SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

Understanding Accidents, or How (Not) to Learn from the Past

Professor Erik Hollnagel
University of Southern Denmark
Odense, Denmark
E-mail: hollnagel.erik@gmail.com

When things go wrong …

.. we try to find a cause - sometimes even a "root cause"

Three ages of industrial safety

Hale & Hovden (1998)

THINGS CAN GO WRONG

BECAUSE TECHNOLOGY FAILS

Age of technology

1850 1900 1950 2000

1769 Industrial Revolution

1893 Railroad Safety Appliance Act

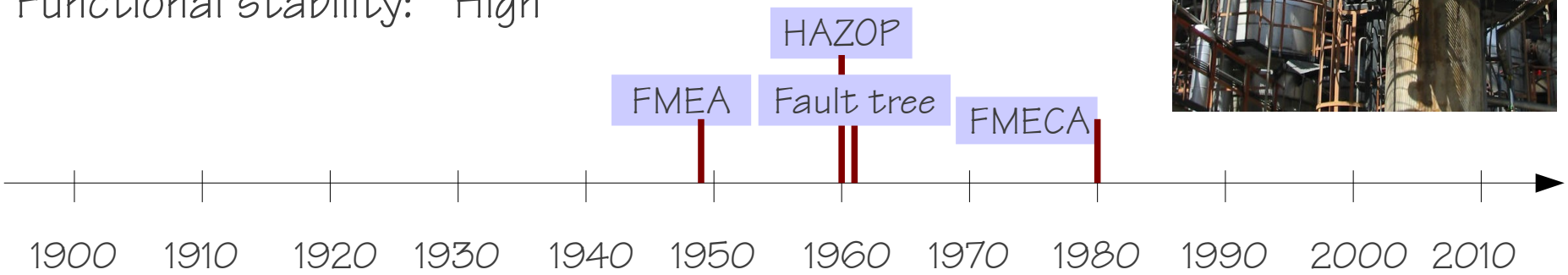
1931 Industrial accident prevention

IT Revolution

1961 Fault tree analysis

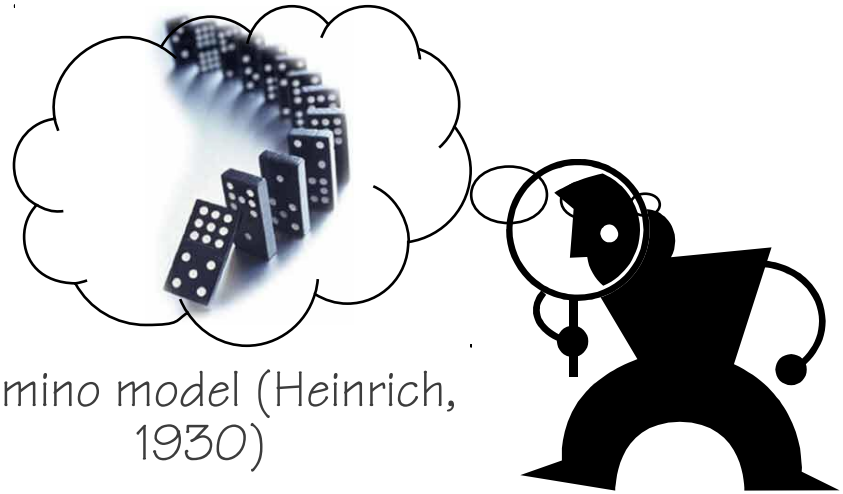
How do we know technology is safe?

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



Simple, linear cause-effect model

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

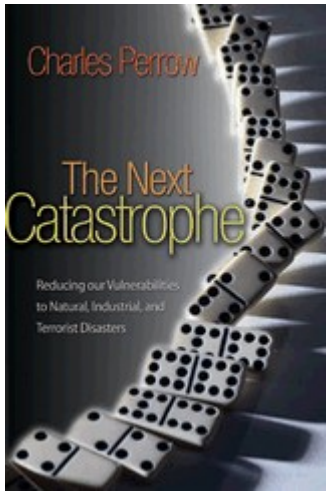


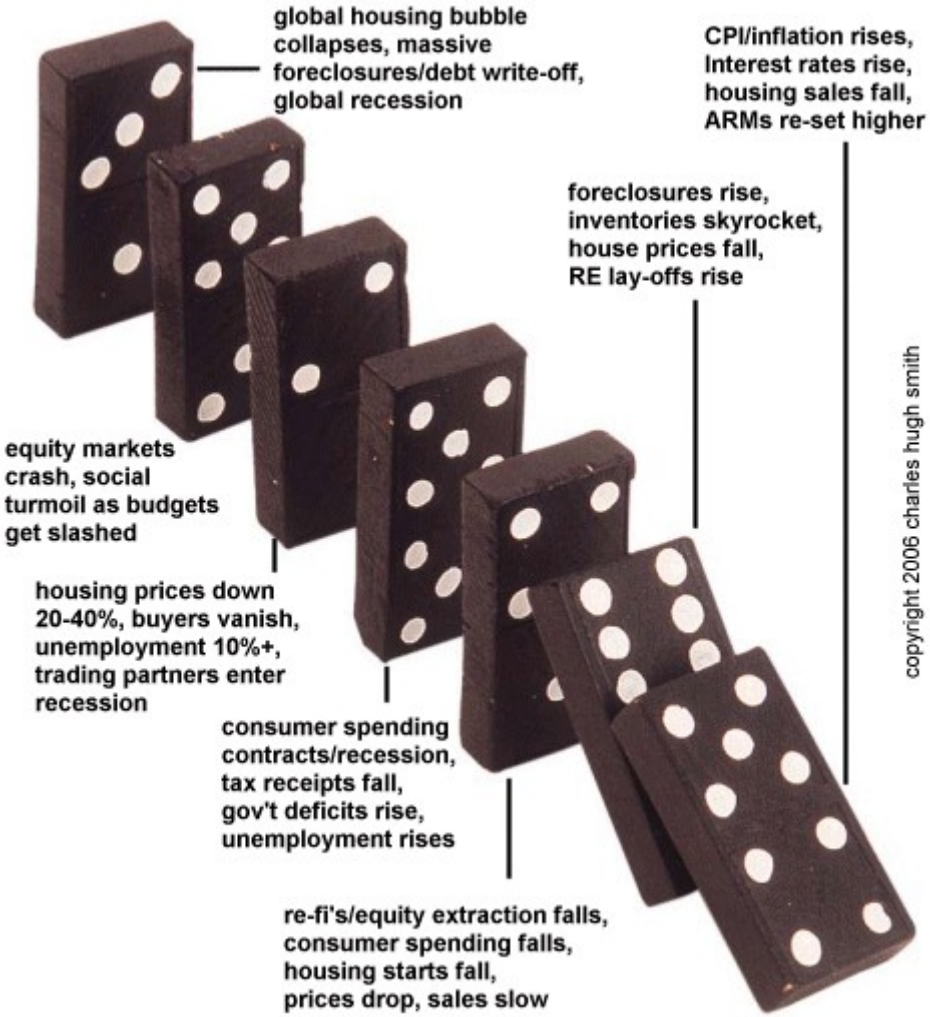
Domino model (Heinrich, 1930)

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). The future is a "mirror" image of the past.

Domino thinking everywhere





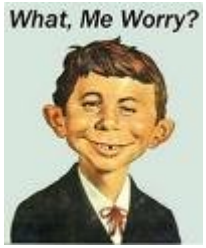
Root cause analysis

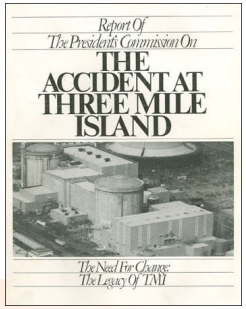
(1) Ask why today's condition occurred,
(2) Record the answers,
(3) Then ask why for each answer, again and again.

This allows to proceed further, by asking why, until the desired goal of finding the "root" causes is reached.

But when should the search for the root cause stop?

Three ages of industrial safety





THINGS CAN GO WRONG BECAUSE THE HUMAN FACTOR FAILS

Age of human factors

Age of technology

1850 1900 1950 2000

1769 Industrial Revolution

1893 Railroad Safety Appliance Act

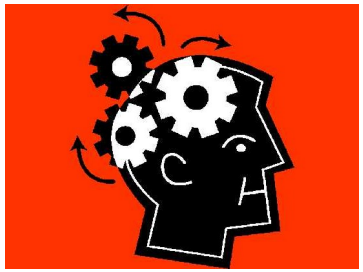
1931 Industrial accident prevention

IT Revolution

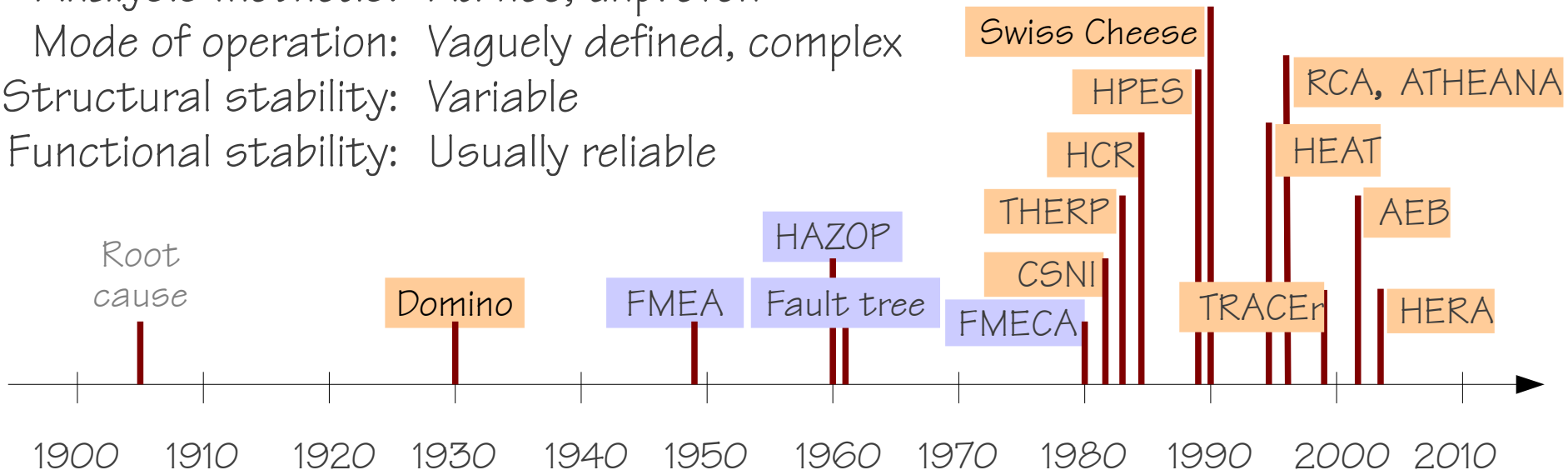
1961 Fault tree analysis

1979 Three Mile Island

How do we know humans are safe?

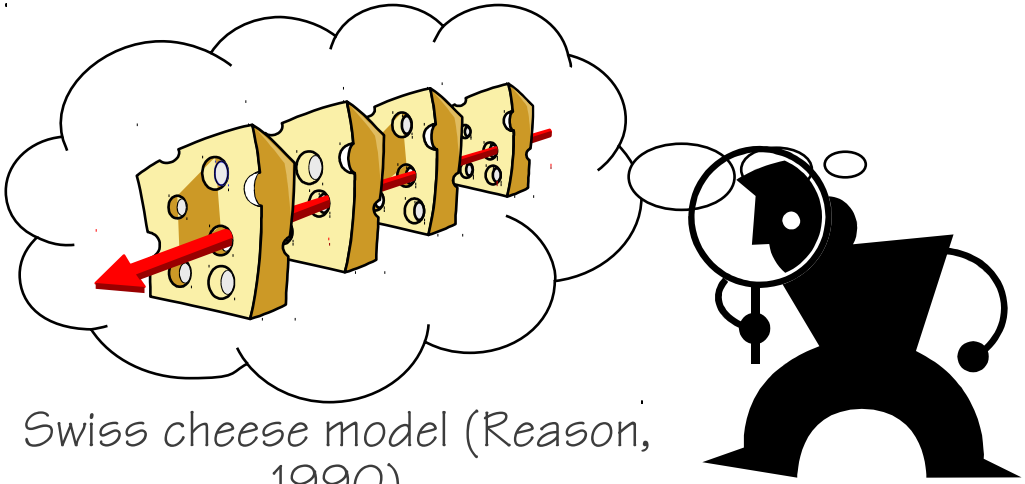


Design principles:	Unknown, inferred
Structure / components:	Incompletely known
Models:	Mainly analogies
Analysis methods:	Ad hoc, unproven
Mode of operation:	Vaguely defined, complex
Structural stability:	Variable
Functional stability:	Usually reliable



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.

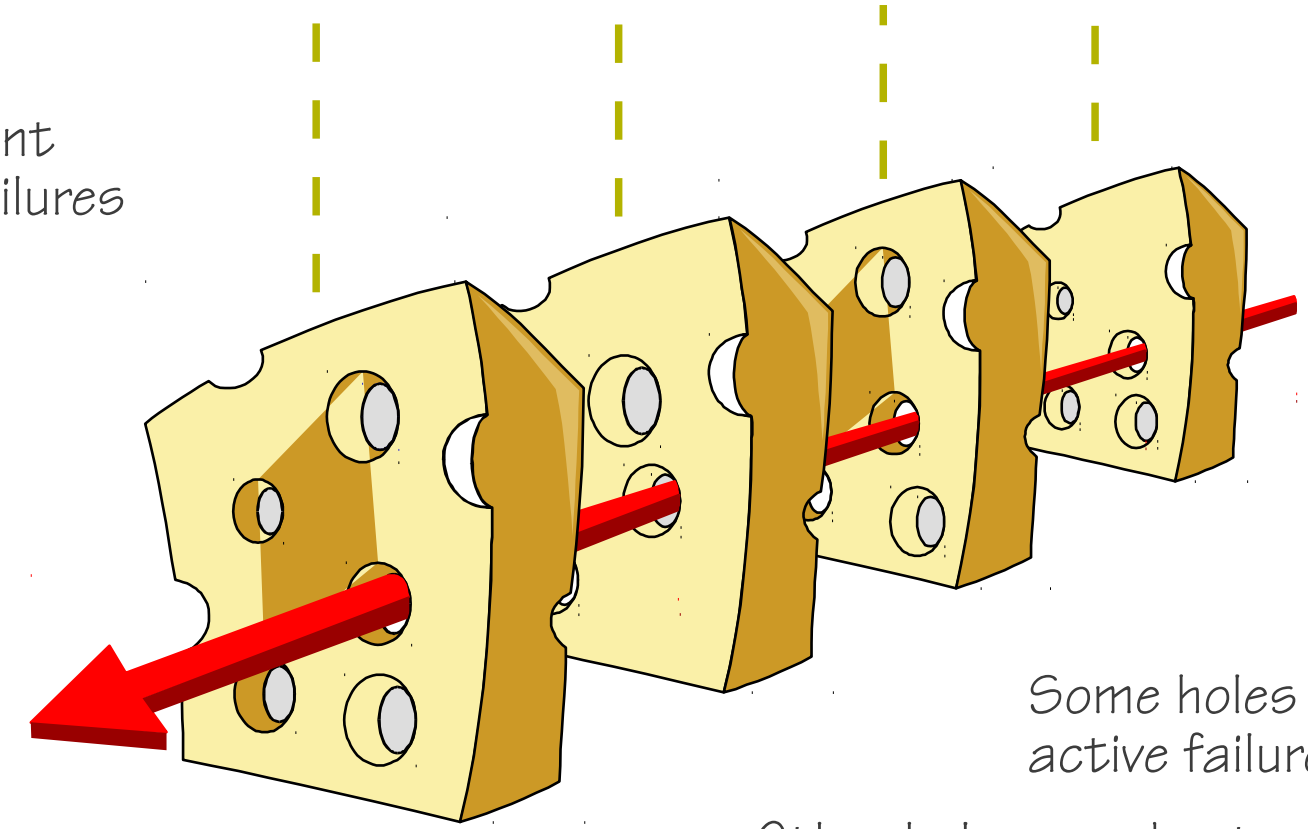
Hazards-risks: Due to degradation of components (organisational, human, technical), hence looking for drift, degradation and weaknesses

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

"Swiss cheese" model

Multiple layers of defences, barriers, and safeguards.

The holes represent weaknesses or failures of defences, barriers, and safeguards



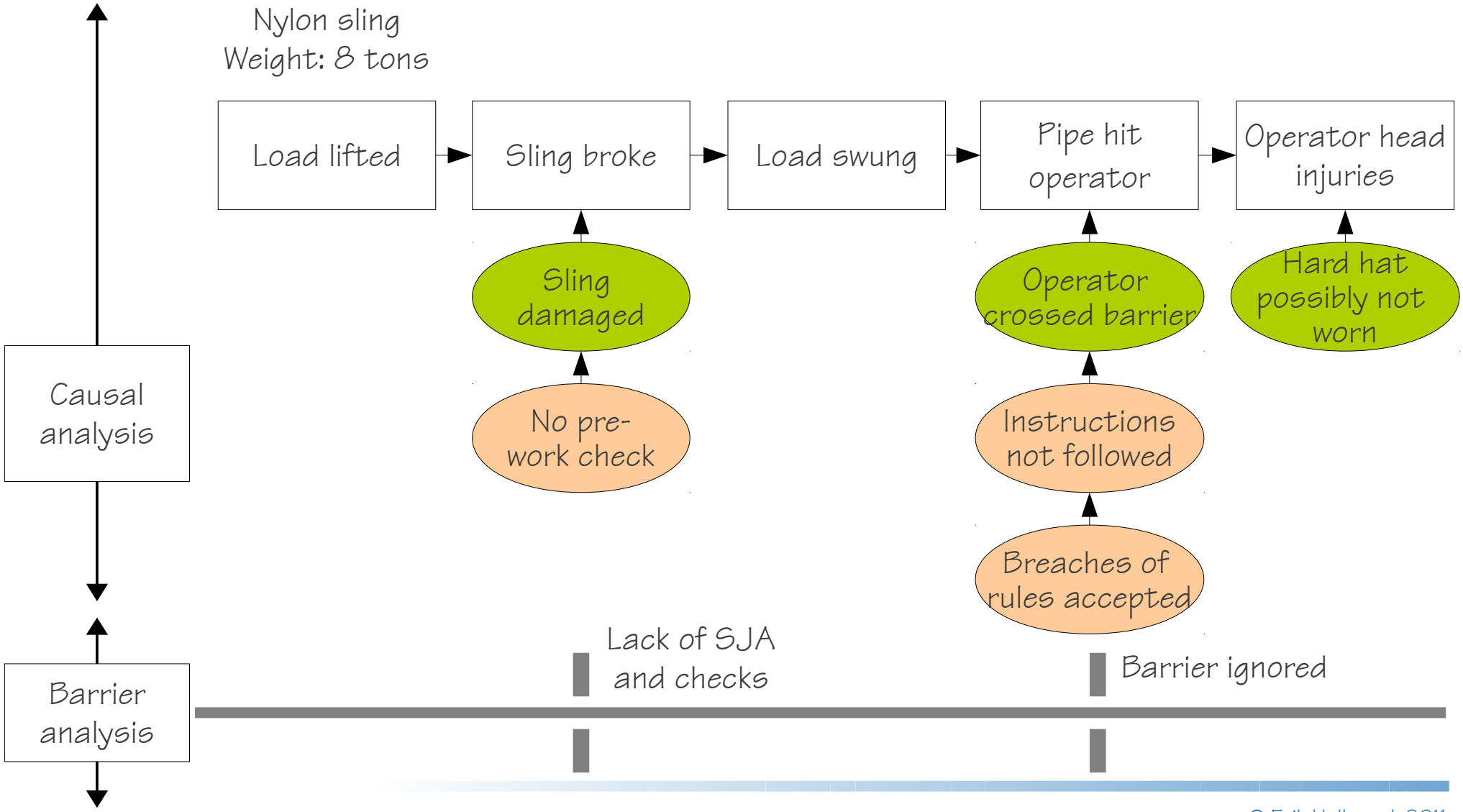
Hazard

Loss

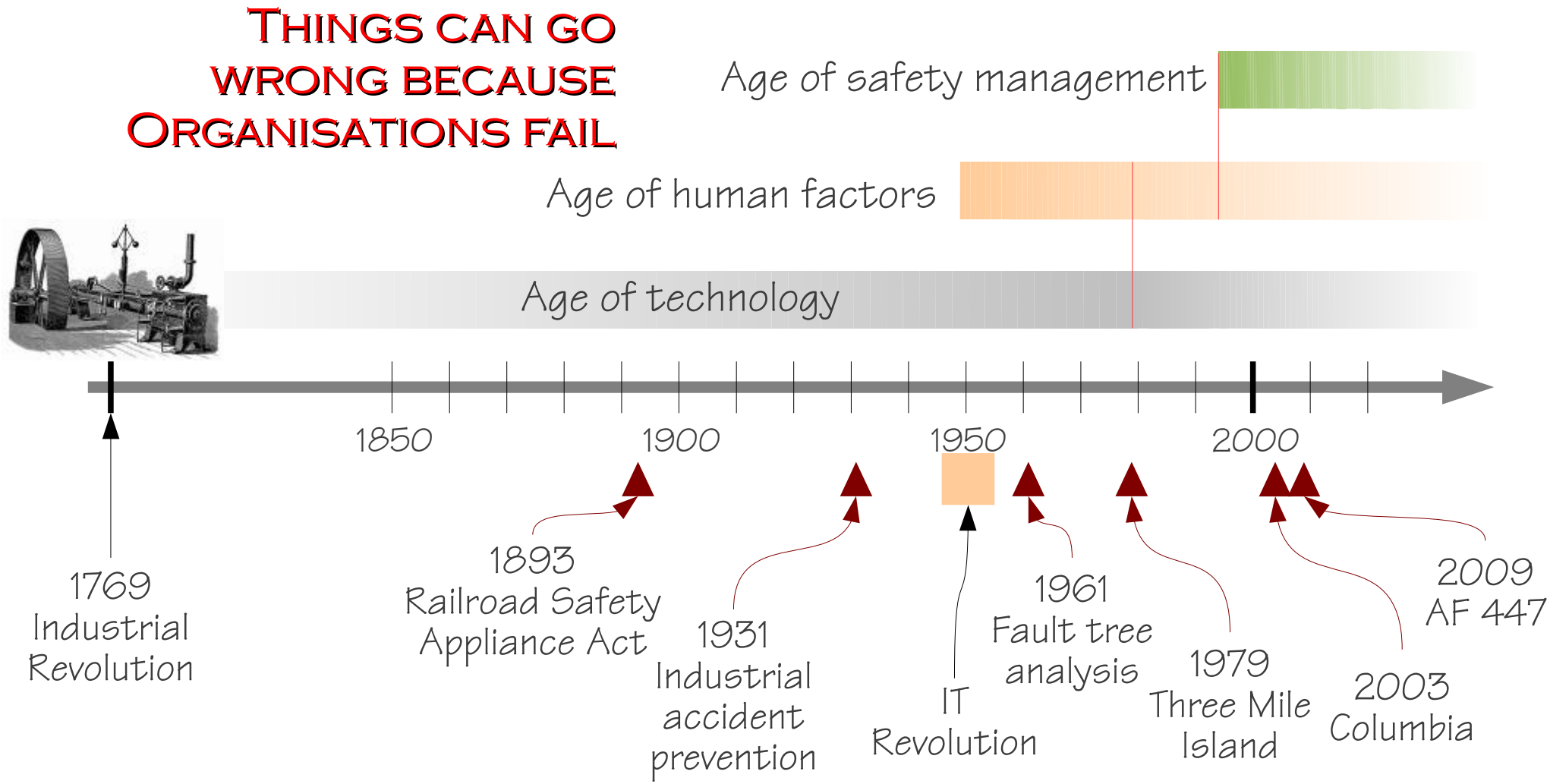
Some holes are due to active failures

Other holes are due to latent conditions

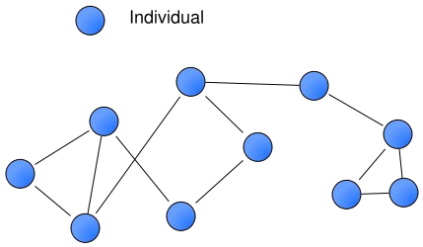
MTO diagram



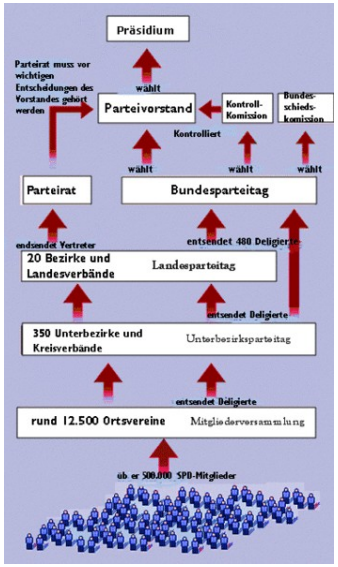
Three ages of industrial safety

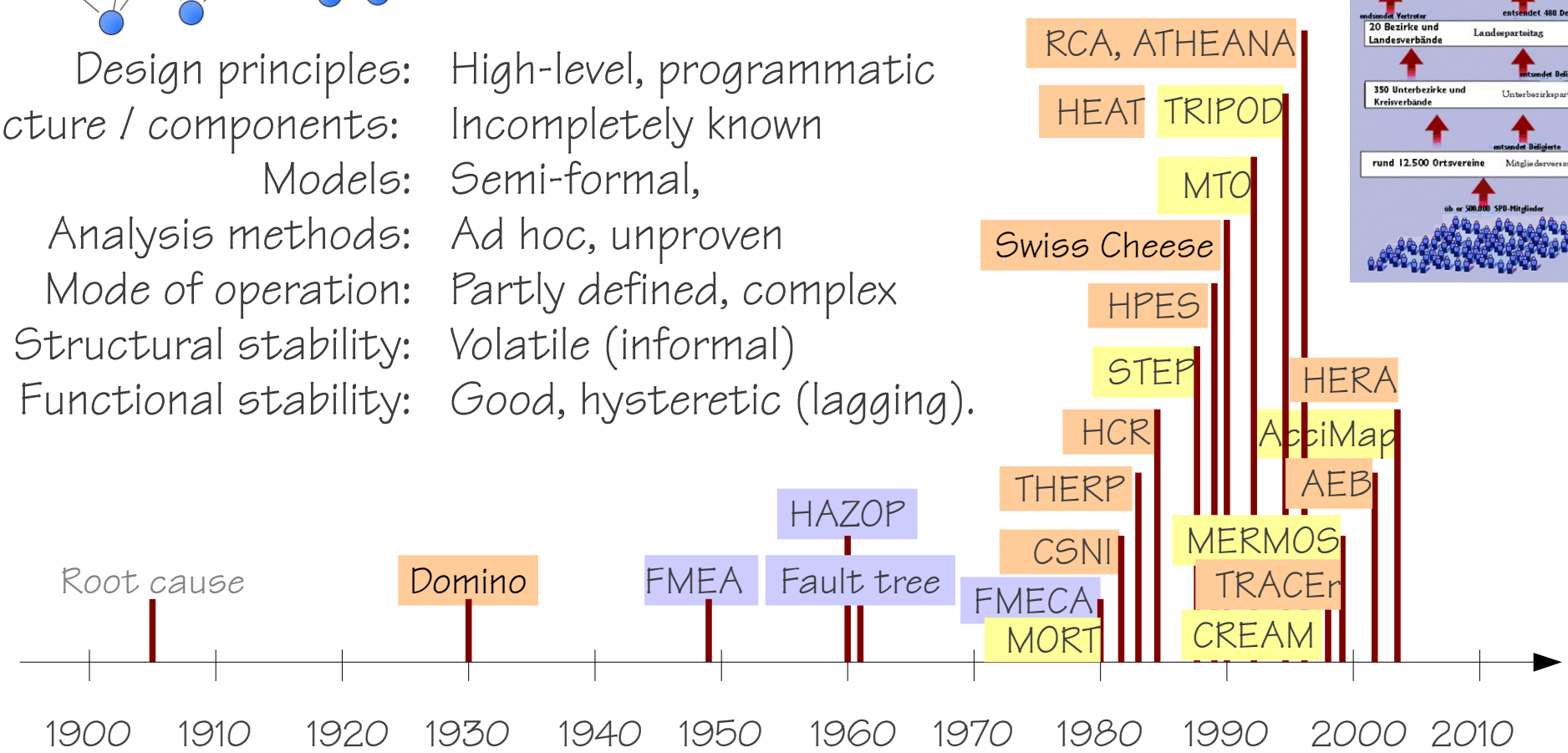


How do we know organisations are safe?



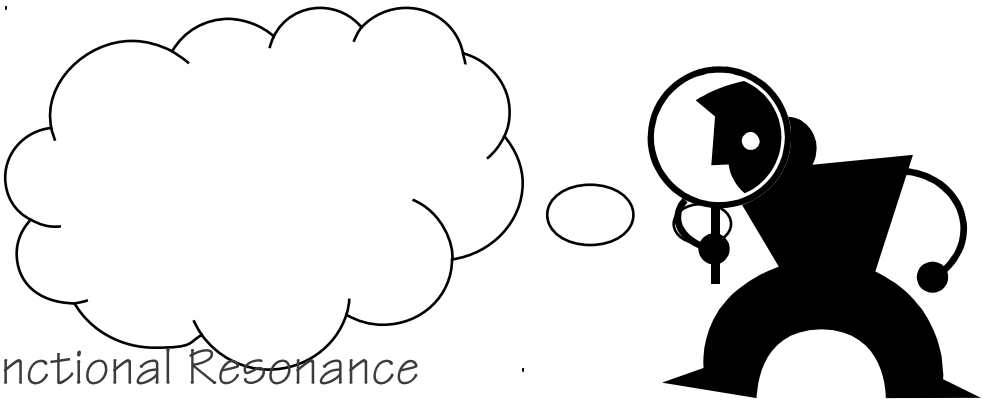
Design principles:	High-level, programmatic
Structure / components:	Incompletely known
Models:	Semi-formal,
Analysis methods:	Ad hoc, unproven
Mode of operation:	Partly defined, complex
Structural stability:	Volatile (informal)
Functional stability:	Good, hysteretic (lagging).





Non-linear accident model

Assumption: Accidents result from unexpected combinations (resonance) of variability of everyday performance.



Functional Resonance Accident Model

Consequence: Accidents are prevented by monitoring and damping variability. Safety requires constant ability to anticipate future events.

Hazards-risks: Emerge from combinations of performance variability (socio-technical system), hence looking for ETTO* and sacrificing decision

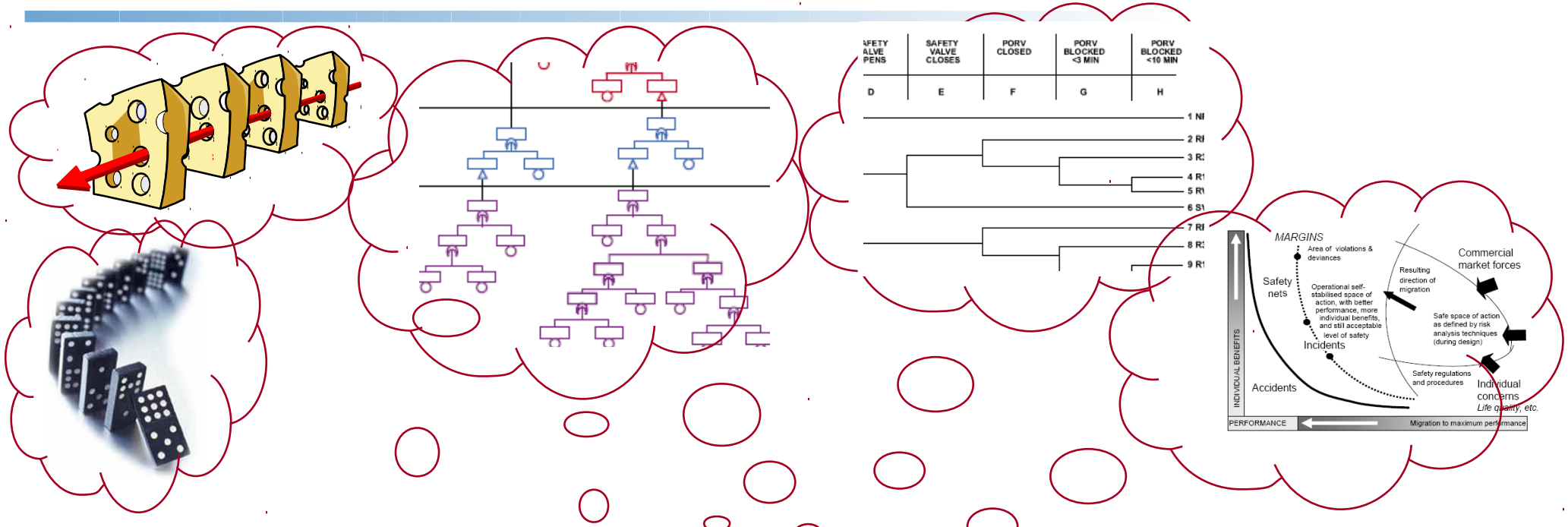
* ETTO = Efficiency-Thoroughness Trade-Off

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

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 everyday performance adjustments based on experience.
Accidents are emergent	Accidents are consequences of everyday adjustments, rather than of failures. Without such adjustments, systems would not work

Theories and models of the negative



Accidents are caused by people, due to carelessness, inexperience, and/or wrong attitudes.

Technology and materials are imperfect so failures are inevitable

Organisations are complex but brittle with limited memory and unclear distribution of authority

Effect-cause reasoning

What happened here?

What happened here?

What happened here?

If there is an effect, there must also be a cause

The search for a cause is guided by how we think accidents happen (= accident model)

↓

The cause is usually the most unreliable component or part. → This is often also the part that is least understood.

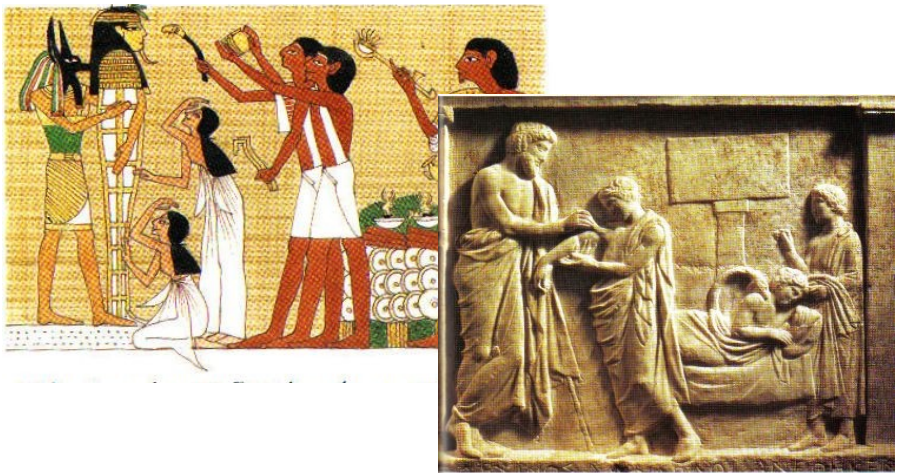
The Code of Hammurabi (1792-1750)

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.

The causality dilemma



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

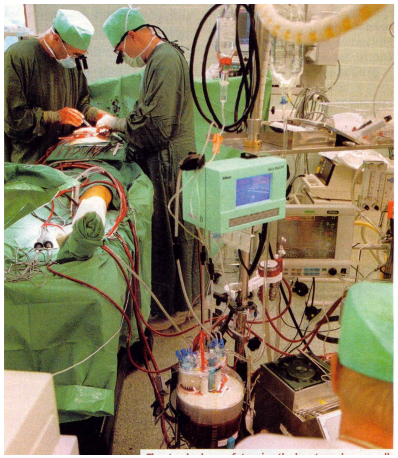
Does it still make sense to think of direct responsibility?

Failures or successes?

When something goes wrong, e.g., 1 event out of 10.000 (10E-4), humans are assumed to be responsible in 80-90% of the cases.

Who or what are responsible for the remaining 10-20%?

Investigation of failures is accepted as important.



When something goes right, e.g., 9.999 events out of 10.000, are humans also responsible in 80-90% of the cases?

Who or what are responsible for the remaining 10-20%?

Investigation of successes is rarely undertaken.

Work as imagined – work as done

Work-as-imagined is what designers, managers, regulators, and authorities believe happens or should happen.

Safety I: Failure is explained as a breakdown or malfunctioning of a system and/or its components (non-compliance, violations).

Work-as-done is what actually happens.

Safety II: Individuals and organisations must adjust to the current conditions in everything they do. Performance must be variable in order for things o work.

Different models => different practices

	Basic principle	Purpose of analysis	Typical reaction
Simple, linear model	Causality (Single or multiple causes)	Find specific causes and cause-effect links.	Eliminate causes and links. Improve responses
Complex, linear model	Hidden dependencies	Combinations of unsafe acts and latent conditions	Strengthen barriers and defences. Improve observation (of indicators)
Non-linear (systemic) model	Dynamic dependency, functional resonance	Close couplings and complex interactions	Monitor & control performance variability. Improve anticipation

WYLFIWYF

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

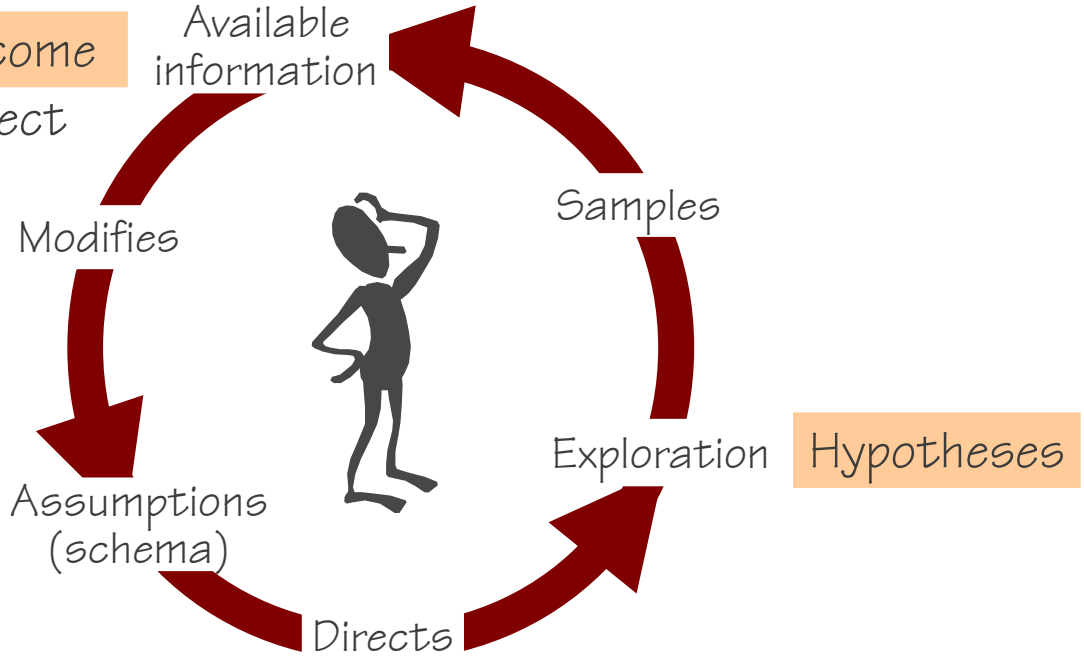
This means that an accident investigation usually finds what it looks for: the assumptions about the nature of accidents guide the analysis.

Accident → Outcome

Cause — Effect

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

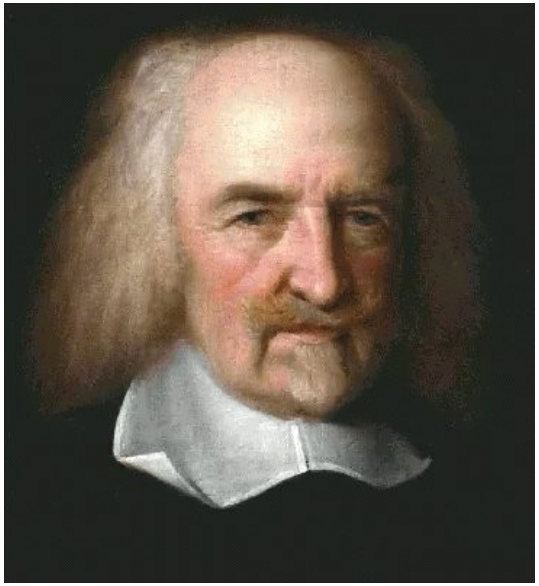
'Causes'



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

Looking and finding

Ignorance of remote causes, disposeth men to attribute all events, to the causes immediate, and Instrumentall: For these are all the causes they perceive.



Thomas Hobbes. Leviathan, Chapter XI (1588-1679)