public enquiry into the Piper Alpha Disaster p192 – Lord Cullen

Individual operating procedures are often written as if the people with defined roles have no other responsibilities or infinite time.

M&M – Methods-and-Models

Human beings have a basic need to feel safe, to feel that nothing can harm them physically, economically, or in other ways[6]. Because accidents take us by surprise, they are psychologically unpleasant. When something unexpected and unpleasant happens, we therefore need to restore our feeling of safety. Finding a cause has a practical value, because knowledge of the cause is seen as necessary to prevent a repeat accident. Finding a cause also has psychological value because it relieves us from the anxiety that follows the unknown.

The philosopher, Friedrich Nietzsche, wrote that to "to trace something unfamiliar back to something familiar is at once a relief, a comfort and a satisfaction, while it also produces a feeling of power. The unfamiliar involves danger, anxiety and care — the fundamental instinct is to get rid of these painful circumstances. First principle — any explanation is better than none at all."[7]

A cause is the identification, after the fact, of a limited set of aspects of the situation that are seen as the necessary and sufficient conditions for the effect(s) to have occurred. We can therefore *feel* safe if we can find an acceptable explanation for the unexpected.

As described by the causality credo[8], if outcomes can be understood in terms of cause-effect relations, then:

- an accident happens because something has failed or malfunctioned
- the causes of the failures or malfunctions can be found if enough evidence is collected
- once the causes have been found, they can be eliminated, encapsulated, or otherwise neutralised
- since all accidents have causes, and since all causes can be found, it follows that all accidents can be prevented.

And we can be safe by ensuring that nothing goes wrong. But is that possible?

According to Kahneman[5], humans often fail to take complexity into account. Their understanding of the world consists of a small and necessarily unrepresentative set of observations. Furthermore, the human mind generally does not account for the role of chance and therefore falsely assumes that a future event will mirror a past event.

The activities of modern organisations are so intertwined and complex that they can never be perfectly specified or fully controlled. Statistical process control allows us to understand the variability in technical systems, monitor trends and set acceptable limits. Should accidents, then, be treated as normal and due to common causes rather than exceptional occurrences due to assignable causes? If performance is variable does it mean that outcomes cannot be deterministic but must be probabilistic?

M&M – Human error

"Saying that an accident is due to human failing is about as helpful as saying a fall is due to gravity."

An engineer's view of human error p3 – Trevor Kletz

M&M – Design compromise

All design "...is the product of arbitrary choice. If you vary the terms of your compromise — say more speed...lower cost, then you vary the ... thing designed. It is quite impossible for any design to be "the logical outcome of the requirements" simply because the requirements being in conflict, their logical outcome is an impossibility."

David Pye quoted in "To engineer is Human – The Role of Failure in Successful Design – Henry Petroski. 1985"

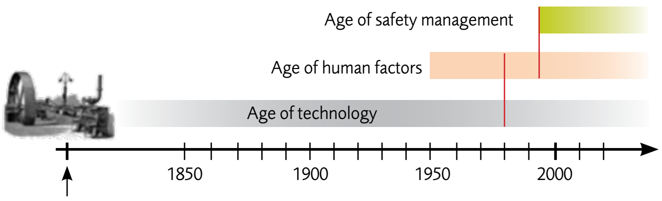
M&M – Accident Investigation methods

The new CCPS *Guidelines for investigating process safety accidents* sets out six steps for investigating process safety accidents, incidents and near misses.

"Investigations into catastrophic events have revealed something of major significance — the key to preventing disasters first lies in recognising leading indicators... By examining abnormal/upset operations, near misses and lower-consequence higher frequency occurrences, companies may identify deficiencies that, if left uncorrected, could eventually result in serious or even catastrophic events."

Guidelines for investigating process safety accidents CCPS AIChemE

WYLFIWYF – What you look for, is what you find



The assumptions about the possible causes (What-You-Look-For) will, to a large extent, determine what lessons are learned (What-You-Find). These assumptions are sometimes explicit but, in many cases, they are implicit to the investigating methods used.

We can see how these assumptions change over time.

IChemE

0260-9576/19/$17.63 + 0.00

- Age of technology — things go wrong because technology fails:
  - Accidents are the (natural) culmination of a series of events or circumstances, which occur in a specific and recognisable order due to component failures (technical, human, organisational).
  - Accidents are prevented by finding and eliminating possible causes. Safety is ensured by improving the organisation's ability to respond.
- Age of human factors — things go wrong because of human factors:
  - Accidents result from a combination of active failures (unsafe acts) and latent conditions (hazards) due to degradation of components (organisational, human, technical).
  - Accidents are prevented by strengthening barriers and defences. Safety is ensured by measuring/sampling performance indicators.
- Age of safety management — things go wrong because organisations fail:
  - Accidents result from failures of leadership.

WYLFIWYF – Bhopal

In 1984 thousands of people died and over 500,000 were injured as a result of a release of toxic gas from a pesticide plant in Bhopal, India.

Union Carbide, part owners of the Indian plant, maintained that the only possible explanation was sabotage.

The tendency of plant workers to omit facts or distort evidence was also clearly evident after the Bhopal incident, making the collection of evidence a time-consuming process. In investigating any incident in which facts seem to have been omitted or distorted, it is necessary to examine the motives of those involved. The story that had been initially told by the workers was a preferable one from their perspective, because it exonerated everyone, except perhaps the supervisor. According to this version, the reaction happened instantaneously; there was no time to take preventive or remedial measures, and there was no known cause. Without a cause, no blame could be established.

Investigation of Large Magnitude Incidents : Bhopal as a case study Ashok. S Kalelkar, Arthur D Little 1998

Although it was not known at the time, the gas was formed when a disgruntled plant employee, apparently bent on spoiling a batch of methyl isocyanate, added water to a storage tank. The water caused a reaction that built up heat and pressure in the tank, quickly transforming the chemical compound into a lethal gas that escaped into the cool night air.

Jackson Browning Report 1993 accessed via Union Carbide website http://www.bhopal.com/Cause-of-Bhopal-Tragedy

Examining the motives behind these reports is an excellent idea. Blaming a single worker for the disaster hardly exonerates the operating company, which has an absolute duty to manage its workforce and prevent harm to them and the surrounding community.

Of the four possible initiating events of the 1984 tragedy*, worker sabotage remains unproven and the least likely.

A more probable initiating event relates to the use of nitrogen to make pressure transfers of hazardous liquids after pump seals failed — a significant deviation from design with a chain of knock-on consequences**.

Regardless of the initiating event, the process safety emergency systems designed to prevent or mitigate loss of containment should never have been removed from service and the management of a facility running down to closure should be fully aware of, and in control of the hazards.

**Macleod – Impressions of Bhopal - LPB Bhopal special Issue 240 December 2004*

*** Bloch. Jung – Understanding the Impact of Unreliable Machinery – LPB Bhopal special Issue 240 December 2004*

WYLFIWYF – Chernobyl

The first investigation into the 1986 Chernobyl accident put the blame squarely on the shift operators who over-rode safety features, despite the fact that they were ordered by senior management to carry out a "safety" test outside of the safe operating envelope of the nuclear reactor.

"the accident was caused by a remarkable range of human errors and violations of operating rules in combination with specific reactor features which compounded and amplified the effects of the errors and led to the reactivity excursion."

"The operators deliberately and in violation of rules withdrew most control and safety rods from the core and switched off some important safety systems."

INSAG-1 1986 Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident of the International Atomic Energy Agency's (IAEA's) International Nuclear Safety Advisory Group

By 1992, the contribution of the RMBK design and the Man Machine Interface was recognised.

"the contributions of particular design features, including the design of the control rods and safety systems, and arrangements for presenting important safety information to the operators. The accident is now seen to have been the result of the concurrence of the following major factors: specific physical characteristics of the reactor; specific design features of the reactor control elements; and the fact that the reactor was brought to a state not specified by procedures or investigated by an independent safety body. Most importantly, the physical characteristics of the reactor made possible its unstable behaviour."

INSAG-7 1992 The Chernobyl Accident: Updating of INSAG-1,

And what of outside pressures - economic and political?

"After I had visited Chernobyl NPP I came to the conclusion that the accident was the inevitable apotheosis of the economic system which had been developed in the USSR over many decades. Neglect by the scientific management and the designers was everywhere with no attention being paid to the condition of instruments or of equipment… When one considers the chain of events leading up to the Chernobyl accident, why one person behaved in such a way and why another person behaved in another etc, it is impossible to find a single culprit, a single initiator of events, because it was like a closed circle."

Testament – Valery Legasov, - 1988, leader of the Soviet delegation to the IAEA Post-Accident Review Meeting, who committed suicide on the second anniversary of the accident.

0260-9576/19/$17.63 + 0.00

  - Accidents are prevented by strengthening safety management systems and by improving safety culture

Accident analysis is ruled by the law of reverse causality. Just as the law of causality states that every cause has an effect, the law of reverse causality states that every effect has a cause. Is it logically possible to reason backwards in time from the effect to the cause? Or does this require a deterministic world that does not really exist.

Alternative, non-linear accident models[9] propose that:

- Accidents result from unexpected combinations (resonance) of normal variability in everyday performance.
- Accidents are prevented by monitoring everyday performance (what goes right) and damping variability.
- Safety is constant vigilance and unease, the imagination to anticipate future events.

Non-linear accident models go beyond simple cause-effect and focus as much on what goes well as what goes badly. Socio-technical systems learn how to adjust in order to absorb everyday variability based on experience. Without such adjustments, systems would not work at all.

Accidents, and the human actions which are seen as causing them, can never be fully understood in isolation, in hindsight.

There are no simple "truths" or discreet causes to be found, and therefore no simple way of learning from accident investigations. Any lesson learned is limited by the assumptions on which the investigation is based.

Even very advanced methods are subject to the pressures of work and all issues may not be examined with equal thoroughness, and not all remedial actions implemented with the same enthusiasm. Some of these performance shaping factors may be systemic, resulting in investigation "blind spots"[10].

Conclusion

Can accident investigations be free from bias?

No – So long as one group of people investigate the actions of another group of people, there will always be bias, conscious or unconscious. The best we can hope for is that the composition of the inquiry panel and the terms of reference are designed to minimise bias when interpreting the findings and recommendations.

Are accident investigations worthwhile?

Yes – So long as our primary focus is on accident prevention (ensuring things go well) and we recognise the limitations of any retrospective investigation after something goes wrong, accident investigations will always be worthwhile.

- as a response to social and psychological needs, helping those affected understand the sequence of events that led up to the accident.
- as a requirement of most legal systems before prosecution of individuals or organisations.
- as a catalyst for changing regulatory framework or laws
- keeping a memorable image or story alive

Can we learn from accident investigations?

Yes – How effective are the imprecations to improve safety culture, or tighten up on management of change or permit to work systems when these things are already required by law?

Experience tells us that organisations do not learn, only individuals do[11].

And this is the reason accident investigations are worthwhile, to remind us of the human cost when things go catastrophically wrong. It is the image of a people jumping into the sea as the offshore oil rig burns behind them[12], the parent scrabbling in the grave of a child to take a last look at her face[13]. These are the things that remind us of the hazards we deal with every day. It is the recognition that the small part each of us play can, if neglected, lead to terrible consequences. It is the reminder of the relationship between the flap of a butterfly's wing and a tornado[14]. It is the sense of chronic unease[15] that makes us do our routine jobs with care and attention, as if our lives, and those of our colleagues, depended on it.

As indeed they do.

Accident investigations chronicle the stories that give us pause.

References

1. *Maslow, A. H. (1966), The Psychology of Science: A Reconnaissance by Abraham H. Maslow, Published by Harper & Row, US.*
2. *Woods, D. & Cook, R. (2002). Nine Steps to Move Forward from Error. Cognition, Technology & Work. 4. 137-144.*
3. *Hollnagel, E. (2009). The ETTO Principle: Why things that go right sometimes go wrong. Published by Ashgate Publishing Limited, UK*
4. *Gladwell, M. (2005). Blink: The Power of Thinking Without Thinking, Published by Back Bay Books, US.*
5. *Kahneman, D. (2011). Thinking, Fast and Slow, Published by Farrar, Straus and Giroux, US.*
6. *Maslow, A. H. (1943). "A theory of human motivation". Psychological Review. 50 (4): 370–396.*
7. *Nietzsche, F. (2007; org. 1895). Twilight of the Idols. Published by Wordsworth Editions, UK.*
8. *Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management.Published by CRC Press, US.*
9. *Hollnagel, E. (2012). FRAM - The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. Published by Ashgate Publishing Limited, UK.*
10. *Lundberg, J. & Josefsson, B. (2019). A Pragmatic Approach to Uncover Blind Spots in Accident Investigation in Ultra-safe Organizations - A Case Study from Air Traffic Management.*
11. *Kletz, T., (1993). Lessons from Disaster: How Organizations Have No Memory and Accidents Recur Hardcover. Published by IChemE, UK.*
12. *IChemE (2018). Piper Alpha special edition, Loss Prevention Bulletin, Issue 261.*
13. *IChemE (2014). Bhopal special edition, Loss Prevention Bulletin, Issue 240.*
14. *Lorenz, Edward N. (March 1963). Deterministic Nonperiodic Flow. Journal of the Atmospheric Sciences. 20 (2): 130–141.*
15. *HSE (2013). Process Safety – focusing on what really matters – leadership! Judith Hackitt, Speech given at Mary Kay O'Connor Process Safety Center symposium, Texas A&M University in College Station, Texas, USA, Tuesday 22nd October 2013. http://www.hse.gov.uk/aboutus/speeches/transcripts/hackitt221013.htm*

0260-9576/19/$17.63 + 0.00