Resilience Engineering and FRAM Today

(June 7, 2012)

The FRAM book (finally) published.

www.functionalresonance.com has been established (and partly populated)

Resilience Engineering basics: “Safety-I and Safety-II”

Growing number of practical applications of the FRAM

FRAM issues / improvements

Clarification of method: "breadth before depth"

Practical advice on how to avoid becoming lost in detail.

Model-cum-method *versus* Method-sine-model

Mapping (interpreting) events onto pre-existing models versus developing a model of (the functions of) a system as a basis for analysis.

Principles of the FRAM

FRAM

I: The principle of approximate adjustments.

Work is always adjusted to match intractable and underspecified conditions. The adjustments are always approximate and contribute to the variability of work conditions.

II: The principle of equivalence of successes and failures.

The approximate performance adjustments are the reason why things go right, but also the reason why things go wrong.

III: The principle of emergence.

The variability of everyday performance is rarely large enough to count as a malfunction, but the variability from multiple functions may in combination lead to disproportionally large consequences. Both failures and everyday performance are emergent rather than resultant phenomena.

IV: The principle of functional resonance.

The variability of several functions may sometimes reinforce each other and the consequences may spread through tight couplings rather than cause-effect links. This can be described as a functional resonance of the everyday variability.

Functional Resonance Analysis Method

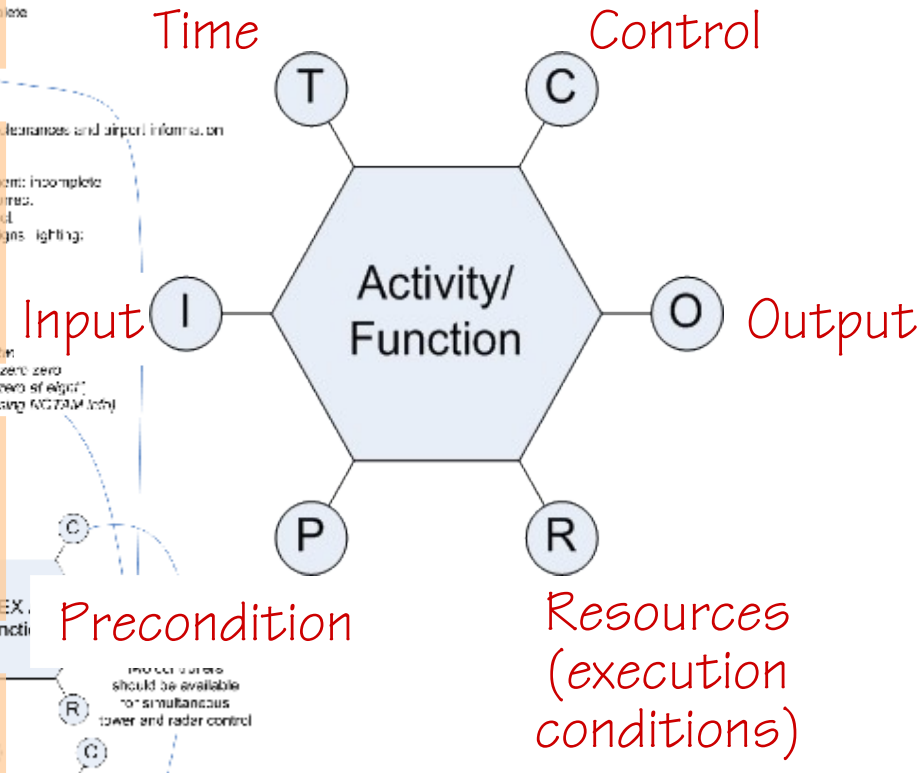
FRAM

The FRAM is a method for describing what happened or what may happen.

The description focuses on the functions needed for everyday performance to succeed, where each function is characterised by a number of aspects.

The FRAM model is developed iteratively, based on a breadth-before-depth approach.

The variability of functions is used to explain both how things go right and how they go wrong.



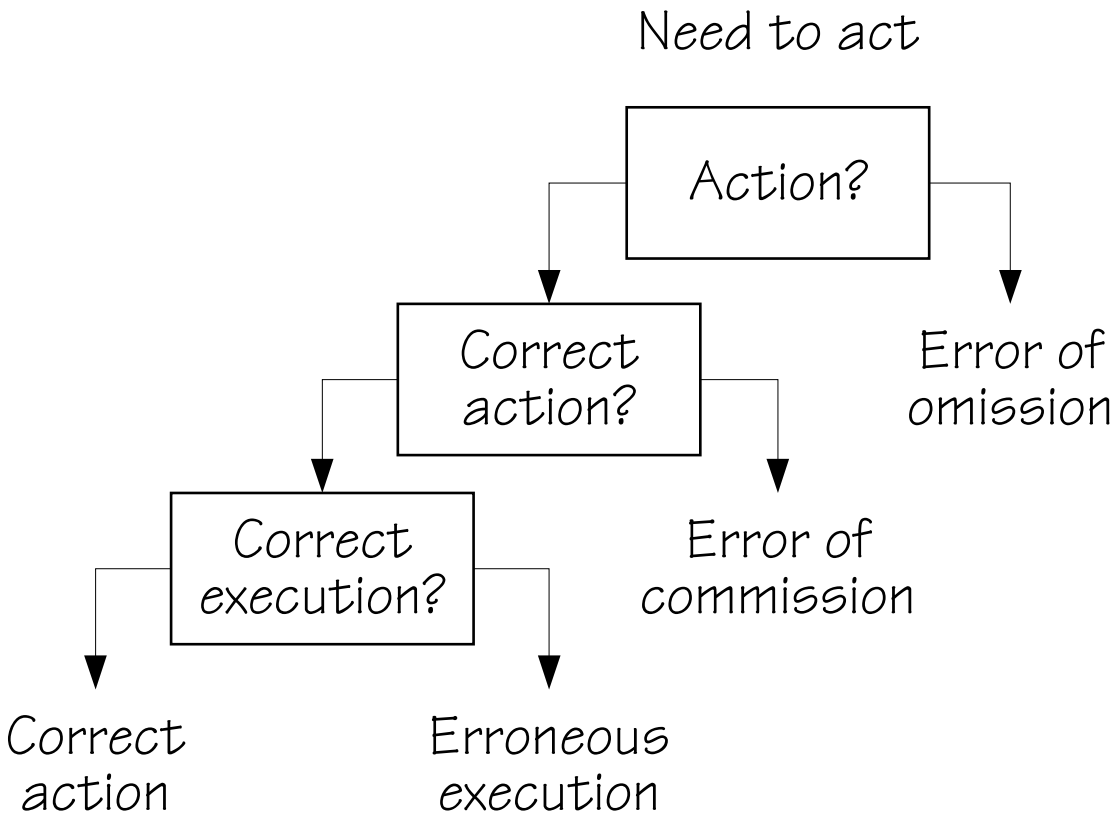
The FRAM book (finally) published.

www.functionalresonance.com has been established (and partly populated)

Resilience Engineering basics: “Safety-I and Safety-II”

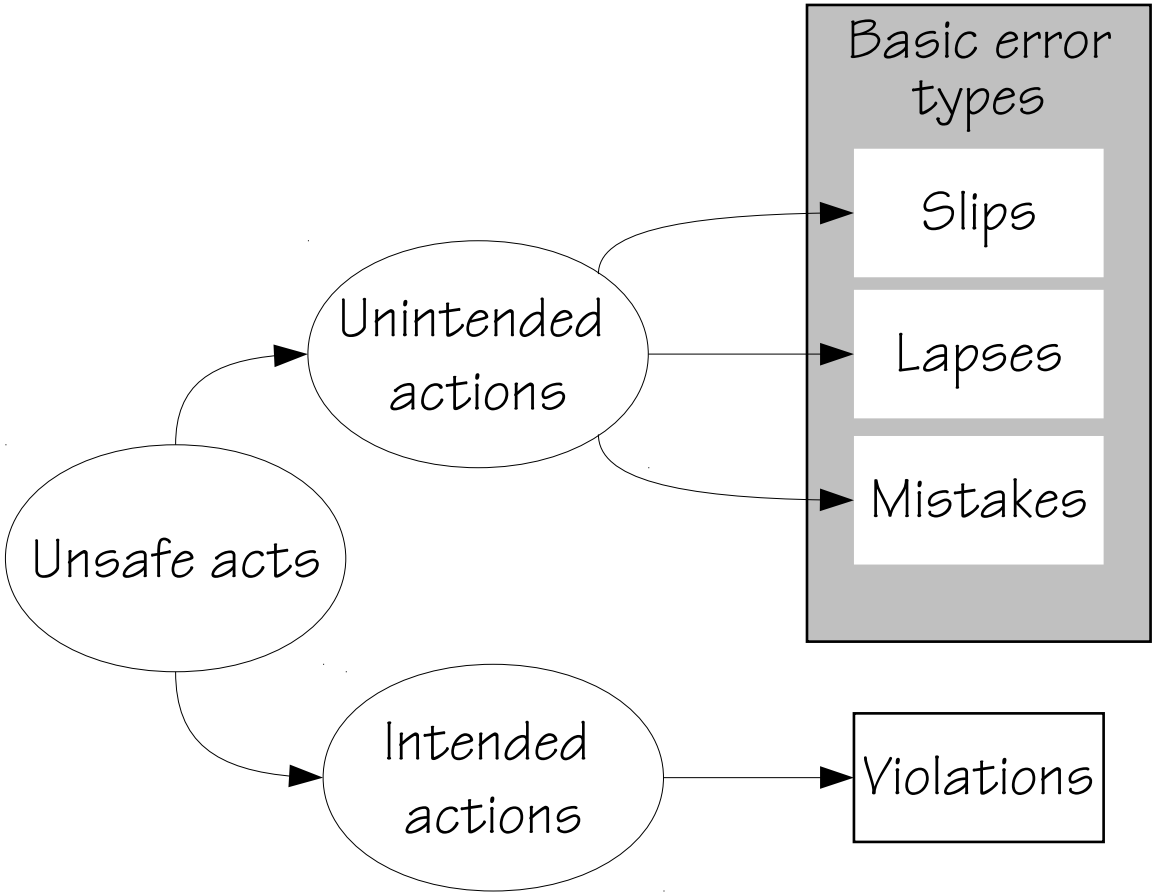
Growing number of practical applications of the FRAM

Simple human "error mechanism"

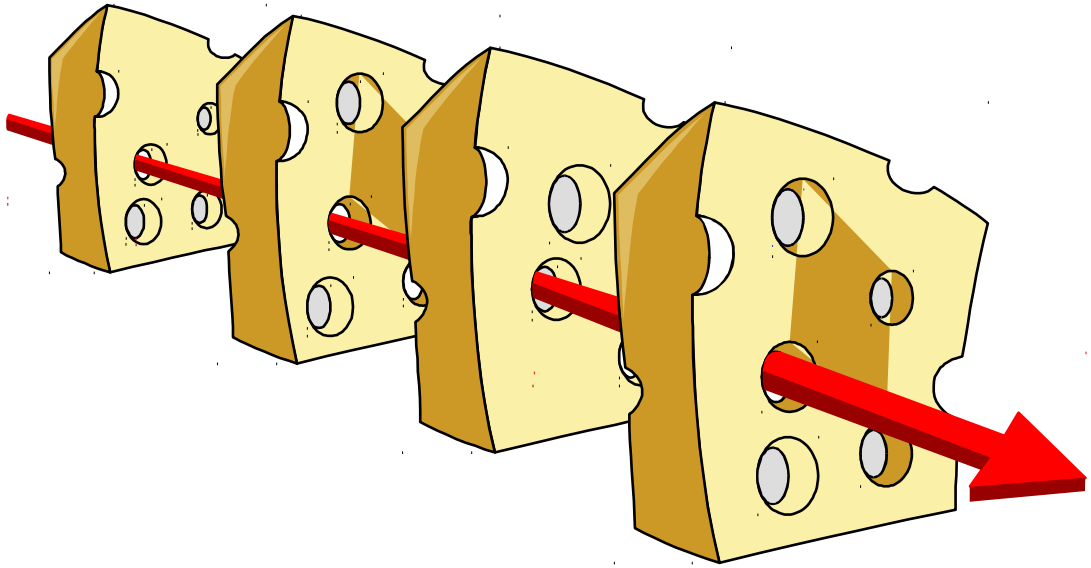


Complicated human "error mechanism"

FRAM

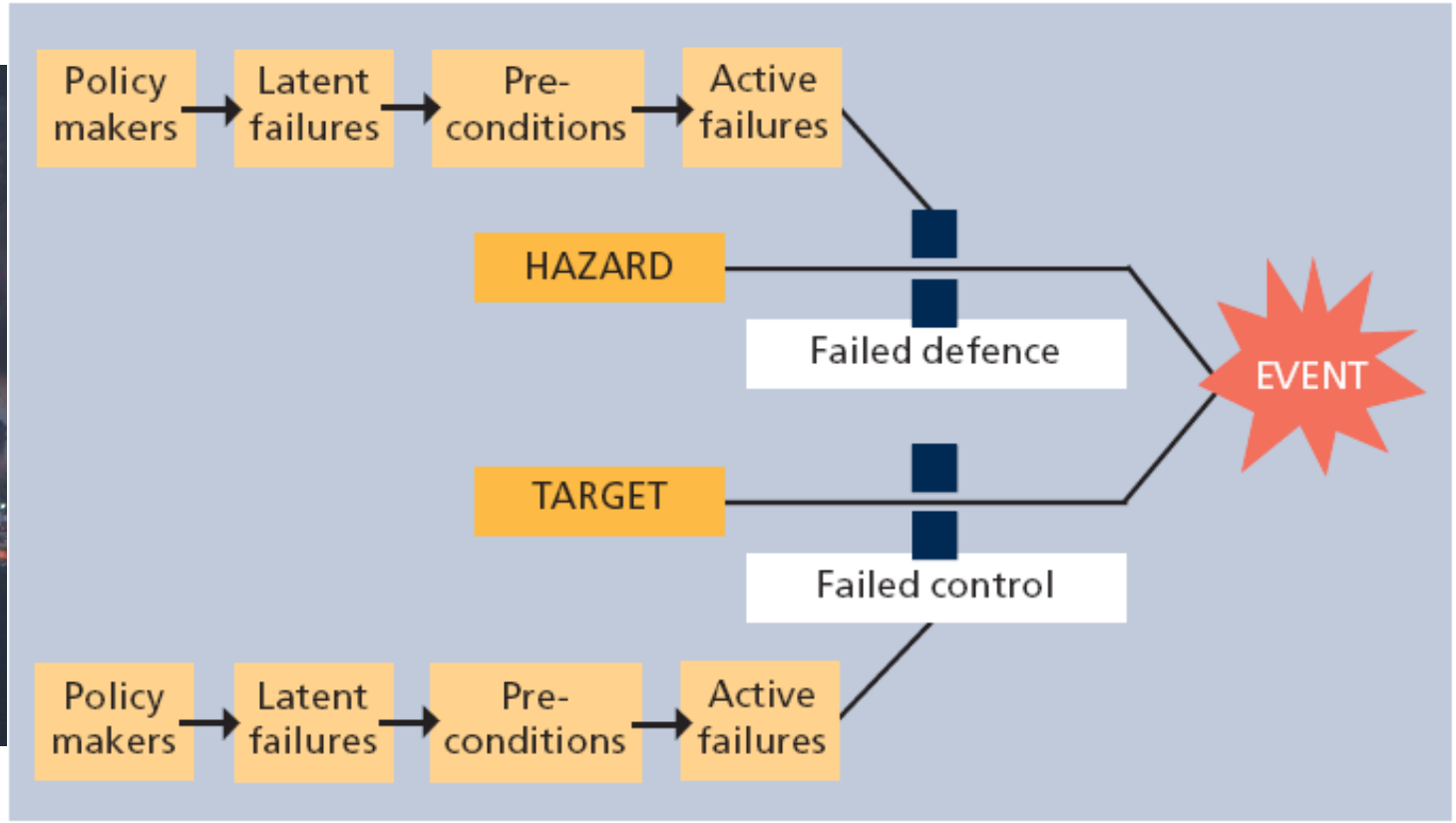


"Swiss cheese" model



TRIPOD: active + latent failures

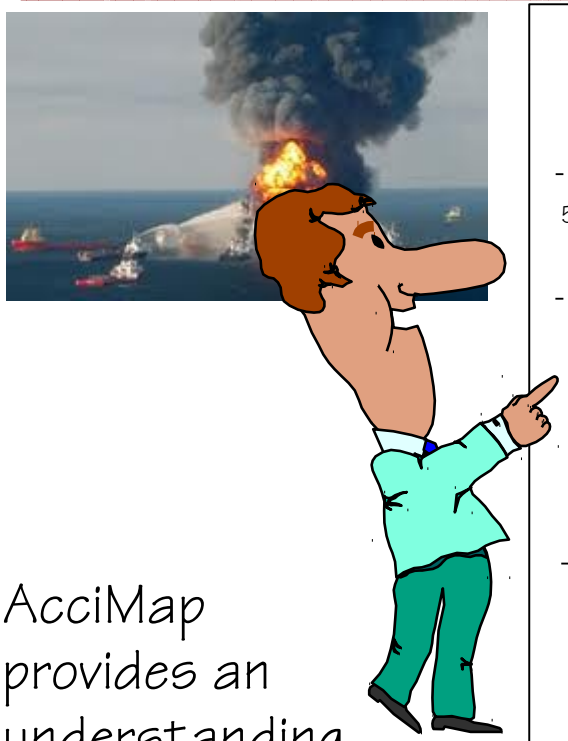
FRAM



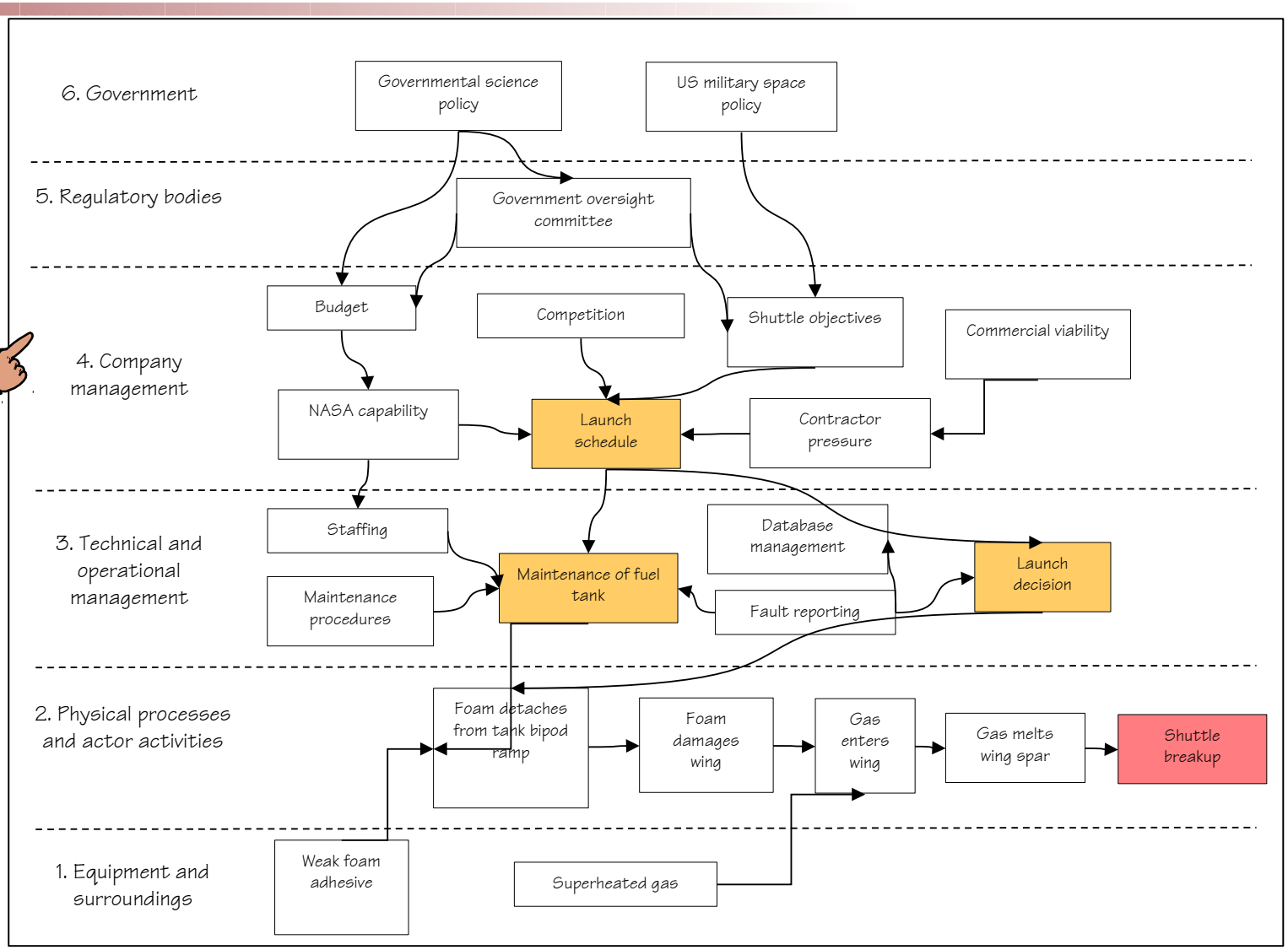
In TRIPOD, risks are associated with the failure of individual "components", that combine linearly.

AcciMap

FRAM

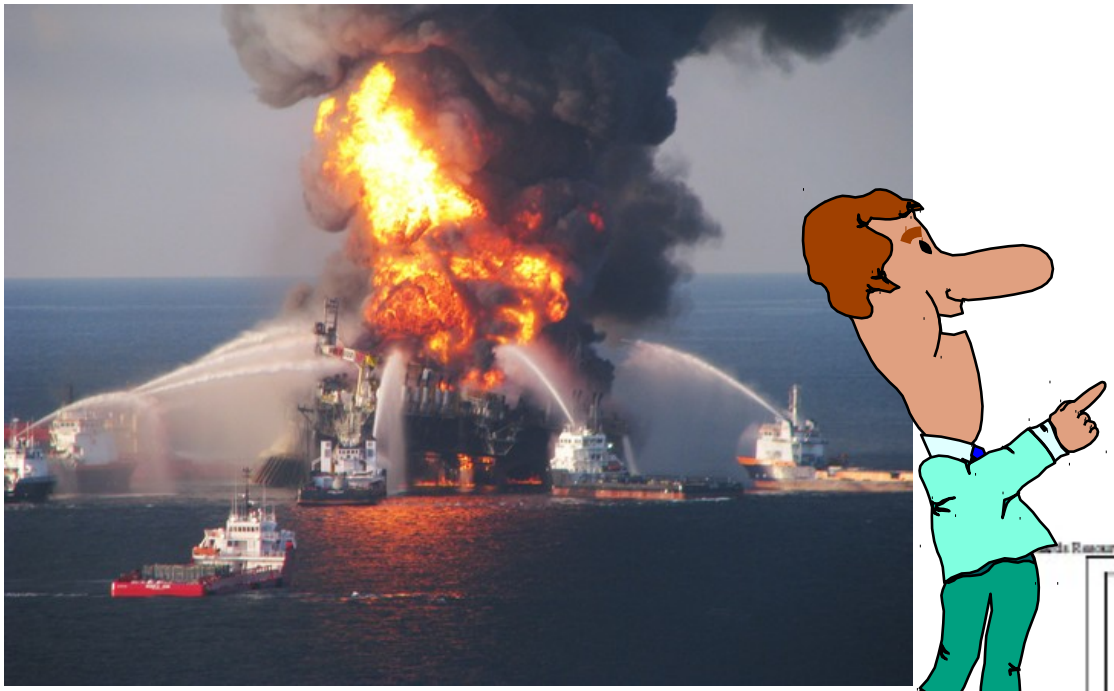


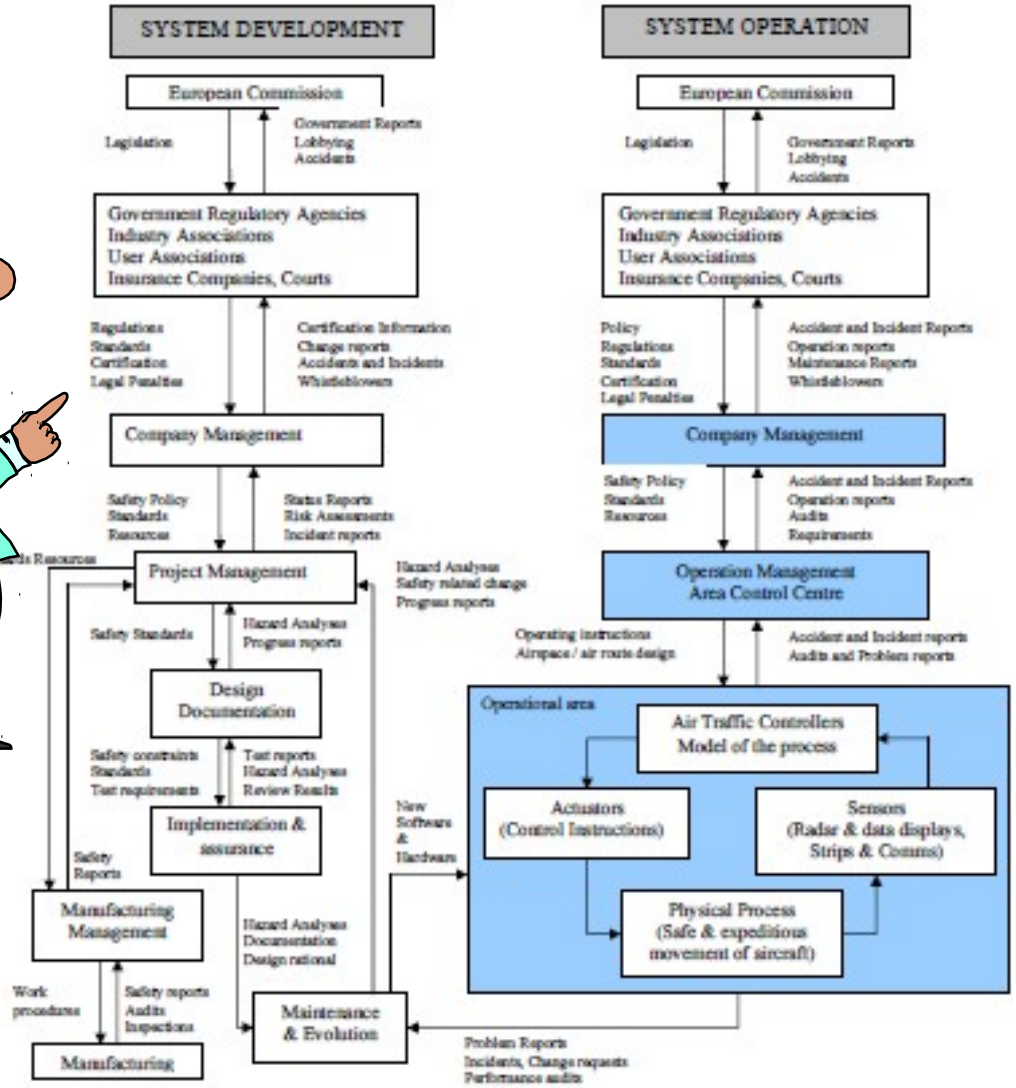
AcciMap provides an understanding of the context. Possible causes are mapped onto six levels to explain the accident.



STAMP: Inadequate control

FRAM

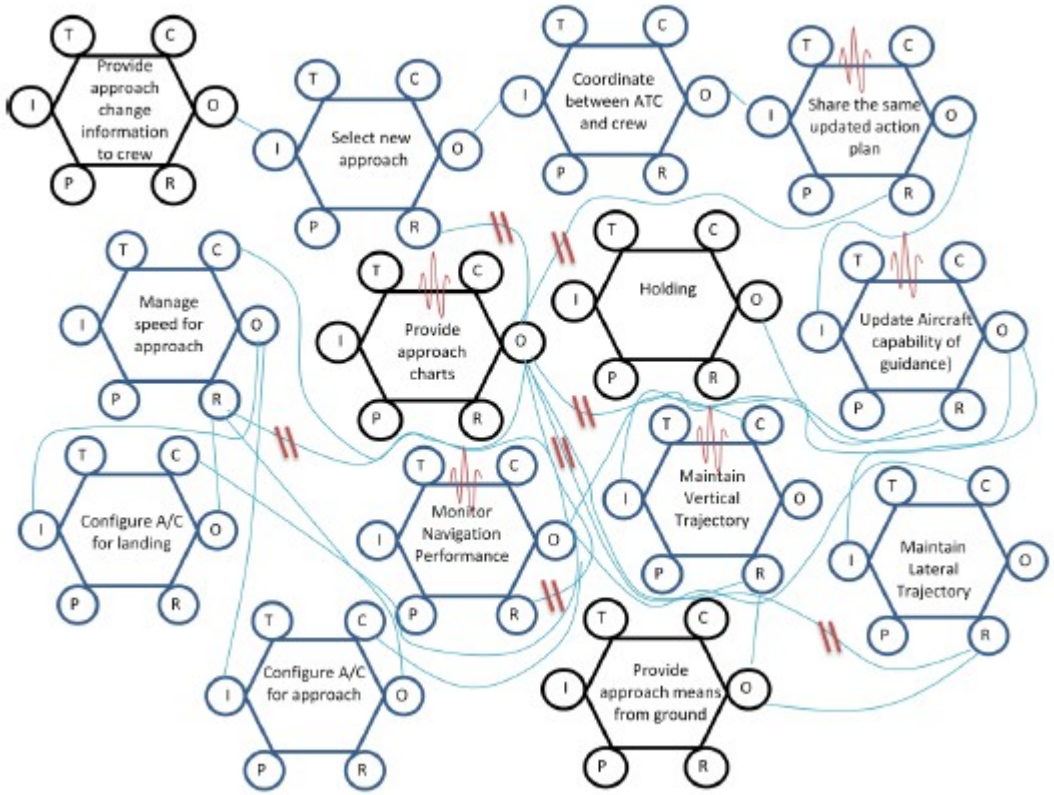




Accidents happen if internal or external events and disturbances are not adequately controlled. This may move the system beyond the safe states defined by the safety constraints.

The FRAM produces a model of the event

FRAM



The FRAM book (finally) published.

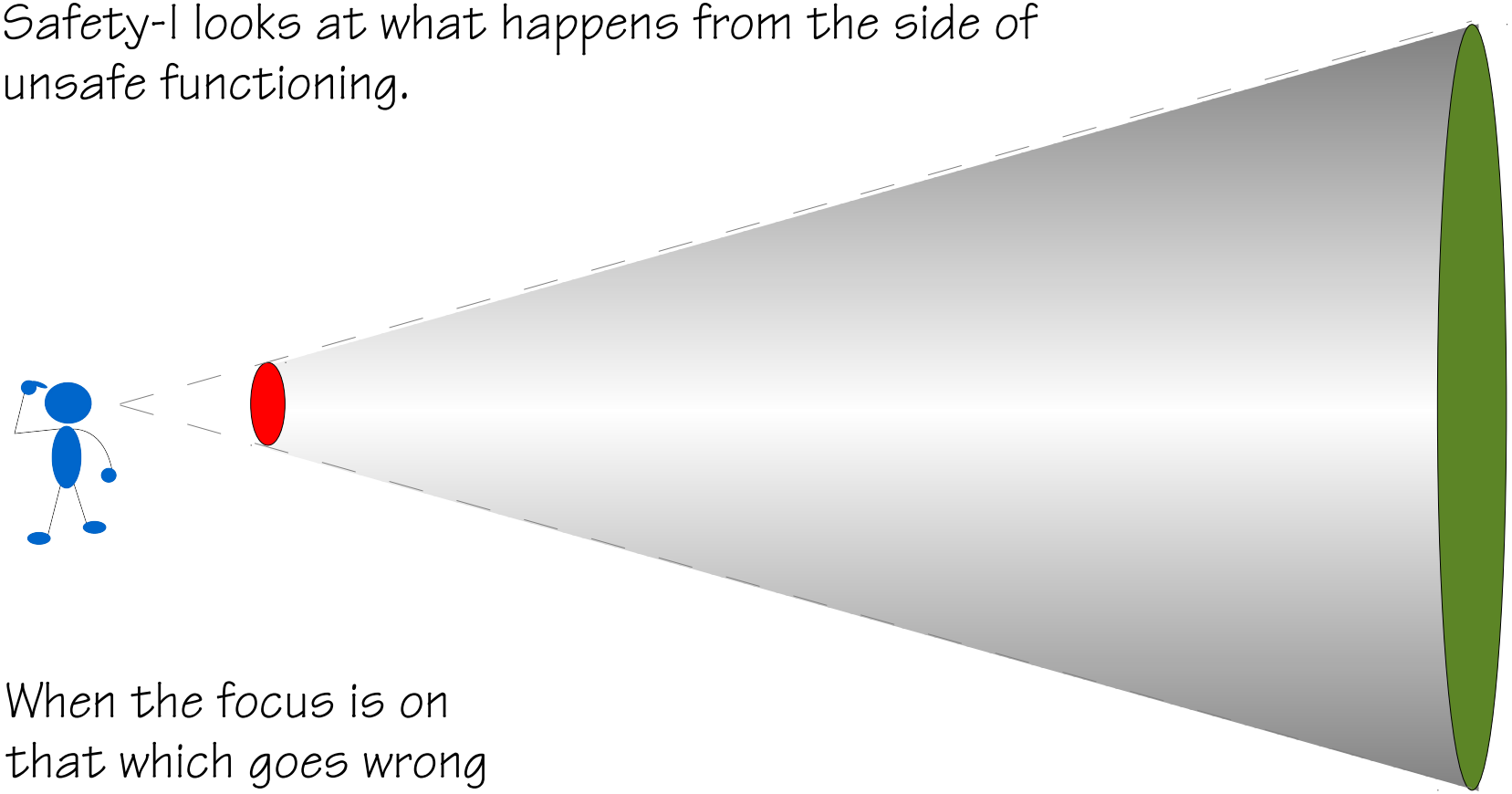
www.functionalresonance.com has been established (and partly populated)

Resilience Engineering basics: “Safety-I and Safety-II”

Growing number of practical applications of the FRAM

Safety-I: Focus on what *goes* wrong

Safety-I looks at what happens from the side of unsafe functioning.



When the focus is on
that which *goes* wrong
(accidents, incidents, etc.),
then it is difficult to *see* that which *goes* right.

Safety-I definitions - examples

FRAM

"Safety is the state in which the risk of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management."

Safety is defined as 'freedom from accidental injury,' which can be achieved by 'Avoiding injuries or harm to patients from care that is intended to help them.'

Industrial safety can be defined as the ability to manage the risks inherent to operations or related to the environment. Industrial safety is not a dislike of risks; rather it is a commitment to clearly identify them in relation to production operations, assess them in terms of quality and quantity, and manage them.

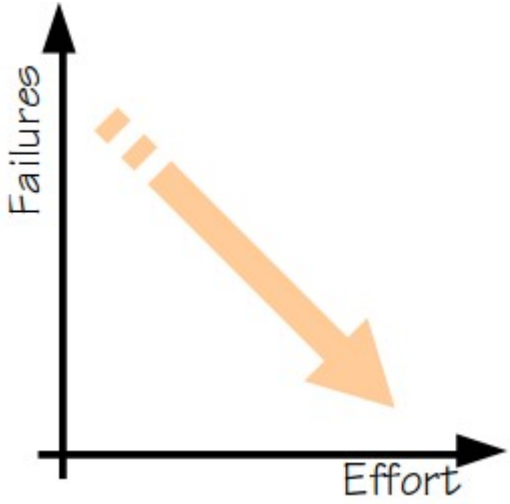
Safety-I – when nothing goes wrong

FRAM

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

Safety has traditionally been defined by its opposite – the lack of safety.

The lack of safety means that something goes wrong or can go wrong.

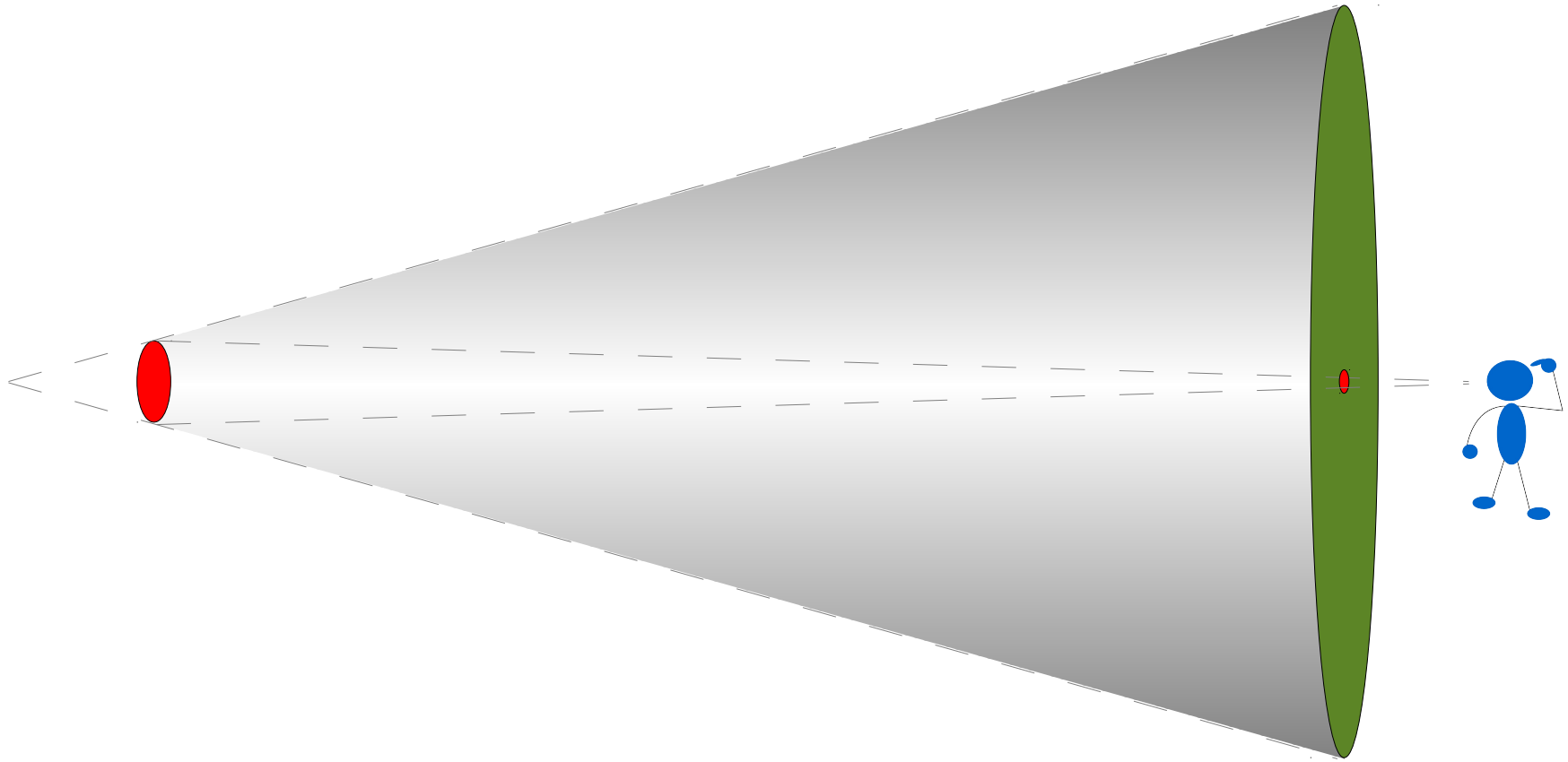


Safety-I requires the ability to prevent that something goes wrong. This is achieved by:

1. Find the causes of what goes wrong (RCA).
2. Eliminate causes, disable possible cause-effect links.
3. Measure results by how many fewer things go wrong.

Safety-II: Focus on what goes right

Safety-II looks at what happens from the side of safe functioning.



When the focus is on that which goes right (everyday performance), 'failures' no longer dominate the picture.

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.

Perceive those things which cannot be seen

Miyamoto Musashi (c. 1584-1645)

Why only look at what goes wrong?

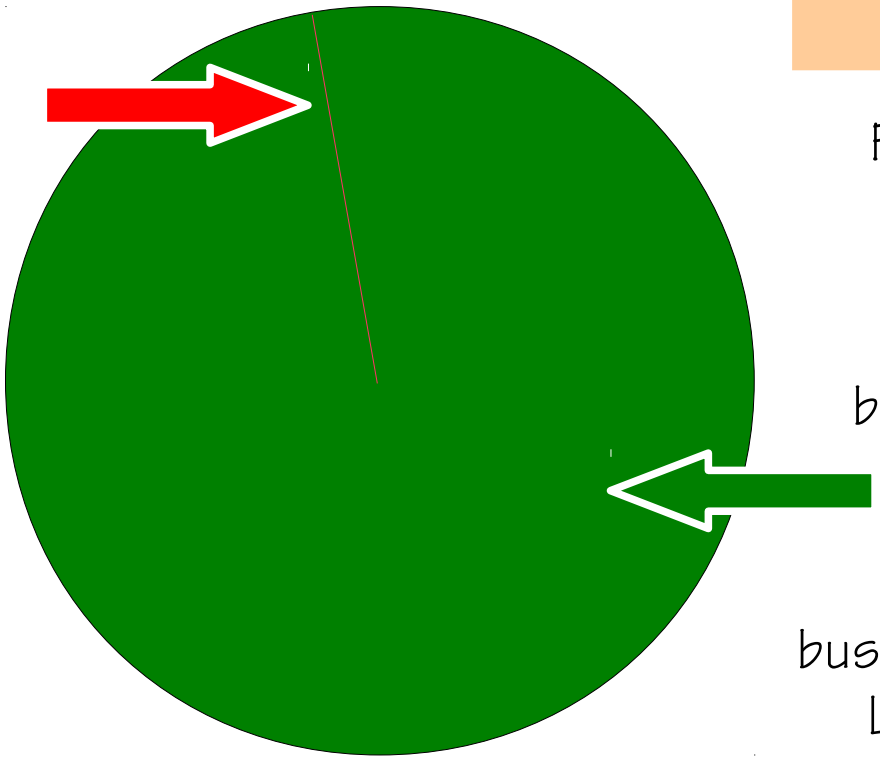
FRAM

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

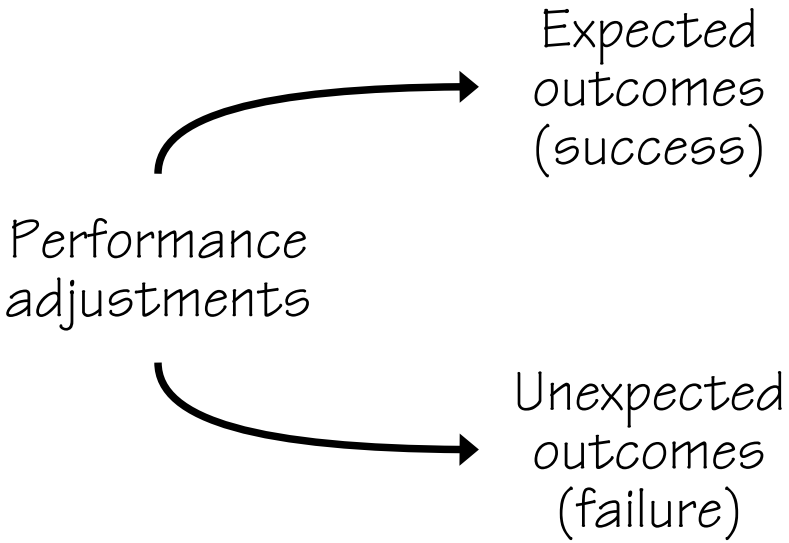
Safety II – when everything goes right

FRAM

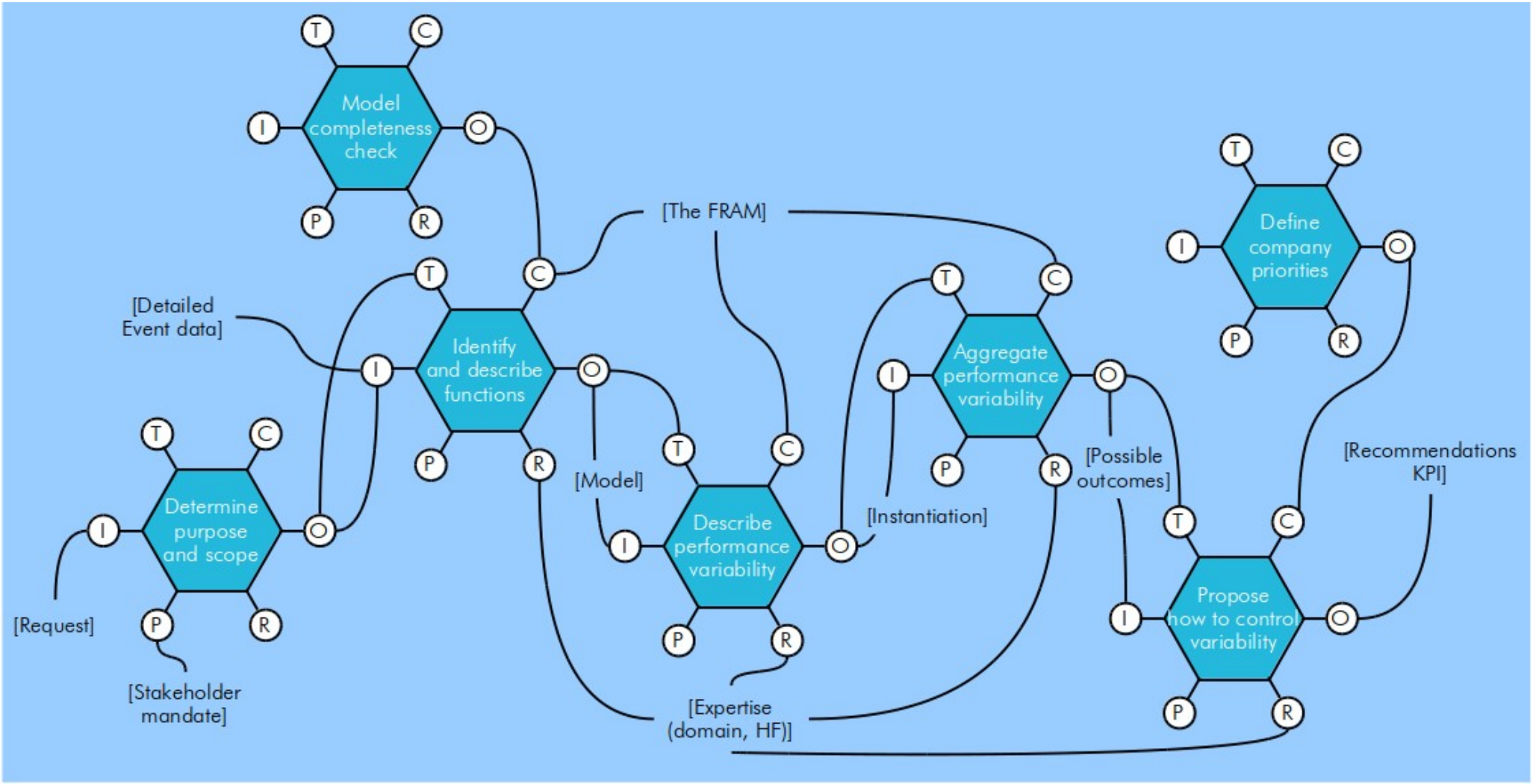
Safety-II is defined by the ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday work) are as high as possible.

Different outcomes ("normal" results vs. failures) are not distinct binary categories, but rather judgements of value.
Unexpected outcomes are not necessarily a consequence of unexpected processes.

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



A FRAM of the FRAM



2007

FRAM

2008

2009

2010 (but not everyone)

2011