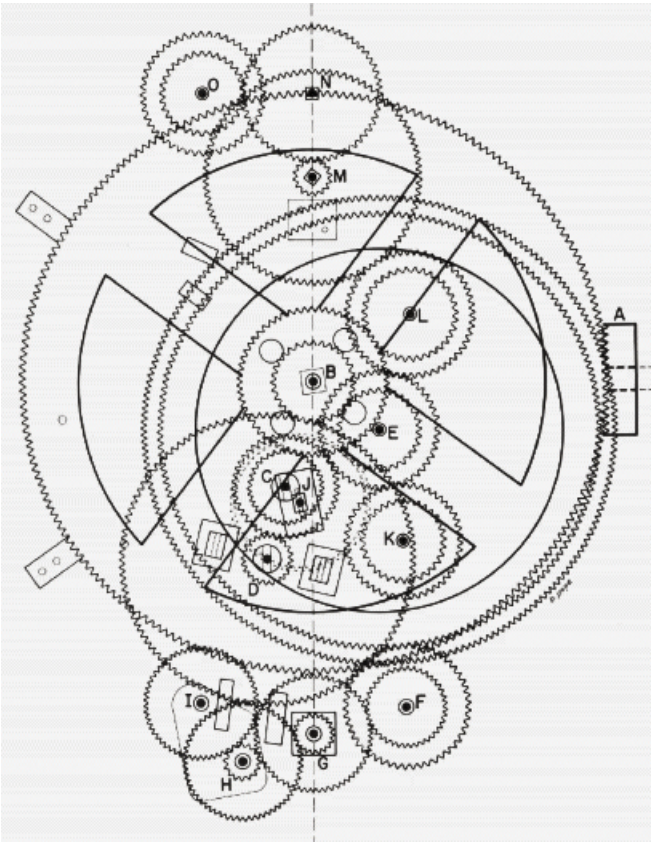
FRAM: Setting the scene

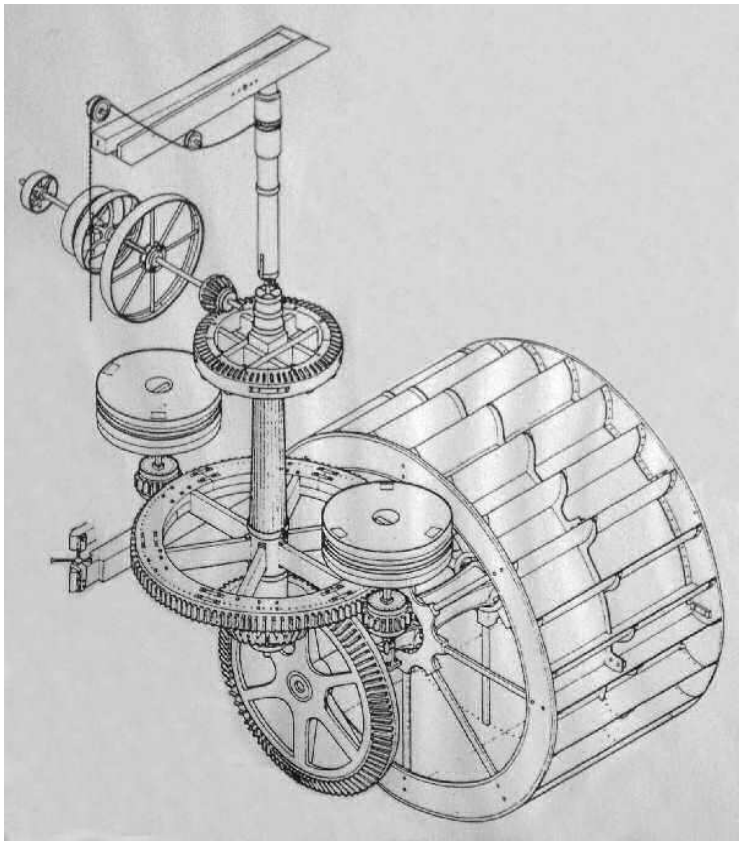
Erik Hollnagel
hollnagel.erik@gmail.com
www.safetysynthesis.com

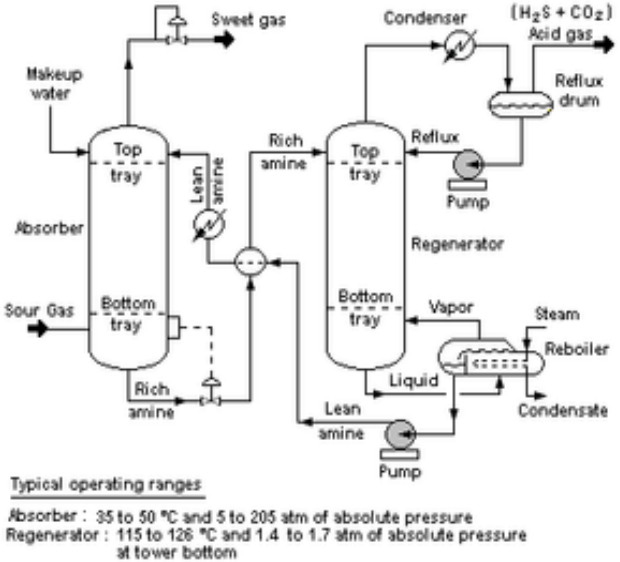
Understanding simple systems



Antikythera mechanism, (150-100 BC)

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





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

What was work like in the 1920s?

Industrial work in the beginning of the 20th Century was very different from what it is today.

Comprehensibility: system functions were easy to understand, independent and work was manual.

Stability: work activities were regular and stable (orderly).

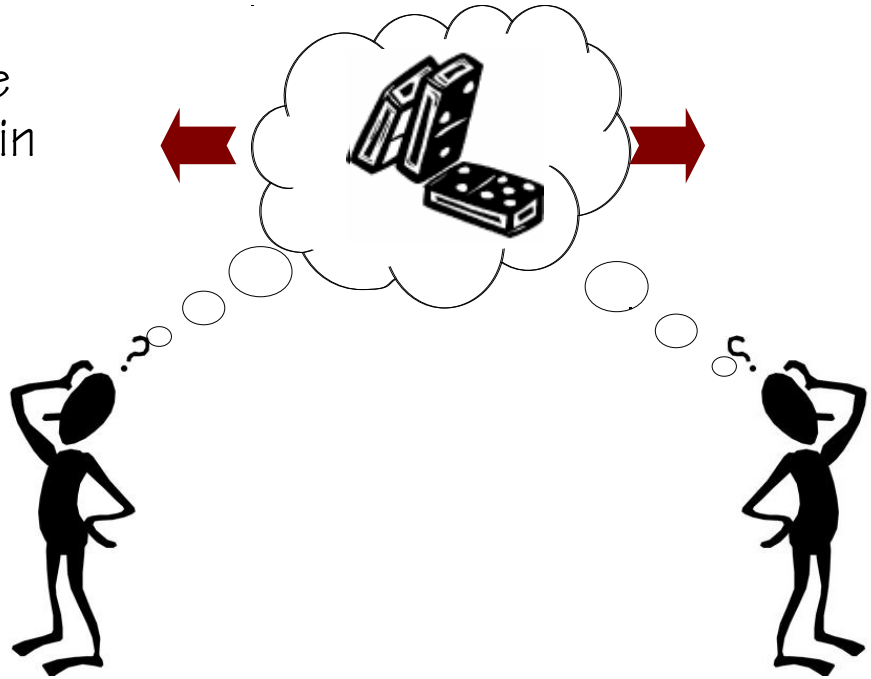
Descriptions: simple (few elements and relations).

Systems were loosely coupled and linear. Simple ("root) causes.

Simple, linear model (cause-effect chain)

Simple linear models
(cause-effect chains)

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

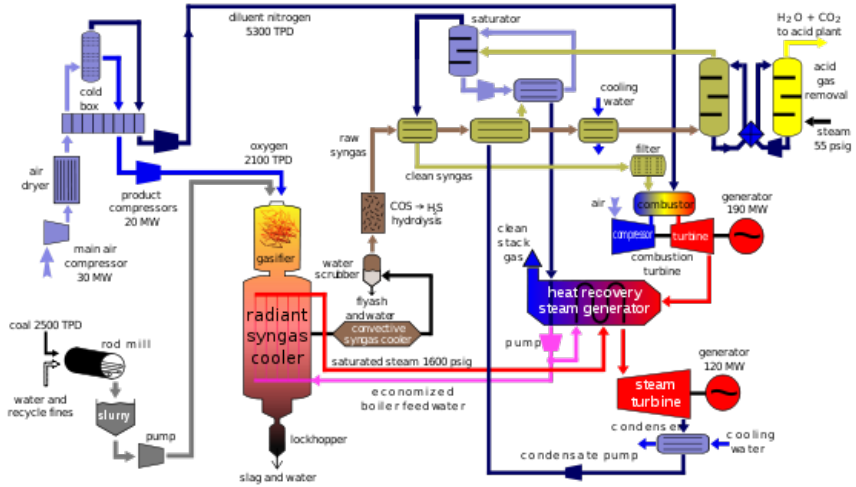


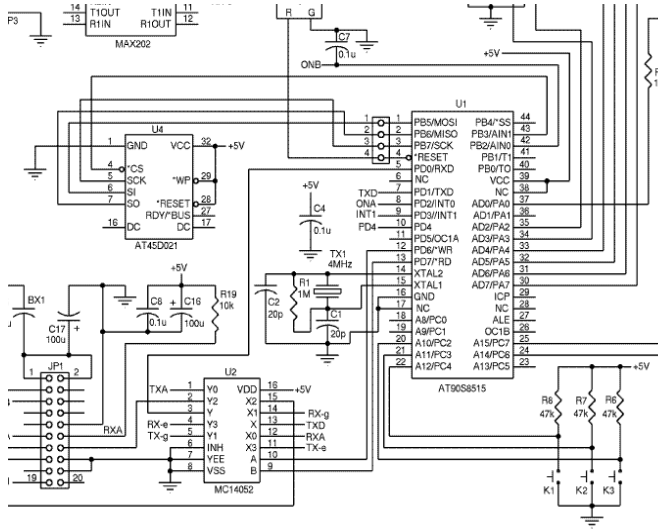
... then risks can be found as the probability of component failures

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.

Understanding not-so-simple systems

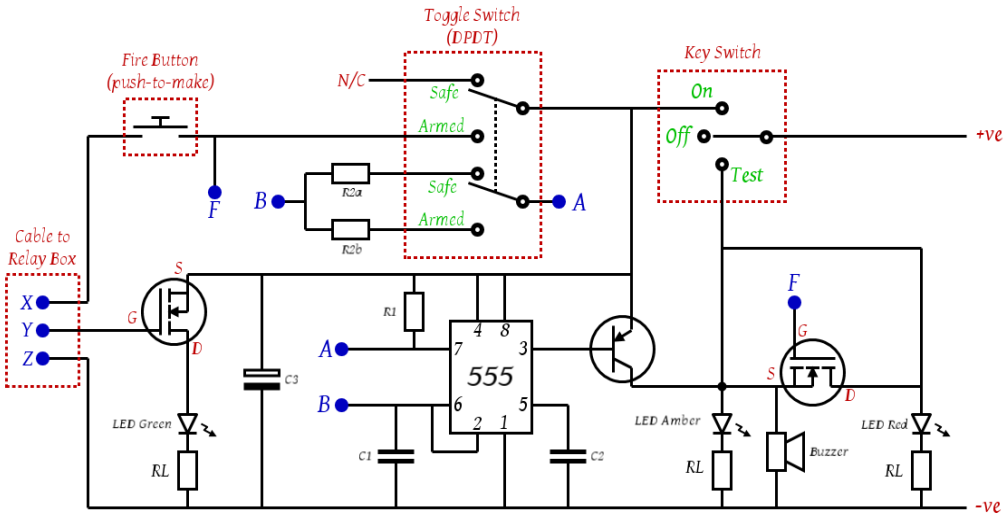




Reasoning in cause-effect relations is no longer adequate.

Difficult to imagine how events and conditions may combined.

A growing number of risks therefore remain unknown.



What was work like in the 1980s?

Industrial work towards the end of the 20th Century had changed dramatically due to computerisation.

Comprehensibility: system functions could be hard to understand, they were dependent and work was automated.

Stability: less stable, affected by demands-resources, coping with unexpected situations.

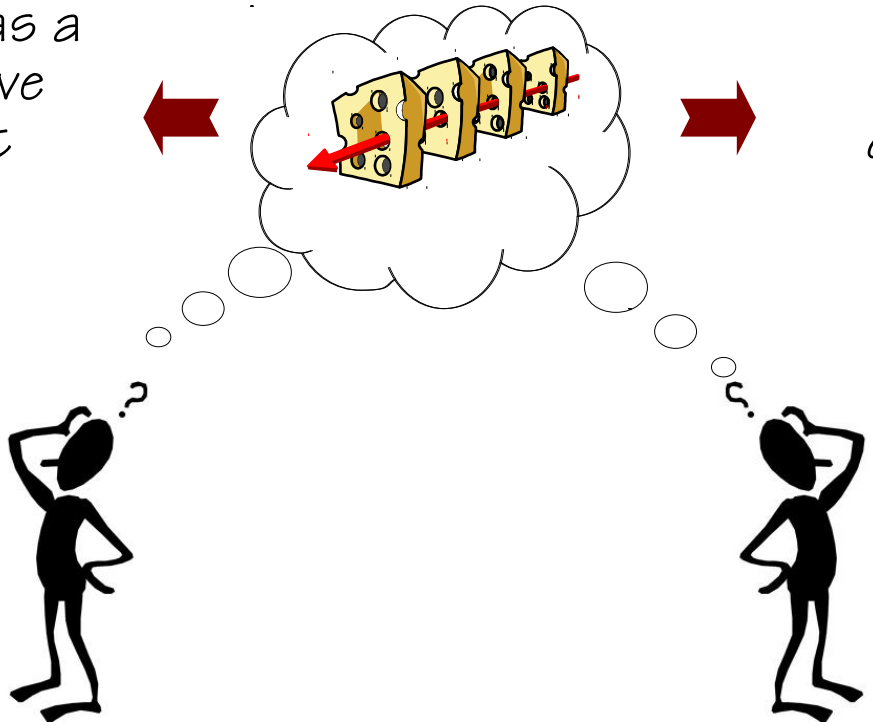
Descriptions: complex (many elements and relations).

Systems were tightly coupled and increasingly non-linear. Multiple interacting causes.

Combinatorial (complex) linear model

Complex linear models

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



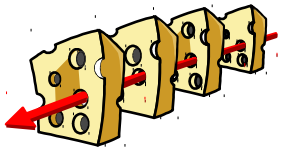
... then risks are the likelihood of weakened defences in combination with active failures

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		Risk analysis
Find the component that failed by reasoning backwards from the final consequence.		Find the probability that components "break", either alone or in simple combinations.
Accidents result from a combination of active failures (unsafe acts) and latent conditions (hazards).		Look for combinations of failures and latent conditions that may constitute a risk.

Safety-I perspective

Function
(Work-as-Imagined)

→

Success
(no adverse
events)

Acceptable
outcomes

Hypothesis of different causes: Things that go right and things that go wrong happen in different ways and have different causes

Malfunction,
non-compliance,
error

—

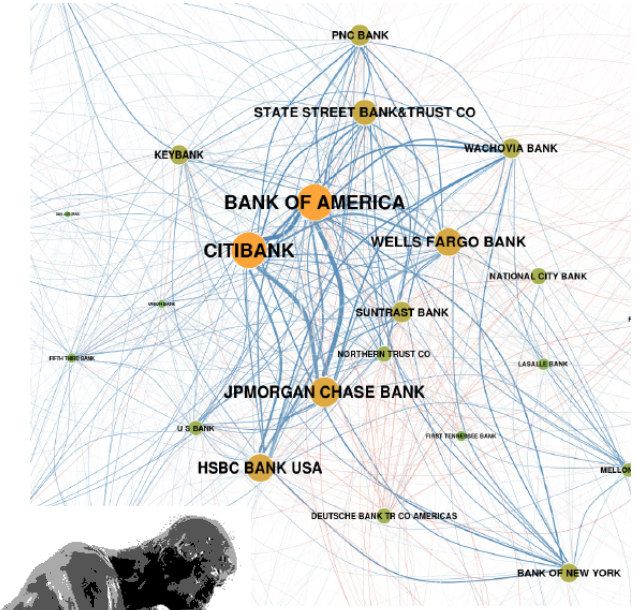
Failure
(accidents,
incidents)

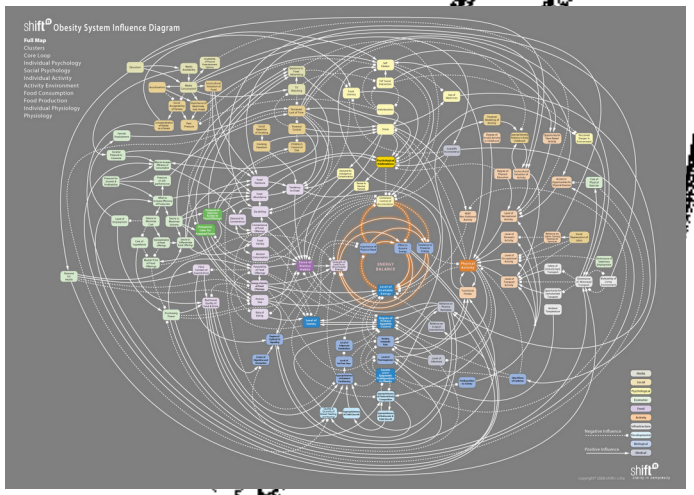
Unacceptable
outcomes

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.

What will work be like tomorrow?

Industrial work at present is in a state of transition driven by technological advances – and hopes.

Comprehensibility: system functions are partly hidden, automation is ubiquitous and obscure.

Stability: system performance changes dynamically and autonomously, environments are partly unpredictable.

Descriptions: intractable – complex with ill-defined boundaries.

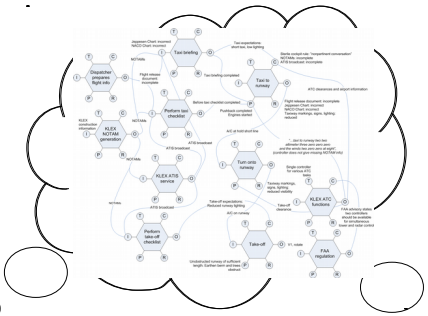
Systems will be non-trivial and non-linear. Consequences emerge from complexity.

Functional non-linear model

Safety Synthesis

Non-linear models

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



... 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.

The need to "imagine" how others work

Preparing work:
roles, workplace,
procedures, training

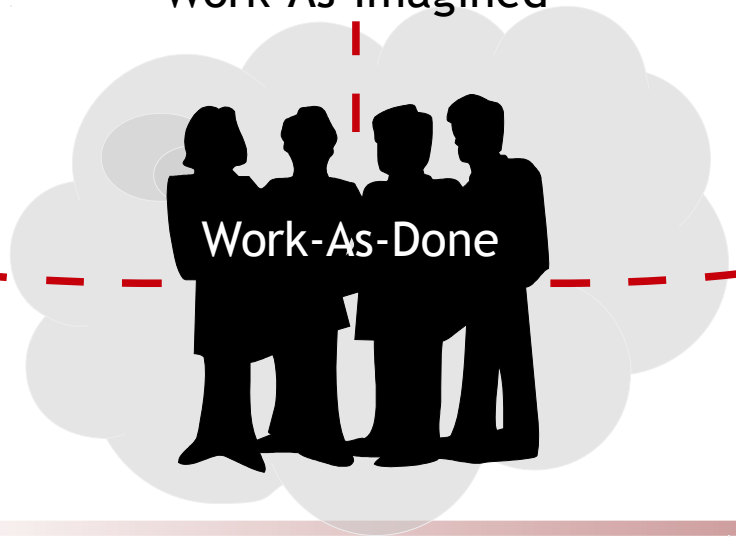
Work-As-Imagined

Managing work:
plan, quality, safety,
productivity, "lean"

Work-As-Imagined

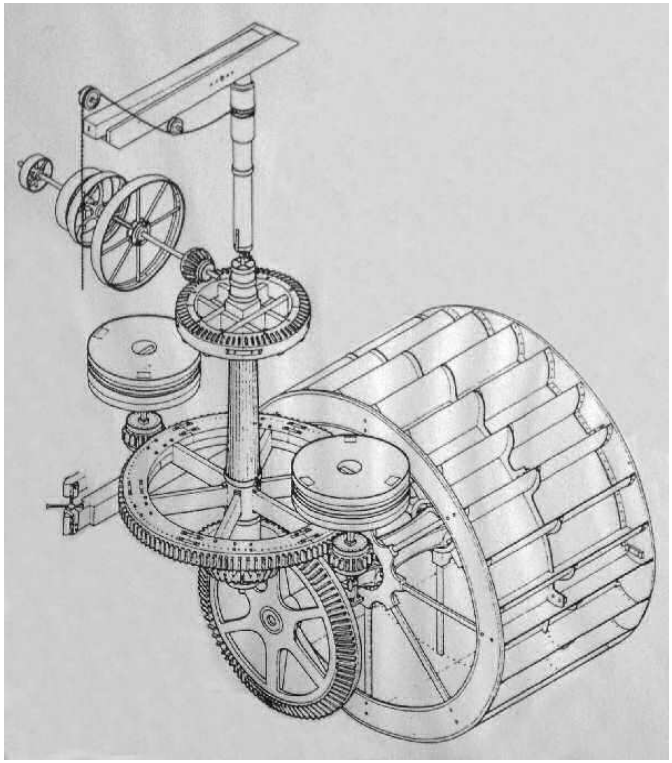
Manage safety & quality:
investigations & auditing

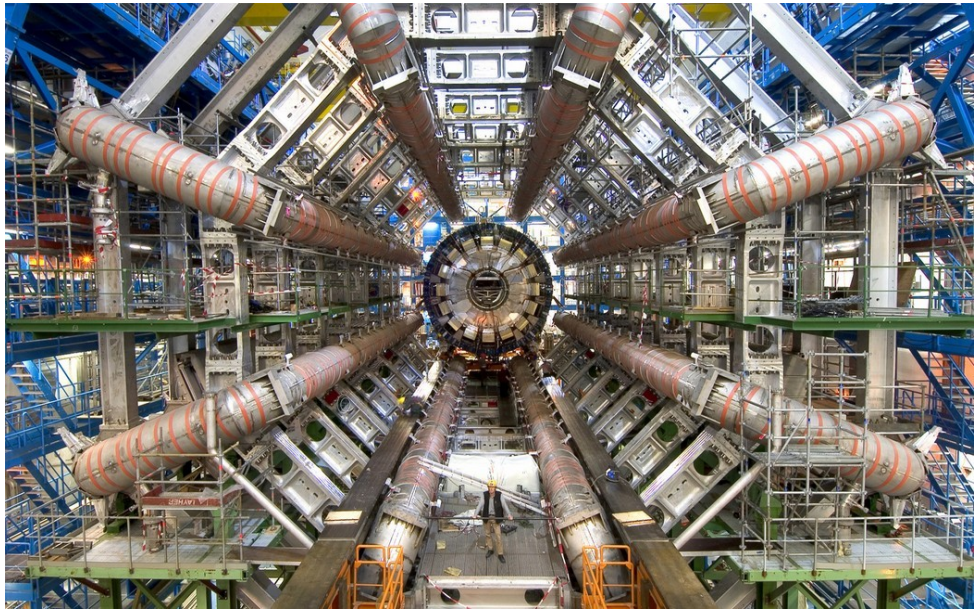
Work-As-Imagined



We understand how this works …

We usually describe and understand systems in terms of interconnected parts.





Systems have known parts - few or many – with well-defined (synchronous) connections

… but not really how this works

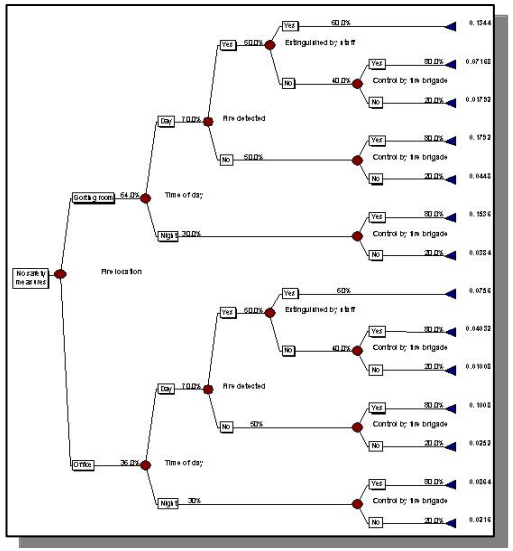
We need to describe and understand socio-technical systems in terms of functions rather than in terms of parts or "components".

Systems include many functions that depend on each other and with ill-defined (asynchronous) connections.

Common assumptions - then and now

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

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

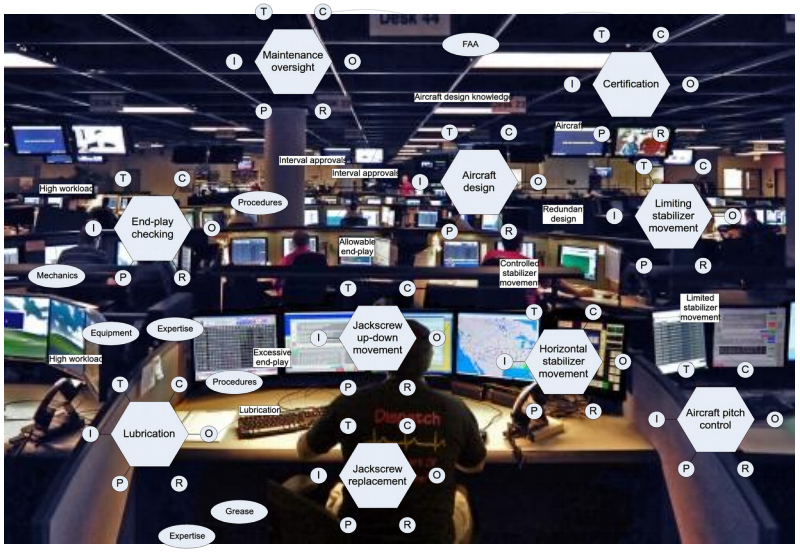


The failure probability of elements can be analysed/described individually

The order or sequence of events is predetermined and fixed

Systems cannot be understood by decomposing them.

System functions are not bimodal, performance is always variable.



Performance variability is a source of success as well as of failure.

The organisation of functions must be flexible to fit the conditions.