弾

Resilience Engineering: The history of safety

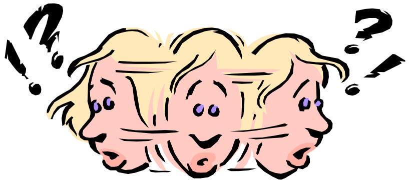
Erik Hollnagel

Professor &
Industrial Safety Chair
MINES ParisTech
Sophia Antipolis, France

Professor II
NTNU
Trondheim, Norge

E-mail: erik.hollnagel@gmail.com

How can we know that we are safe?



Accident analysis

Explaining and understanding what has happened (actual causes)

Elimination or reduction of attributed causes

How can we know what did go wrong?

Risk assessment

Predicting what may happen (possible consequences)

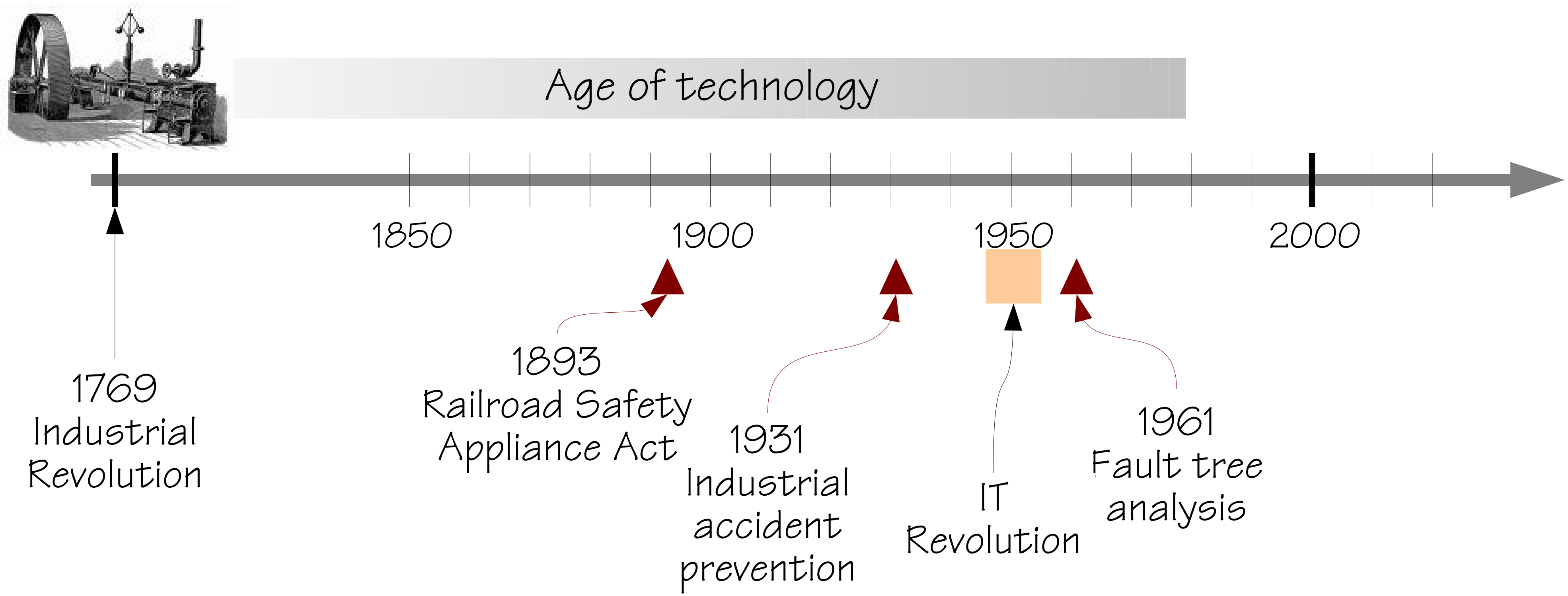
Elimination or prevention of potential risks

How can we predict what may go wrong?

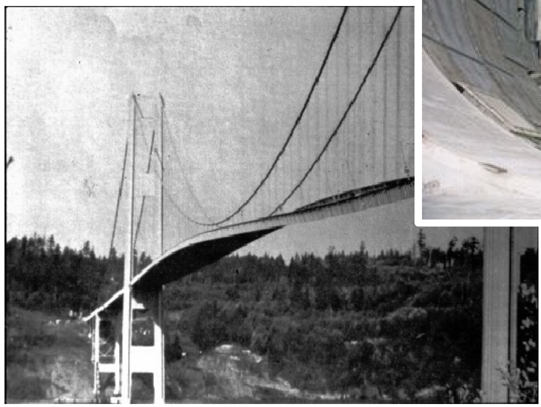
In order to achieve freedom from risks, models, concepts and methods must be compatible, and be able to describe 'reality' in an adequate fashion.

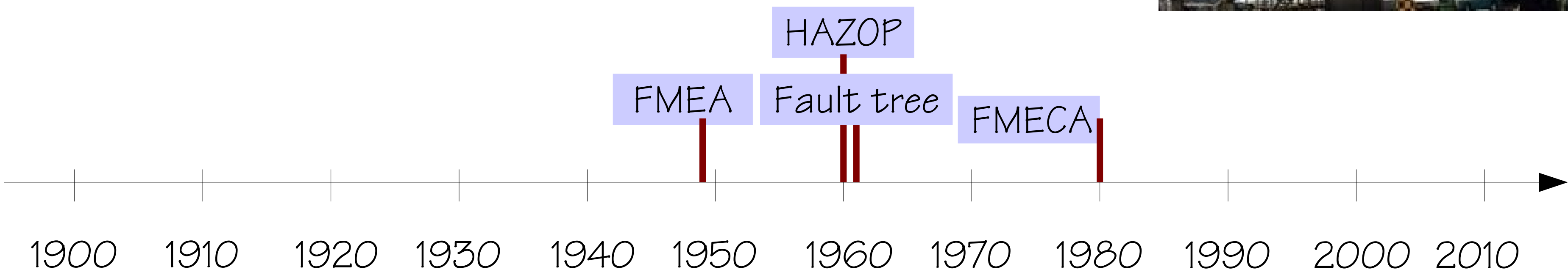
Three ages of industrial safety

Hale & Hovden (1998)



Technical analysis methods



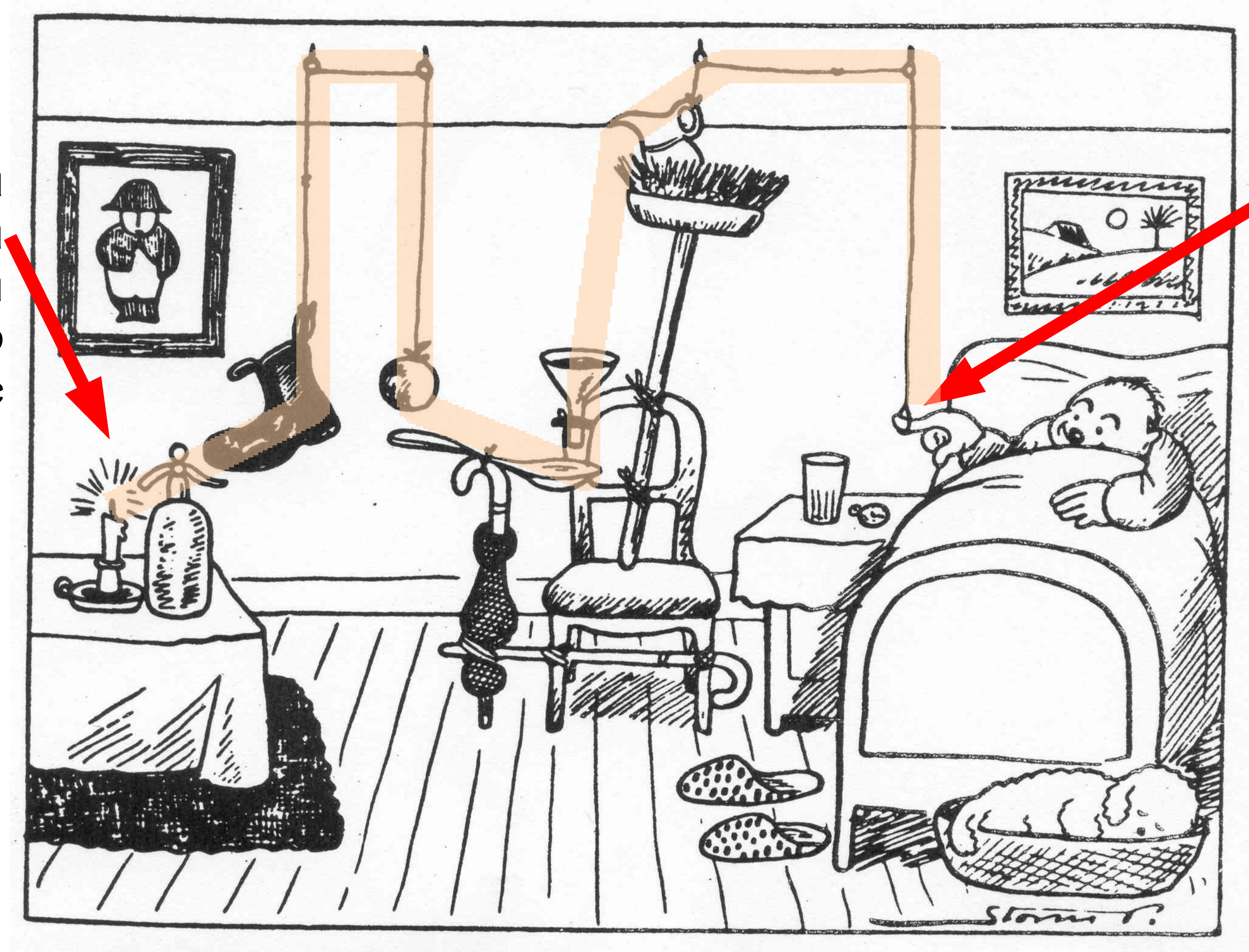


How do we know technology is safe?

Design principles: Clear and explicit
Architecture and components: Known
Models: Formal, explicit
Analysis methods: Standardised, validated
Mode of operation: Well-defined (simple)
Structural stability: High (permanent)
Functional stability: High

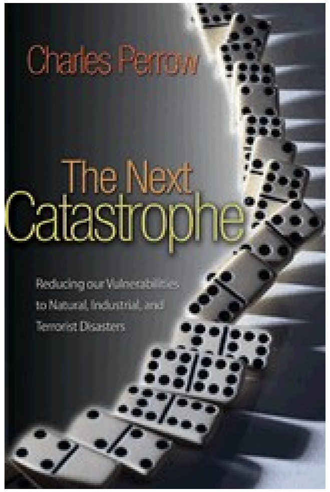
Sequential thinking (cause-effect)

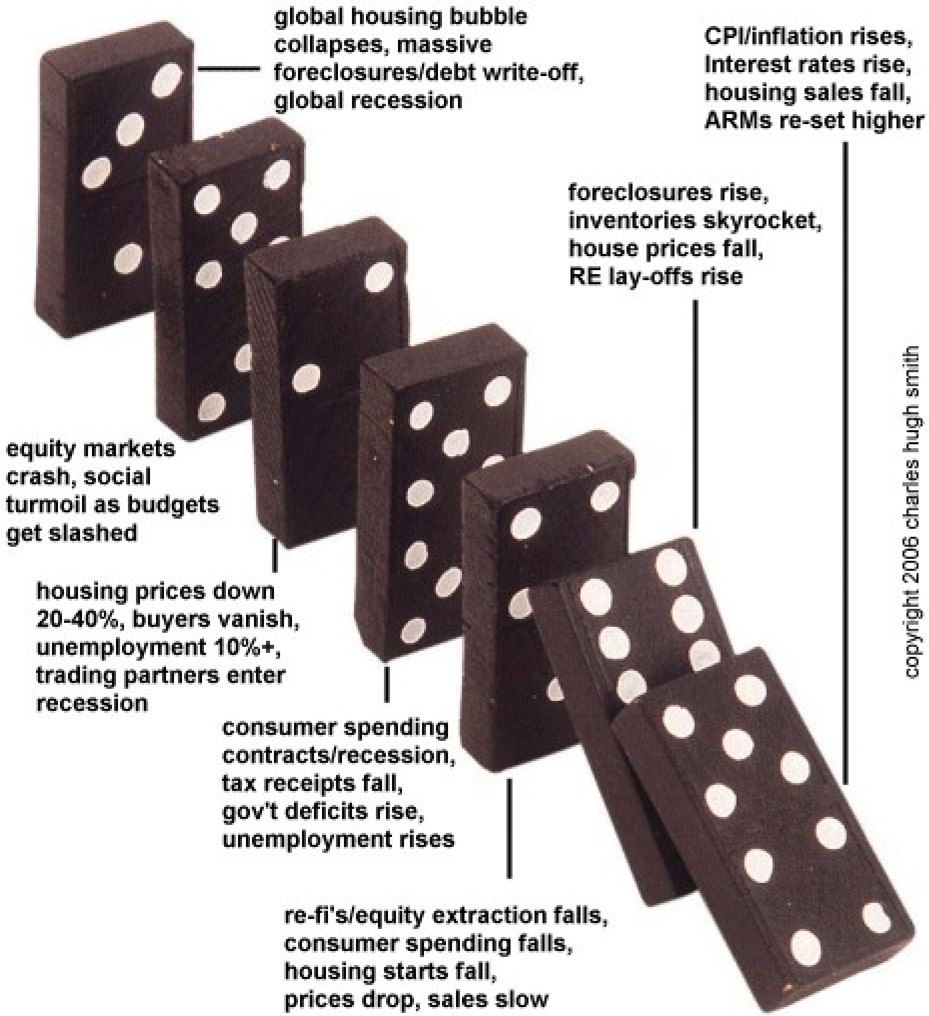
Starting from the effect, you can reason backwards to find the cause



Starting from the cause, you can reason forwards to find the effect

Domino thinking everywhere

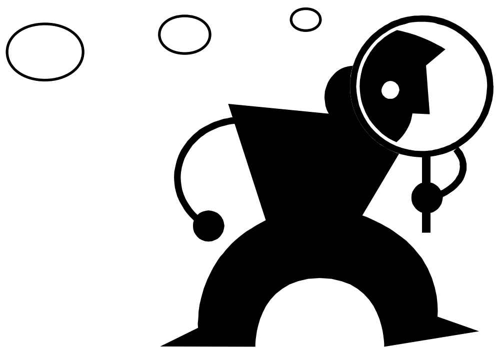




Simple linear models

Assumption: Accidents are the (natural) culmination of a series of events or circumstances, which occur in a specific and recognisable order.

Domino model
(Heinrich, 1930)



Consequence: Accidents are prevented by finding and eliminating possible causes. Safety is ensured by improving the organisation's ability to respond.

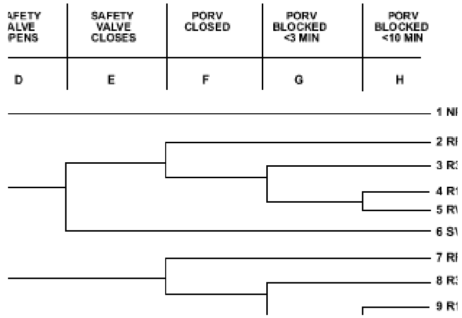
Hazards-risks: Due to component failures (technical, human, organisational), hence looking for failure probabilities (event tree, PRA/HRA).

Risks as propagation of failures

If accidents happen like this ...

The culmination of a chain of events.

... then risks can be found like this ...



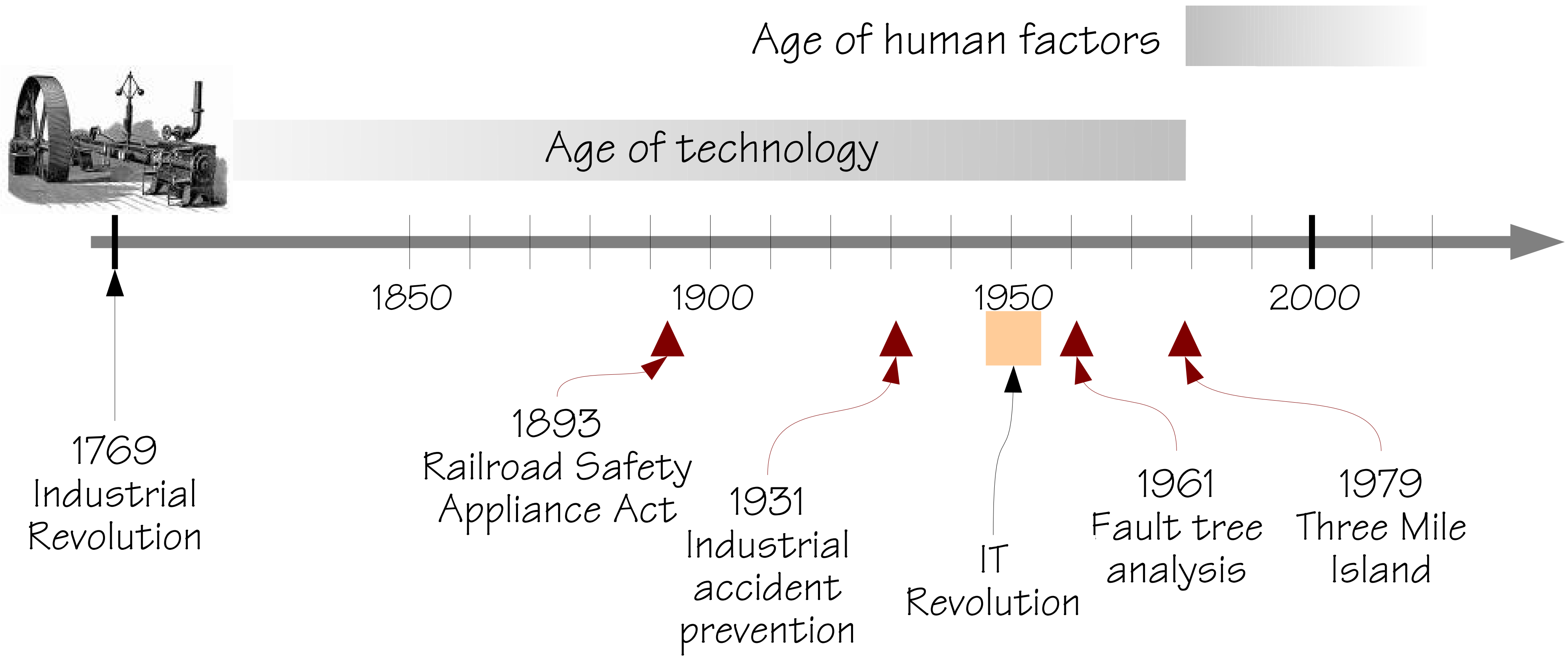
Probability of component failures

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

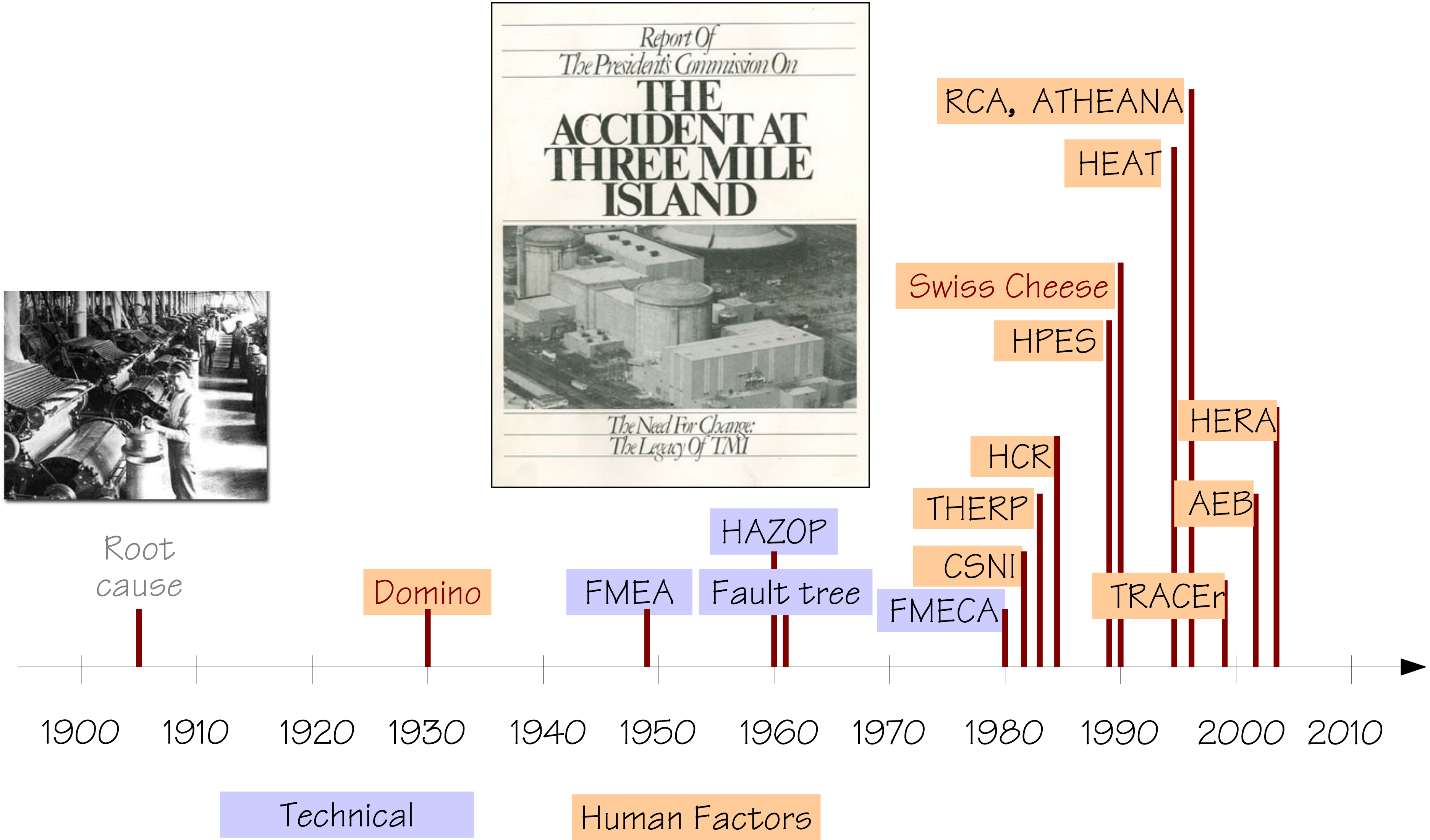
Find the probability that something “breaks”, either alone or by simple, logical and fixed combinations.

Three ages of industrial safety

Hale & Hovden (1998)



Human factors analysis methods



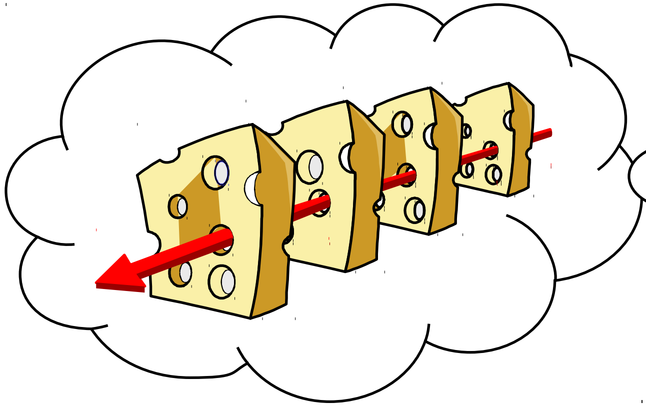
How do we know humans are safe?



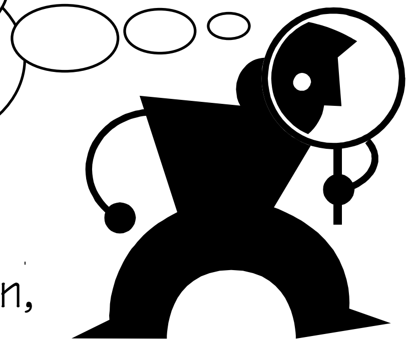
Design principles:	Unknown, inferred
Architecture and components:	Partly known, partly unknown
Models:	Mainly analogies
Analysis methods:	Ad hoc, unproven
Mode of operation:	Vaguely defined, complex
Structural stability:	Variable
Functional stability:	Usually reliable

Complex, linear cause-effect model

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



Swiss cheese model (Reason, 1990)

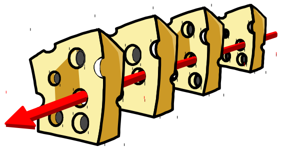


Consequence: Accidents are prevented by strengthening barriers and defences. Safety is ensured by measuring/sampling performance indicators.

Hazards-risks: Due to degradation of components (organisational, human, technical), hence looking for drift, degradation and weaknesses

Risks as combinations of failures

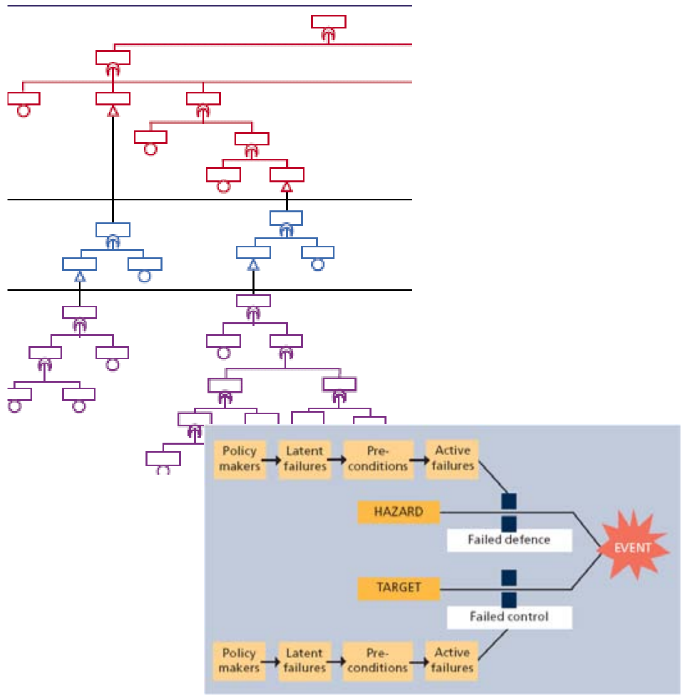
If accidents happen like this …



Combinations of active failures and latent conditions.

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

… then risks can be found like this …

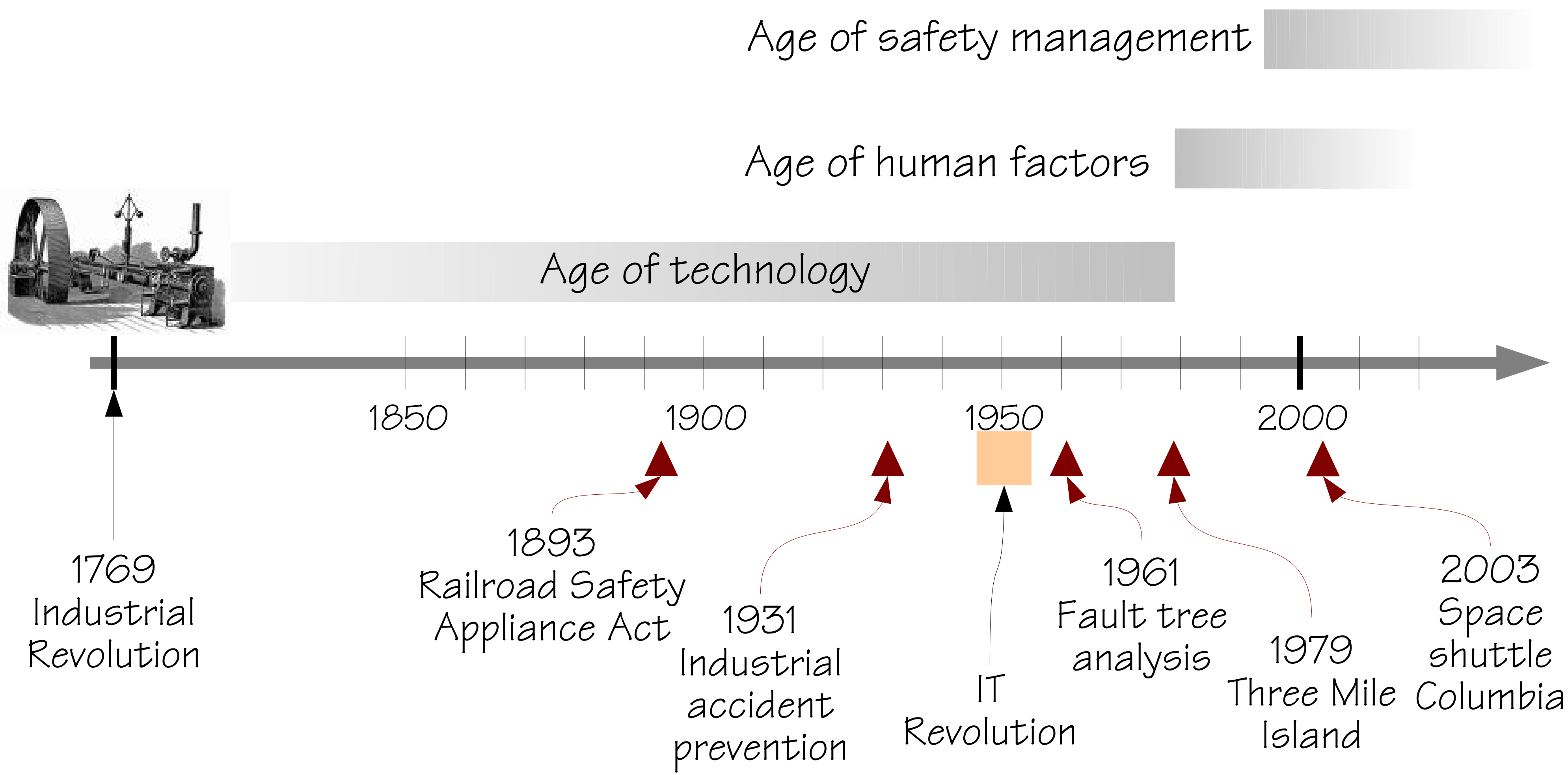


Likelihood of weakened defenses, combinations

Single failures combined with latent conditions, leading to degradation of barriers and defences.

Three ages of industrial safety

Hale & Hovden (1998)



Safety culture / organisational failures

Chernobyl, 1986

Several very serious accidents made it clear, that safety could not be ensured by addressing technical and human factors alone.

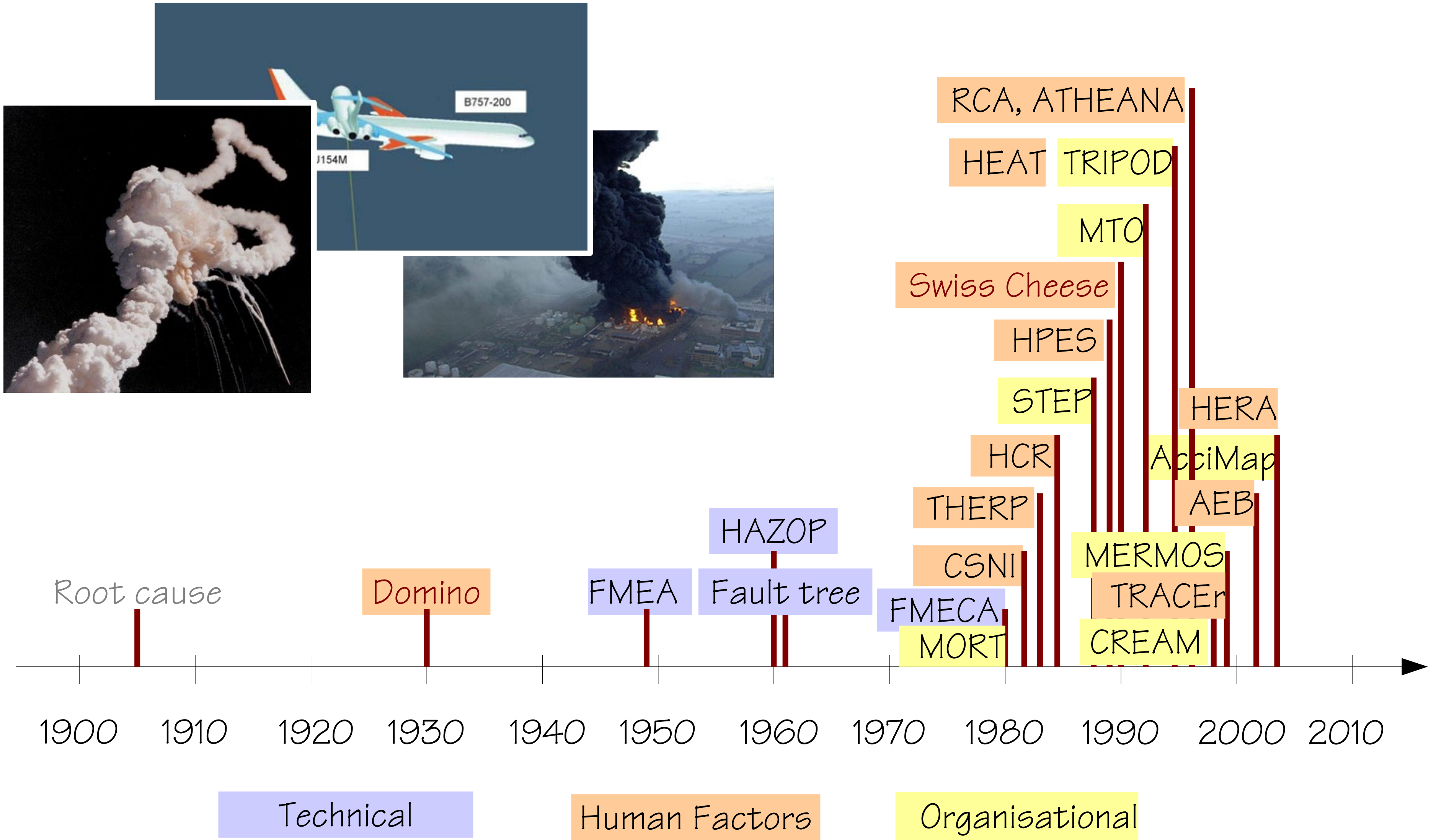
Safety culture

Challenger, 1986

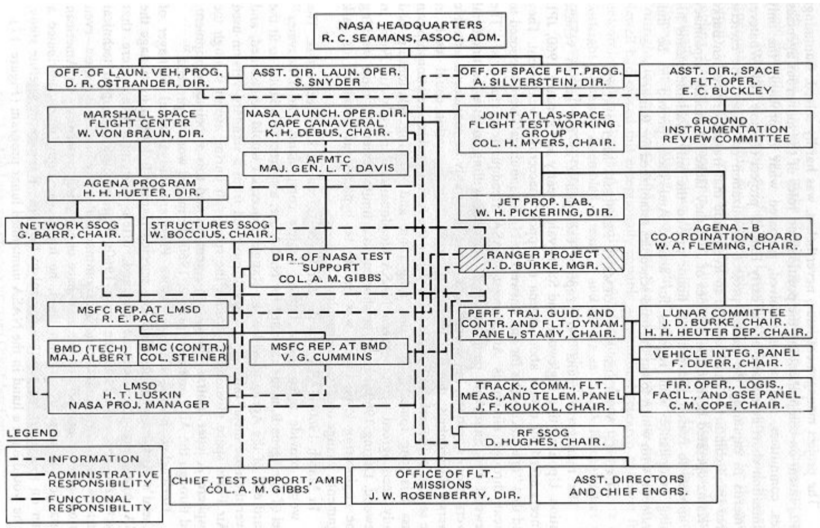
"That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance."

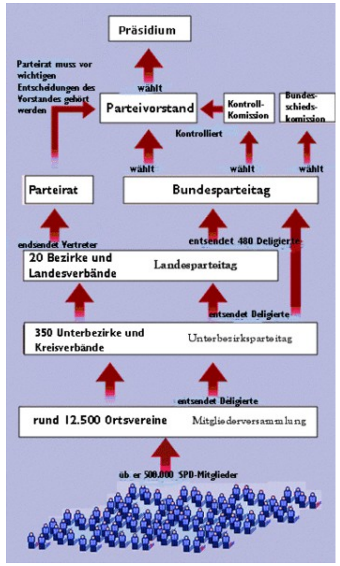
IAEA, INSAG-1 (1986)

Organisational analysis methods

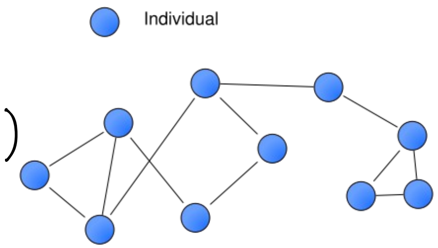


How do we know organisations are safe?





Design principles:	High-level, programmatic
Architecture and components:	Partly known, partly unknown
Models:	Semi-formal,
Analysis methods:	Ad hoc, unproven
Mode of operation:	Partly defined, complex
Structural stability:	Stable (formal), volatile (informal)
Functional stability:	Good, hysteretic (lagging).



Safety as reduction/elimination of risk

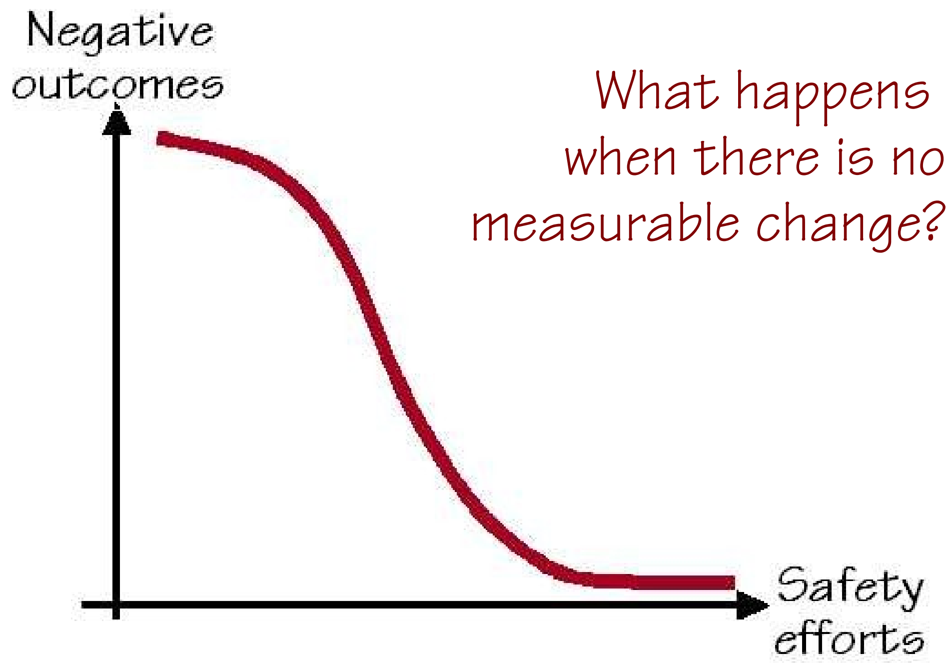
The common understanding of safety implies a distinction between:

- A normal state where everything works as it should and where the outcomes / products are acceptable (positive or as intended).
- A failed state where normal operations are disrupted or impossible, and where the outcomes/products are unacceptable (negative or not as intended).

The purpose of safety (management) is to maintain a normal state by preventing disruptions or disturbances.

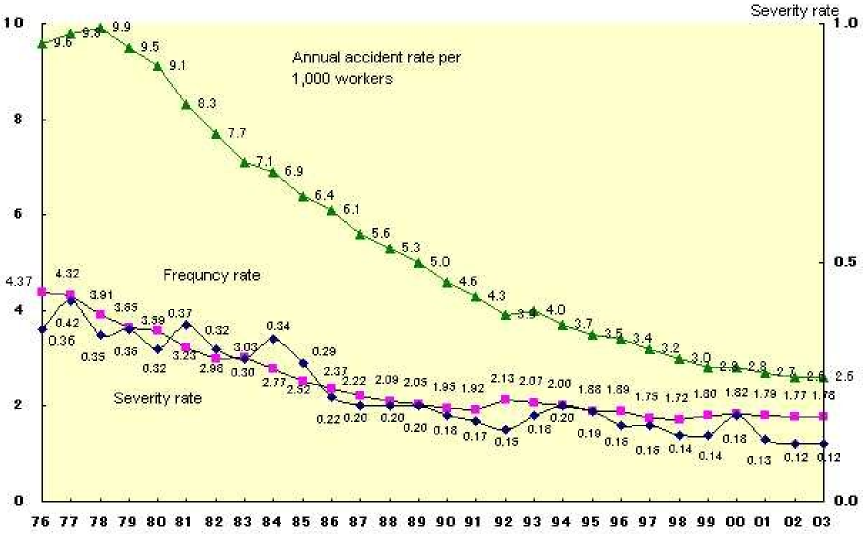
Safety efforts are normally driven by what has happened in the past, and are therefore reactive.

The level of safety is measured by the absence of negative outcomes.

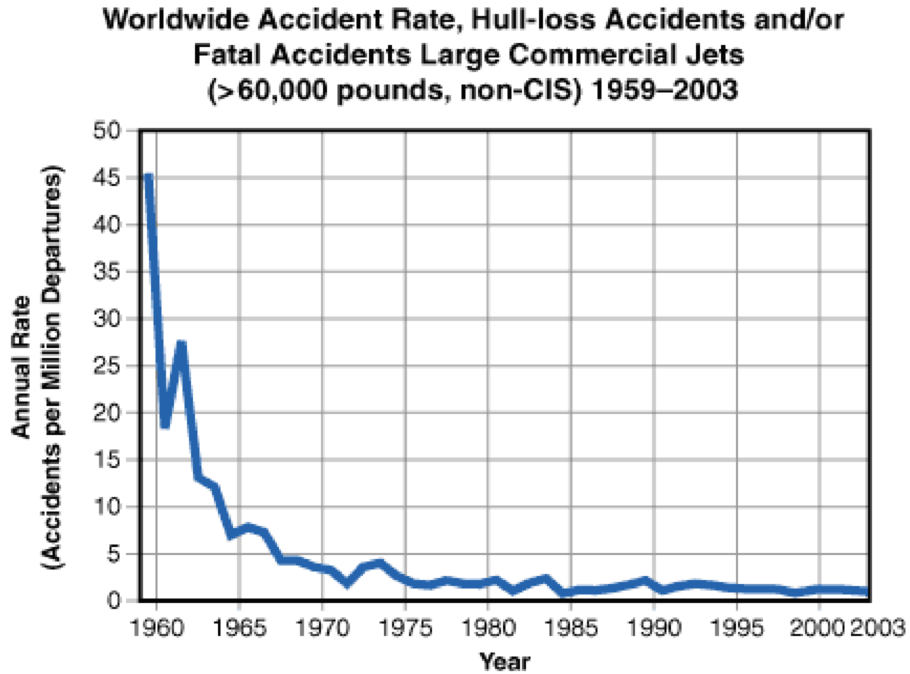


What happens when there is no measurable change?

Safety measured by accident/incidents



European Technology Platform on Industrial Safety (ETPIS) milestones:
- 25% reduction in accidents by 2020
- Programmes in place by 2020 to continue accident reduction at a rate of > 5% per year.

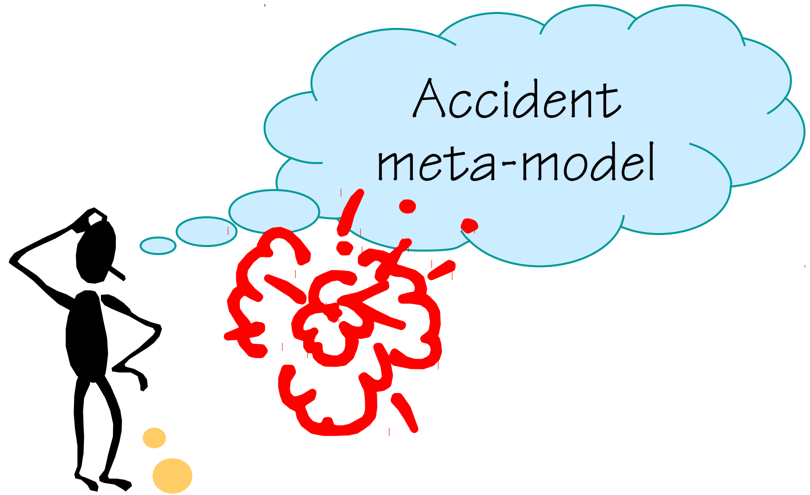


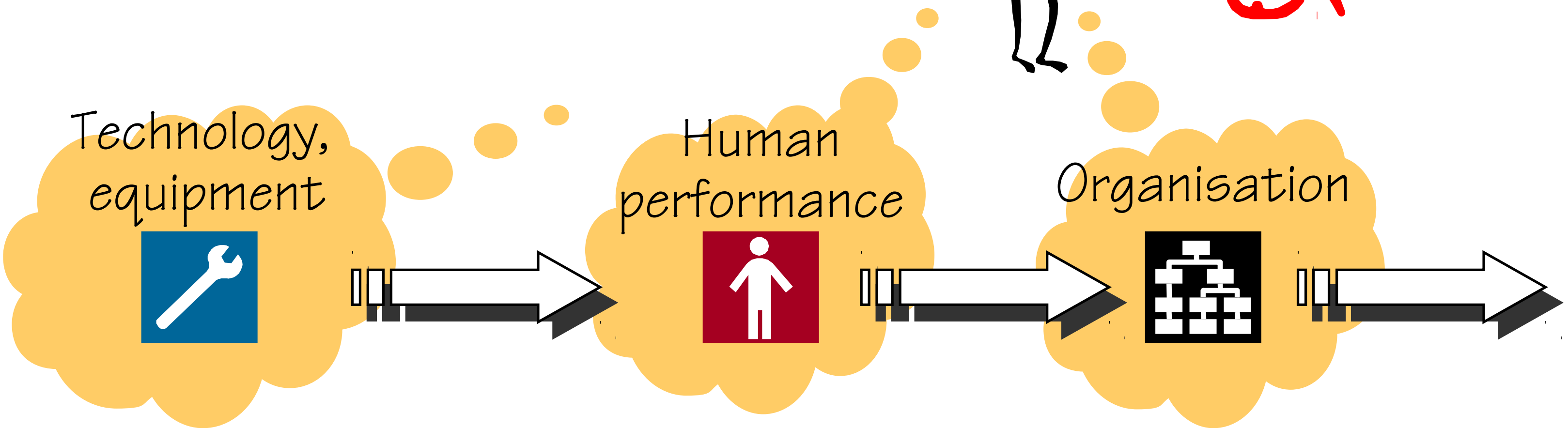
"Safety is a dynamic non-event"
(Karl Weick)

But how can a non-event be measured?

Thinking about accidents

"If something has happened, then there must be a cause"





Over the years, the attribution of causes has changed, but the accident meta-model remains the same.

Conclusions so far

- We need to be safe!
- We therefore need to know how and why things can go wrong
- Our understanding of how things can go wrong must match reality.
- Safety thinking has developed through three 'ages': technical, human factors, organisational.
- This has led to a revision of the possible / typical causes, but thinking is still dominated by a focus on failures and a belief in cause-effect relations (causal explanations).