

# AN INTRODUCTION TO SAFETY-II

ERIK HOLLNAGEL, PROFESSOR, PH.D.  
SENIOR PROFESSOR, UNIVERSITY OF JÖNKÖPING (SWEDEN)  
VISITING PROFESSORIAL FELLOW, MACQUARIE UNIVERSITY, SYDNEY (AUSTRALIA)  
E-MAIL: [HOLLNAGEL.ERIK@GMAIL.COM](mailto:HOLLNAGEL.ERIK@GMAIL.COM)

# Safety first



It is the intention of **Safety First** to strive for continuous improvement to achieve excellence in the management of a safe and healthy environment for all workers and visitors to our premises and at workplaces where our workers are required to work that are not directly under our control.

## Mission Statement

To offer safe and effective care for our patients, as well as to provide a safe working environment for our staff.



An organization's safety policy is a recognized, written statement of its commitment to protect the health and safety of the employees, as well as the surrounding community.

[www.safeopedia.com](http://www.safeopedia.com)



# The problem is safety!



## 3. DEFINITIONS

3.20 **Safety.** Freedom from unacceptable risk.



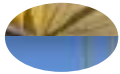
Safety is the activity of ensuring that accidents are avoided.

$$\text{Safety} = \sum_{i=1}^n \text{Accident}_i$$

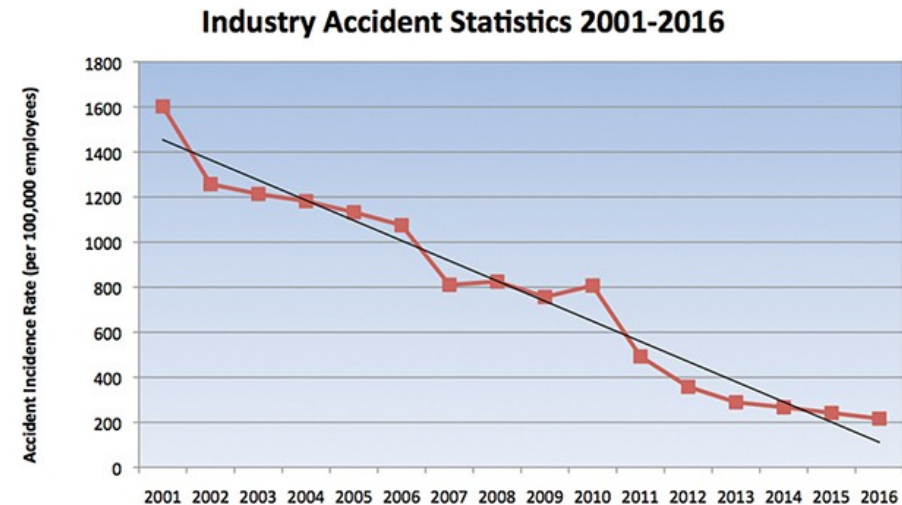
With Our Highest Level of  
OSH Expertise  
We Will Realize the Lowest Rate of  
Occupational Accidents



# How do we think about safety?



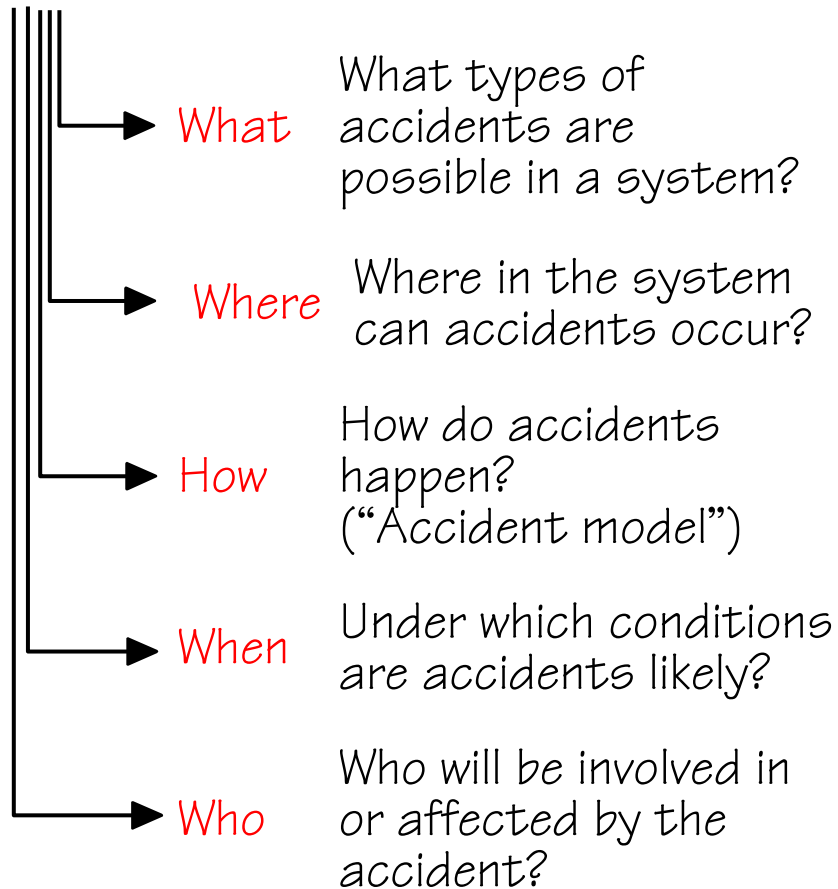
When we think about safety, we usually think about accidents - (low probability) events with adverse outcomes.



A system is therefore safe if as little as possible goes wrong.

# Safety through accident prevention

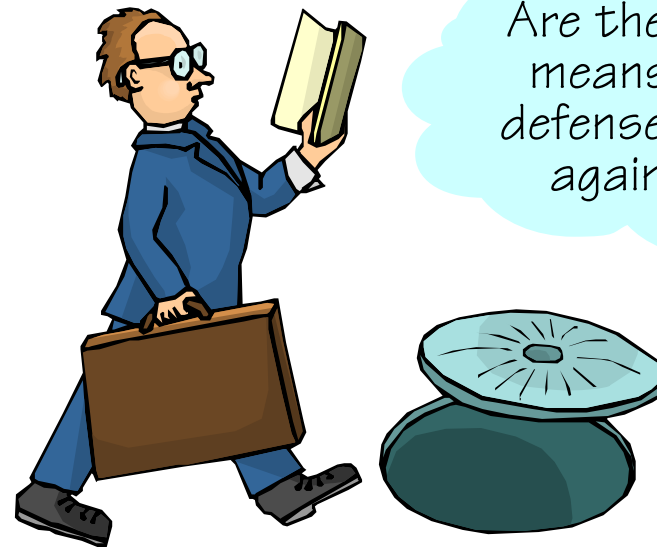
In order to be safe it is necessary to know:



How can accidents be described (accident model)?

Are there any known or valid indicators (early warnings)?

Are there effective means (barriers, defenses) to guard against them?





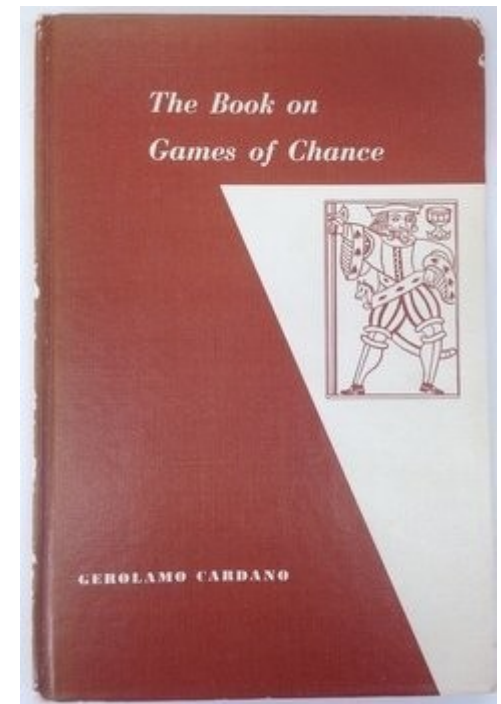
# A need to be safe and to feel safe ...

At first, whatever happened was attributed to higher powers (gods, nature)



“Act of god”

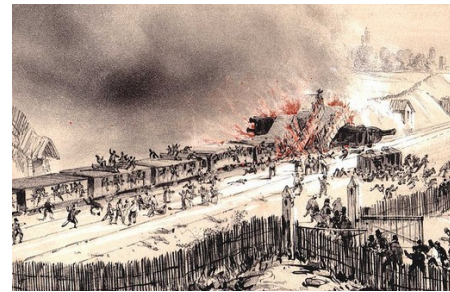
Solution: Pray



Liber de ludo aleae  
(Cardano, ca. 1564)

# A need to be safe and to feel safe ...

After the Enlightenment adverse outcomes were seen as caused - often by technological failures.



Meudon (F), May 8, 1849 (55 dead)



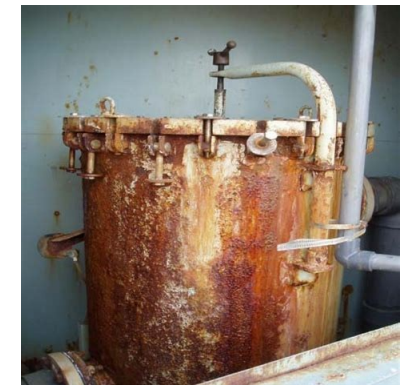
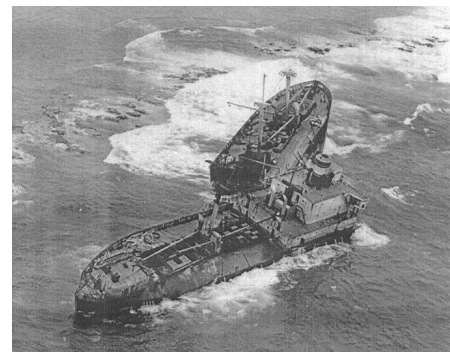
“Act of god”



Technical failure

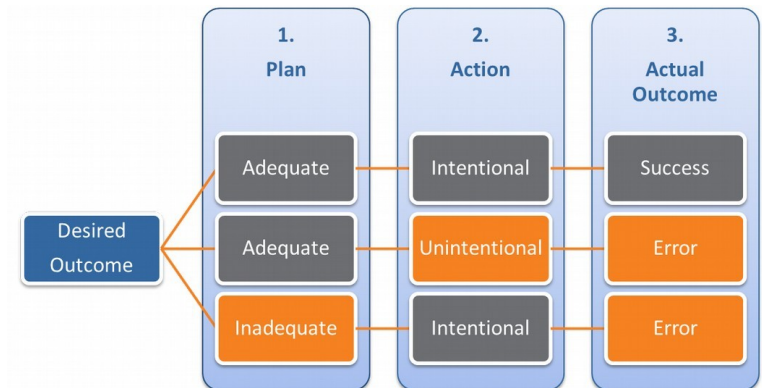
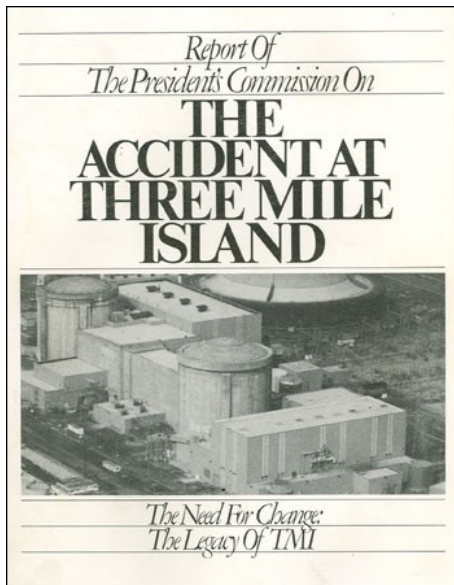
Solution: Pray

Solution: Repair



# A need to be safe and to feel safe ...

In the 1970s - especially after the TMI accident - accidents became linked to “human error” and human factors issues.

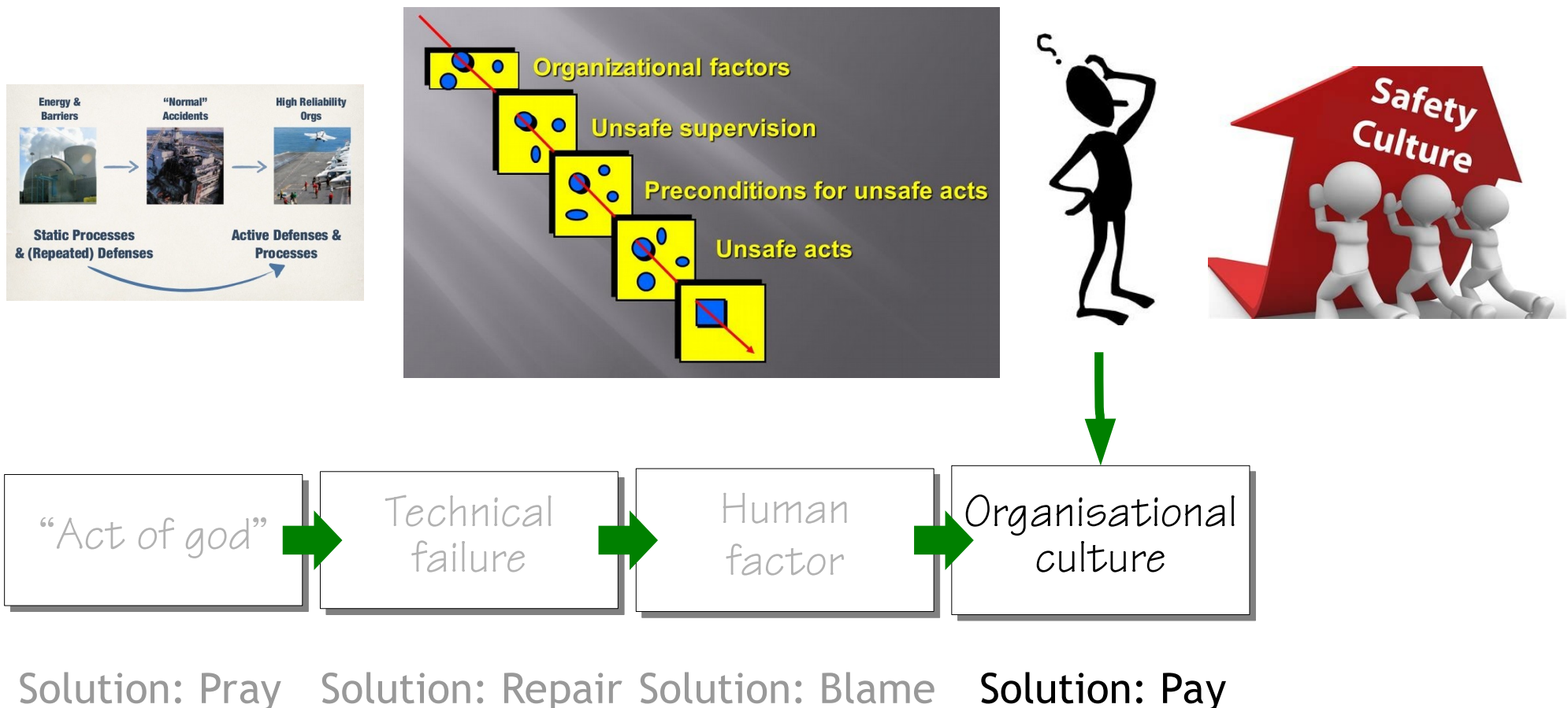


Solution: Pray    Solution: Repair    Solution: Blame



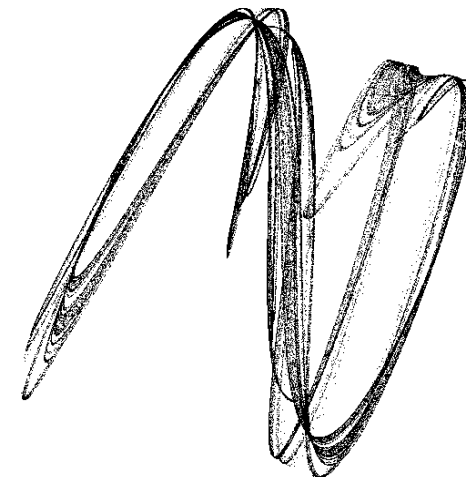
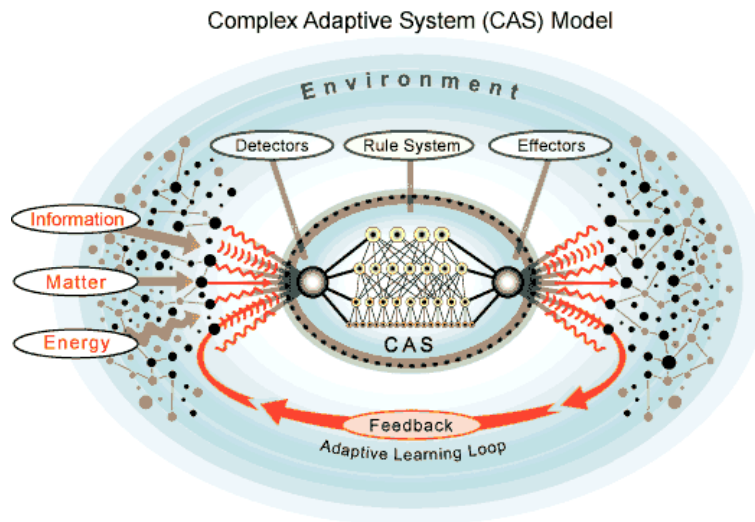
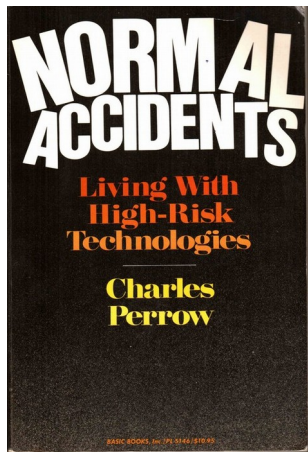
# A need to be safe and to feel safe ...

In the late 1980s - following Chernobyl and Challenger - the search for causes turned to organisations and culture.



# A need to be safe and to feel safe ...

The hope that innovative technology can fix problems that are only partly understood have resulted in unmanageable complexity.



Solution: Pray

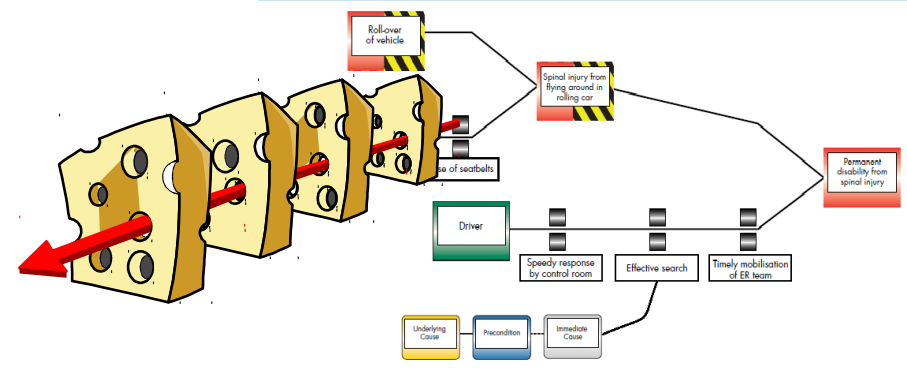
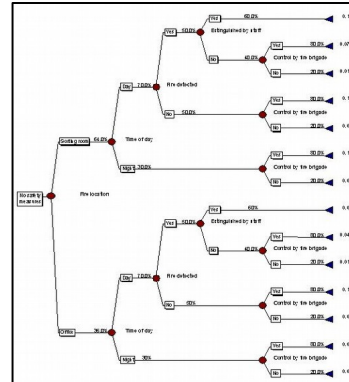
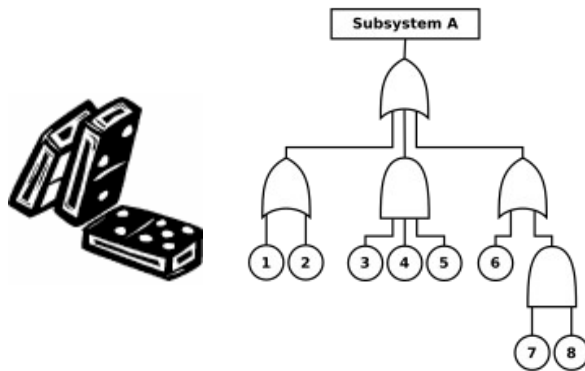
Solution: Repair

Solution: Blame

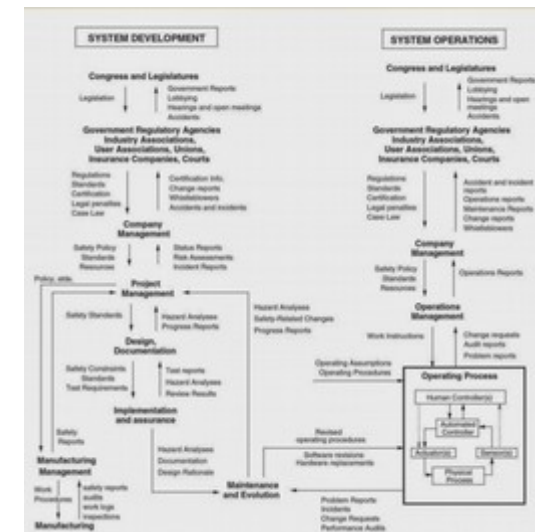
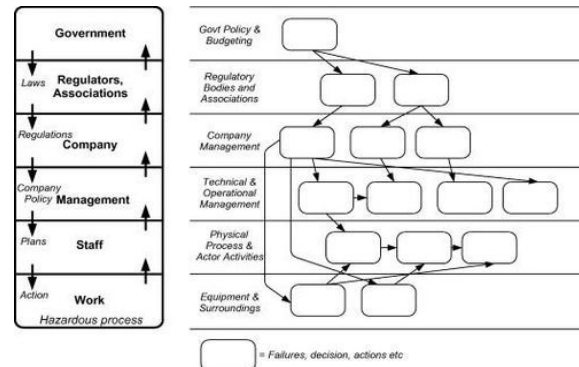
Solution: Pay

Solution: Pray

# A genealogy of accident models



We have many different ways of explaining how something can fail or malfunction.

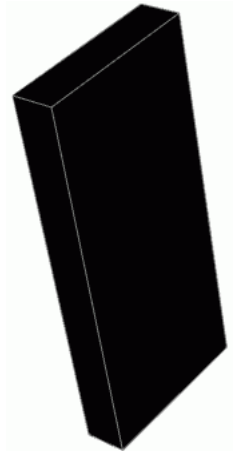


# Preference for monolithic explanations *SafetySynthesis*



Humans prefer monolithic explanations that refer to a single concept or factor. Such explanations are *efficient* (easily found and accepted) but lack in *thoroughness* and precision.

Monolithic explanations reinforce a linear, causal understanding of the world.



## Monolithic causes:

- Technical failures
- Human error
- (Lack of) safety culture
- Deviations from norms
- Brittleness

...

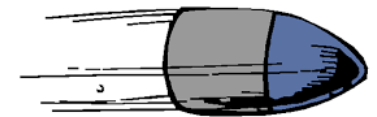


Captain Hindsight

## Monolithic solutions:

- Design, construction, maintenance
- Train, automate, redesign, simplify
- Improved safety culture
- Compliance
- Resilience

...

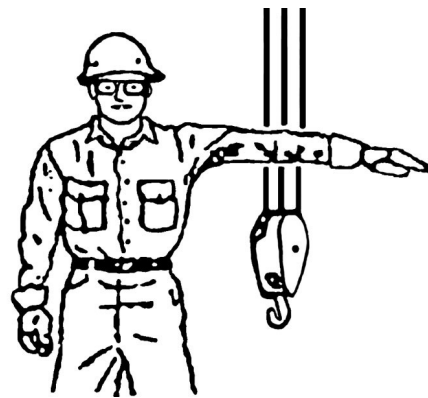


The Silver Bullet



# Different process ➡ different outcome *SafetySynthesis*

---



Normal function  
(everything works  
as imagined)



Success  
(no adverse  
events)

Acceptable  
outcomes



Things that go well and things that  
go wrong happen in different ways  
and have different causes

Malfunction,  
non-compliance,  
error

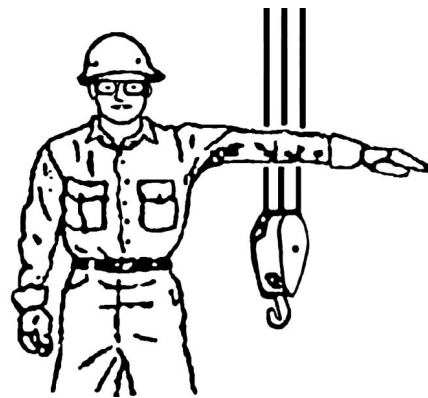


Failure  
(accidents,  
incidents)

Unacceptable  
outcomes



# 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)~~



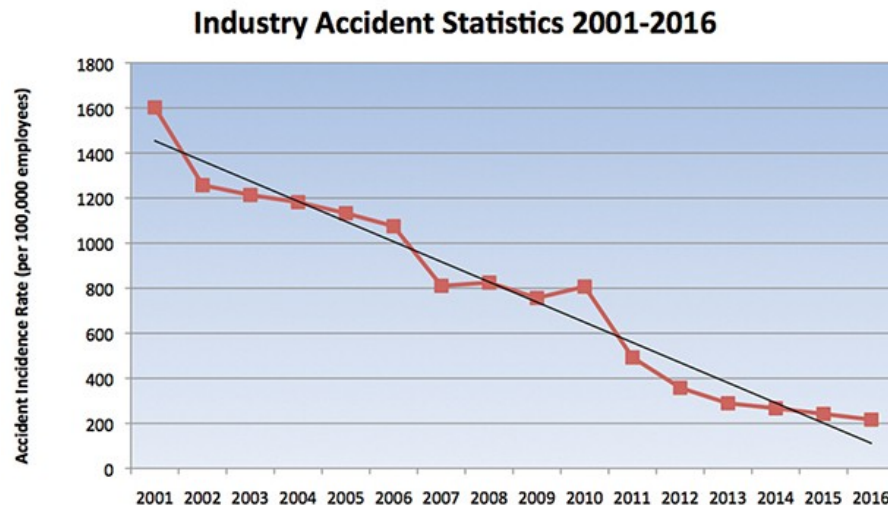
~~Unacceptable  
outcomes~~



**“Find, fix - and  
forget”**

# Safety-I – when nothing goes wrong

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



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

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

How can we improve safety by studying situations where there is a lack of safety?

---

## *Talk to your neighbour*



*Accidents actually rarely  
happen! But why does work  
usually go well?*



# The world from a Safety-I perspective

Accidents happen because ...

Components (HW/SW) will fail sooner or later.

Humans always make “errors” and always will.

There will always be unexpected and unrecognised situations.

Combinations of components can hide sneak faults and other flaws.

“Nothing” happens because

Systems are well designed and perfectly maintained.

People behave as they are expected to – as they are taught

Procedures are complete and correct.

Designers can anticipate and prepare for every contingency.

If nothing fails, then it will work.  
Therefore, try to make sure that nothing fails.  
To do so we must understand how and why something fails.

# The negativity bias

---

## Events

Accidents conflict with our expectations and intentions.

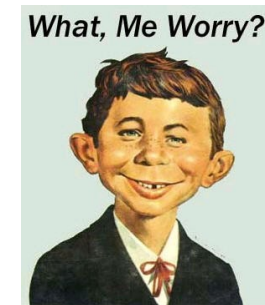


Accidents are evidence that our understanding is incomplete or deficient.

We therefore have to improve our understanding.

## Non-events

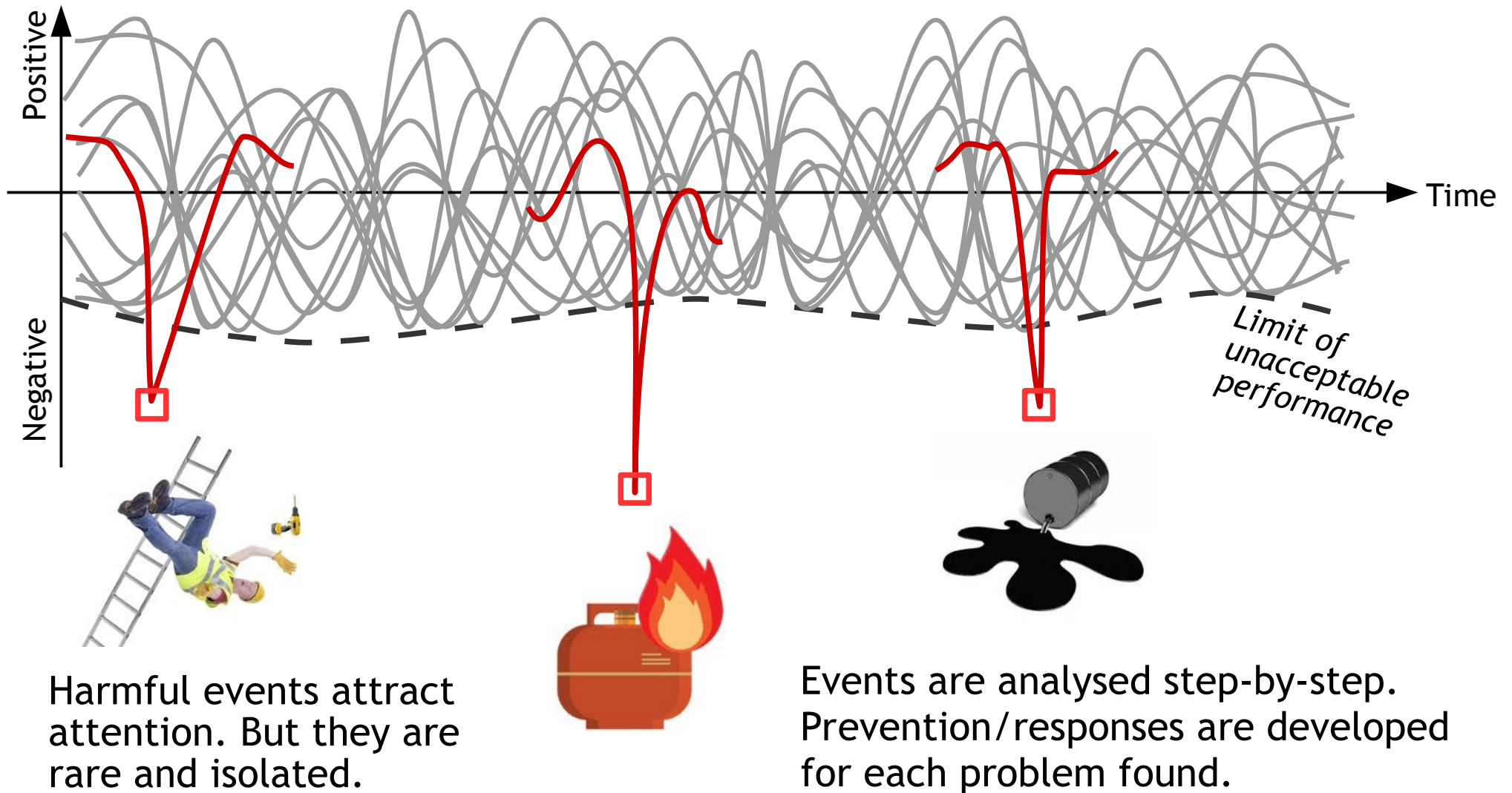
Acceptable outcomes agree with our expectations and intentions.



Acceptable outcomes are evidence that our understanding and actions are correct.

There is therefore no need to take a closer look.

# Safety is managed by snapshots



# The happy marriage?

---

Is it possible to understand what a happy marriage is by analysing and learning from divorces alone?



*\*Analogy suggested by Marit de Vos*



Is it possible to understand what safety is by analysing and learning from accidents and incidents alone?






# 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)

Numerator  
—————  
Denominator



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

$$\frac{1}{7,000,000}$$

$$\frac{1}{20,000}$$

$$\frac{1}{10}$$


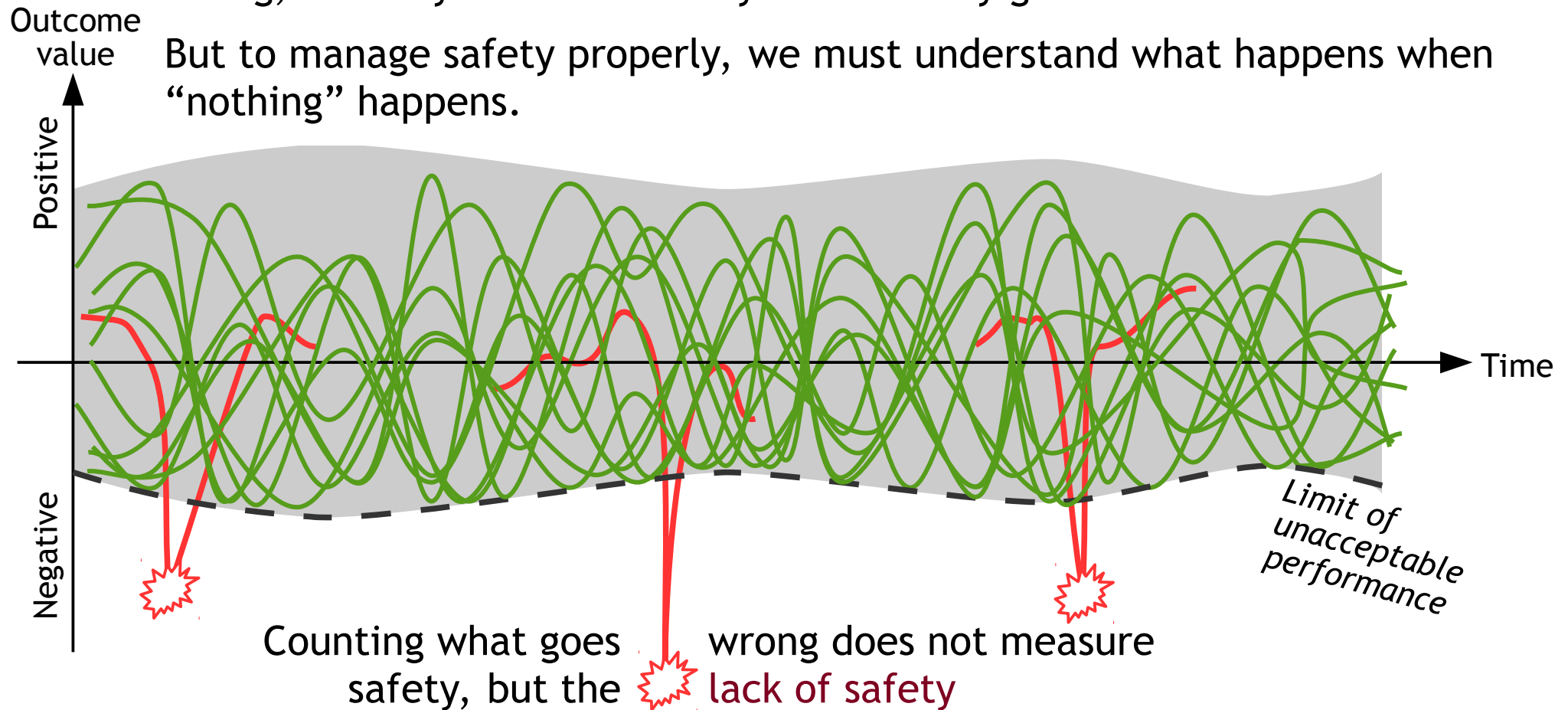
The denominator is how many cases something could have happened but did not. This number is usually disregarded and is mostly unknown.

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

# Do we really know why things go well?

The result of Safety-I is that we know a lot about why something can go wrong, but very little about why work usually goes well!

But to manage safety properly, we must understand what happens when “nothing” happens.



# The problem is NOT safety!

Safety is defined and measured more by its *absence* than by its presence.

Reason, J. (2000). Safety paradoxes and safety culture. Injury Control & Safety Promotion, 7(1), 3-14.



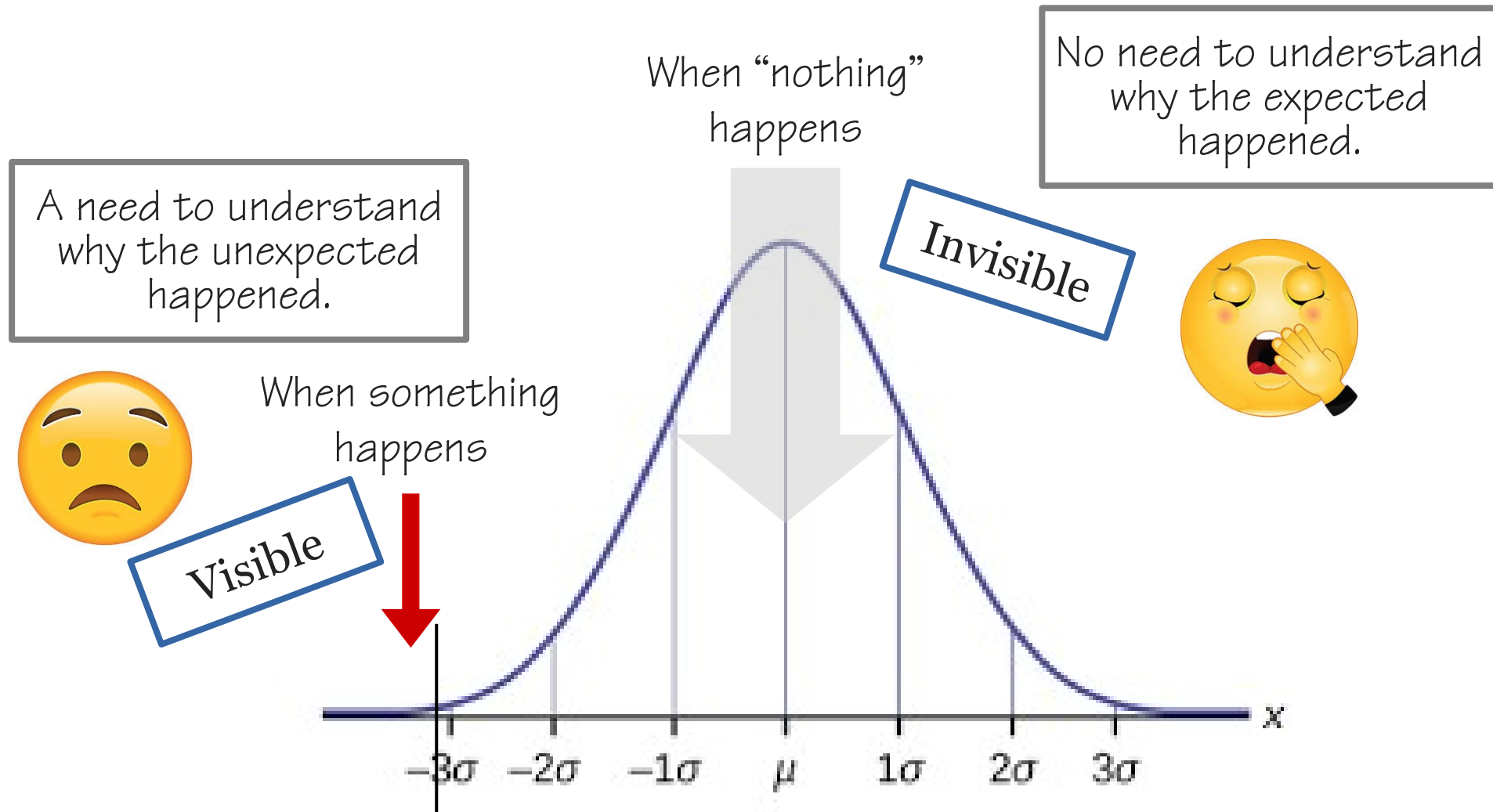
It is *invisible*: people often don't know how many mistakes they could have made but didn't ...

It is *invisible*: reliable outcomes are constant, which means there is nothing to pay attention to.

Reliability is a dynamic non-event ... it is an ongoing condition in which problems are momentarily under control due to compensating changes ... Weick, K. E. 1987.

Organizational culture as a source of high reliability. California Management Review 29 (2), 112-128.

# Explaining what happens and how





# Life is full of “dynamic non-events”

*Every day, from  
morning to night,*



*practically everything  
we do*



*works just as it  
should ...*



*... and we take it for  
granted*

# Performance adjustments are needed



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 why things usually go well.



**Same process -  
Different outcomes**



Performance variability is why things sometimes go wrong.



# Why do people make adjustments?



## AVOID

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

## COMPENSATE FOR

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

## CREATE & MAINTAIN

conditions that are necessary for doing the work.

# Efficiency-Thoroughness Trade-Off

The ETTO principle describes how people (and organisations) nearly always make a trade-off between the time and effort spent on doing something and the time and effort spent on preparing it.



**Efficiency:** Time to do  
Implementing plans.  
Executing actions.

**Thoroughness:** Time to think  
Recognising situation.  
Choosing and planning.



*Looks fine  
Not really important  
Normally OK, no need to check it  
We always do it this way  
Will be checked by someone else  
Has been checked by someone else  
This way is much quicker  
We can do this at a later time  
Can't remember how to do it  
It looks like 'X' - so it probably is X  
We must be ready in time  
Must not use too much of X  
We must get this done*

# The wet floor

A mill employee slipped and fell on a wet floor and fractured his kneecap. For more than six years it had been the practice to wet down too great an area of floor space at one time and to delay unnecessarily the process of wiping up.



Slipping on the part of one or more employees was a daily occurrence. The ratio of no-injury slips to the injury was 1,800 to 1.  
(Heinrich, 1931)





# Adjusting to information input overload *SafetySynthesis*

IT can generate unlimited amounts of data/information and present it in a bewildering variety of forms or modalities.

There are no 'natural' limitations on data push. A display is a window – a keyhole – into a limitless world.



Miller (1960)

Escape
Decentralise
Work in parallel
Cut categories
Filter
Queue
Reduce precision
Omit

Abandon the task; leave field of action

Distribute processing if possible; get assistance

Do two - or more - things at the same time; time sharing

Reduce the level of discrimination

Neglect to process certain categories; task shedding

Delay response during high load, in hope of a pause

Trade precision for speed and time; shallow reasoning

Temporary non-processing of information

# Hoegh Osaka



The Hoegh Osaka ran aground January 3, 2015 on its way from Southampton to Bremerhaven carrying high-end cars.

The 51,000-tonne vessel was “rounding West Bramble buoy in the Solent when it developed a significant starboard list, causing some cargo shift and consequent flooding”.

A “significant difference” between the actual and estimated cargo weight left it unstable and contributed to the accident, marine investigators found.

Given that stability had not previously given him cause for concern, *Hoegh Osaka*’s chief officer was content to follow what had become a routine practice for a ship to sail before its departure stability condition had been accurately calculated. [2.7]

Witness and anecdotal evidence suggests that the practice of not calculating the actual stability condition on completion of cargo operations but before the ship sails extends to the PCC/PCTC sector in general. For reasons of efficiency, what is a fundamental principle of seamanship appears to have been allowed to drift, giving rise to potential unsafe practices. [2.7.2]

Marine Accident Report

# FRA Approach Phraseology

“DLH123, Langen Radar identified, cleared OSMAX 25 Transition, high speed approved”

Standard phraseology  
(4.7 sec)



Time saved: about 1.7  
seconds



Non-standard phraseology  
(3.0 sec)

“Gude, DLH123, OSMAX 25 Transition, high speed”

There are about 14 transmissions per arrival – not including the time for readbacks.

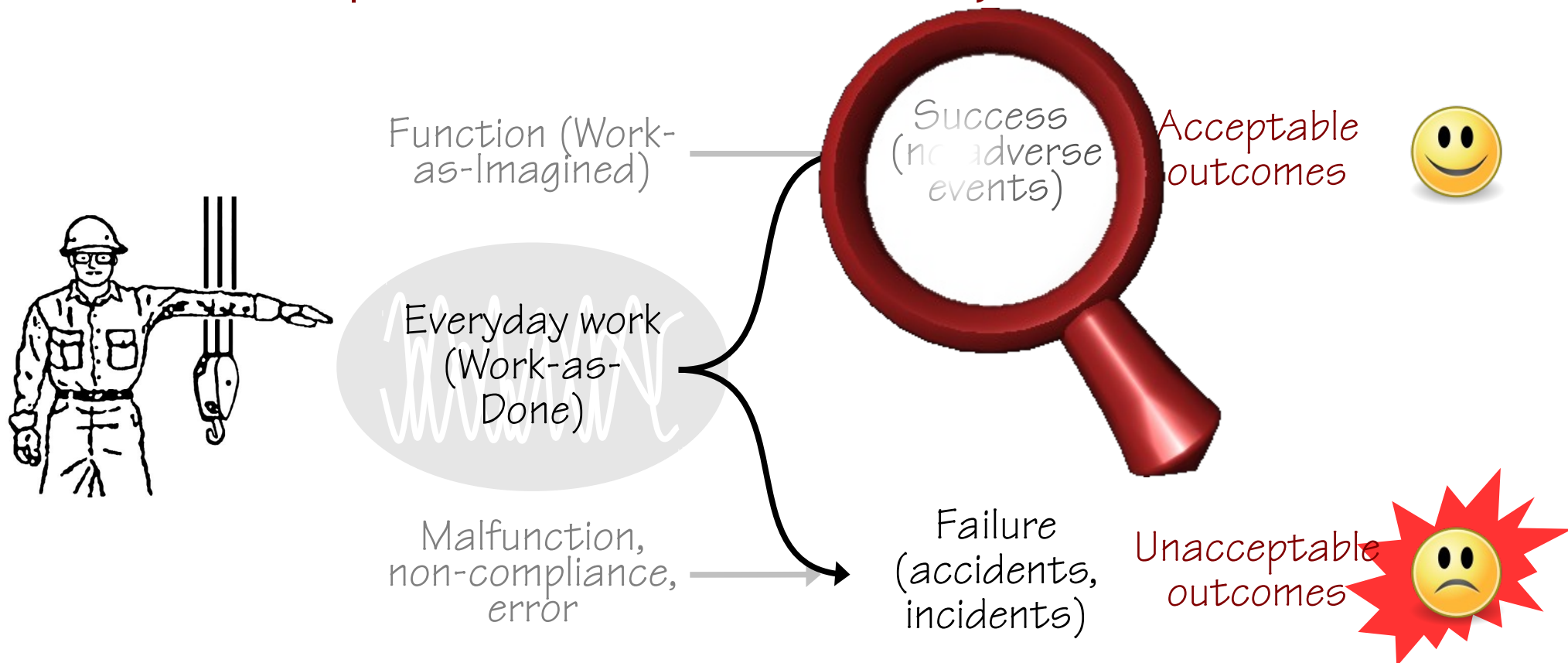


With 50 arrivals/hour this means more than 700 transmissions/hour on frequency.

Saving just 1 second per transmission corresponds to 11 minutes saved per hour.

# Same process ➡ different outcomes

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



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

# Safety II – when everything goes right *SafetySynthesis*

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.



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

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

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.



# The world from a Safety-II perspective *SafetySynthesis*

“Nothing” happens because

Humans find ways to overcome design flaws and hindrances.

Humans adjust their performance to match demands and conditions.

Humans interpret and apply procedures to match the situation.

Humans can intervene when things look like they will go wrong.

Accidents happen because ...

Humans find ways to overcome design flaws and hindrances.

Humans adjust their performance to match demands and conditions.

Humans interpret and apply procedures to match the situation.

Humans can intervene when things look like they will go wrong.

If all goes well, then it will work.  
Therefore, try to make sure that all goes well.  
This requires that we understand how things go well

---

## *Talk to your neighbour*



*What happens, when "nothing"  
happens.*

# How do “dynamic non-events” happen? *SafetySynthesis*



By responding in a flexible way



By monitoring what goes on



By learning what works and what doesn't



By anticipating  
- looking ahead

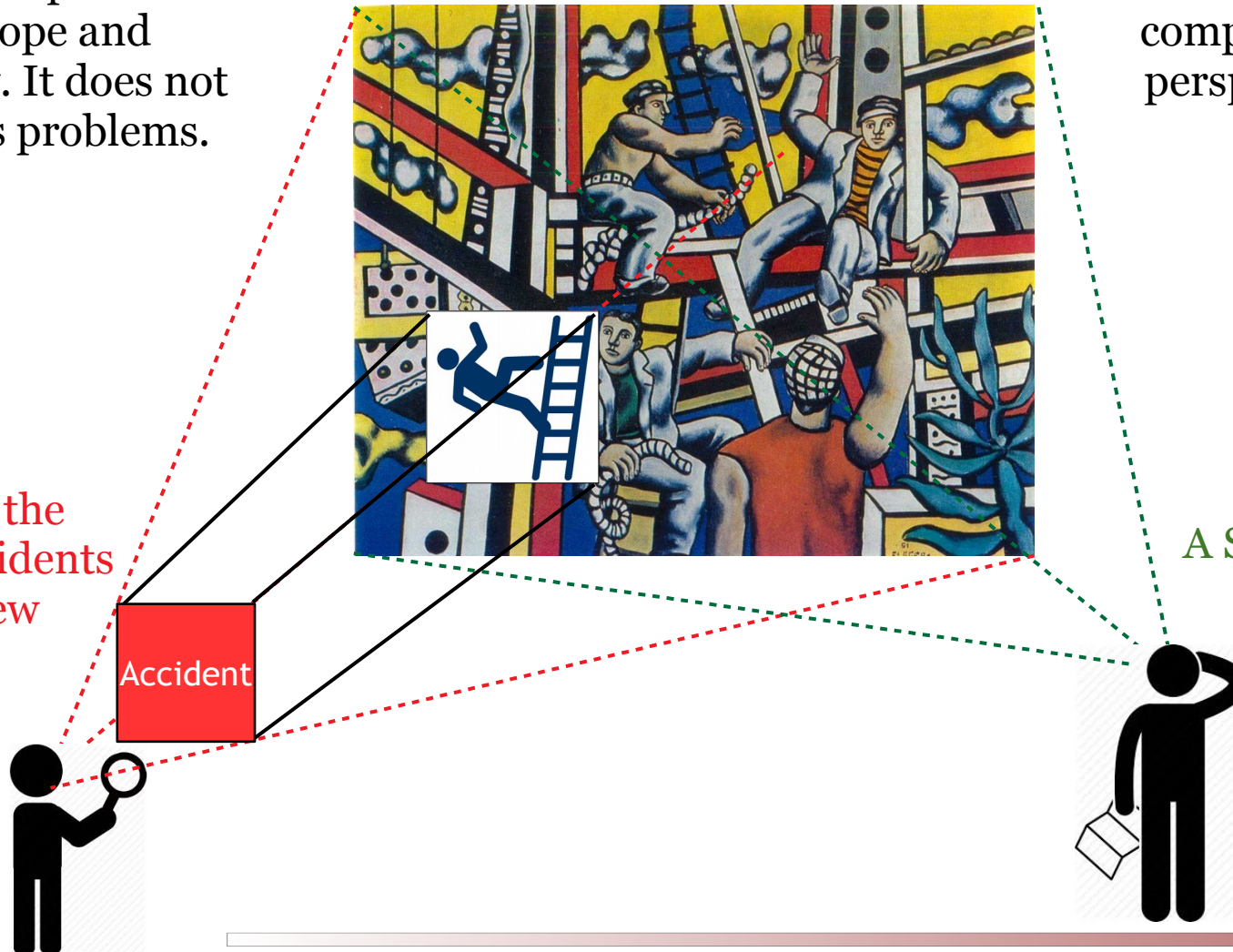




# A different perspective

A Safety-I perspective is limited in scope and applicability. It does not solve today's problems.

In a Safety-I perspective, the focus on accidents hinders a view of work that goes well.



A Safety-II perspective is a complement to a Safety-I perspective rather than a replacement.

A Safety-II perspective considers all outcomes and provides a better understanding of how things happen.

# Thank you for your attention



Any  
questions?