Safe
tySyn
thesis

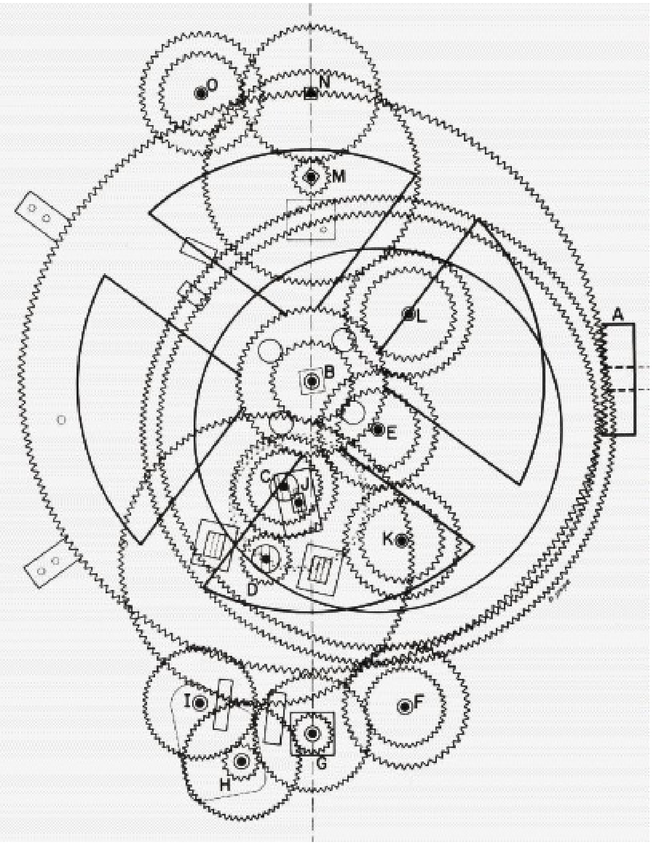
# Understanding How Something Happens – When It Works And When It Fails

Erik Hollnagel

Professor, University of Southern Denmark
Chief Consultant Center for Quality, RSD (DK)

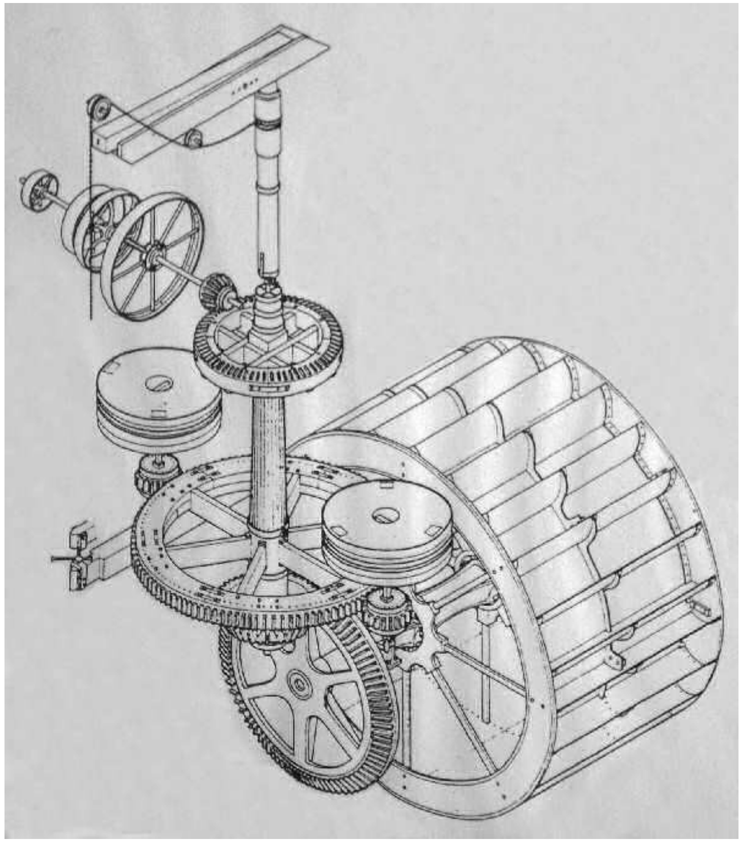
hollnagel.erik@gmail.com

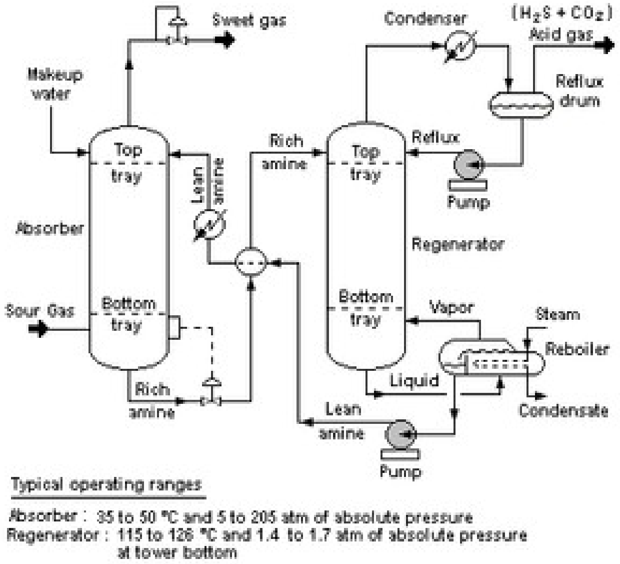
# Understanding simple systems



Antikythera mechanism, (150-100 BC)

We can explain how things work in terms of cause-effect relations





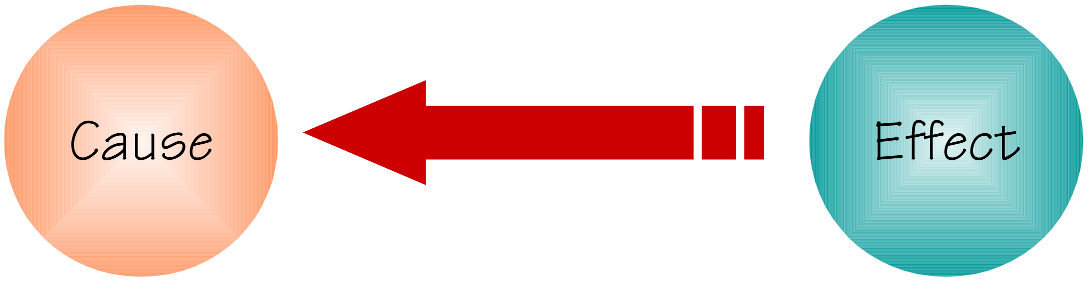
Typical operating ranges

Absorber : 35 to 50 °C and 5 to 205 atm of absolute pressure
Regenerator : 115 to 126 °C and 1.4 to 1.7 atm of absolute pressure at tower bottom

We can therefore understand risks in the same way: as cause-effect chains starting from a component failure.

# Reverse causation

Then we can
find out what
this is!

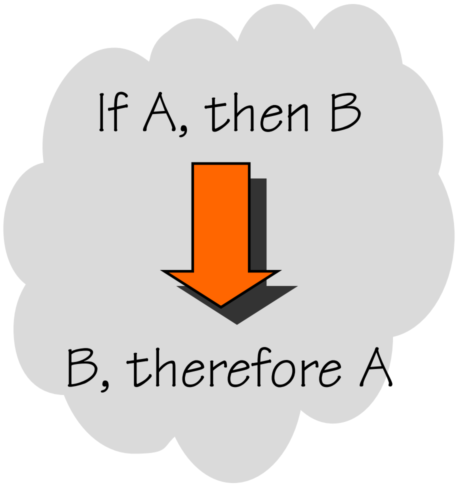


If we can see
what this
is ...

Every event (effect) has a prior cause

Humans are prone to reason in ways that are not logically valid.

(Affirming the consequent.)



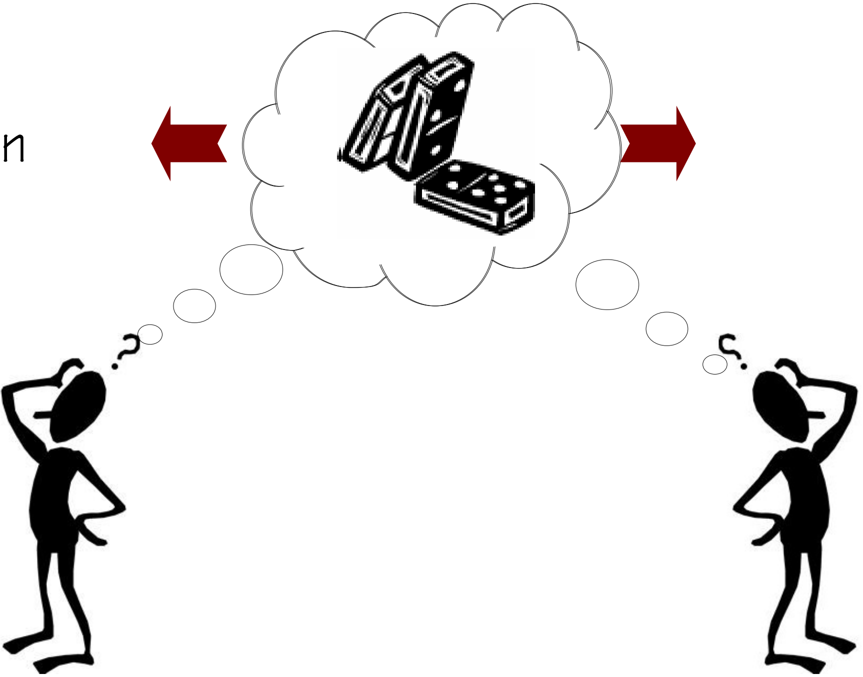
Sequentiality in a description is partly an artefact of time being one-dimensional.

# Simple, linear model (cause-effect chain)

Simple linear models
(cause-effect chains)

If accidents are the culmination of a chain of events ...

... then risks can be found as the probability of component failures



Find the component that failed by reasoning backwards from the final consequence.

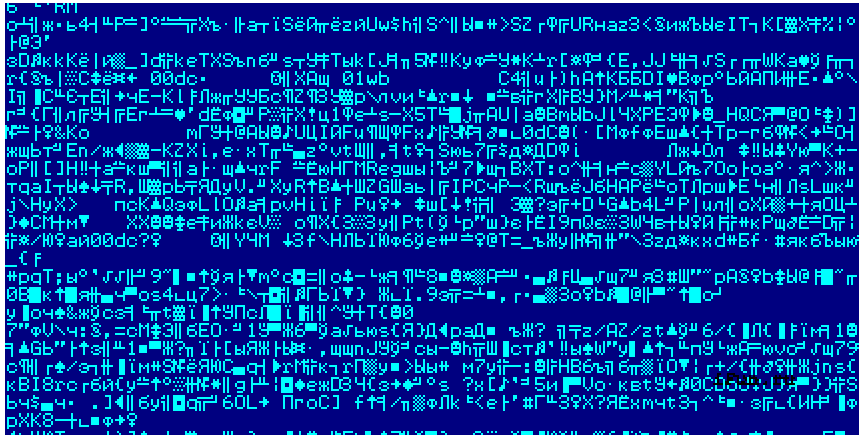
Find the probability that something "breaks", either alone or by simple, logical and fixed combinations.

# US Flight delays (August 15, 2015)

**Thousands of travellers in the US faced delays on Saturday after a technical glitch grounded flights into and out of New York and Washington.**

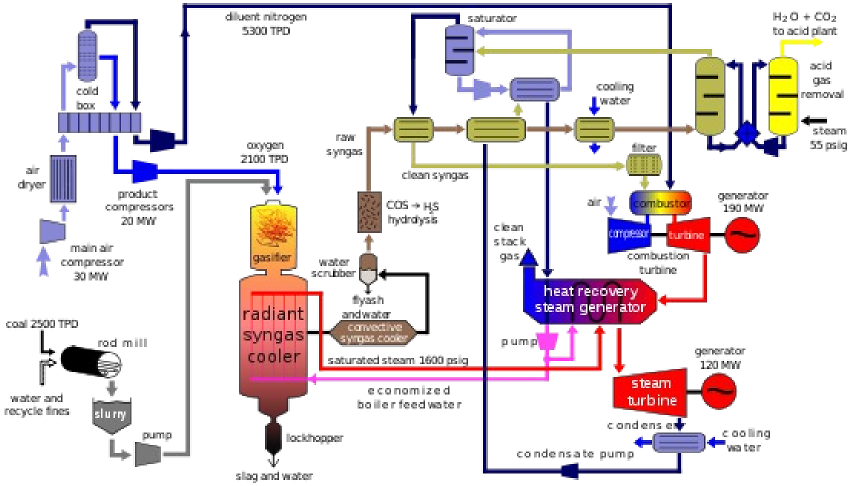
The FAA said the problem is not believed to be caused by any accident or hacking.

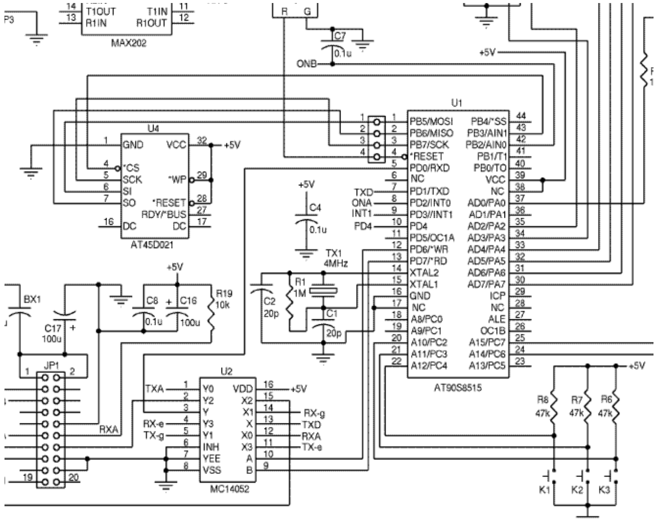
According to the agency, the fault was with a computer system known as ERAM which is used at 20 air traffic control centres around the country that handle high-altitude air traffic. The system was installed earlier this year but was already years behind schedule.

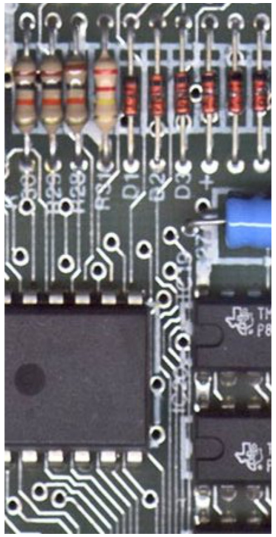


**"The FAA is continuing its root cause analysis to determine what caused the problem and is working closely with the airlines to minimize impacts to travellers," the agency said in a statement.**

# Understanding not-so-simple systems



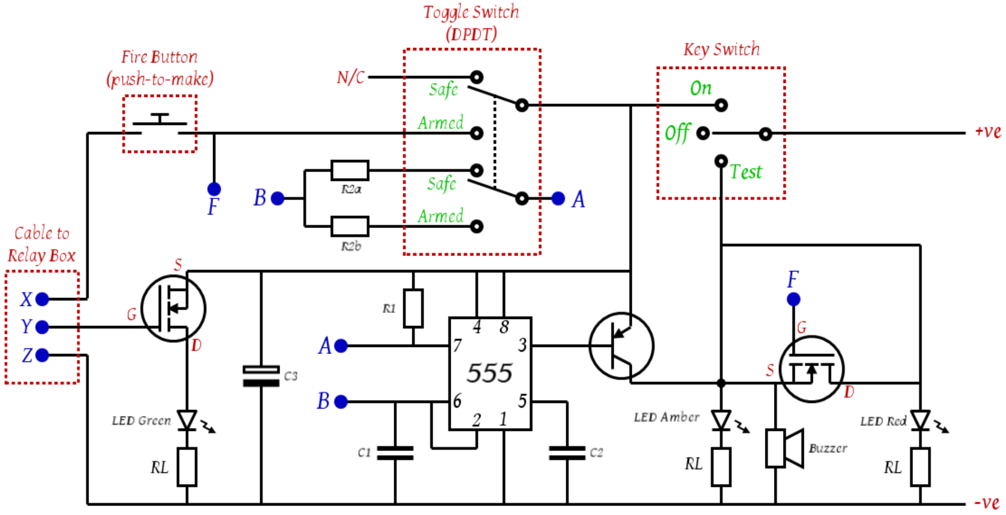




Reasoning in cause-effect relations is no longer adequate.

Difficult to imagine how events and conditions may combined.

A growing number of risks therefore remain unknown.



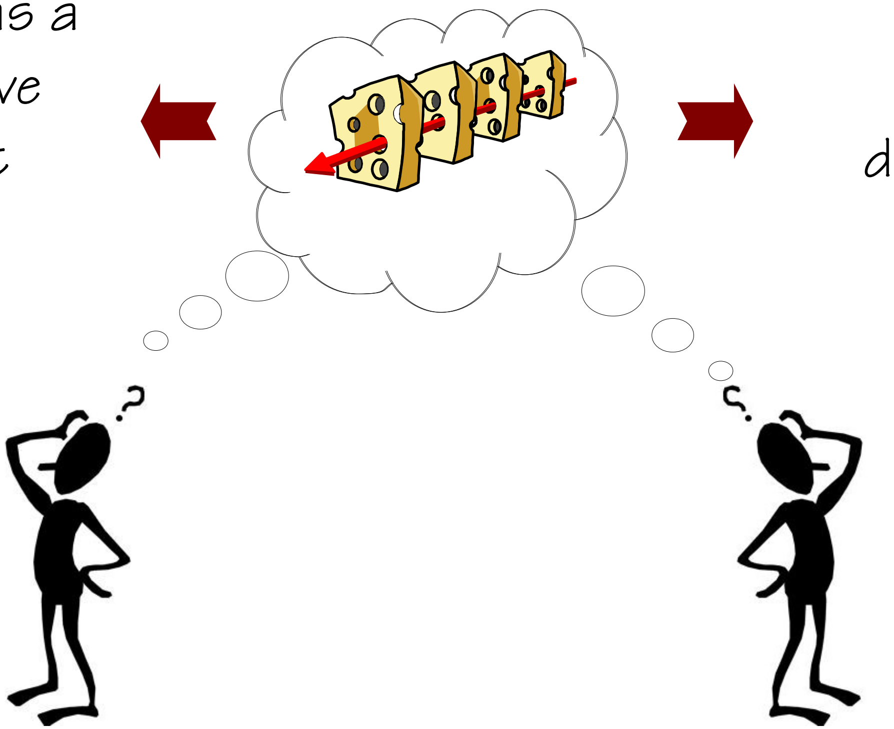
© Erik Hollnagel, 2016

# Combinatorial (complex) linear model

## Complex linear models

If accidents happen as a combination of active failures and latent conditions ...

… then risks are the likelihood of weakened defences in combination with active failures



Look for how degraded barriers or defences combined with an active (human) failure.

Combinations of single failures and latent conditions, leading to degradation of barriers and defences.

# The causality credo

(1) Adverse outcomes happen because something has gone wrong (causality + value symmetry).

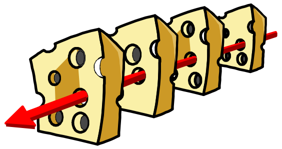
(2) Causes can be found and treated (deduction).

(3) All accidents are preventable (zero harm).

## Accident investigation

Find the component that failed by reasoning backwards from the final consequence.

Accidents result from a combination of active failures (unsafe acts) and latent conditions (hazards).

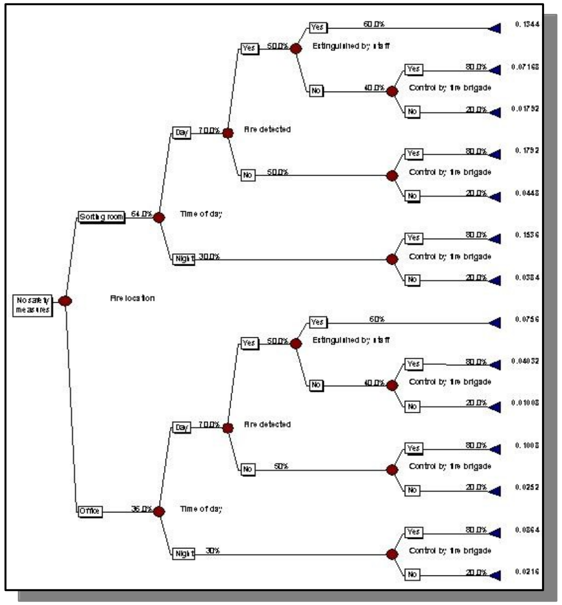


## Risk analysis

Find the probability that components “break”, either alone or in simple combinations.

Look for combinations of failures and latent conditions that may constitute a risk.

# Common assumptions (~ 1970)



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

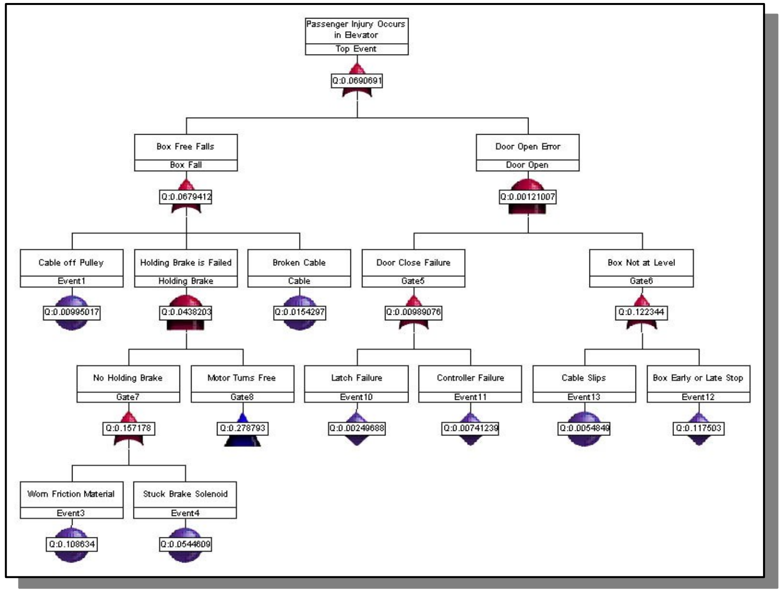
The function of each element is bimodal (true/false, work/fail)

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



# Nature of socio-technical systems

All systems unique

Must be described top-down in terms of functions and objectives.

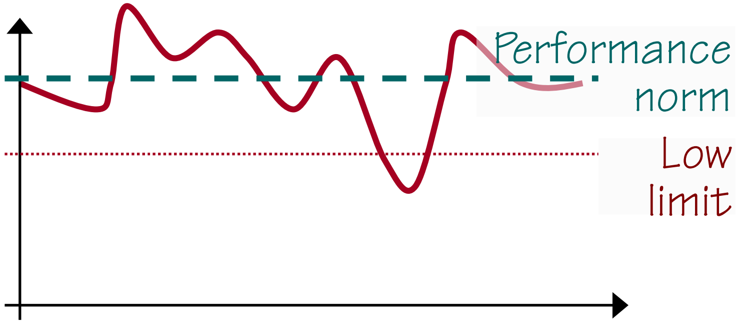
Decomposition does not work for socio-technical systems, because they are emergent.

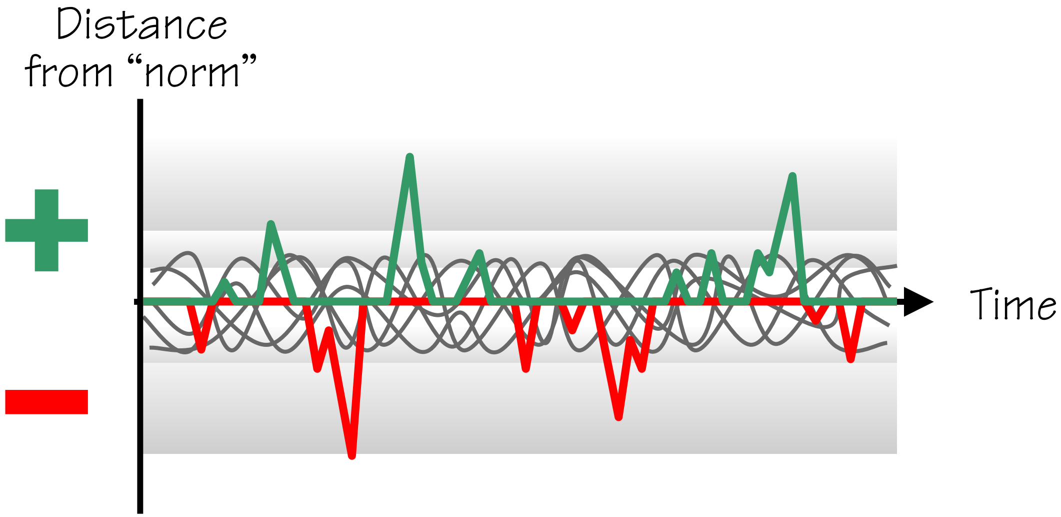
Risks and failures must therefore be described relative to functional wholes.

Complex relations between input (causes) and output (effects) give rise to unexpected and disproportionate consequences. Socio-technical systems are non-linear and event outcomes are intractable.

# Socio-technical systems are not bimodal

Humans and social systems are not bimodal. Everyday performance is variable and this – rather than failures and 'errors' – is why accidents happen. Since performance shortfalls are not a simple (additive or proportional) result of the variability, more powerful, non-linear models are needed.





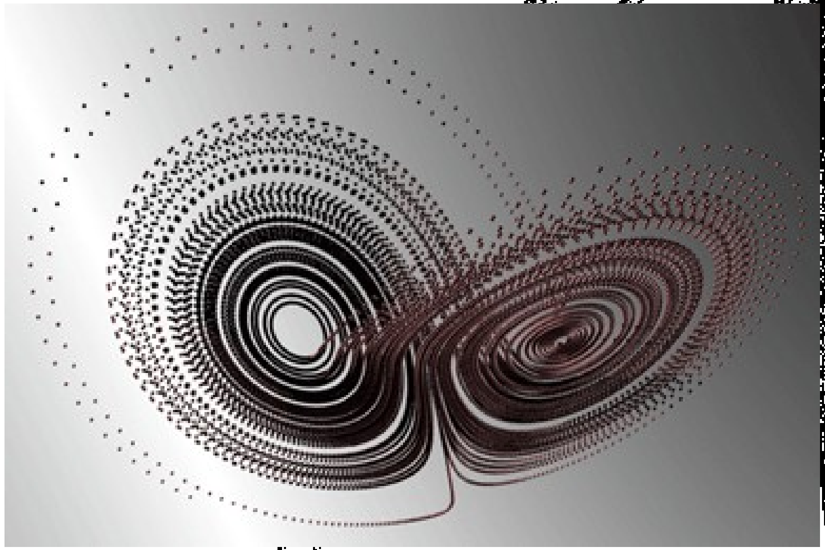
Performance variations can be have positive as well as negative outcomes!

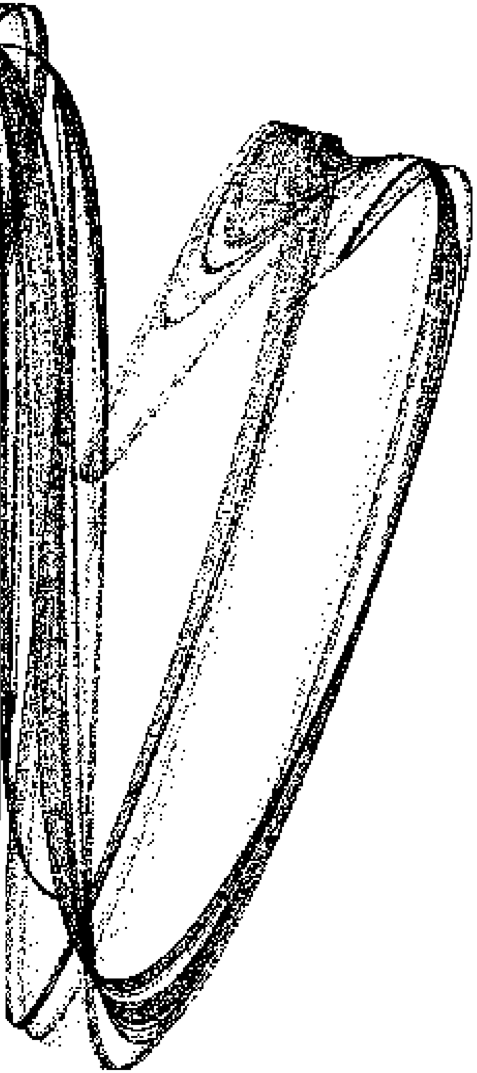
But human factors has tended to look for negative aspects of performance - deviations or "errors"

# Understanding complex systems

Systems have become too complex to understand in detail (chaotic, emergent).

Systems change so fast that complete descriptions – of the real system – are impossible.

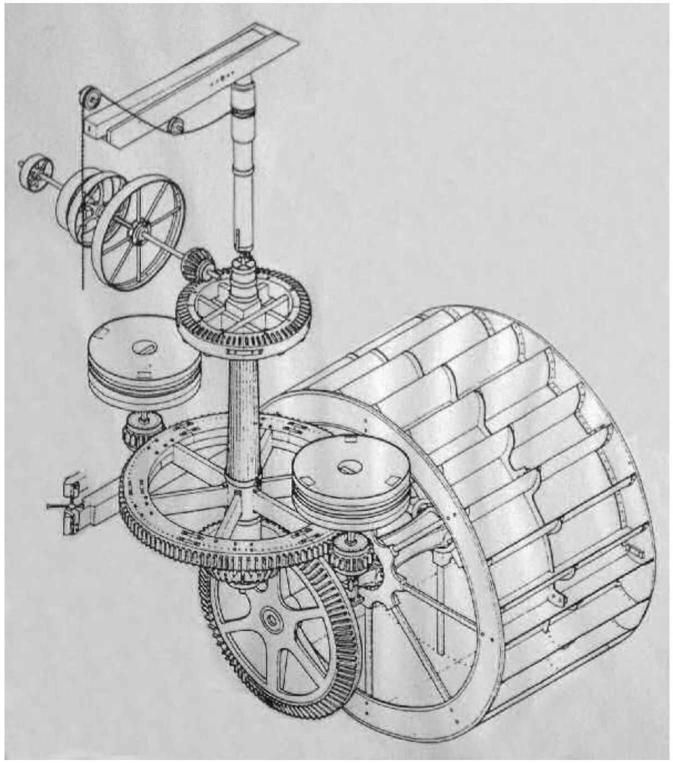




Working / operating environments are unstable and unpredictable. Actions / changes therefore often have unanticipated consequences.

# Understanding how systems work

Understanding in terms of interconnected parts.



Few parts and well-defined (synchronous) connections

Understanding in terms of functions that depend on each other.

Many "parts" and ill-defined (asynchronous) connections.

# The need to “imagine” how others work

Plan and design work:
roles, workplace

Work-As-Imagined

Manage work:
“lean” - quality - guidelines

Work-As-Imagined

Manage safety:
investigations & auditing

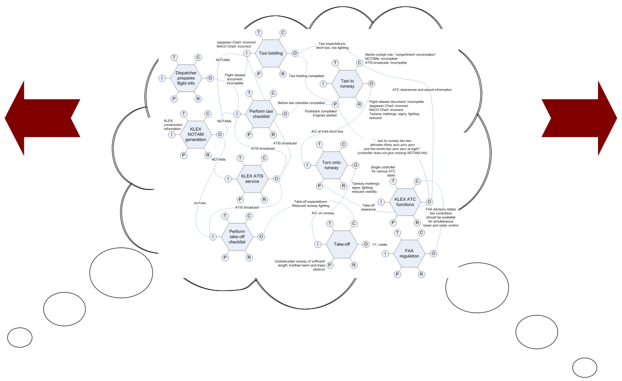
Work-As-Imagined

Work-As-Done

# Functional non-linear model

Non-linear models

If accidents can be understood as emerging from everyday performance adjustments ...

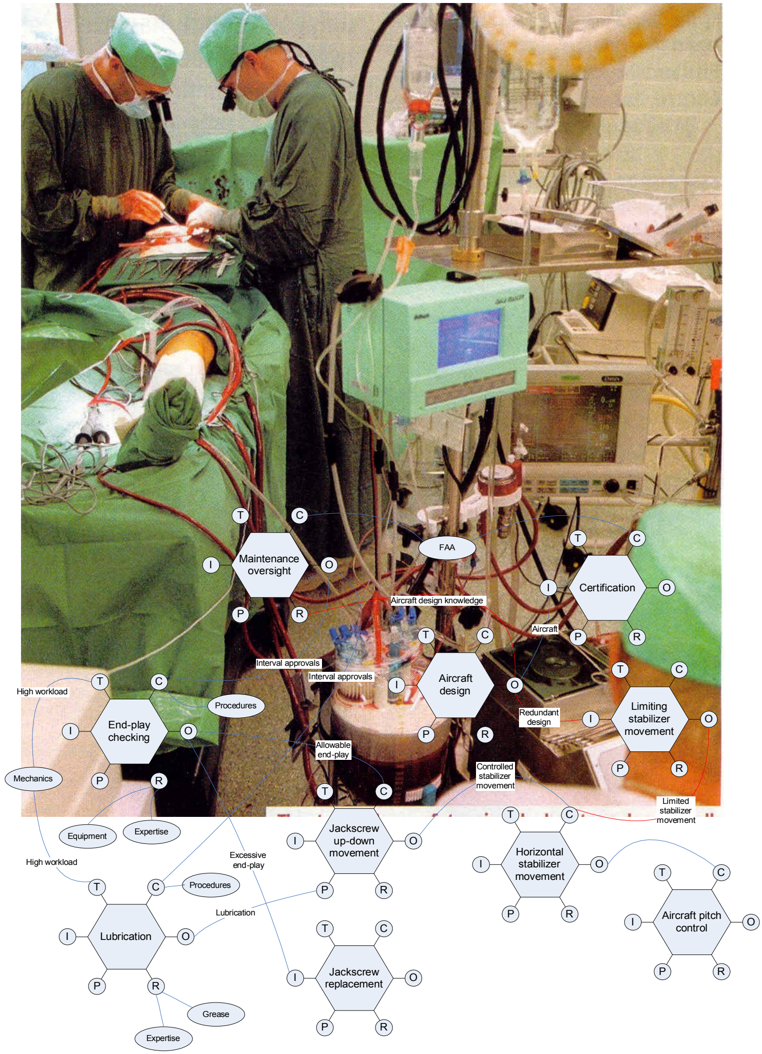

Taxi briefing
Dispatcher prepares flight info
Taxi to runway
Perform taxi checklist
KLEX NOTAM generation
KLEX ATIS service
Turn onto runway
KLEX ATC functions
Perform take-off checklist
Take-off
FAA regulation
Jeppesen Chart: incorrect
NACO Chart: incorrect
NOTAMs
Flight release document: incomplete
Taxi expectations: short taxi, low lighting
Sterile cockpit rule: "nonpertinent conversation"
NOTAMs: incomplete
ATIS broadcast: incomplete
Taxi briefing completed
ATC clearances and airport information
Before taxi checklist completed
Pushback completed
Engines started
Flight release document: incomplete
Jeppesen Chart: incorrect
NACO Chart: incorrect
Taxiway markings, signs, lighting: reduced
KLEX construction information
A/C at hold short line
ATIS broadcast
"...taxi to runway two two altimeter three zero zero zero and the winds two zero zero at eight", (controller does not give missing NOTAM info)
Single controller for various ATC tasks
Taxiway markings, signs, lighting: reduced visibility
Take-off expectations: Reduced runway lighting
Take-off clearance
A/C on runway
FAA advisory states two controllers should be available for simultaneous tower and radar control
V1, rotate
Unobstructed runway of sufficient length: Earthen berm and trees obstruct

... then risks can be understood as emerging from everyday performance adjustments

Systems at risk are intractable rather than tractable.

The future can be understood by considering the characteristic variability of the present.

# Revised assumptions - 2016



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

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

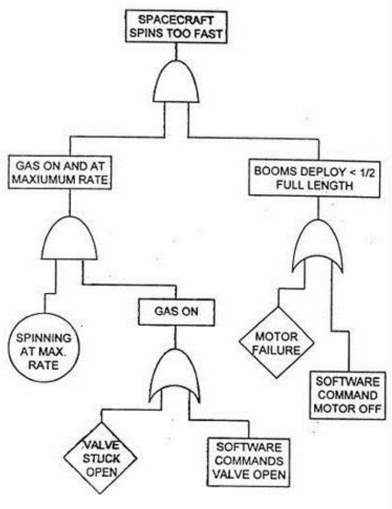
Outcomes are determined by performance variability, which is a source of success as well as of failure.

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

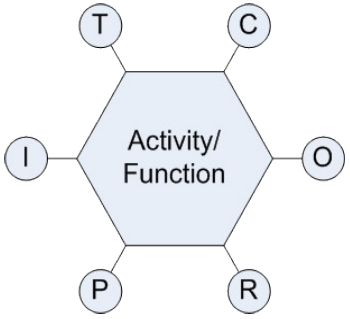
Risk and safety analyses should try to understand the variability of everyday performance and use that to identify conditions that may lead to both positive and adverse outcomes.

# Models and methods

An analysis of something inevitably involves some assumptions about how that something happens. These assumptions correspond to a model: a simplified explanation of how something can happen and of how the 'world' is organised. The organisation usually implies some kind of hierarchical ordering of layers, parts, or component (structural models).


SPACECRAFT SPINS TOO FAST
GAS ON AND AT MAXIUMUM RATE
BOOMS DEPLOY < 1/2 FULL LENGTH
SPINNING AT MAX. RATE
GAS ON
MOTOR FAILURE
SOFTWARE COMMAND MOTOR OFF
VALVE STUCK OPEN
SOFTWARE COMMANDS VALVE OPEN

The model defines what the method can be used for, and therefore also sets the limits of the method.



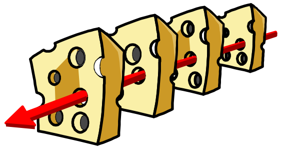
The FRAM is a method to develop a representation or model of how something happens. This model can then be the basis for various kinds of analyses (reactive, proactive). A FRAM model represents the functions that sufficient and necessary for an activity to take place – not when it goes wrong but when it goes right.

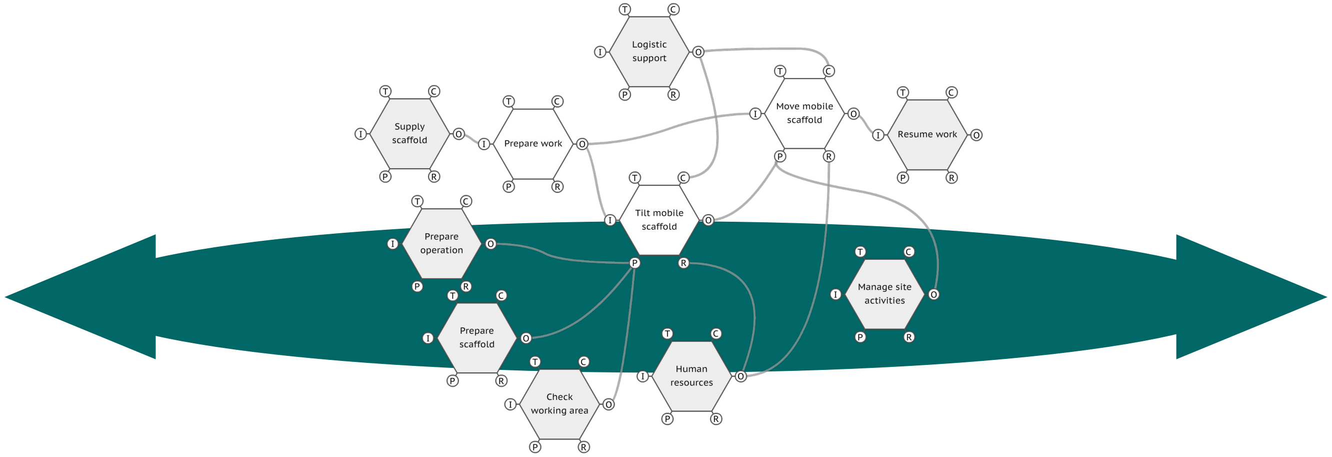
# Three kinds of analysis

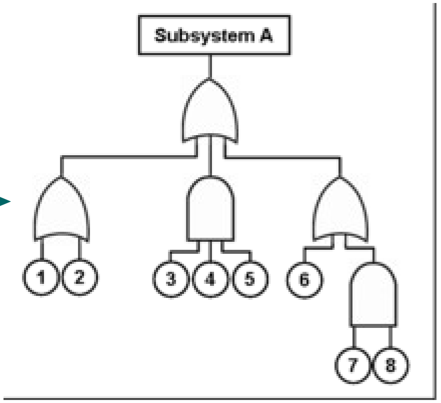
Analysis of the past
(retrospective)

Analysis of the present
(work-as-done)

Analysis of the future
(predictive)







Accident analysis:
Root Cause
Bow-tie
Swiss cheeses
...

Functional model of
everyday work.

A FRAM model can be used for both
retrospective and predictive analyses.

Risk analysis:
Fault tree
FMECA
HAZOP/HAZID
...