From FRAM (Functional Resonance Accident Model)

to FRAM (Functional Resonance Analysis Method)

Erik Hollnagel
École des Mines de Paris – Centre for Research on Risk and Crises (CRC)
Sophia Antipolis, France
E-mail: erik.hollnagel@crc.ensmp.fr

Risk in reality

Type of risk	History
Loss of property during transportation	4.000 – 3.000 B.C. (China, Babylon): "bottomry" contracts – insurance of commercial vessels. Later becomes maritime insurance. Oldest policy in existence from 24 April, 1384
Loss by gambling	1645 – Blaise Pascal develops probability calculus
Loss of property by fire	The great fire of London (1666) marks the beginning of insurance against fire.
Loss of life or capabilities	1759 first life-insurance company in the USA (Presbyterian Ministers' Fund)
First train accident	1830 William Huskisson killed in train accident
First car accident	1869 (Aug. 31) Mary Ward fell under the wheels of a steam car
Steam engine	1786, James Watt gets a patent on low pressure steam engine, warns against use of high pressure engines. Many accidents in US Navy (1816-1848: 2 562 dead in 233 accidents).

Understanding risks

Formal methods

Models

Requisite imagination

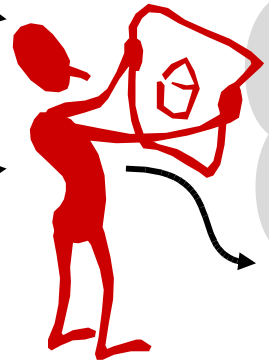
Expert judgment

Hazard

Coincidence

Demands

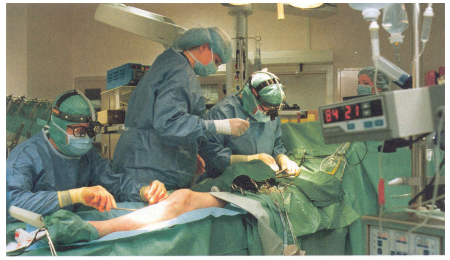
What has happened



SCENARIO

Single events vs. series of events

What may happen



Probability p(x|S)

Situations

Events

Understanding and assessing risks

1 Is it possible to understand what the problem is?

Recognise that there is a risk
NO SYSTEMS ARE INHERENTLY SAFE!
Understand the reasons for it (availability of examples)

2 Is it possible to imagine the consequences and to differentiate between large and small risks?

Envisage the consequences concretely
Understand failure "mechanism" (representativeness).
Intuitive feeling that the risks are real.

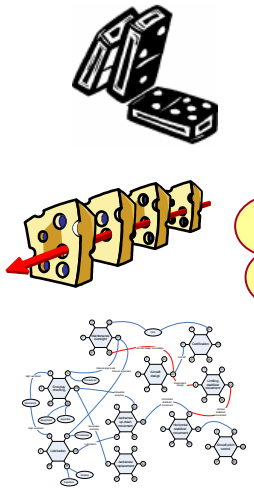
3 Are there are any known solutions by which the risk can be reduced or eliminated?

Specify concrete solutions, i.e., specific actions or precautions.
Solutions must correspond to the failure "mechanisms"

If "safety = the freedom from unacceptable risk", then how do we find the risk?

Accounting for the unpredictable

Risk assessment requires an adequate representation – or model – of the possible future events.



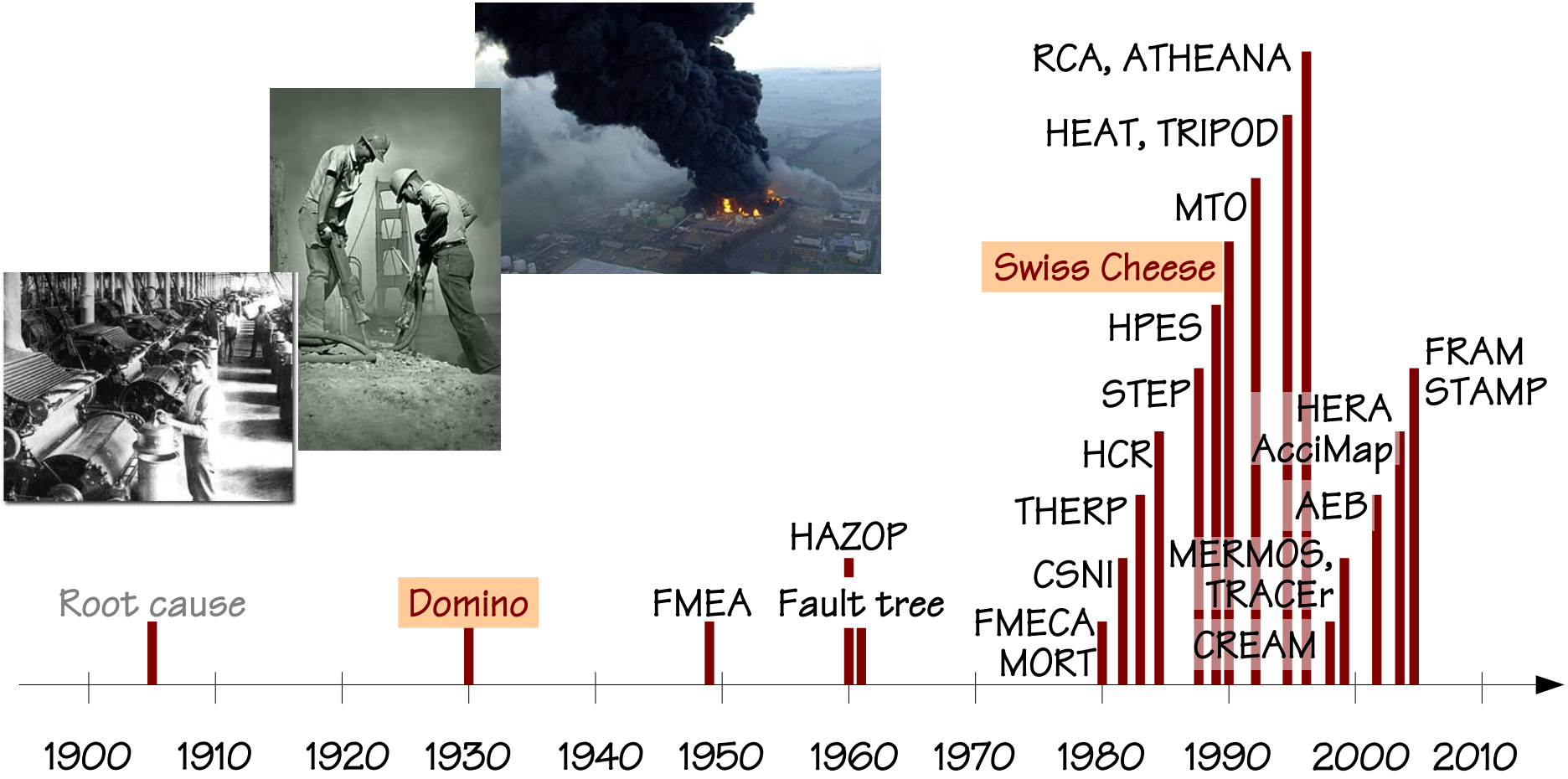
Accident model / risk model

What may happen?

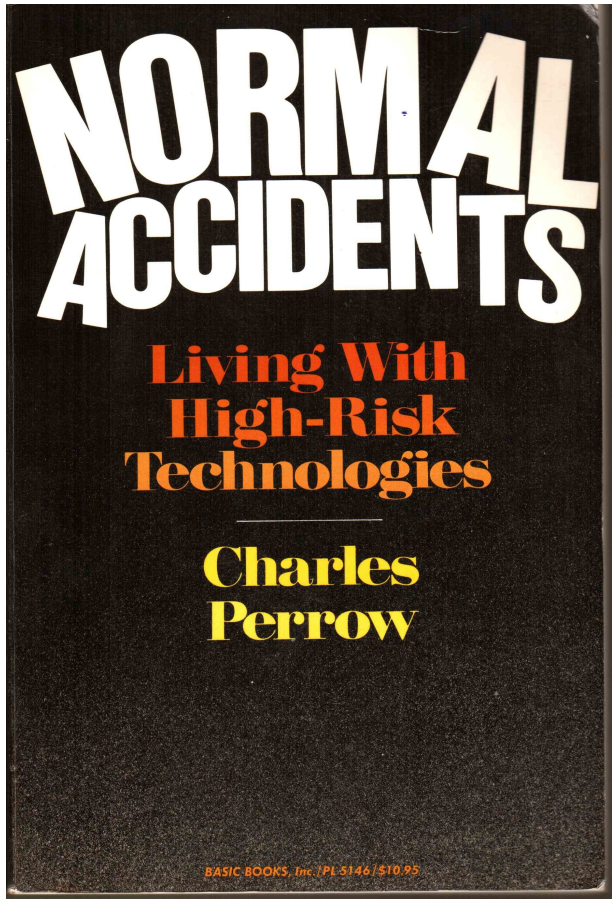
How should we respond?

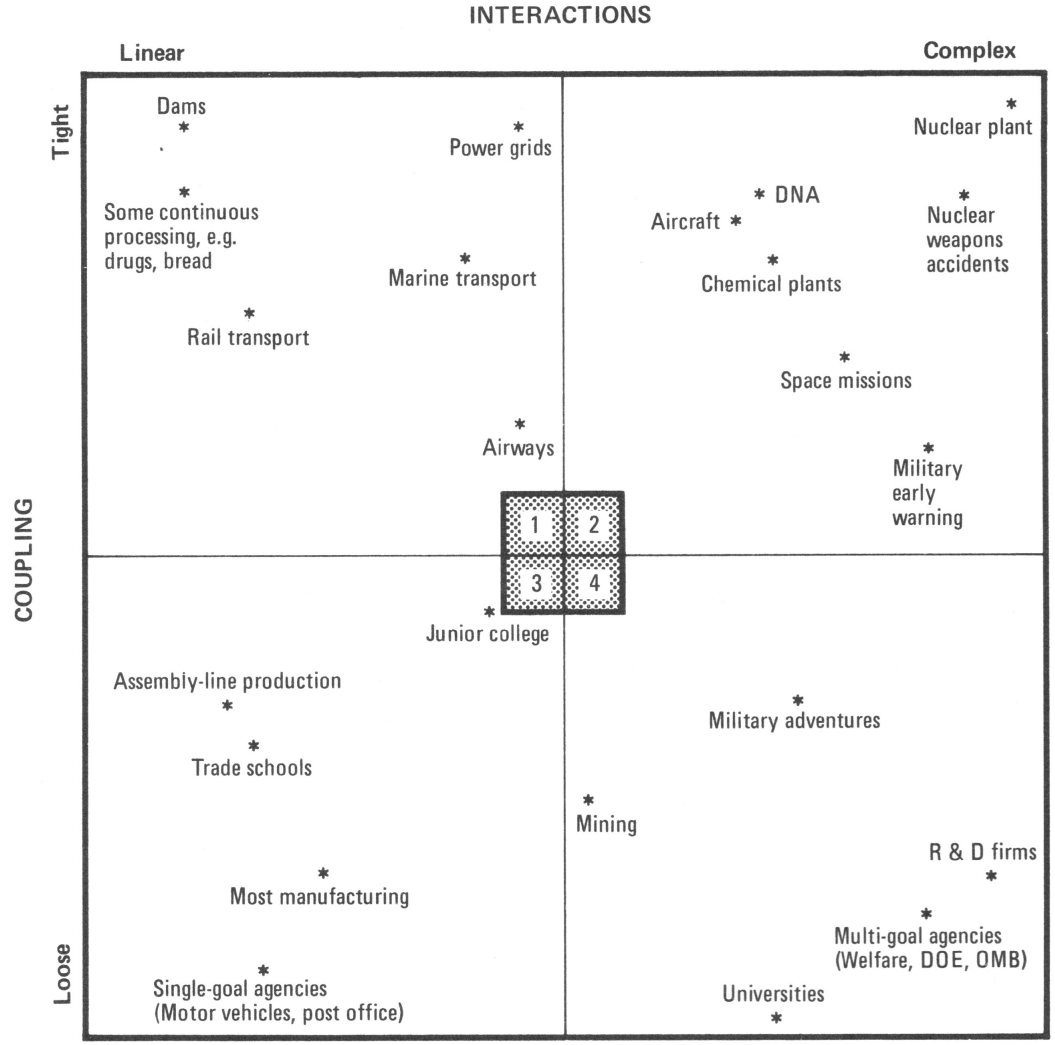
The representation must be powerful enough to capture the functional complexity of the system being analysed.

Accident & Risk Analysis Methods

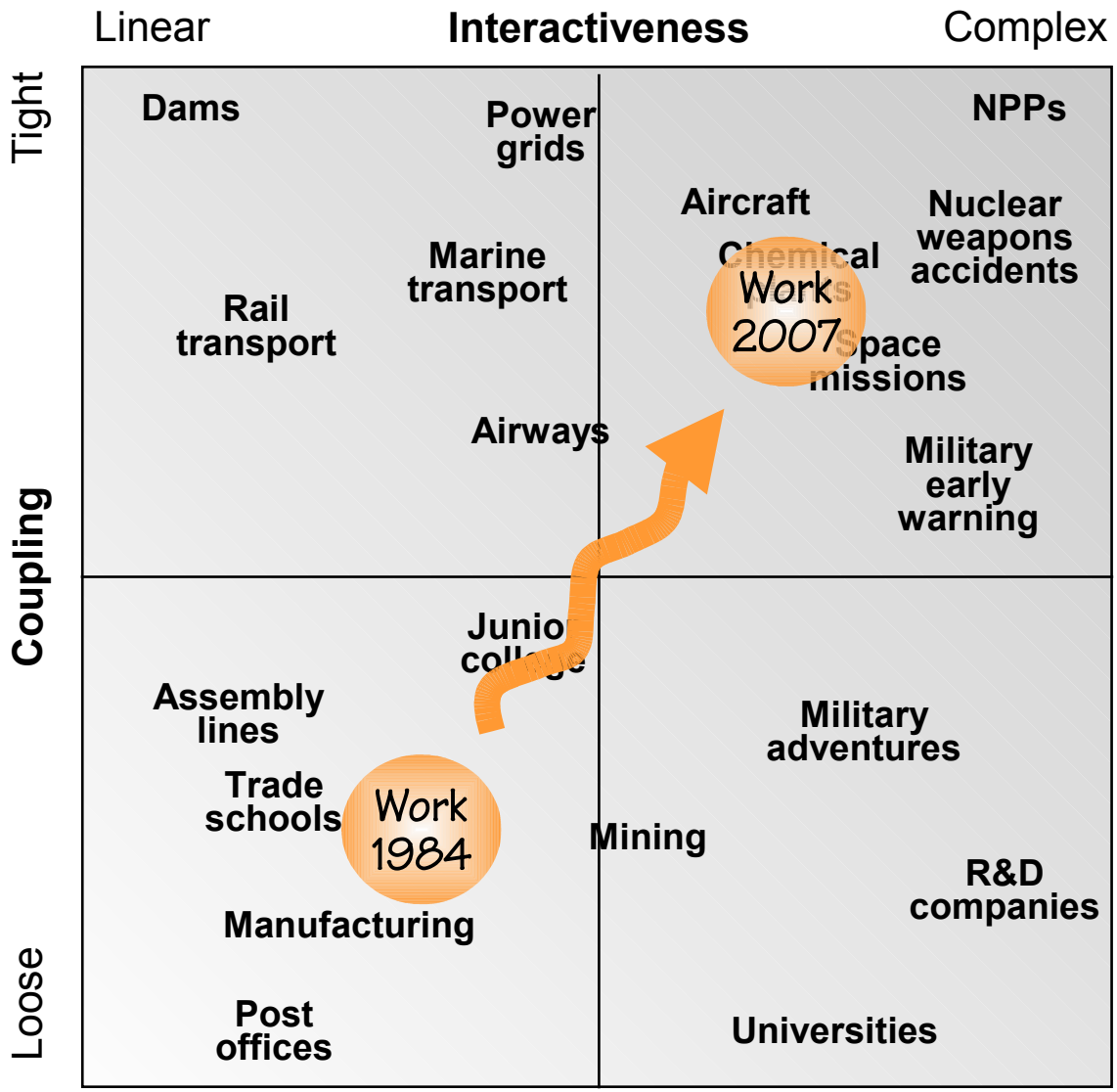


Normal accident theory (1984)





Coupling and interactiveness



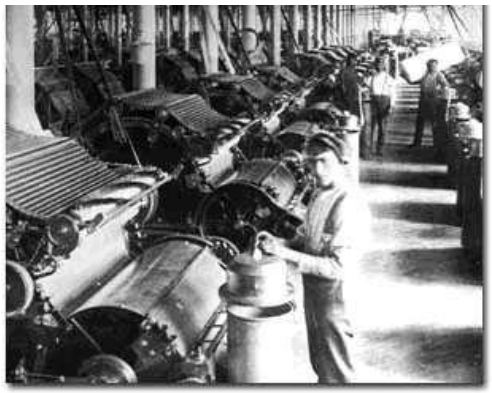
Complex systems / interactions:
Tight spacing / proximity
Common-mode connections
Interconnected subsystems
Many feedback loops
Indirect information
Limited understanding

Tight couplings:
Delays in processing not possible
Invariant sequence
Little slack (supplies, equipment, staff)
Buffers and redundancies designed-in
Limited substitutability

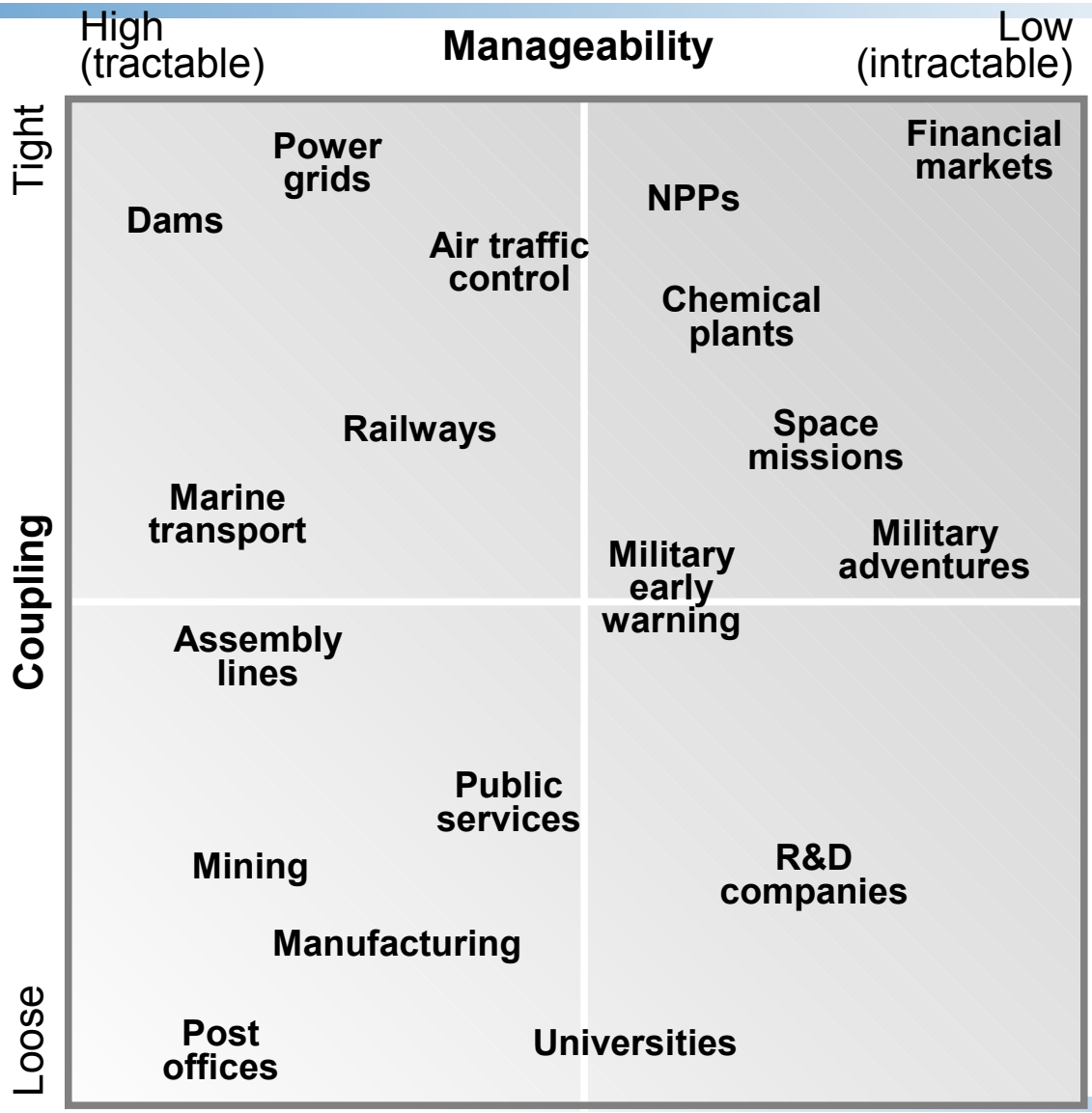
"On the whole, we have complex systems because we don't know how to produce the output through linear systems."

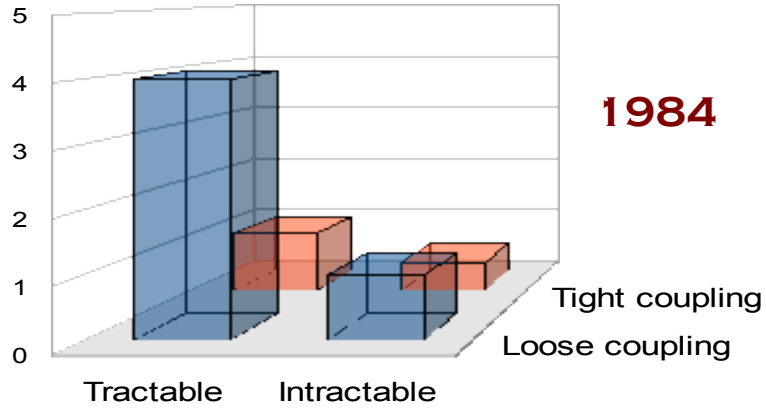
Complexity or tractability?

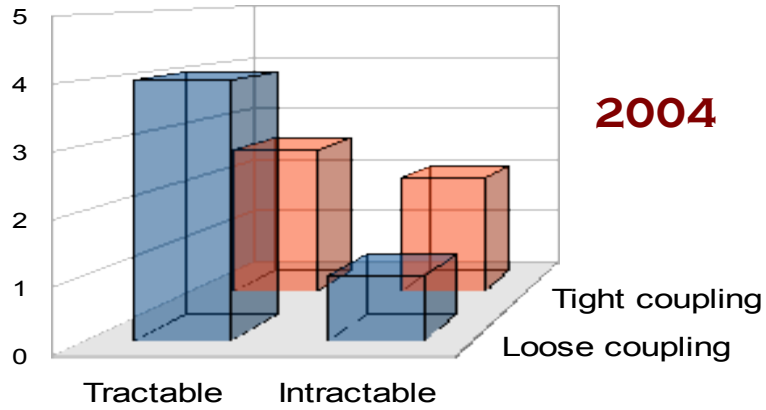
Tractable system		Intractable system
Principles of functioning are known	⇔	Principles of functioning are unknown or only partly known
Description of system is easy and contains few details	⇔	Description of system is difficult and contains many details
Description can be made quickly	⇔	Description takes a long time to make
System does not change while being described	⇔	System changes before description is completed



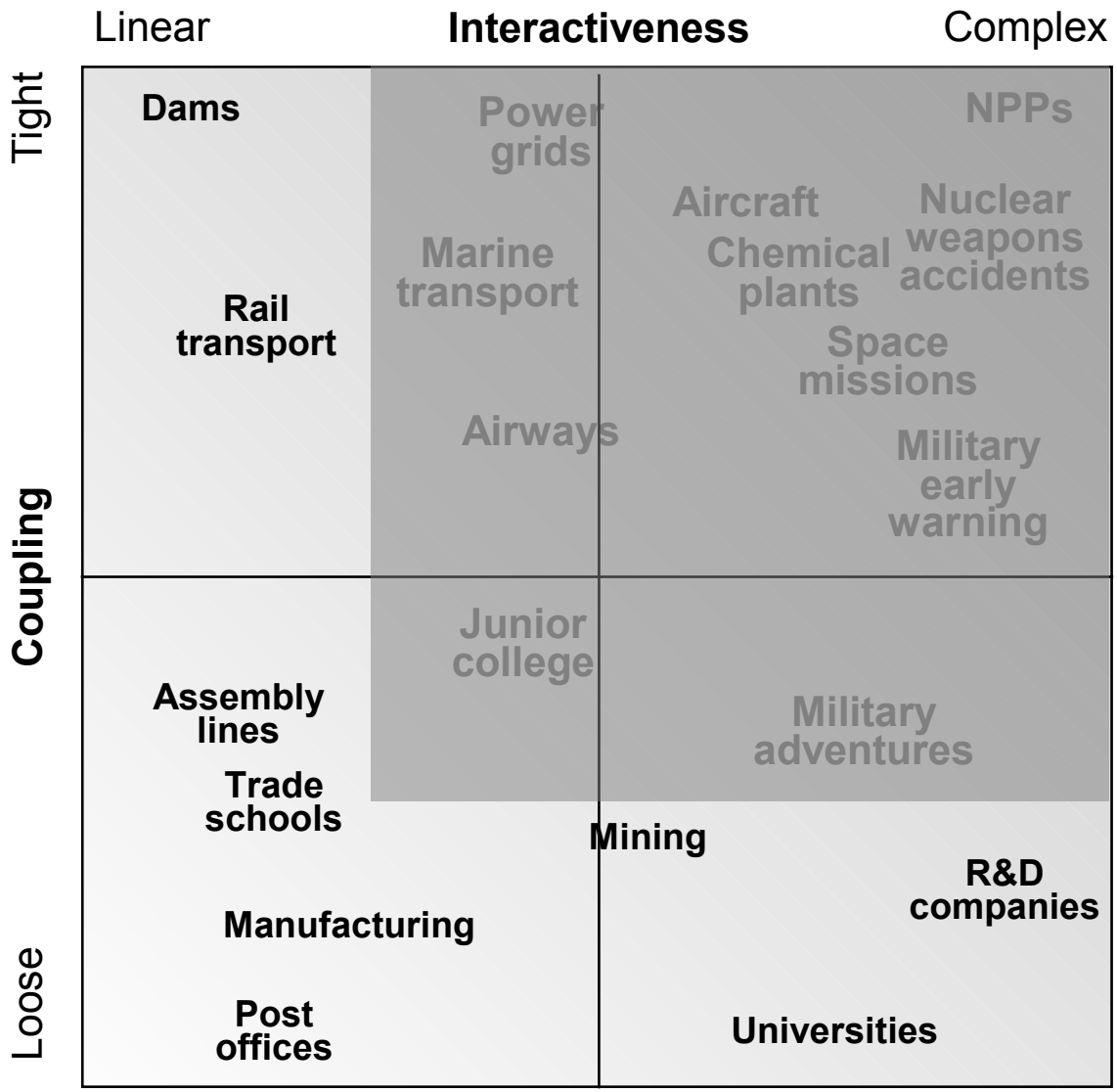
From complexity to tractability







Systems and methods, pre-1930



Accidents often limited to single user-equipment system.

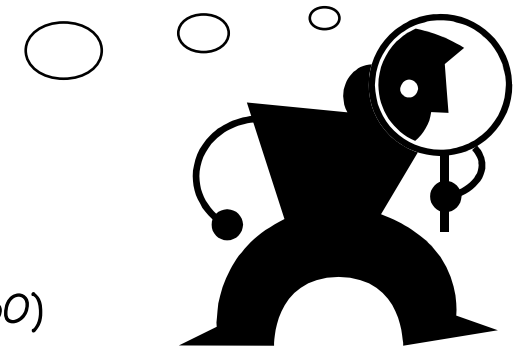
Interactiveness generally linear, hence easy to comprehend.

"The occurrence of a preventable injury is the natural culmination of a series of events or circumstances, which invariably occur in a fixed and logical order."

Understanding safety: linear models

Assumption: Accidents are the (natural) culmination of a series of events or circumstances, which occur in a specific and recognisable order.

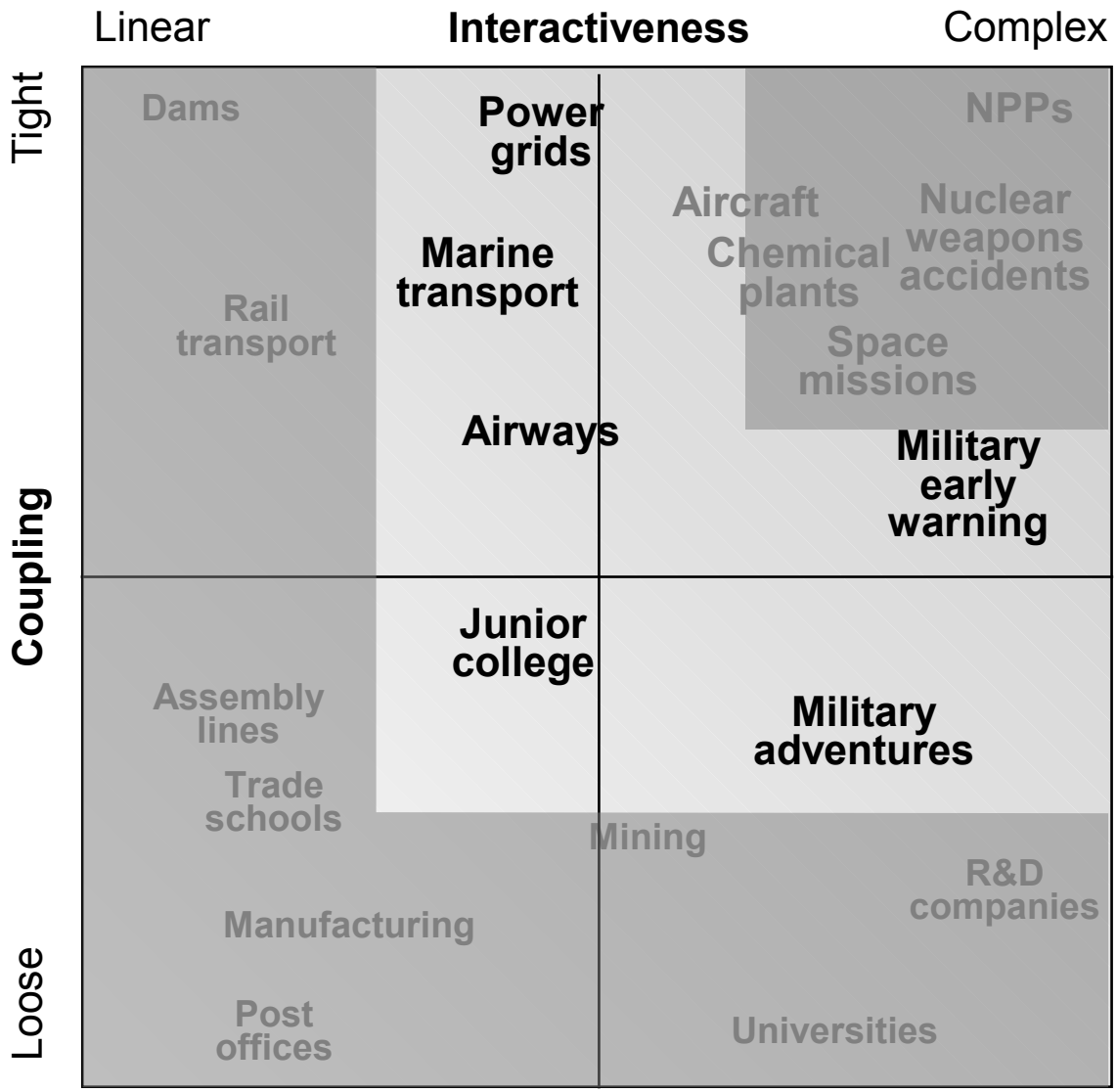
Domino model (Heinrich, 1930)



Consequence: Accidents are prevented by finding and eliminating possible causes.
Safety is ensured by improving the organisation's ability to respond.

Hazards-risks: Due to component failures (technical, human, organisational), hence looking for failure probabilities (event tree, PRA/HRA).
The future is a "mirror" image of the past.

Systems and methods, pre-1984



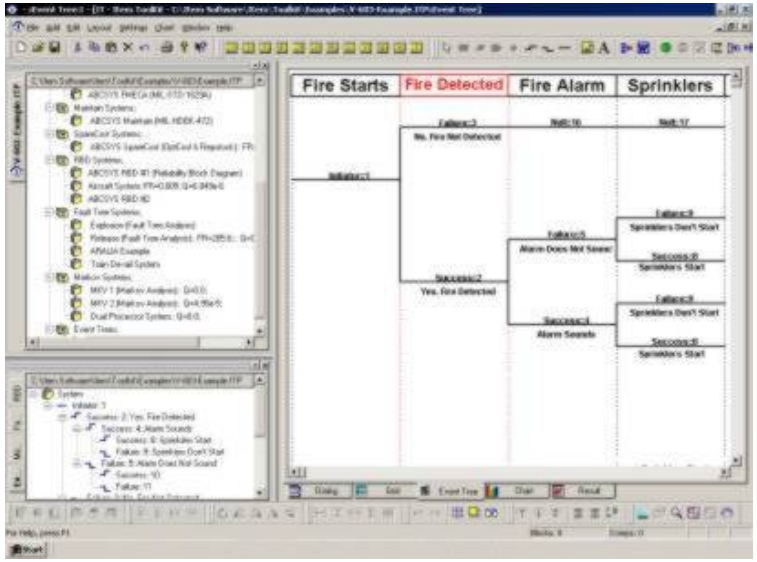
Accidents often have consequences beyond the single user-equipment system.

Interactiveness and dynamics often complex and difficult to comprehend.

Powerful technology drives system development.

Risks seen as caused by failures and malfunctions that can combine in so many ways that formal models and methods are needed.

Common assumptions



System can be decomposed into meaningful elements (components, events)

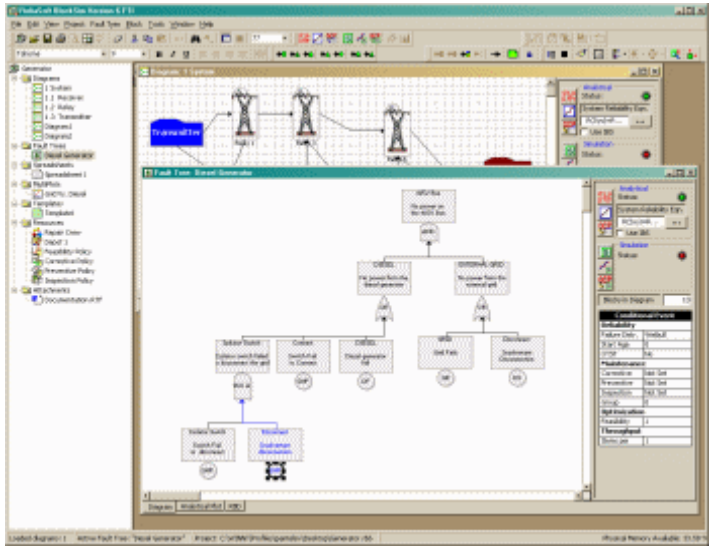
The function of each element is bimodal (true/false, work/fail)

The failure probability of elements can be analysed/described individually

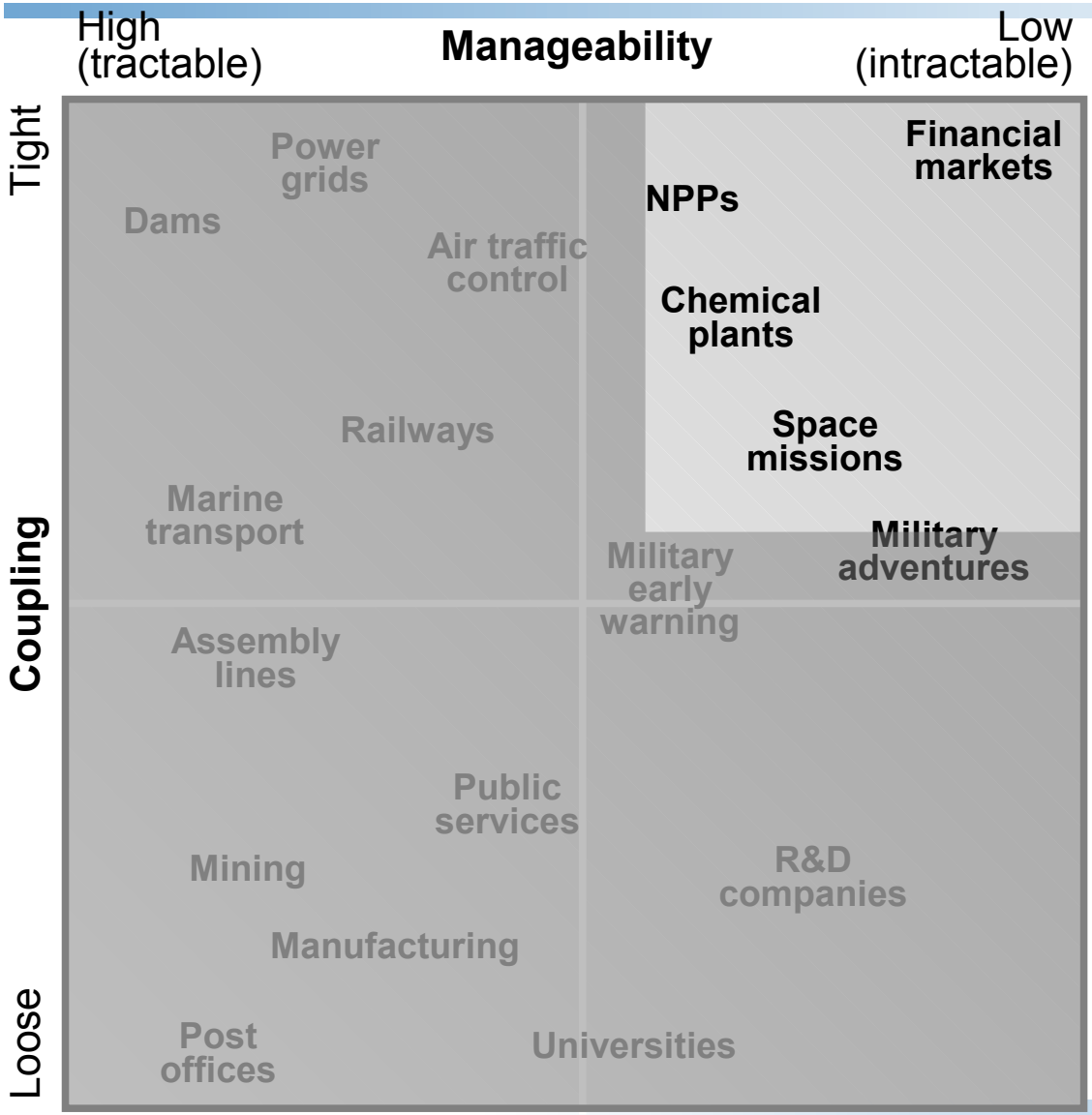
The order or sequence of events is predetermined and fixed

When combinations occur they can be described as linear (tractable, non-interacting)

The influence from context/conditions is limited and quantifiable



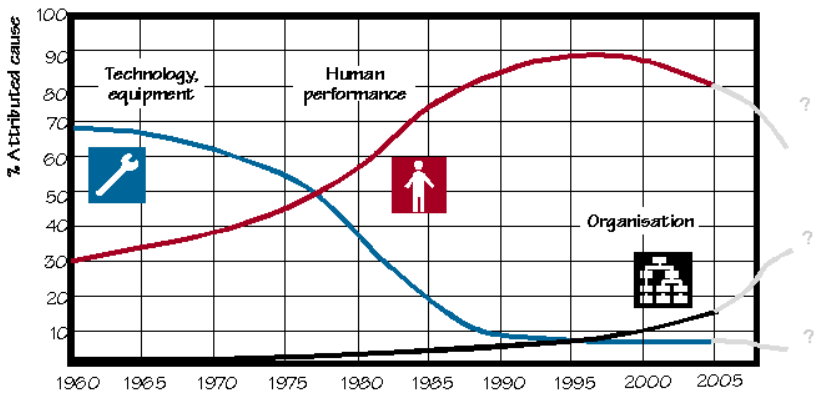
The post-NAT period



Accidents proposed as being normal occurrences.

Large scale systems stretch established methods to the limit.

Human and social factors become recognised as important contributors – both to accident and to safety.



The awakening of HRA

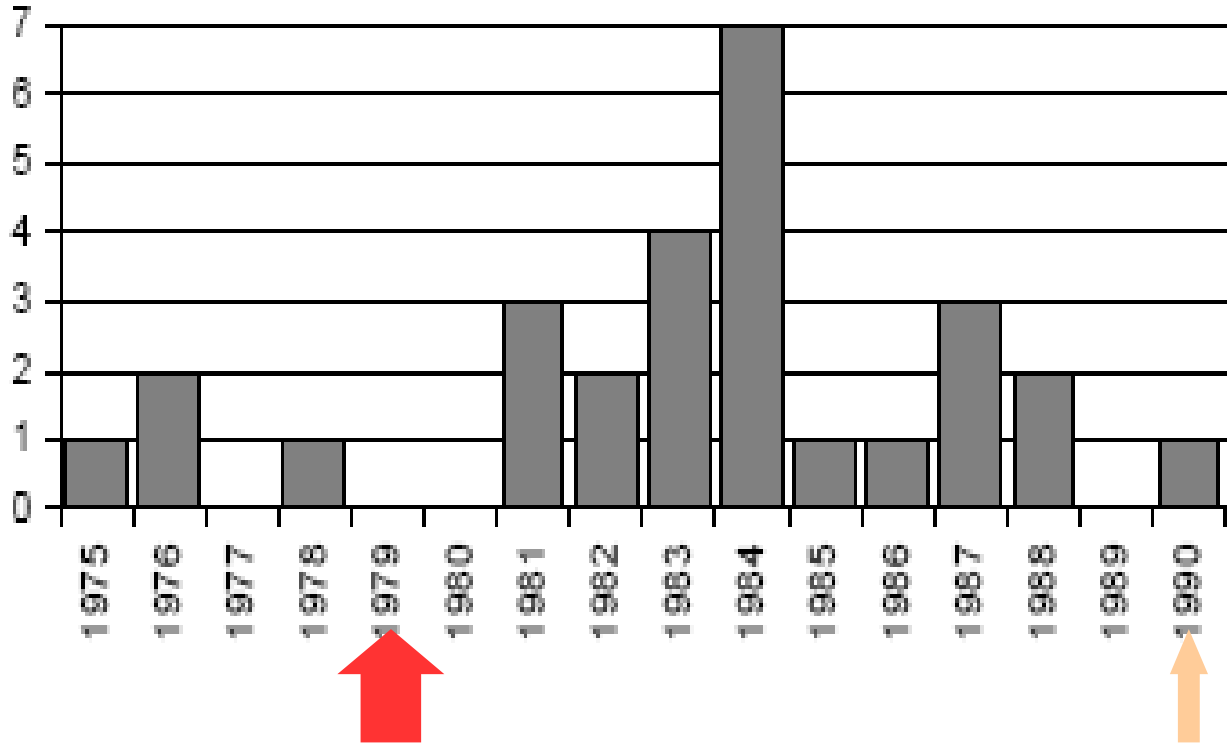


Figure 1: Distribution of HRA approaches according to year of publication.

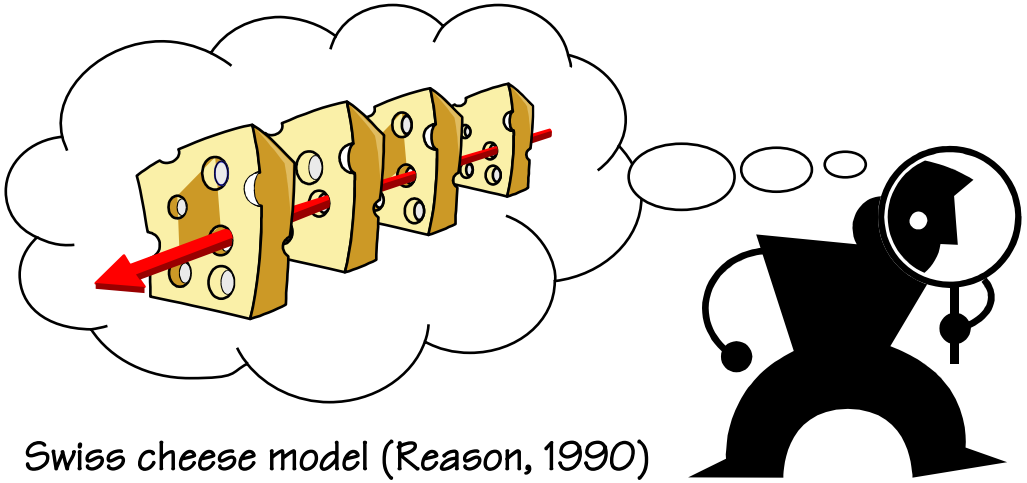
TMI **RESS**

TMI-2 (1979)

TIM-2 underlined the importance of the human factor, and gave rise to the development of a large number of different assessment methods.

Understanding safety: linear models

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



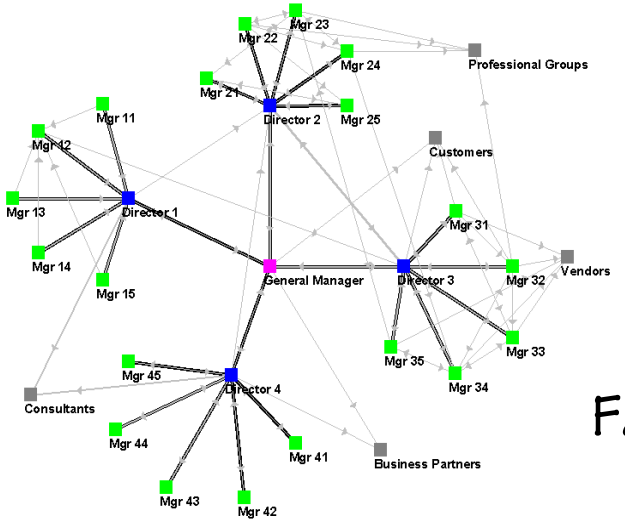
Swiss cheese model (Reason, 1990)

Consequence: Accidents are prevented by strengthening barriers and defences. Safety is ensured by measuring/sampling performance indicators.

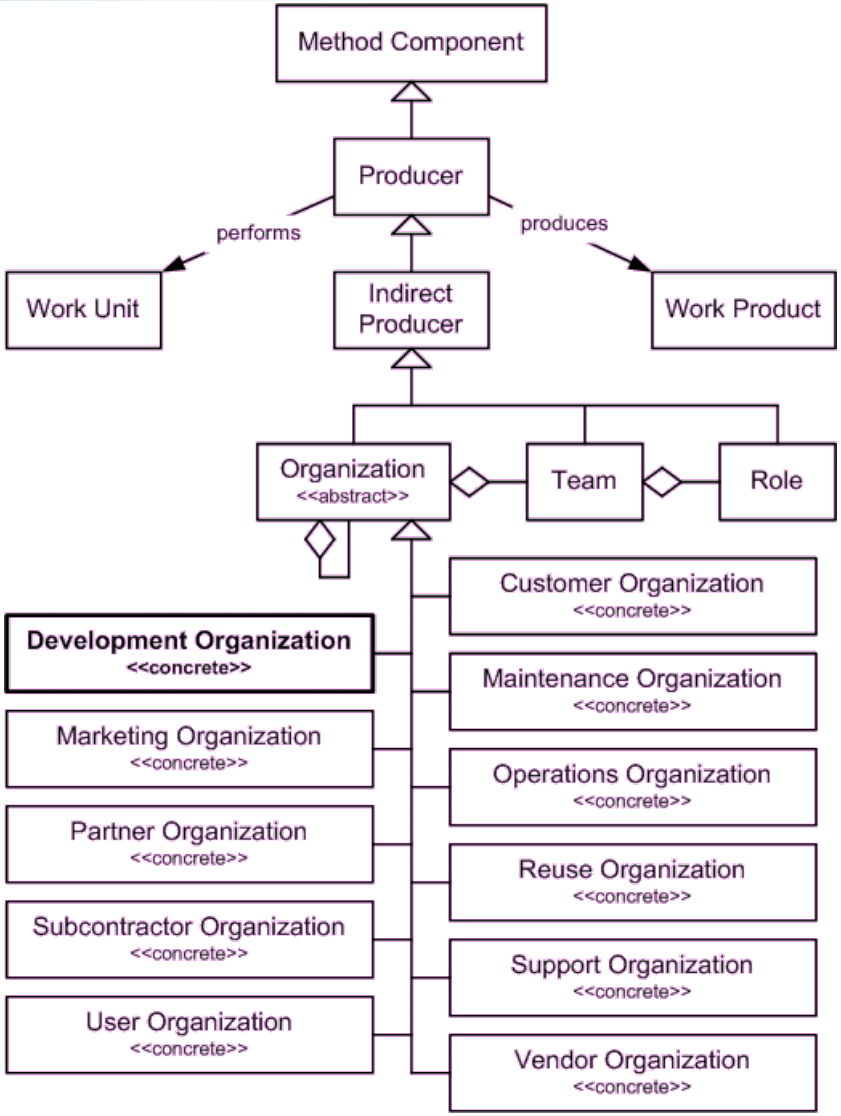
Hazards-risks: Due to degradation of components (organisational, human, technical), hence looking for drift, degradation and weaknesses

The future is described as a combination of past events and conditions.

Organizational malfunctions

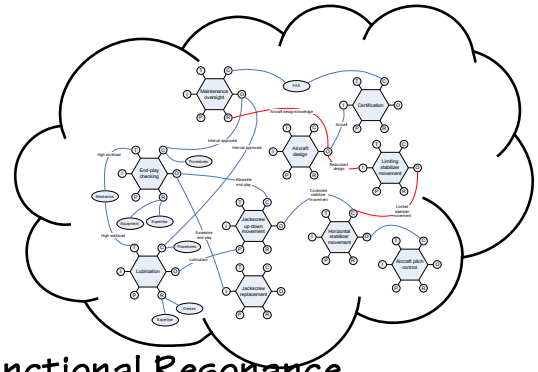


Failure mode?
Failure probability?
MTBF?

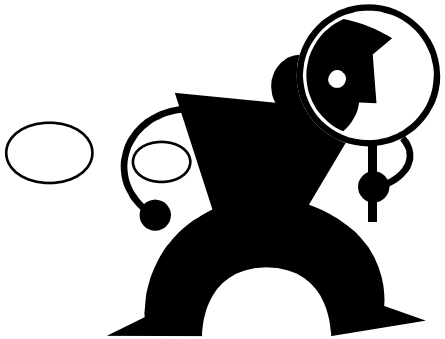


Non-linear accident model

Assumption: Accidents result from unexpected combinations (resonance) of normal performance variability.



Functional Resonance Accident Model



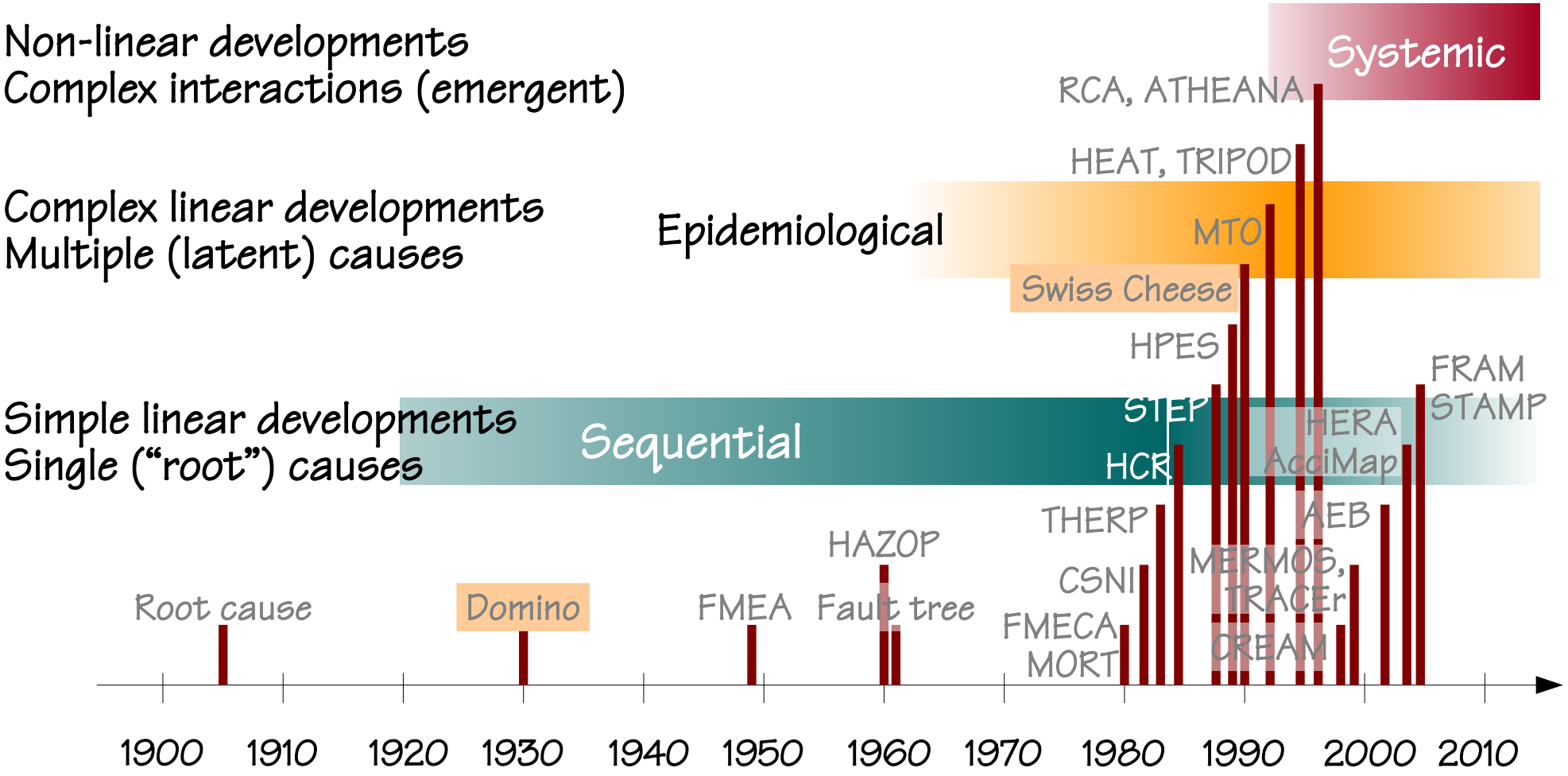
Consequence: Accidents are prevented by monitoring and damping variability. Safety requires constant ability to anticipate future events.

Hazards-risks: Emerge from combinations of normal variability (socio-technical system), hence looking for ETTO* and sacrificing decision

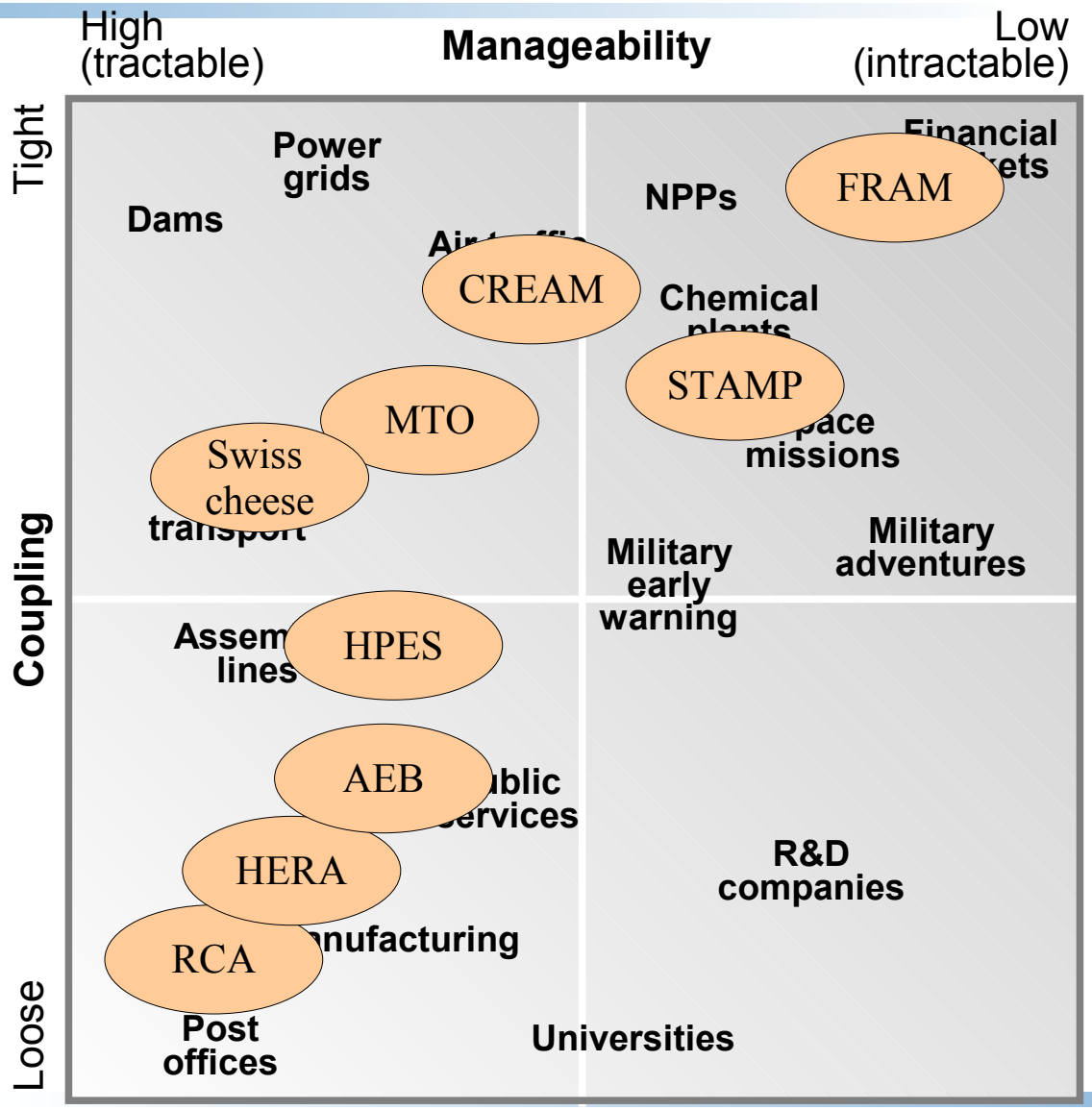
* ETTO = Efficiency-Thoroughness Trade-Off

The future can be understood by considering the characteristic variability of the present.

Accident & Risk Analysis Methods



Relation between methods and systems



Principles for FRAM

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.

Equivalence of successes and failures

FRAM adheres to the resilience engineering view that failures represent the flip side of the adaptations necessary to cope with the real world complexity rather than a failure of normal system functions. Success depends on the ability of organisations, groups and individuals to anticipate risks and critical situations, to recognise them in time, and to take appropriate action; failure is due to the temporary or permanent absence of that ability.

"Knowledge and error flow from the same mental sources, only success can tell one from the other."
(Ernst Mach, 1838-1916; "Knowledge and error", 1905)

Success and failure

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.

Most systems (work environments) and tasks are underspecified. Work can therefore not simply follow prescriptions / procedures). Individuals and organisations must adjust to the current conditions in everything they do.

- 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.
- Failure 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.

Principle of approximate adjustments

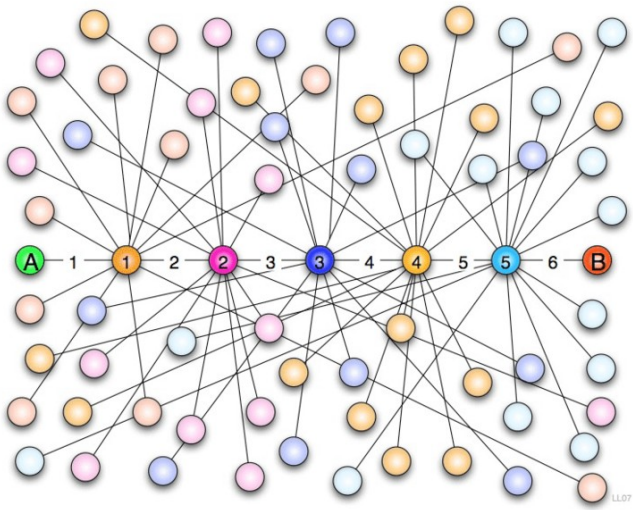
Systems are so complex that work situations always are underspecified – hence partly unpredictable

Few – if any – tasks can successfully be carried out unless procedures and tools are adapted to the situation. Performance variability is both normal and necessary.

Because many socio-technical systems are intractable, the conditions of work never completely match what has been specified or prescribed. Individuals, groups, and organisations must normally adjust their performance so that it can succeed under the existing conditions, specifically the actual resources and requirements. Because resources (time, manpower, information, etc.) always are finite, such adjustments are invariably approximate rather than exact.

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. But the variability from multiple functions may combine in unexpected ways, leading to consequences that are disproportionally large, hence produce a non-linear effect. 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.

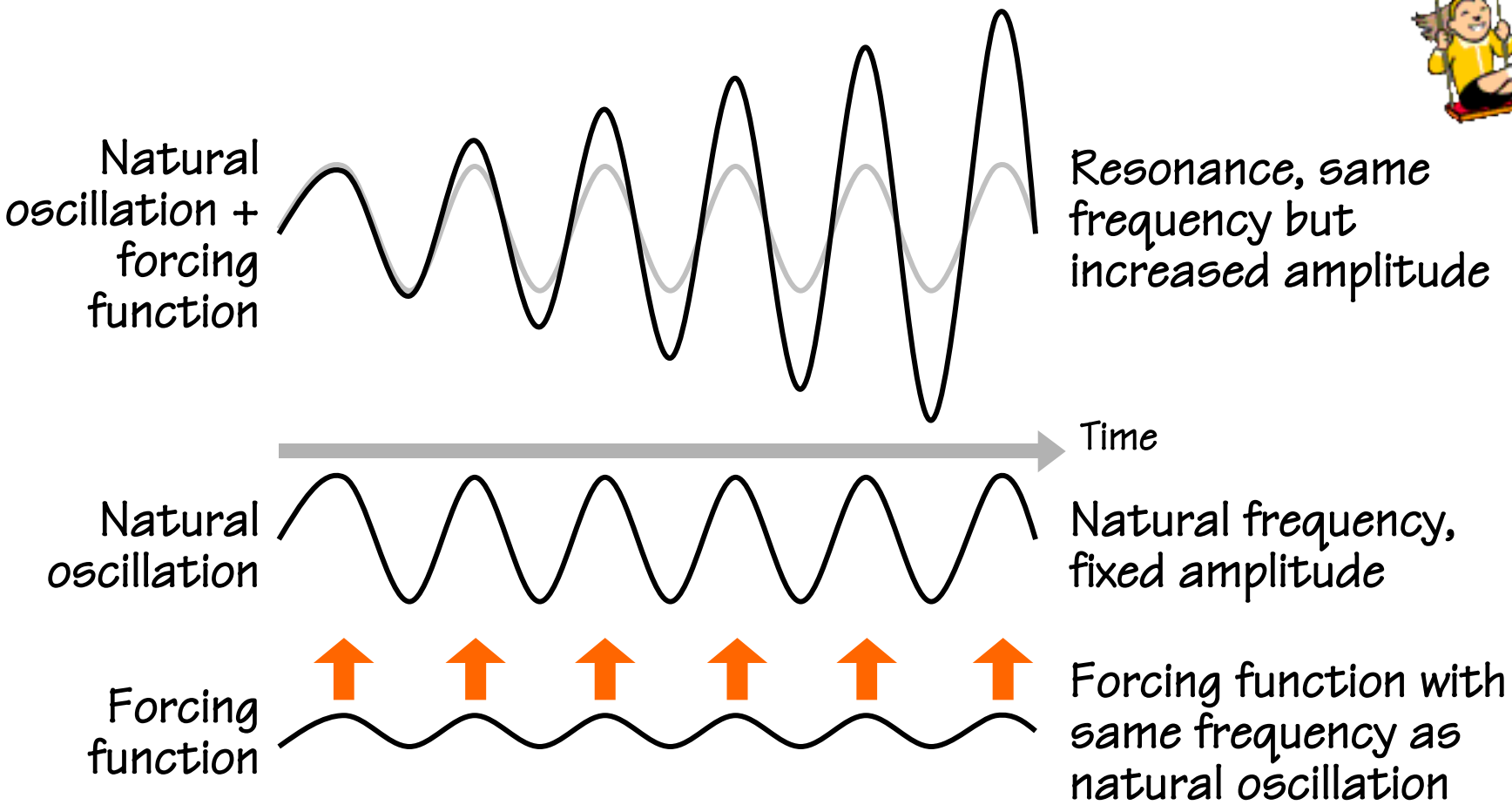
Principle of functional resonance

The variability of a number of functions may every now and then resonate, i.e., reinforce each other and thereby cause the variability of one function to exceed normal limits. The consequences may spread through tight couplings rather than via identifiable and enumerable cause-effect links, e.g., as described by the Small World Phenomenon. This can be described as a resonance of the normal variability of functions, hence as functional resonance. The resonance analogy emphasises that this is a dynamic phenomenon, hence not attributable to a simple combination of causal links.

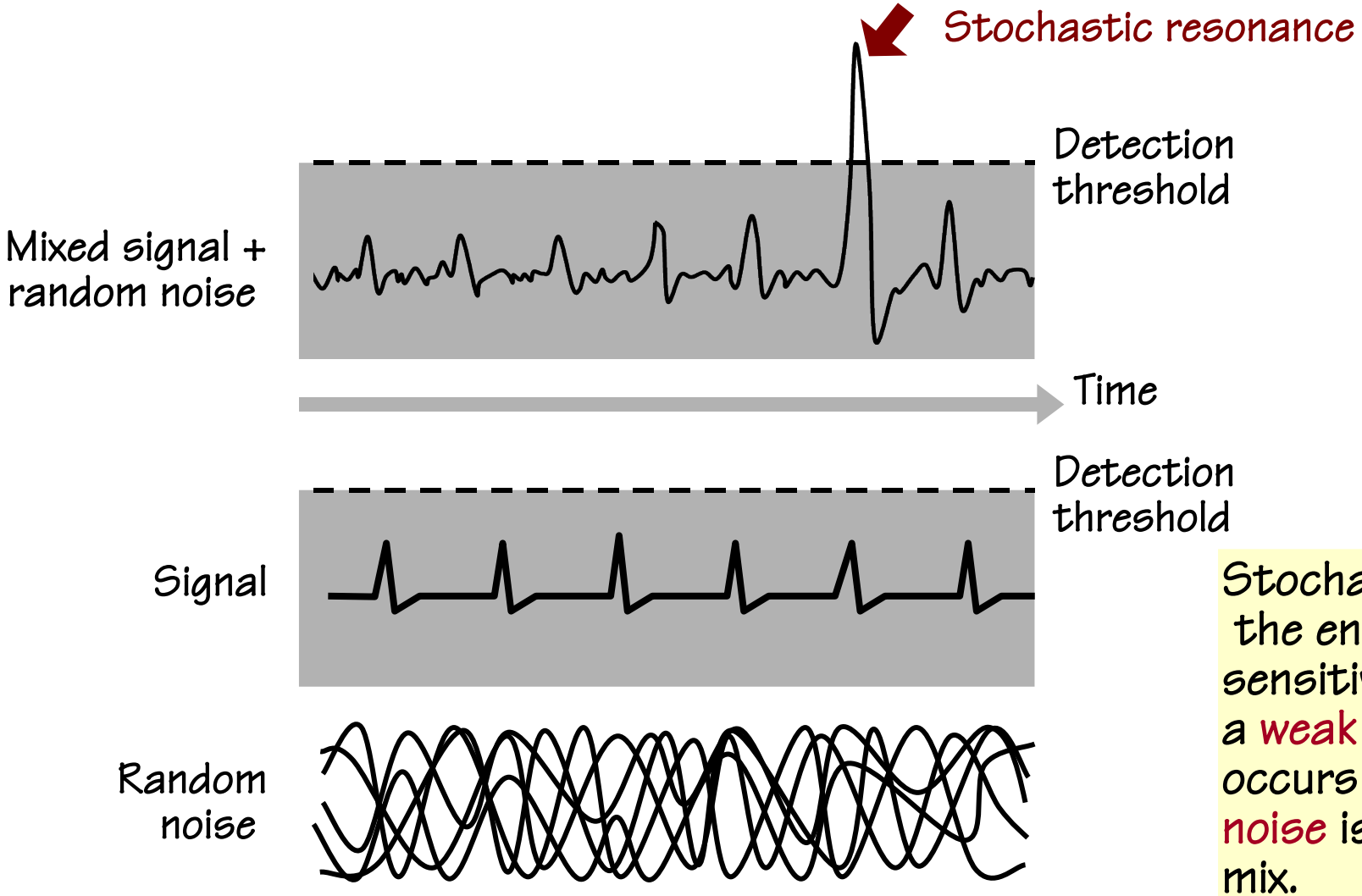
Ways of looking at the future:

As a repetition or recurrence of the past (deterministic or probabilistic).
As a linear extrapolation of the past (combinatorial, probabilistic).
As randomly occurring events (defaitism).
As a non-linear but also non-random development (functional resonance),

Resonance



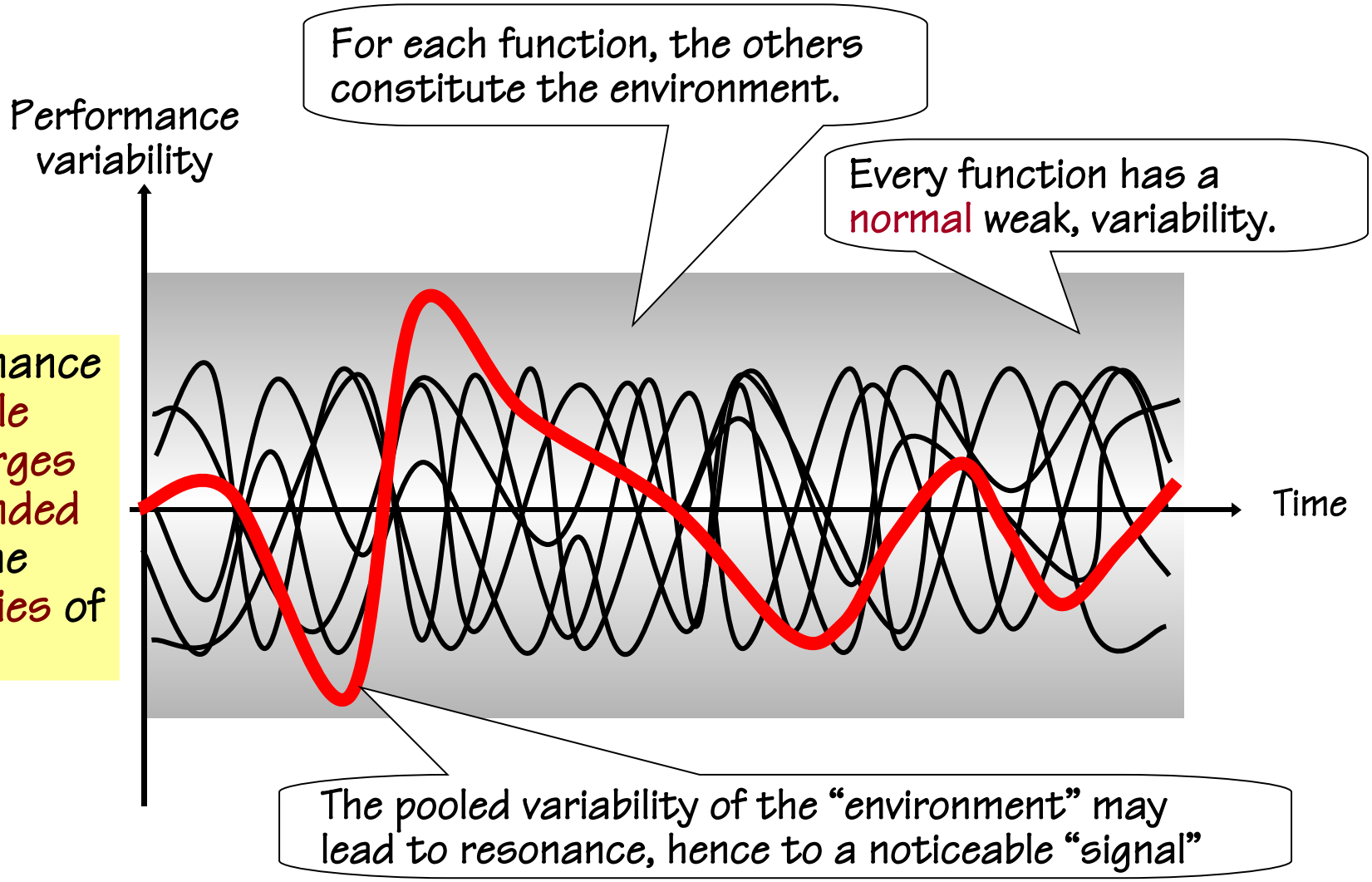
Stochastic resonance



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 accident model

Functional resonance is the detectable signal that emerges from the unintended interaction of the normal variabilities of many signals.

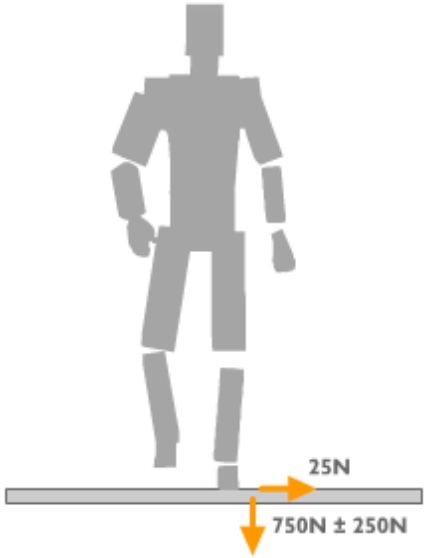


London Millennium Bridge

Opened June 10, 2000

Closed June 12, 2000.
Reason: bridge swayed severely as people walked across it.

Reopened after reconstruction, January 2002



Traffic and randomness

Traffic is a system in which millions of cars every day move so that their driving paths cross each other and critical situations arise due to pure random processes:
cars meet with a speed difference of 100 to more than 200 km/h, separated only by a few meters, with variability of the drivers' attentiveness, the steering, the lateral slope of the road, wind and other factors.

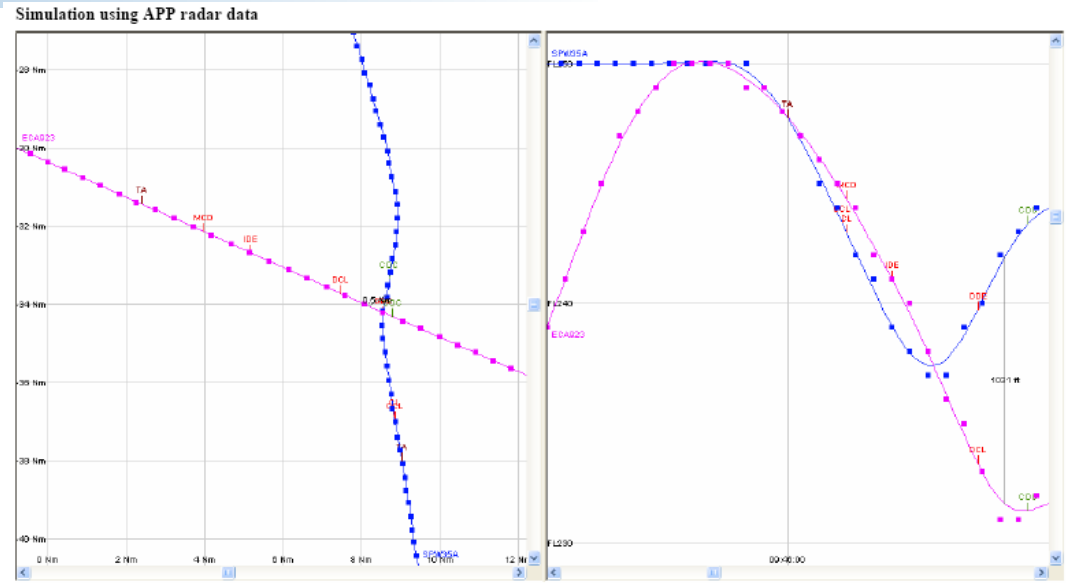
Drivers learn by experience the dimensions of the own car and of other cars, how much space is needed and how much should be allocated to other road users, the maximum speed to approach a curve ahead, etc. If drivers anticipate that these minimum safety margins will be violated, they will shift behavior.

The very basis of traffic accidents consists of random processes, of the fact that we have complicated traffic system with many participants and much kinetic energy involved.
When millions of drivers habitually drive at too small safety margins and make insufficient allowance for (infrequent) deviant behavior or for (infrequent) coincidences, this very normal behavior results in accidents.

Summala (1985)

Airprox

As the analysis shows there is no root cause. Deeper investigation would most probably bring up further contributing factors. A set of working methods that have been developed over many years, suddenly turn out as insufficient for this specific combination of circumstances.

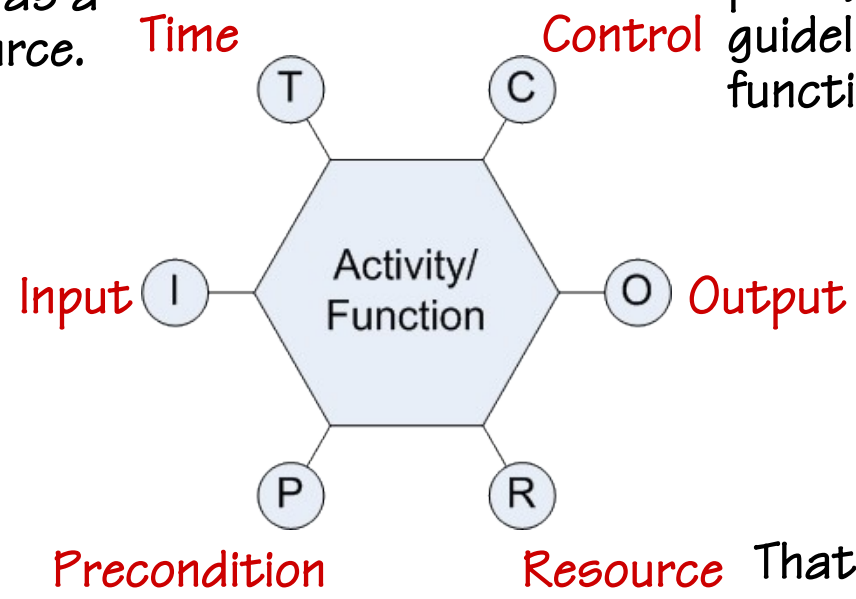


The change of concept was created from the uncertainty of the outcome of the original plan that had been formed during a sector handover. The execution of this and the following concepts were hampered by goal conflicts between two sectors. Time- and environmental- constraints created a demand resource mismatch in the attempt to adapt to the developing situation. This also included coordination breakdowns and automation surprises (TCAS).
The combination of this and further contributing factors of which some are listed above, lead to an airprox with a minimum separation of 1.6NM/400 ft.

FRAM functional unit (module)

Time available: This can be a constraint but can also be considered as a special kind of resource.

That which supervises or adjusts a function. Can be plans, procedures, guidelines or other functions.



That which is used or transformed to produce the output. Constitutes the link to previous functions.

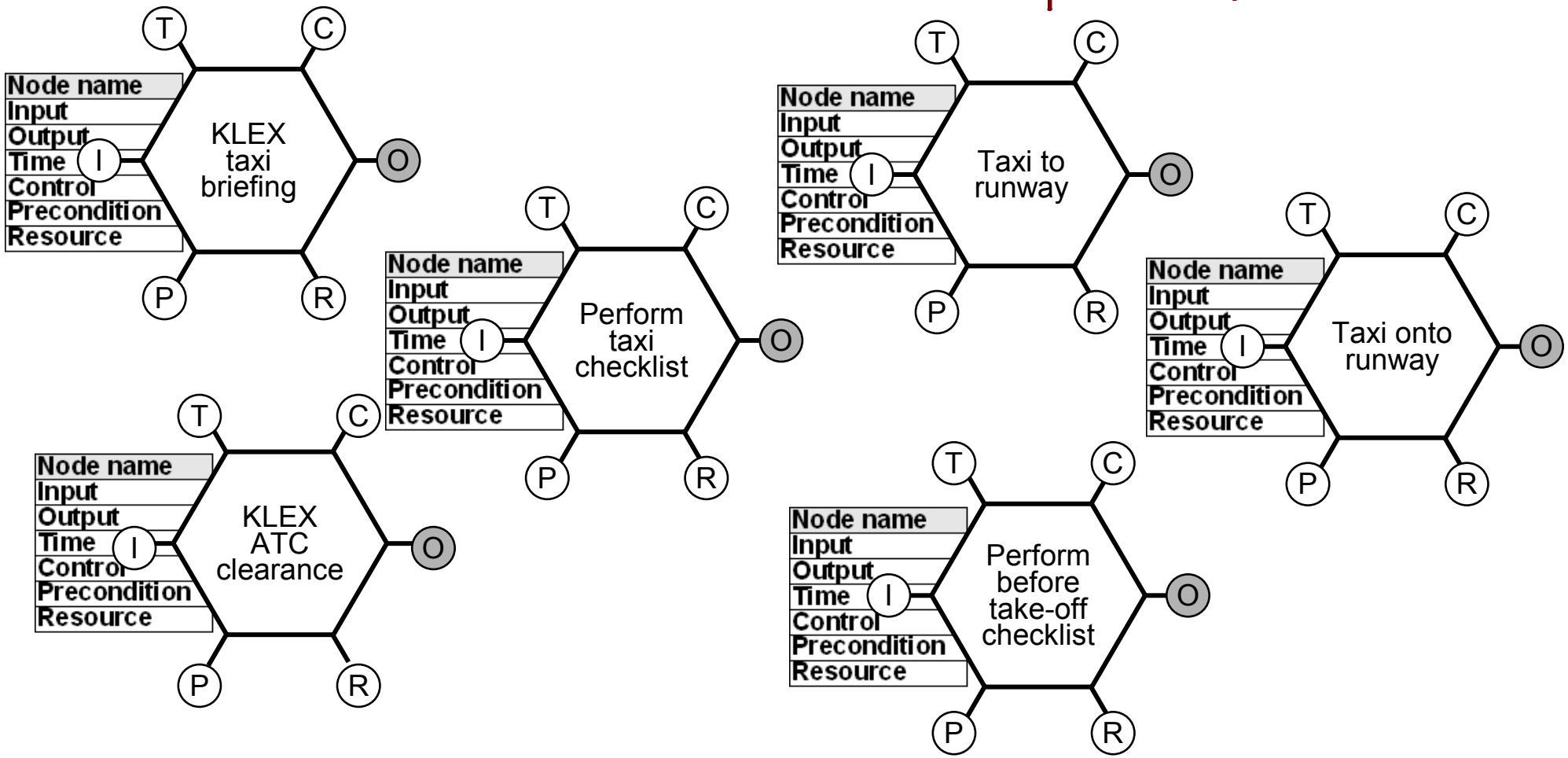
That which is produced by function. Constitute links to subsequent functions.

System conditions that must be fulfilled before a function can be carried out.

That which is needed or consumed by function to process input (e.g., matter, energy, hardware, software, manpower).

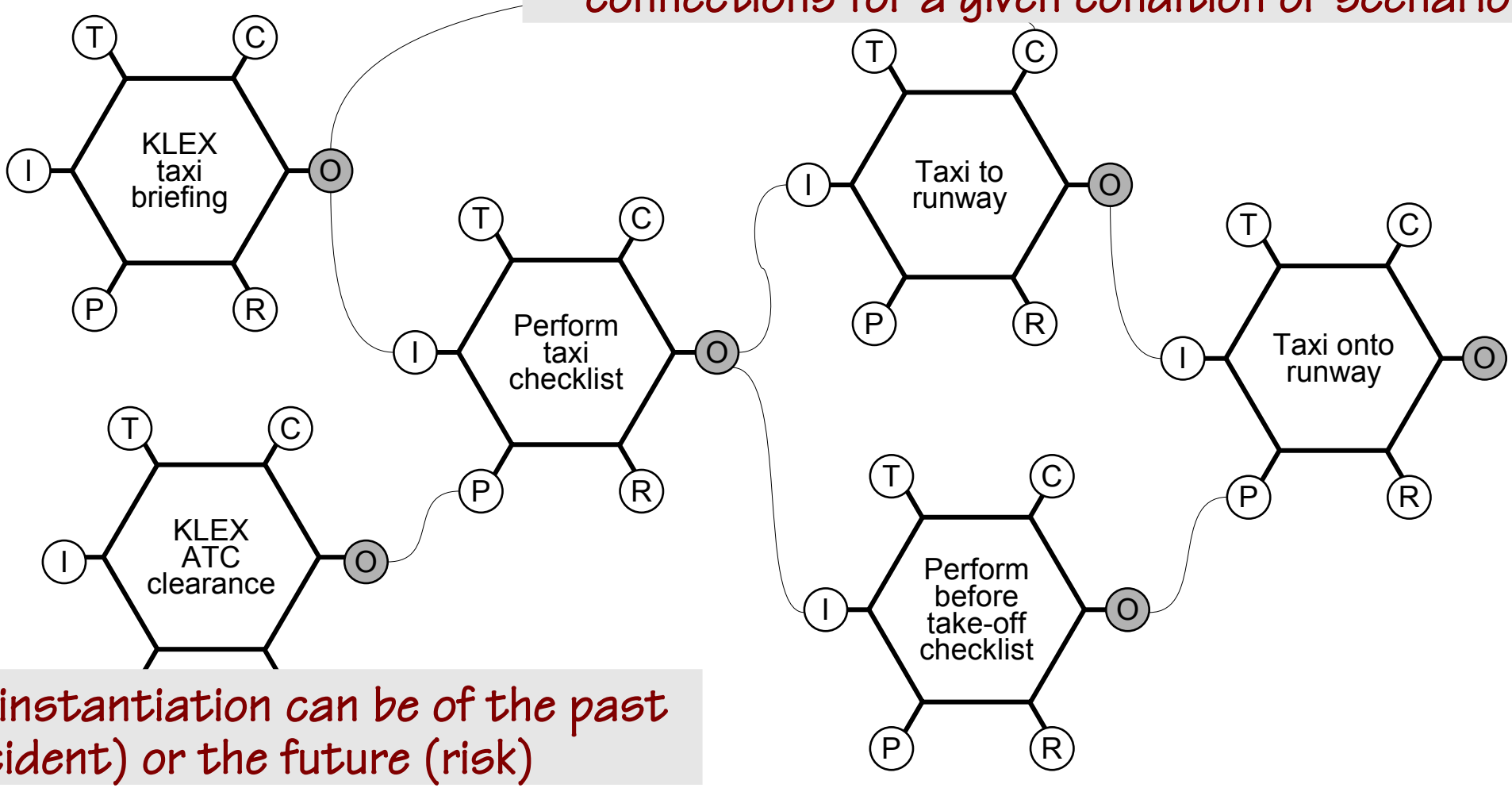
This is a FRAM

The couplings / connections between the nodes of a model are potential, but not actual



This is an instantiation of a FRAM

The links show the instantiation of couplings / connections for a given condition or scenario.



The instantiation can be of the past (accident) or the future (risk)

For the predictive use of FRAM (risk assessment), the basis is often an existing task description or a flowchart.

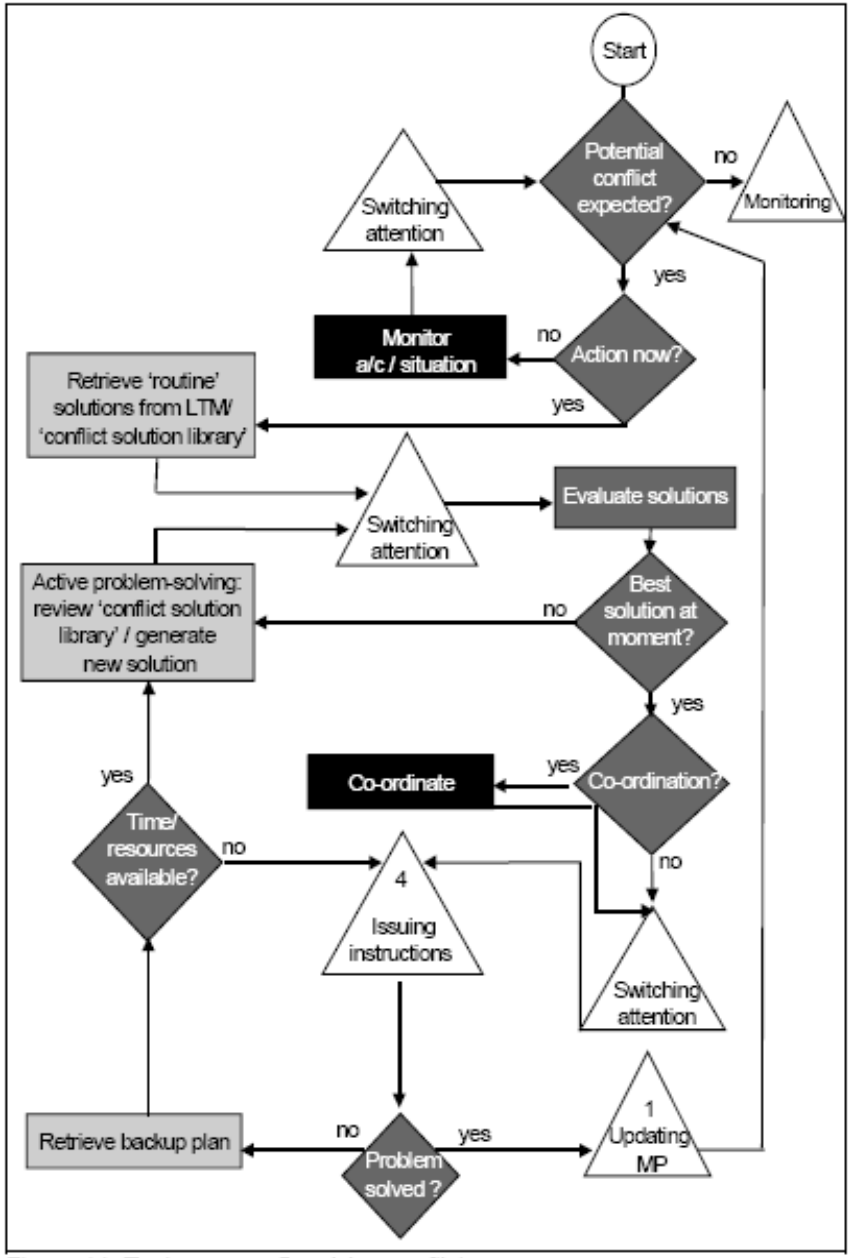
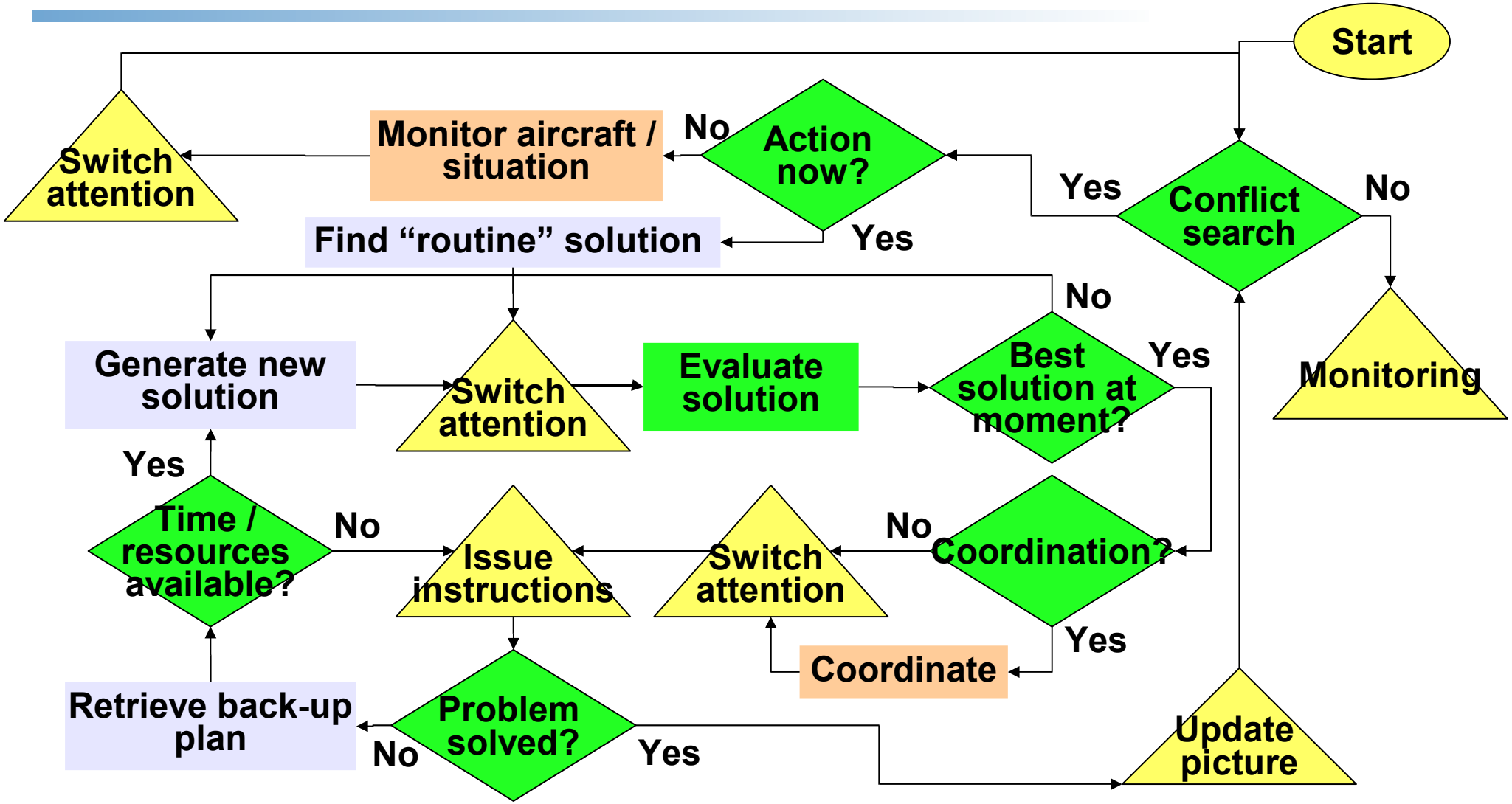


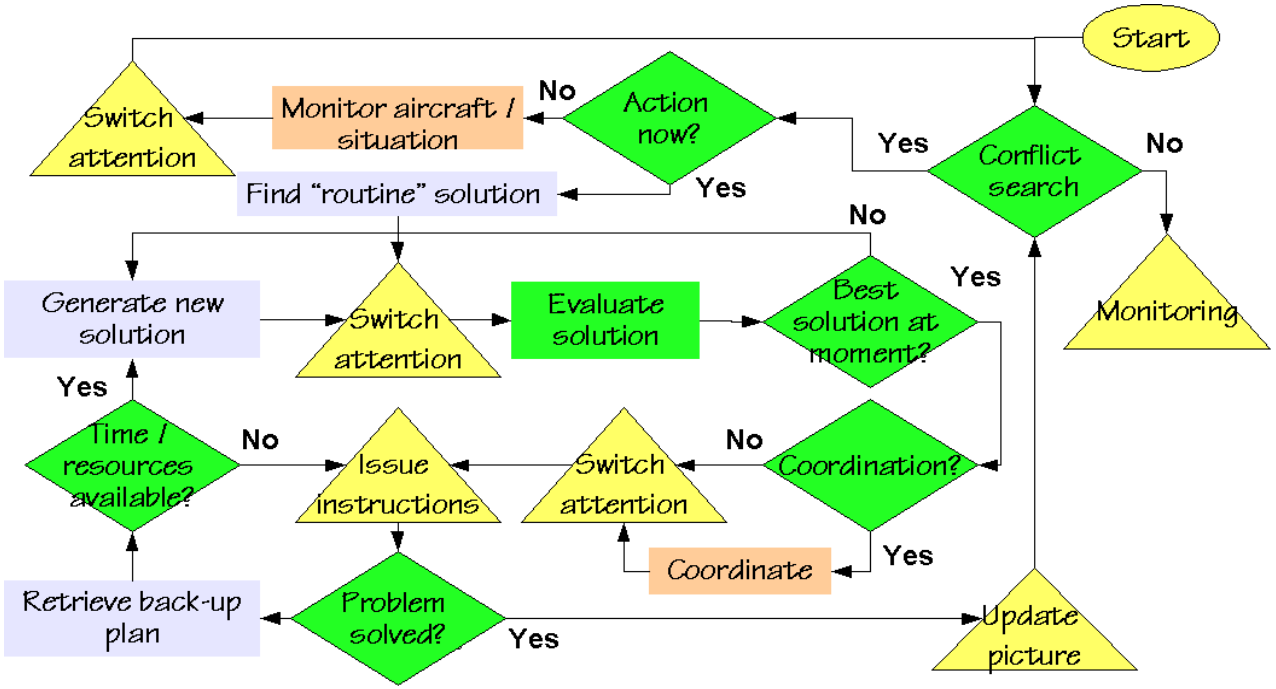
Figure 11: Task process 5: solving conflicts

EATMP2 (1999, p. 47): Solving Conflicts

EATMP2 (1999, p. 47): Solving Conflicts

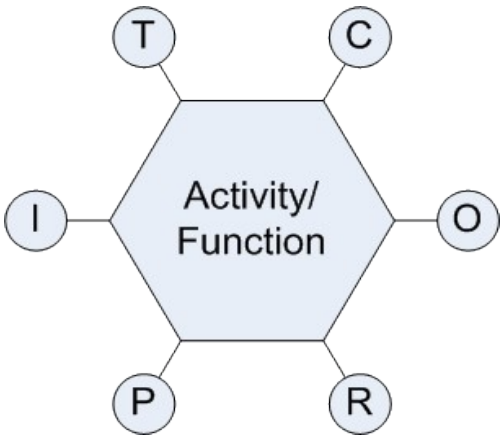


Which functions should be analysed?

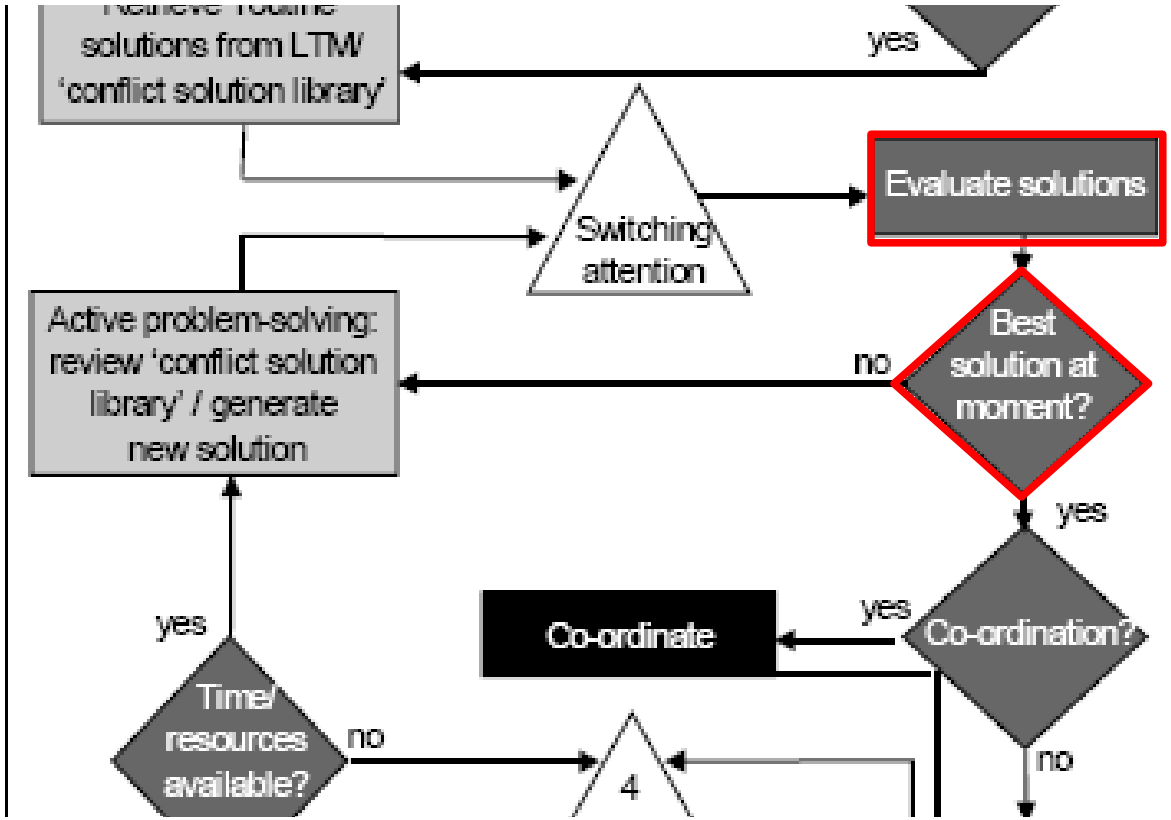


Conflict search and monitoring
Determine action urgency

Find solution (routine, novel)
Evaluate and assess solution
Implement solution

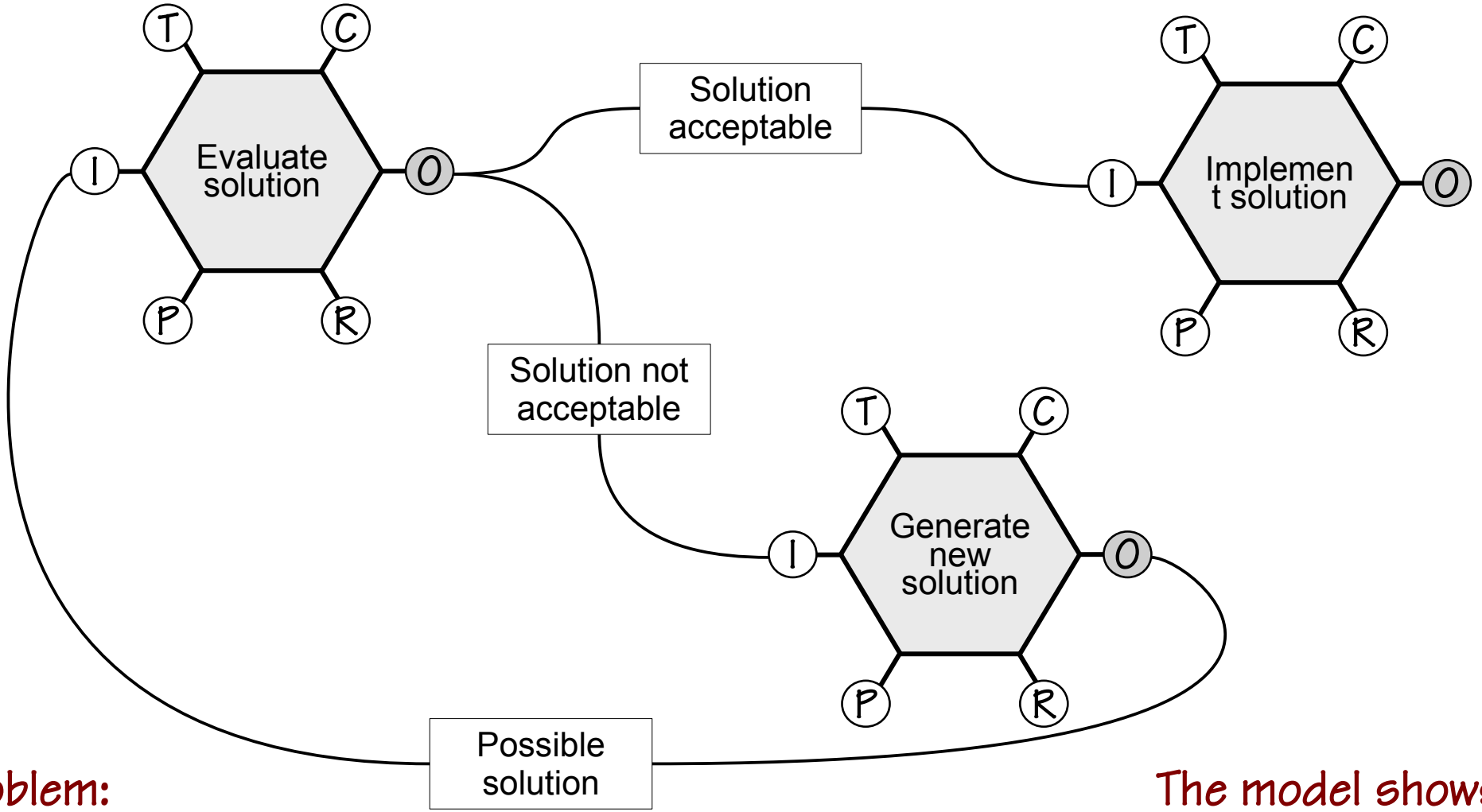


Evaluate and assess solution



It is almost irresistible to model this in the same way with FRAM.
But how should the decision node be described?

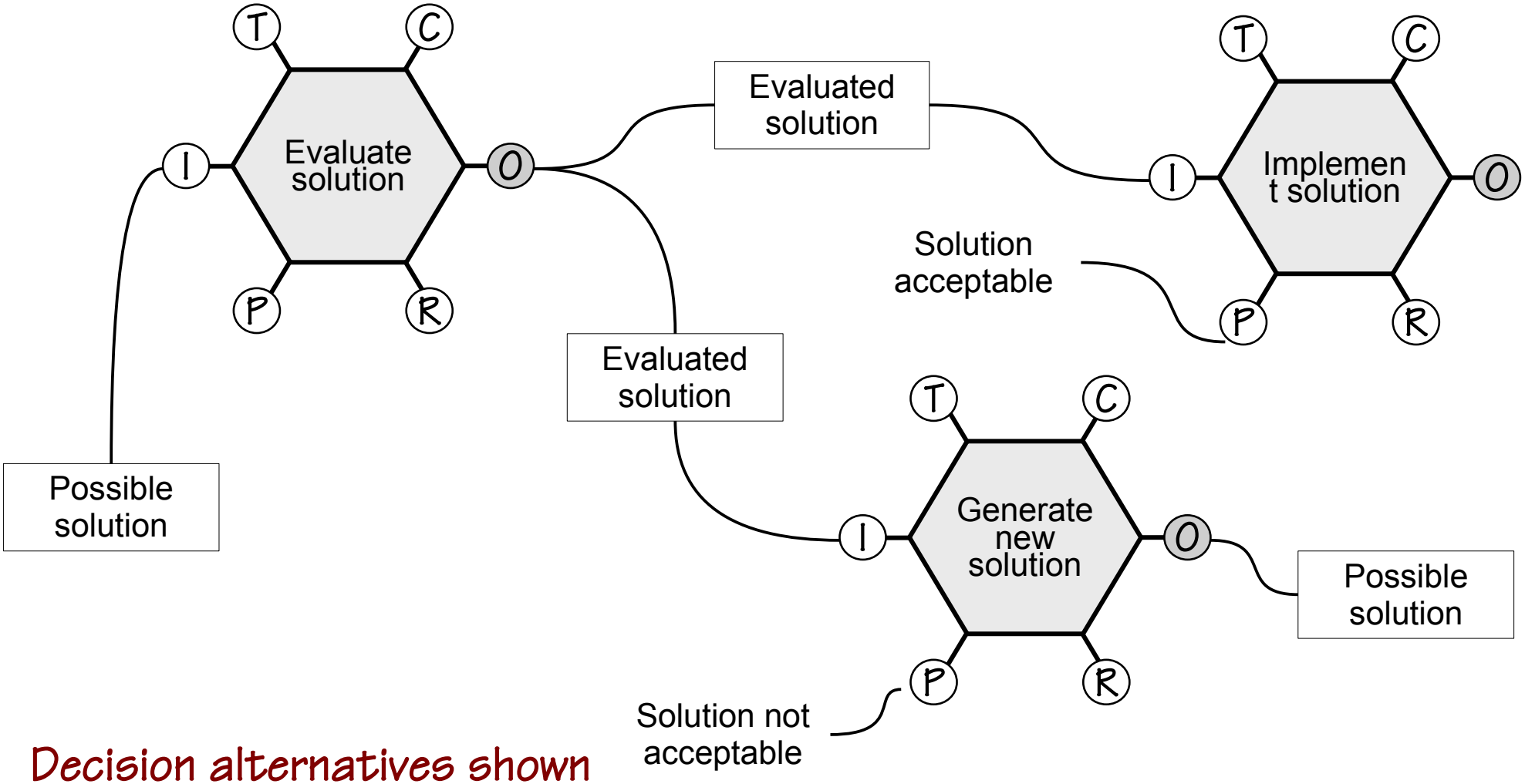
FRAM as a flow chart?



Problem: alternative outputs!

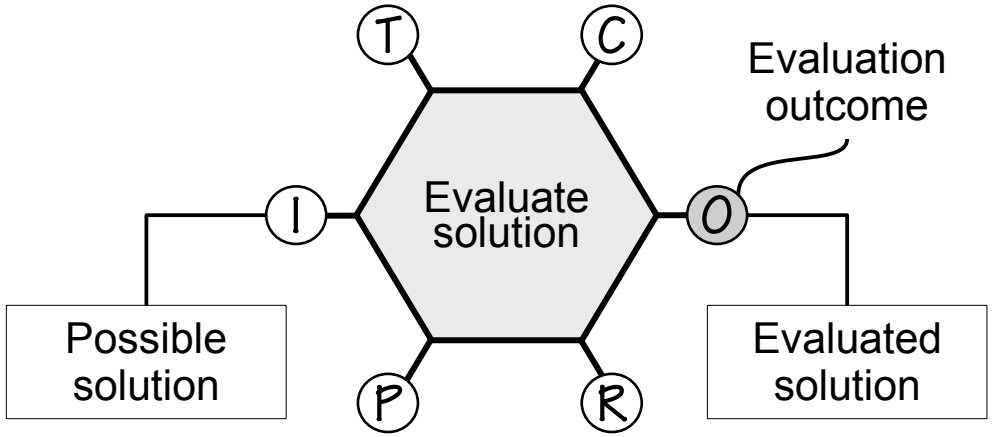
The model shows multiple instances!

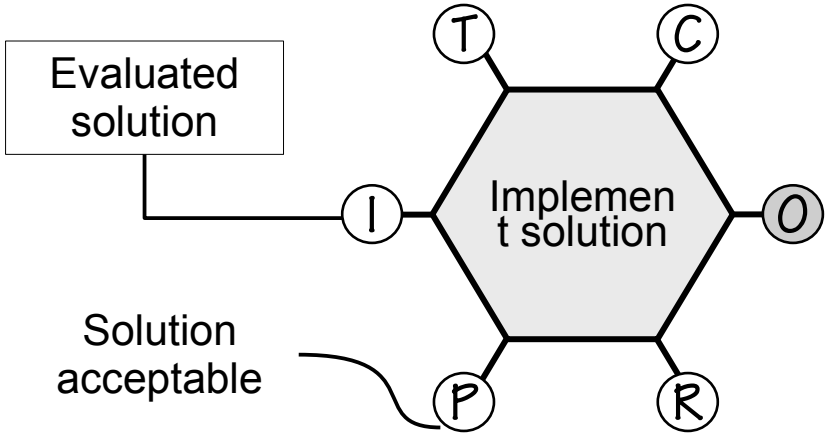
FRAM showing actual couplings



Decision alternatives shown as outputs + preconditions

FRAM showing potential couplings

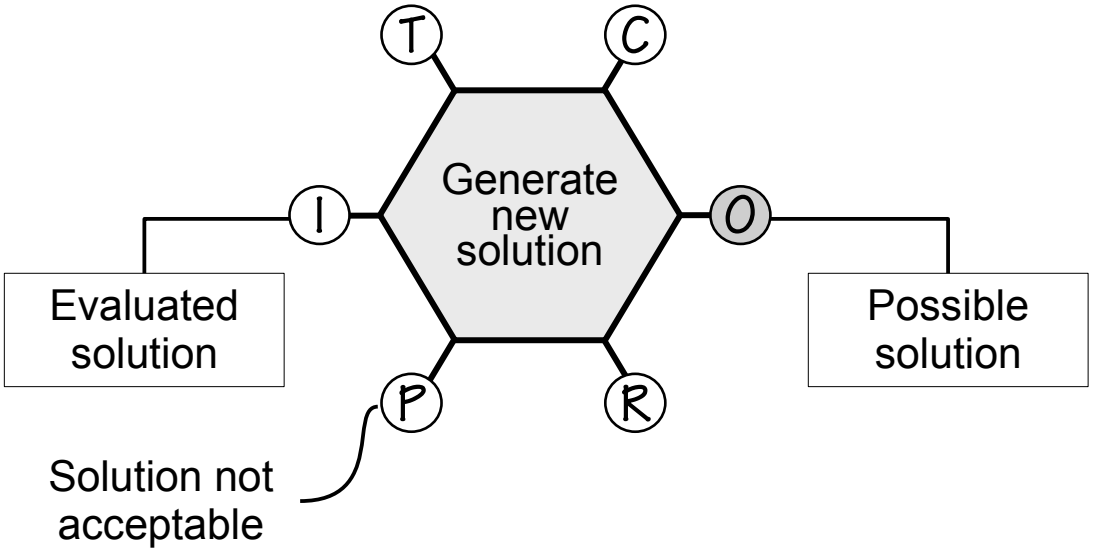




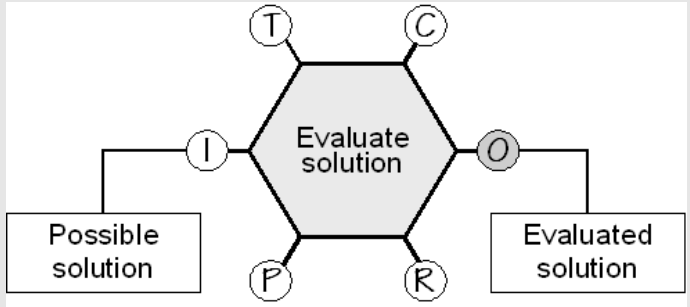
Decision alternatives shown as output + state (evaluation outcome)

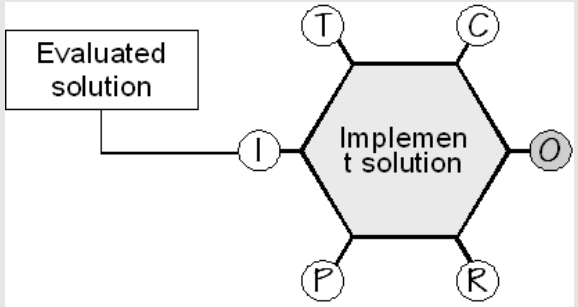
States can be changed and interrogated

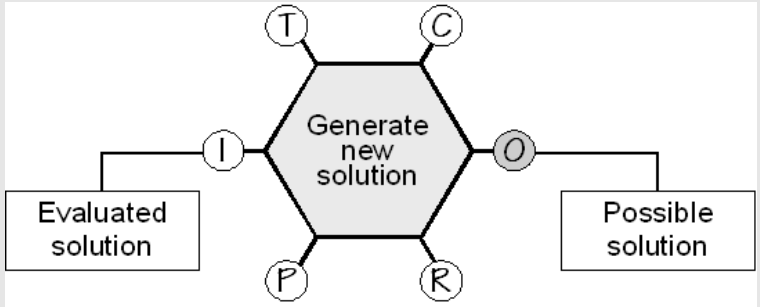
States are not functions!



FRAM: functions and states







FRAM Functions

Evaluation outcome

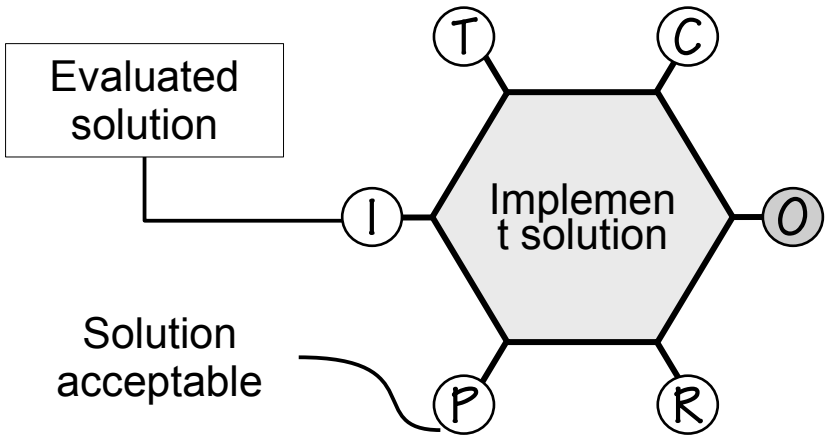
FRAM States

FRAM functions can set and interrogate states

FRAM: performance variability

The performance may be variable, e.g., because time is too short (or too long), because resources are missing, because controls are inadequate, etc.)

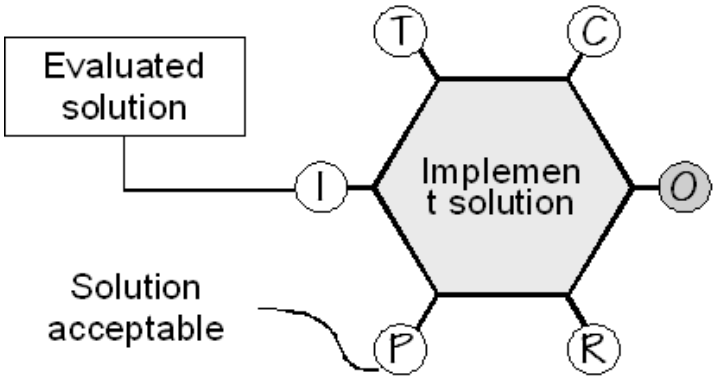
The relation between performance conditions and functions may be
1:n,
n:1, or
n:n

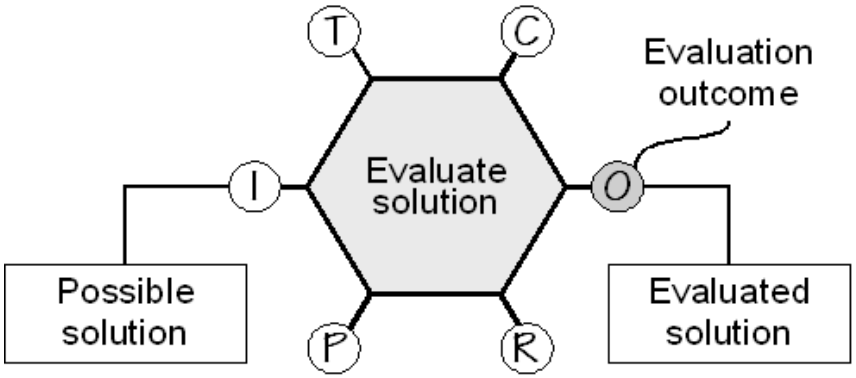


If the performance of a function is variable, it may be carried out even if, e.g., an input is missing or a precondition is not fulfilled.

FRAM: performance variability

If functions are by the same entity:
Efficiency-thoroughness trade-off (ETTO)
Habit
External resource-demand variability
External pressures
Endogenous variability



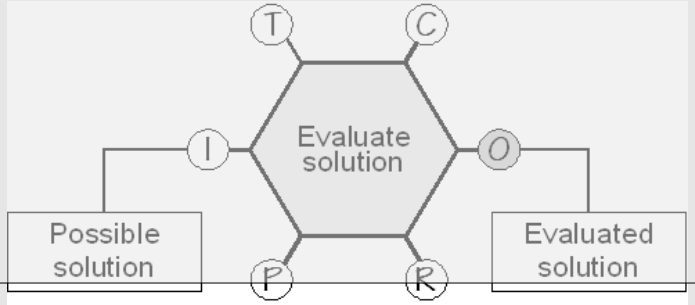


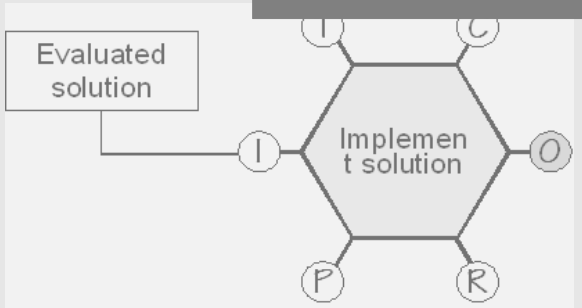
If functions are by different entities:
Working methods,
Expectations (ETTO),
Misunderstanding of cues/signals,
Miscommunication
Exogenous variability

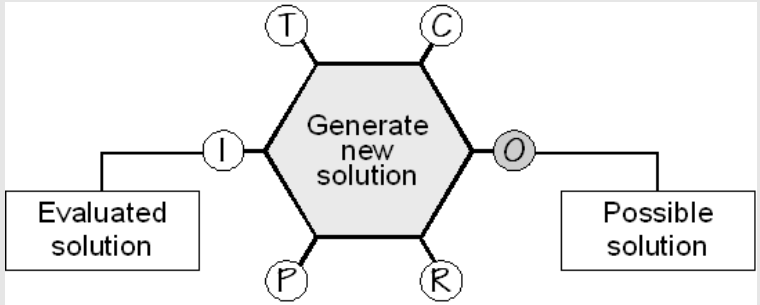
FRAM: conditions, functions and states

Performance conditions can affect functions

FRAM performance conditions







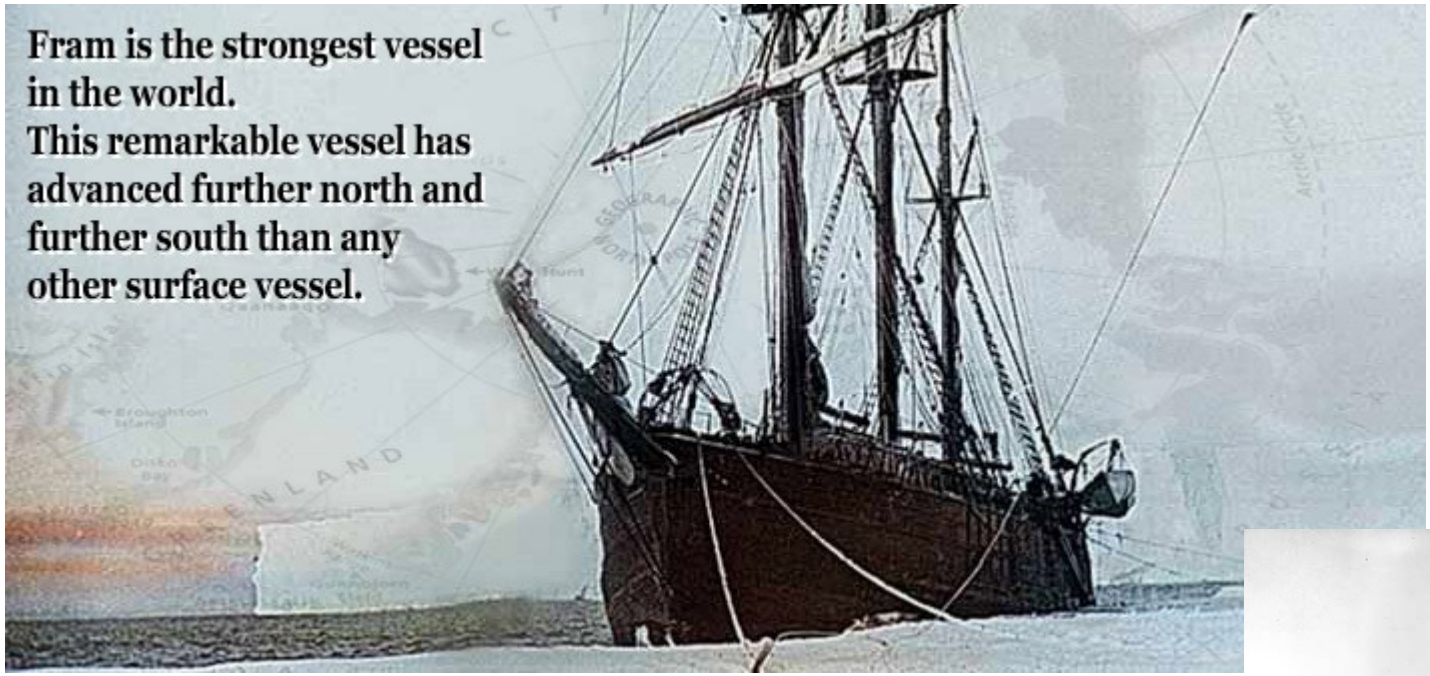
FRAM Functions

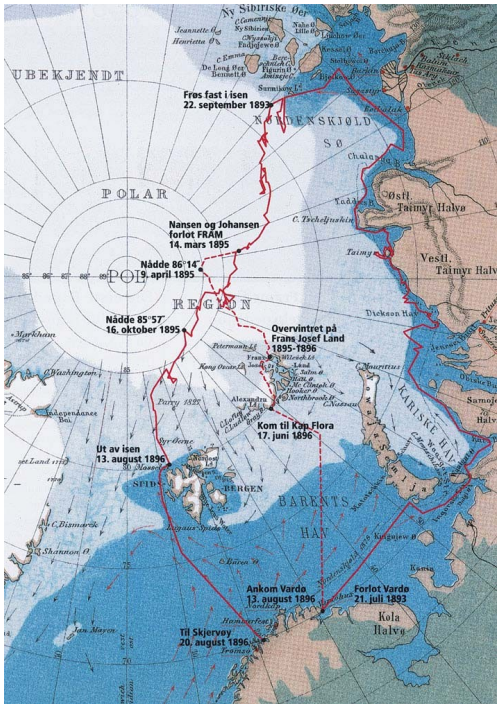
Evaluation outcome

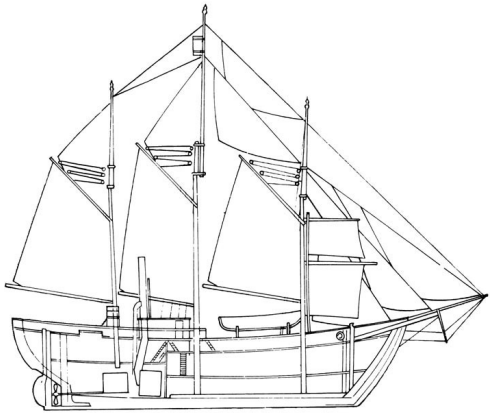
FRAM States

FRAM functions can set and interrogate states

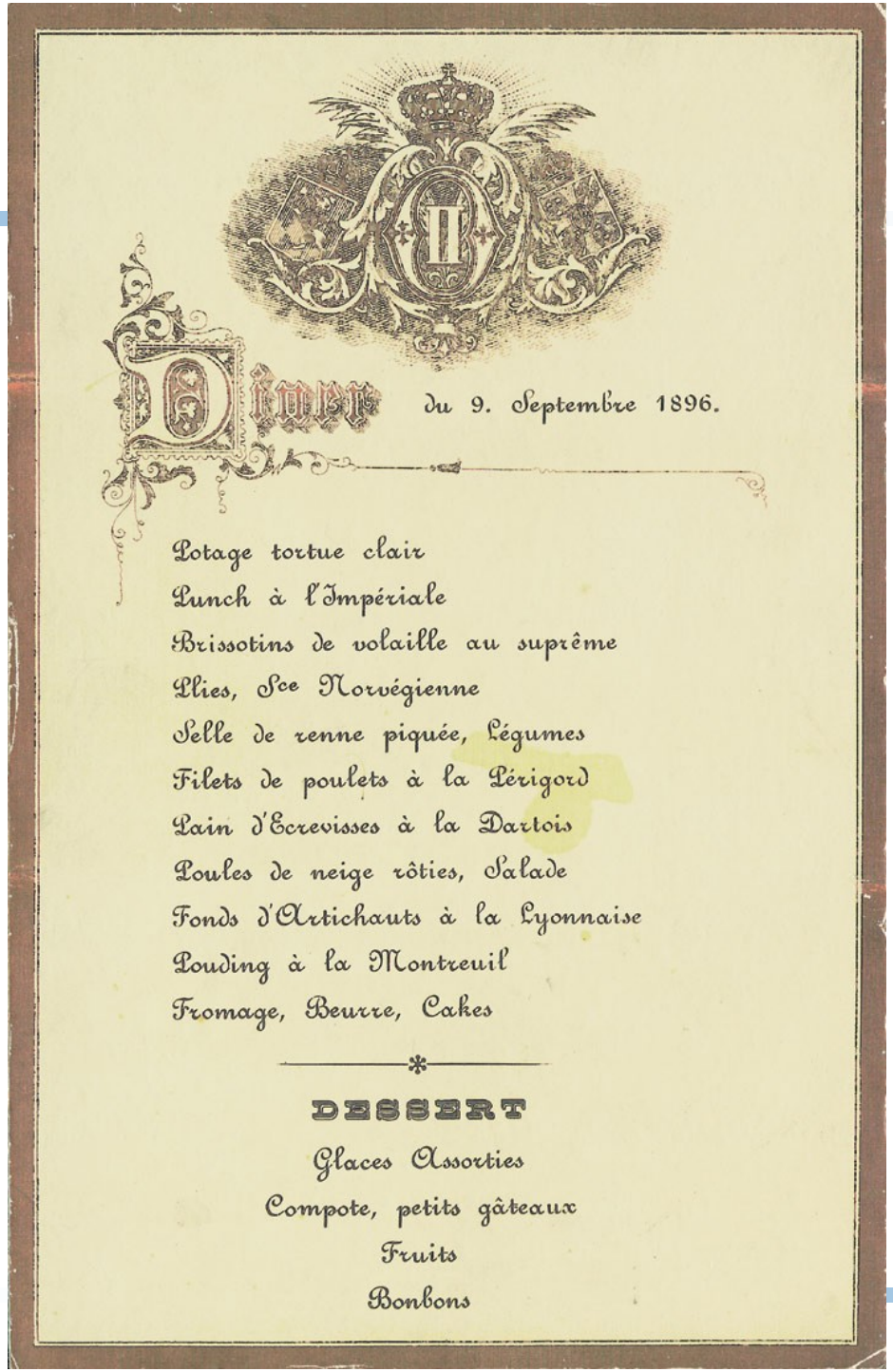
The real FRAM







Design: Colin Archer
Launched: 1892



Dîner du 9. Septembre 1896.

Potage tortue clair
Punch à l'Impériale
Brissotins de volaille au suprême
Plies, Sce Norvégienne
Selle de renne piquée, Légumes
Filets de poulets à la Périgord
Pain d'Ecrevisses à la Dartois
Poules de neige rôties, Salade
Fonds d'Artichauts à la Lyonnaise
Pouding à la Montreuil
Fromage, Beurre, Cakes

DESSERT

Glaces Assorties
Compote, petits gâteaux
Fruits
Bonbons