SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

HOW TO BE SAFE BY LOOKING AT WHAT GOES RIGHT INSTEAD OF WHAT GOES WRONG

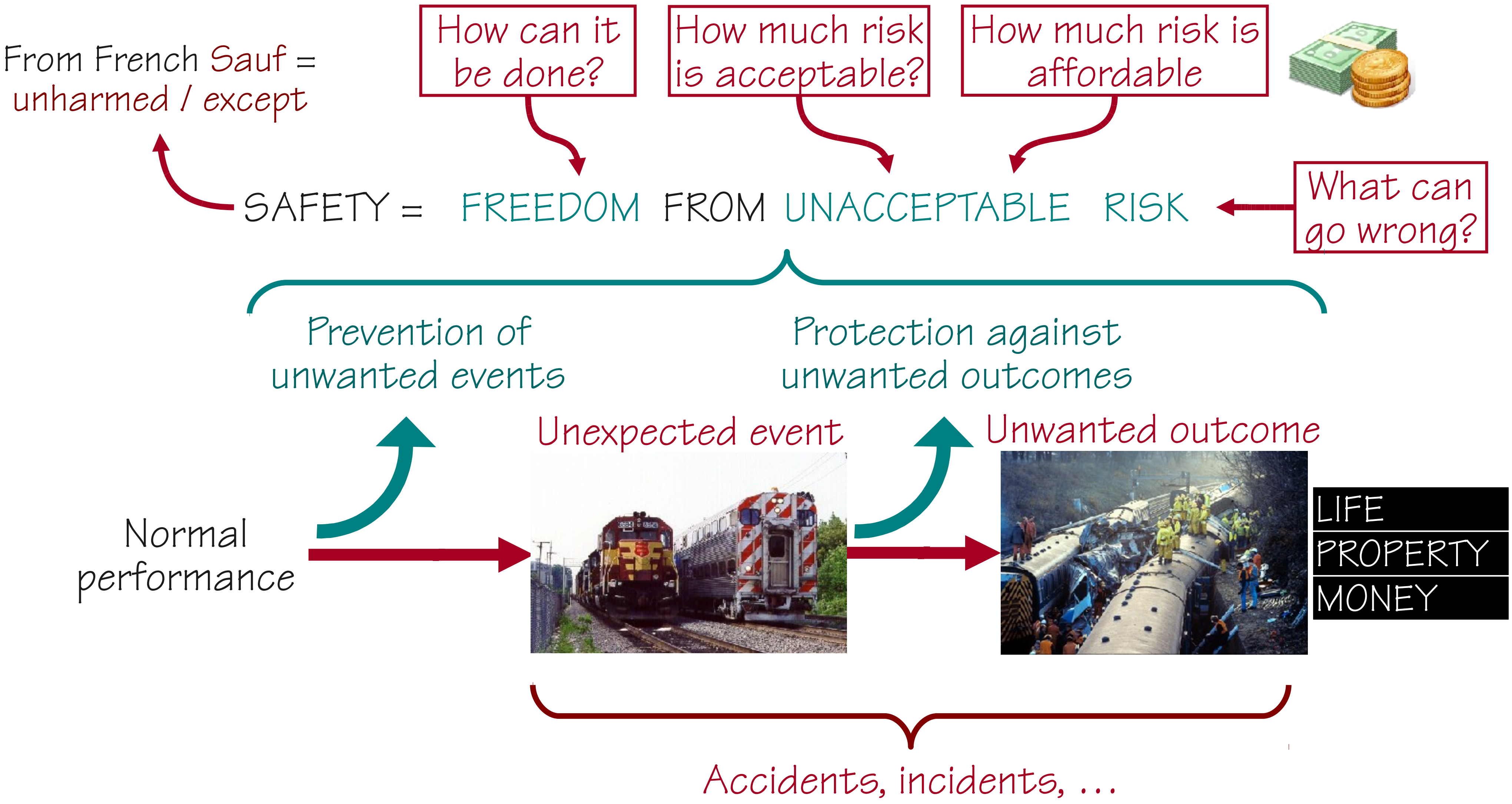
Erik Hollnagel

Professor
Institute of Public Health
University of Southern Denmark

Professor & Industrial Safety Chair
MINES ParisTech
Sophia Antipolis, France

erik.hollnagel@gmail.com

The meaning of safety



From French Sauf = unharmed / except

How can it be done?

How much risk is acceptable?

How much risk is affordable

SAFETY = FREEDOM FROM UNACCEPTABLE RISK

What can go wrong?

Prevention of unwanted events

Protection against unwanted outcomes

Normal performance

Unexpected event

Unwanted outcome

LIFE

PROPERTY

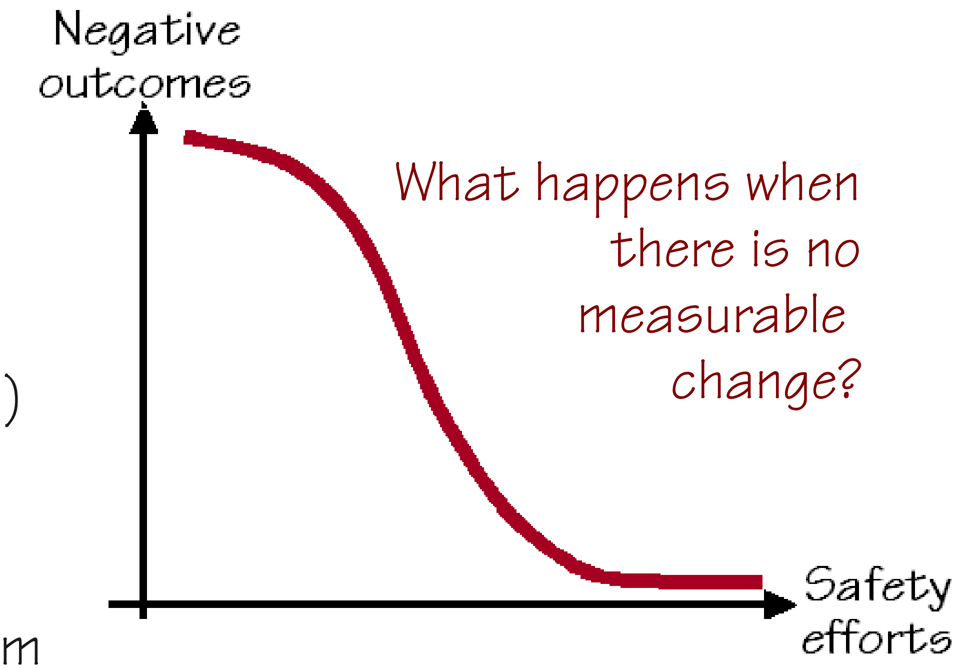
MONEY

Accidents, incidents, …

© Erik Hollnagel, 2011

Safety measured by what goes wrong

Safety is normally measured by the absence of negative outcomes.
This can be achieved in three different ways:
- eliminating hazards (design),
- preventing initiating events (constraints)
- protecting against consequences (barriers)



What happens when there is no measurable change?

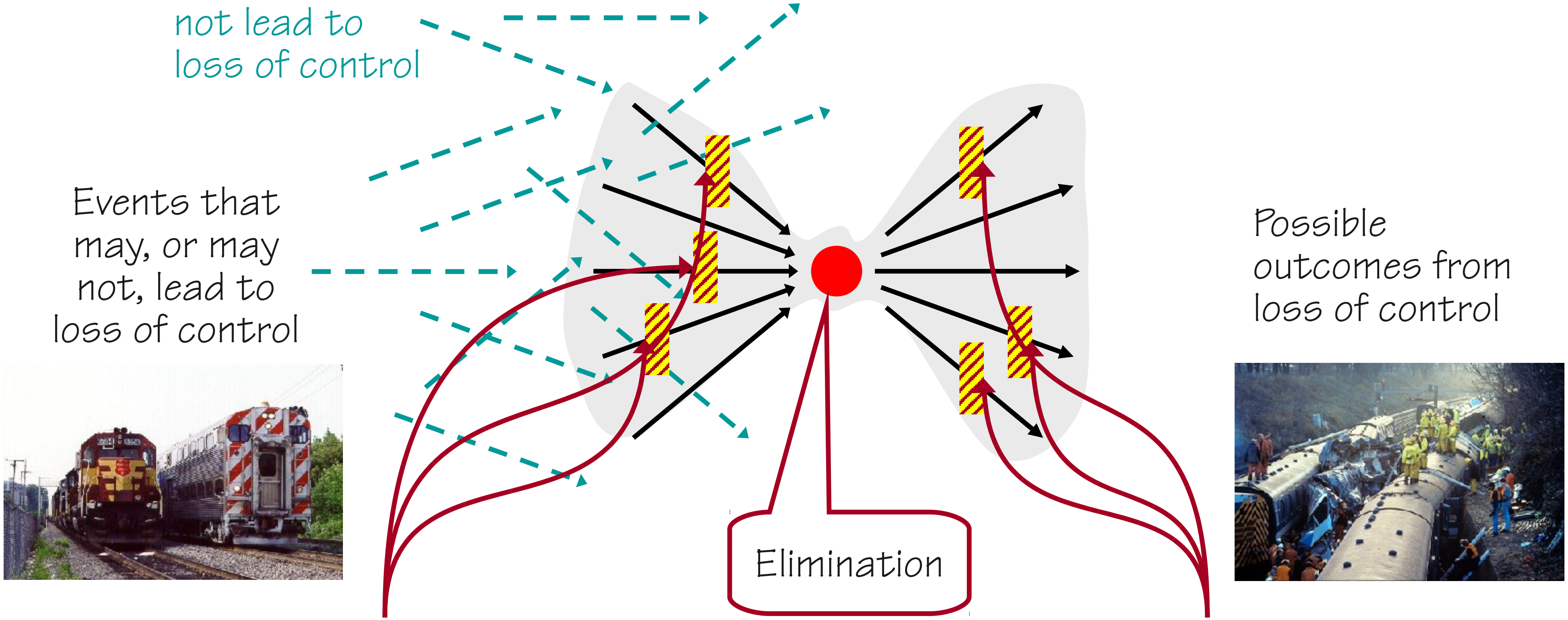
Safety, as commonly practised, implies a distinction between:

Everyday operations that ensure the system works as it should and produces the intended outcomes.

Unusual operations that disrupt or disturb everyday operations or otherwise render them ineffective.

The purpose of safety management is to maintain everyday operations by preventing disruptions or disturbances. Safety efforts are usually driven by what has happened in the past, and are therefore mainly reactive.

Industrial safety model



Events that do not lead to loss of control

Events that may, or may not, lead to loss of control

Possible outcomes from loss of control

Elimination

Preventive of initiating conditions

Protection against outcomes

Safety Performance Assessment

Transport Canada

A railway company shall maintain records of the following information for the purpose of assessing its safety performance:

Accident and incident investigation reports and a description of the corrective actions taken for accidents and incidents that meet the reporting criteria.

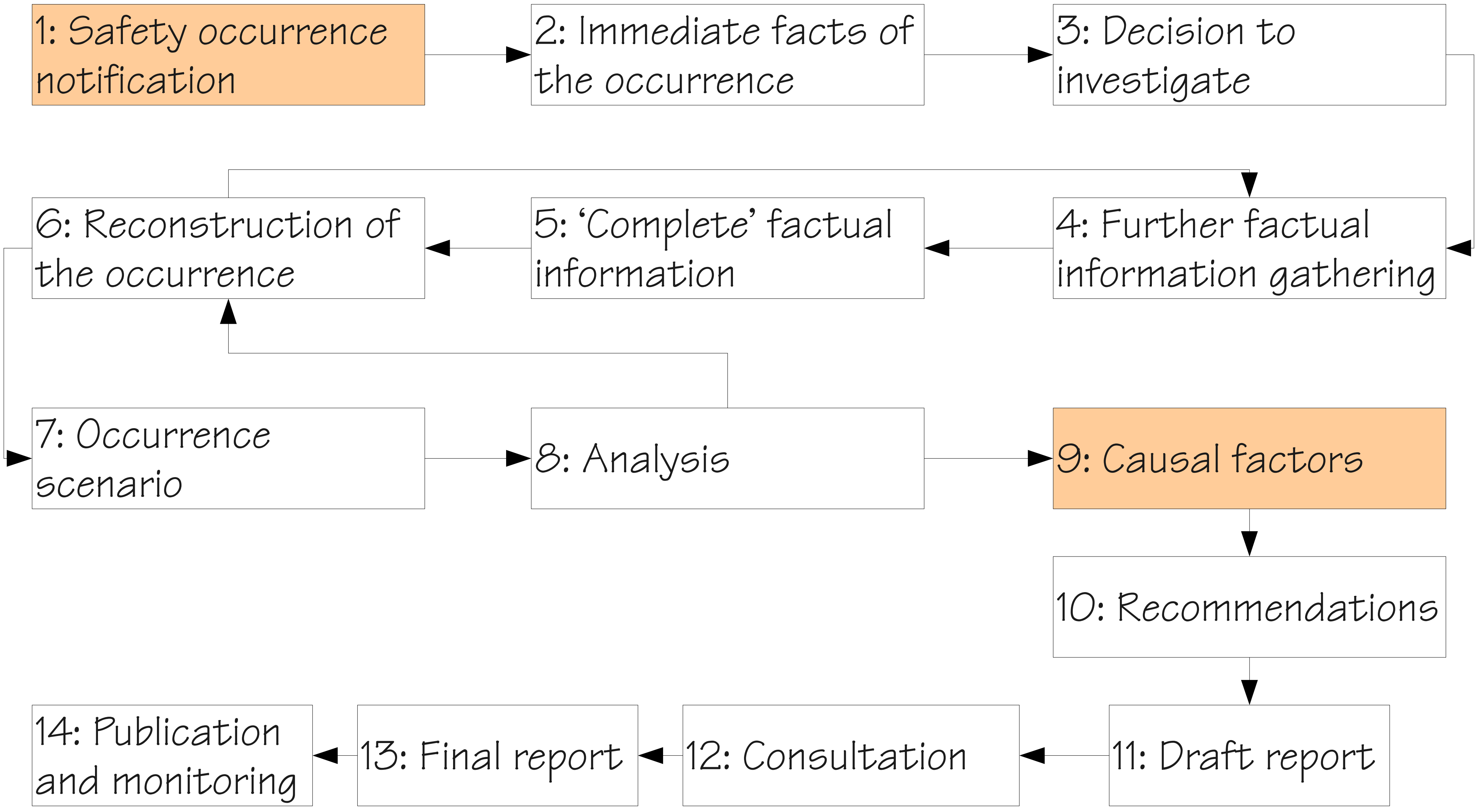
Accident rates expressed as follows:

Employee deaths, disabling injuries and minor injuries, per 200,000 hours worked by the employees of the railway company.

Train and grade crossing accidents that meet the reporting criteria, per million train miles.

At the request of the Minister, a railway company shall collect, maintain and submit to the Minister specified performance or safety data for the purpose of monitoring the effectiveness of its safety management system and its safety performance.

ERA Generic Occurrence Investigation


1: Safety occurrence notification
2: Immediate facts of the occurrence
3: Decision to investigate
4: Further factual information gathering
5: 'Complete' factual information
6: Reconstruction of the occurrence
7: Occurrence scenario
8: Analysis
9: Causal factors
10: Recommendations
11: Draft report
12: Consultation
13: Final report
14: Publication and monitoring

Syddansk Universitet
University of Southern Denmark

Looking for causes

Single causes
Simple causes
Belief in causality

If something has gone wrong (effect), we can find the cause by reasoning backwards

Technical failure

Human failure

Organisational failure

"Act of god"

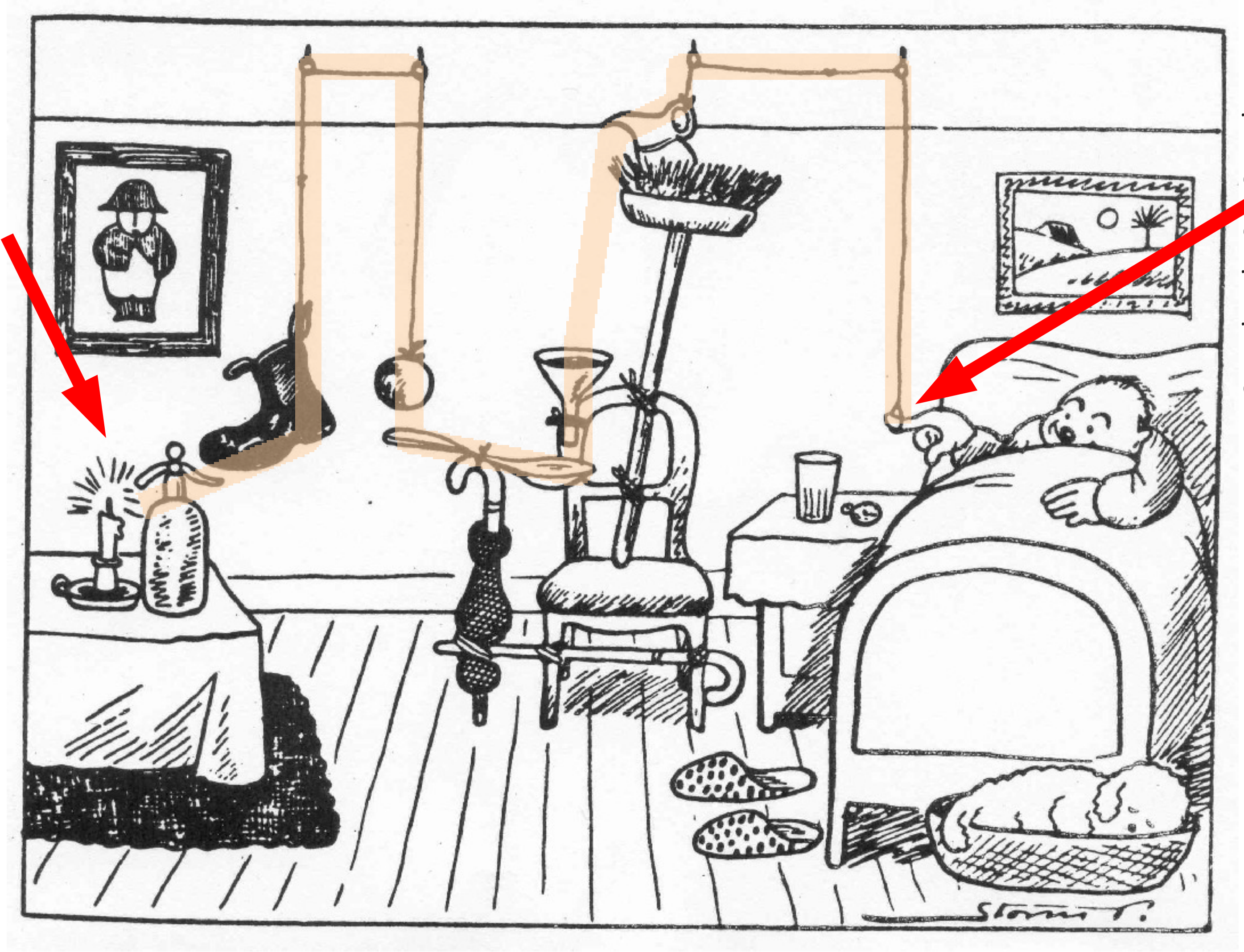
But which assumptions do we make about how things work?

And what is our model of how accidents happen?

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

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

SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

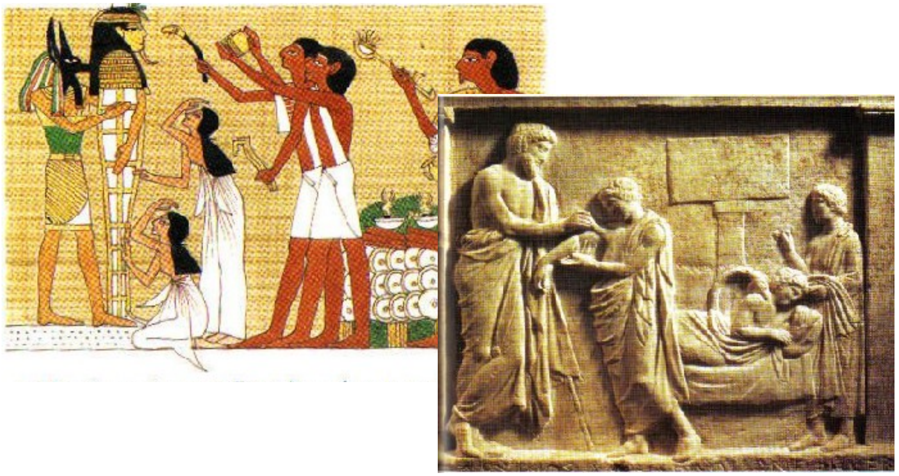
Causality in simple systems

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.

Causality in complex systems



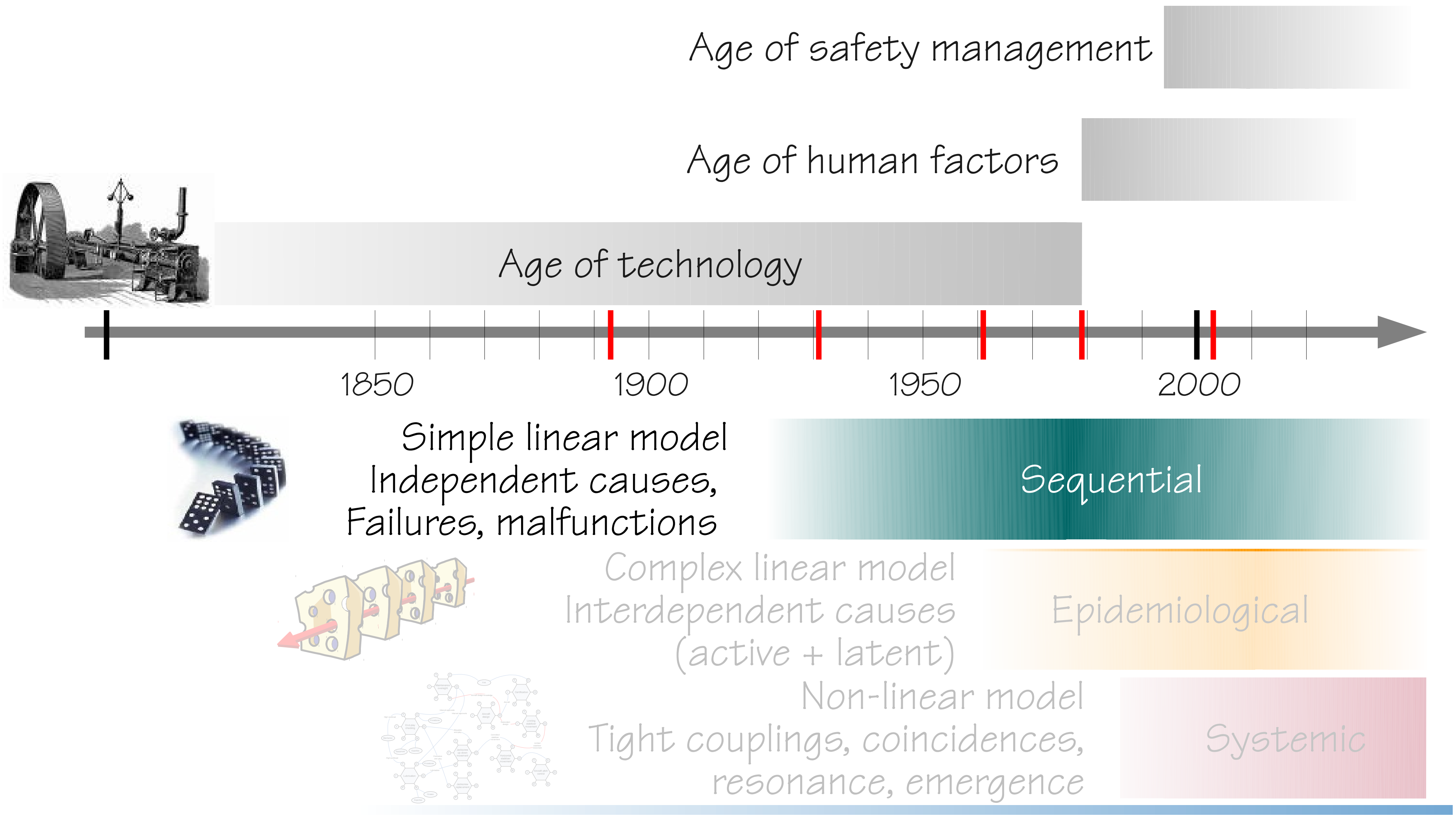
Historically, the physician-patient relation was one-to-one. The first modern hospital (The Charité, Berlin) is from 1710.

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?

Three types of accident models



Age of safety management

Age of human factors

Age of technology

Simple linear model
Independent causes,
Failures, malfunctions

Sequential

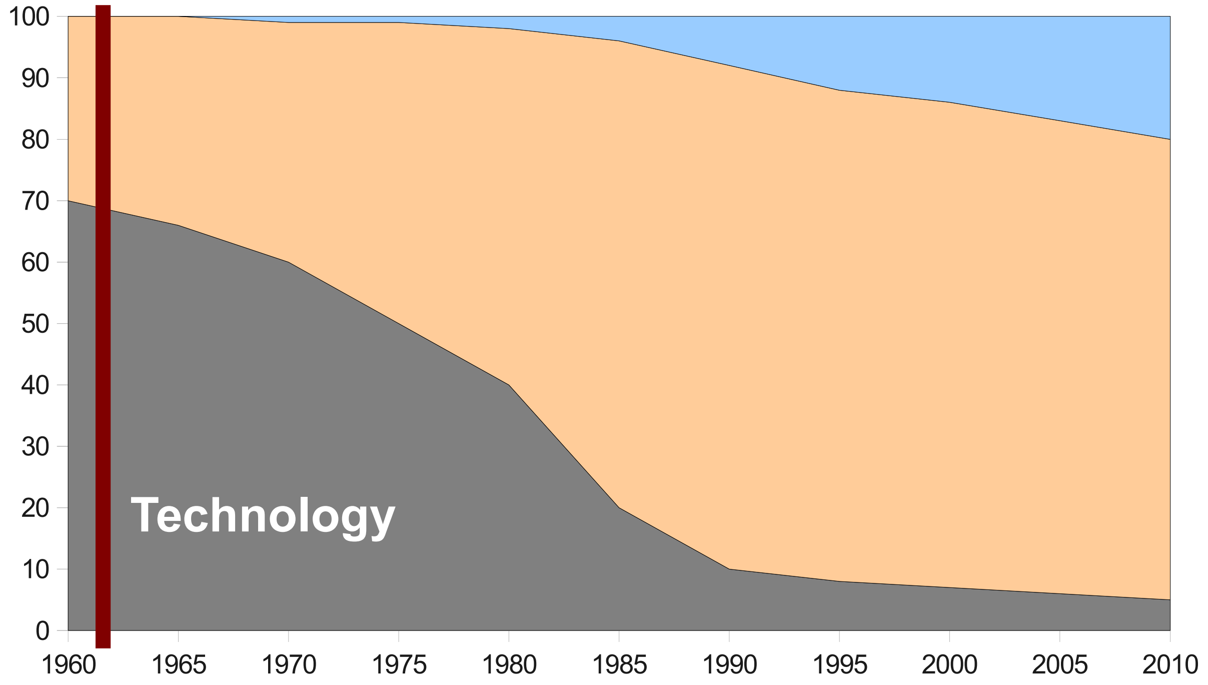
Complex linear model
Interdependent causes
(active + latent)

Epidemiological

Non-linear model
Tight couplings, coincidences,
resonance, emergence

Systemic

Looking for technical failures

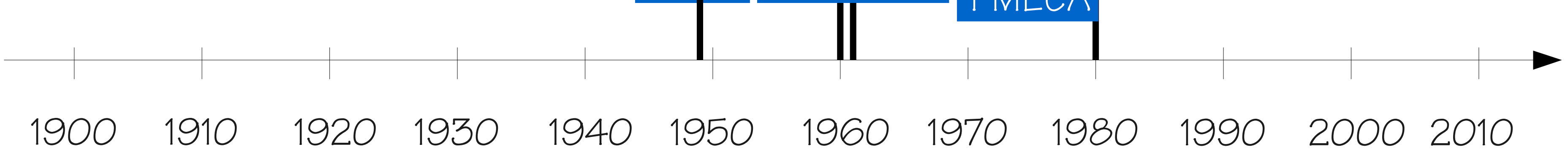


HAZOP

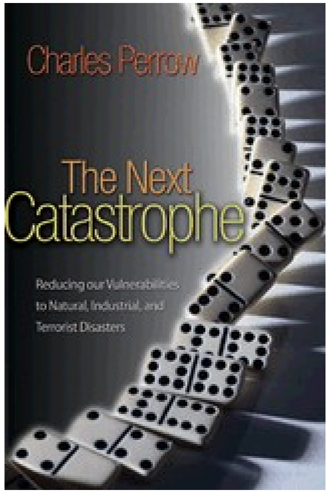
FMEA

Fault tree

FMECA



Domino thinking everywhere



Charles Perrow

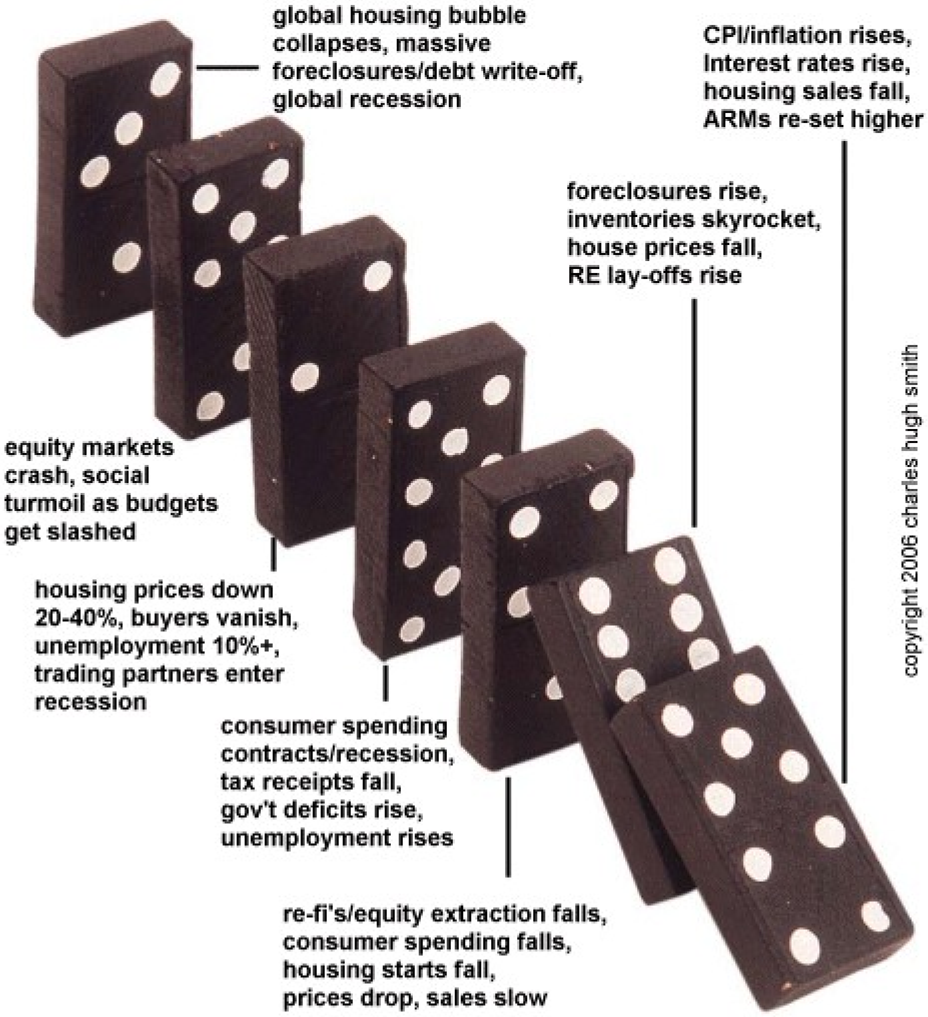
The Next Catastrophe

Reducing our Vulnerabilities to Natural, Industrial, and Terrorist Disasters

Welke bank gaat nu voor de bijl?

De kredietcrisis maakt overal in de geldwereld slachtoffers. Centrale banken strooien met honderden miljarden, maar is het genoeg? 8

LEHMAN BROTHERS
LEHMAN BROTHERS
AIG
FORTIS BANK
BANK OF SCOTLAND
Washington Mutual



global housing bubble collapses, massive foreclosures/debt write-off, global recession

CPI/inflation rises, Interest rates rise, housing sales fall, ARMs re-set higher

foreclosures rise, inventories skyrocket, house prices fall, RE lay-offs rise

equity markets crash, social turmoil as budgets get slashed

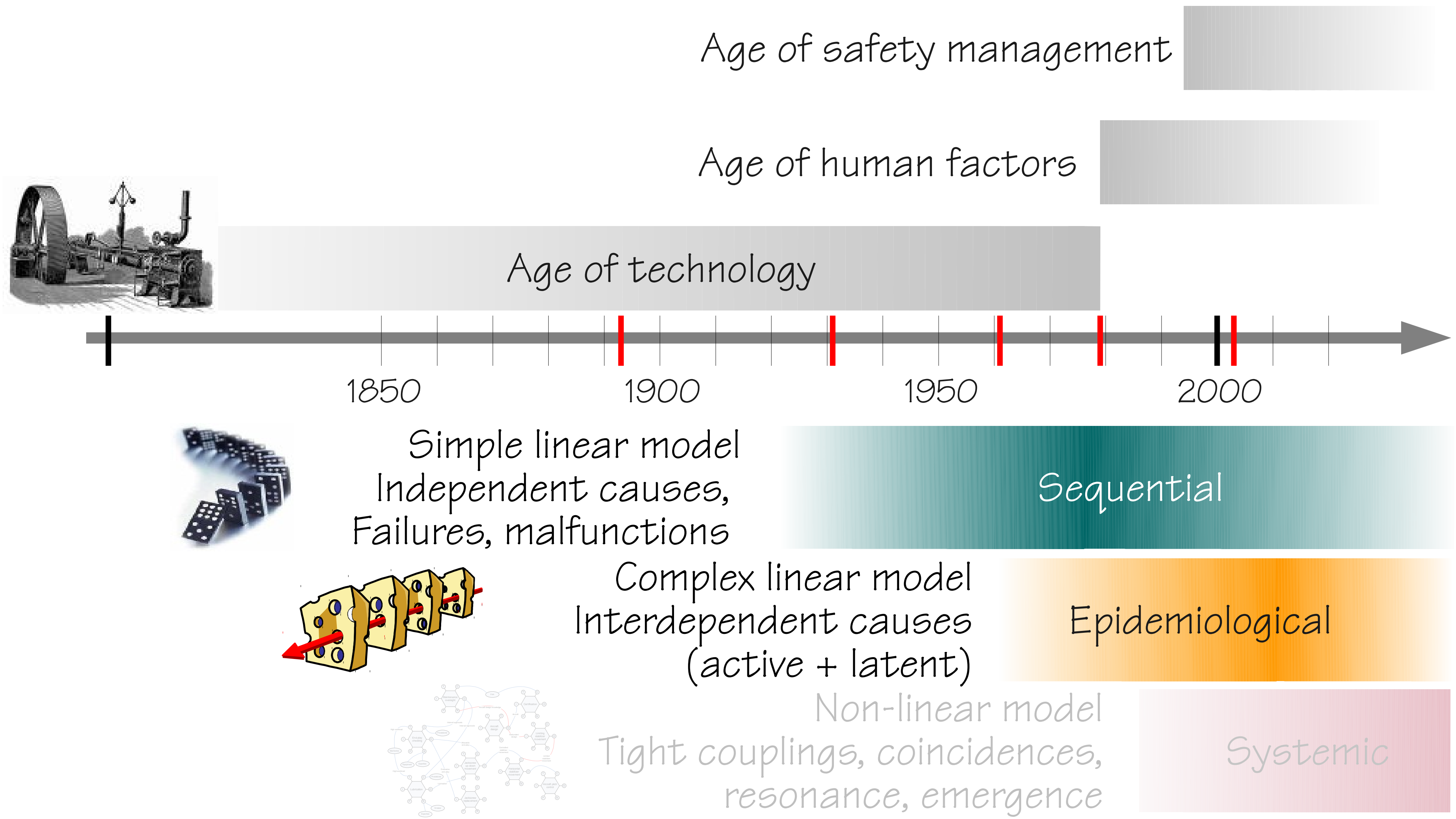
housing prices down 20-40%, buyers vanish, unemployment 10%+, trading partners enter recession

consumer spending contracts/recession, tax receipts fall, gov't deficits rise, unemployment rises

re-fi's/equity extraction falls, consumer spending falls, housing starts fall, prices drop, sales slow

copyright 2006 charles hugh smith

Three types of accident models



Age of safety management

Age of human factors

Age of technology

Simple linear model
Independent causes,
Failures, malfunctions

Sequential

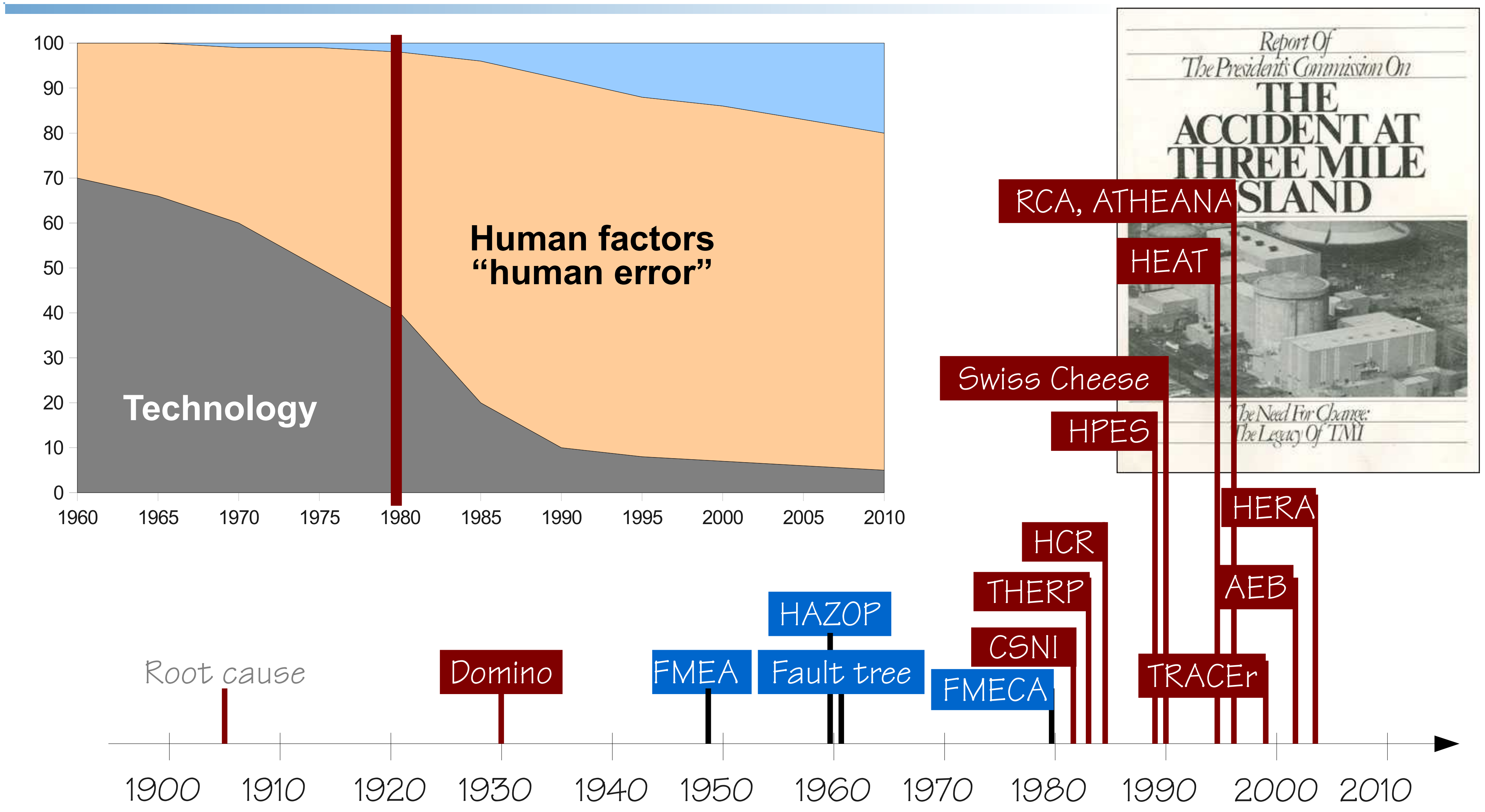
Complex linear model
Interdependent causes
(active + latent)

Epidemiological

Non-linear model
Tight couplings, coincidences,
resonance, emergence

Systemic

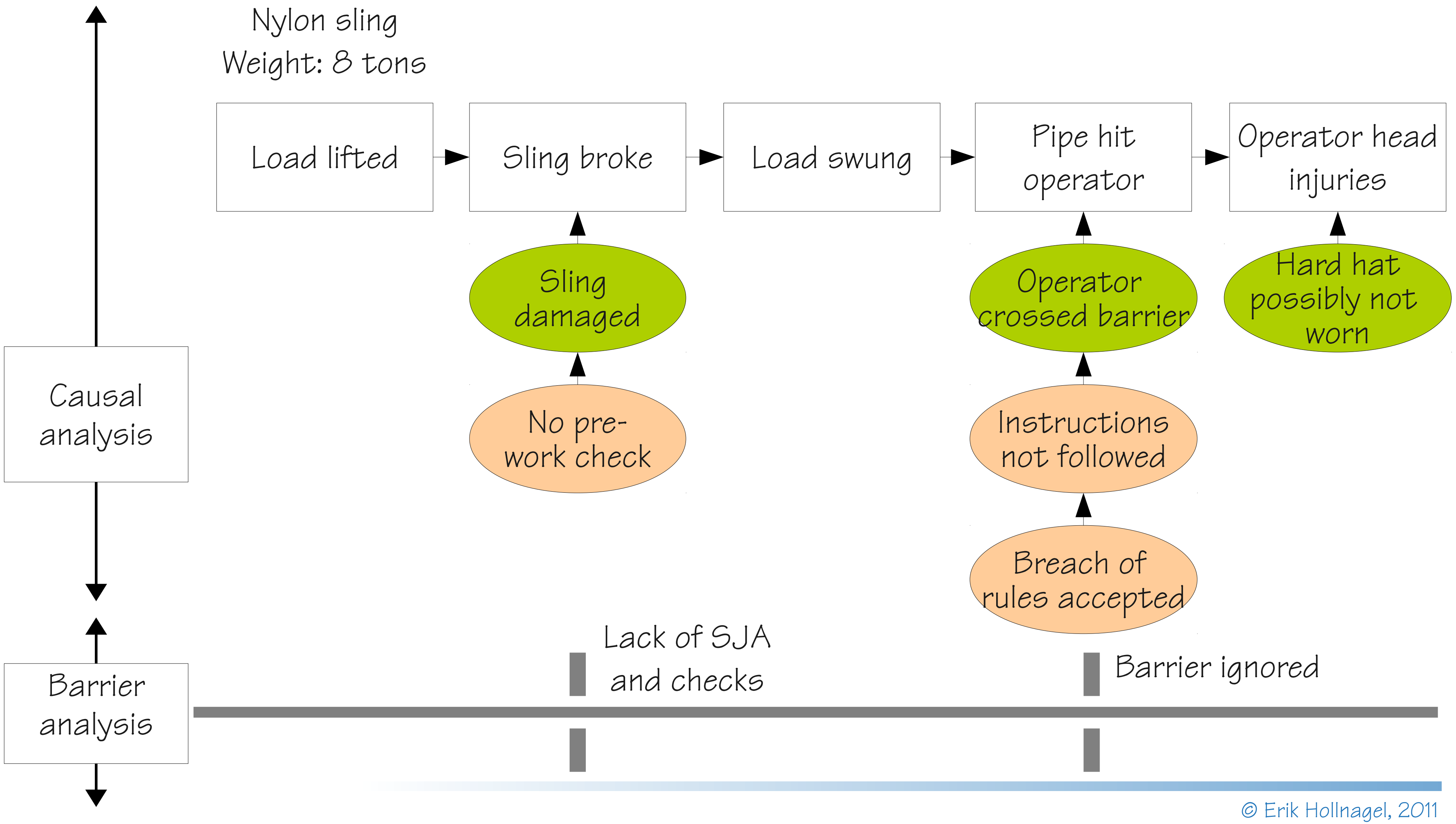
Looking for human failures ("errors")



Report Of
The President's Commission On
THE ACCIDENT AT THREE MILE ISLAND

The Need For Change:
The Legacy Of TMI

MTO digram

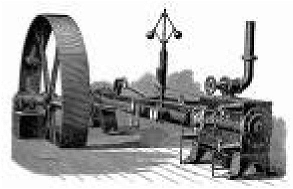


© Erik Hollnagel, 2011

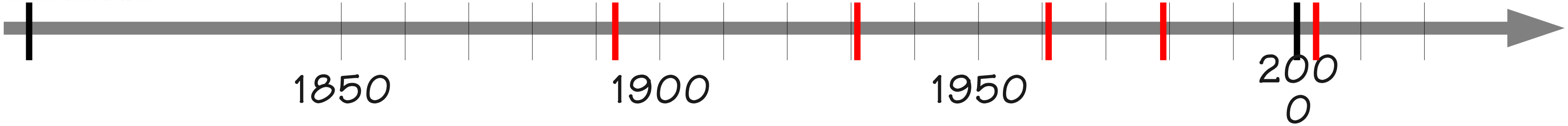
Three types of accident models

Age of safety management

Age of human factors

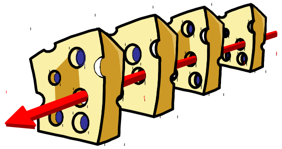


Age of technology



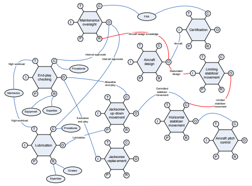
Simple linear model
Independent causes,
Failures, malfunctions

Sequential



Complex linear model
Interdependent causes
(active + latent)

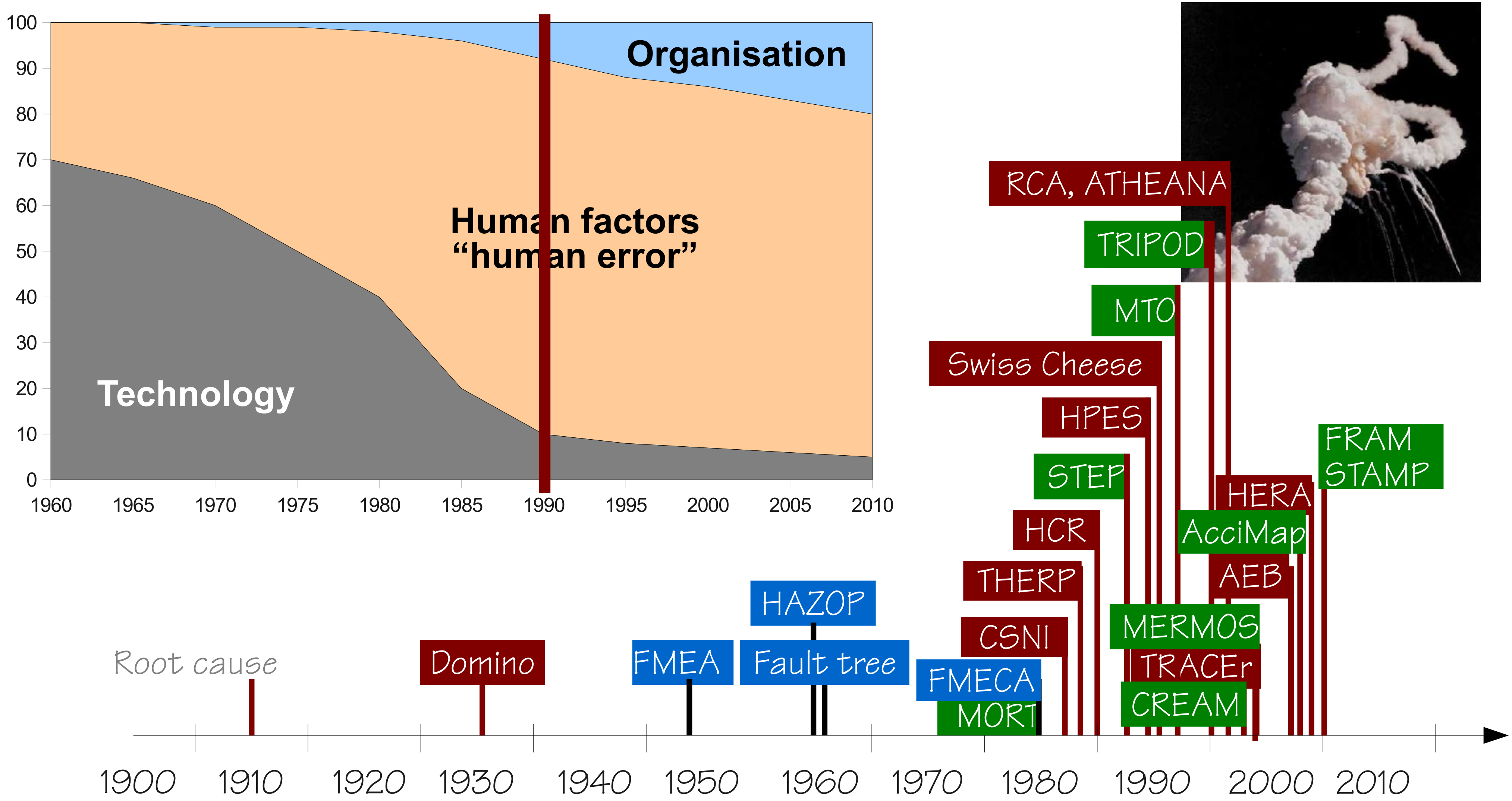
Epidemiological



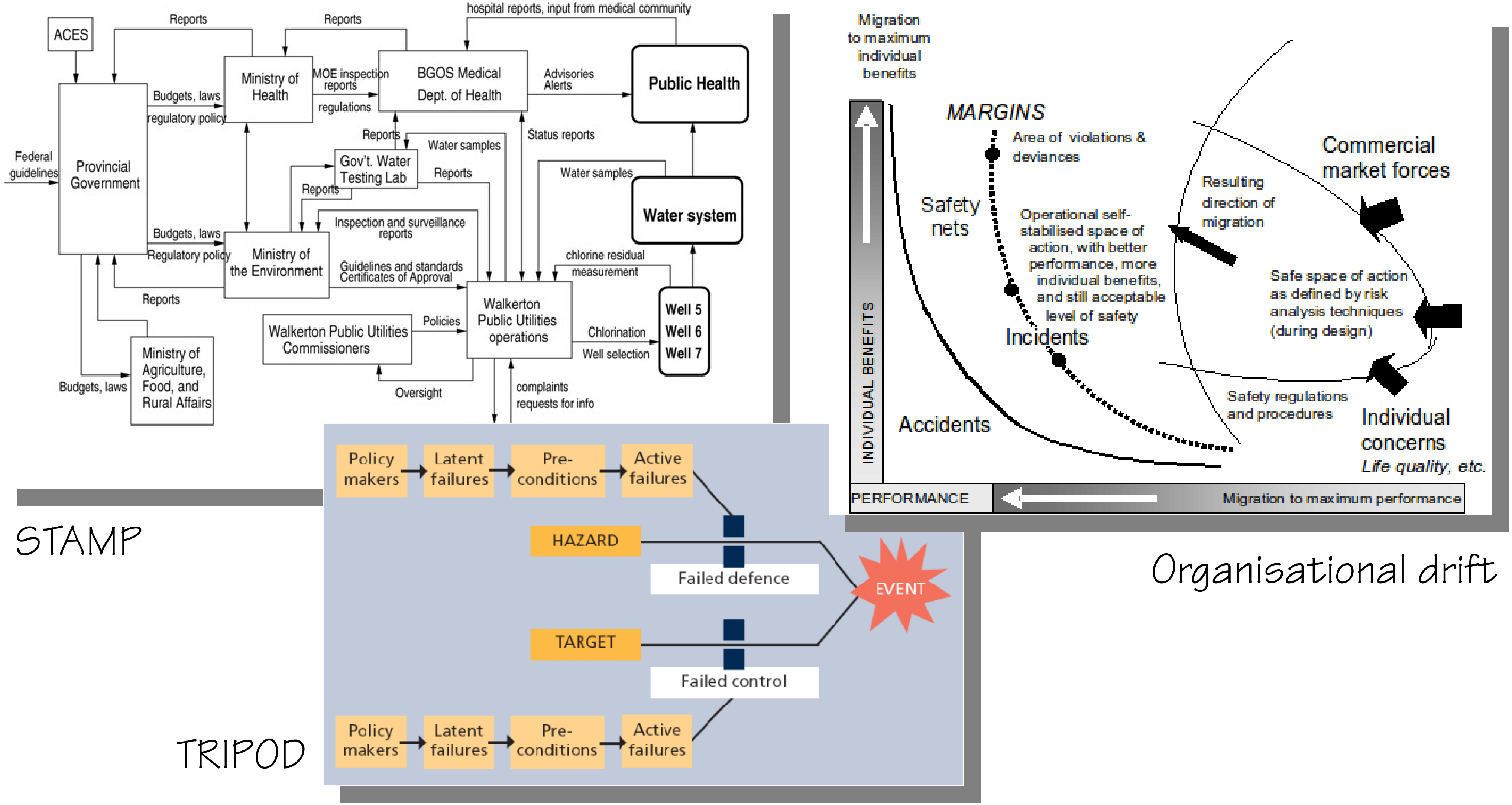
Non-linear model
Tight couplings, coincidences,
resonance, emergence

Systemic

Looking for organisational failures



Models of organisational "failures"


ACES
Reports
Reports
hospital reports, input from medical community
Ministry of Health
MOE inspection reports
regulations
BGOS Medical Dept. of Health
Advisories Alerts
Public Health
Budgets, laws
regulatory policy
Reports
Water samples
Status reports
Federal guidelines
Provincial Government
Gov't. Water Testing Lab
Reports
Reports
Water samples
Water system
Budgets, laws
Regulatory policy
Ministry of the Environment
Inspection and surveillance reports
Guidelines and standards Certificates of Approval
chlorine residual measurement
Reports
Walkerton Public Utilities operations
Walkerton Public Utilities Commissioners
Policies
Chlorination
Well selection
Well 5
Well 6
Well 7
Budgets, laws
Ministry of Agriculture, Food, and Rural Affairs
Oversight
complaints requests for info
Policy makers
Latent failures
Pre-conditions
Active failures
HAZARD
Failed defence
EVENT
TARGET
Failed control
Policy makers
Latent failures
Pre-conditions
Active failures
Migration to maximum individual benefits
MARGINS
Area of violations & deviances
Safety nets
Operational self-stabilised space of action, with better performance, more individual benefits, and still acceptable level of safety
Incidents
Accidents
INDIVIDUAL BENEFITS
Resulting direction of migration
Commercial market forces
Safe space of action as defined by risk analysis techniques (during design)
Safety regulations and procedures
Individual concerns
Life quality, etc.
PERFORMANCE
Migration to maximum performance

STAMP

TRIPOD

Organisational drift

© Erik Hollnagel, 2011

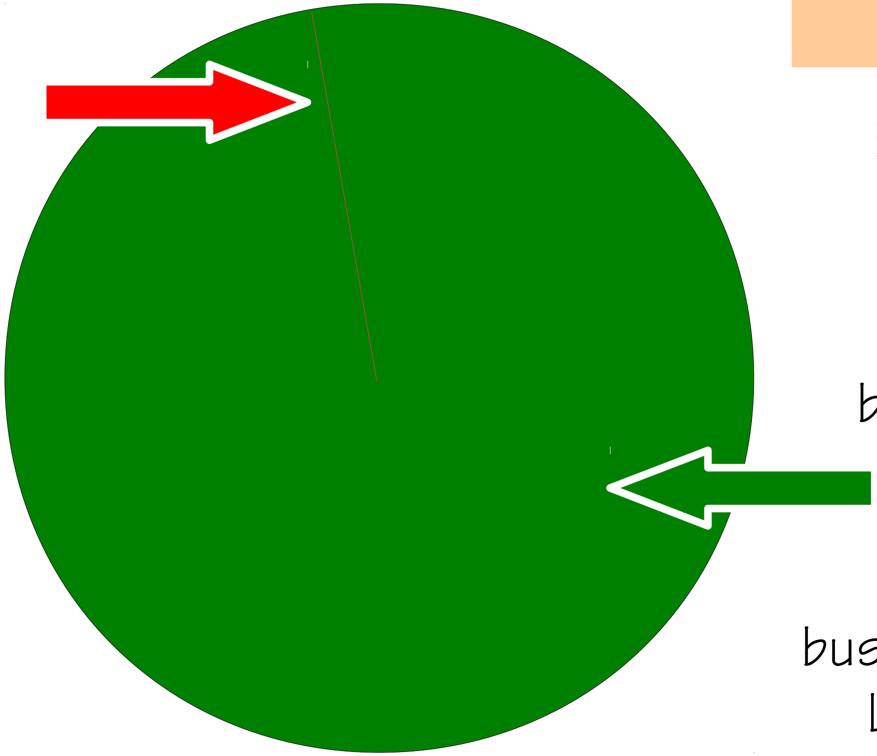
Why only look at what goes wrong?

Safety = Reduced number of adverse events.

Focus is on what goes wrong. Look for failures and malfunctions. Try to eliminate causes and improve barriers.

Safety and core business compete for resources. Learning only uses a fraction of the data available

10^{-4} := 1 failure in 10.000 events



$1 - 10^{-4}$:= 9.999 non-failures in 10.000 events

Safety = Ability to succeed under varying conditions.

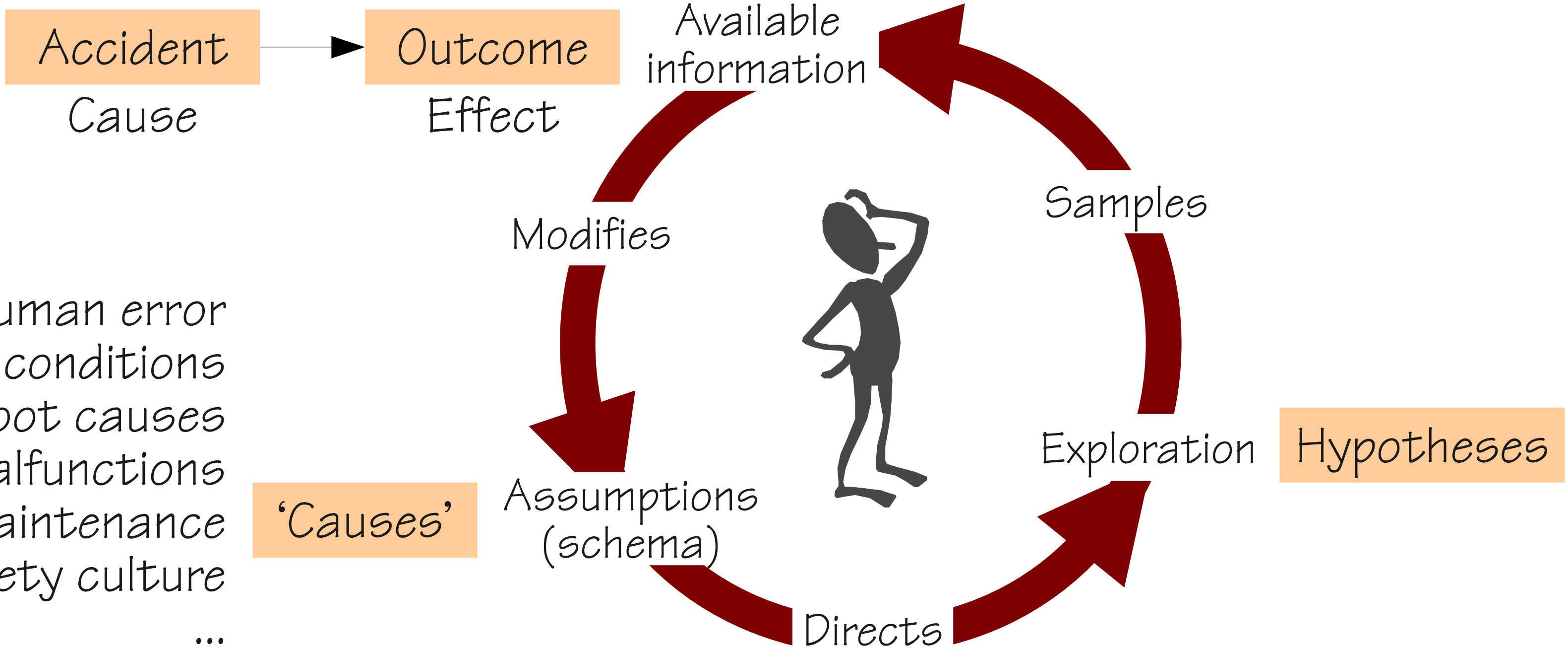
Focus is on what goes right. Use that to understand normal performance, to do better and to be safer.

Safety and core business help each other. Learning uses most of the data available

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.

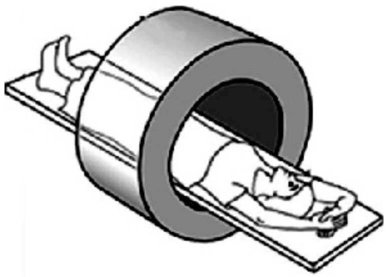


Human error
Latent conditions
Root causes
Technical malfunctions
Maintenance
Safety culture
...

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

From words to deeds

Regulations:
Where the employer knows or has reason to believe that an incident has or may have occurred in which a person, while undergoing a medical exposure was, otherwise than as a result of a malfunction or defect in equipment, exposed to ionising radiation to an extent much greater than intended, he shall make an immediate preliminary investigation of the incident and, unless that investigation shows beyond a reasonable doubt that no such overexposure has occurred, he shall forthwith notify the appropriate authority and make or arrange for a detailed investigation of the circumstances of the exposure and an assessment of the dose received.



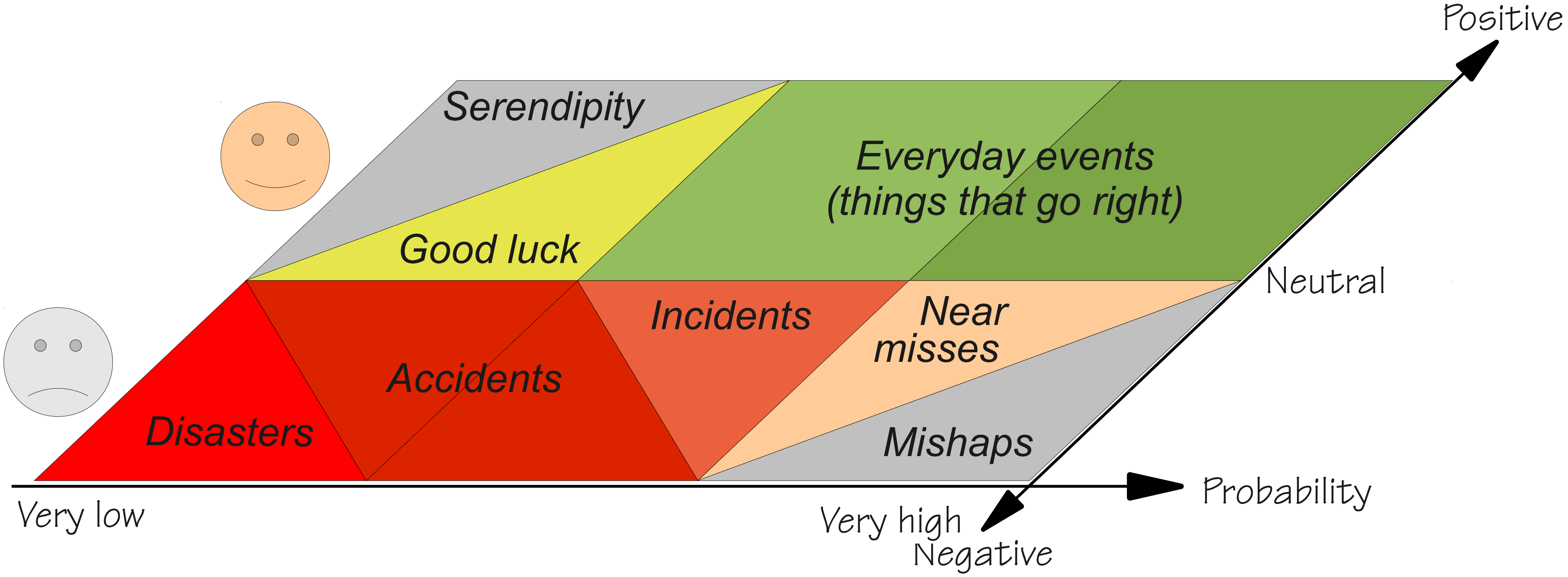
Which means that

If an incident has occurred (or may have occurred),
if it was not due to a malfunction of equipment, and
if as a result a patient has received too great a dose of ionising radiation,
then the incident shall be investigated.

Or

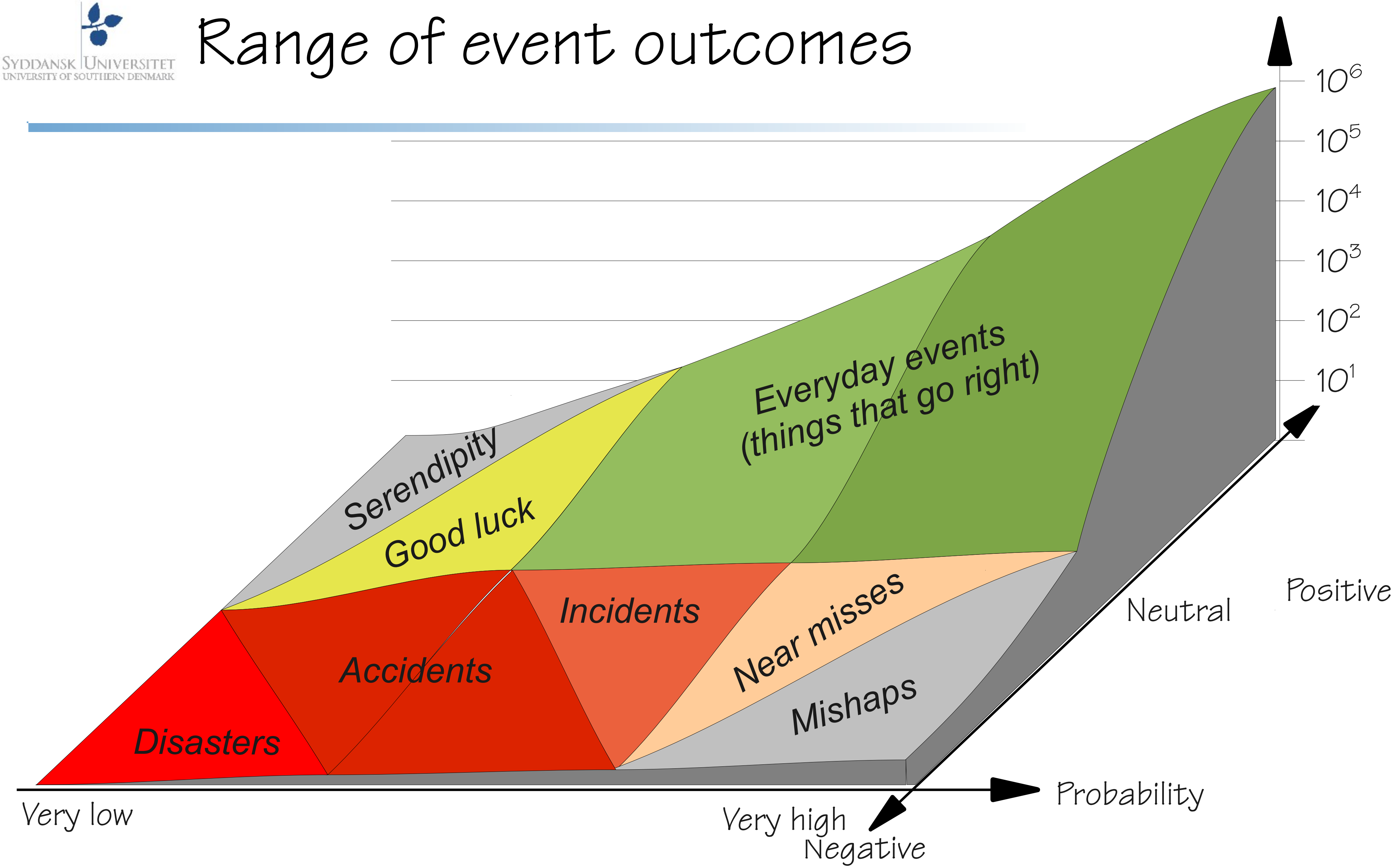
If an incident happens where a human error is the cause,
then it shall be investigated. Otherwise it shall not.

Range of event outcomes



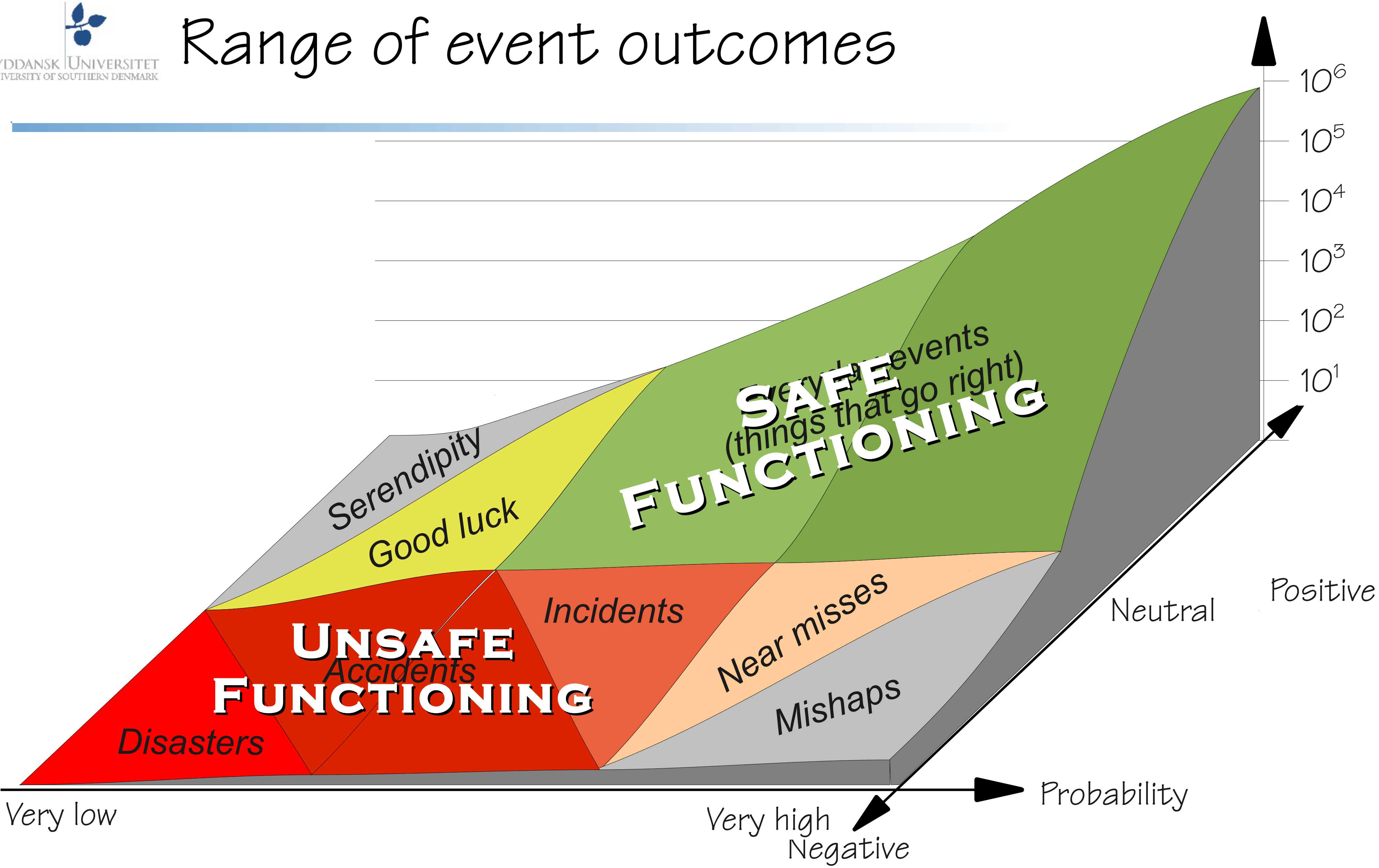
SYDDANSK UNIVERSITET
UNIVERSITY OF SOUTHERN DENMARK

Range of event outcomes



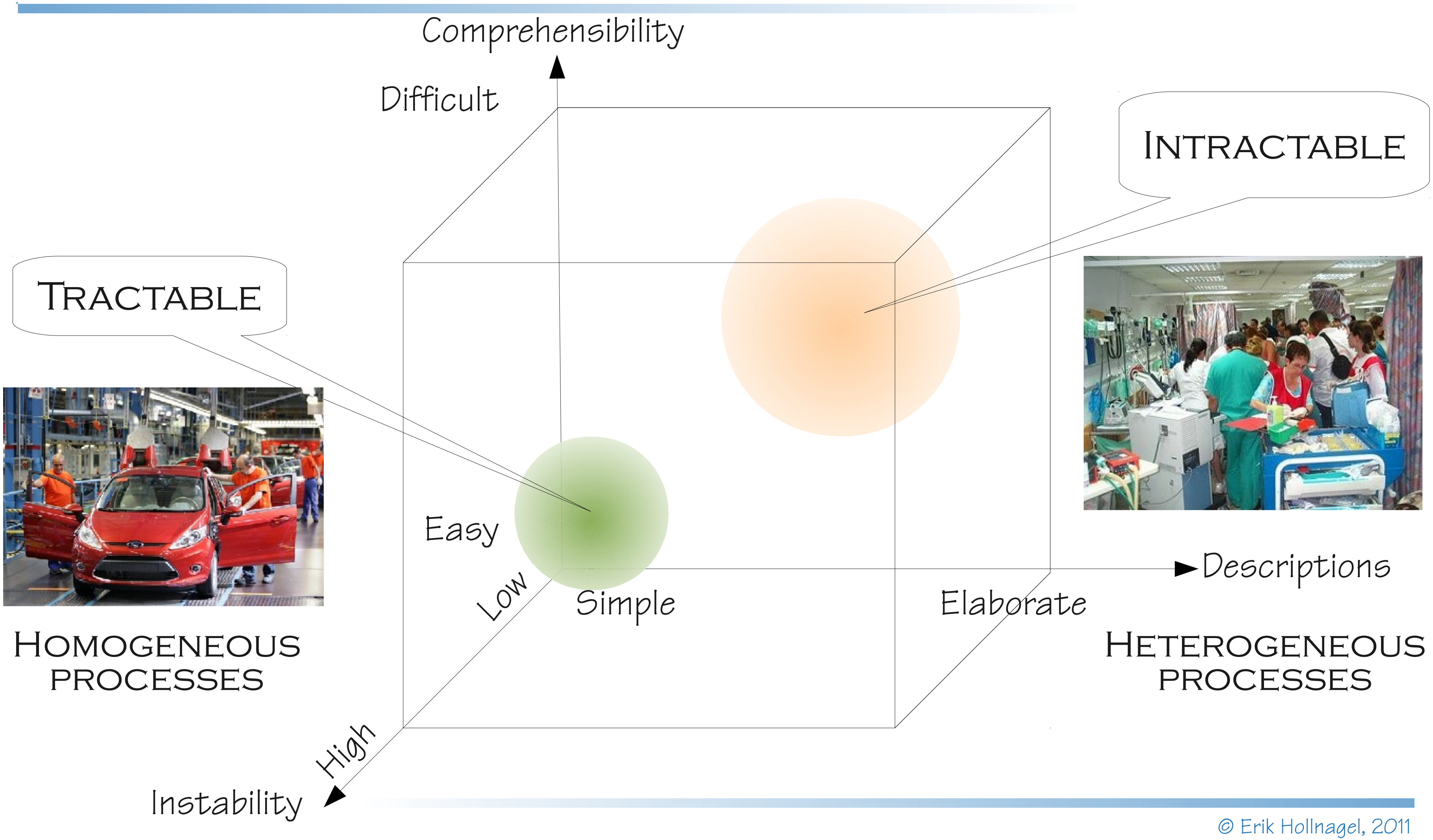
Syddansk Universitet
University of Southern Denmark

Range of event outcomes



© Erik Hollnagel, 2011

Tractable and intractable systems



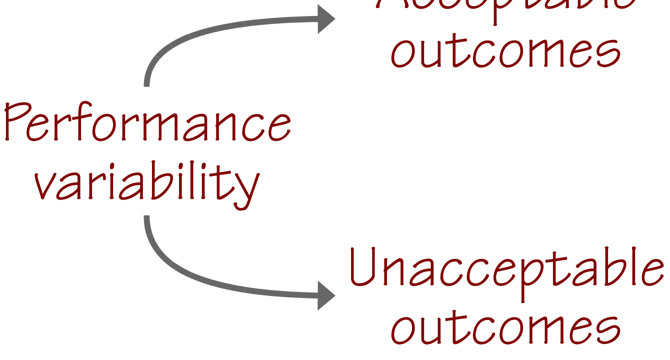
Performance variability is necessary

Most socio-technical systems are intractable. Conditions of work are therefore underspecified.

Resources (time, manpower, materials, information, etc.) may be limited or unavailable

People (individually and collectively) must adjust what they do to match the conditions.

For the very same reasons, the adjustments will always be approximate.



☺ The approximate adjustments are the reason why everyday work is safe and effective.

☹ But the approximate adjustments are also the reason why things sometimes go wrong.

Efficiency-Thoroughness Trade-Off

Thoroughness: Time to think

Recognising situation.
Choosing and planning.

If thoroughness dominates, there may be too little time to carry out the actions.

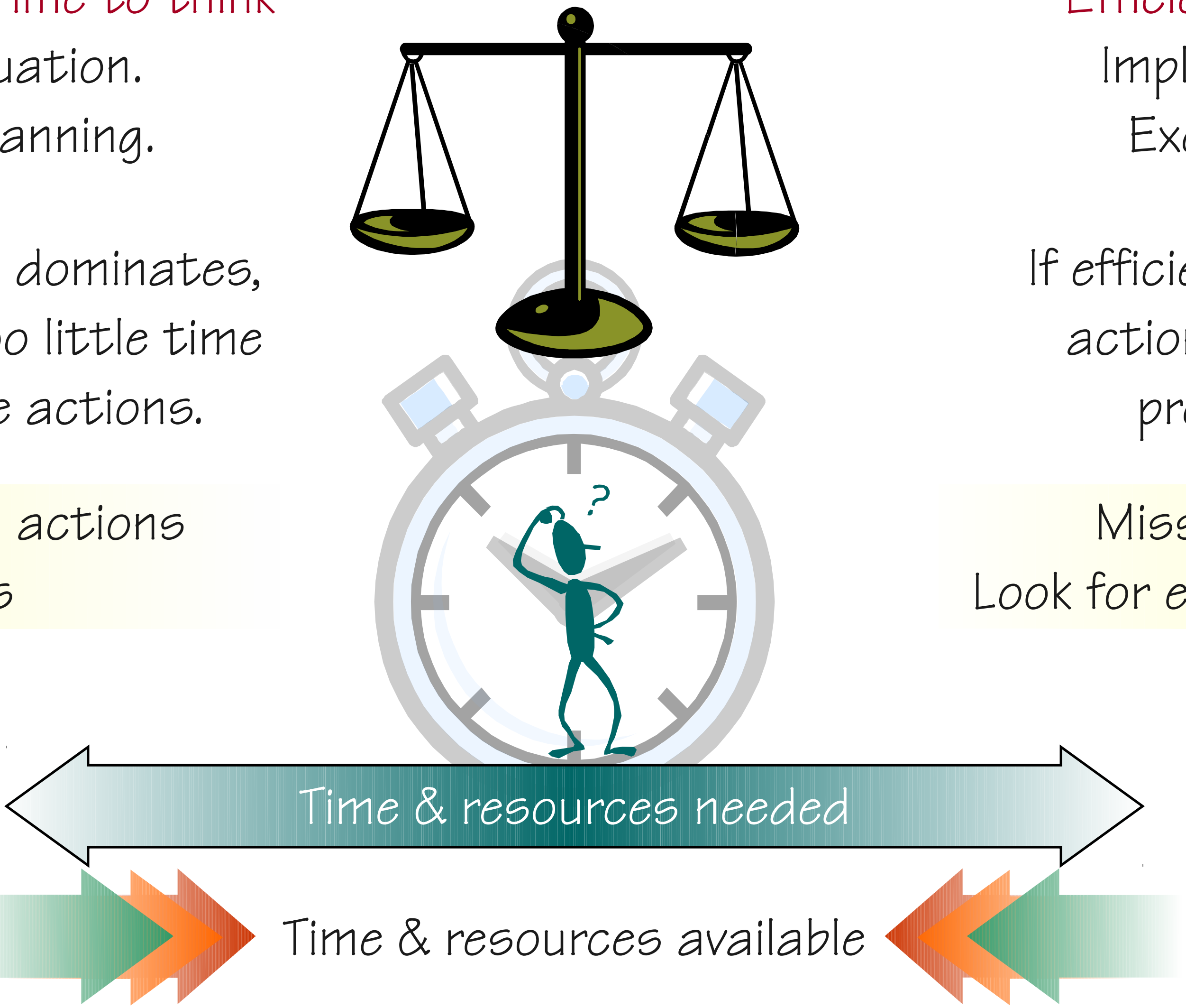
Neglect pending actions
Miss new events

Efficiency: Time to do

Implementing plans.
Executing actions.

If efficiency dominates, actions may be badly prepared or wrong

Miss pre-conditions
Look for expected results



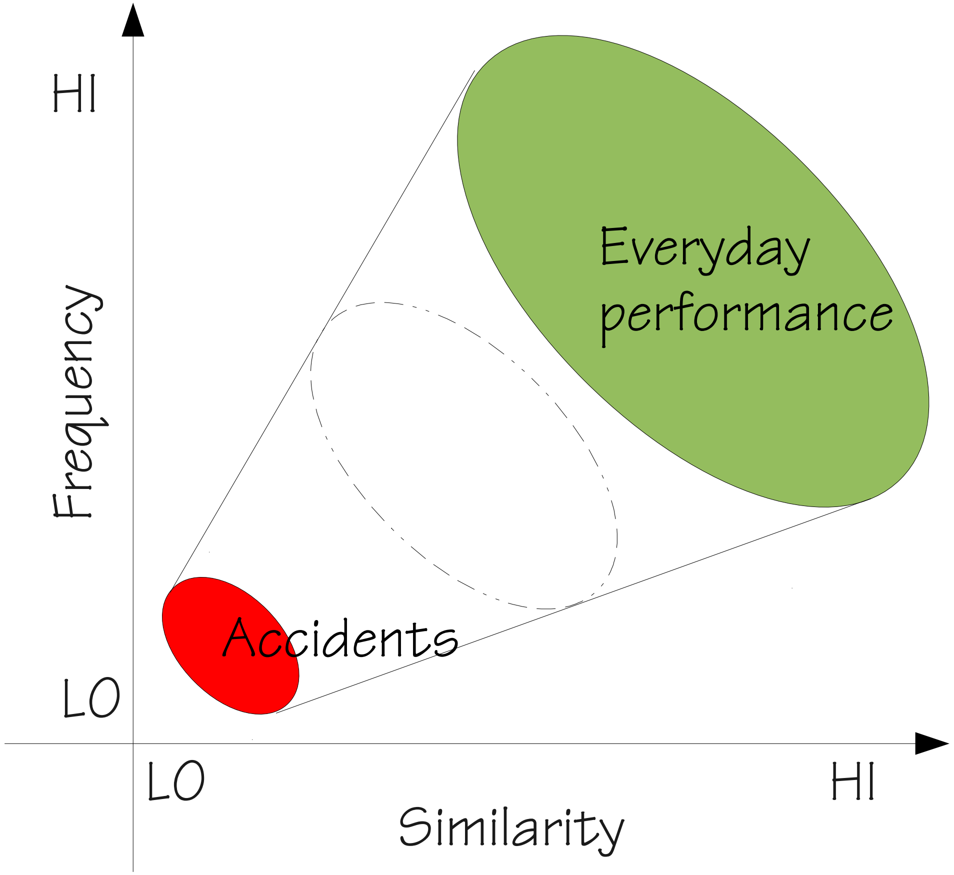
ETTOing in grid control

Balancing of load and generation capacity in real time. California electricity crisis, 2001. (Schulman et al., 2004).

		System instability (uncontrollable load changes)	
		High	Low
Network option variety (electricity generation resources)	High	Just-in-time (keep real-time capability)	Just-in-case (be ready in case something happens)
	Low	Just-for-now (firefighting)	Just-this-way (constrain environment to match options)

"Part of the experience is to know when not to follow procedures ...there are bad days when a procedure doesn't cover it, and then you have to use your wits."

What does it take to learn?



Opportunity (to learn): Learning situations (cases) must be frequent enough for a learning practice to develop

Comparable /similar: Learning situations must have enough in common to allow for generalisation.

Opportunity (to verify): It must be possible to verify that the learning was 'correct' (feedback)

The purpose of learning (from accidents, etc.) is to change behaviour so that certain outcomes become more likely and other outcomes less likely.

The learning paradox

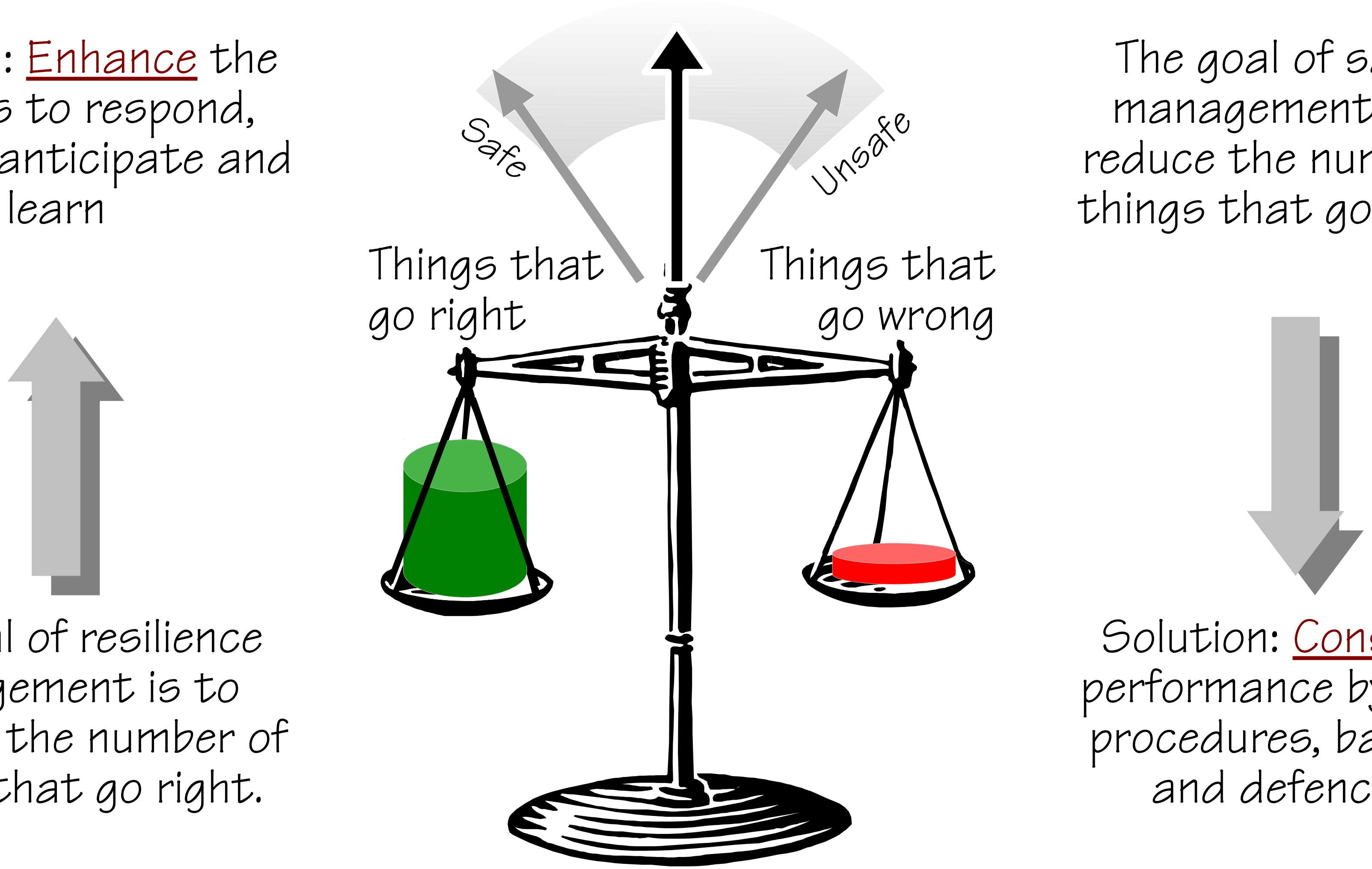
Things that go wrong: accidents, incidents, etc.		Things that go right: everyday performance
Not good: things rarely go wrong, especially for serious outcomes	Opportunity to learn: How often does it happen?	Excellent: everyday performance is usually “correct”
Very little, and less the more serious the events are.	Similarity / comparability: How much do different events have in common?	Very much, particularly for every performance
Not good: accidents and incidents are both infrequent and dissimilar	Opportunity to verify: Is it possible to confirm that the learning was correct?	Very good: everyday performance is always at hand

It is ironical that we usually spend most of the effort on events that are the least well suited for learning.

Engineering resilience

Solution: Enhance the abilities to respond, monitor, anticipate and learn

The goal of resilience management is to increase the number of things that go right.



The goal of safety management is to reduce the number of things that go wrong.

Solution: Constrain performance by rules, procedures, barriers, and defences.

What You Find Is What You Learn

Type of event	Frequency, characteristics	Aetiology	Transfer of learning, (verifiable)
Rare events (unexampled, irregular)	Happens exceptionally, each event is unique	Emergent rather than cause-effect	Very low, comparison not possible
Accidents & incidents	Happens rarely, highly dissimilar	Causes and conditions combined	Very low, comparison difficult, little feedback
Successful recoveries (near misses)	Happens occasionally, many common traits	Context-driven trade-offs.	Low, delayed feedback
Normal performance	Happens all the time, highly similar	Performance adjustments	Very high, easy to verify and evaluate

Thank you for your attention