MINES ParisTech

弾

Resilience Engineering: The changing nature of safety

Erik Hollnagel

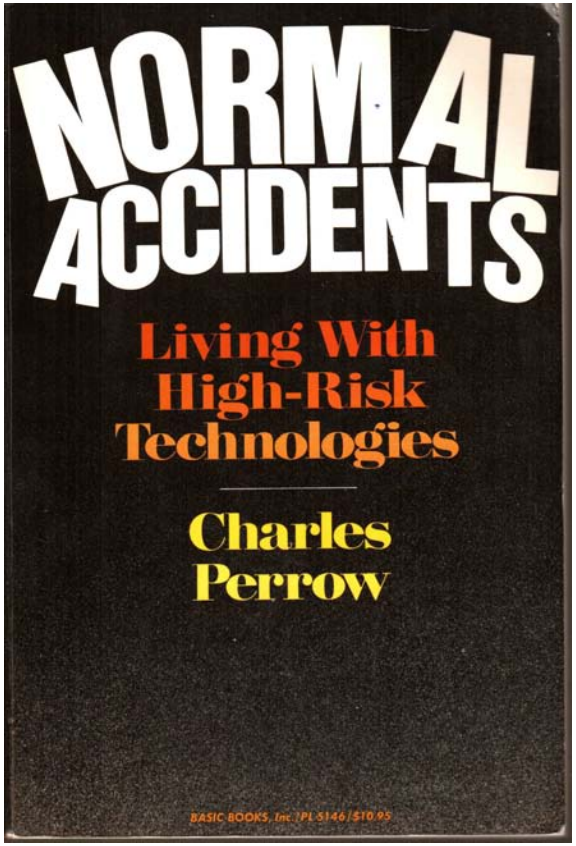
Professor &
Industrial Safety Chair
MINES ParisTech
Sophia Antipolis, France

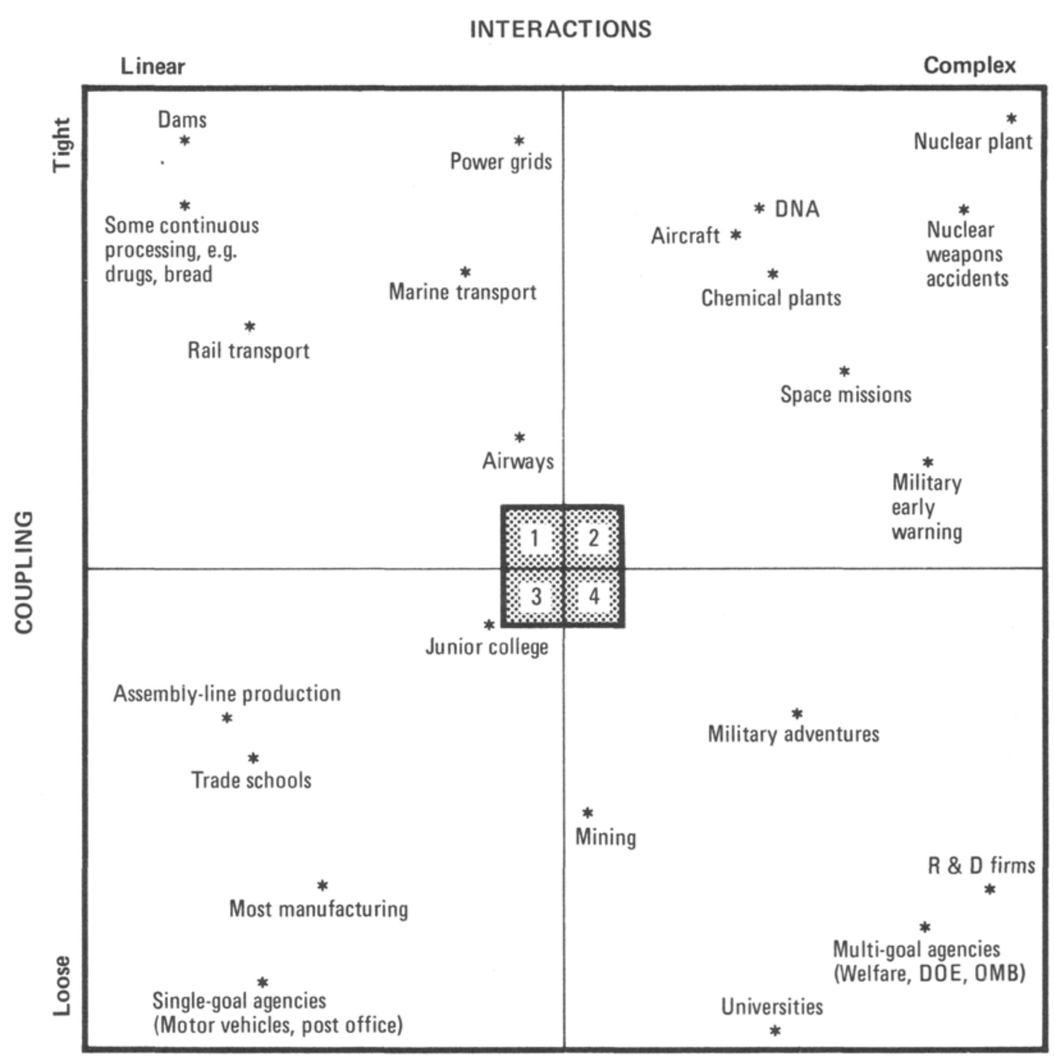
Professor II
NTNU
Trondheim, Norge

E-mail: erik.hollnagel@gmail.com

MINES ParisTech

Normal accident theory (1984)

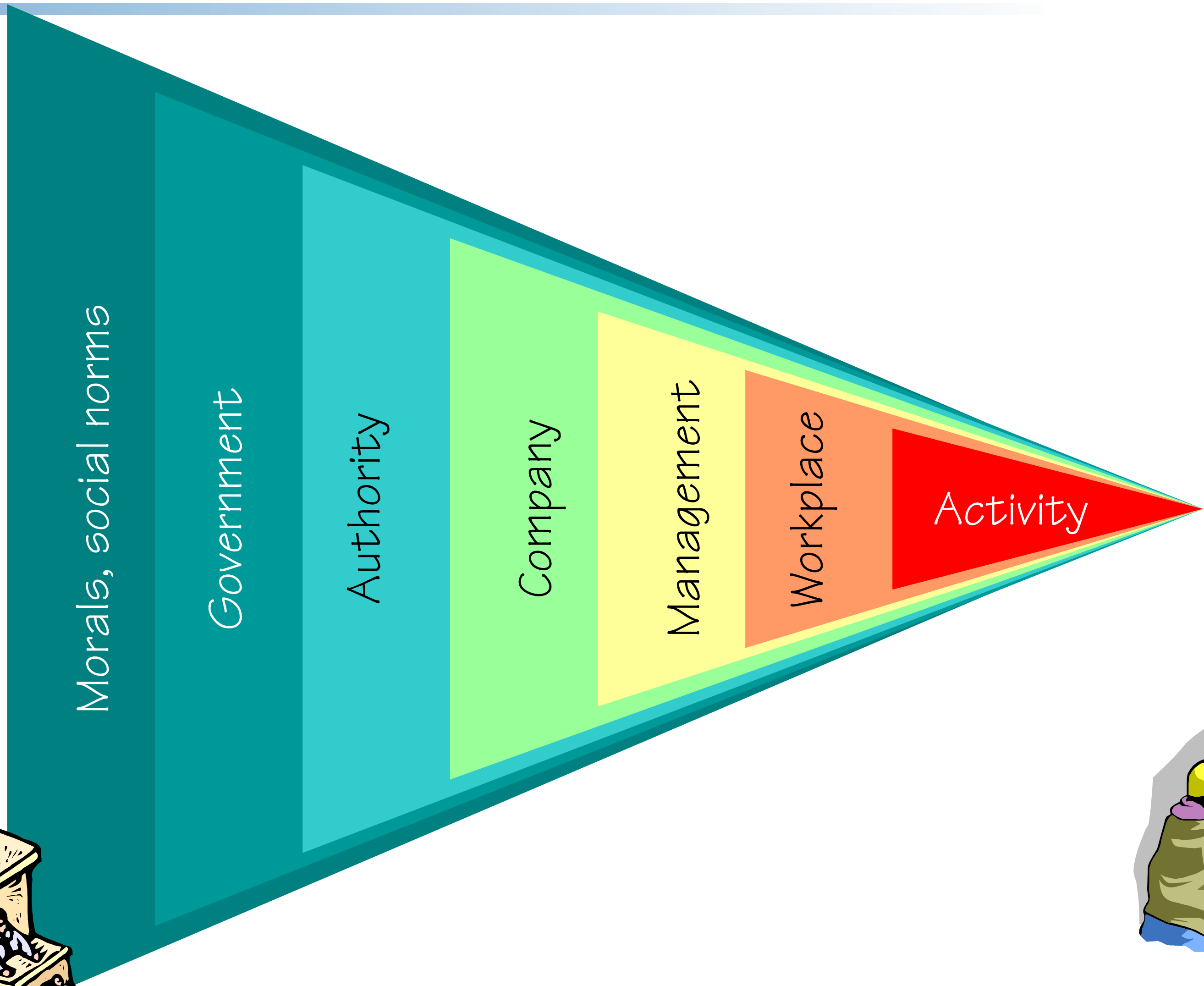




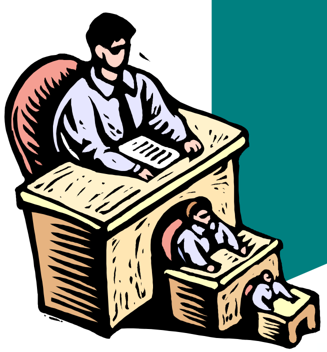
"On the whole, we have complex systems because we don't know how to produce the output through linear systems."

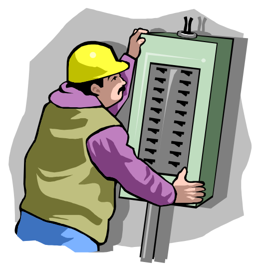
MTO view: sharp-end, blunt-end

Blunt-end failures happened earlier and somewhere else

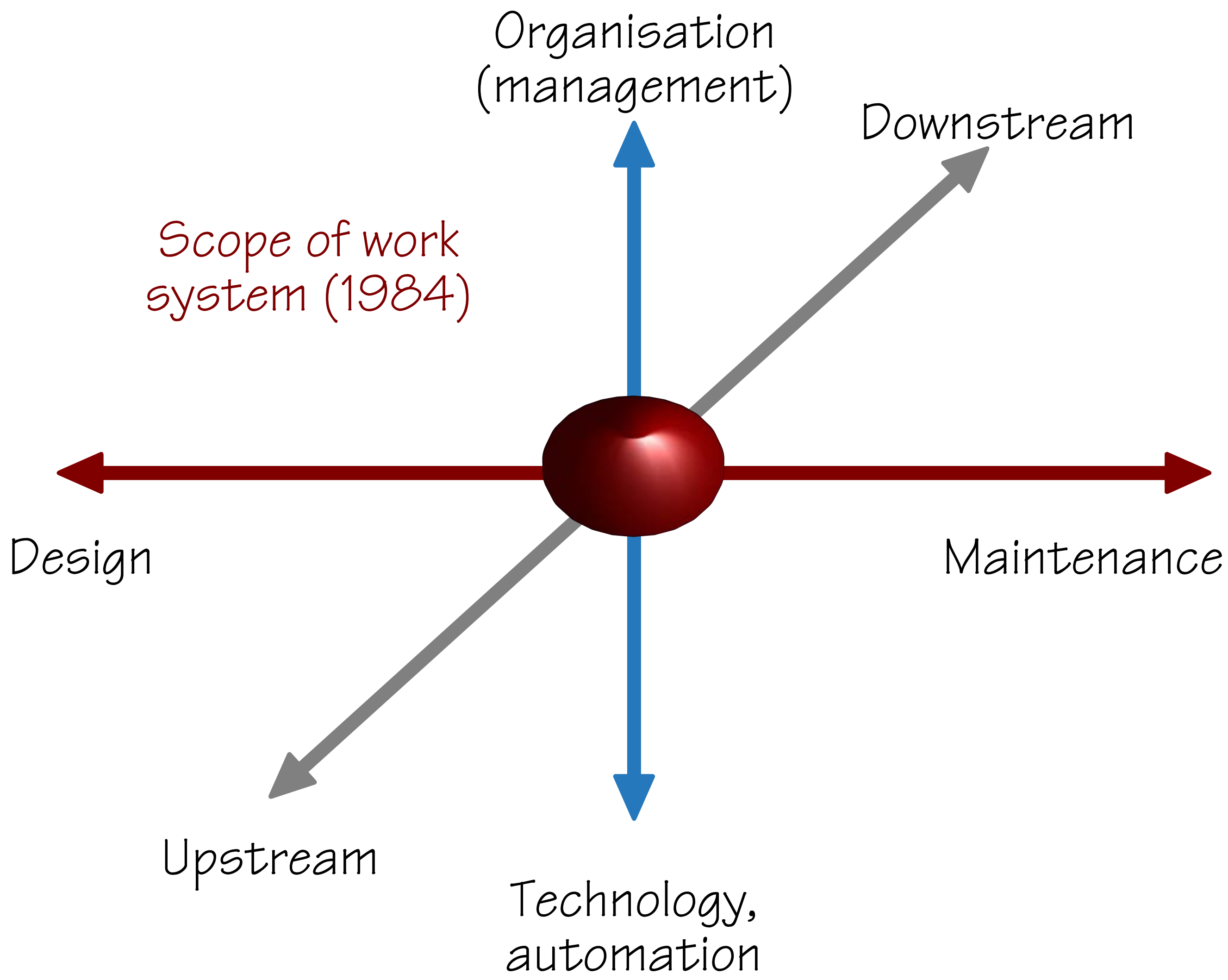


Sharp-end failures happen here and now



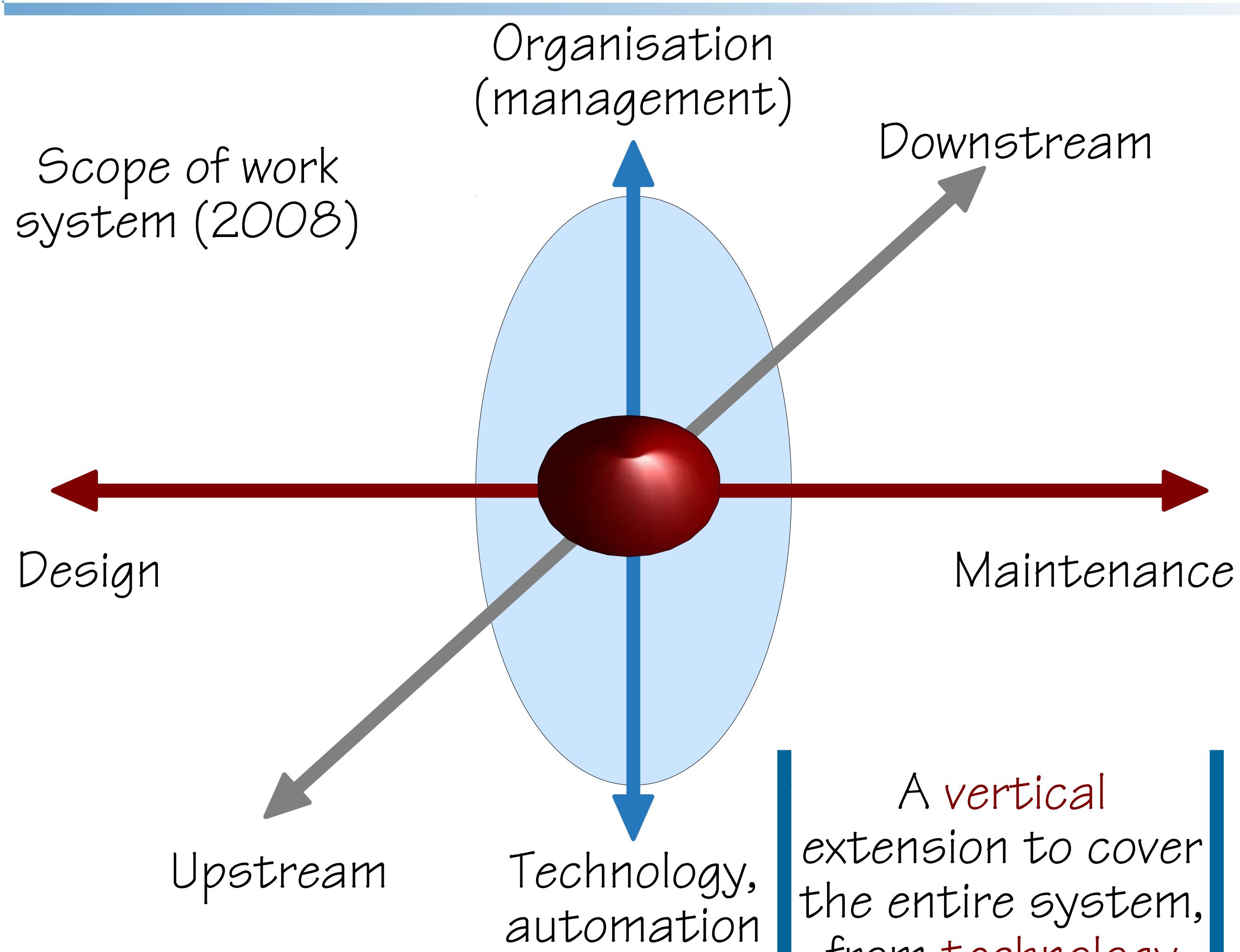


Focus on operation (sharp end)



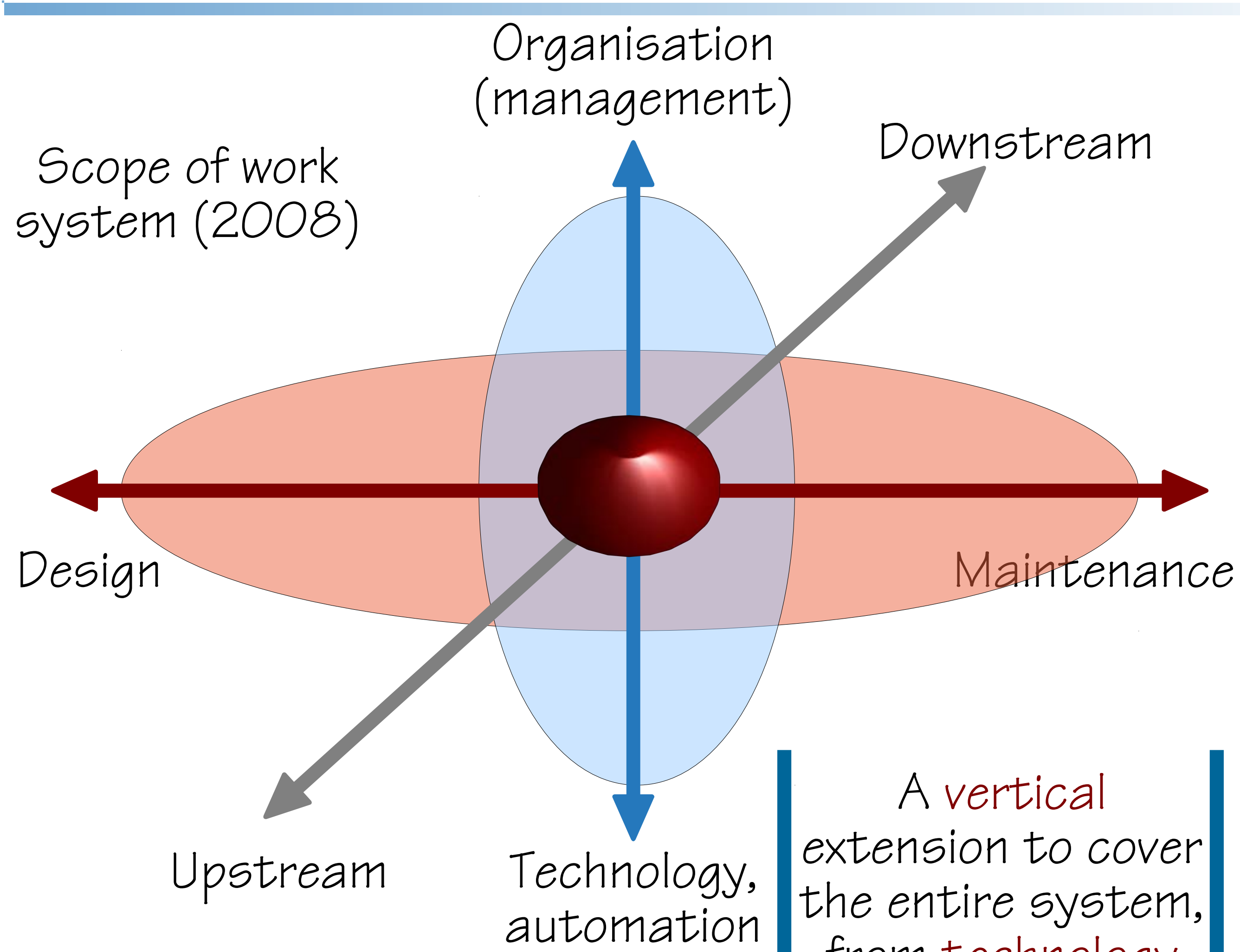
Work has clear objectives and takes place in well-defined situations. Systems and technologies are loosely coupled and tractable.

Vertical and horizontal extensions



A vertical extension to cover the entire system, from technology to organisation

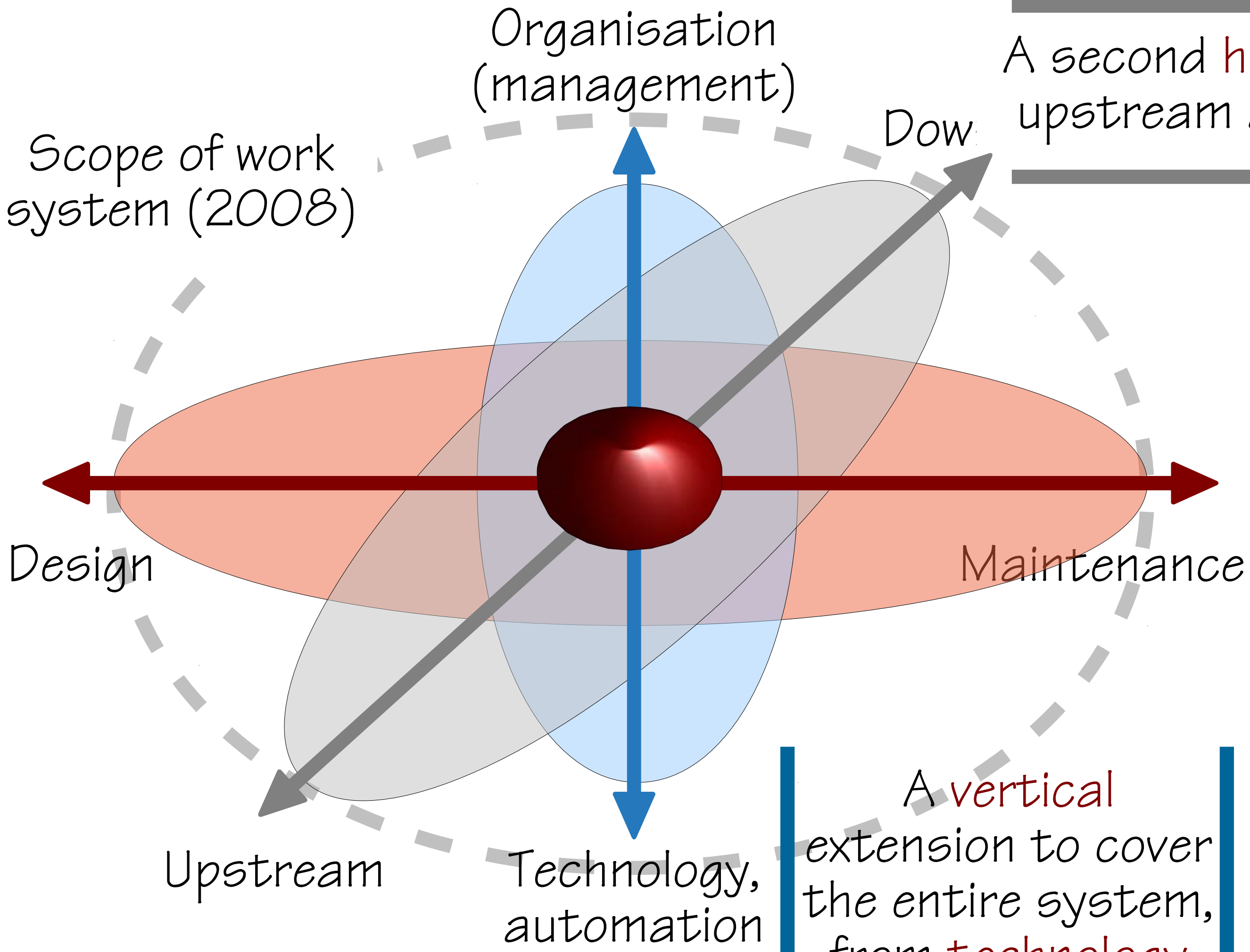
Vertical and horizontal extensions



One horizontal extension, to cover the lifecycle, from design to maintenance

A vertical extension to cover the entire system, from technology to organisation

Vertical and horizontal extensions



A second horizontal extension, to cover upstream and downstream processes

One horizontal extension, to cover the lifecycle, from design to maintenance

A vertical extension to cover the entire system, from technology to organisation

Tractable and intractable systems

Tractable system (independent, clockwork)		Intractable system (interdependent, teamwork)
Description are simple with few details	Complicacy	Elaborate descriptions with many details
Principles of functioning known (white box)	Comprehensibility	Principles of functioning unknown (black box)
System does not change while being described	Stability	System changes before description is completed

Fully specified

Partly specified

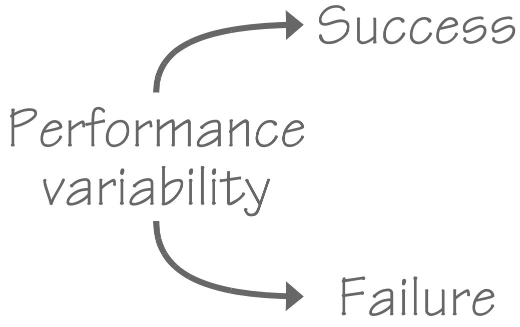
Underspecified

Performance variability is necessary

Systems are so complex that work situations always ar
underspecified – hence partly unpredictable

Few – if any – tasks can successfully be carried out
unless procedures and tools are adapted to the situati
Performance variability is both normal and necessary.

Many socio-technical systems are intractable. The conditions of work therefore never completely match what has been specified or prescribed.



Individuals, groups, and organisations normally adjust their performance to meet existing conditions, specifically actual resources and requirements.

Because resources (time, manpower, information, etc.) always are finite, such adjustments will always be approximate rather than exact.

Efficiency-Thoroughness Trade-Off

MINES ParisTech

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

Time & resources needed

Time & resources available

The ETTO principle

The ETTO principle describes the fact that people (and organisations) as part of their activities practically always must make a trade-off between the resources (time and effort) they spend on preparing an activity and the resources (time, effort and materials) they spend on doing it.

ETTOing favours thoroughness over efficiency if safety and quality are the dominant concerns, and efficiency over thoroughness if throughput and output are the dominant concerns.

The ETTO principle means that it is impossible to maximise efficiency and thoroughness at the same time. Neither can an activity expect to succeed, if there is not a minimum of either.

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.

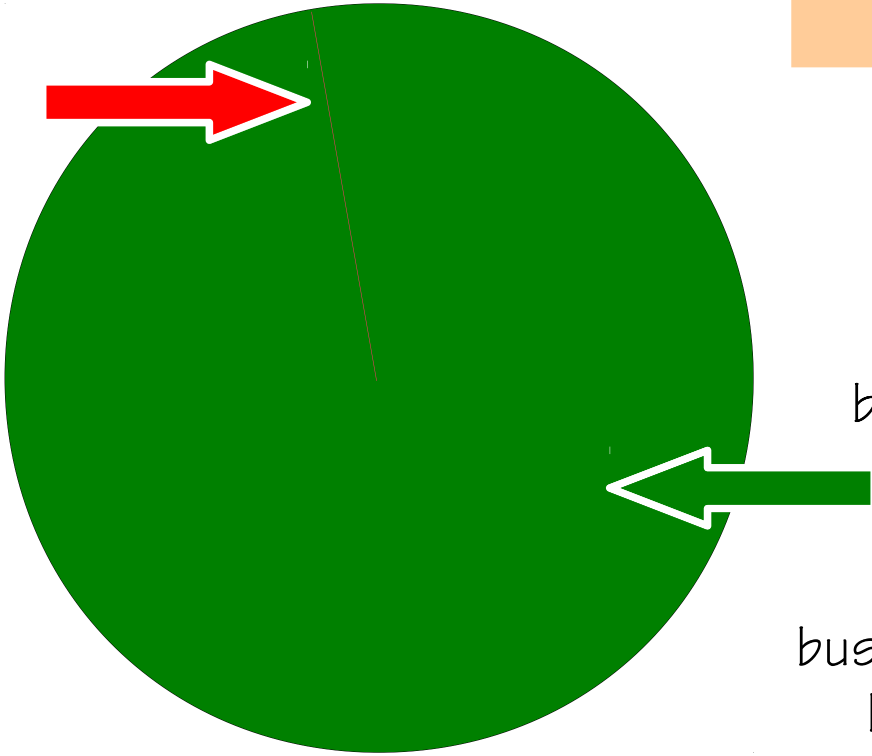
Why only look at what goes wrong?

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

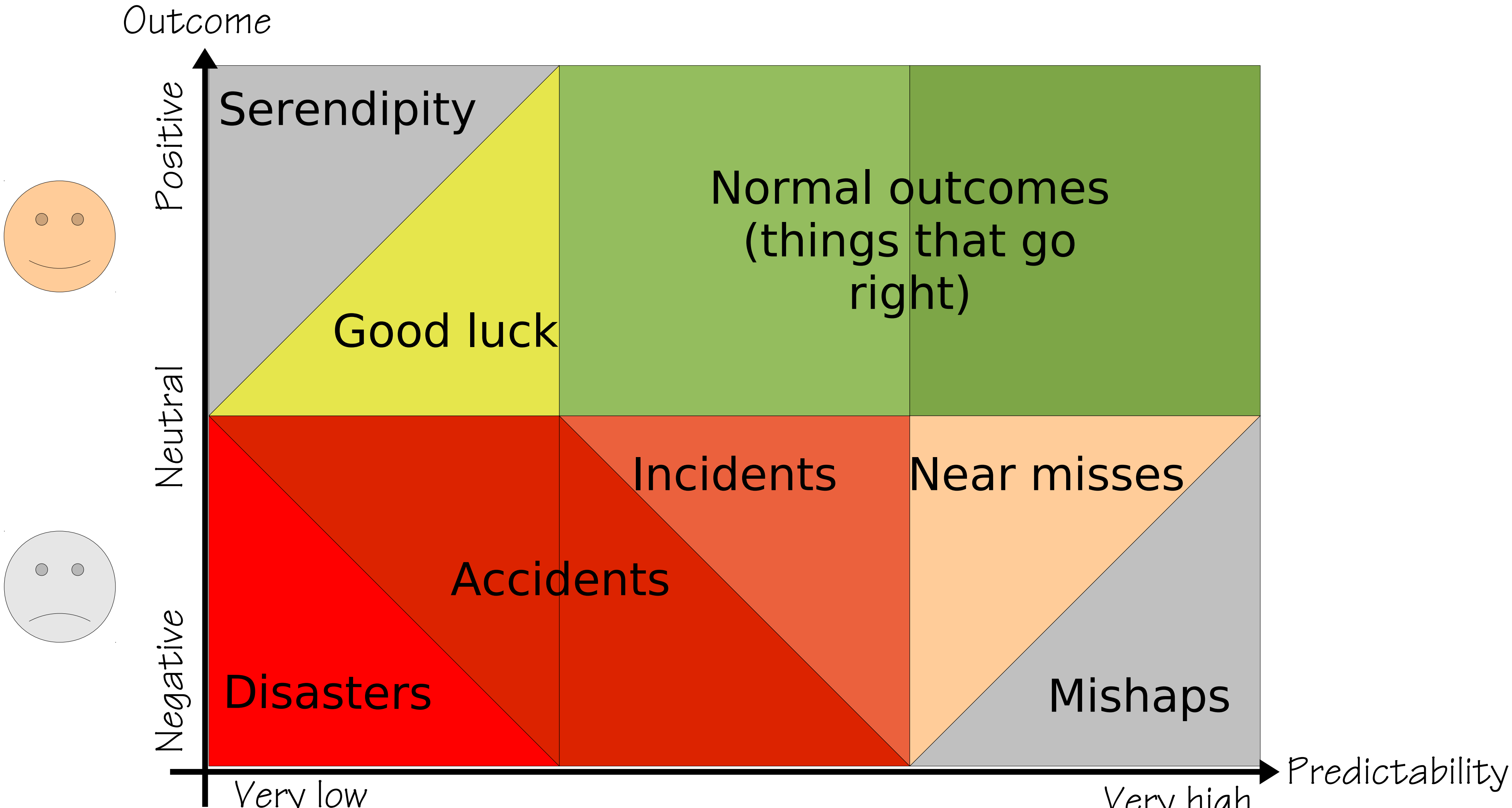
Risk profile (= lack of safety)

Consequence ↓ / Probability →	Rare	Unlikely	Possible	Likely	Certain
Negligible	Low	Low	Low	Moderate	Moderate
Marginal	Low	Low	Moderate	High	High
Critical	Moderate	Moderate	High	High	Extreme
Very critical	High	High	Extreme	Extreme	Extreme

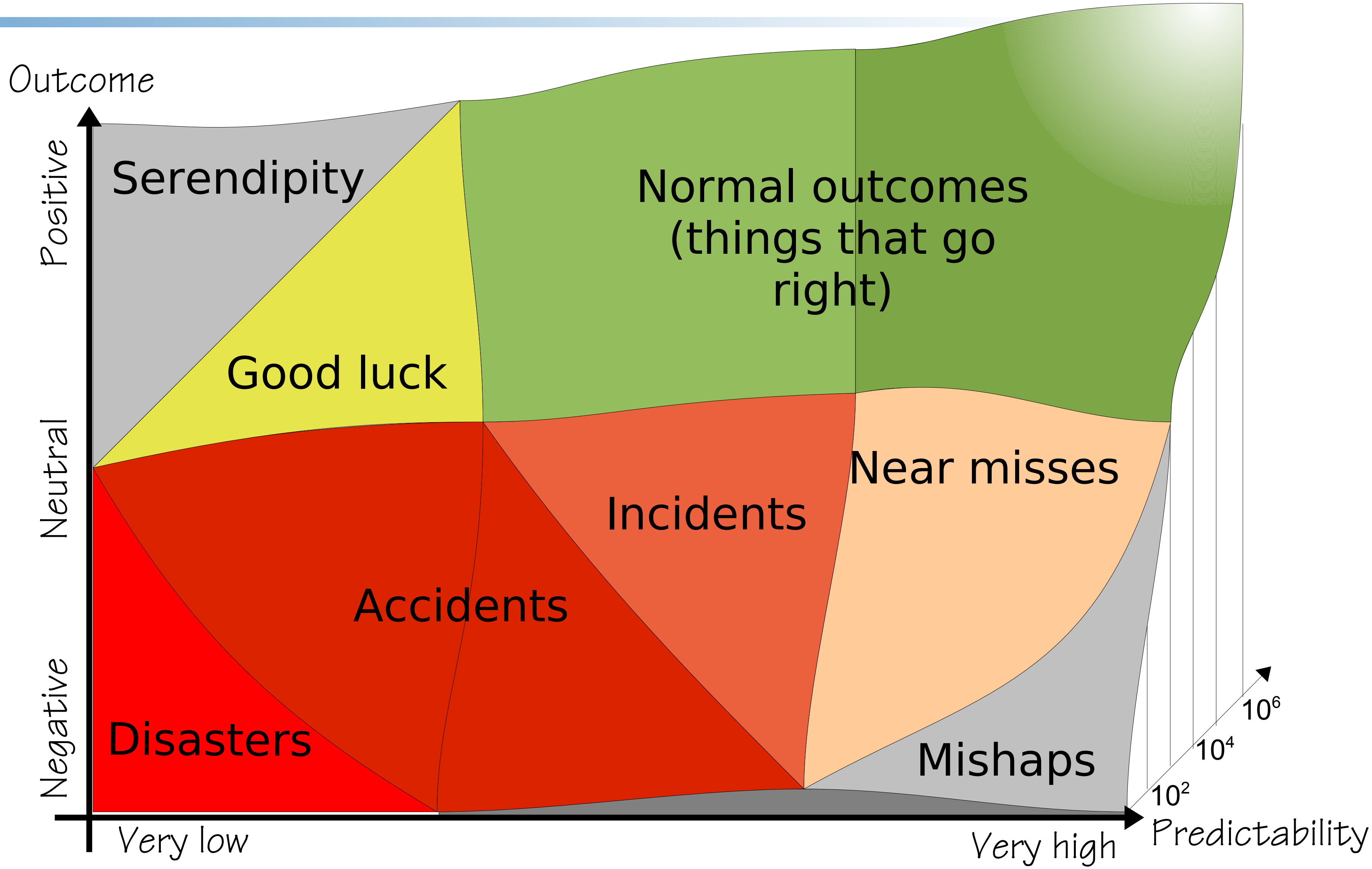
Benefit profile (= safety)

Consequence \ Probability	Rare	Unlikely	Possible	Likely	Certain
Innovative	High	High	Very high	Very high	Very high
Effective	Moderate	Moderate	High	High	Very high
Acceptable	Low	Low	Moderate	High	High
Negligible	Low	Low	Low	Moderate	Moderate

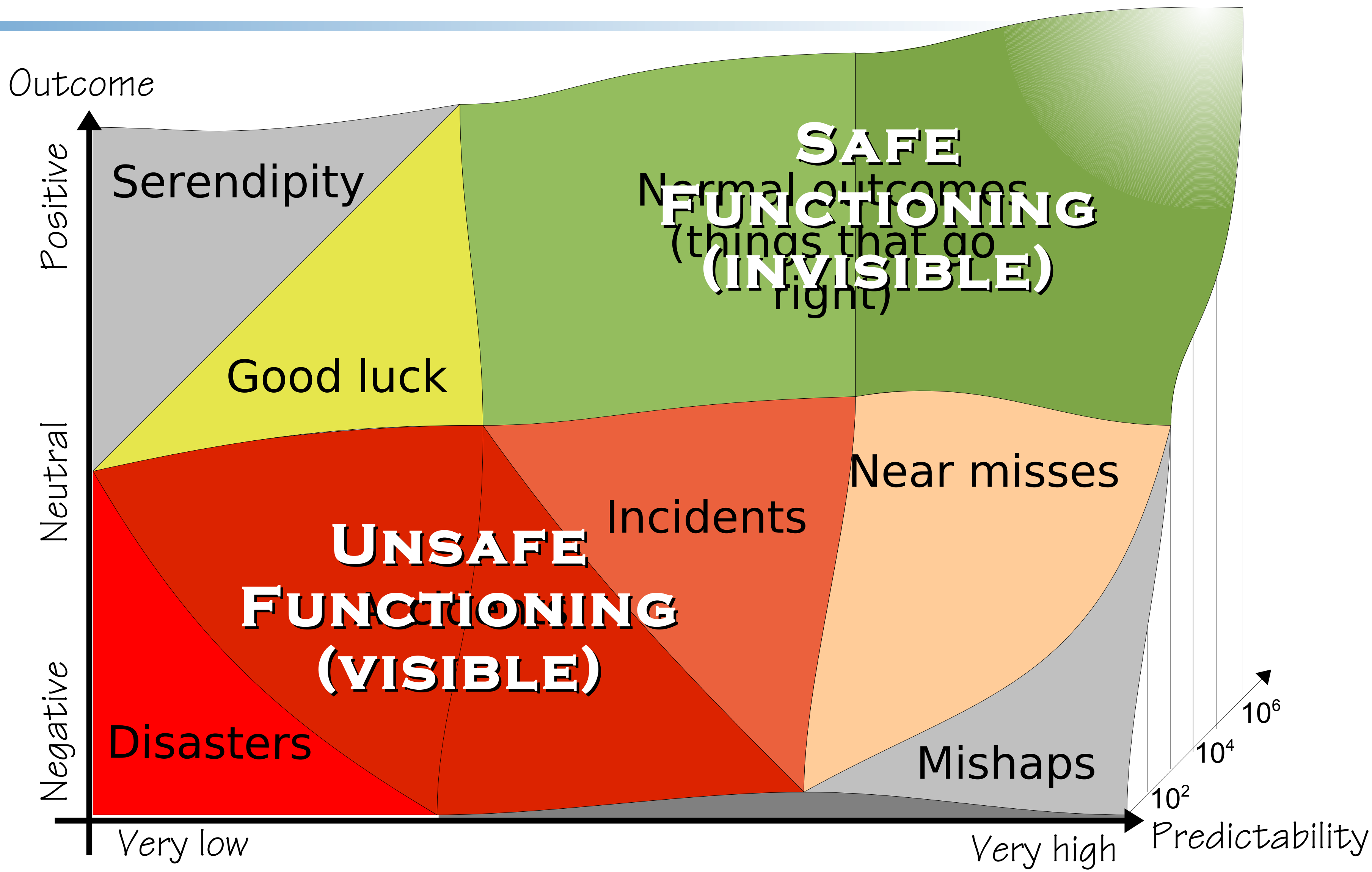
Range of event outcomes



Frequency of event outcomes

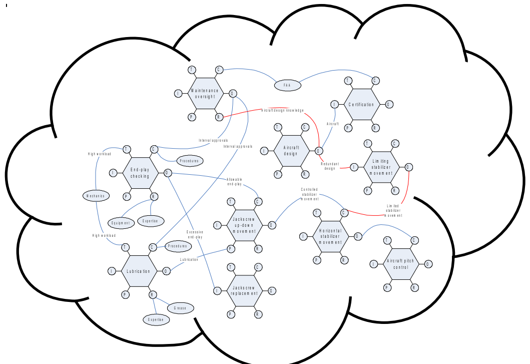


Being safe versus being unsafe

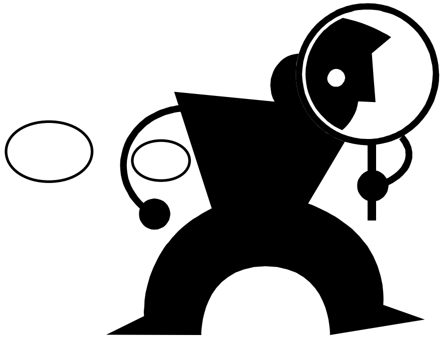


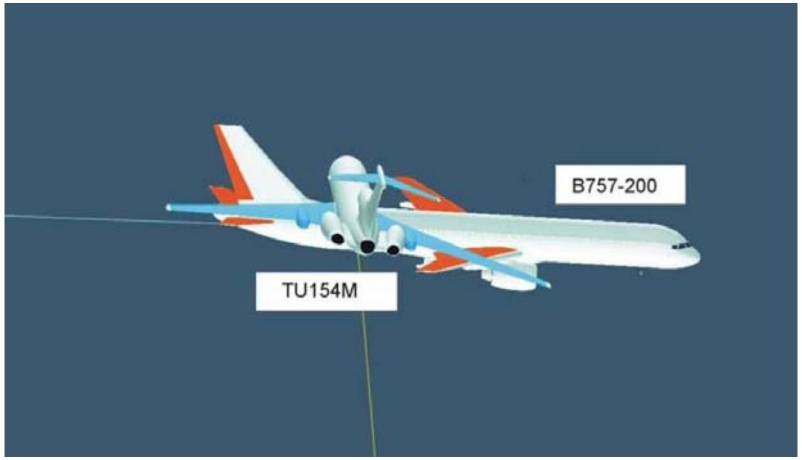
Non-linear accident model

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



Functional Resonance Accident Model





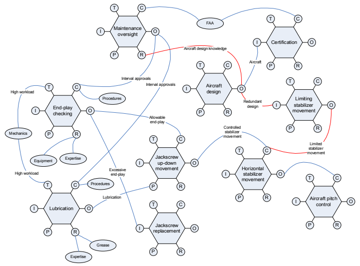
Consequence: Accidents are prevented by monitoring and damping variability. Safety requires constant ability to anticipate future events.

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

* ETTO = Efficiency-Thoroughness Trade-Off

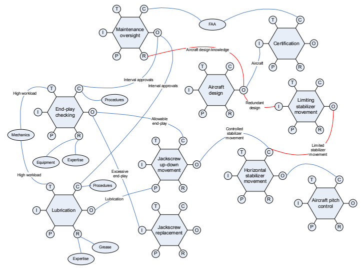
Risks as non-linear combinations

If accidents happen like this …



Unexpected combinations (resonance) of variability of normal performance.

… then risks can be found like this …



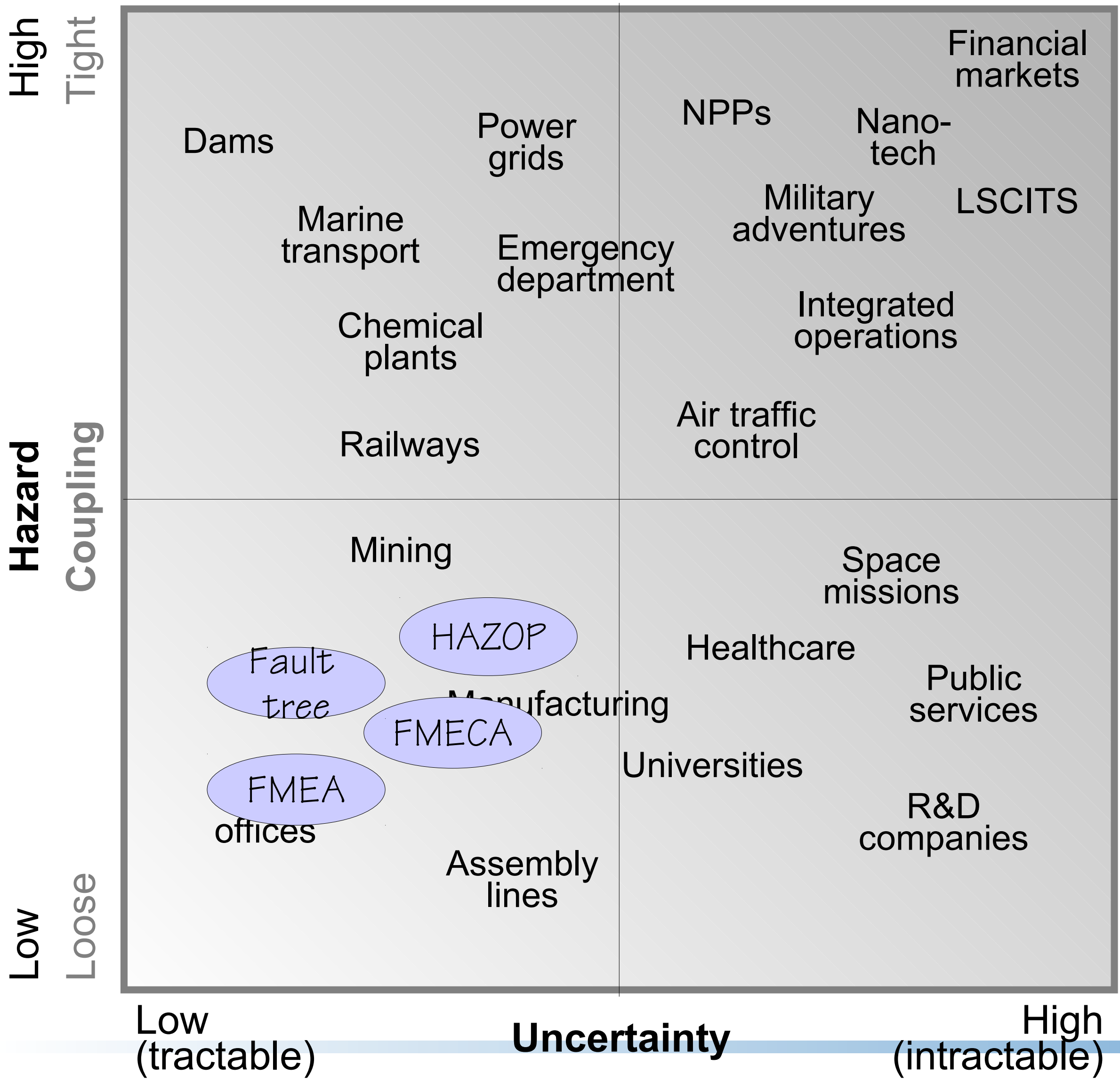
Unexpected combinations (resonance) of variability of normal performance.

Systems at risk are intractable rather than tractable. → The established assumptions therefore have to be revised

Methods and reality

Simple linear

Focus on technology



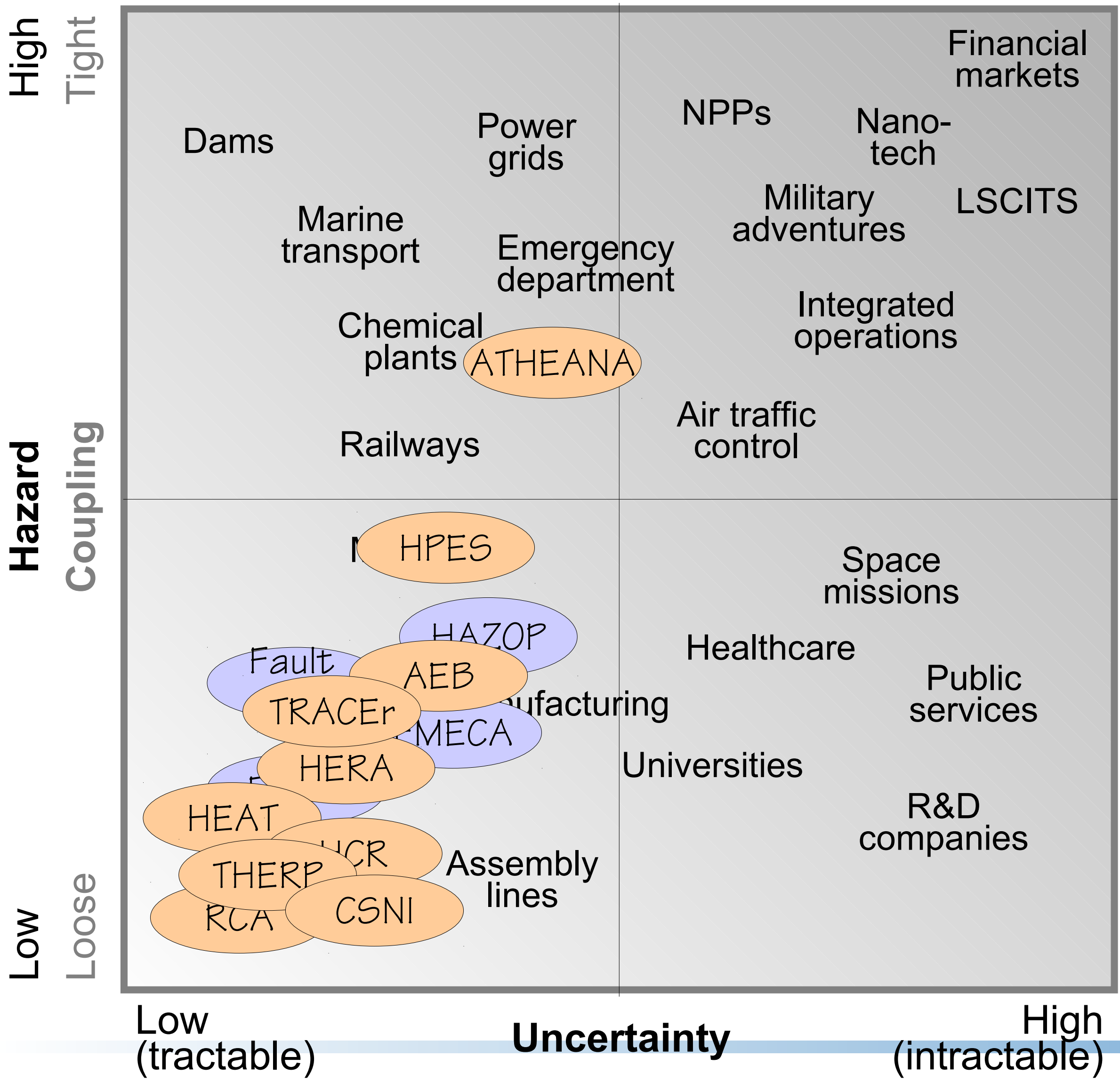
Methods and reality

Simple linear

Focus on technology

Complex linear

Focus on Human Factors



Hazard and uncertainty

Simple linear

Focus on technology

Complex linear

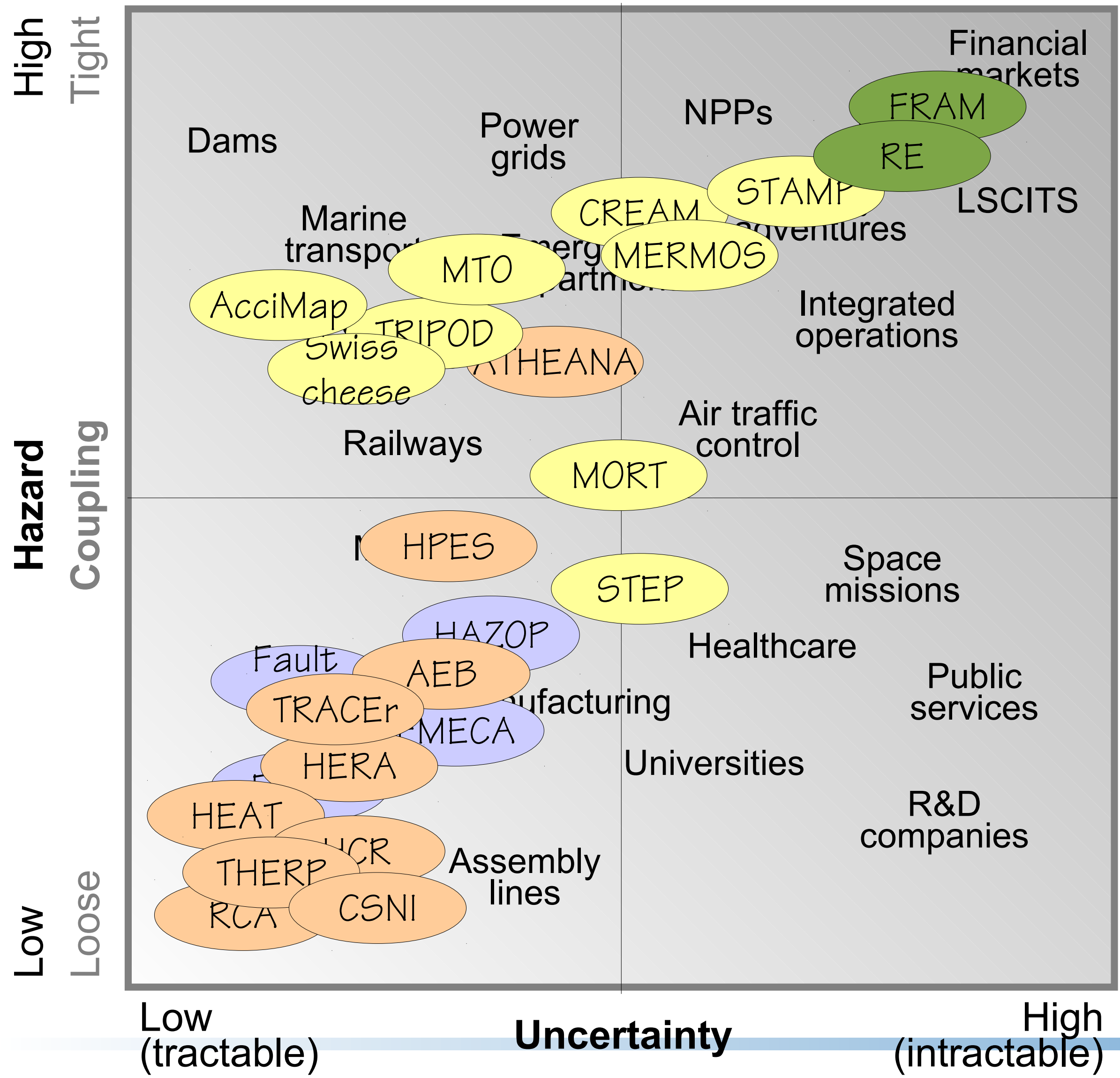
Focus on Human Factors

Complex linear

Focus on organisations

Non-linear

Focus on normal functions



From the negative to the positive

Negative outcomes are caused by failures and malfunctions.

All outcomes (positive and negative) are due to performance variability..

− +

Safety = Reduced number of adverse events.

Safety = Ability to respond when something fails.

Safety = Ability to succeed under varying conditions.

Eliminate failures and malfunctions as far as possible.

Improve ability to respond to adverse events.

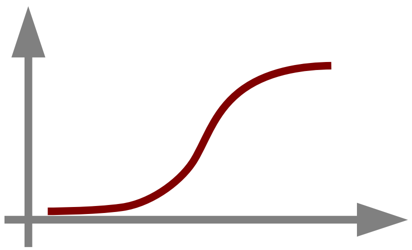
Improve resilience.

What is safety?

Safety

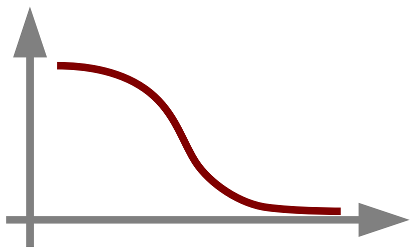
The ability to succeed under varying conditions (respond, monitor, anticipate, learn)

Systemic (process view)
Safety should be As High As Reasonably Practicable (AHARP)



The reduction of unnecessary harm to an acceptable minimum

Particularistic (product view)
Risk should be As Low As Reasonably Practicable (ALARP)



Conclusions so far ...

- Complex socio-technical systems can only function if performance is adjusted to conditions (ETTO)
- Performance variability is the reason why things go right, but also the reason why things sometimes go wrong.
- We need to understand how things go right before we can understand how they go wrong.
- Resilience engineering is about how we can ensure that systems remain productive and safe in expected and unexpected conditions alike.