Resilience Engineering: Concepts and philosophy

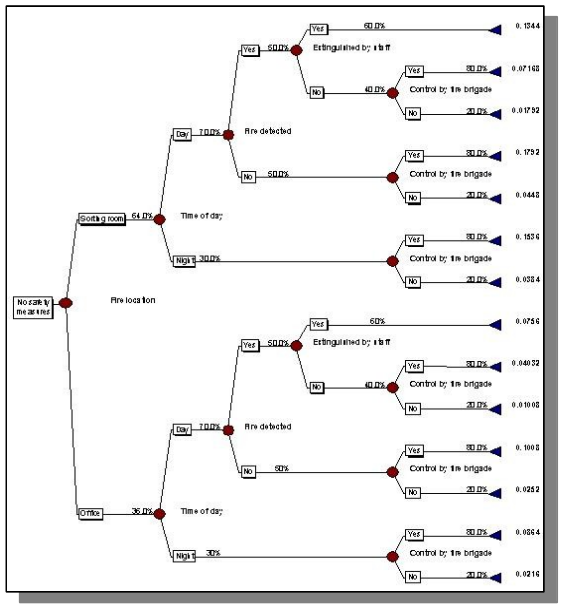
Erik Hollnagel

Professor &
Industrial Safety Chair
MINES ParisTech
Sophia Antipolis, France

Professor II
NTNU
Trondheim, Norge

E-mail: erik.hollnagel@gmail.com

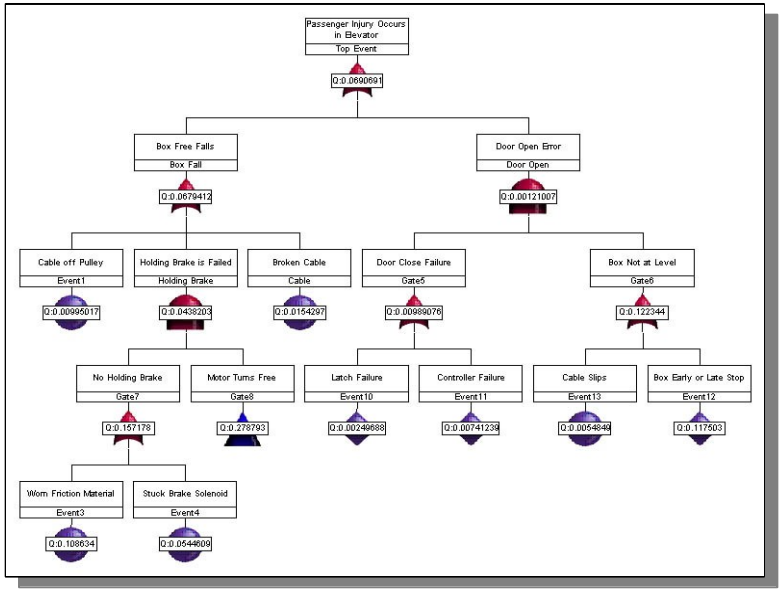
Common assumptions



System can be decomposed into meaningful elements (components, events)

The function of each element is bimodal (true/false, work/fail)

The failure probability of elements can be analysed/described individually

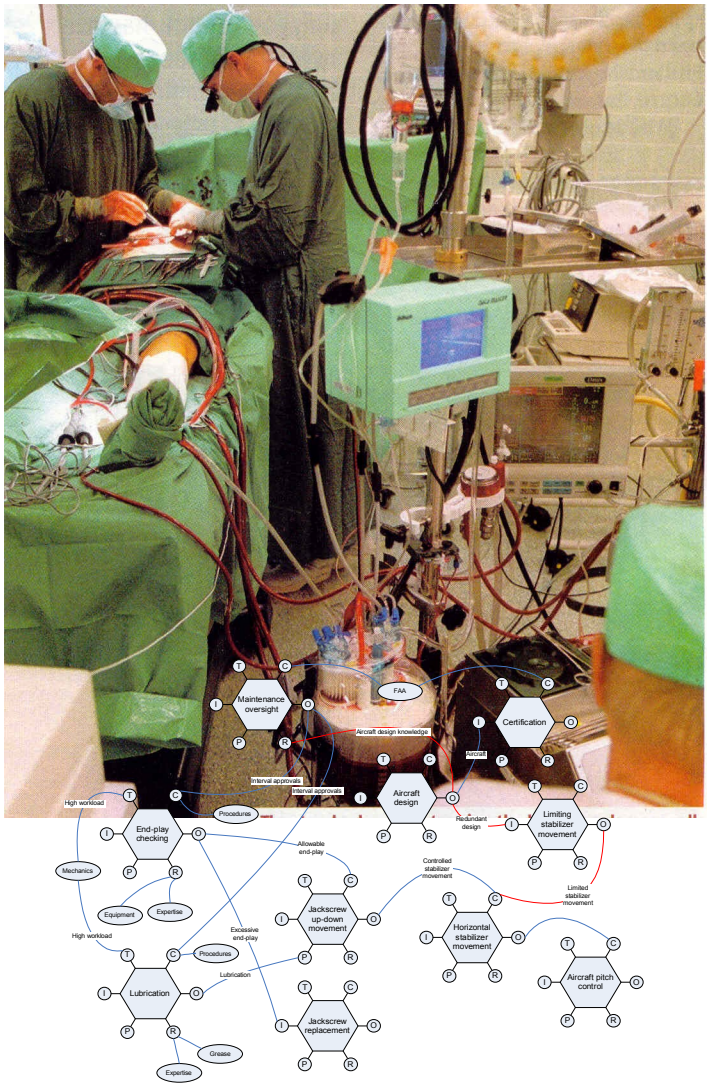


The order or sequence of events is predetermined and fixed

When combinations occur they can be described as linear (tractable, non-interacting)

The influence from context/conditions is limited and quantifiable

Revised assumptions - 2010



Systems cannot be decomposed in a meaningful way (no natural elements or components)

The function of the system is not bimodal, but normal performance is – and must be – variable.

Outcomes are determined by performance variability rather than by (human) failure probability. Performance variability is a source of success as well as of failure.

While some adverse events can be attributed to failures and malfunctions of normal functions, others are best understood as the result of combinations of variability of normal performance.

Risk and safety analyses should try to understand the nature of variability of normal performance and use that to identify conditions that may lead to both positive and adverse outcomes.

Premises for resilience engineering (1)

Traditional safety practices	Resilience engineering
Performance conditions can completely specified. Safety can be achieved by compliance to rules and procedures, and failure to do so constitutes a source of risk. Performance variability is a threat, and should be constrained as far as possible.	Performance conditions are always underspecified. Individuals and organisations must always adjust what they do to match current demands and resources. Since resources and time are finite, such adjustments will inevitably be approximate.
Adverse events can be attributed to failure or malfunctioning of components. All possible risks can be identified by determining out how components can fail and how failures can combine.	While many adverse events can be attributed to failure or malfunctioning of components, many cannot. These events can be understood as the result of unexpected combinations of performance variability

Premises for resilience engineering (2)

Traditional safety practices	Resilience engineering
Safety management can be based on error tabulation and the calculation of failure probabilities. The purpose of safety management is to respond appropriately to reported adverse events.	Safety management cannot be based on hindsight, nor rely on error tabulation and the calculation of failure probabilities. Safety management must be proactive as well as reactive.
Safety is an important issue in its own right. Safety is the highest priority of a system and must not be compromised by productivity and efficiency concerns.	Safety cannot be isolated from the core (business) process, nor vice versa. Safety is the prerequisite for productivity, and productivity is the prerequisite for safety. Safety is achieved by improvements rather than by constraints.

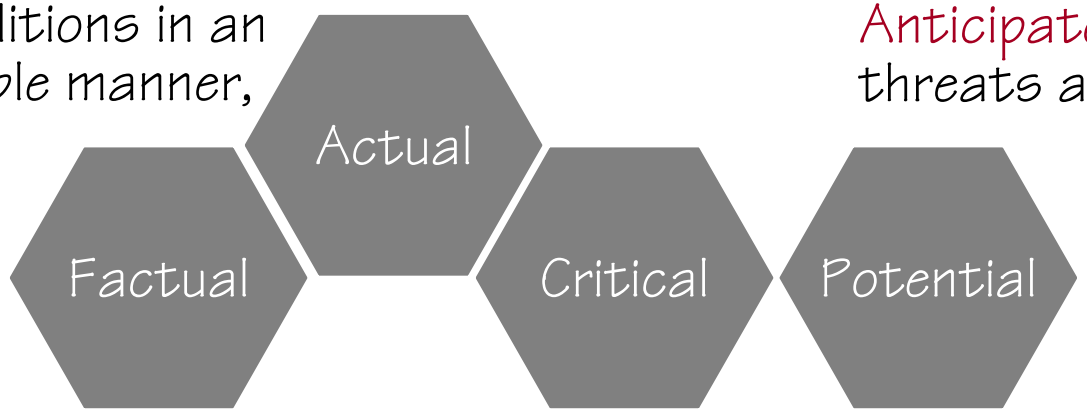
Resilience and safety management

Resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

A practice of Resilience Engineering / Proactive Safety Management requires that all levels of the organisation are able to:

Respond to regular and irregular conditions in an effective, flexible manner,

Anticipate long-term threats and opportunities

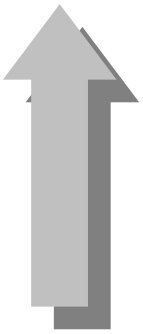


Learn from past events, understand correctly what happened and why

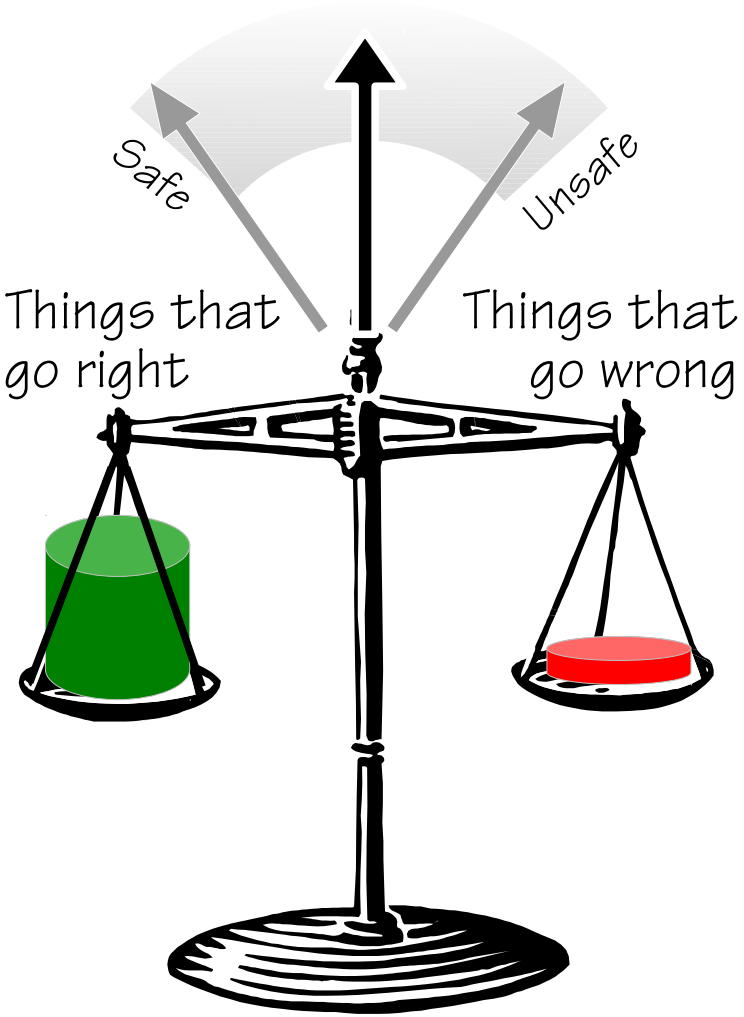
Monitor short-term developments and threats; revise risk models

Engineering resilience

Solution: Enhance the abilities to respond, monitor, anticipate and learn



The goal of resilience management is to increase the number of things that go right.



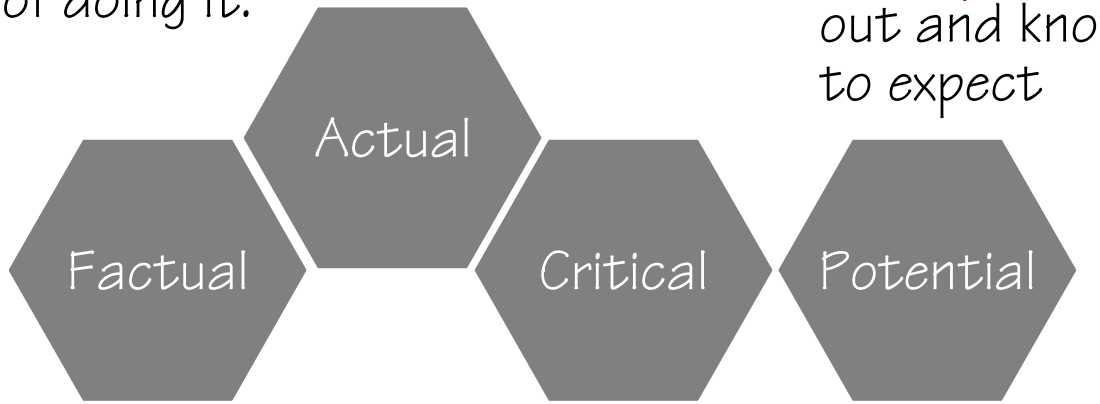
The goal of safety management is to reduce the number of things that go wrong.

Solution: Constrain performance by rules, procedures, barriers, and defences.

Designing for resilience

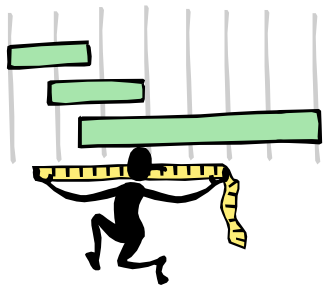
Responding: Knowing what to do, being capable of doing it.

Anticipating: Finding out and knowing what to expect



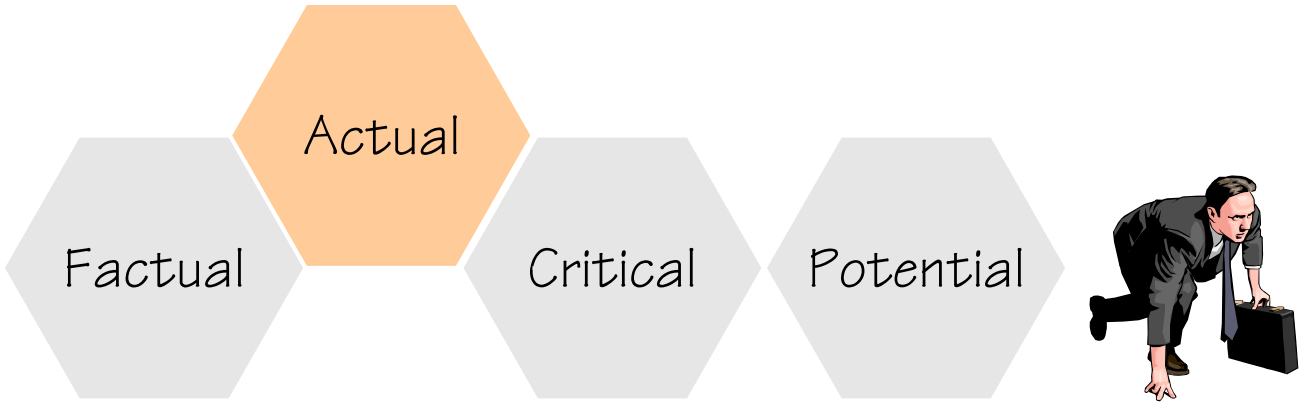
Learning: Knowing what has happened

Monitoring: Knowing what to look for (indicators)



An increased availability and reliability of functioning on all levels will not only improve safety but also enhance control, hence the ability to predict, plan, and produce.

The ability to respond (actual)



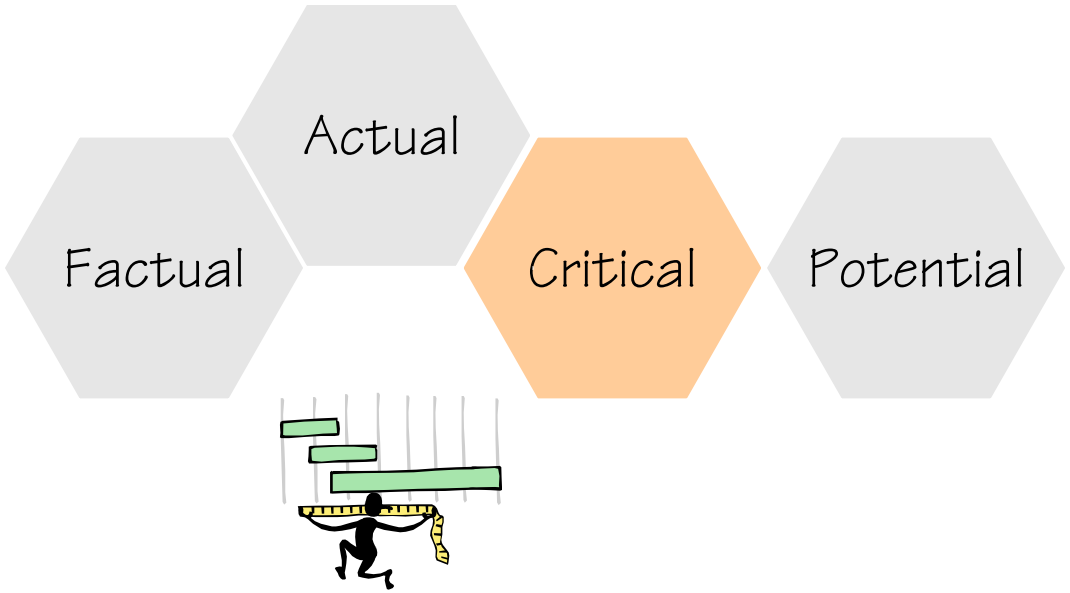
What	For which events is there a response ready?
	How was the list of events created?
	When – and why – is the list revised?
When	What is the threshold of response?
	How soon can a response been given?
	How long can it be sustained?
How	How was the type of response determined?
	How many resources are allocated to response readiness?
	How is the readiness verified or maintained?

BP Deepwater Horizon, April 20, 2010

On April 20, 2010, an explosion occurred on the rig and she caught fire. The rig was in the final phases of drilling a well in which casing is cemented in place, reinforcing the well. 7 workers were taken to the hospital, but 11 people are missing.

The Blowout Preventers or BOPs are controlled with redundant systems from the rig. In the event of a serious emergency, they should be engaged manually or automatically when something of this proportion breaks out. None of them were apparently activated. Deepwater Horizon sank on April 22, 2010, in water approximately 5,000 feet deep, and has been located on the seafloor about 1/4 mile NW of the well.

The ability to monitor (critical)



How have the indicators been defined? (Articulated vs. "common sense")?
How, and when, are they revised?
How many are leading indicators and how many are lagging?
How are the "measurements" made? (qualitative, quantitative)
When are the measurements made (continuously, regularly)?
What are the delays between measurement and interpretation?
Are effects transient or permanent?

The ability to monitor – which indicators?

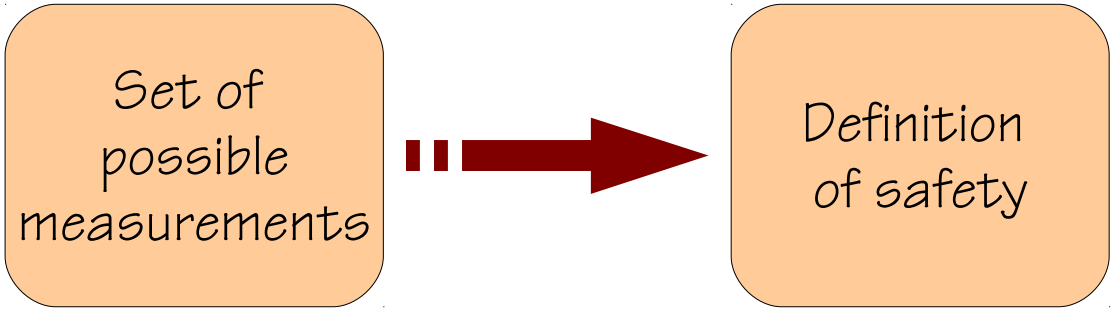
	Weight	Safety
Goal	Well-defined, operational	Loosely defined, "conceptual"
Measurement	Simple, direct	Complex, indirect, lagging
Instrument	Simple, reliable	Multiple, not well calibrated
Interpretation	Simple, relative to own standard	Complex, subjective
Means	Well-known (lose weight)	Traditional, but uncertain value

The ability to monitor – which indicators?

Patient Safety Indicators are defined as 'a set of measures (of) adverse events that patients experience as a result of exposure to the health care system.'

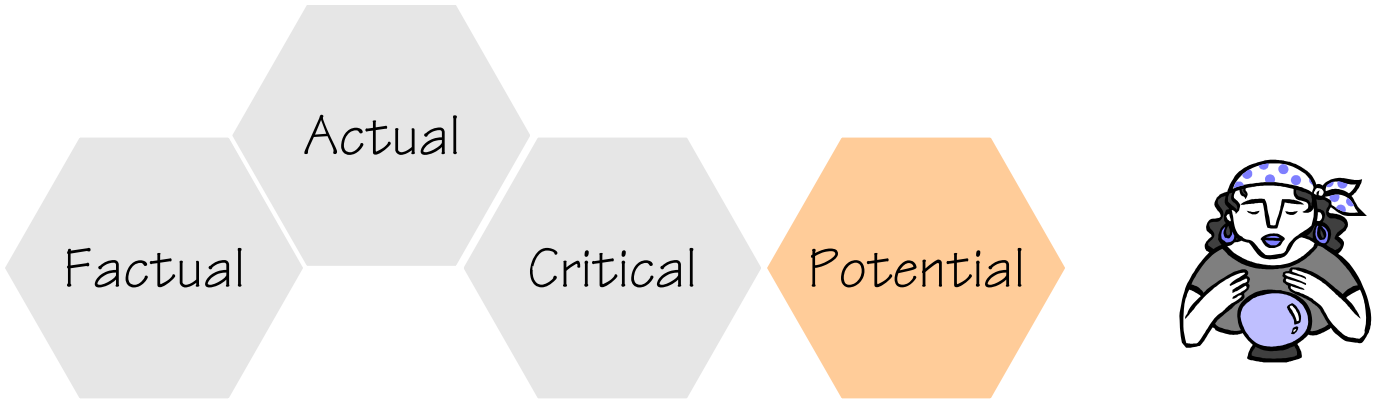
Catheter-related bloodstream infection
Decubitus ulcer
Complications of anaesthesia
Postoperative hip fracture
Postoperative pulmonary embolism (PE) or deep vein thrombosis (DVT)
Postoperative sepsis
Accidental puncture or laceration
Postoperative respiratory failure
Iatrogenic pneumothorax
Transfusion reaction
Foreign body left in during procedure
Birth trauma - injury to neonate
Obstetric trauma – vaginal delivery with instrument
Obstetric trauma – vaginal delivery without instrument
Obstetric trauma - caesarean section

Safety is defined by its phenomenology, i.e., by what it is possible to measure.



Ensuring patient safety "involves the establishment of operational systems and processes that minimize the likelihood of errors and maximizes the likelihood of intercepting them when they occur."

The ability to look ahead (potential)



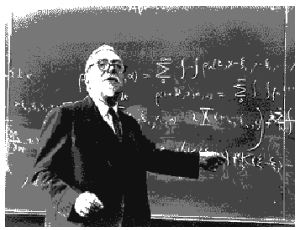
What is the implicit/explicit "model" of the future?
How long is the organisation willing to look ahead ("horizon")?
How many efforts are allocated to looking ahead?
What risks are the organisation willing to take?
Who believes what and why?

The ability to anticipate

The future is a "mirror" image of the past (repetition, extrapolation)

The future is described as a (re)combination of past events and conditions.

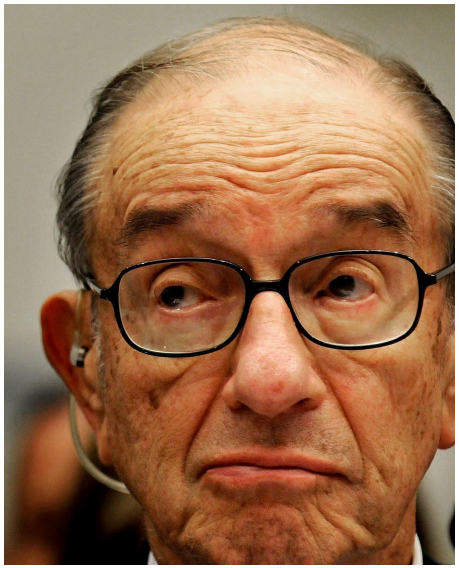
The future has not been seen before. It involves a combination of known performance variability, that usually is seen as irrelevant for safety

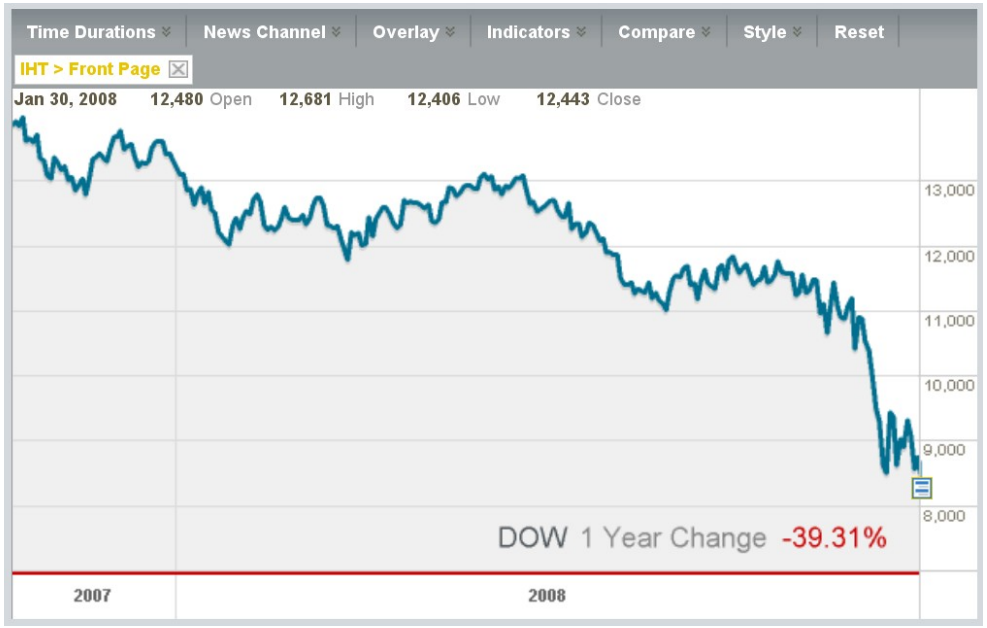


The present is unlike the past, and the future is unlike the present (Wiener, 1956)

Financial crisis of 2008

Partially … I made the mistake in presuming that the self-interest of organisations, specifically banks, is such that they were best capable of protecting shareholders and equity in the firms … I discovered a flaw in the model that I perceived is the critical functioning structure that defines how the world works. I had been going for 40 years with considerable evidence that it was working exceptionally well.





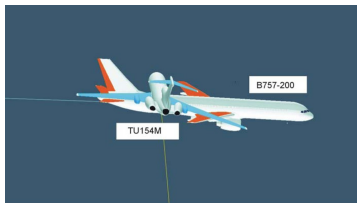
.. once-in-a-century credit tsunami, … that … turned out to be much broader than anything I could have imagined.
Alan Greenspan, Guardian, October 24, 2008

Three categories of threats (Westrum)

I: Regular threats

Events that occur so often that the system can learn how to respond.
E.g., medication errors that only implicate a single patient, and potentially can be brought under control.
Solutions can be based on standard responses

II: Irregular threats

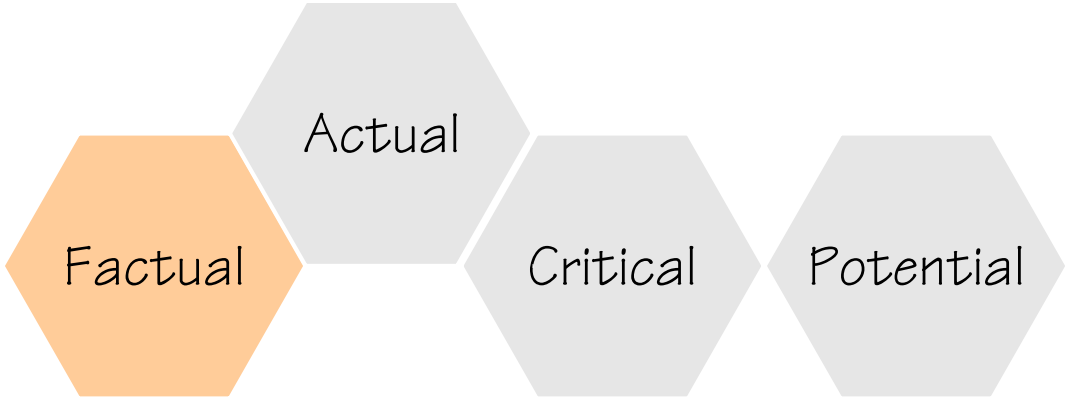


One-off events, but so many and so different that it is practically impossible to provide a standard response. They are often unexpected although they are imaginable. (E.g., Apollo 13)
Solutions require flexibility and improvisation.

III: Unexampled events

Events that are virtually impossible to imagine and which exceed the organisation's collective experience.
(E.g. Chernobyl, 9/11, Financial crisis 2007-2008)
Solution requires the ability to re-organize and revise goals.

The ability to learn (factual)



What is the learning based on (successes – failures)?
When does learning take place (continuously or event-driven)?
What is the nature of learning (qualitative, quantitative)?
What is the target of learning (individuals, organisation)?
How are the effects of learning verified and maintained?

WYLFIWYF

Accident investigation can be described as expressing the principle of:
What You Look For Is What You Find (WYLFIWYF)

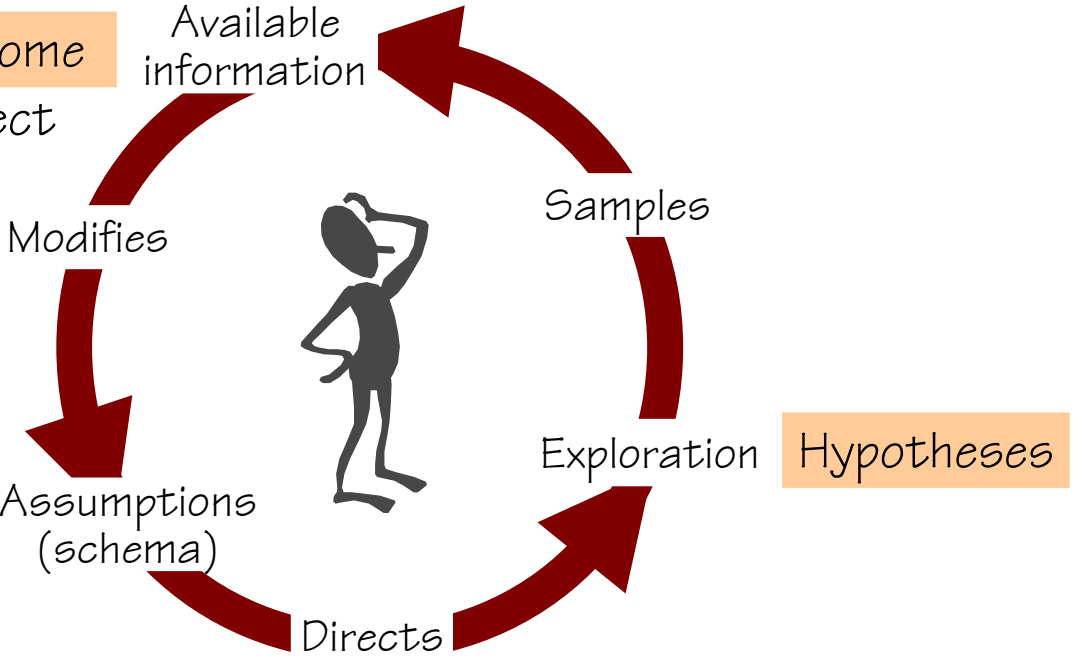
This means that an accident investigation usually finds what it looks for: the assumptions about the nature of accidents guide the analysis.

Accident → Outcome

Cause — Effect

Human error
Latent conditions
Root causes
Technical malfunctions
Maintenance
Safety culture
...

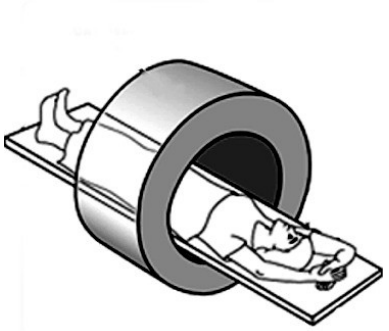
'Causes'



To this can be added the principle of WYFIWYL: What You Find Is What You Learn

From words to deeds

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.

The ability to learn

Chemical Safety and Hazard Investigation Board (CSB),	Technical failures and management oversights
Occupational Safety and Health Administration (OSHA)	+300 violations of workplace safety
BP'S Investigation of the Texas City Accident (Mogford Report)	Root causes, mainly human malfunctioning
The Stanley Report (June 15, 2005)	Leadership, risk awareness, control of work, workplace conditions, and contractor management.
The Baker Report (January, 2007)	Corporate safety culture, process management systems, Performance evaluation, corrective action, and corporate oversight

BP Texas City, March 23 2005

Baker panel: recommendations

Improve	Process safety leadership
Establish	Integrated and comprehensive process safety management system
Develop and implement	Process safety knowledge and expertise
Develop	Process safety culture
Provide	Clearly defined expectations and accountability for process safety
Provide	Support for line management
Develop, implement, maintain and update	Leading and lagging performance indicators for process safety
Establish and implement	Process safety auditing
Provide – for five years	Board monitoring
Become	Industry leader in process safety management

From recommendations to reality

Baker panel report (January, 2007):
Become industry leader in process safety management

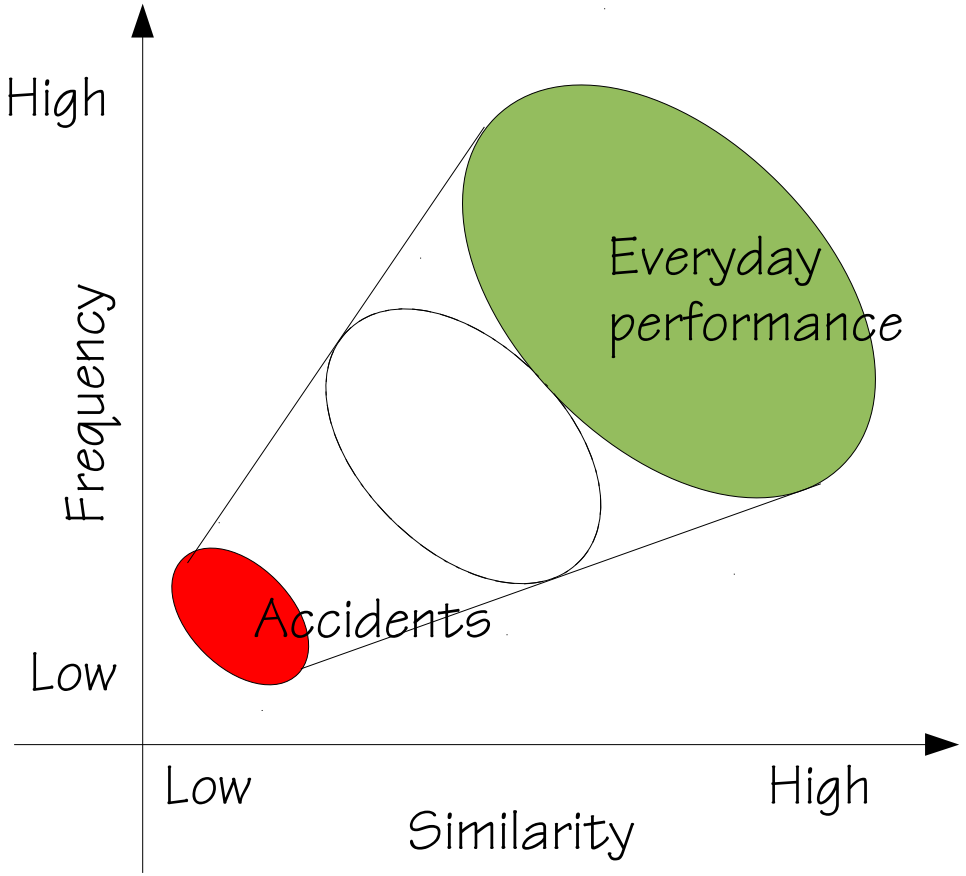
Tony Hayward, BP CEO (Interview in Financial times, October 2007)
So we want to get back to leading the industry. We aren't today because our financial performance is poor. ... The issue is one of leadership. You can't lead the industry if your financial performance isn't leading the industry. ... It starts with, we're in the business of business.

(2010), BP's first-quarter replacement cost profit was $5,6 billion, compared with $2,4 billion in 2009, an increase of 135%.

April 20-22, 2010. Blowout at BP operated Deepwater Horizon rig, which explodes and sinks. Total costs > 30 billion USD. Largest oilspill ever in the USA.

July 27, 2010. Tony Hayward resigns as CEO of BP.
BP's second-quarter loss was $17 billion. Company shares have dropped from 690p to 402p (lowest was ~300p).

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 You Find Is What You Learn

Type of event	Frequency, characteristics	Aetiology	Transfer of learning, (verifiable)
Rare events (unexampled, irregular)	Happens exceptionally, each event is unique	Emergent rather than cause-effect	Very low, comparison not possible
Accidents & incidents	Happens rarely, highly dissimilar	Causes and conditions combined	Very low, comparison difficult, little feedback
Successful recoveries (near misses)	Happens occasionally, many common traits	Context-driven trade-offs.	Low, delayed feedback
Normal performance	Happens all the time, highly similar	Performance adjustments	Very high, easy to verify and evaluate

Conclusions so far ...

- Resilience is the ability to succeed under expected and unexpected conditions, rather than the ability to avoid failure.
- Resilience can be analysed in terms of four main abilities:
  - The ability to respond
  - The ability to monitor
  - The ability to anticipate
  - The ability to learn
- The four abilities also provide a basis for concrete proposals on how to engineer (and improve) the resilience of a system.