On How (Not) To Learn from Accidents

Erik Hollnagel

Professor & Industrial Safety Chair
Crisis and Risk Research Centre (CRC)
MINES ParisTech
Sophia Antipolis, France
E-mail: erik.hollnagel@crc.ensmp.fr

© Erik Hollnagel, 2010
Looking for causes

If something has gone wrong (effect), we can find the cause by reasoning backwards.

But which assumptions do we make about how things work?

And what is our model of how accidents happen?

- Single causes
- Simple causes
- Belief in causality
- Technical failure
- Human failure
- Organisational failure
- “Act of god”
AF 447 – an accident without causes

Known conditions:
- Weather (thunderstorms)
- Equipment (Pitot tubes, ...)
- Culture (‘Mermoz’, ...)

Hypotheses:
- Several – plausible and implausible

Verification:
- Impossible so far
Sequential thinking (cause-effect)

Starting from the effect, you can reason backwards to find the cause.

Starting from the cause, you can reason forwards to find the effect.
If a physician heal the broken bone or diseased soft part of a man, the patient shall pay the physician five shekels in money. If he were a freed man he shall pay three shekels. If he were a slave his owner shall pay the physician two shekels.

If a physician make a large incision with an operating knife and cure it, or if he open a tumor (over the eye) with an operating knife, and saves the eye, he shall receive ten shekels in money. If the patient be a freed man, he receives five shekels. If he be the slave of some one, his owner shall give the physician two shekels.

If a physician make a large incision with the operating knife, and kill him, or open a tumor with the operating knife, and cut out the eye, his hands shall be cut off. If a physician make a large incision in the slave of a freed man, and kill him, he shall replace the slave with another slave. If he had opened a tumor with the operating knife, and put out his eye, he shall pay half his value.
Causality in complex systems

Historically, the physician-patient relation was one-to-one. The first modern hospital (The Charité, Berlin) is from 1710.
In a one-to-one relation, it makes sense to assign praise – and blame – directly to the physician.

Staff: ~ 8,000 (Rigshospitalet, 2008)
Number of bed days 322,033
Number of surgical operations 43,344
Number of outpatients 383,609
Average duration of stay 5.2 days
Does it still make sense to think of direct responsibility?
Accident investigation can be described as expressing the principle of: 
What You Look For Is What You Find (WYLFIWYF)

This means that an accident investigation usually finds what it looks for: the assumptions about the nature of accidents guide the analysis.

To this can be added the principle of WYFIWYL: What You Find Is What You Learn
<table>
<thead>
<tr>
<th>Investigation</th>
<th>Root Causes</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chemical Safety and Hazard Investigation Board (CSB), Occupational Safety and Health Administration (OSHA)</td>
<td>Technical failures and management oversights</td>
<td>+300 violations of workplace safety</td>
</tr>
<tr>
<td>BP’s Investigation of the Texas City Accident (Mogford Report)</td>
<td>Root causes, mainly human malfunctioning</td>
<td></td>
</tr>
<tr>
<td>The Stanley Report (June 15, 2005)</td>
<td>Leadership, risk awareness, control of work, workplace conditions, and contractor management.</td>
<td></td>
</tr>
<tr>
<td>The Baker Report (January, 2007)</td>
<td>Corporate safety culture, process management systems, Performance evaluation, corrective action, and corporate oversight</td>
<td></td>
</tr>
</tbody>
</table>
Regulations:
Where the employer knows or has reason to believe that an incident has or may have occurred in which a person, while undergoing a medical exposure was, otherwise than as a result of a malfunction or defect in equipment, exposed to ionising radiation to an extent much greater than intended, he shall make an immediate preliminary investigation of the incident and, unless that investigation shows beyond a reasonable doubt that no such overexposure has occurred, he shall forthwith notify the appropriate authority and make or arrange for a detailed investigation of the circumstances of the exposure and an assessment of the dose received.

Which means that
If an incident has occurred (or may have occurred), if it was not due to a malfunction of equipment, and if as a result a patient has received too great a dose of ionising radiation, then the incident shall be investigated.

Or
If an incident happens where a human error is the cause, then it shall be investigated. Otherwise it shall not.
Three types of accident models

Age of technology

1850 1900 1950 2000

Simple linear model
Independent causes,
Failures, malfunctions

Sequential

Complex linear model
Interdependent causes
(active + latent)

Epidemiological

Non-linear model
Tight couplings, coincidences,
resonance, emergence

Systemic

Age of safety management

Age of human factors

© Erik Hollnagel, 2010
Looking for technical failures
Domino thinking everywhere

- Global housing bubble collapses, massive foreclosures/debt write-off, global recession
- CPI/inflation rises, interest rates rise, housing sales fall, ARM rates re-set higher
- Foreclosures rise, inventories skyrocket, house prices fall, RE lay-offs rise
- Equity markets crash, social turmoil as budgets get slashed
- Housing prices down 20-40%, buyers vanish, unemployment 10%, trading partners enter recession
- Consumer spending contracts/recession, tax receipts fall, gov’t deficits rise, unemployment rises
- Re-fi’s/equity extraction falls, consumer spending falls, housing starts fall, prices drop, sales slow

Welke bank gaat nu voor de bijl?
De kredietcrisis maakt overal in de geldwereld slachtoffers. Centrale banken strooien met honderden miljarden, maar is het genoeg?
Looking for human failures ("errors")

Human factors "human error"

Technology

Root cause

Domino

HAZOP

Fault tree

FMECA

FMEA

Swiss Cheese

RCA, ATHEANA

HEAT

HPES

CSNI

THERP

AEB

HERA

TRACEr


© Erik Hollnagel, 2010
**MTO digram**

- **Nylon sling**
  - Weight: 8 tons

- **Load lifted** → **Sling broke** → **Load swung** → **Pipe hit operator** → **Operator head injuries**

  - **Sling damaged**
    - **No pre-work check**

  - **Operator crossed barrier**
    - **Instructions not followed**
      - **Breach of rules accepted**
        - **Barrier ignored**
          - **Lack of SJA and checks**

- **Causal analysis**
- **Barrier analysis**

© Erik Hollnagel, 2010
Three types of accident models

- **Age of technology**
  - **1850**: Simple linear model, independent causes, failures, malfunctions
  - **1900**: Complex linear model, interdependent causes (active + latent)
  - **1950**: Non-linear model, tight couplings, coincidences, resonance, emergence
  - **2000**: Sequential, epidemiological, systemic

- **Age of human factors**
  - Certification

- **Age of safety management**
  - FAA, mechanics, high workload, grease, lubrication, maintenance oversight

- **Horizontal stabilizer movement**
  - Jackscrew up-down movement

- **Expertise**
  - Controlled stabilizer movement

- **Aircraft design knowledge**
  - Aircraft pitch control, limiting, controlled stabilizer movement

- **Limited stabilizer movement**
  - Aircraft design knowledge, procedures, procedures

- **Limiting stabilizer movement**
  - Aircraft design knowledge, procedures, procedures

- **Allowable end-play checking**
  - Jackscrew replacement, excessive end-play

- **Three types of accident models**
  - Complex linear model, interdependent causes (active + latent)
  - Simple linear model, independent causes, failures, malfunctions
  - Non-linear model, tight couplings, coincidences, resonance, emergence

© Erik Hollnagel, 2010
Looking for organisational failures

Technology

Organisation

Human factors "human error"


Root cause

Domino FMEA Fault tree HAZOP THERP CSNI MORT MERMOS

FMECA

HEAT

HPES

STEP

HCR

RCA, ATHEANA TRIPOD MTO

Swiss Cheese AEB HERA AcciMap

CREAM FRAM STAMP

Technology

Human factors "human error"

Organisation

Root cause
Models of organisational “failures”
“On the whole, we have complex systems because we don’t know how to produce the output through linear systems.”
Coupling and interactiveness

Complex systems / interactions:
- Tight spacing / proximity
- Common-mode connections
- Interconnected subsystems
- Many feedback loops
- Indirect information
- Limited understanding

Tight couplings:
- Delays in processing not possible
- Invariant sequence
- Little slack (supplies, equipment, staff)
- Buffers and redundancies designed-in
- Limited substitutability
Traffic and randomness

Traffic is a system in which millions of cars every day move so that their driving paths cross each other and critical situations arise due to pure random processes:
cars meet with a speed difference of 100 to more than 200 km/h, separated only by a few meters, with variability of the drivers’ attentiveness, the steering, the lateral slope of the road, wind and other factors.

Drivers learn by experience the dimensions of the own car and of other cars, how much space is needed and how much should be allocated to other road users, the maximum speed to approach a curve ahead, etc. If drivers anticipate that these minimum safety margins will be violated, they will shift behavior.

The very basis of traffic accidents consists of random processes, of the fact that we have complicated traffic system with many participants and much kinetic energy involved.

When millions of drivers habitually drive at too small safety margins and make insufficient allowance for (infrequent) deviant behavior or for (infrequent) coincidences, this very normal behavior results in accidents.

Summala (1985)
As the analysis shows there is no root cause. Deeper investigation would most probably bring up further contributing factors. A set of working methods that have been developed over many years, suddenly turn out as insufficient for this specific combination of circumstances.

The change of concept was created from the uncertainty of the outcome of the original plan that had been formed during a sector handover. The execution of this and the following concepts were hampered by goal conflicts between two sectors. Time- and environmental- constraints created a demand resource mismatch in the attempt to adapt to the developing situation. This also included coordination breakdowns and automation surprises (TCAS). The combination of this and further contributing factors of which some are listed above, lead to an airprox with a minimum separation of 1.6NM/400 ft.
Coupling and complexity anno 2010

- Tight
  - Dams
  - NPPs
  - Financial markets
- Coupling
  - Marine transport
  - Chemical plants
  - Air traffic control
- Loose
  - Religious activities
  - Post offices
  - Manufacturing
- Manageability
  - Emergency department
  - Integrated operations
  - Health care
  - Universities
- Low (intractable)
  - Railways
  - Space missions
  - Public services
  - Assembly lines

© Erik Hollnagel, 2010
Non-linear accident models

Accident models go beyond simple cause-effect relations. Accidents result from alignment of conditions and occurrences. Human actions cannot be understood in isolation.

Causes are not found but constructed. More important to understand nature of system dynamics (variability) than to model individual technological or human failures.

Systems try to balance efficiency and thoroughness. System as a whole adjusts to absorb normal performance adjustments (dynamic accommodation) based on experience.

Accidents are emergent. Accidents are consequences of normal adjustments, rather than of failures. Without such adjustments, systems would not work.
Why only look at what goes wrong?

Safety = Reduced number of adverse events.

Focus is on what goes wrong. Look for failures and malfunctions. Try to eliminate causes and improve barriers.

Safety and core business compete for resources. Learning only uses a fraction of the data available.

10^4 := 1 failure in 10,000 events

Safety = Ability to succeed under varying conditions.

Focus is on what goes right. Use that to understand normal performance, to do better and to be safer.

1 - 10^4 := 9,999 non-failures in 10,000 events

Safety and core business help each other. Learning uses most of the data available.

© Erik Hollnagel, 2010
Range of event outcomes

- **Normal outcomes (things that go right)**
- **Near misses**
- **Mishaps**
- **Accidents**
- **Incidents**
- **Disasters**
- **Good luck**
- **Serendipity**

Outcome vs. Predictability:

- **Very low**
- **Very high**

Diagram by Erik Hollnagel, 2010
Frequency of event outcomes

Outcome

Serendipity

Normal outcomes (things that go right)

Good luck

Near misses

Accidents

Incidents

Mishaps

Disasters

Positive

Neutral

Negative

Very low

Very high

Predictability

© Erik Hollnagel, 2010
More safe or less unsafe?

Outcome

Positive

Serendipity

Normal outcomes (things that go right)

Unsafe Functioning (invisible)

Good luck

Unsafe Functioning (visible)

Neutral

Disasters

Incidents

Near misses

Negative

Mishaps

Very low

10^6

Very high

Predictability

© Erik Hollnagel, 2010
What does it take to learn?

Opportunity (to learn): Learning situations (cases) must be frequent enough for a learning practice to develop.

Comparable / similar: Learning situations must have enough in common to allow for generalisation.

Opportunity (to verify): It must be possible to verify that the learning was ‘correct’ (feedback).

The purpose of learning (from accidents, etc.) is to change behaviour so that certain outcomes become more likely and other outcomes less likely.
What can we learn?

- Generalise across cases
- Look for patterns and relations
- “Translate” into technical terms
- Aggregate raw data

Models and theories

Empirical data

- Raw data ('facts,' observations)
- Organised data (timeline)
- Analysed data (technical report)
- Interpreted data (causes)
- Generic 'mechanisms'

© Erik Hollnagel, 2010
<table>
<thead>
<tr>
<th>Type of event</th>
<th>Frequency, characteristics</th>
<th>Aetiology</th>
<th>Transfer of learning, (verifiable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare events (unexampled, irregular)</td>
<td>Happens exceptionally, each event is unique</td>
<td>Emergent rather than cause-effect</td>
<td>Very low, comparison not possible</td>
</tr>
<tr>
<td>Accidents &amp; incidents</td>
<td>Happens rarely, highly dissimilar</td>
<td>Causes and conditions combined</td>
<td>Very low, comparison difficult, little feedback</td>
</tr>
<tr>
<td>Successful recoveries (near misses)</td>
<td>Happens occasionally, many common traits</td>
<td>Context-driven trade-offs.</td>
<td>Low, delayed feedback</td>
</tr>
<tr>
<td>Normal performance</td>
<td>Happens all the time, highly similar</td>
<td>Performance adjustments</td>
<td>Very high, easy to verify and evaluate</td>
</tr>
</tbody>
</table>
Thank you for your attention