SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# The Requisite Variety of Risk Assessment: Catching up with nature

Erik Hollnagel

Professor
Department of Public Health
University of Southern Denmark

TÜV Stiftung Süd Visiting Professor
Technische Universität München
Germany

hollnagel.erik@gmail.com
www.functionalresonance.com

© Erik Hollnagel, 2011

# Law of requisite variety

Variety of outcome | Variety of system | Variety of regulator

$$\text{Min}\ (V_O) = V_D - V_R$$

The variety of the outcomes (of a system) can only be decreased by increasing the variety in the controller of that system. (Ashby, 1957)

Every good regulator of a system must be a model of that system”

(Conant & Ashby, 1970).

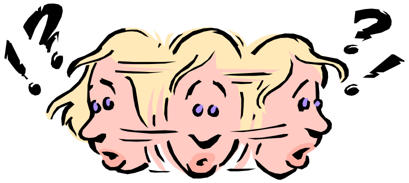
Requisite imagination is the ability to imagine key aspects of the future we are planning. … (I)t involves anticipating what might go wrong, and how to test for problems when the design is developed.

Adamski & Westrum (2003)

Requisite variety of risk assessment: The models, concepts, and methods used in risk assessment must be able to represent the ‘socio-technical reality.’

© Erik Hollnagel, 2011

# 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 find out what did go wrong?

How can we predict what may go wrong?

Risk assessment

Predicting what may happen (possible consequences)

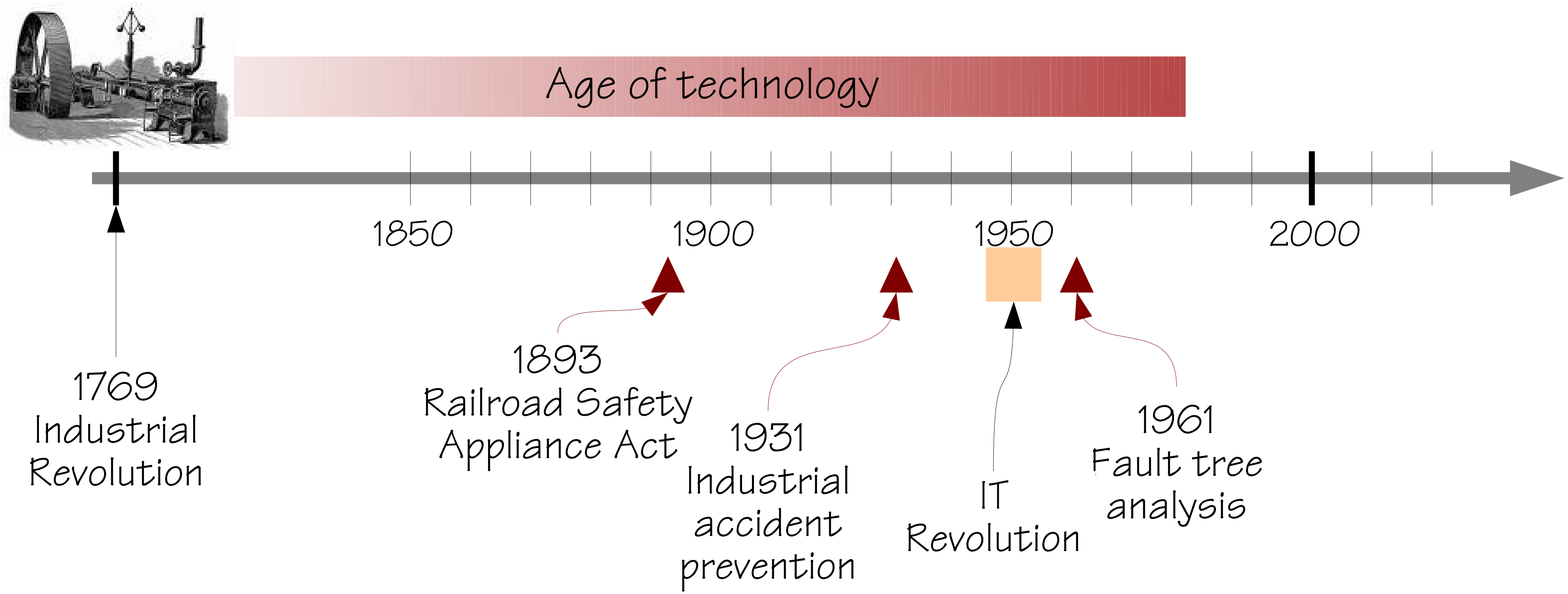
Elimination or prevention of potential risks

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

© Erik Hollnagel, 2011

# Three ages of industrial safety

Hale & Hovden (1998)



Age of technology

1850

1900

1950

2000

1769
Industrial
Revolution

1893
Railroad Safety
Appliance Act

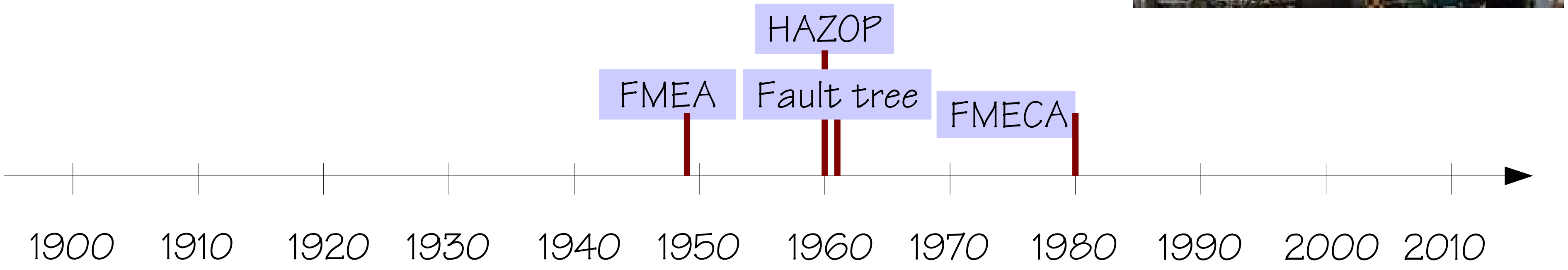
1931
Industrial
accident
prevention

IT
Revolution

1961
Fault tree
analysis

© Erik Hollnagel, 2011

# Technical analysis methods



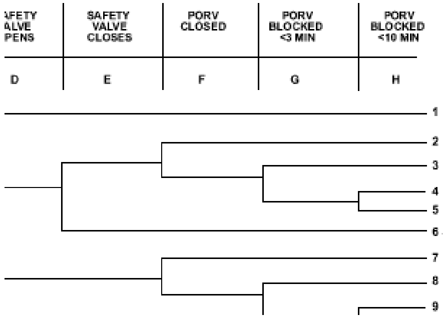
© Erik Hollnagel, 2011

# Risks as propagation of failures

If accidents happen like this ...

The culmination of a chain of events (linear cause-effect).

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



Probability of component failures in linear combinations.

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.

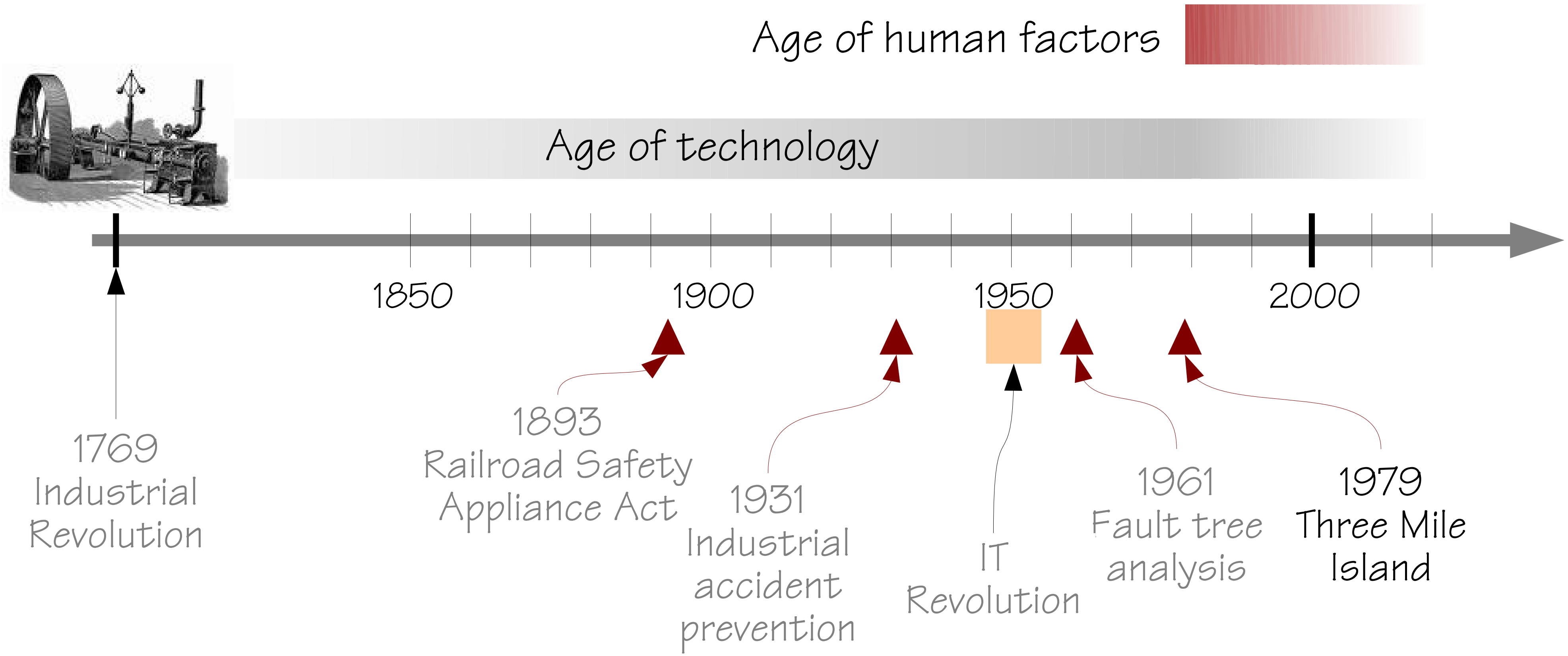
For simple causes it is enough to have simple models and simple methods.
The requisite variety is low.

© Erik Hollnagel, 2011

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# Three ages of industrial safety

Hale & Hovden (1998)



Age of human factors

Age of technology

1769
Industrial
Revolution

1893
Railroad Safety
Appliance Act

1931
Industrial
accident
prevention

IT
Revolution

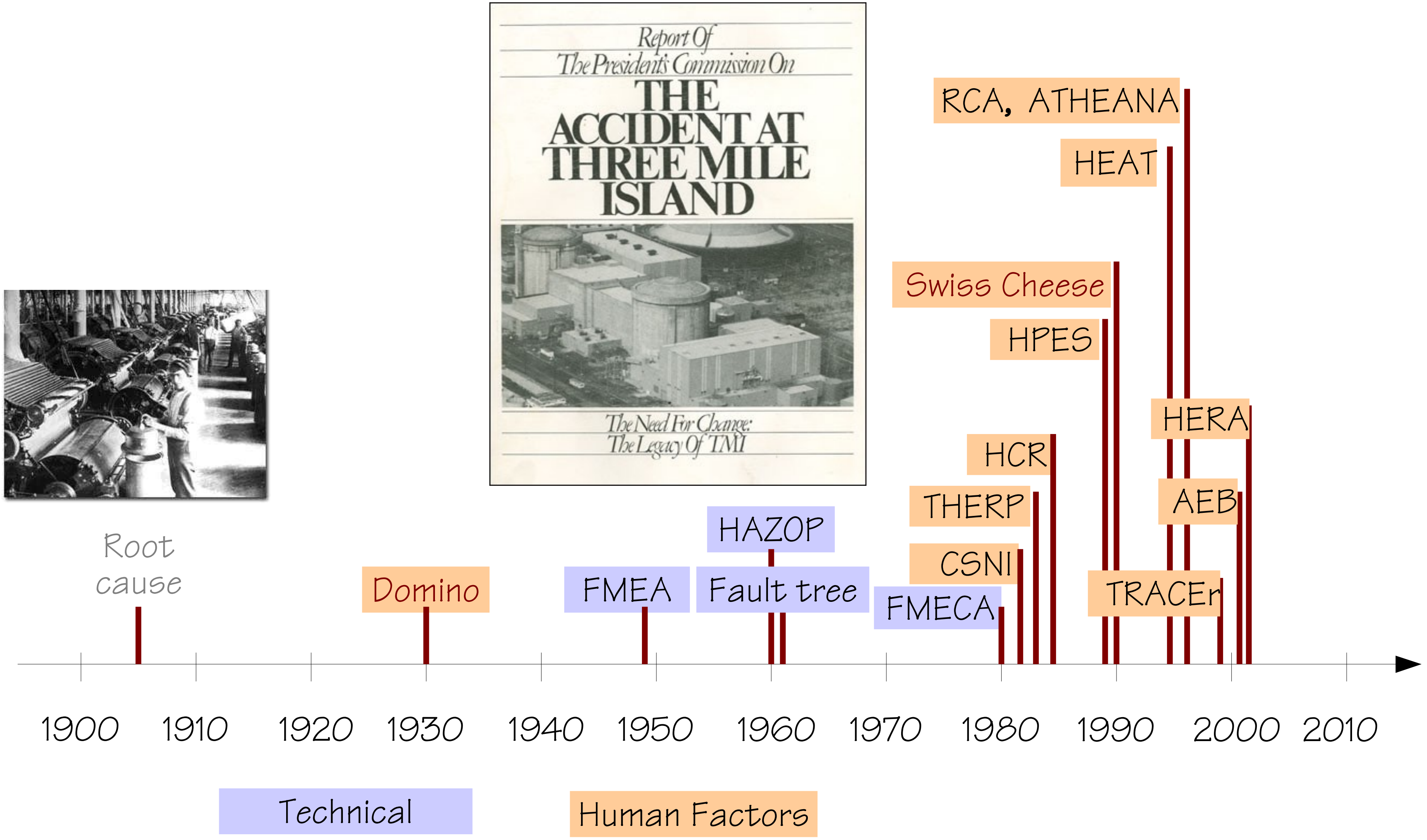
1961
Fault tree
analysis

1979
Three Mile
Island

© Erik Hollnagel, 2011

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# Human factors analysis methods

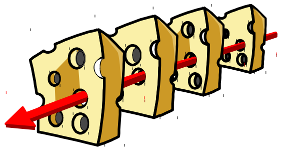


Report Of
The President's Commission On
THE ACCIDENT AT THREE MILE ISLAND
The Need For Change:
The Legacy Of TMI

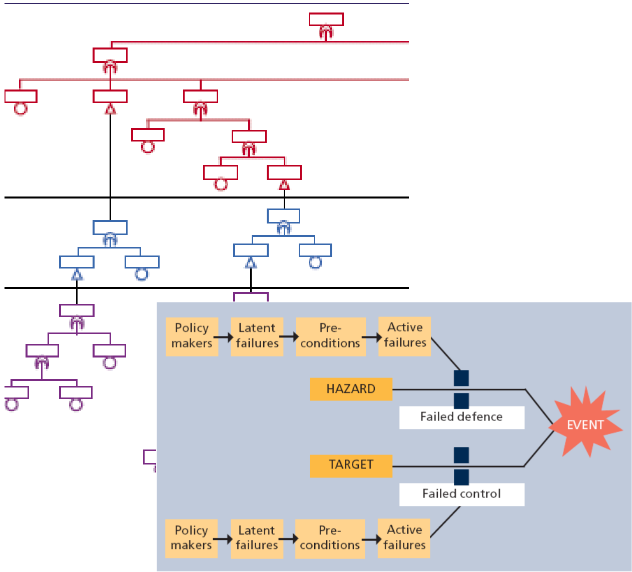
© Erik Hollnagel, 2011

# Risks as combinations of failures

If accidents happen like this ...



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



Combinations of active failures and latent conditions.

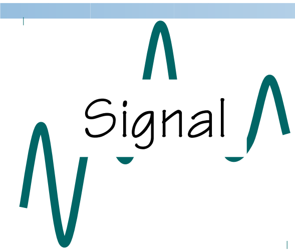
Likelihood of weakened defenses combined with active failures

Look for degraded barriers or defences in combination with active failures.

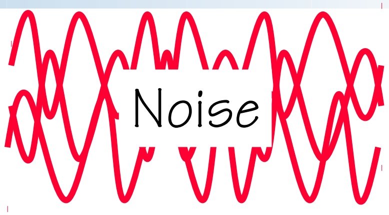
Multiple causal sequences with manifest or latent effects.

Complicated socio-technical systems require more elaborate models and methods.
The requisite variety is larger and steadily growing.

# From first to second generation HRA

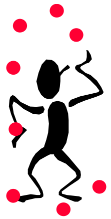


+

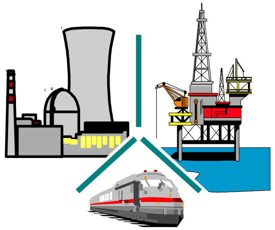


→ Failure probability

First generation HRA



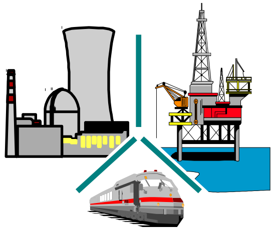
+



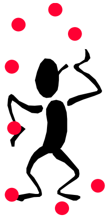
→ Human Error Probability

Failure probability is an attribute of the human operator.
The requisite variety is set by how human performance can fail..

Second generation HRA



+



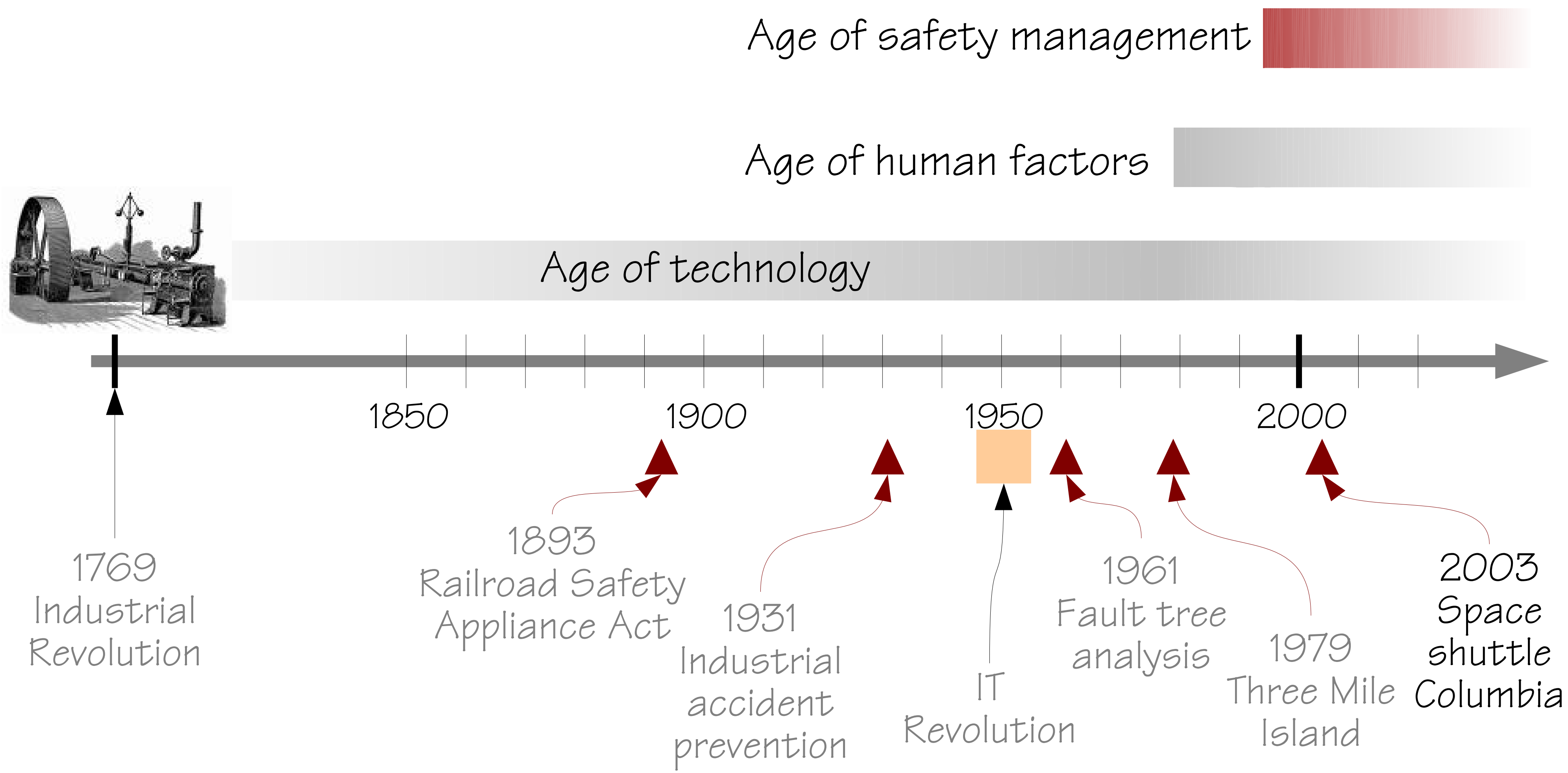
→ p(failure)

Failure probability is an attribute of the working conditions or context.
The requisite variety is set by what can happen in the context.

© Erik Hollnagel, 2011

# Three ages of industrial safety

Hale & Hovden (1998)



Age of safety management

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

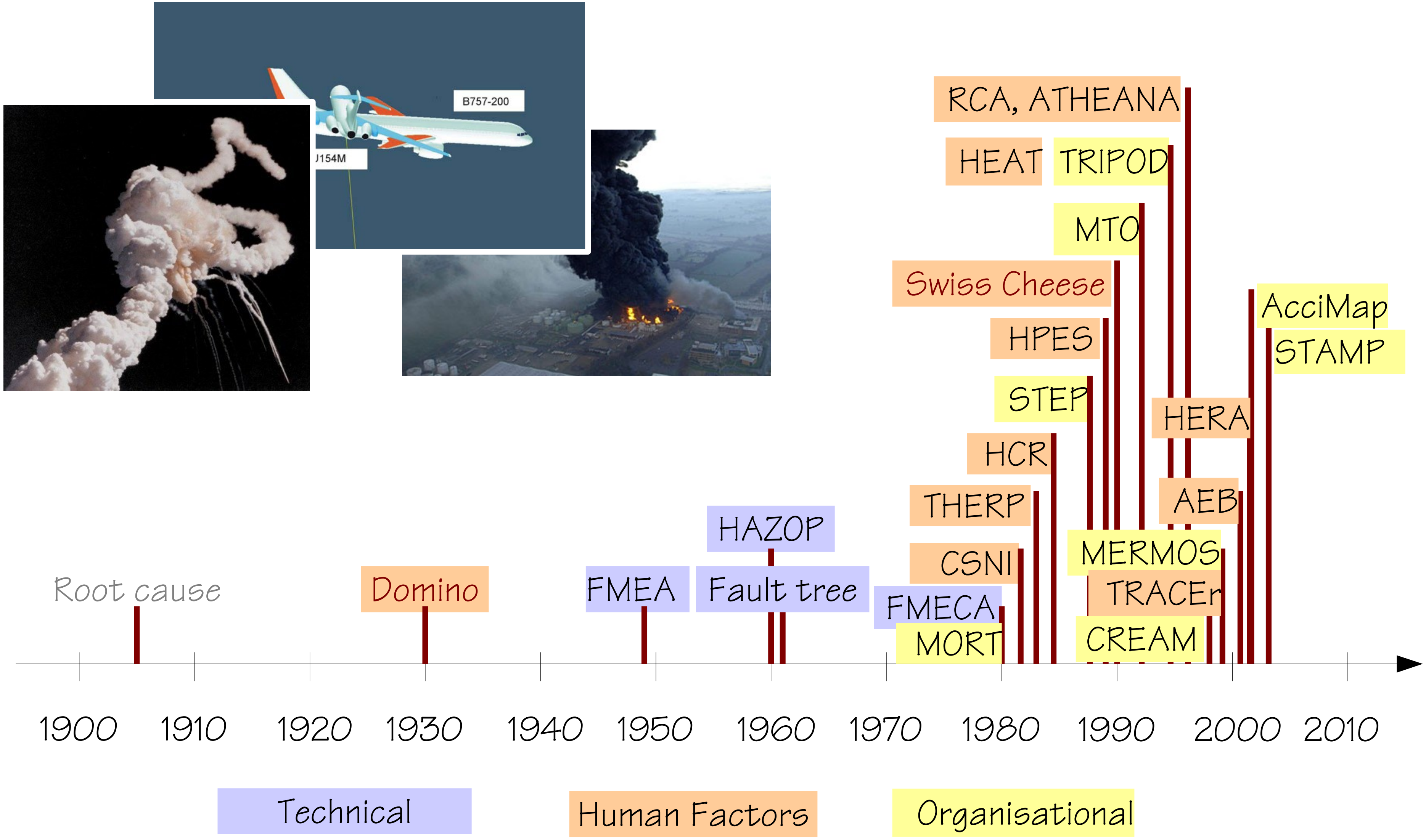
1961
Fault tree
analysis

1979
Three Mile
Island

2003
Space
shuttle
Columbia

© Erik Hollnagel, 2011

# Organisational analysis methods



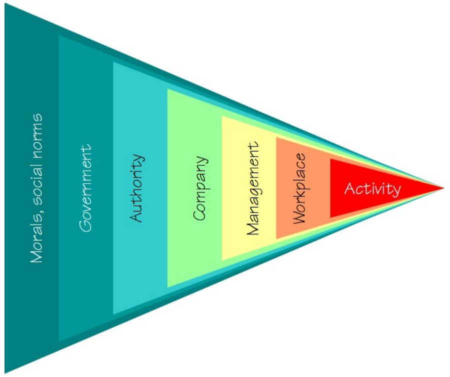
© Erik Hollnagel, 2011

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# Risk as determined by safety culture

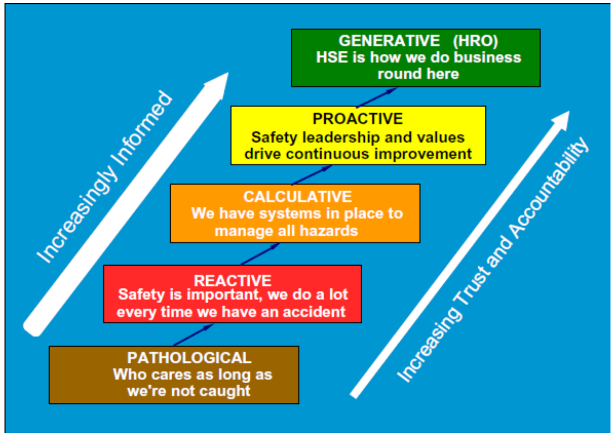
If accidents happen like this ...

Blunt end – sharp end



Organisational oversights and deficiencies

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


GENERATIVE (HRO)
HSE is how we do business round here
PROACTIVE
Safety leadership and values drive continuous improvement
CALCULATIVE
We have systems in place to manage all hazards
REACTIVE
Safety is important, we do a lot every time we have an accident
PATHOLOGICAL
Who cares as long as we're not caught
Increasingly Informed
Increasing Trust and Accountability

Level of safety culture

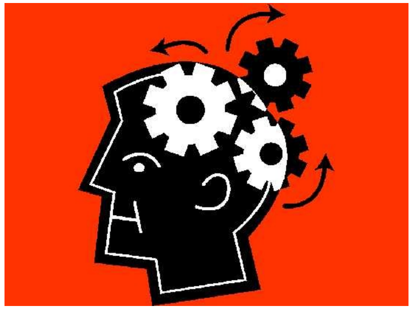
Look for organisational pathogens, violations, non-compliance

Deficiencies in organisational communication and management.

Safety management and safety culture require models and methods that can account for the organisational factor. The requisite variety is larger than what commonly used models and methods can provide.

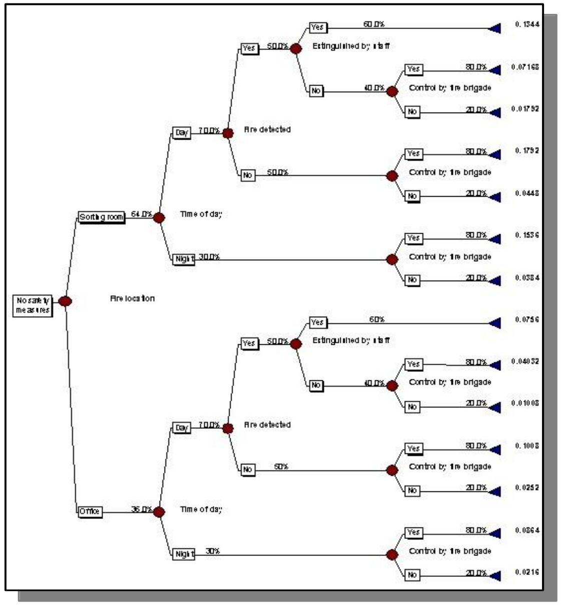
© Erik Hollnagel, 2011

# How do we know something is safe?

| | |  | |
|---|---|---|---|
| Design principles: | Clear and explicit | Unknown, inferred | High-level, programmatic |
| Architecture and components: | Known | Partly known, partly unknown | Partly known, partly unknown |
| Models: | Formal, explicit | Mainly analogies | Semi-formal |
| Analysis methods: | Standardised, validated | Ad hoc, unproven | Ad hoc, unproven |
| Mode of operation: | Well-defined (simple) | Vaguely defined, complex | Partly defined, complex |
| Structural stability: | High (permanent) | Variable | Stable (formal), volatile (informal) |
| Functional stability: | High | Usually reliable | Good (lagging). |

© Erik Hollnagel, 2011

# Common assumptions (~ 1970)



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

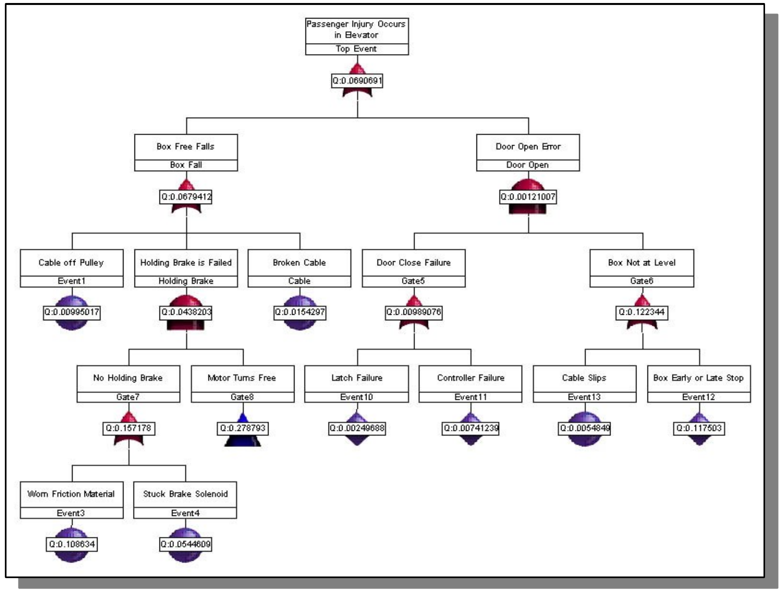
The function of each element is bimodal (true/false, work/fail)

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)

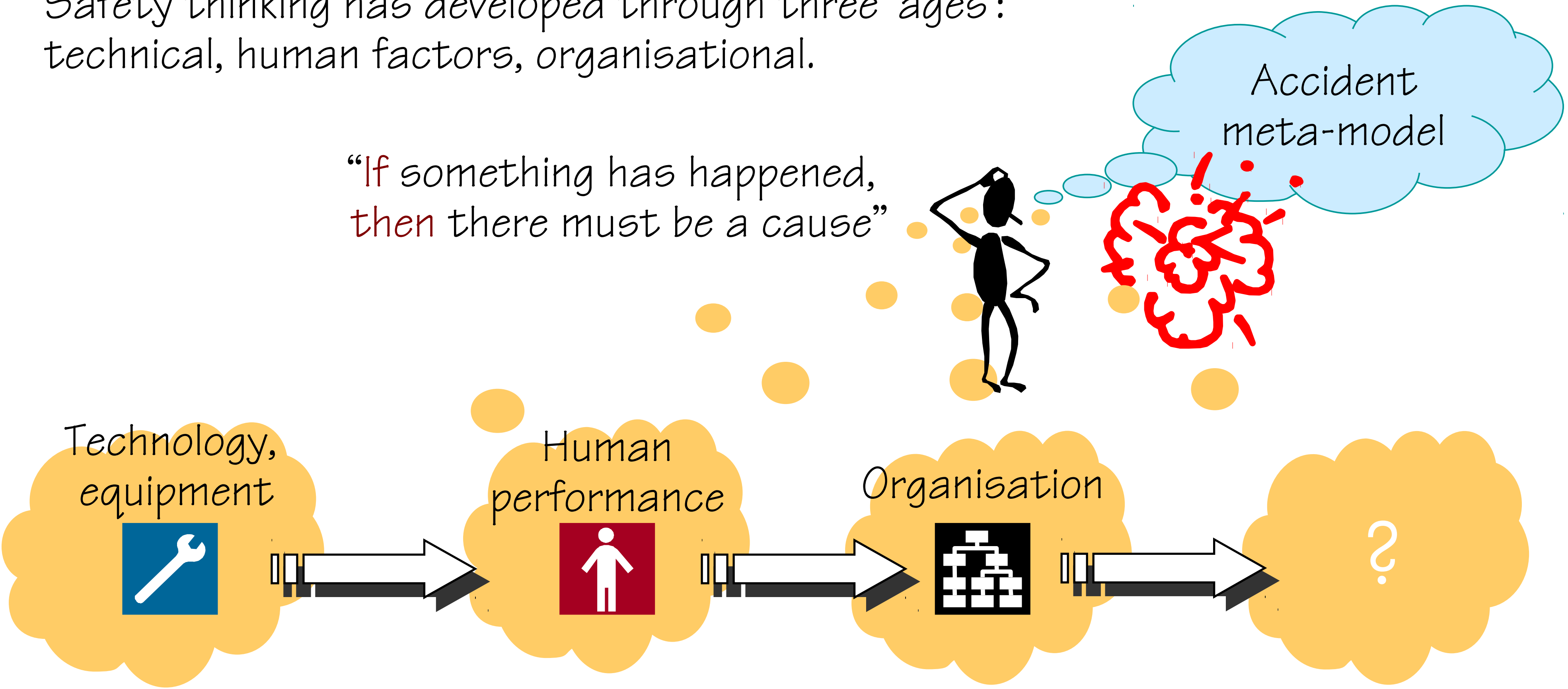
The influence from context/conditions is limited and quantifiable



© Erik Hollnagel, 2011

# Thinking about accidents

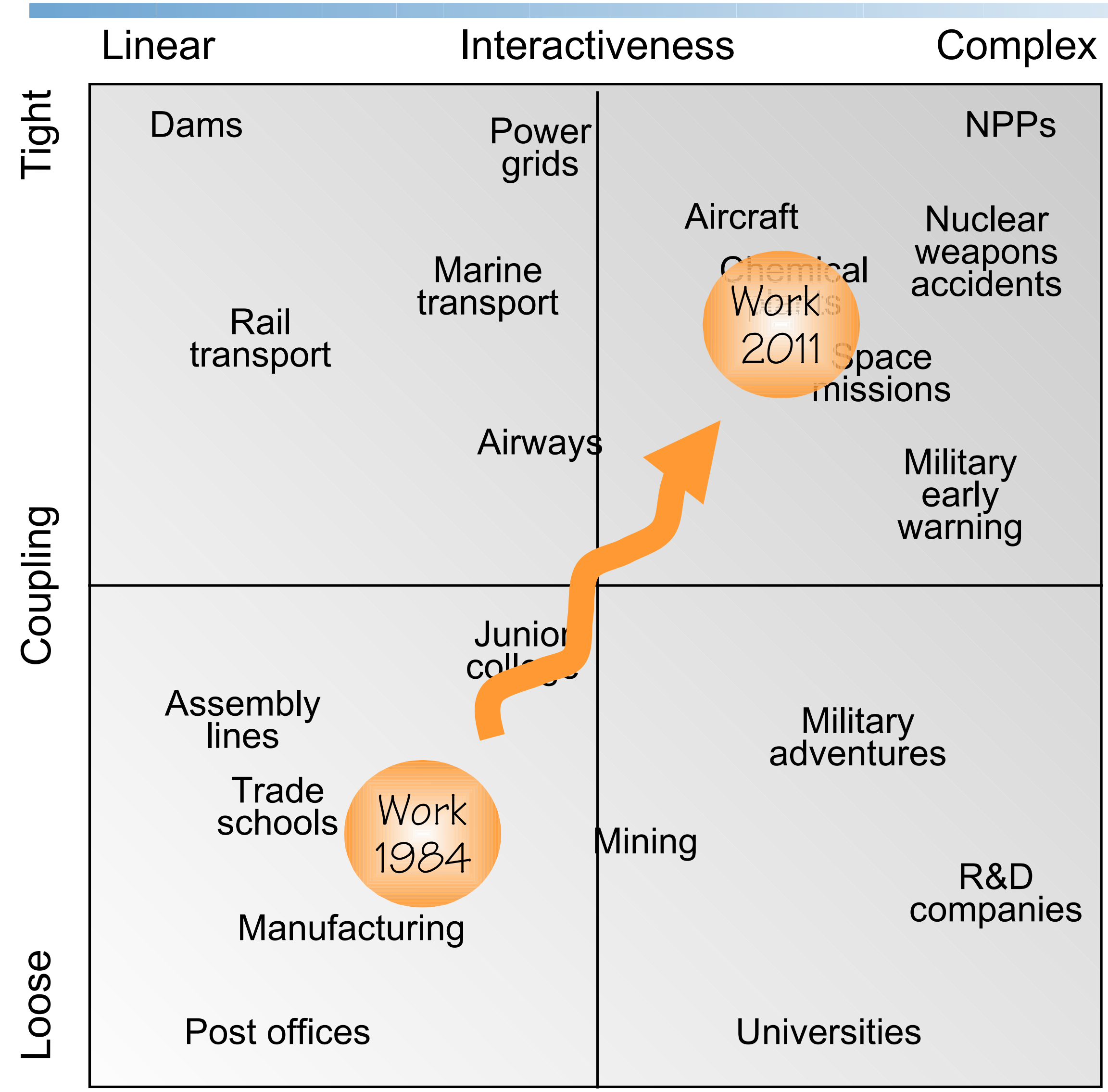
Safety thinking has developed through three 'ages': technical, human factors, organisational.



This has led to a revision of the typical causes, but models and methods still focus on failures and cause-effect relations. The variety is less than the requisite variety.

© Erik Hollnagel, 2011

# Coupling and interactiveness



Complex systems / interactions:
Tight spacing / proximity
Common-mode connections
Interconnected subsystems
Many feedback loops
Indirect information
Limited understanding

Tight couplings:
Delays in processing not possible
Invariant sequence
Little slack (supplies, equipment, staff)
Buffers and redundancies designed-in
Limited substitutability

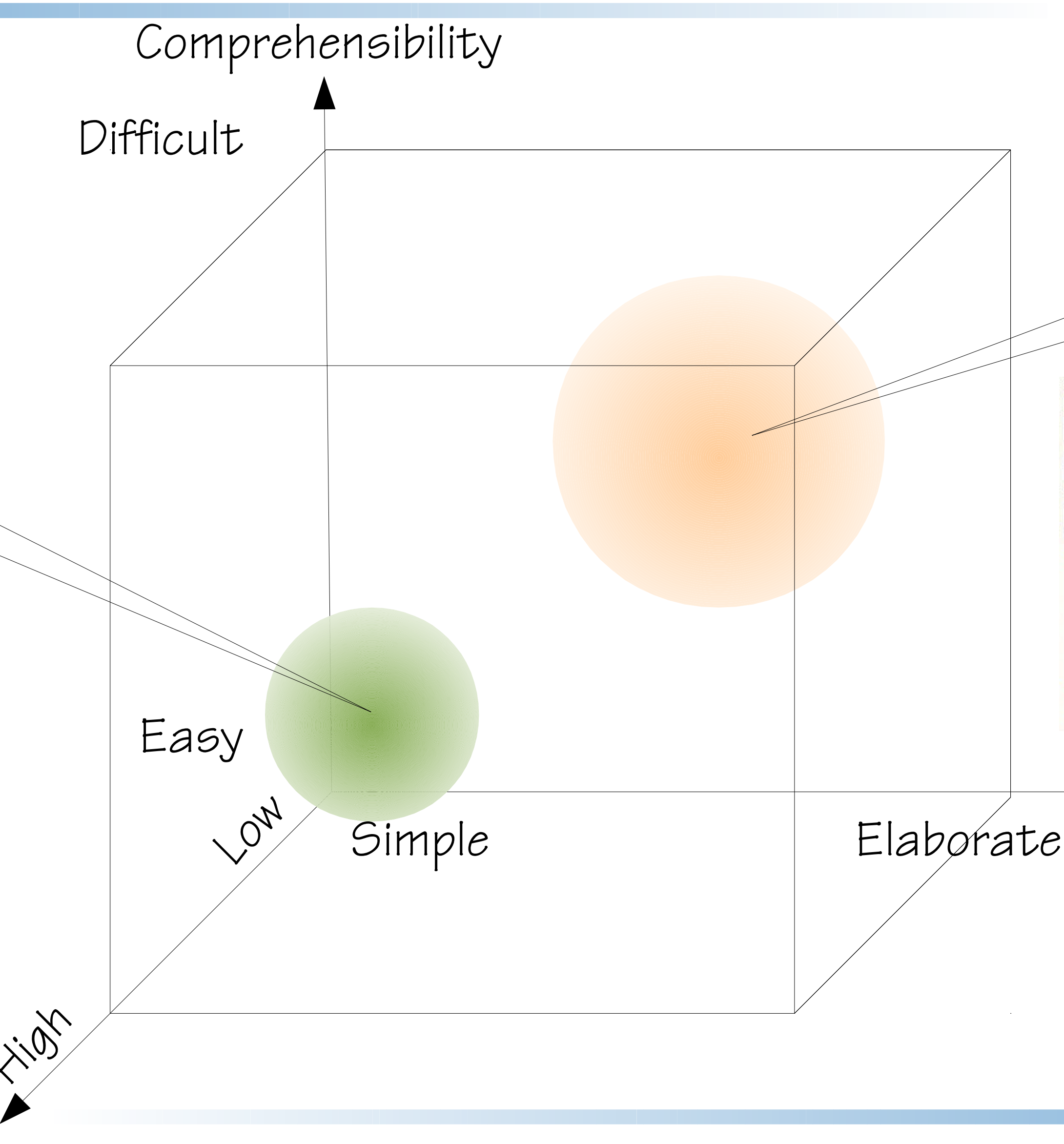
"On the whole, we have complex systems because we don't know how to produce the output through linear systems."

© Erik Hollnagel, 2011

# Tractable and intractable systems

TRACTABLE

HOMOGENEOUS PROCESSES



INTRACTABLE

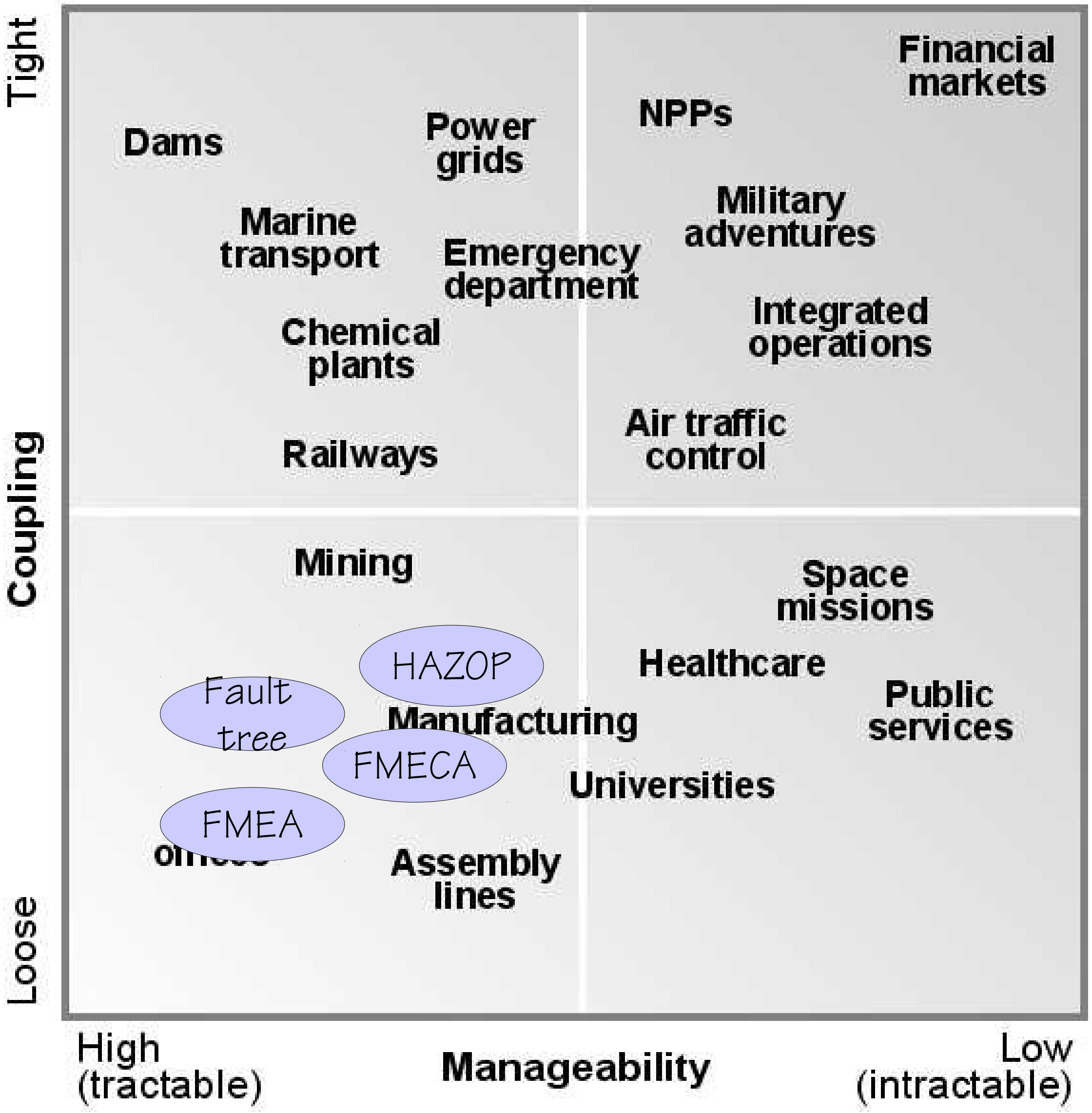
HETEROGENEOUS PROCESSES

© Erik Hollnagel, 2011

# Fit between methods and reality

Technical

Military / space



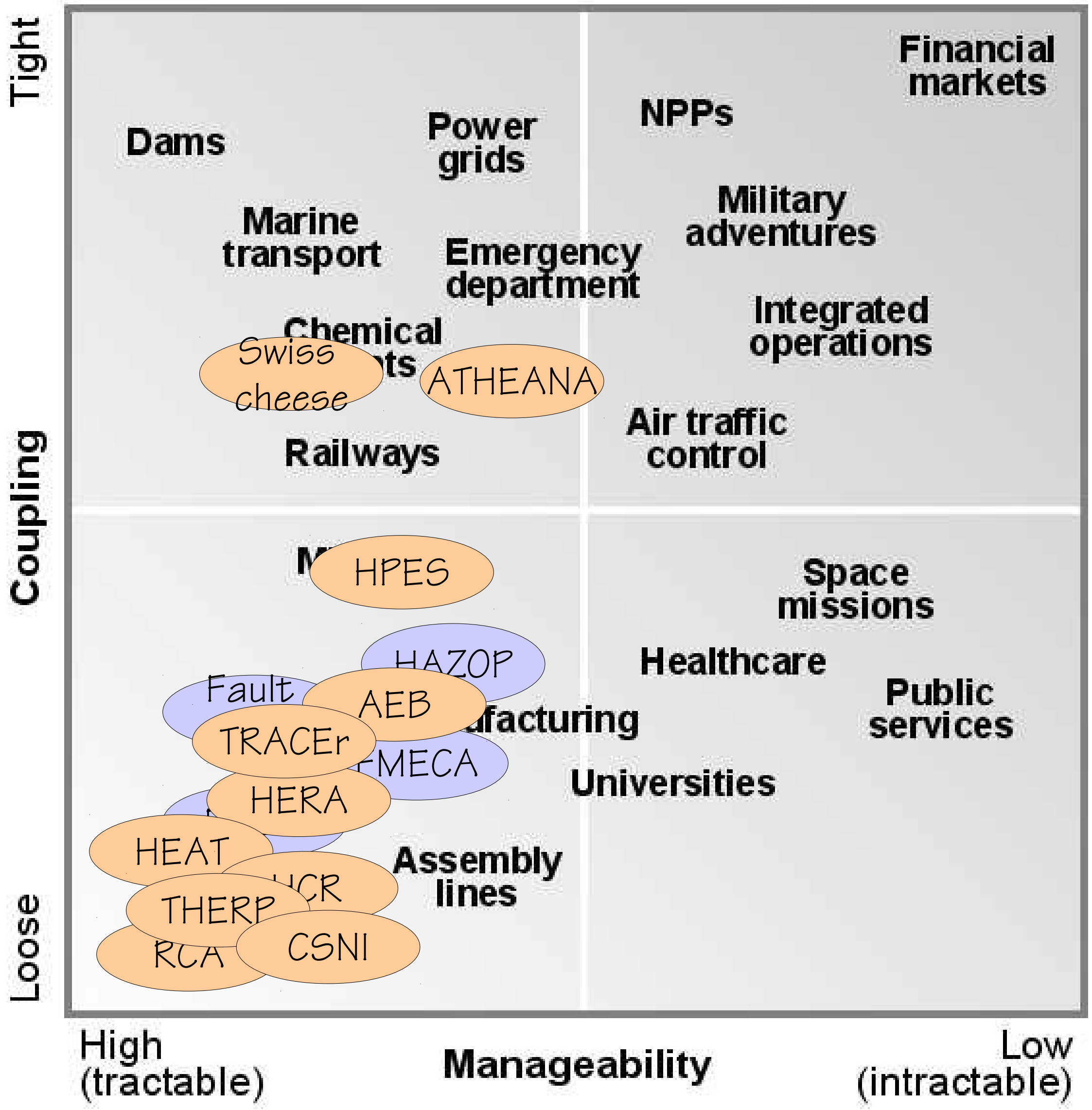
# Fit between methods and reality

Technical

Military / space

Human Factors
HRA

TMI
2G HRA



Tight

Coupling

Loose

High
(tractable)

Manageability

Low
(intractable)

Dams

Power grids

NPPs

Financial markets

Marine transport

Emergency department

Military adventures

Chemical ts

Swiss cheese

ATHEANA

Integrated operations

Air traffic control

Railways

M

HPES

Space missions

HAZOP

Healthcare

Fault

AEB

facturing

Public services

TRACEr

FMECA

Universities

HERA

HEAT

Assembly lines

HCR

THERP

RCA

CSNI

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# Fit between methods and reality

Technical

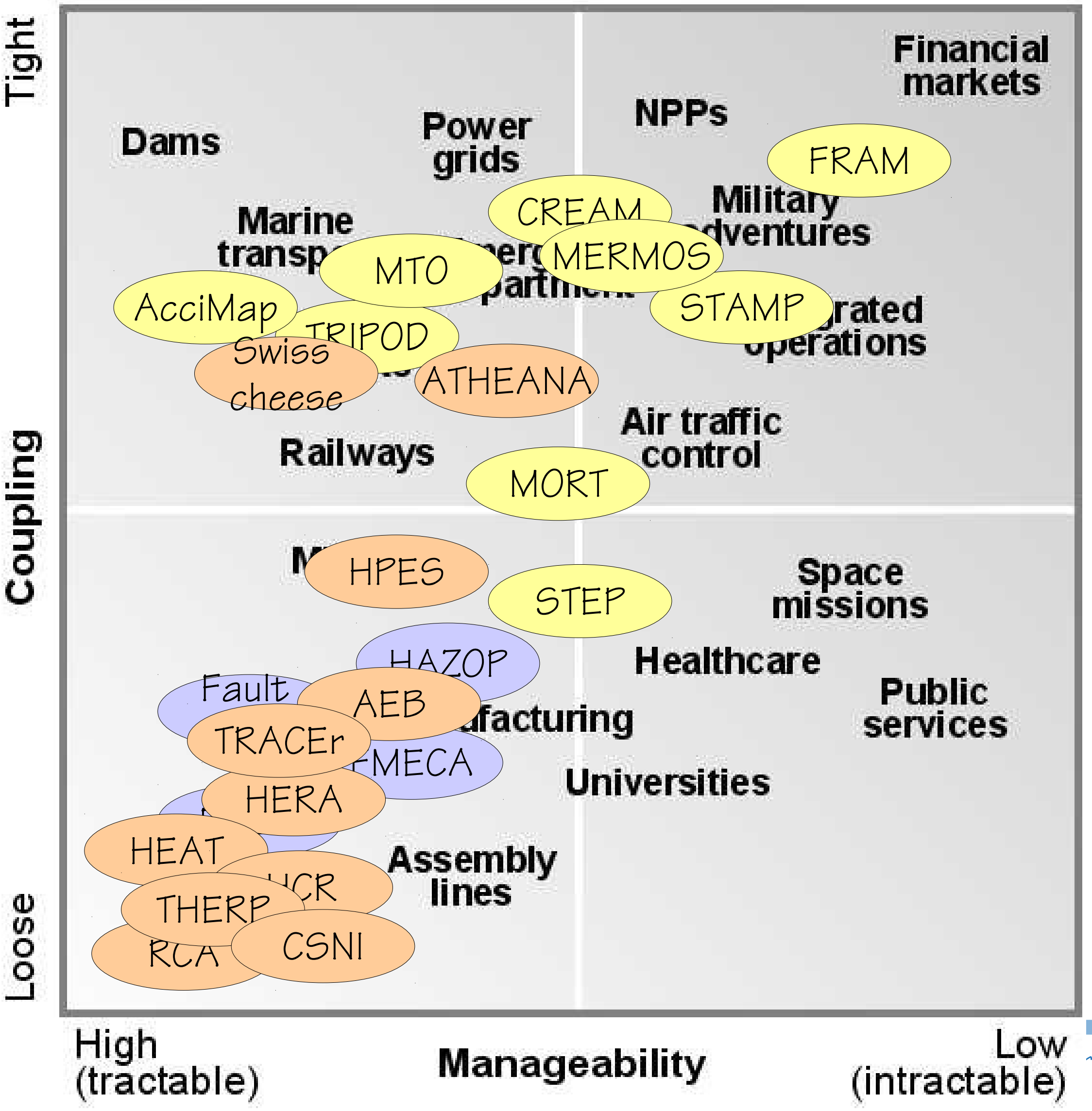
Military / space

Human Factors
HRA

TMI
2G HRA

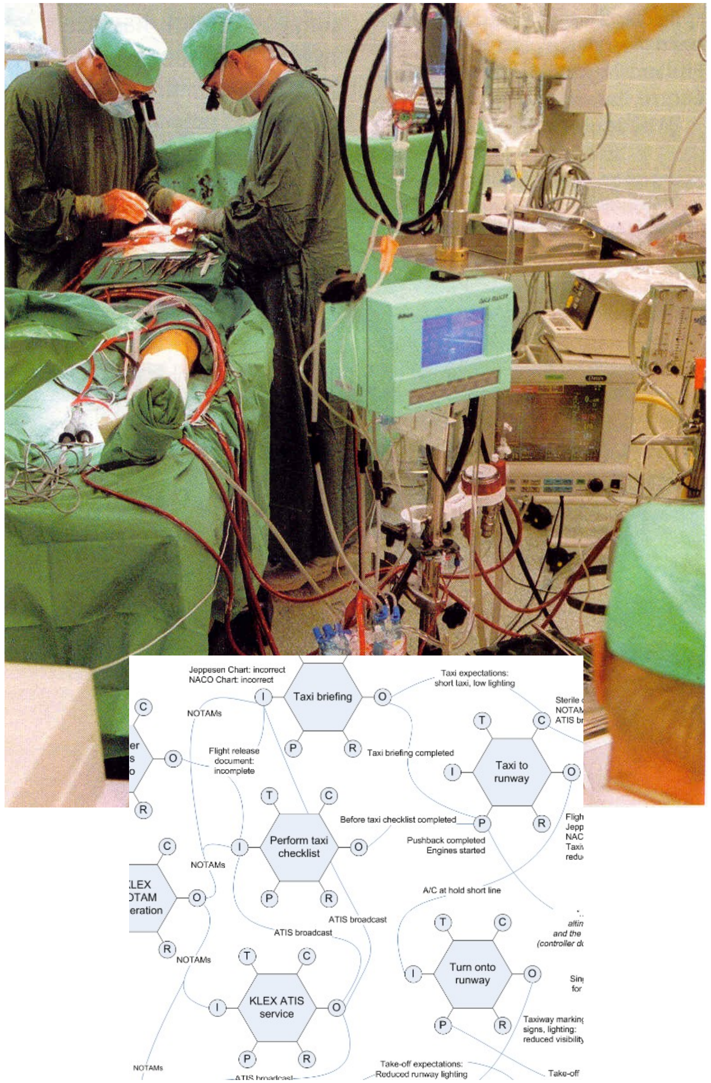
Organisational / systemic

NAT
Resilience Eng.



Syddansk Universitet
University of Southern Denmark

# Revised assumptions - 2011



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

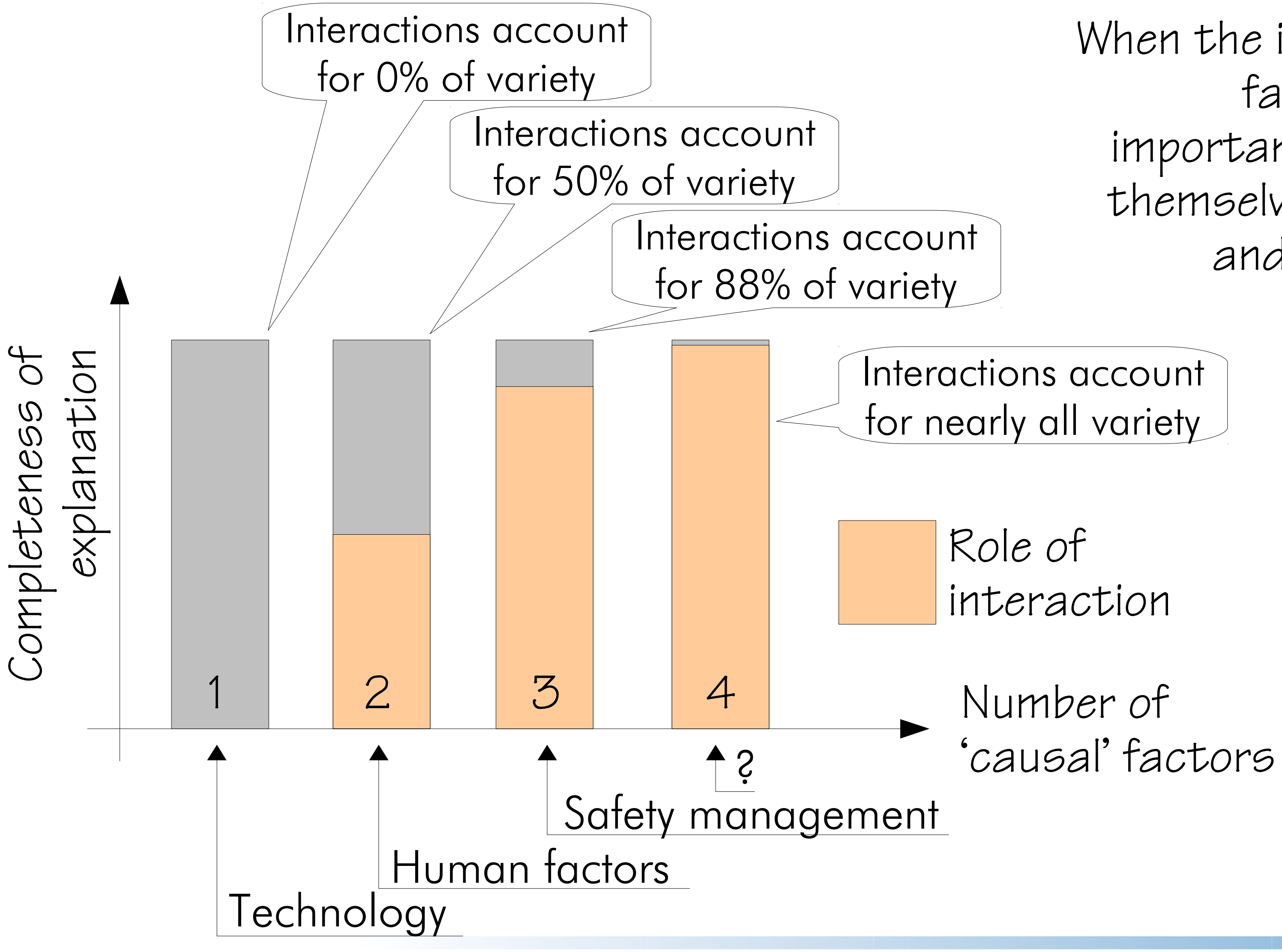
System functions are not bimodal, but everyday performance is – and must be – variable.

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 outcomes can be attributed to failures and malfunctions, others are best understood as the result of coupled performance variability.

Risk and safety analyses should try to  understand the nature of everyday performance variability and how this lead to both positive and adverse outcomes.

# Incremental development is not enough



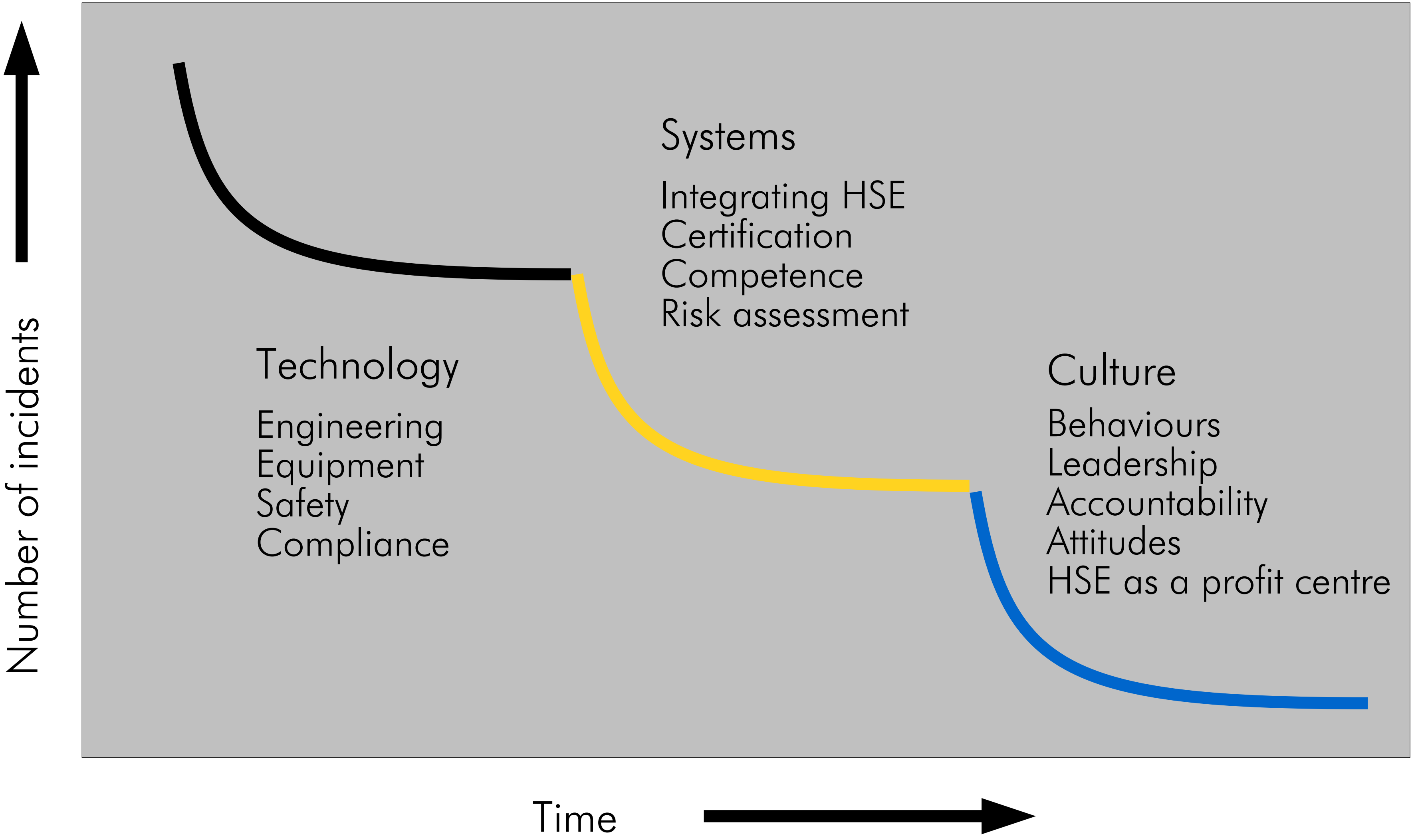
When the interactions among factors become more important than the factors themselves, we need models and methods that can account for that.

The requisite variety depends on the complexity of the interactions, rather than on the number of factors.

© Erik Hollnagel, 2011

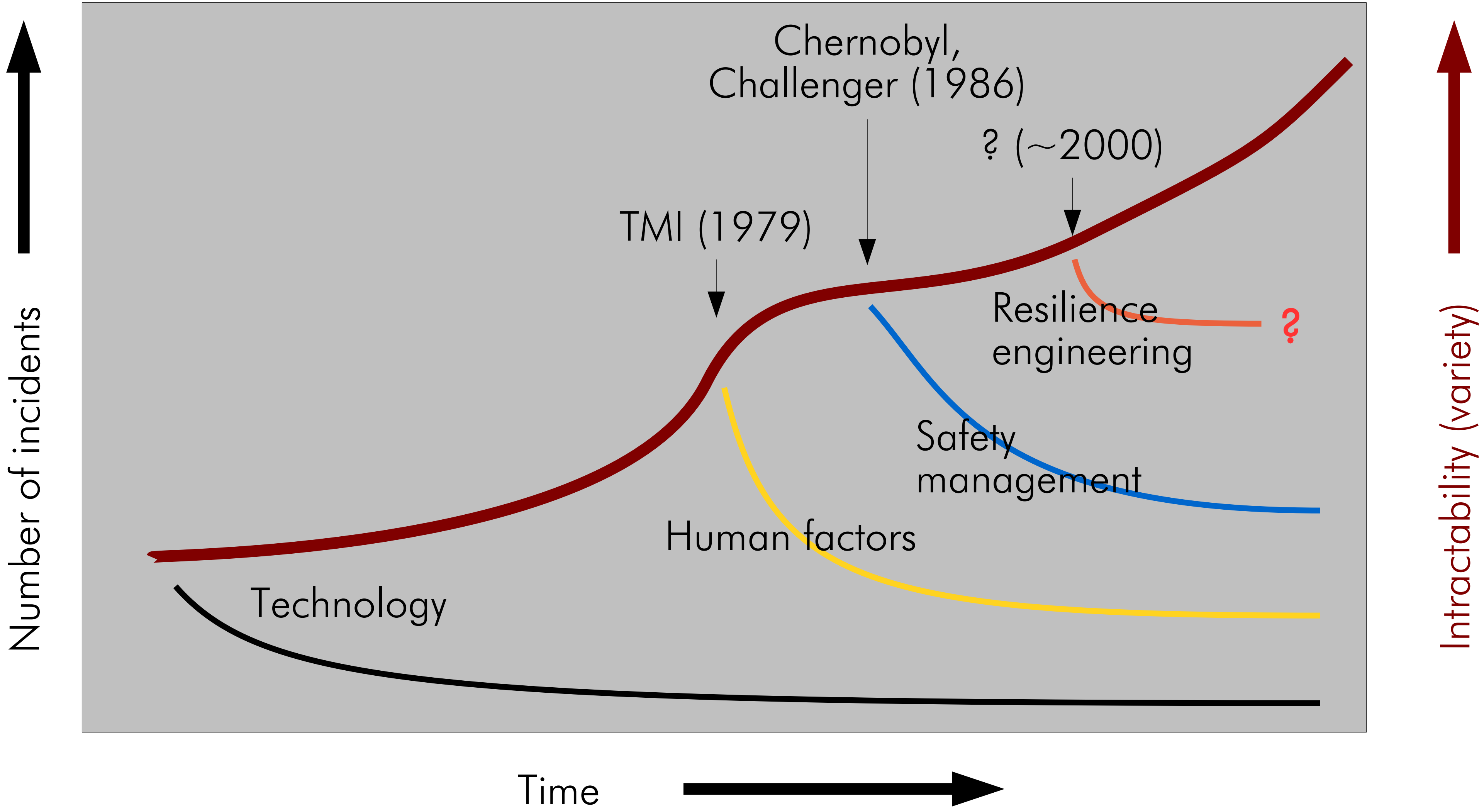
SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

# Development of SMS (Hudson, 2007)



© Erik Hollnagel, 2011

# Growing demands to requisite variety



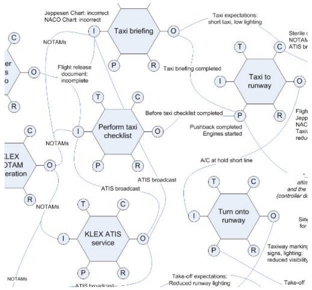
© Erik Hollnagel, 2011

# Risks as non-linear couplings

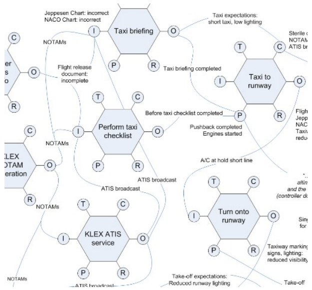
Non-decomposable, non-linear models

Functional resonance analysis model

If accidents happen like this ...


Jeppesen Chart: incorrect
NACO Chart: incorrect
Taxi briefing
Taxi expectations: short taxi, low lighting
NOTAMs
Flight release document: incomplete
Taxi briefing completed
Taxi to runway
Perform taxi checklist
Before taxi checklist completed
Pushback completed
Engines started
A/C at hold short line
ATIS broadcast
KLEX ATIS service
Turn onto runway
Taxiway marking signs, lighting: reduced visibility
Take-off expectations: Reduced runway lighting
Take-off

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


Jeppesen Chart: incorrect
NACO Chart: incorrect
Taxi briefing
Taxi expectations: short taxi, low lighting
NOTAMs
Flight release document: incomplete
Taxi briefing completed
Taxi to runway
Perform taxi checklist
Before taxi checklist completed
Pushback completed
Engines started
A/C at hold short line
ATIS broadcast
KLEX ATIS service
Turn onto runway
Taxiway marking signs, lighting: reduced visibility
Take-off expectations: Reduced runway lighting
Take-off

Unexpected combinations (resonance) of variability of normal performance.

Unexpected combinations (resonance) of variability of normal performance.

Systems at risk are intractable rather than tractable.

The established assumptions therefore have to be revised

Today outcomes can be emergent as well as resultant: models and methods must be developed to account for that.

# Conclusions

If the variety of the concepts, models, and methods used in risk assessment is less than the requisite variety, we will lose control of the socio-technical systems on which we depend.

It is the dilemma of Safety Management and Risk Assessment that we inadvertently create the Problems of the Future by trying to solve the Challenges of the Present with the Mindset (models, theories & methods) of the Past.

Tempora mutantur, et nos in illis