Safety-I and Safety-II:
From Protective to Productive Safety

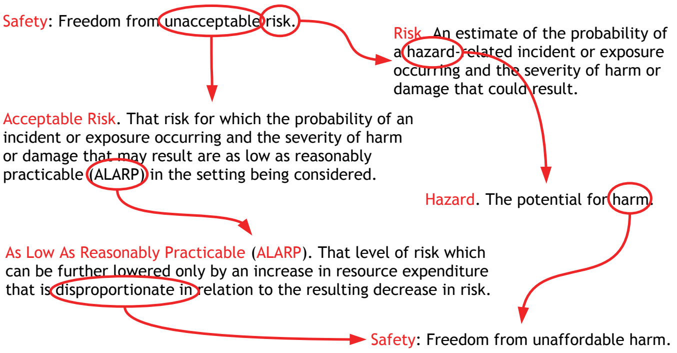
Erik Hollnagel

Professor
University of Southern Denmark

Chief Consultant
Center for Quality, RSD (DK)

hollnagel.erik@gmail.com

American National Standards Institute



Safety: Freedom from unacceptable risk.

Risk. An estimate of the probability of a hazard-related incident or exposure occurring and the severity of harm or damage that could result.

Acceptable Risk. That risk for which the probability of an incident or exposure occurring and the severity of harm or damage that may result are as low as reasonably practicable (ALARP) in the setting being considered.

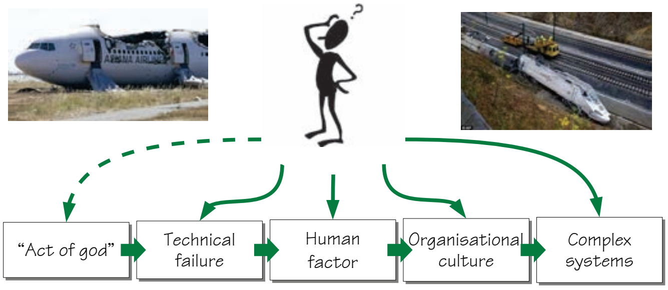
Hazard. The potential for harm.

As Low As Reasonably Practicable (ALARP). That level of risk which can be further lowered only by an increase in resource expenditure that is disproportionate in relation to the resulting decrease in risk.

Safety: Freedom from unaffordable harm.

Understanding a complicated world

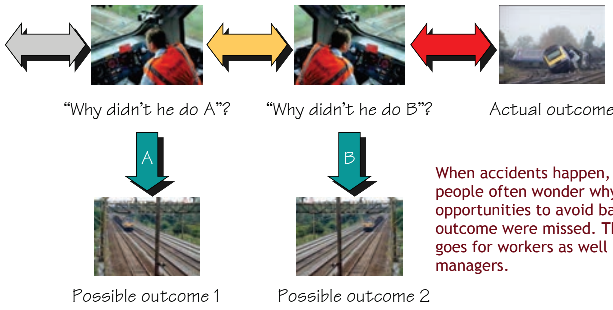
Accidents, incidents, breakdowns, disruptions,



The types of causes may change over time, but we still believe in causality

Counterfactual reasoning

Going back through a sequence, investigators often wonder why opportunities to avoid the bad outcome were missed. This, however, does not explain the failure



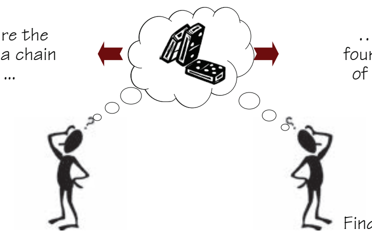
When accidents happen, people often wonder why opportunities to avoid bad outcome were missed. This goes for workers as well as managers.

Simple, linear model (cause-effect chain)

Simple linear models
(cause-effect chains)

If accidents are the
culmination of a chain
of events ...

… then risks can be
found as the probability
of component failures

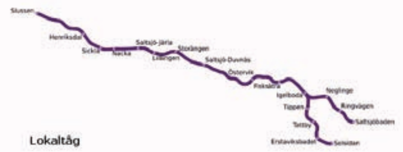


Find the component that
failed by reasoning backwards
from the final consequence.

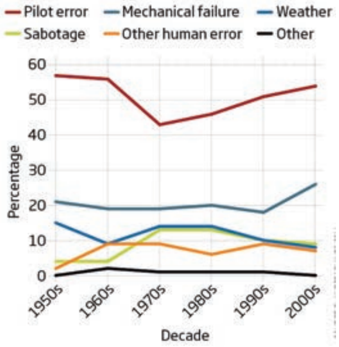
Find the probability that
something “breaks”, either
alone or by simple, logical
and fixed combinations.

Train crash, Saltsjöbanan (2013-01-15)

The last train of the day train arrived at the depot in Neglinge 01:45.
On-board was a train operator and a female cleaner.
It is known that the train left the depot at 02:23.
The female cleaner was on board
The train drove about 2.2 km to Saltsjöbaden, which is the last station on the line.
It was found that the train had been going at about 80 km/h, for the last 1.5 km.
Around 02:30 it came to the last stop but did not slow down. It drove straight through the buffer stop and ran into an apartment block about fifty meters away.
One of the train cars was suspended in mid-air.



Human error



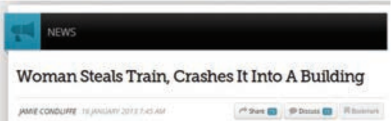
More than seventy percent of all crashes of scheduled aircraft are caused directly by ‘controlled flight into terrain’.
FAA (2001)

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

Woman steals train! (2013-01-15)

The 22-year old woman was found right behind the driver’s cabin with injuries to both legs, fractures of the pelvis, nine broken ribs, one punctured lung and a half torn ear. It took more than two hours to free her from the train wreckage, after which she was flown by helicopter to the Karolinska University Hospital in Stockholm. Here she was treated and was kept sedated for three days.

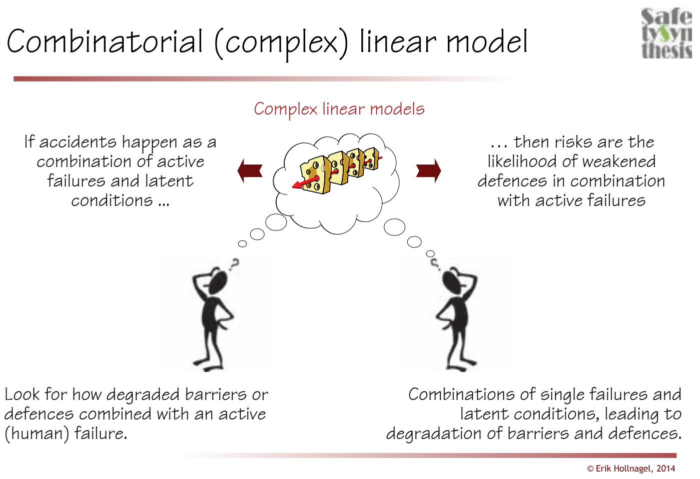
In the dead of night, a 20-year-old
cleaning lady stole a train in
Saltsjöbaden, for unknown reasons.
Running the train through two
stations at 50 mp.h., she lost control of
the train and it derailed.



NEWS

Woman Steals Train, Crashes It Into A Building

JAMIE CONDLIFFE 16 JANUARY 2013 7:45 AM



Combinatorial (complex) linear model

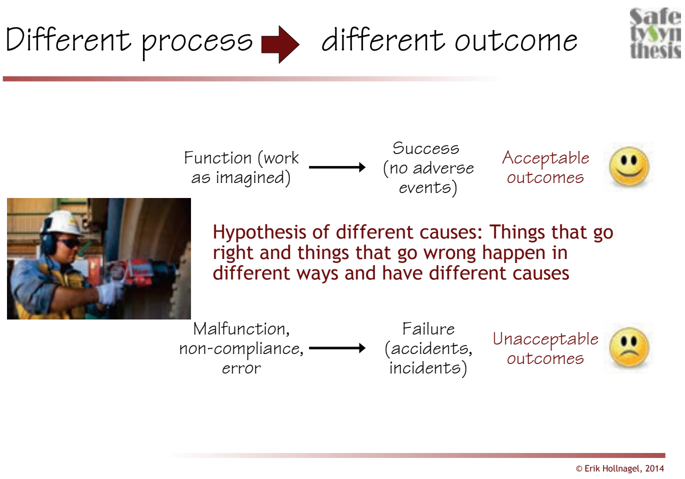
Complex linear models

If accidents happen as a combination of active failures and latent conditions ...

... then risks are the likelihood of weakened defences in combination with active failures

Look for how degraded barriers or defences combined with an active (human) failure.

Combinations of single failures and latent conditions, leading to degradation of barriers and defences.

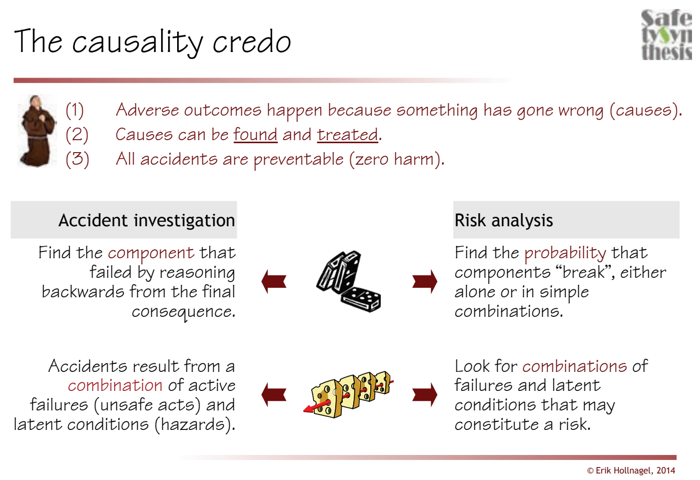


Different process → different outcome

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

Hypothesis of different causes: Things that go right and things that go wrong happen in different ways and have different causes

Malfunction, non-compliance, error → Failure (accidents, incidents) — Unacceptable outcomes



The causality credo

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

Accident investigation

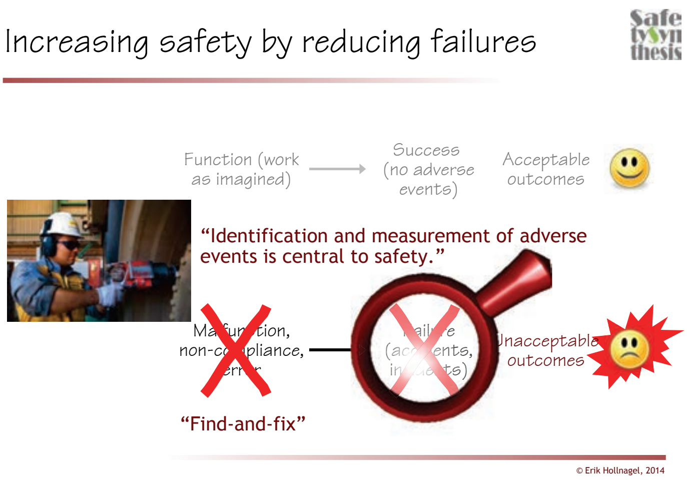
Find the component that failed by reasoning backwards from the final consequence.

Accidents result from a combination of active failures (unsafe acts) and latent conditions (hazards).

Risk analysis

Find the probability that components "break", either alone or in simple combinations.

Look for combinations of failures and latent conditions that may constitute a risk.



Increasing safety by reducing failures

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

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

Malfunction, non-compliance, error → Failure (accidents, incidents) — Unacceptable outcomes

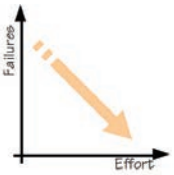
"Find-and-fix"

Safety-I – when nothing goes wrong

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

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

We focus on the events where safety is absent, rather on those where safety is present.



If we want something to INCREASE, why do we use a proxy measure that DECREASES?

Why is a HIGHER level of safety measured by a LOWER number of adverse outcomes?

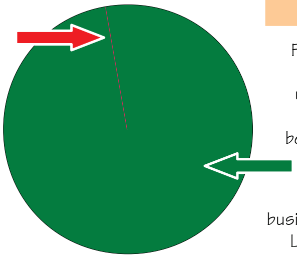
Why only look at what goes wrong?

Safety-I = 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-II = Ability to succeed under varying conditions.

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

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

Counting and understanding

The numerator is how many there are of a type of event (accidents, incidents, etc.) This number is known (with some uncertainty)

We always count the number of times something goes wrong. We analyse the rare events.

Numerator

Denominator

In 2011 there were a total of 490,007 movements in Frankfurt Airport, but only 10 infringements of separation and 11 runway incursions. The ratio was 2.04 10-5 and 2.25 10-5, respectively.

The denominator is how many cases something could have happened but did not. This number is usually disregarded and is mostly unknown.

We rarely count the number of times something goes right. We should try to understand the common events.

Noticing the unnoticeable

"Is there any point to which you would wish to draw my attention"?

"To the curious incident of the dog in the night-time."

"The dog did nothing in the night-time."

"That was the curious incident," remarked Sherlock Holmes.

It is necessary to know what is 'normal' – what usually happens or should happen – in order to notice and/or understand what is unusual.

Why don't people bump into each other?

When we move in a crowd, we continuously adjust to what other people do.

Just as others continuously adjust to what we do – or will do.

Why do people vary in their work?

CREATE & MAINTAIN

conditions that are necessary for doing the work.

AVOID

anything that may have negative consequences for yourself, your group, or organisation

COMPENSATE FOR

unacceptable conditions so that it becomes possible to do your work.

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.

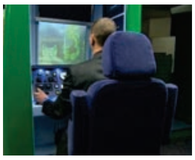
Because of resource limitations, performance adjustments will always be approximate.

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

🙁 Performance variability is the reason why things sometimes go wrong.

Work as imagined – work as done

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

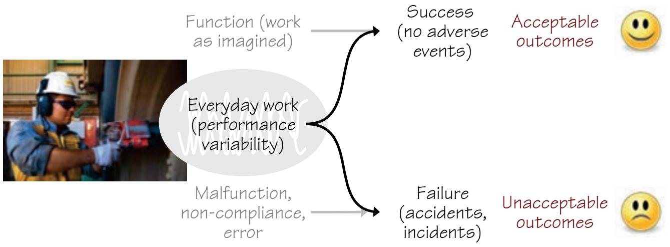


Safety I: Failure is explained as a breakdown or malfunctioning of a system and/or its components (non-compliance, violations).

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.

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

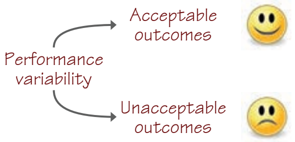
Safety II – when everything goes right

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

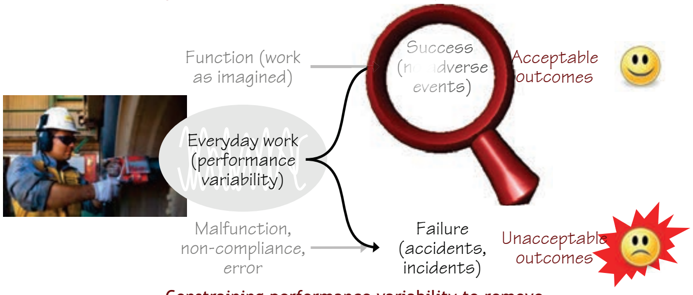
Safety is defined by its presence. ➡ The focus is on everyday situations where things go right – as they should.

Individuals and organisations must adjust everything they do to match the current conditions. Everyday performance must be variable in order for things to work.



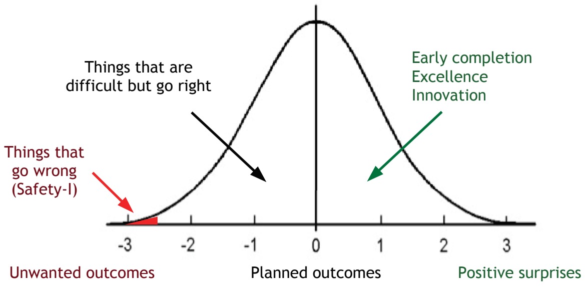
Increase safety by facilitating work

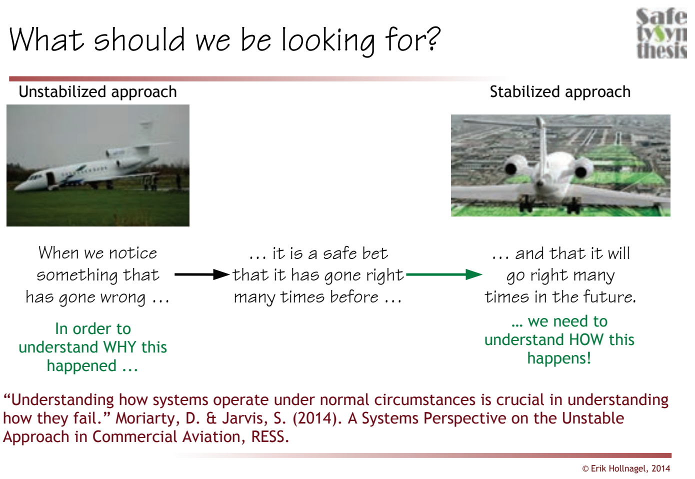
Understanding the variability of everyday performance is the basis for safety.


Function (work as imagined)
Everyday work (performance variability)
Malfunction, non-compliance, error
Success (no adverse events)
Failure (accidents, incidents)
Acceptable outcomes
Unacceptable outcomes

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

Safety-II: Focus on everyday work





What should we be looking for?

Unstabilized approach

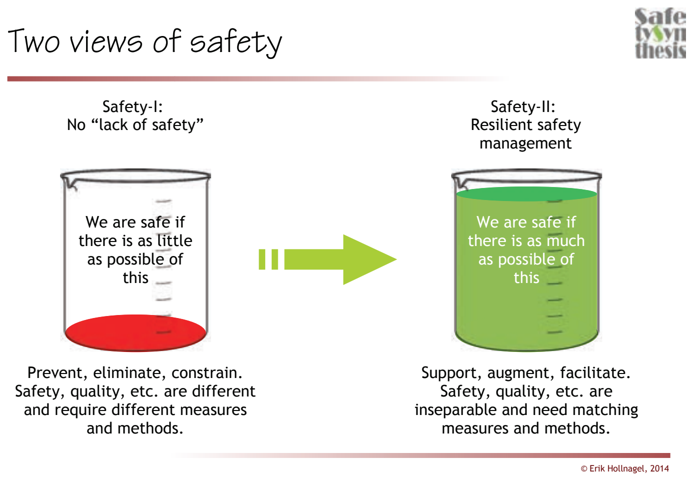
Stabilized approach

When we notice something that has gone wrong … → … it is a safe bet that it has gone right many times before … → … and that it will go right many times in the future.

In order to understand WHY this happened ...

… we need to understand HOW this happens!

“Understanding how systems operate under normal circumstances is crucial in understanding how they fail.” Moriarty, D. & Jarvis, S. (2014). A Systems Perspective on the Unstable Approach in Commercial Aviation, RESS.



Two views of safety

Safety-I:
No “lack of safety”

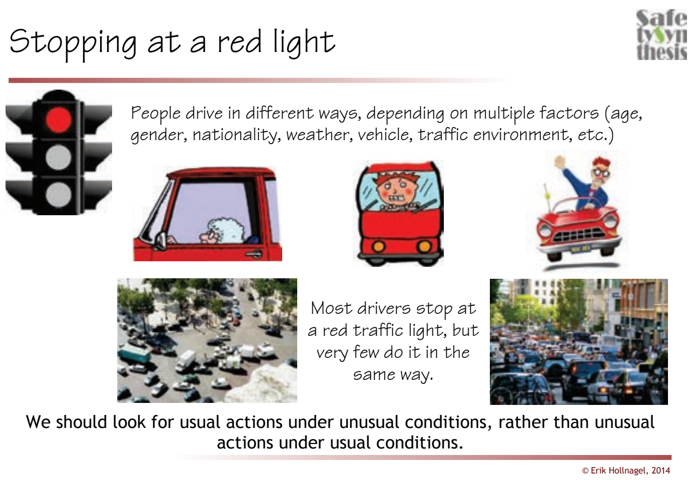
We are safe if there is as little as possible of this

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

Safety-II:
Resilient safety management

We are safe if there is as much as possible of this

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



Stopping at a red light

People drive in different ways, depending on multiple factors (age, gender, nationality, weather, vehicle, traffic environment, etc.)

Most drivers stop at a red traffic light, but very few do it in the same way.

We should look for usual actions under unusual conditions, rather than unusual actions under usual conditions.

Thank you for your attention

Any questions?