Some myths about industrial safety

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

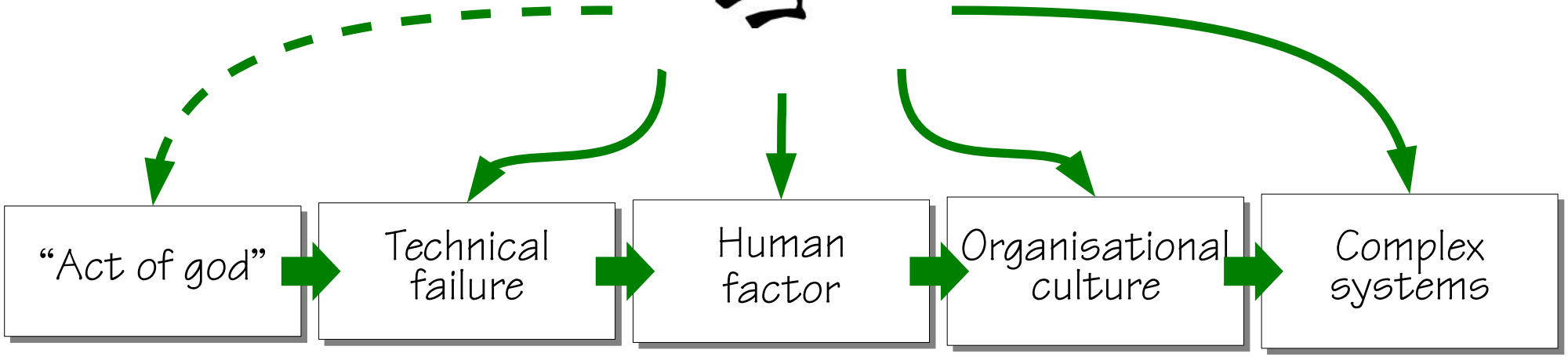
A need to explain and understand.

Safe tysyn thesis

Accidents, incidents, breakdowns, disruptions,

A need to <u>be</u> safe

A need to <u>feel</u> safe



The types of causes have changed over time, but we still believe in causality

Increasing safety by reducing failures

Safe tysyn thesis

Function (work as imagined) → Success (no adverse events) → Acceptable outcomes

"Identification and measurement of adverse events is central to safety."

Malfunction, non-compliance, error

"Find-and-fix"

Failure (accidents, incidents)

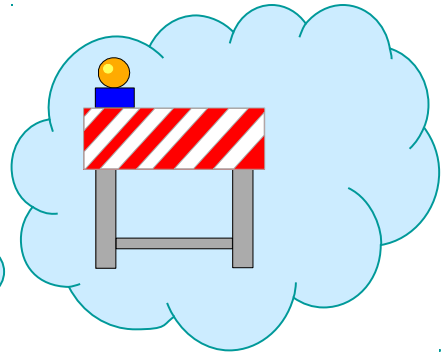
Unacceptable outcomes

From analysis to prevention

Safe tysyn thesis

What REALLY happened?

What were the CAUSES?



How should we RESPOND?

"Laws"
Theories
Hypotheses
Assumptions/myths

Causes: WHY do things go wrong?

"Mechanisms": HOW do things go wrong?

Laws, theories, hypotheses, and myths.

Safe tysyn thesis

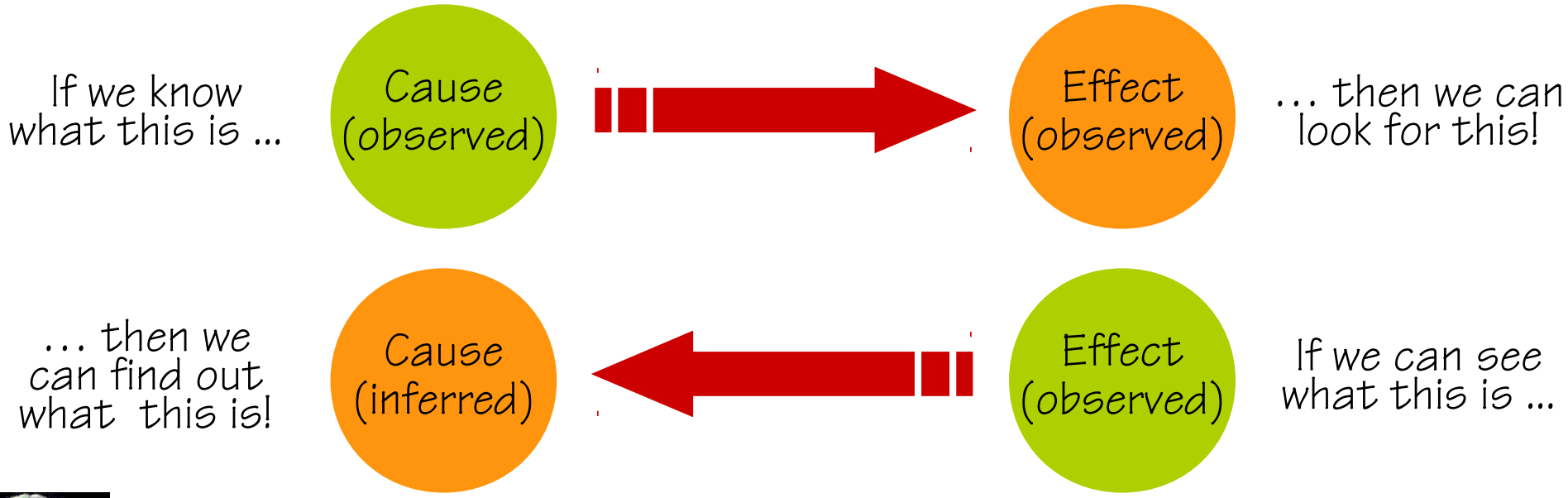
Law	A universal principle that describes the fundamental nature of something and the relationships between things. Example: The Law of Gravity. There are no “laws” of safety.
Theory	An explanation for some observation, which may lead to a number of possible hypotheses that can be tested in order to confirm or reject the theory. Example: GEMS (Generic Error Modelling System). There are many theories that apply to safety.
Hypothesis	A proposed explanation or a provisional idea whose merit requires evaluation. Example: “Accident risk increases as economic performance declines”. Hypotheses can be found almost everywhere in safety.
Myth	A myth is a convenient idea or assumption that people believe but which is not true. Myths express common beliefs and are therefore excellent vehicles for communication. Myths are taken for granted, and therefore never questioned.

Safety is achieved by "find-and-fix"

Safety tysynthesis

Myth #1: All accidents have causes which can be found and fixed.

Every cause has a consequence (effect)

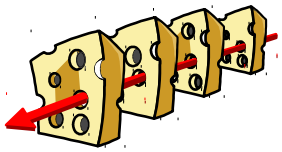


Every consequence (effect) has a prior cause

David Hume (1711-1776)

The causality credo

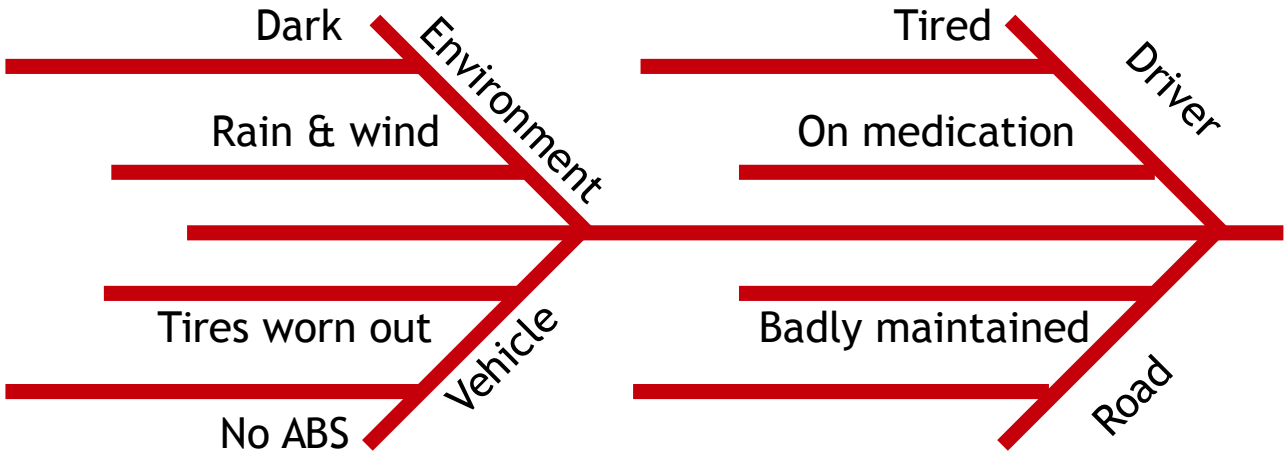
(1) Adverse outcomes happen because something has gone wrong (causality + value symmetry).
(2) Causes can be found and treated (deduction).
(3) All accidents are preventable (zero harm).

Accident investigation		Risk analysis
Find the component that failed by reasoning backwards from the final consequence.		Find the probability that components "break", either alone or in simple combinations.
Accidents result from a combination of active failures (unsafe acts) and latent conditions (hazards).		Look for combinations of failures and latent conditions that may constitute a risk.

Causes are assumed to be stable

Causes are assumed to be stable. Causes can be 'found' by backwards tracing from the effect. Causes are 'real.'

Final effects are (relatively) stable changes to some part of the system. Effects are 'real.'

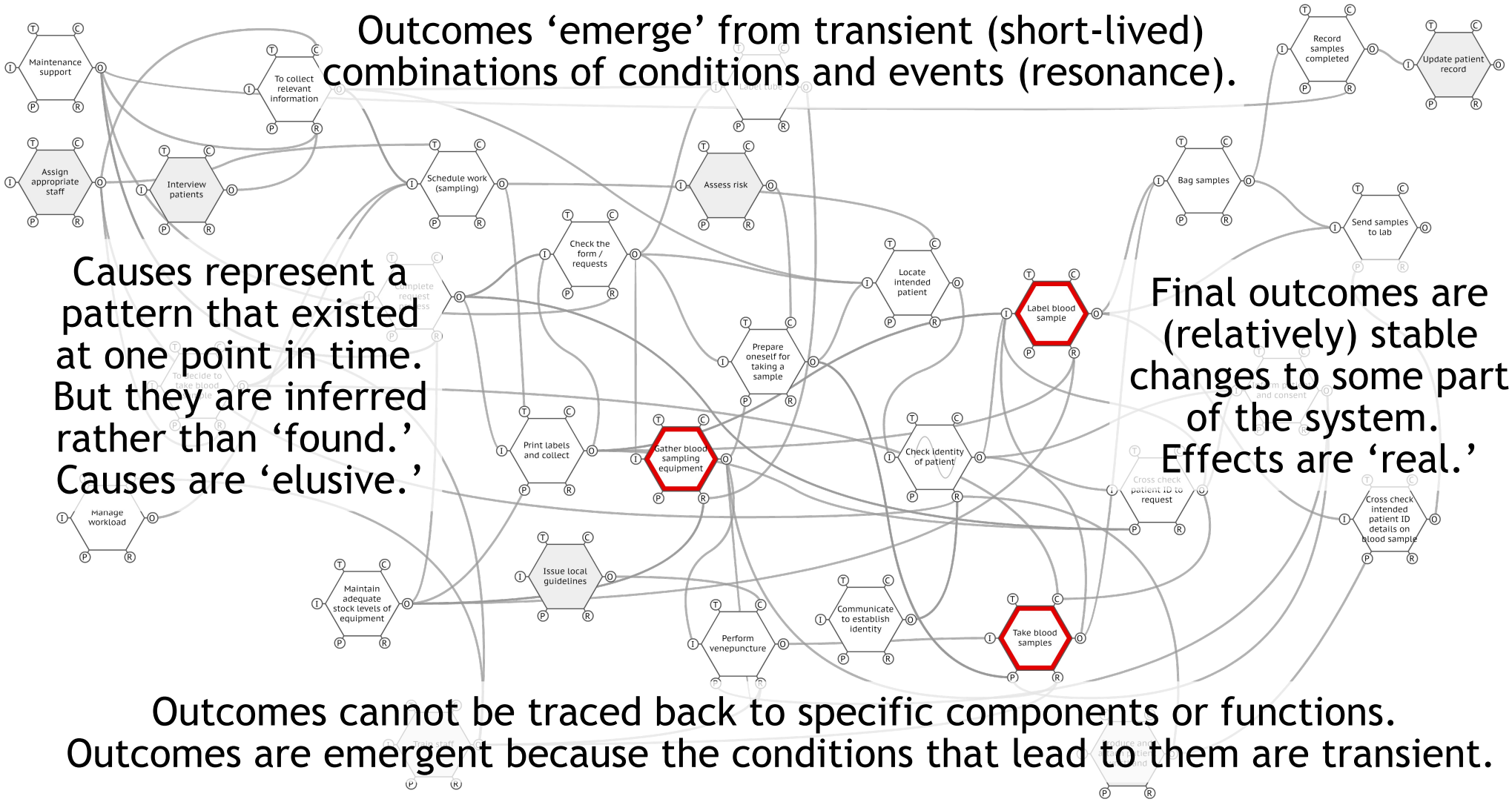


Causes can be associated with components or functions that in some way have 'failed.' The 'failure' is either visible after the fact, or can be deduced from the facts.

In reality, causes are often transient

Safe tysyn thesis

Outcomes ‘emerge’ from transient (short-lived) combinations of conditions and events (resonance).



Causes represent a pattern that existed at one point in time. But they are inferred rather than ‘found.’ Causes are ‘elusive.’

Final outcomes are (relatively) stable changes to some part of the system. Effects are ‘real.’

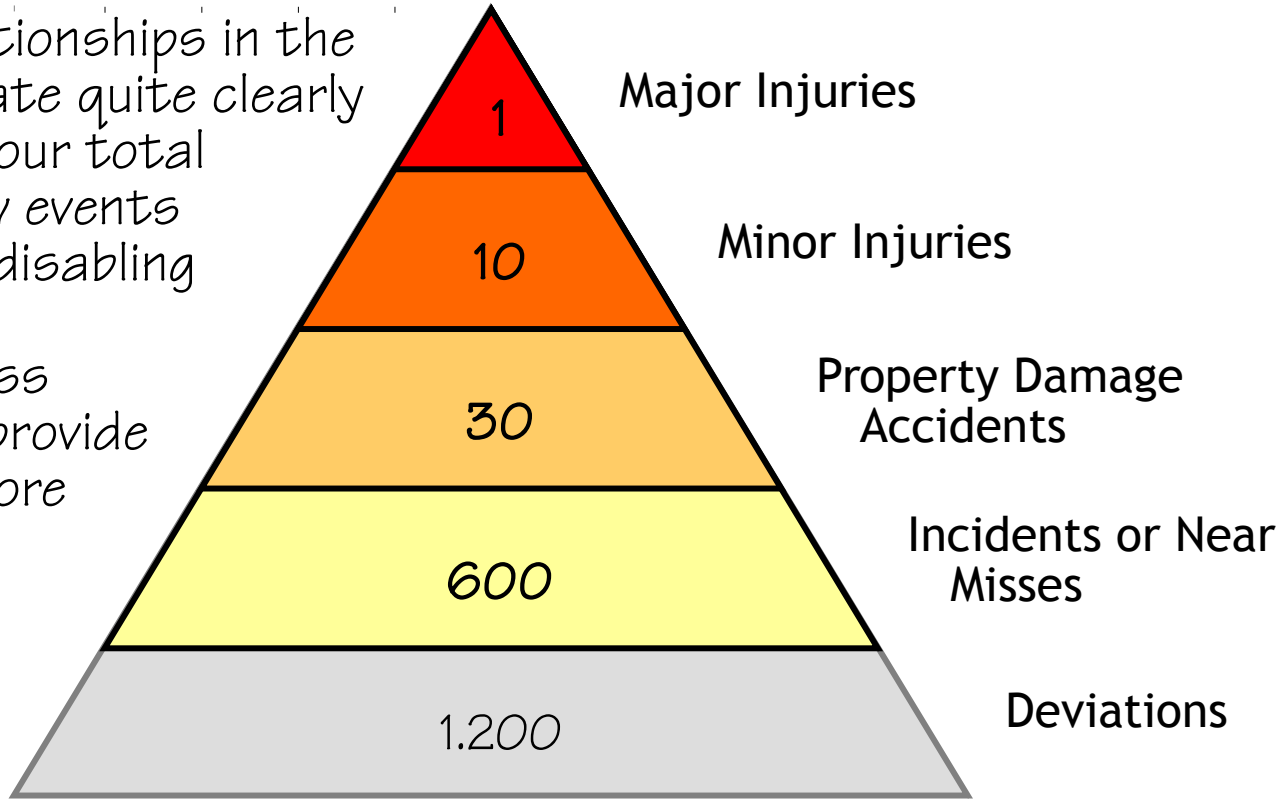
Outcomes cannot be traced back to specific components or functions. Outcomes are emergent because the conditions that lead to them are transient.

Adverse outcomes have a fixed ratio.

Safe tysyn thesis

Myth #2: Different types of adverse outcomes occur in characteristic ratios.

"The 1 : 10 : 30 : 600 relationships in the ratio would seem to indicate quite clearly how foolish it is to direct our total effort at the relatively few events terminating in serious or disabling injury when there are 630 property damage or no-loss incidents occurring that provide a much larger basis for more effective control of total accident losses."

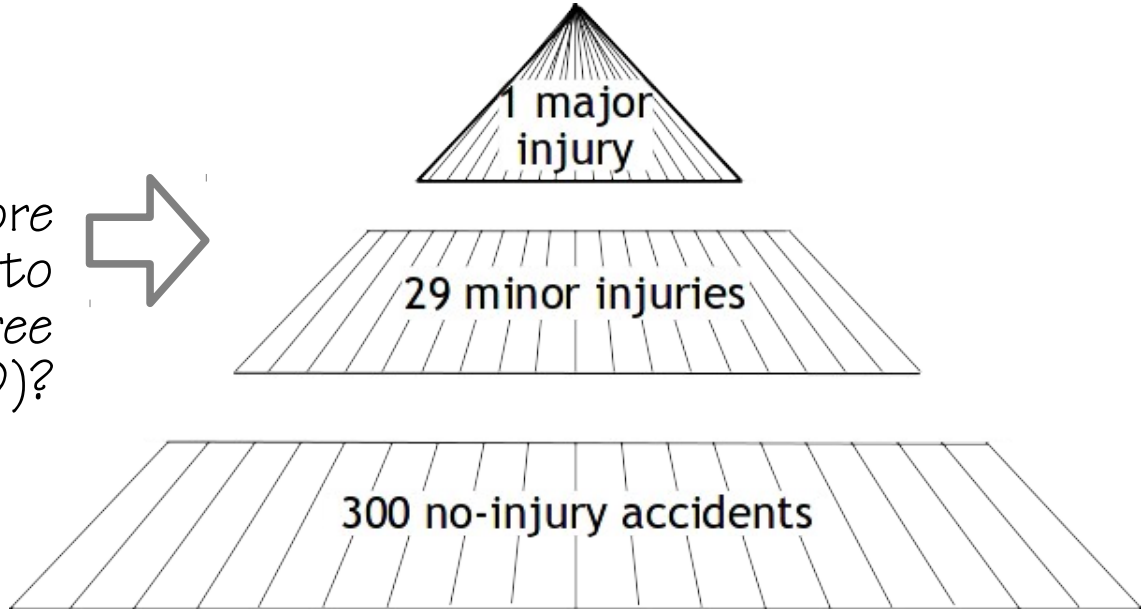


Source: Bird, F. (1974). Management guide to loss control. Atlanta, GA: Institute Press. analysis of 1 753 498 reported accidents, representing 21 different industrial groups.

Where does the pyramid come from?

The first version (1929) describes the "foundation of a major injury". It shows the relative occurrence of three types of outcomes. The text implies they happen in the same way, and that one therefore should study the no-injury events.

A later version (1959) is more ambiguous. But do the lines try to show perspective (3D), or three pieces of a pyramid (2D)?



What do we count? What is an accident?

Safe tysyn thesis

Events that involve serious injuries or significant damage to equipment or infrastructure > millions of DKR.

All reportable events (collisions, derailments, etc.) causing damage > $6,700 (2003); highway-rail crossing incidents and reportable incidents that cause a fatality or injury to any person, or occupational illness to a railroad employee.

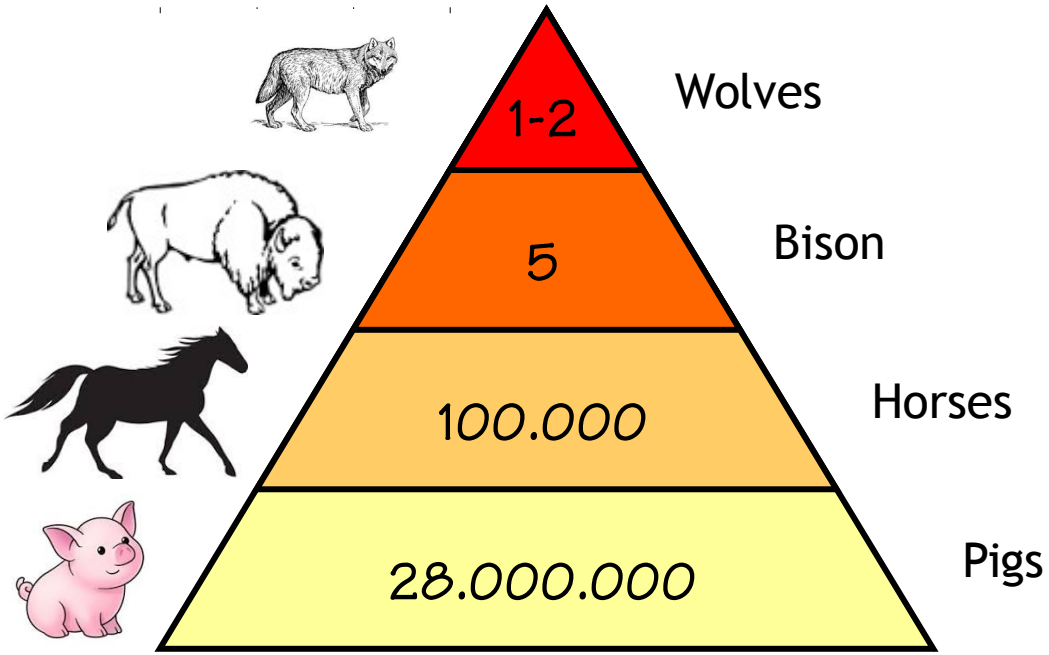
Something that either involves a loss of more than 500,000 Japanese yen, or causes a delay of more than 10 minutes to the first Shinkansen of the day.

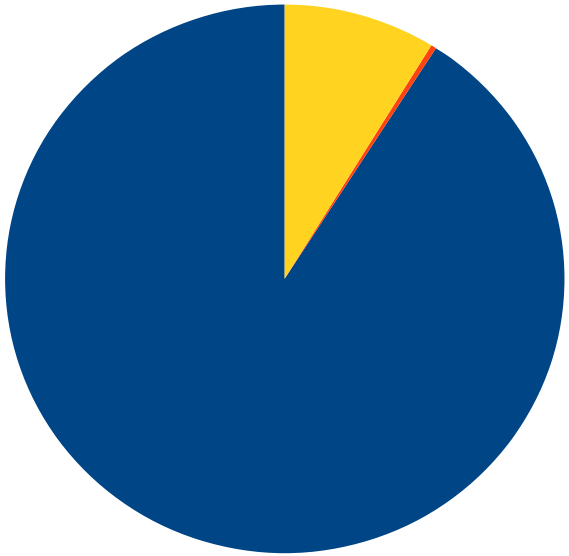
Events leading to loss of life, grievous harm to passengers, or serious damage to railway property > Rs. 2,500,000. Except 'cases of trespassers or of passengers run over and injured or killed through their own carelessness.'

Are all ratios or graphics meaningful?

Safe tysyn thesis

Approximate number of animals of different types in Denmark (2012).



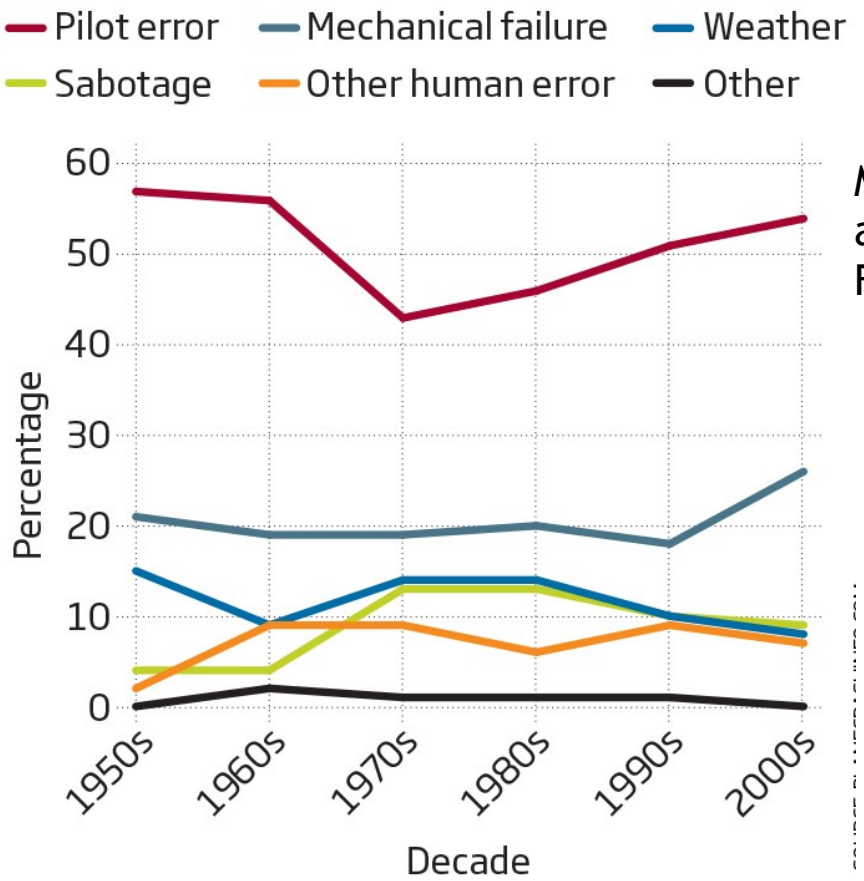


The Heinrich injury types
major: 1
minor: 29
no-injury: 300
as a pie chart.

"Human error": The 90% solution

Safe tysyn thesis

Myth #3: Human error is the major cause of accidents and incidents.



More than seventy percent of all crashes of scheduled aircraft are caused directly by 'controlled flight into terrain'. FAA (2001)

90.3%1 of crashes involved human error, such as risky driving behavior, inadvertent errors, and impaired states. (Foundation for Traffic Safety (2006)

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.

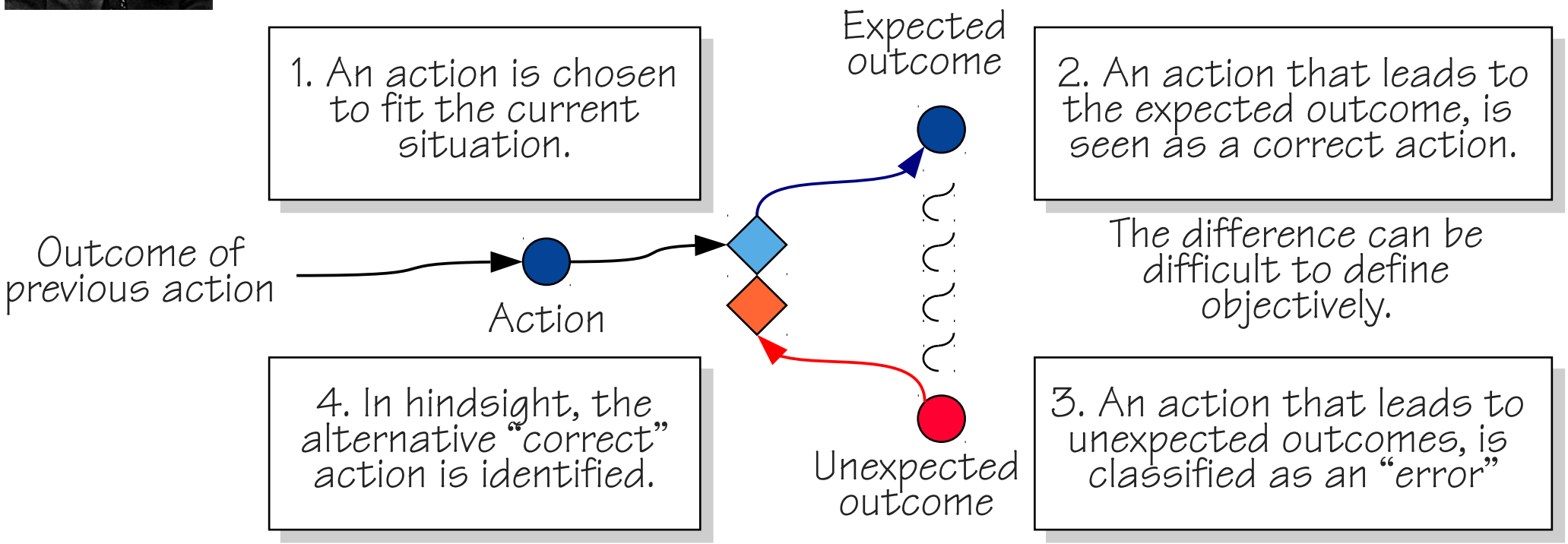
When something goes right, e.g., 9.999 events out of 10.000, are humans also responsible in 80-90% of the cases?

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

Investigation of successes is rarely undertaken.

Actions and "errors"

"Knowledge and error flow from the same mental sources, only success can tell one from the other."
(Ernst Mach, 1838-1916)



Performance adjustments are necessary

Availability of resources (time, manpower, materials, information, etc.) may be limited and uncertain.

People adjust what they do to match the situation.

Performance variability is inevitable, ubiquitous, and necessary.

Because of resource limitations, performance adjustments will always be approximate.

Performance variability is the reason why everyday work is safe and effective.

Performance variability is the reason why things sometimes go wrong.

Finding causes is a rational process.

Safe tysyn thesis

Myth #4: Accident investigation is a rational search for (root) causes

Investigations have practical limitations

Significant time and public (political) pressure for the more serious events.
Depth of analysis is limited by available resources and deadlines.
Range of available (traditional) methods is limited.
Looks for liabilities as well as causes.

"Twilight of the Idols"
Friedrich Wilhelm Nietzsche (1844-1900)

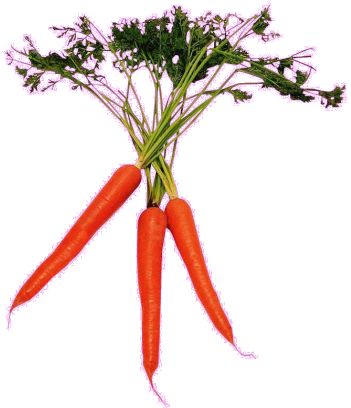
Investigations have psychological limitations

Danger, disquiet, anxiety attend the unknown – the first instinct is to eliminate these distressing states.
First principle: any explanation is better than none ... The cause creating drive is thus conditioned and excited by the feeling of fear.

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?

WYLFIWYF

Accident investigation follow a What-You-Look-For-Is-What-You-Find (WYLFIWYF) principle.

Accident investigations that look for causes, find causes. The assumptions about the nature of accidents (causality credo) constrain the analysis.

Human error
Technical malfunction
Organisational failure
Incorrect design

We can be safe – with a little more effort, a few more resources, a more refined set of recommendations from a knowledgeable inquiry, some new tools, an updated IT system, a better policy, and an improved safety culture.
In other words, WAD should be made more like WAI.

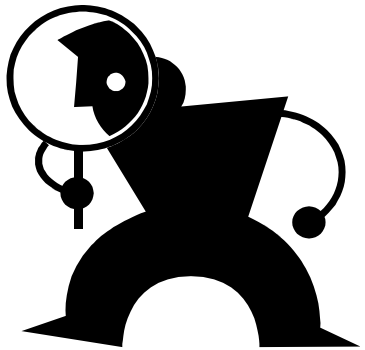
Bad maintenance
Safety culture
Latent conditions
Violation, non-compliance

The "logic" of causes

Safety synthesis

Determining the cause of an accident is a psychological (social) rather than logical (rational) process.

Causes are not found but constructed.



There are no true – or "root" – causes waiting to be detected

Causes are the outcome of a (tacit) social agreement, often based on tradition and common experience

Simple and non-negotiable standards

Safe tysyn thesis

Myth #5: Systems will be safe if people comply with procedures / standards.

"Zero Accident Mindset"

All accidents, injuries, and occupational risks are preventable.

"No repeats"

All adverse outcomes are investigated to find out what happened and why.

"Simple and non-negotiable standards"

Define and enforce a common, simple set of standards.

Work as imagined – work as done

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

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

Work-as-done (informal work) is what people have to do to get the job done. It is what actually happens.

Individuals and organisations must adjust what they do to the current conditions. Performance variability is necessary for things to work.

The need to "imagine" how others work

Safe tysyn thesis

Design (tools, roles, environment)

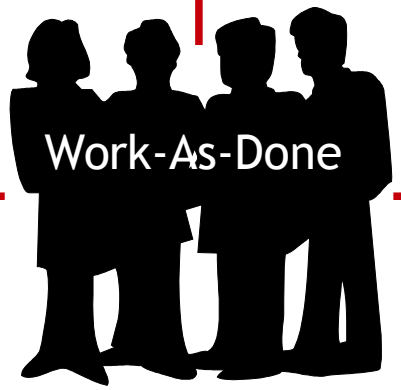
Work-As-Imagined

Work & production planning ("lean" - optimisation)

Work-As-Imagined

Safety management, investigations & auditing

Work-As-Imagined



When views collide …

WAI ≠ WAD

WAI ≠ WAD

Solution: Ensure that WAD matches WAI.

Tempting because WAI seems to be clear and well-defined, and it is easier to prescribe that WAD should be changed than to change WAI.

WAI ≠ WAD

Solution: Adjust WAI to be more like WAD.

Difficult because WAD appears to be unclear and difficult to grasp, because WAD is forever changing, and because it will threaten those in charge.

WAI ≠ WAD

Solution: Reconcile WAI and WAD.

To change WAI: Get information about WAD faster. Improve quality of information about WAD (Safety-II).

To change WAD: Encourage mindfulness. Make informal communication easier.

Five common myths rebutted

Safety synthesis

Myth #1: All accidents have causes which can be found and fixed.

Unwanted outcomes generally do not have special causes. Things that go wrong and things that go right happen in the same way.

Myth #2: Different types of adverse outcomes occur in characteristic ratios.

Assigning an outcome to a category is influenced by many different motives and interests. Ratios of outcomes are not meaningful and graphics can be misleading.

Myth #3: Human error is the major contribution to accidents and incidents.

'Human error' assumes that humans are just (fallible) machines and overlooks how performance adjustments are used to match the working conditions.

Myth #4: Accident investigation is a rational search for root causes

Accident investigation is a social process, where causes are constructed rather than found. The need to feel safe may dominate the need to be safe.

Myth #5: Systems will be safe if people comply with procedures / standards.

Actual working situations always differ from what the procedures assume. Strict compliance may therefore be detrimental to both safety and efficiency.

Same process ➡ different outcomes

Function (work as imagined)

Everyday work (performance variability)

Malfunction, non-compliance, error

Success (no adverse events)

Failure (accidents, incidents)

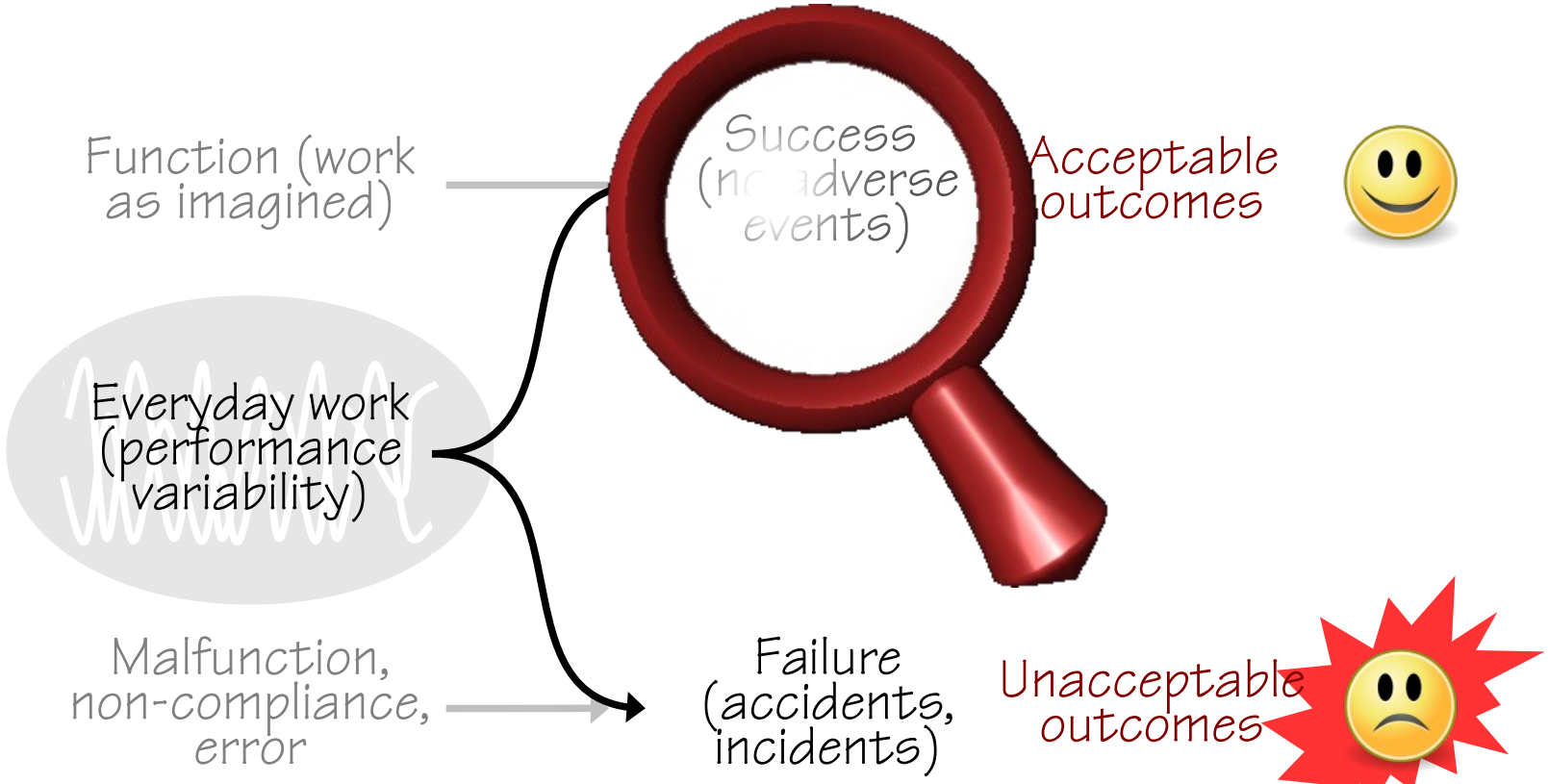
Acceptable outcomes

Unacceptable outcomes

Increase safety by facilitating work

Safe tysyn thesis

Understanding the variability of everyday performance is the basis for safety.



Constraining performance variability to remove failures will also remove successful everyday work.

Safety-I – when nothing goes wrong

Safety is the condition where the number of adverse outcomes (accidents / incidents / near misses) is as low as possible.

Safety-I is defined by its opposite – by the lack of safety (accidents, incidents, risks).

The premise for Safety-I is the need to understand why accidents happen.

Accidents and incidents are situations that, by definition, lack safety.

If we want something to increase, why do we use a proxy measure that decreases?

How can we improve safety by studying situations where there is NO safety?

Safety II – when everything goes right

Safety-II: Safety is a condition where the number of successful outcomes (meaning everyday work) is as high as possible. It is the ability to succeed under varying conditions.

Safety is defined by its presence.

If the level of safety increases, the proxy measure should also increase.

The premise for Safety-II is the need to understand everyday performance.

Safety can only be improved by studying situations where it is present!

Safety-II is achieved by trying to make sure that things go right, rather than by preventing them from going wrong.

Towards resilient safety management

Safety-I:
No “lack of safety”

Prevent, eliminate, constrain.
Safety, quality, etc. are different and require different measures and methods.

Safety-II:
Resilient safety management

Support, augment, facilitate.
Safety, quality, etc. are inseparable and need matching measures and methods.

Safe tysyn thesis

Thank you for your attention!

Any questions?