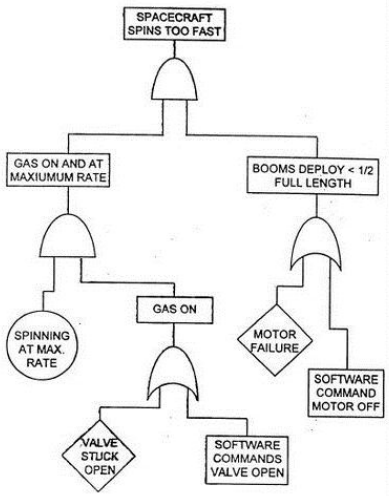
FRAM: Four Principles

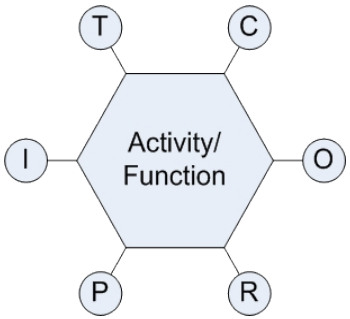
Erik Hollnagel
hollnagel.erik@gmail.com
www.safetysynthesis.com

Models and methods

An analysis of something inevitably involves some assumptions about how that something happens.
These assumptions correspond to a model: a simplified explanation of how something can happen and of how the 'world' is organised. The organisation usually implies some kind of hierarchical ordering of layers, parts, or components (structural models).



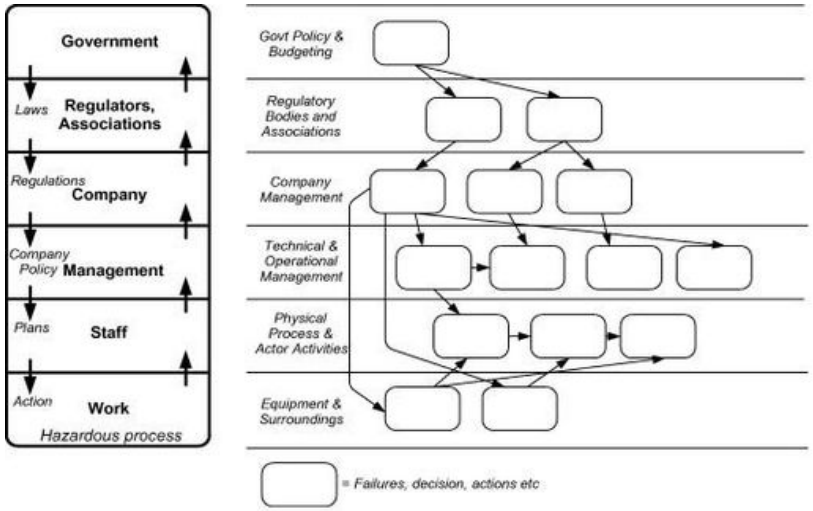
The model defines what the method can be used for, and therefore also sets the limits of the method.



The FRAM is a method to analyse how something happens and to builda model of that. The model can be used for various purposes (reactive, proactive). A FRAM model represents the functions that sufficient and necessary for an activity to take place – not when it goes wrong but when it goes right.

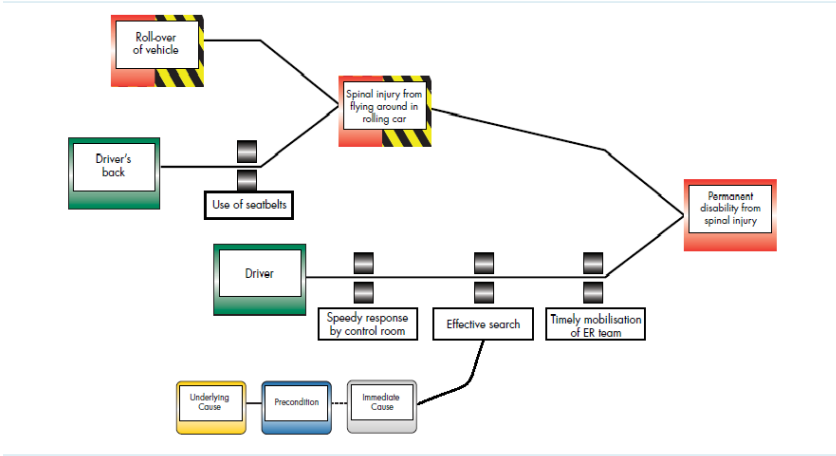
Methods usually "hide" their models

AcciMap - The abstraction hierarchy (Rasmussen, 1985)

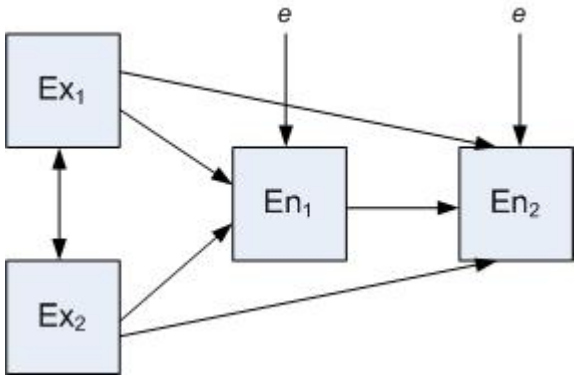


Bowtie – combined fault tree and event tree

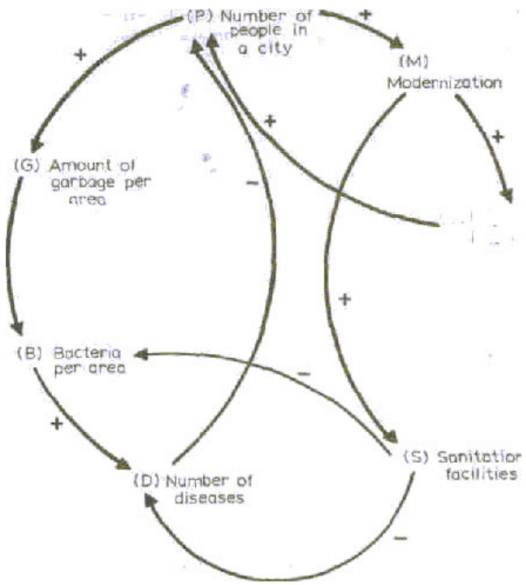
TRIPOD Beta



Explaining ("normal") dependencies



Path modelling
(Wright, 1921)



Second order cybernetics
Maruyama (1963)

Descriptions of directed dependencies among a set of variables (population genetics).

Mutual causal systems, where the elements influence each other either simultaneously or alternatingly.

What is a function?

In a mathematical function, one quantity (the argument or the input) completely determines another quantity (the value, or the output).

$$Y = F(x)$$

In engineering, a function refers to a specific process, action or task that a system is able to perform.
The function of a calculator, the function of a windmill, the function of a pump, etc. etc.

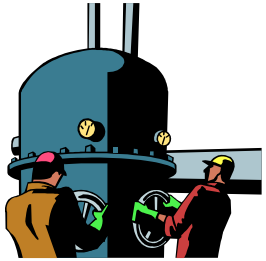
In human factors, a function refers to the task or activity – or set of tasks or activities - that must be done to produce a certain outcome.
A function describes what people – as individuals or collectives – or organisations have to do to achieve something (an aim).
Functions are the means that are necessary to reach stipulated goals.

Developments of functions in focus

Individual movements

Time & Motion studies

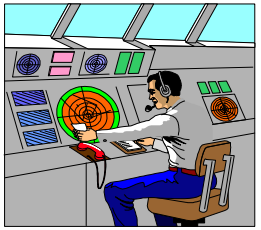
Gilbreth, Taylor (1911)



Tasks (manual)

Task decomposition

Miller (1953)



Tasks (cognitive)

Hierarchical Task Analysis

Annett & Duncan (1967)

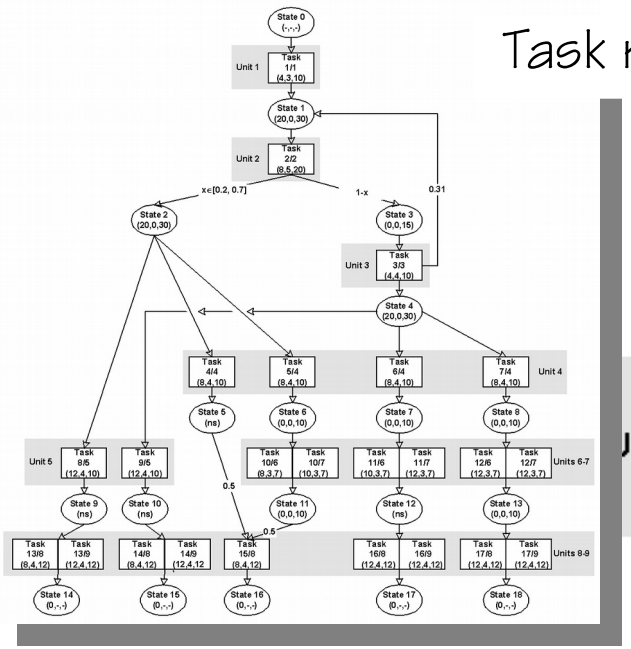
Distributed work

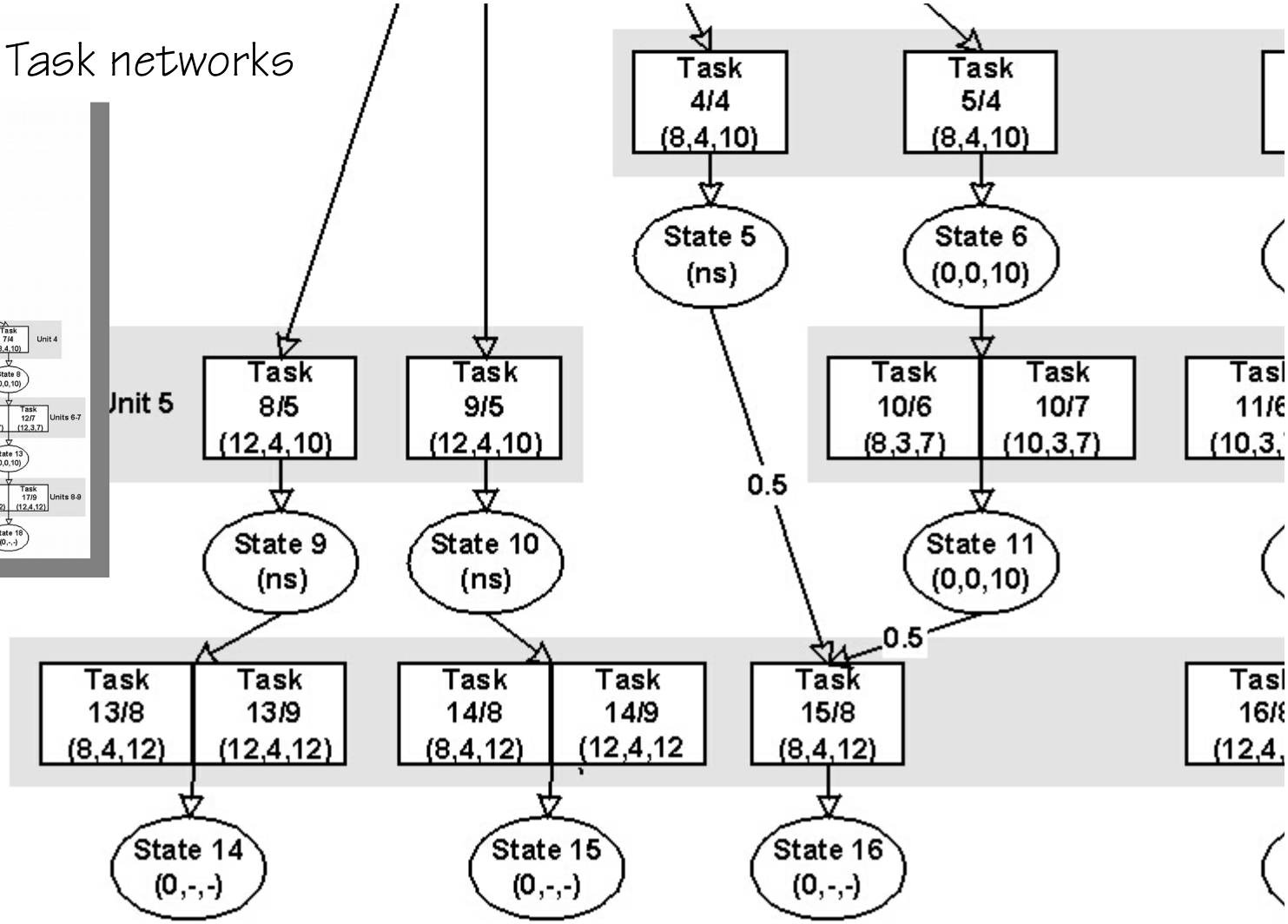
Cognitive task analysis

Hollnagel & Woods (1982)

Hierarchical Task Analysis

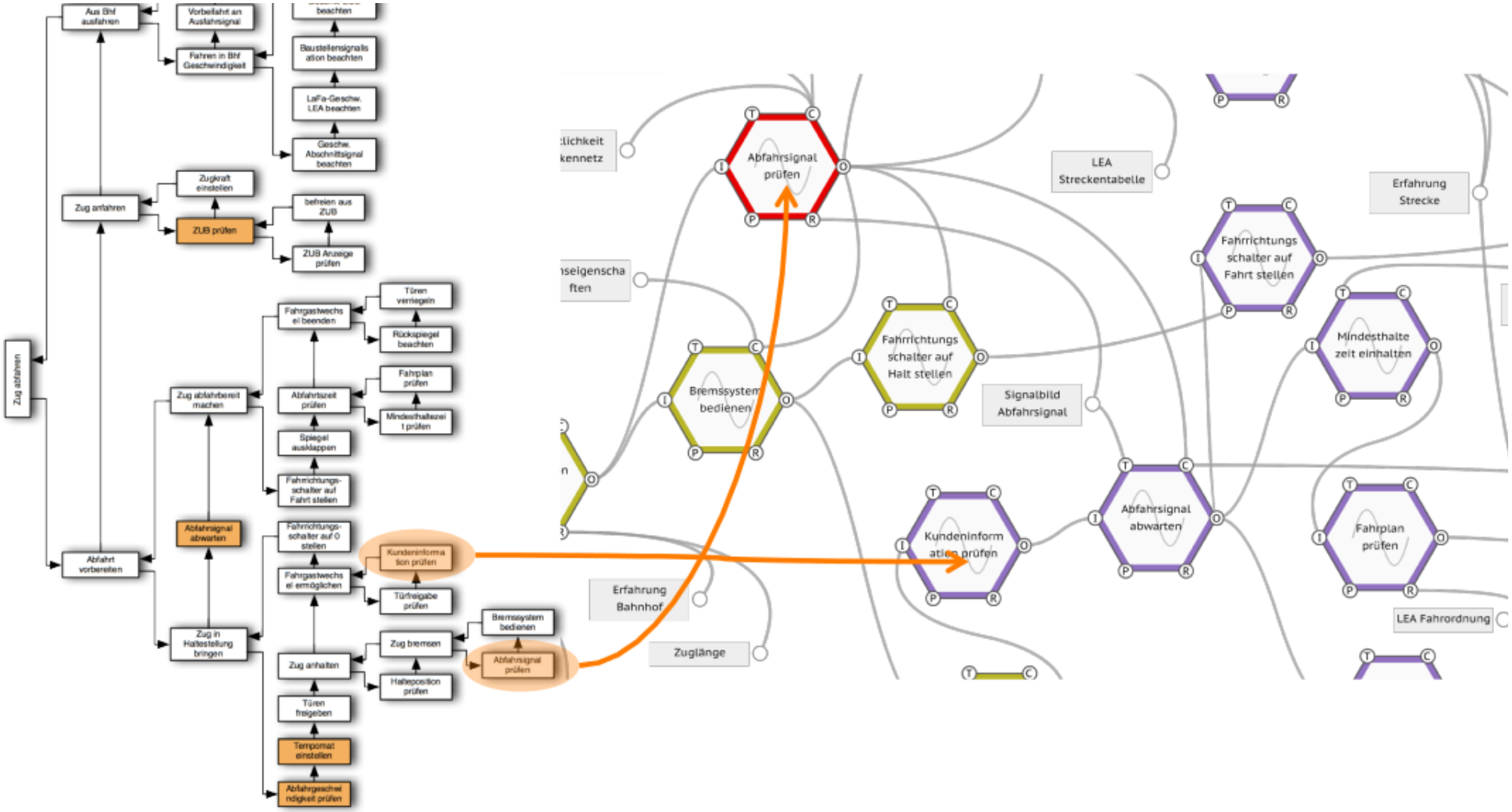
Task networks





The connectors (arrows) represent temporal (or logical) order.

HTA to FRAM



Principles for the FRAM

Safety Synthesis

- I -
The principle of equivalence of successes and failures

- II -
The principle of approximate adjustments

- III -
The principle of emergence

- IV -
The principle of functional resonance

1 - Equivalence of success and failures

Safety Synthesis

Failure is normally explained as a breakdown or malfunctioning of a system and/or its components.

This view assumes that success and failure are of a fundamentally different nature.

Resilience Engineering recognises that individuals and organisations must adjust to the current conditions in everything they do. Because information, resources and time always are finite, the adjustments will always be approximate.

- Success is due to the ability of organisations, groups and individuals correctly to make these adjustments, in particular correctly to anticipate risks before failures and harm occur.
- Failures can be explained as the absence of that ability – either temporarily or permanently.

The aim of Resilience Engineering is to strengthen that ability, rather than just to avoid or eliminate failures.

II: Approximate adjustments

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.

Efficiency-Thoroughness Trade-Off

Safety Synthesis

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

Efficiency: Time to do
Implementing plans.
Executing actions.

If thoroughness dominates, there may be too little time to carry out the actions.

If efficiency dominates, actions may be badly prepared or wrong

Neglect pending actions
Miss new events

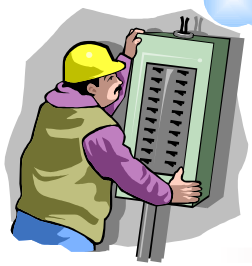
Miss pre-conditions
Look for expected results

Time & resources needed

Time & resources available

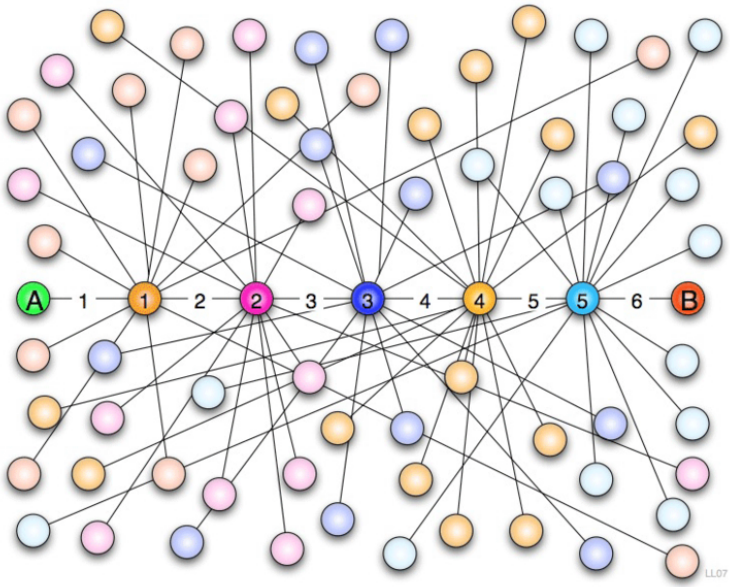
Some ETTO heuristics

Cognitive (individual)	Idiosyncratic (work related)	Collective (organisation)
Judgement under uncertainty	Looks fine	Negative reporting
Cognitive primitives (SM – FG)	Not really important	Reduce redundancy
Reactions to information input overload and underload	Normally OK, no need to check	Meet "production" targets
Cognitive style	I've done it millions of time before	Reduce unnecessary cost
Confirmation bias	Will be checked by someone else	Double-bind
	Has been checked by someone else	Reject conflicting information
	This way is much quicker	
	No time (or resources) to do it now	
	Can't remember how to do it	
	We always do it this way	
	It looks like X (so it probably is X)	
	We must get this done	
	Must be ready in time	
	Must not use too much of X	



III - Principle of emergence

The variability of normal performance is rarely large enough to be the cause of an accident in itself or even to constitute a malfunction.
The variability from multiple functions may combine in unexpected ways, leading to consequences that are disproportionally large, hence produce non-linear effects.
Both failures and normal performance are emergent rather than resultant phenomena, because neither can be attributed to or explained only by referring to the (mal)functions of specific components or parts.



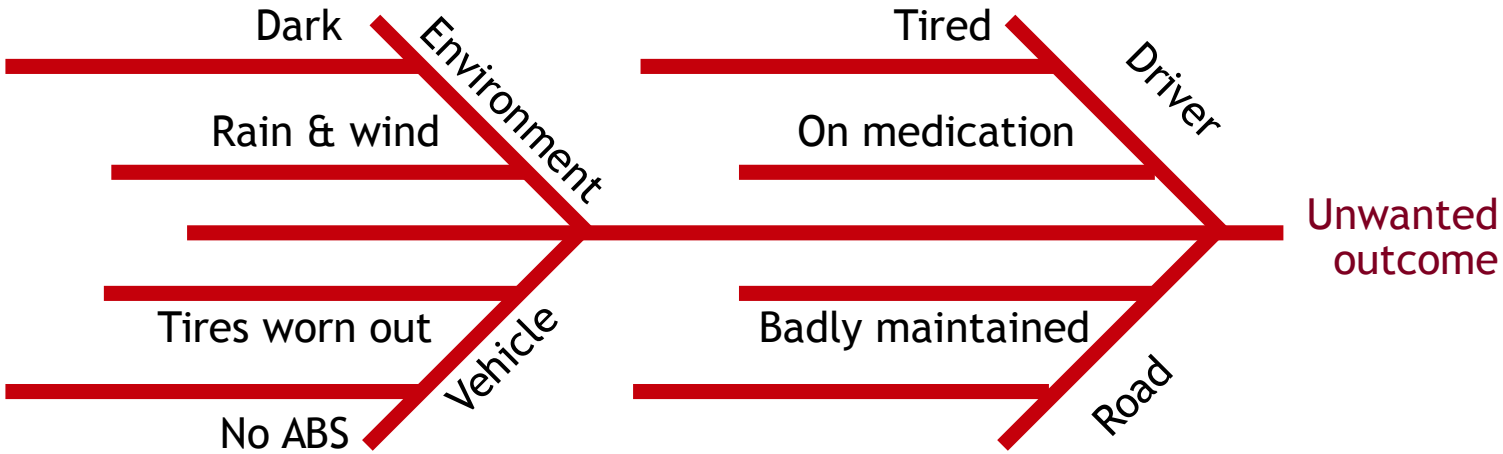
The Small World Problem

Socio-technical systems are intractable because they change and develop in response to conditions and demands. It is therefore impossible to know all the couplings in the system, hence impossible to anticipate more than the regular events. The couplings are mostly useful, but can also constitute a risk.

Stable causes

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

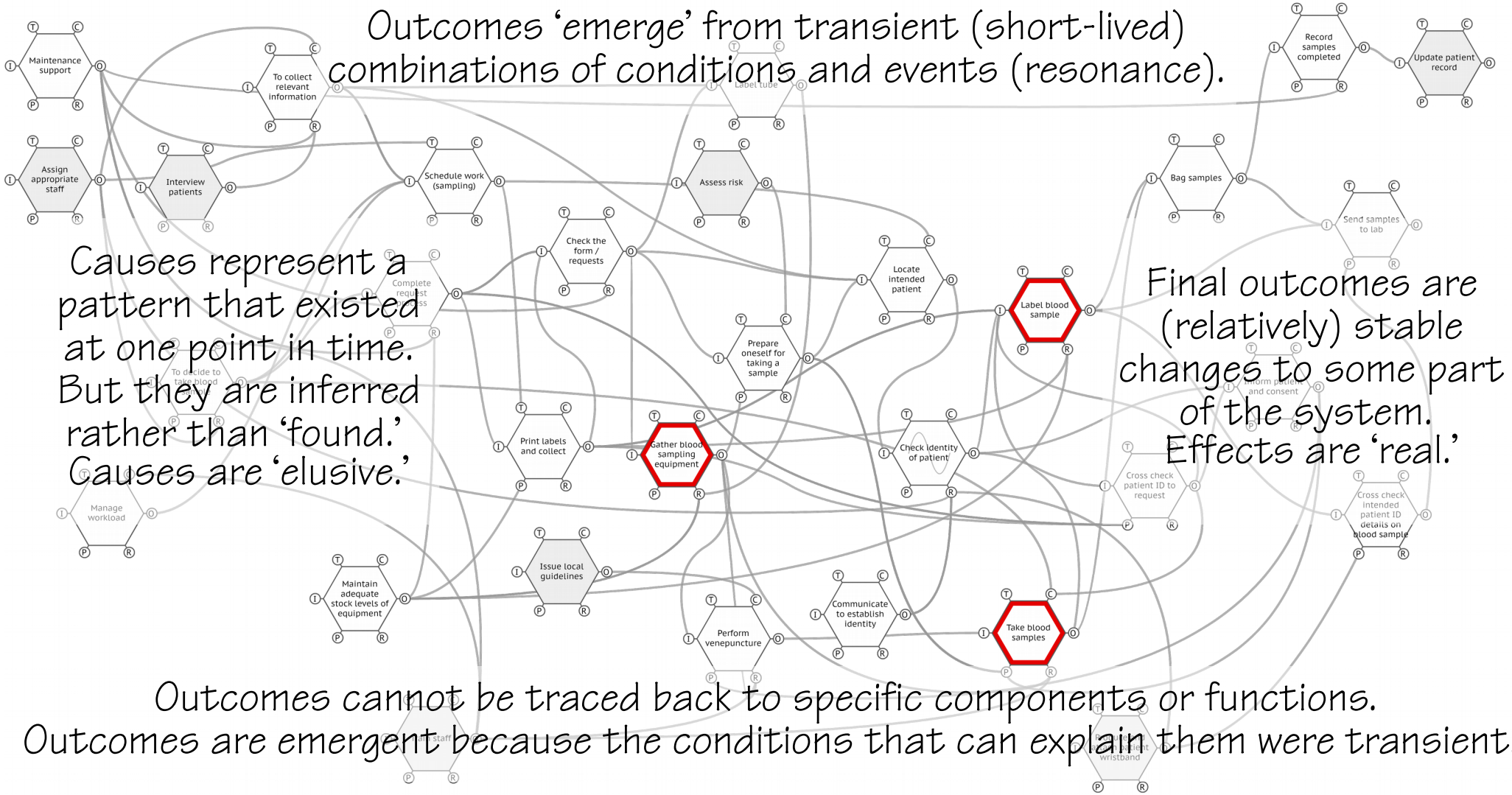
Final effects are (relatively) stable changes to some part of the system. Effects are 'real.'



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.

Transient causes

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

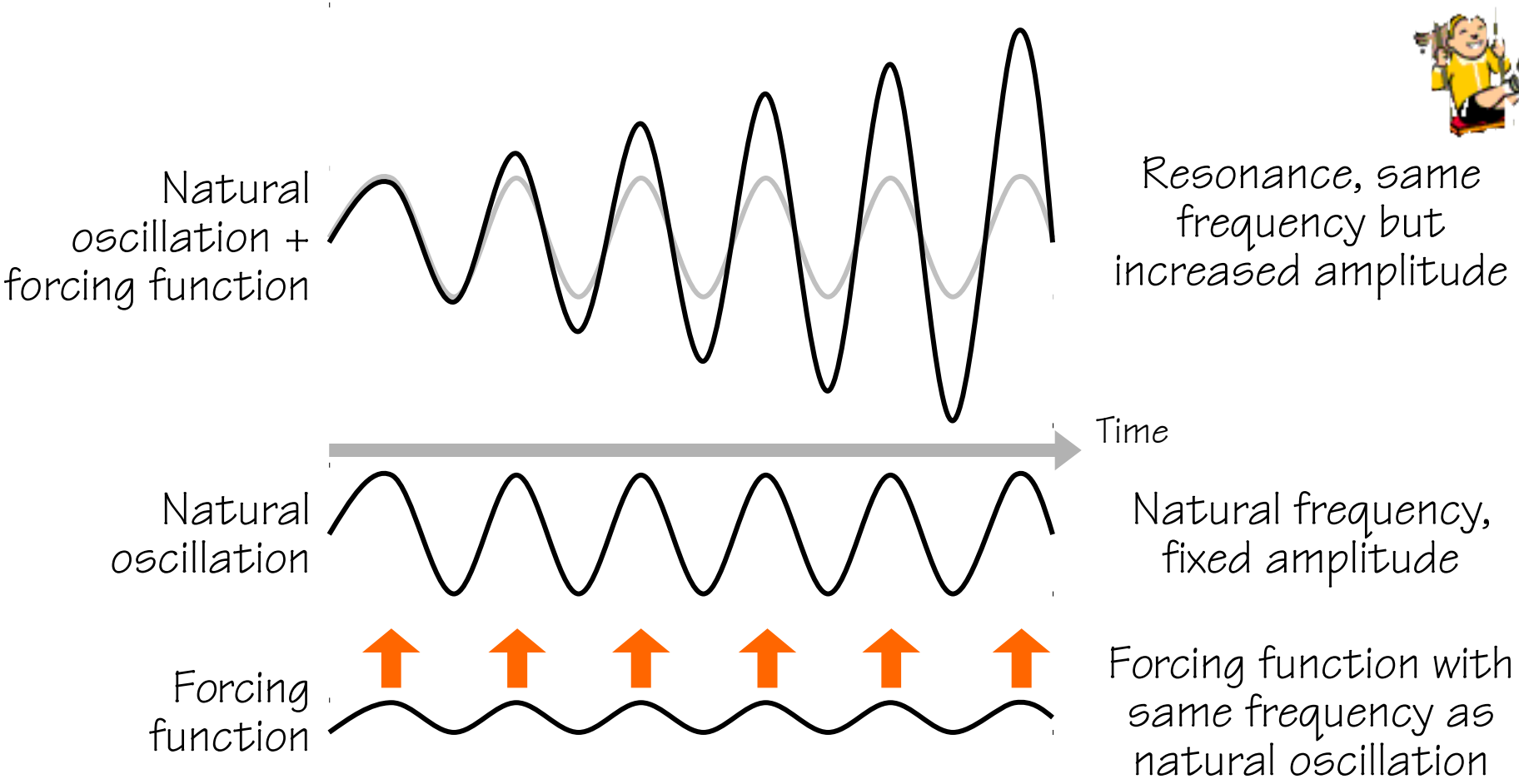


Causes represent a pattern that existed at one point in time. But they are inferred rather than 'found.' Causes are 'elusive.'

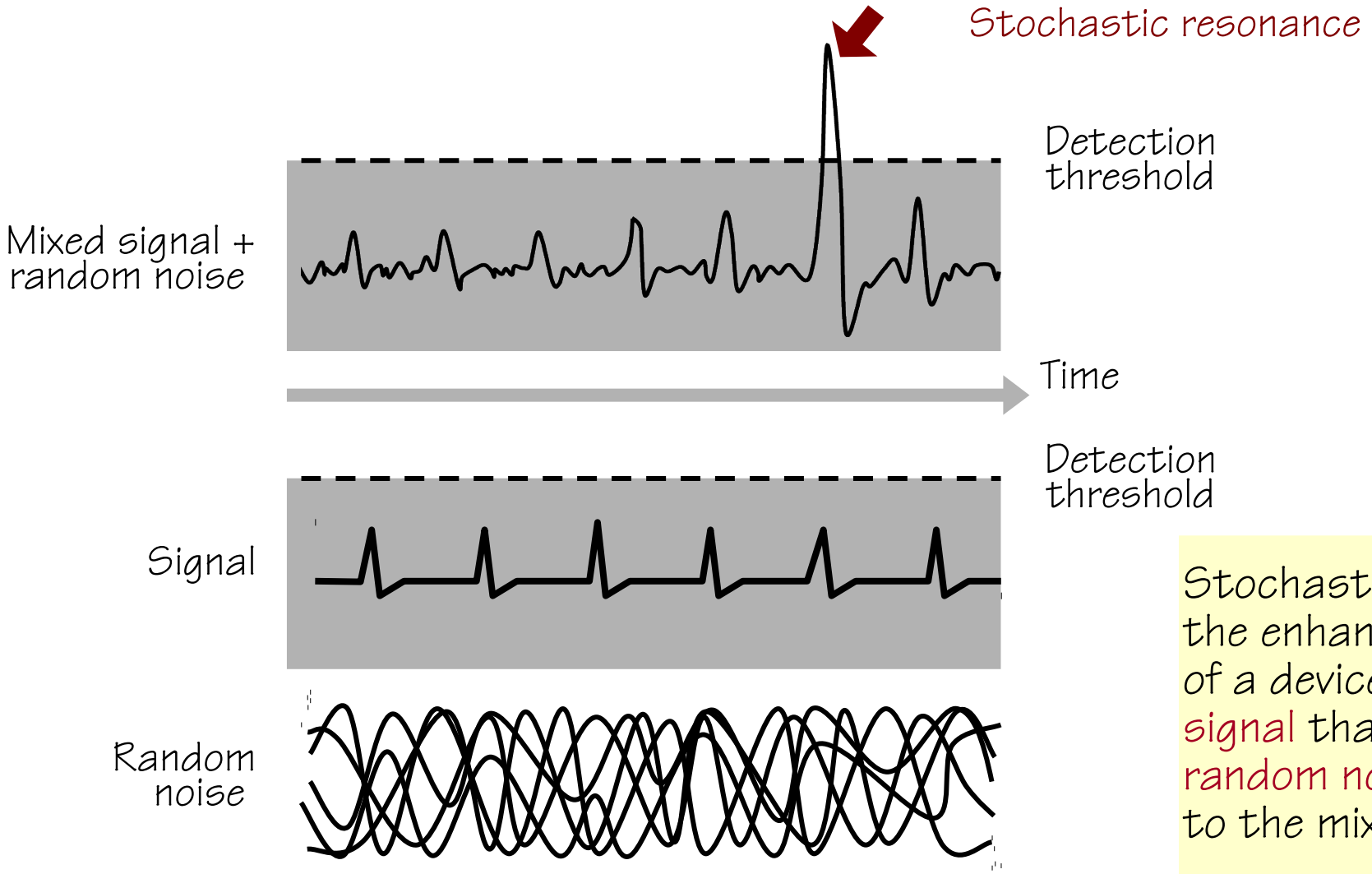
Final outcomes are (relatively) stable changes to some part of the system. Effects are 'real.'

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

IV – Functional resonance

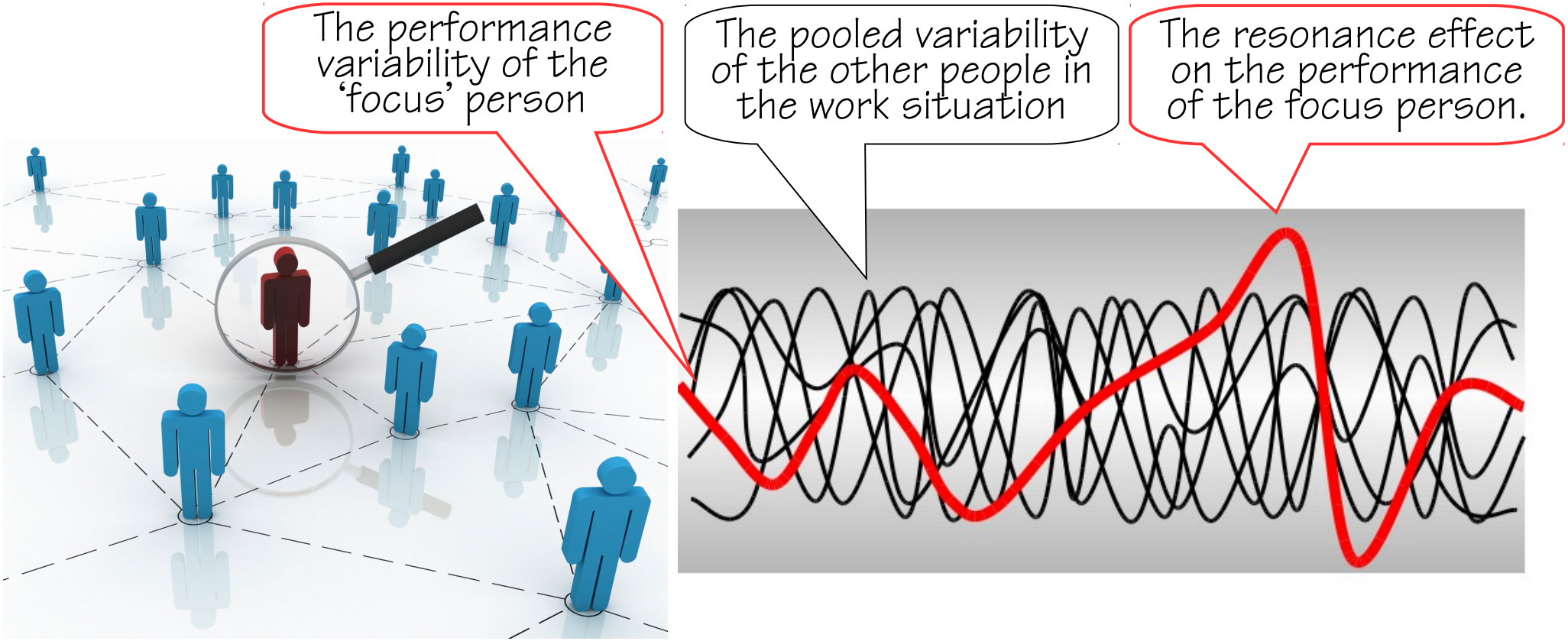


Stochastic resonance



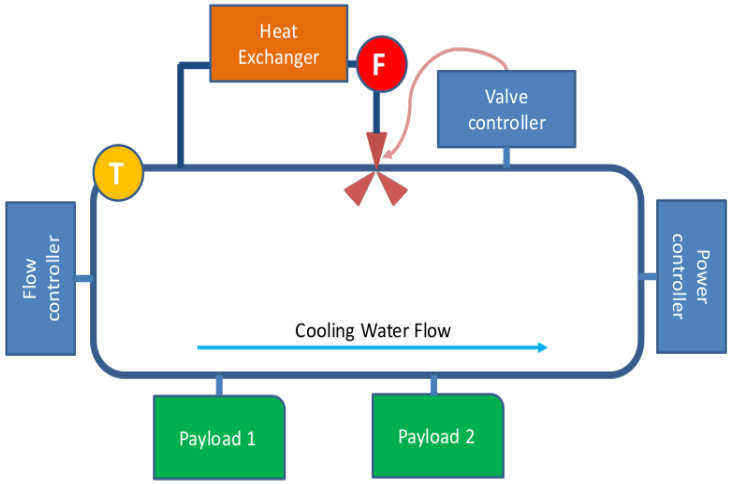
Stochastic resonance is the enhanced sensitivity of a device to a weak signal that occurs when random noise is added to the mix.

Functional resonance

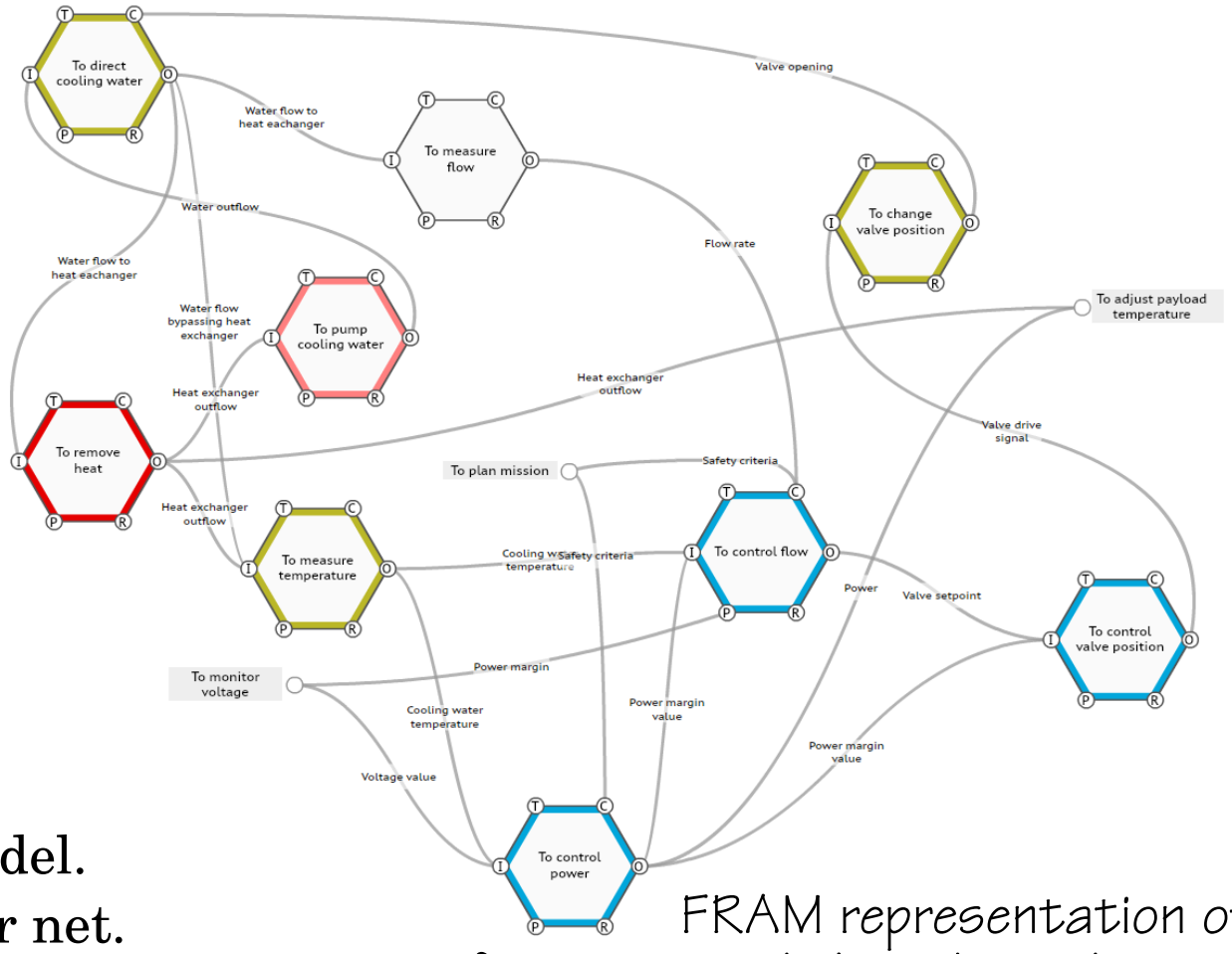


Functional resonance is the detectable signal that emerges from the unintended combination of the variability of many signals.

System as parts or as functions



Classic description of parts / components and their relations.



A FRAM model is not a flow model.
A FRAM model is not a graph or net.

FRAM representation of functions and their dependencies

Different uses of FRAM models

FRAM: The Method

↓

FRAM models
& instantiations

↓

Past situations:
Why did it happen?
How did it happen?

Present situations:
How is work done?
Daily adjustments

Future situations:
What if?
How to do?