Capturing an Uncertain Future:
The Functional Resonance Accident Model

Erik Hollnagel
Industrial Safety Chair
ENSMP – Pôle Cindyniques, Sophia Antipolis, France
E-mail: erik.hollnagel@cindy.ensmp.fr

The future is uncertain

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

Accident model / risk model

What may happen?

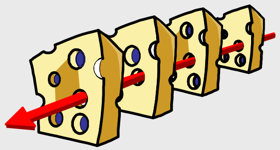
How should we respond?

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

Developments in accident models

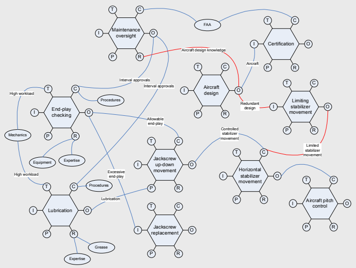
Sequential accident model → Probability of component failures

Decomposable, simple linear



Epidemiological accident model → Likelihood of weakened defenses, combinations

Decomposable, complex linear



Systemic accident model → Coincidences, links, resonance

Non-decomposable, non-linear

THERE HAS BEEN NO SIMILAR DEVELOPMENTS IN RISK MODELS!

What is the nature of accidents?

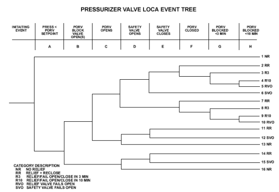
The purpose of risk assessment is to identify in a systematic manner how unwanted outcomes can obtain (= severe accidents).

Traditional view:

- Accidents are due to failures or malfunctions of humans or machines. Example: Event Tree
- Risks can be represented by linear combinations of failures or malfunctions. Example: Fault Tree

Traditional risk assessment is constrained by two assumptions.

- Events develop in a pre-defined sequence.
- The major source of risk is component malfunctions.

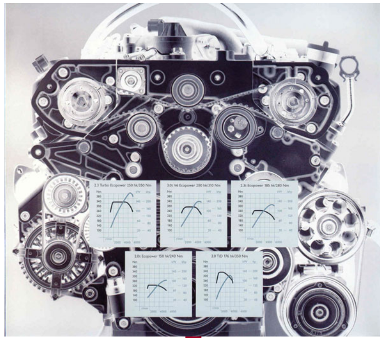


Systemic view:

- Accidents are due to unexpected combinations of actions rather than action failures. Example: ETTO.
- Risks can be represented by non-linear combinations of performance variability. Example: FRAM.

Nature of technical systems

Many identical systems



They can be described bottom-up in terms of components and subsystems.

Decomposition works for technical systems, because they have been designed.

Risks and failures can therefore be analysed relative to individual components and events.

Output (effects) are proportional to input (causes) and predictable from knowledge of the components. Technical systems are linear.

Risk assessment: sequential models

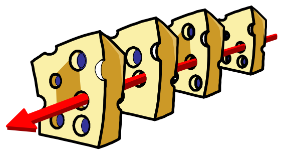
Decomposable, simple linear

Sequential accident model → Probability of component failures

Purpose: find the probability that something "breaks", either at the component level or in simple, logical and fixed combinations.

Human failure is treated at the "component" level.

Decomposable, complex linear



Epidemiological accident model → Likelihood of weakened defenses, combinations

Single failures combined with latent conditions, leading to degradation of barriers and defences.

Nature of socio-technical systems

All systems unique

Must be described top-down in terms of functions and objectives.

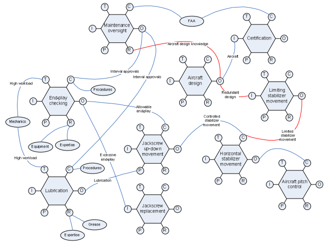
Decomposition does not work for socio-technical systems, because they are emergent.

Risks and failures must therefore be described relative to functional wholes.

Complex relations between input (causes) and output (effects) give rise to unexpected and disproportionate consequences. Socio-technical systems are non-linear.

Risk assessment: Systemic model

Non-decomposable non-linear

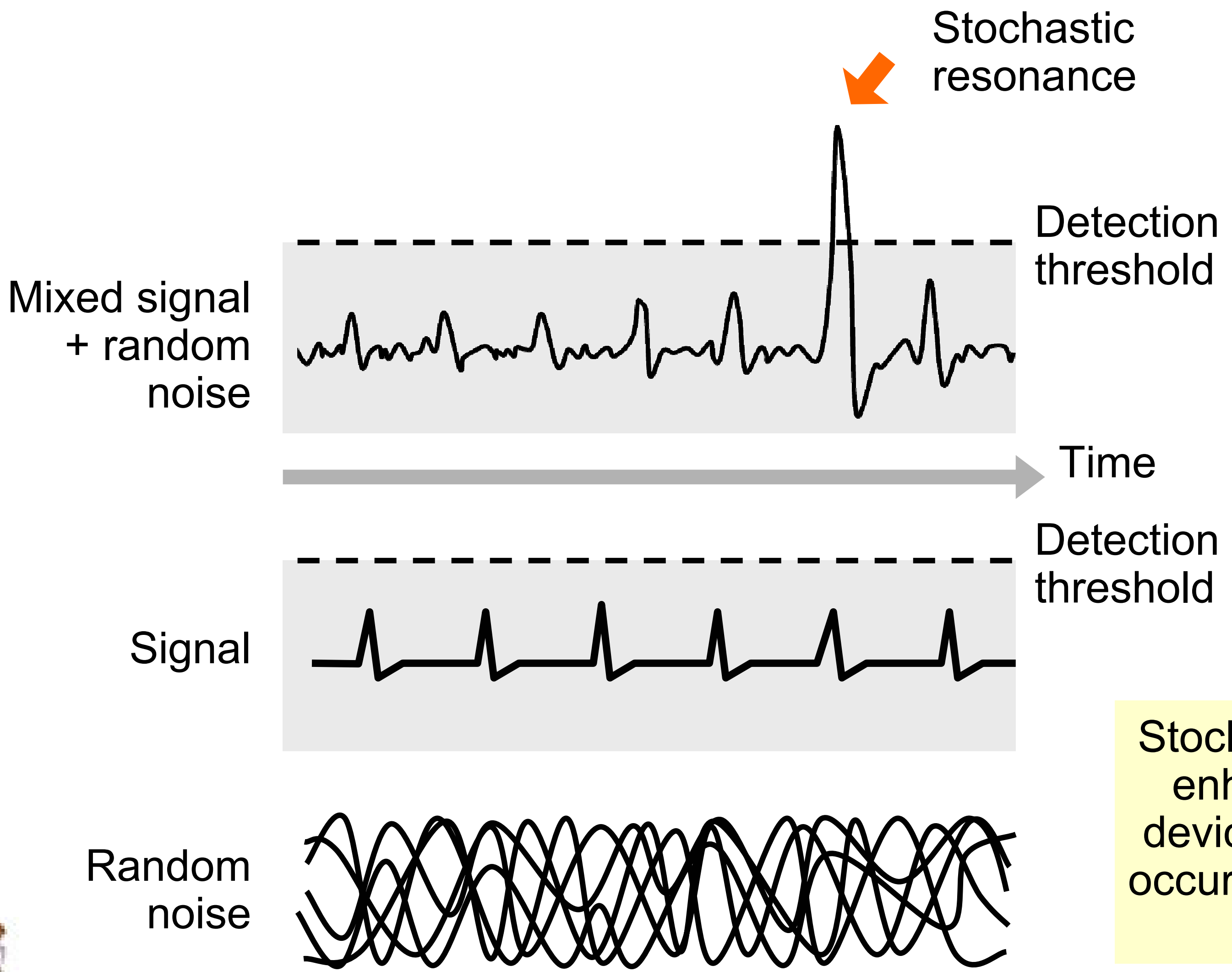


Systemic accident model → Coincidences, links, resonance

Risk assessment goes beyond component failures to look at system dynamics and must consider issues of non-linear risk assessment.

The emergence of failures from normal performance variability can be explained by the concept of functional resonance, derived from the theory of stochastic resonance.

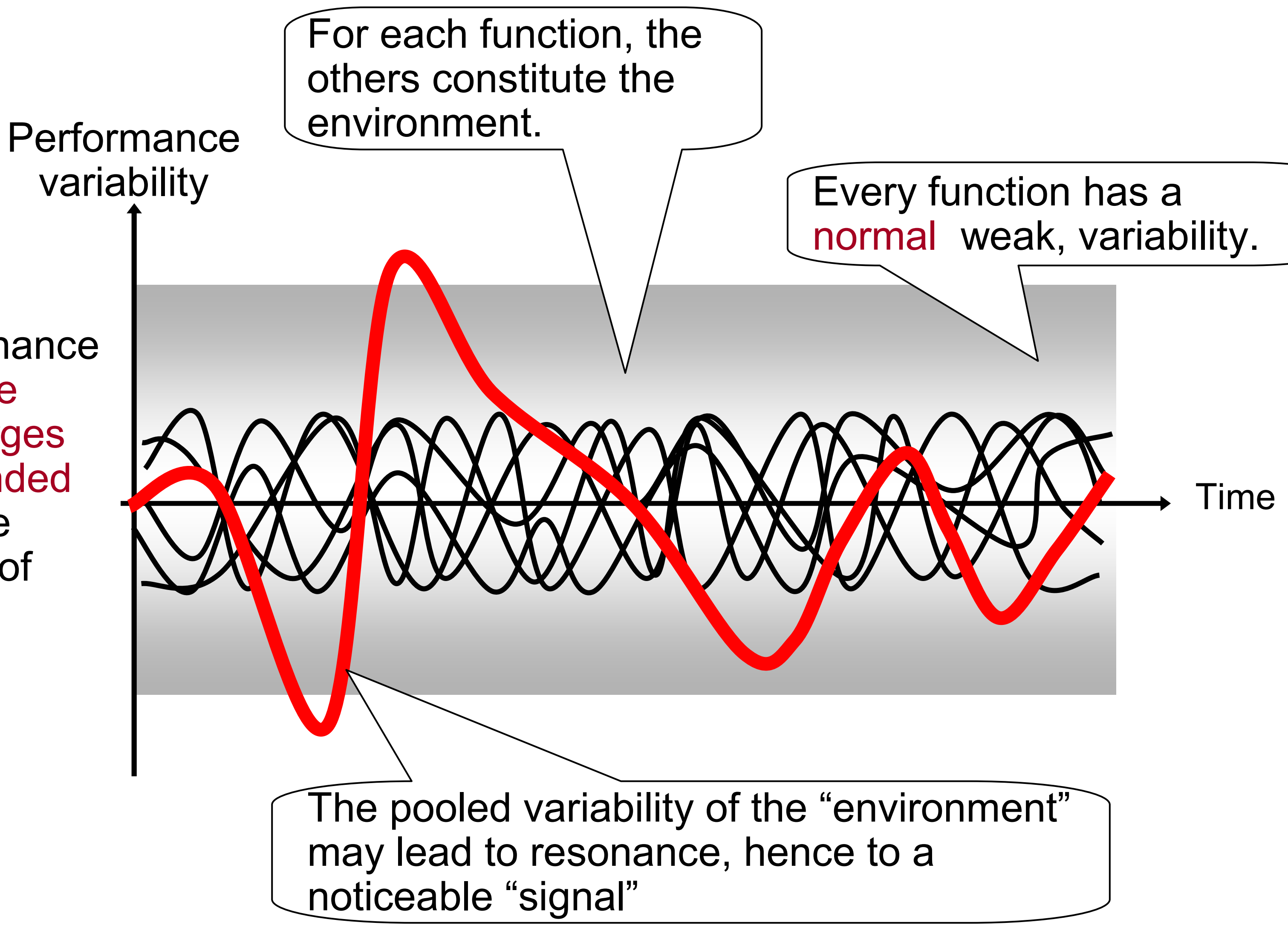
Stochastic resonance



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 interaction of the weak variability of many signals.



MINES PARIS

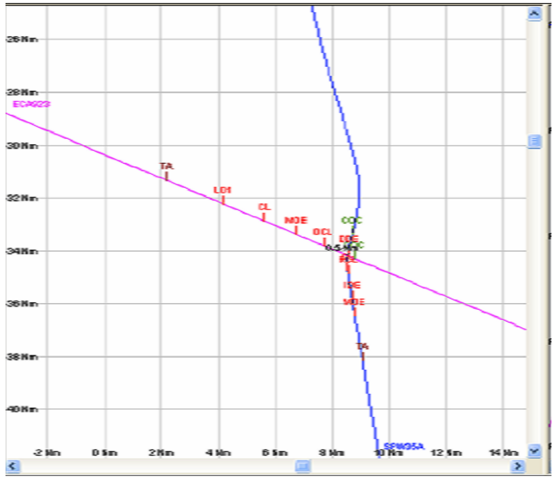
Normal behaviour is variable

Human failures cannot be modelled as deviations from designed and required performance:
- humans are not designed.
- conditions of work are usually underspecified
- humans are multifunctional, and can do many different things

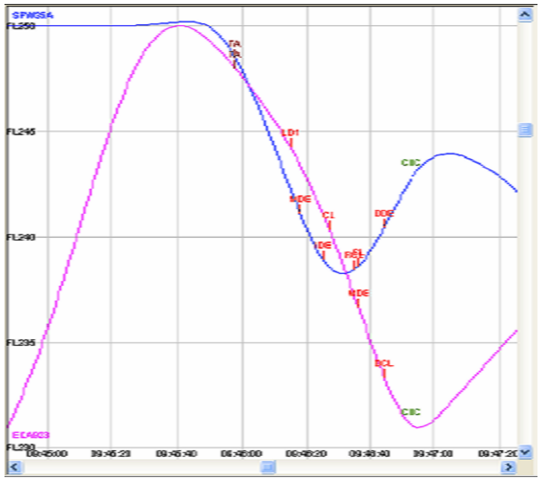
Performance variability is natural in socio-technical systems, and a valuable part of normal performance. The many small adjustments enable humans to cope with the complexity and uncertainty of work.

The adjustments allow the system to achieve its functional goals more efficiently by sacrificing details that under normal conditions are unnecessary. Humans are adept at developing working methods that allow them to take shortcuts, thereby often saving valuable time.

Airprox



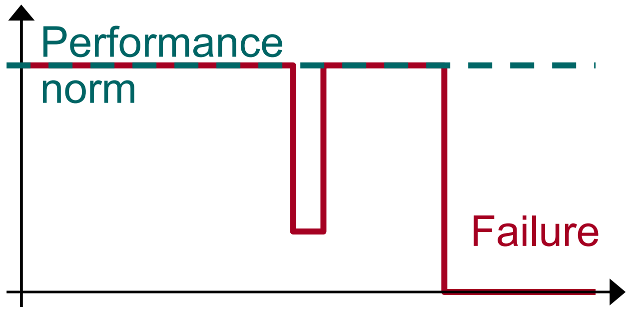
As the analysis shows there is no root cause. Deeper investigation would most probably bring up further contributing factors. A set of working methods that have been developed over many years, suddenly turn out as insufficient for this specific combination of circumstances.



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).

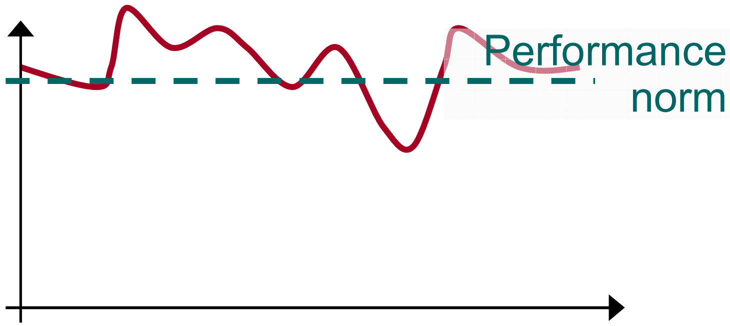
Principle of bimodal functioning

Technical components usually function until they fail. E.g., light bulbs or engines are designed to deliver a uniform performance until, for some reason, they fail.



Technical systems work in the same way, but some failures may be intermittent (SW). Performance is bimodal: the system either works or doesn't.

Humans and social systems are not bimodal. Normal performance is variable and this – rather than failures or 'errors' – is why accidents happen. Since performance shortfalls are not a simple (additive or proportional) result of the variability, more powerful, non-linear models are needed.



Functional resonance analysis

1. Identify essential system functions; characterise each function by six basic parameters.
2. Characterise the (context dependent) potential variability using a checklist.
3. Define functional resonance based on possible dependencies (couplings) among functions.
4. Identify barriers for variability (damping factors) and specify required performance monitoring.

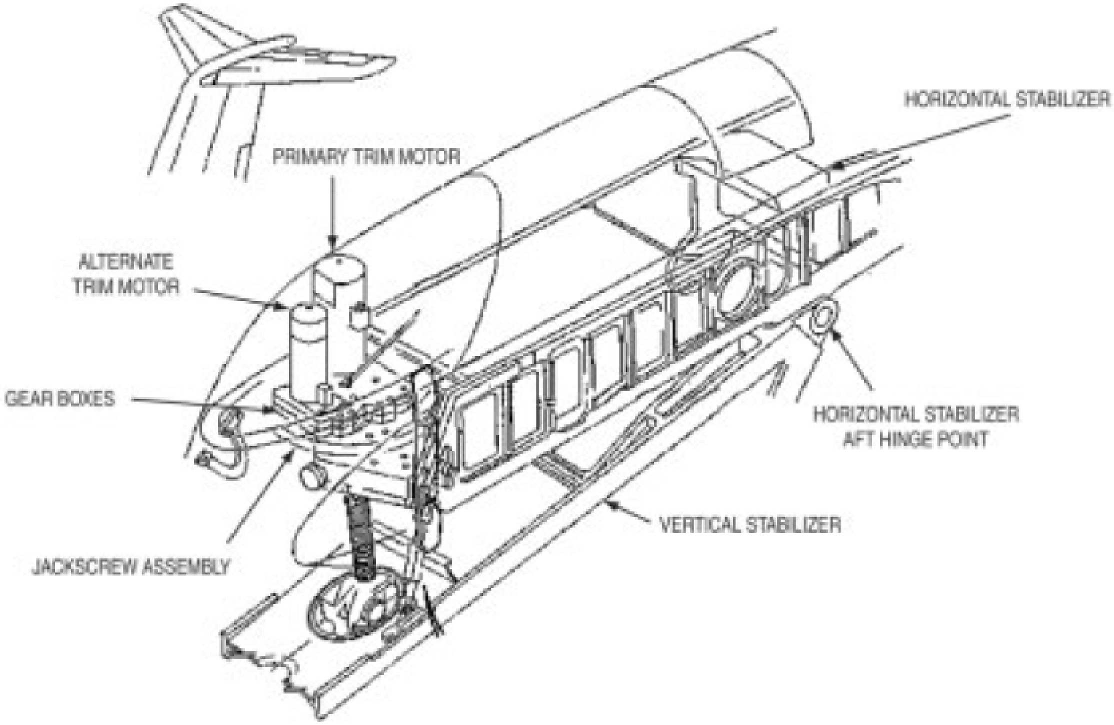
The MD-80 Airplane, horizontal stabilizer

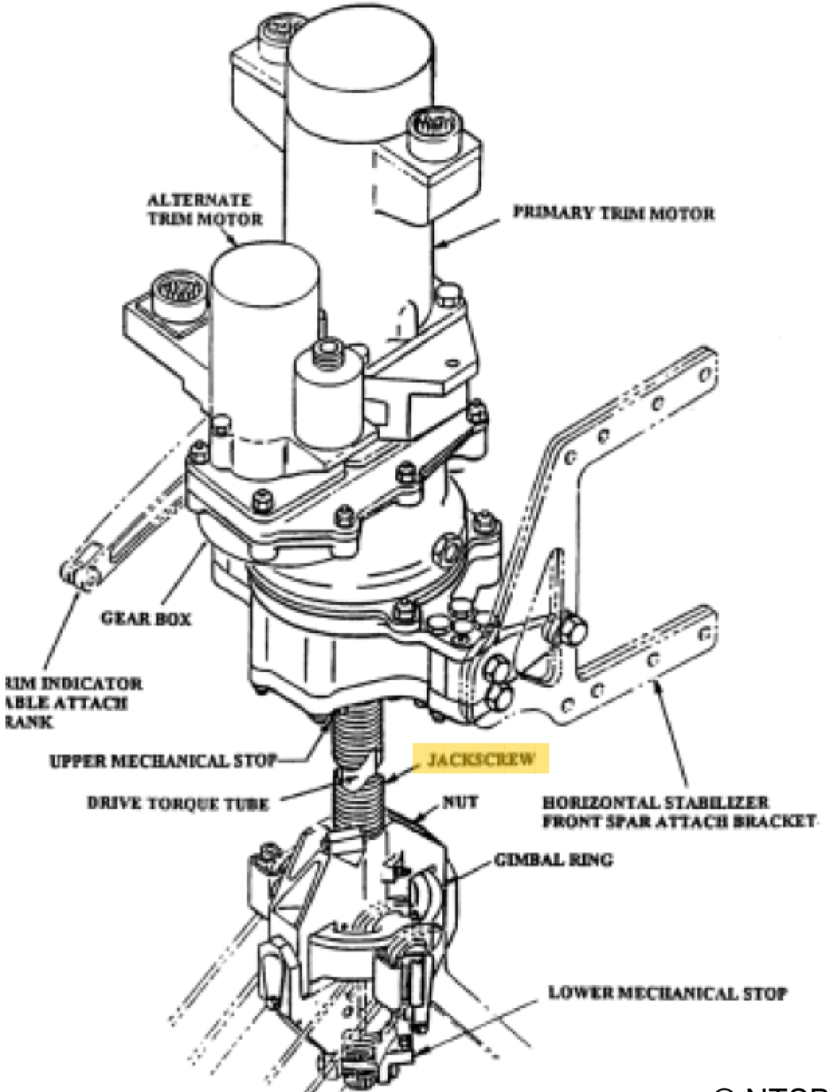
The stabilizer of the MD-83 has small pivoting wings and is mounted on the top of the vertical tail fin of the aircraft. The horizontal stabilizers help control the pitch of the plane's nose during flight.

Stabilizer trim tabs located on the horizontal stabilizer help adjust the wing's air flow. The pilot trims the stabilizer via a wheel in the cockpit.

Example prepared by Rogier Woltjer, LIU

Stabilizer Jackscrew Assembly



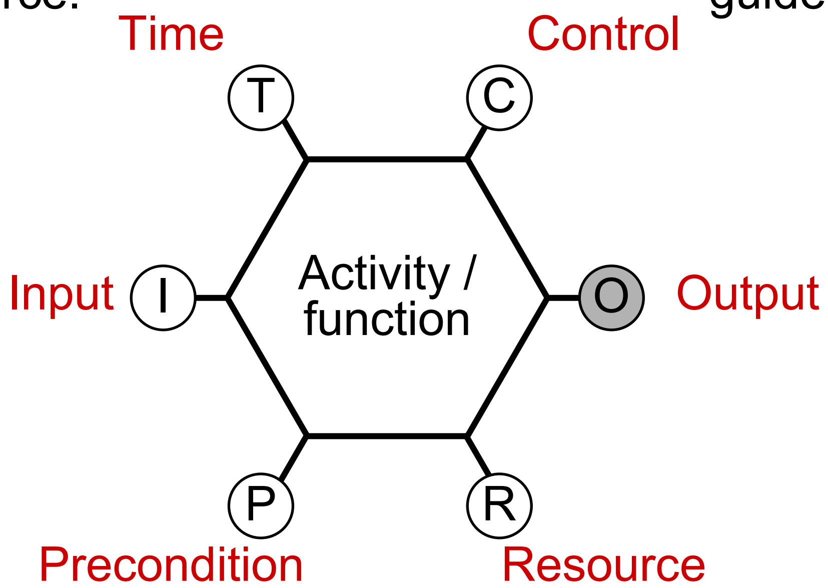


FRAM functional unit (module)

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.

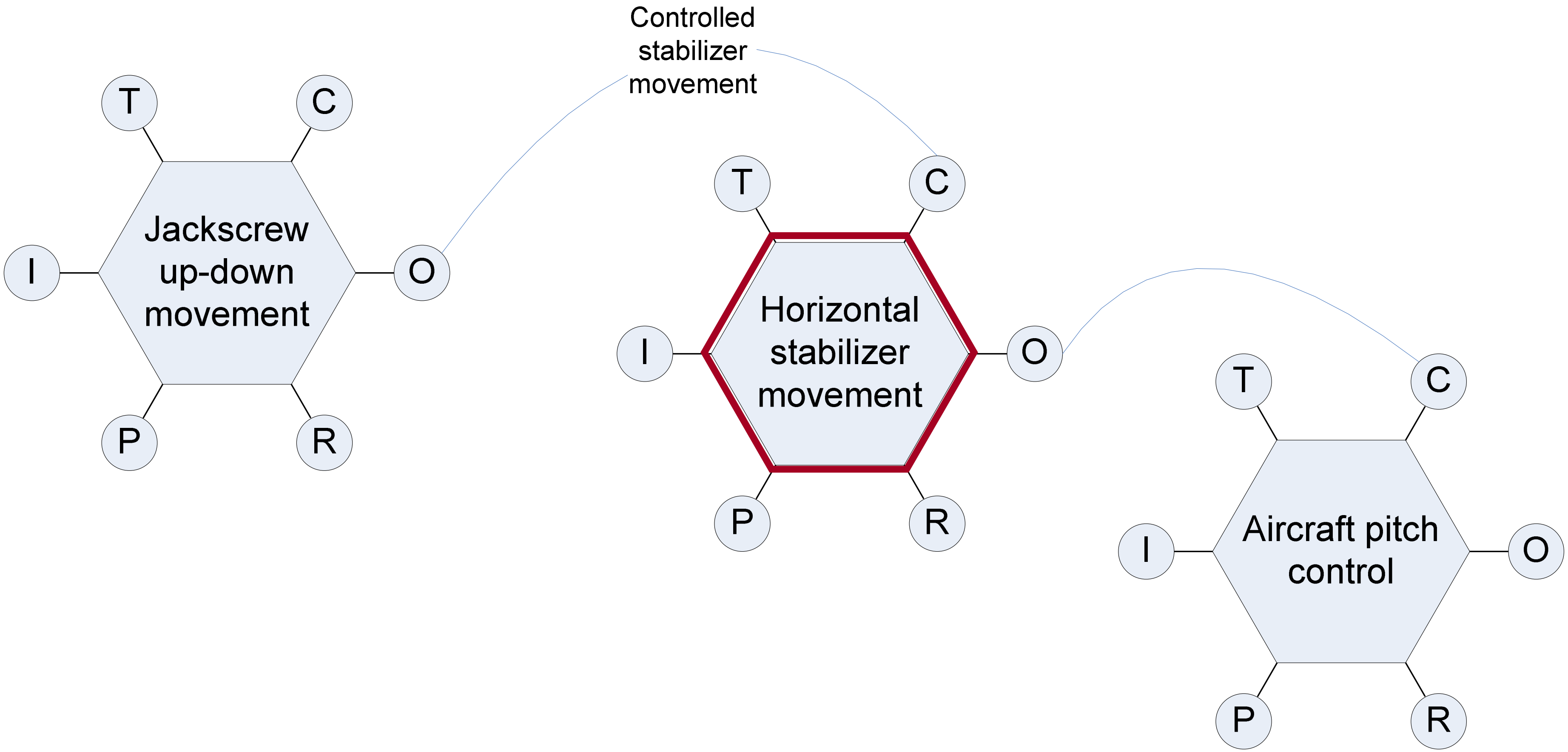


That which is produced by function. Constitute links to subsequent functions.

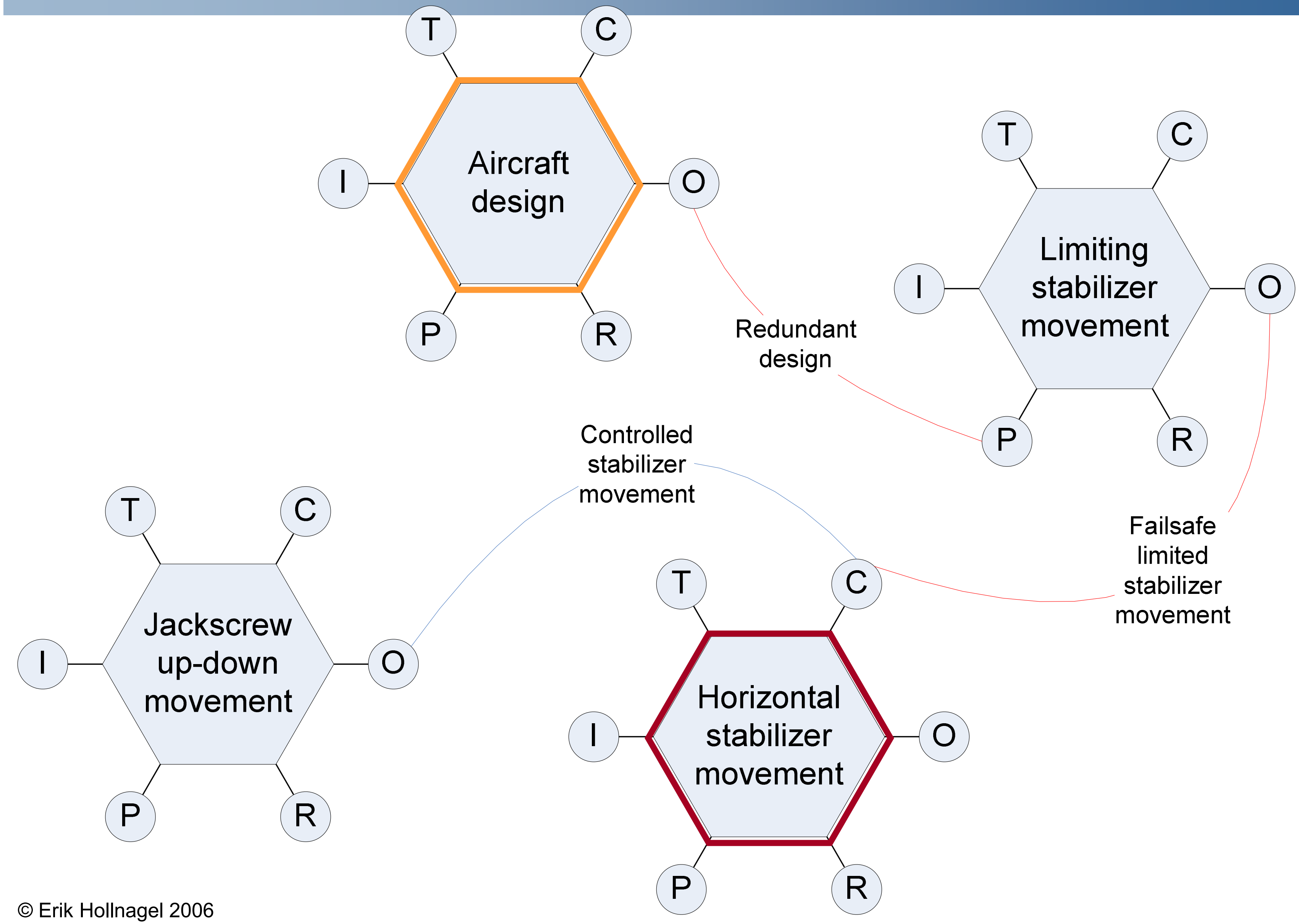
System conditions that must be fulfilled before a function can be carried out.

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

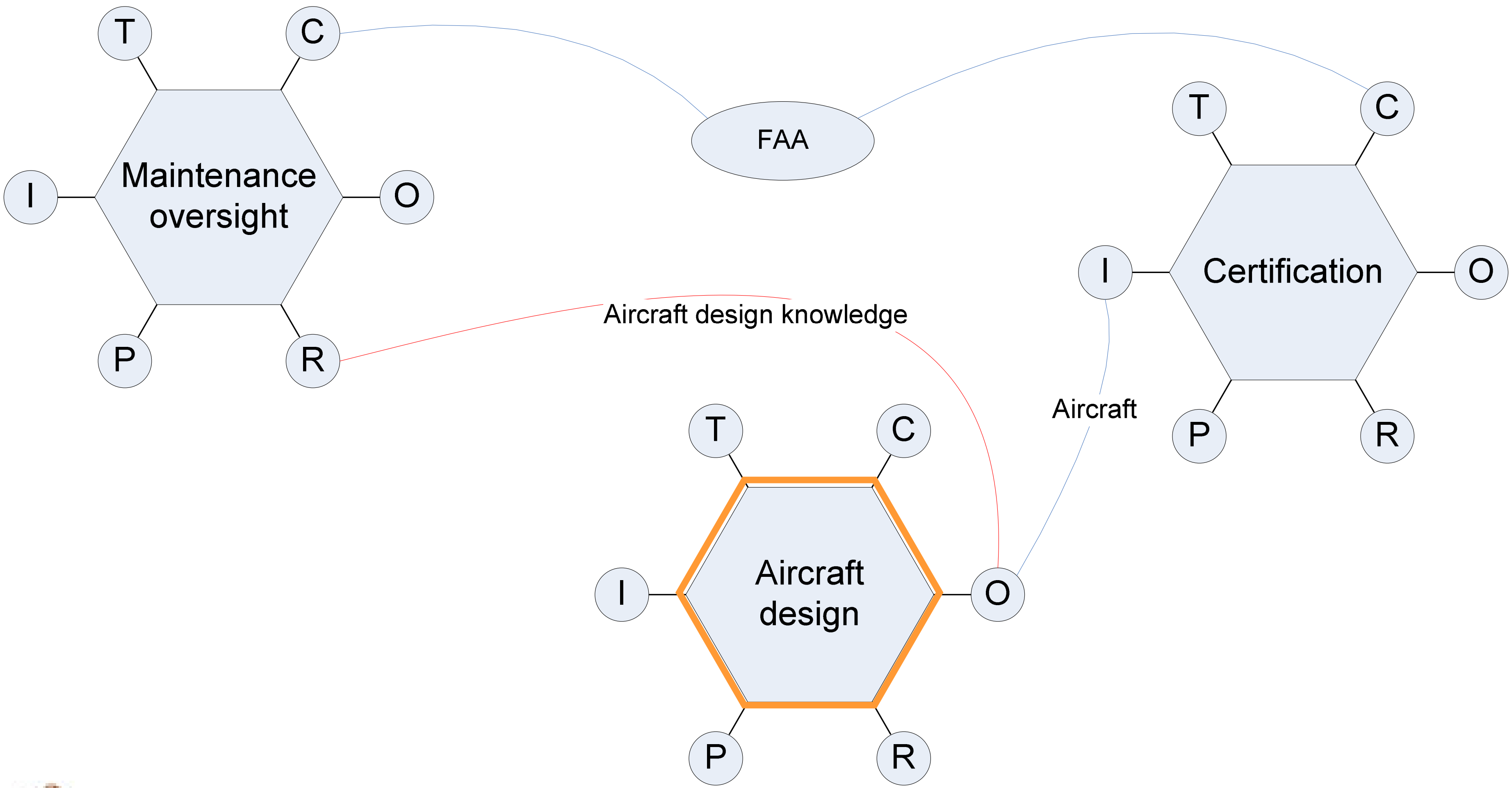
Horizontal stabilizer movement



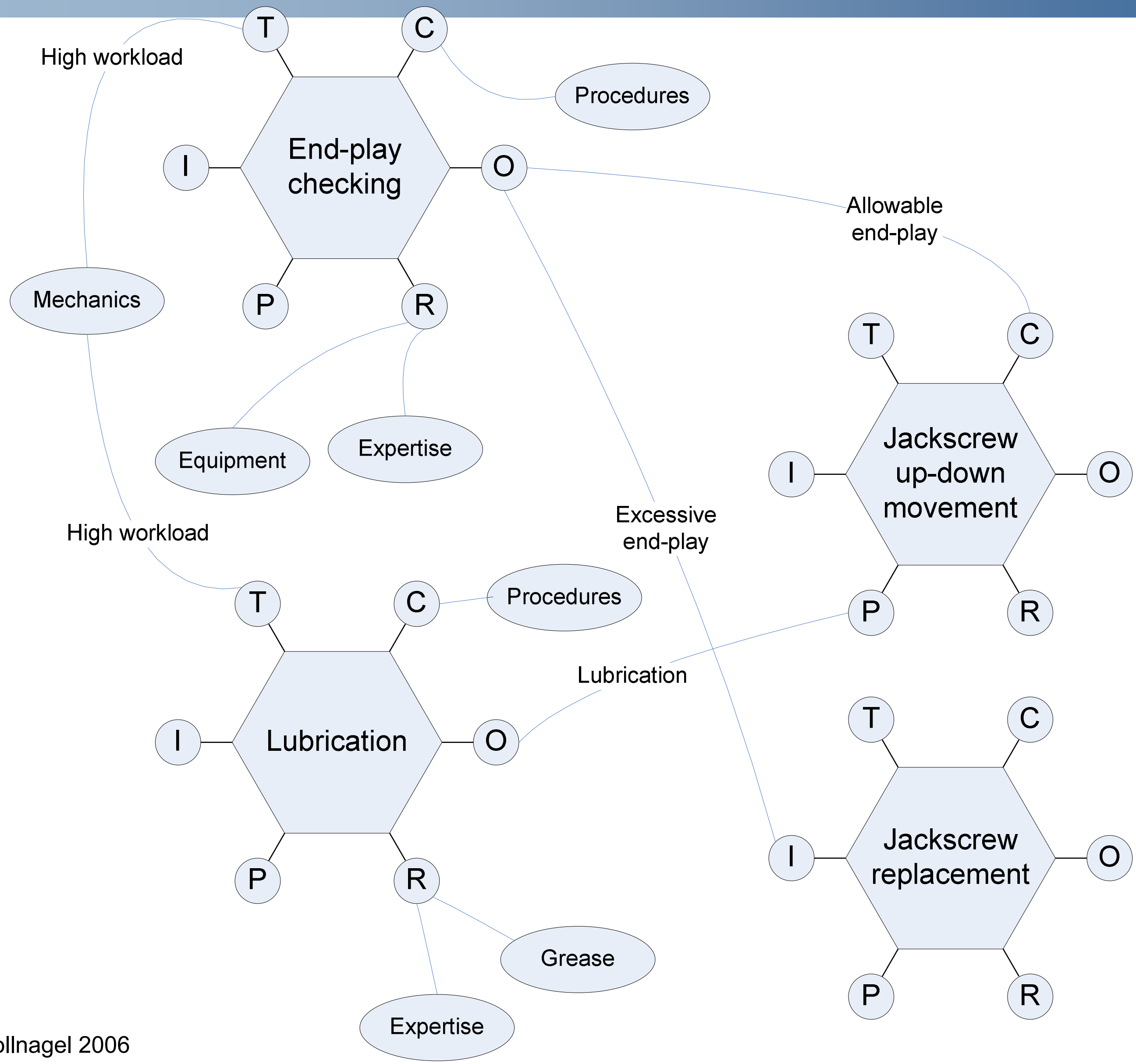
Aircraft design for redundancy



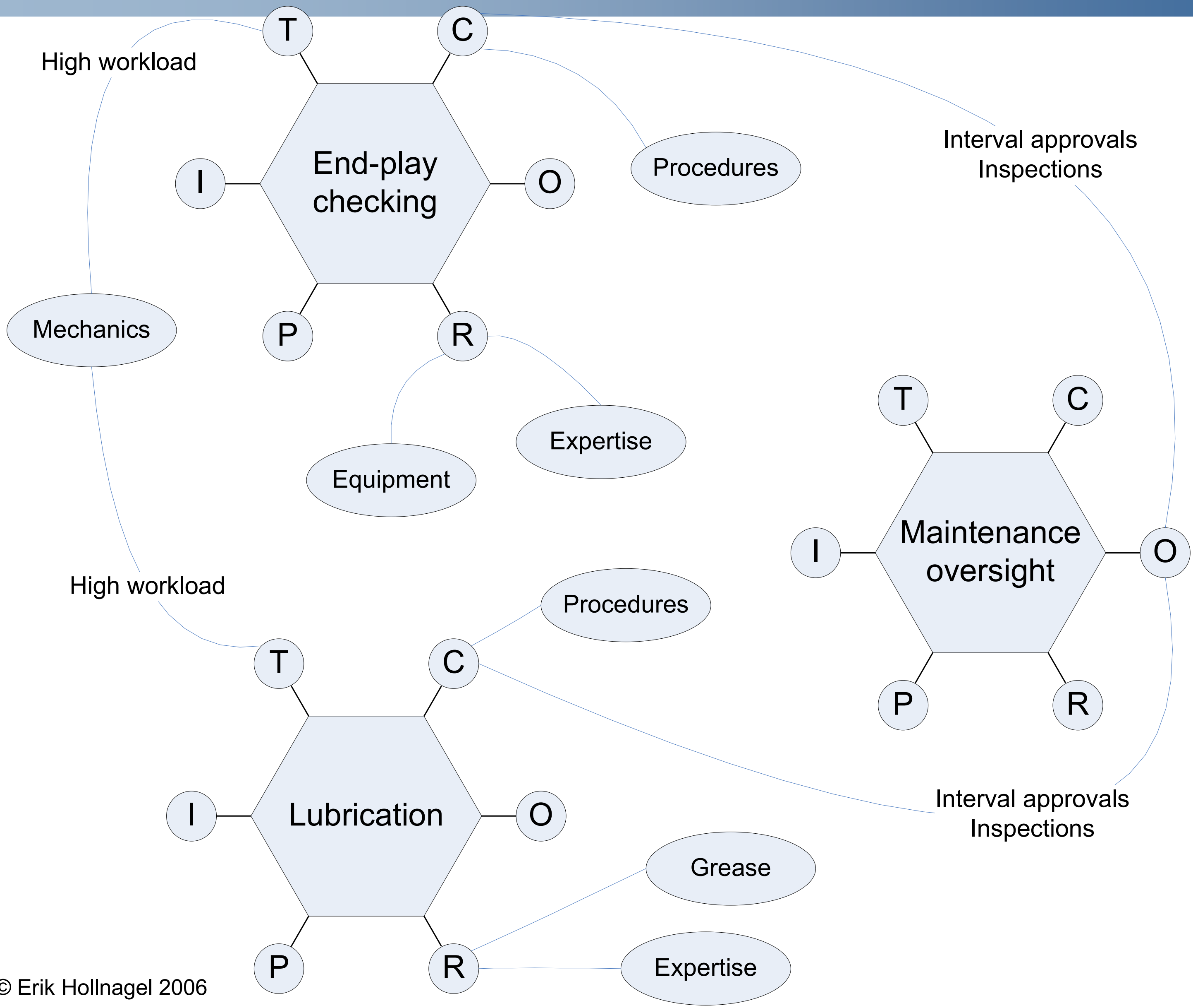
Design and maintenance certification



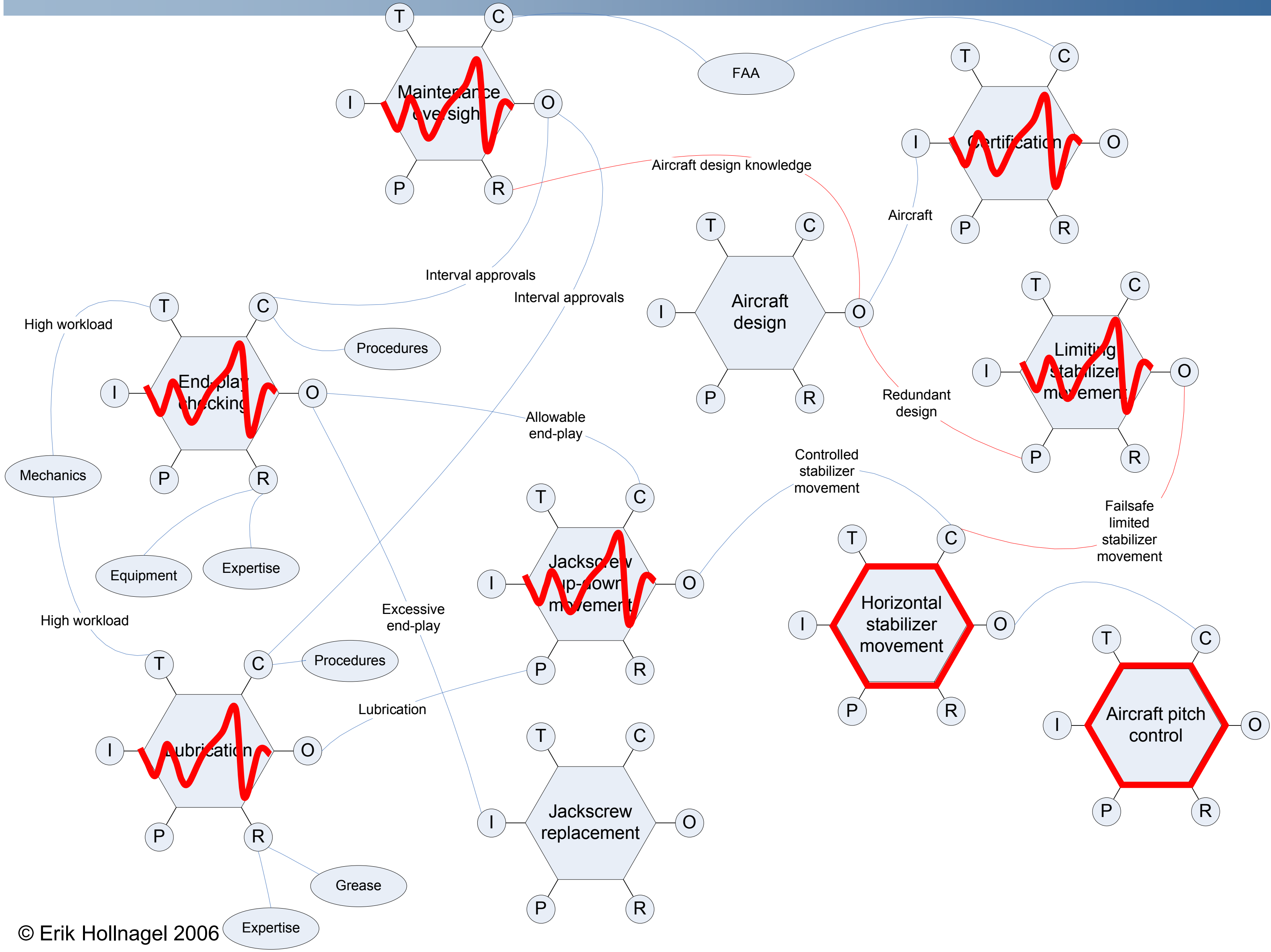
Jackscrew assembly maintenance



Maintenance Oversight



FRAM modules synthesis



Conclusions

Risk assessment must comprise a model of the system and its behaviour, which is as complex as the system itself.

- Conventional risk assessment is based on linear models (e.g., event tree) and on calculating failure probabilities.
- Socio-technical systems are non-linear. Risk is an emergent rather than a resultant phenomenon.

Risk assessment should address how irregularities can arise from performance variability, rather than on how individual functions fail.

- Performance variability reflects the nature of the work environment, including social and organisational factors.
- Performance variability is predictable for identified conditions.

The principle of functional resonance can be used to identify possible combinations of performance variability which may lead to the occurrence of undesirable outcomes.

MINES PARIS