Modelling of failures: From chains to coincidences

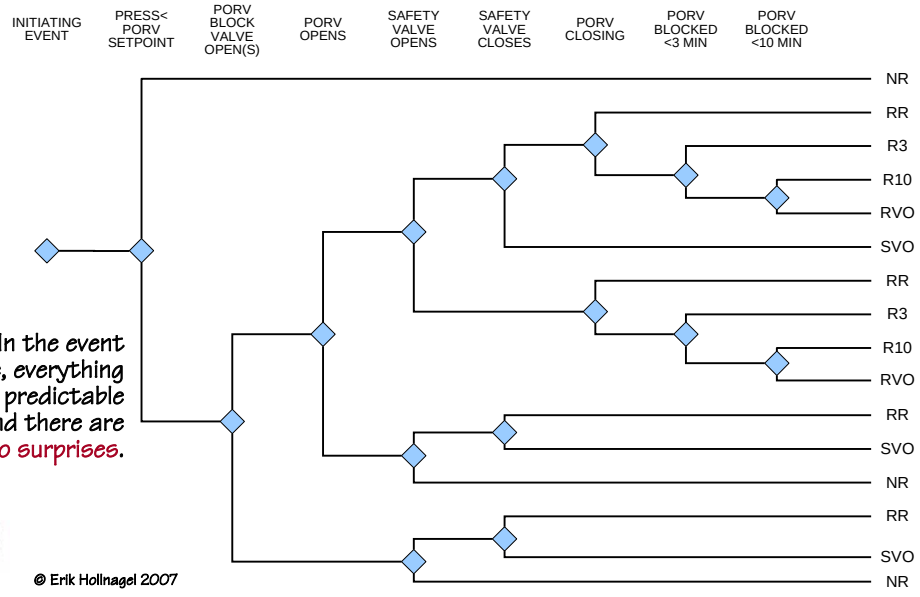
Erik Hollnagel
Professor, Industrial Safety Chair
École nationale supérieure des Mines de Paris, Pôle Cindyniques
Sophia Antipolis, France
E-mail: erik.hollnagel@cindy.ensmp.fr

The future is uncertain

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

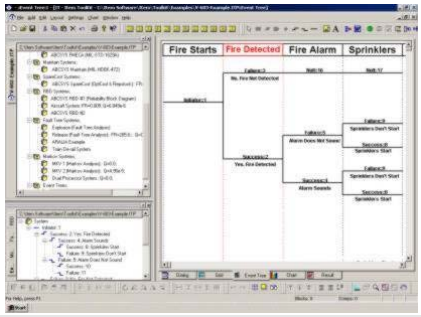
The representation must be powerful enough to capture the functional complexity of the system being analysed.

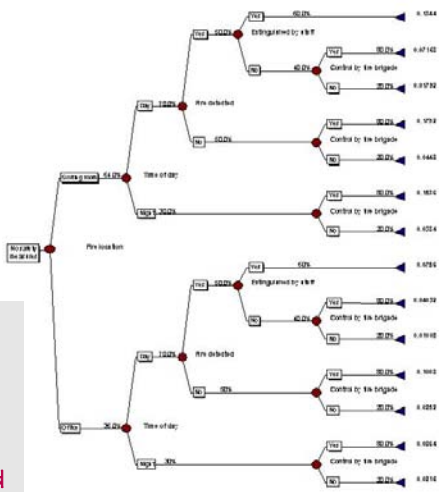
Typical representation: Event tree



In the event tree, everything is predictable and there are no surprises.

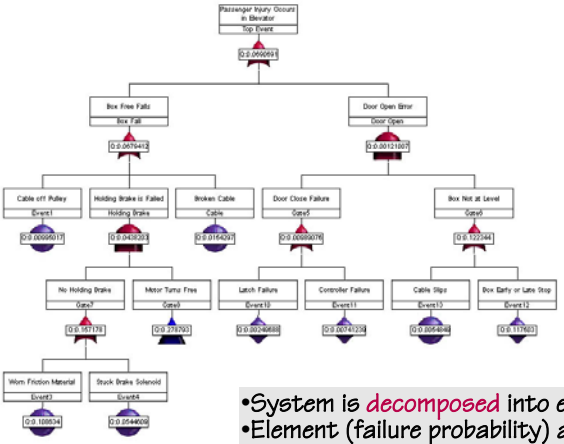
The event tree

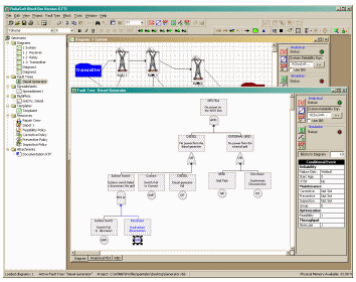




- System is decomposed into elements (components, events)
- Element (failure probability) are described individually
- Element functions are bimodal (true/false, work/fail)
- Order (sequence) is predetermined and fixed
- Linear (non-interacting) combinations
- Limited influence from context/conditions

The fault tree

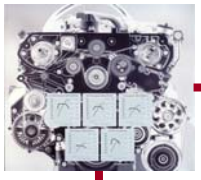




- System is decomposed into elements (components, events)
- Element (failure probability) are described individually
- Element functions are bimodal (true/false, work/fail)
- Order (sequence) is predetermined and fixed
- Linear (non-interacting) combinations
- Limited influence from context/conditions

Nature of technical (formal) systems

Many identical systems



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

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

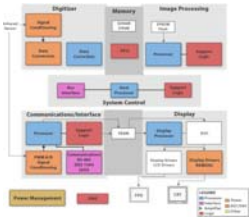
Decomposition works for technical systems, because they have been designed.

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

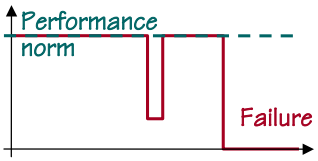
Principle of bimodal functioning

In the technological world, things usually function until they fail.
When simple systems, such as a light bulb, fail, they are discarded and replaced by a new (and identical) one.

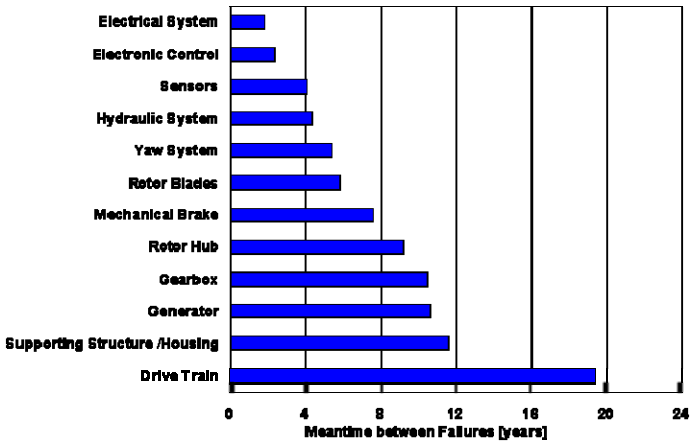
More intricate systems, such as engines, can be maintained and repaired, as long as it is considered worthwhile.



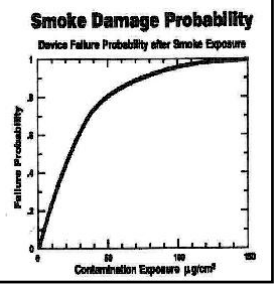
Complex, technological systems work according to the same principle. Failures may, however, be intermittent – especially if complex logic (software) plays a part.
Performance is basically bimodal: either the system works correctly (as designed) or it has failed.



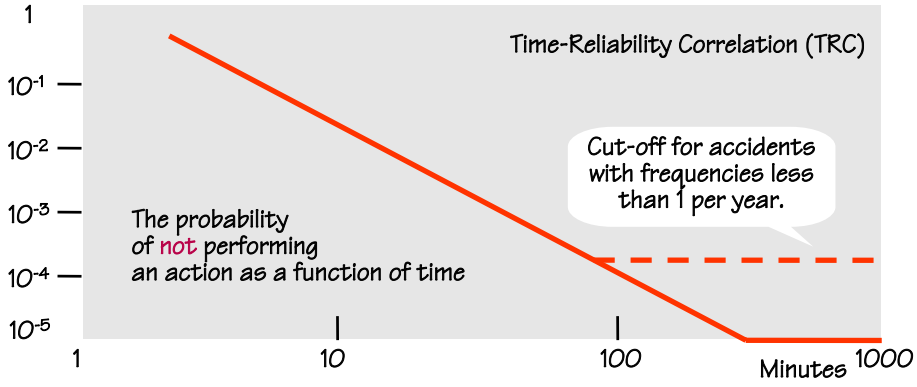
Technological malfunctions



Failure mode
Failure probability
MTBF



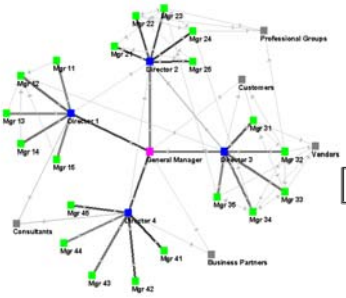
Human malfunctions

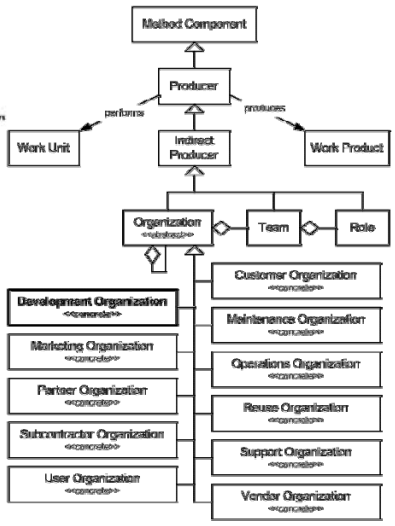


Error of omission (EOO)
Error of commission (EOC)

Failure mode?
Failure probability?
MTBF?

Organizational malfunctions





Failure mode?
Failure probability?
MTBF?

Nature of socio-technical systems

All systems unique

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

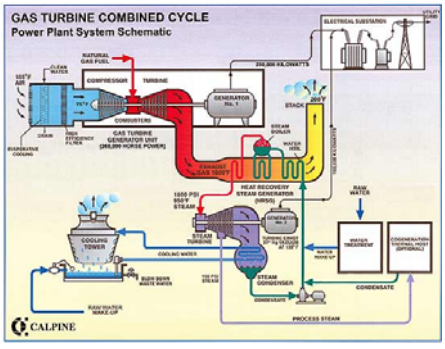
Decomposition does not work for socio-technical systems, because they are emergent.

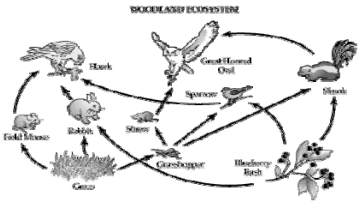
Risks and failures must therefore be described relative to functional wholes.

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

What is a system?

A system can be defined as "a set of objects together with relationships between the objects and between their attributes"
(Hall & Fagen, 1969, p. 81)



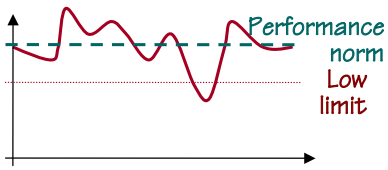


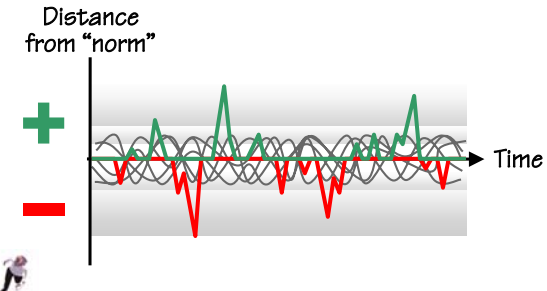
Beer (1964): a manufacturing cell in a garment factory may be considered as a system, as a component of a larger system for garment production, and as containing components, for instance a number of person-cum-scissor units.

There is no 'natural' way of setting the boundary between a system and its environment: it depends on the purpose of the analysis.

Socio-technical systems are not bimodal

Humans and social systems are not bimodal. Normal performance is variable and this – rather than failures and '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.





Performance variations can be have positive as well as negative outcomes!

Human factors has tended to look for negative aspects of performance - deviations or "errors"

Traditional view 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

The chain analogy requires that failures are thought of in a bimodal manner, i.e., something breaks the chain or there is an initial initiating event

Traditional risk assessment is constrained by two assumptions.

Events develop in a pre-defined sequence.

The major source of risk is component malfunctions.

Risk assessment: linear 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

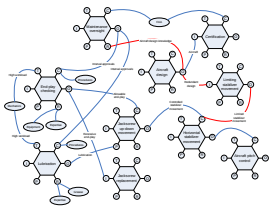
Single failures combined with latent conditions, leading to degradation of barriers and defences.

Systemic view of accidents

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

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.

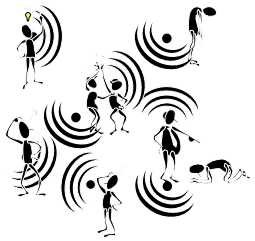


If failures are seen as a result of combinations of normal performance variability rather than of malfunctions, then the chain analogy is no longer adequate.
An alternative approach must be found that emphasises the dynamic nature of how events develop, i.e., coincidences rather than chains.
One possibility is to use resonance rather than failure.

Normal behaviour is variable

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

Accounting for the sources and range of normal performance variability:



Inherent variability (psychological / physiological phenomena).
Ingenuity and creativity – adaptability (overcoming constraints and underspecification).
Organizationally induced performance variability (meeting demands, stretching resources).
Socially induced variability (meeting expectations, informal work standards).
Contextually induced performance variability (performance conditions).

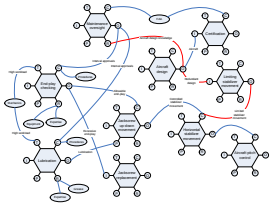
Risk assessment: non-linear models

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.

Accounting for how performance variability may combine:

Functional resonance (unintended, non-linear outcomes of normal performance adjustments).
Actions based on expectations (of what others have done or will do)
Unanticipated consequences (exact predictions impossible)
Combinations of "unsafe" actions and latent conditions



Traffic and randomness

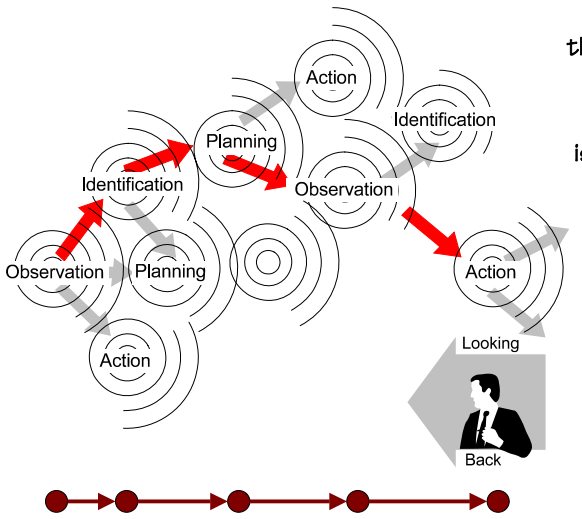
Traffic is a system in which millions of cars every day move so that their driving paths cross each other and critical situations arise due to pure random processes:
cars meet with a speed difference of 100 to more than 200 km/h, separated only by a few meters, with variability of the drivers' attentiveness,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

Looking back only ONE thing happened



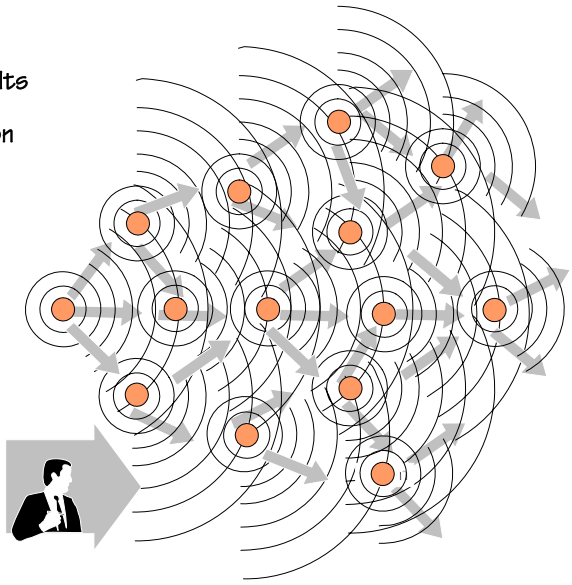
Given the actual context, the events seem to describe an orderly sequence.

The order (chain of events) is, however, an artefact due to the asymmetry of time

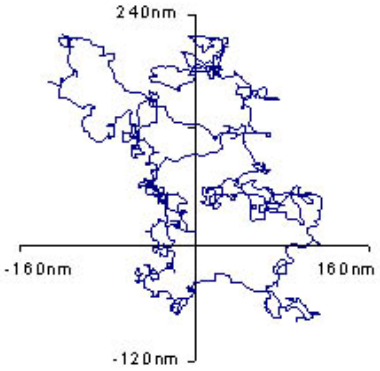
Looking ahead ANYTHING can happen

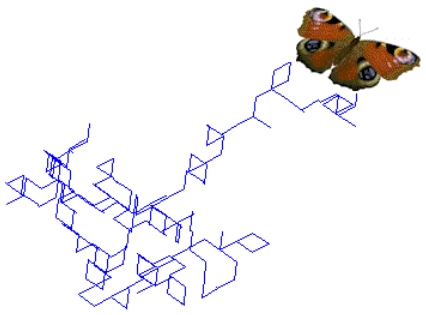
Prediction that is not constrained, is basically a combinatorial effort. The results therefore represent the complexity of the classification system, rather than real performance.

Actions are more often determined by the final cause (telos) than by the efficient cause.
Causal chains are thus of an a posteriori rather than an a priori nature.



The future as non-linear events

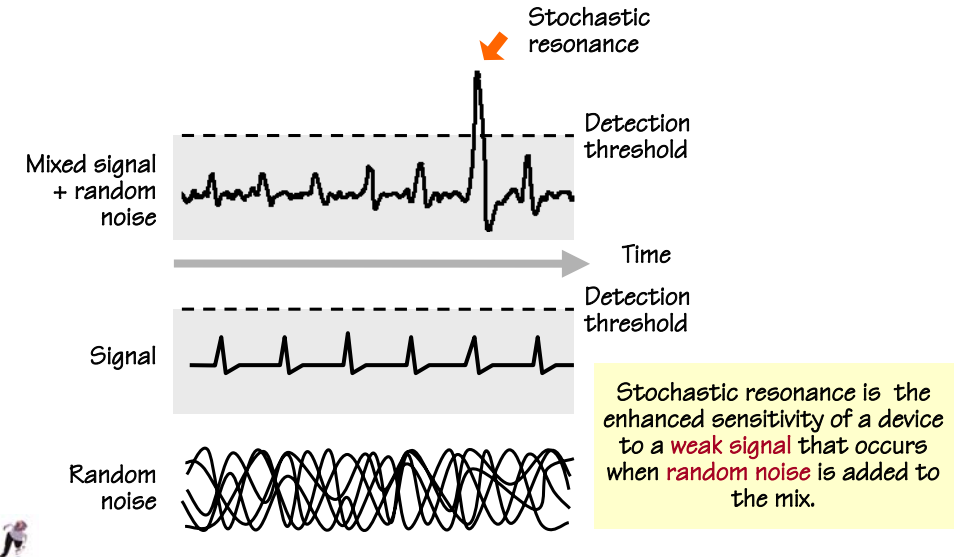




Non-linear events have been likened to Brownian movements or random walks.
Risk assessment requires something that is non-linear (non-trivial) at the same time as it is systematic (predictable)

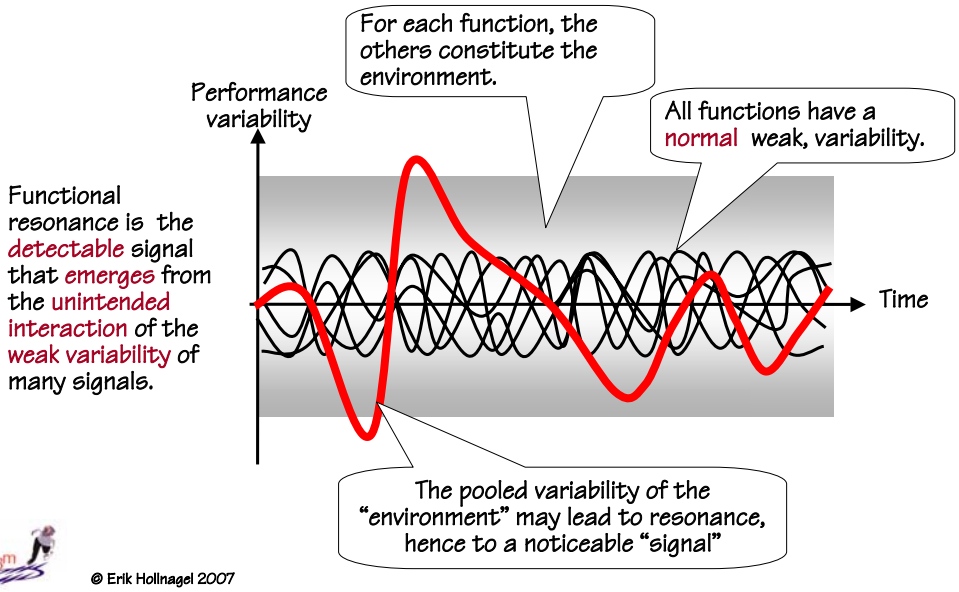
Resonance

Stochastic resonance



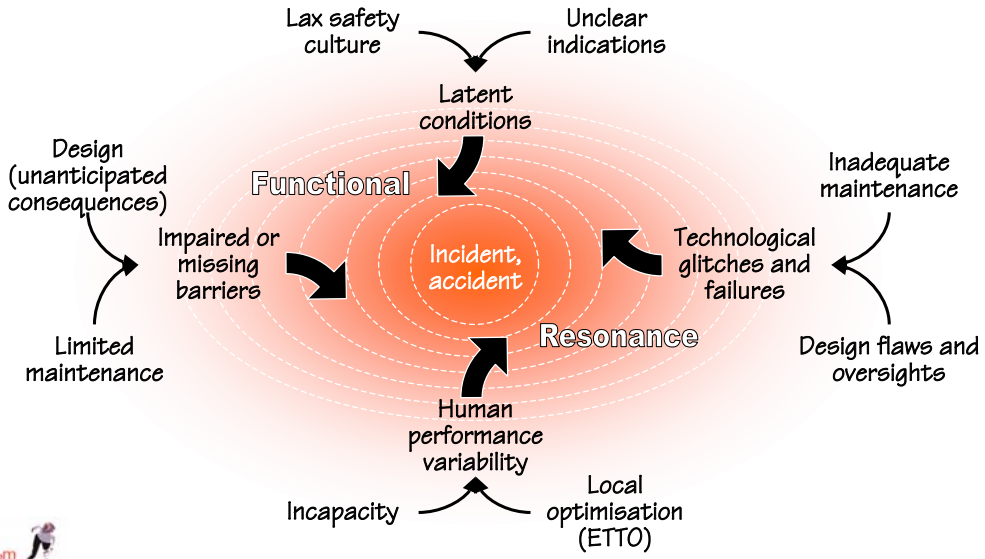
Stochastic resonance is the enhanced sensitivity of a device to a weak signal that occurs when random noise is added to the mix.

Functional resonance

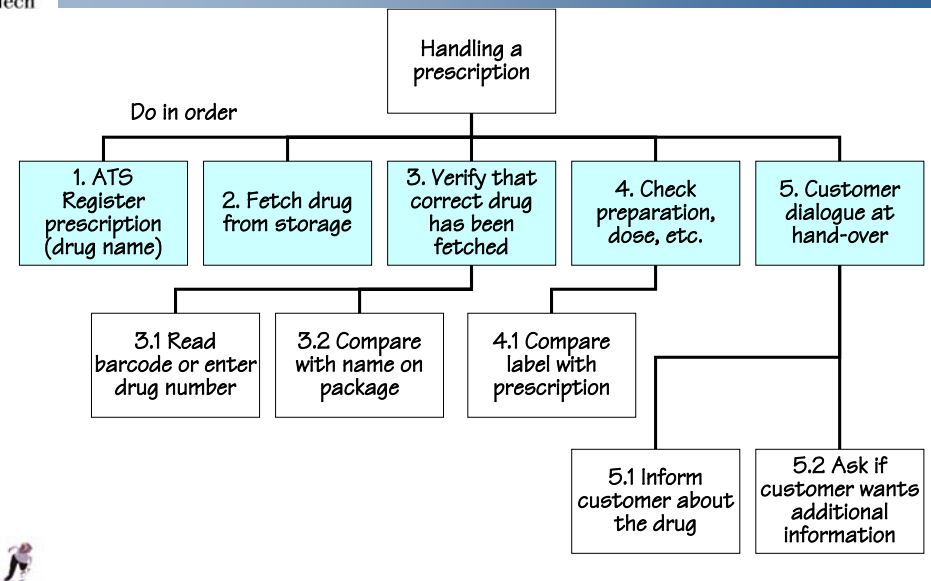


Functional resonance is the detectable signal that emerges from the unintended interaction of the weak variability of many signals.

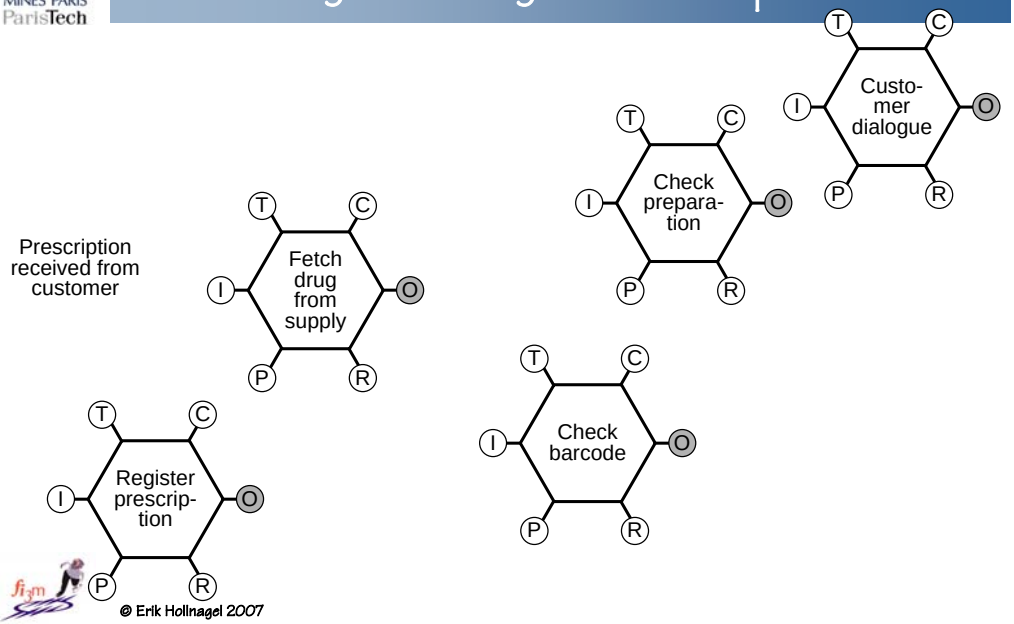
Functional Resonance Accident Model



Handling drug prescriptions (HTA)



Drug handling – normal procedure



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 normal 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.

Three premises of resilience engineering

- Performance conditions are always underspecified.
  It is impossible to specify in every detail what should be done and how. Individuals and organisations must therefore always adjust their performance to the current conditions; and because resources and time are finite, such adjustments will inevitably be approximate.
  Performance variability is unavoidable, but it is a source of successes as well as of failures.
- Many adverse events can be attributed to a breakdown or malfunctioning of components and normal system functions, but many cannot.
  These are best understood as the result of unexpected combination of normal performance variability. Adverse events therefore represent the converse of the adaptations necessary to cope with the complexity of the real world.
- Effective safety management cannot be based on hindsight, nor rely on error tabulation and the calculation of failure probabilities.
  Safety management must be proactive as well as reactive. Resilience Engineering looks for ways to enhance the ability of organisations to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures.

Resilience engineering

- Resilience requires an organisation that at all times is:

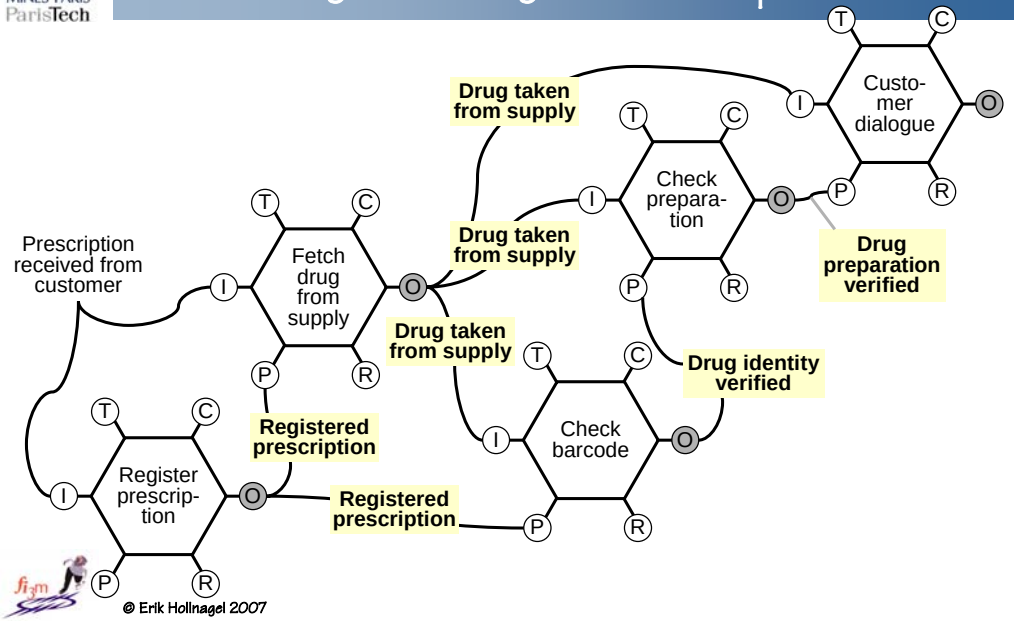
  Responsive - able to respond effectively when something happens
  Attentive - knows what to look for and regularly updates its knowledge, competence and resources
  Looking ahead - prepared for what might conceivably happen in the future in both the short and the long term.

- The development and application of Resilience Engineering requires

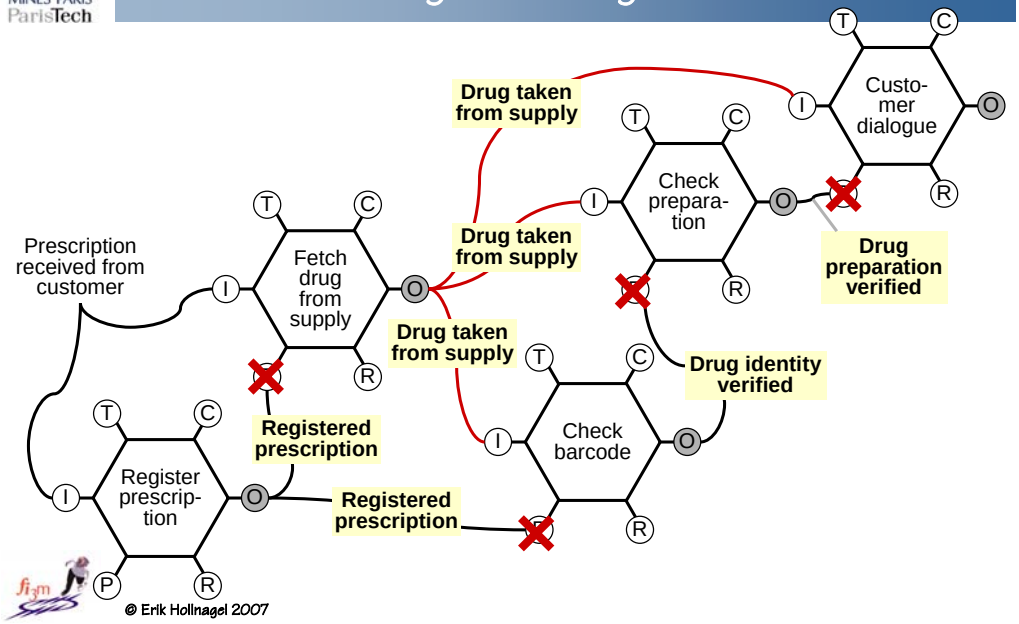
  The ability to measure, monitor, and analyse the resilience of an organisation in its operating environment,
  Tools and methods to improve an organisation's resilience vis-à-vis the environment, and finally
  Techniques to model and predict the short- and long-term effects of changes to operational, organisations, and targets..

- The purpose of safety management is not to reduce risks or the number of adverse events, but to increase on all levels the ability to adjust performance in the face of changes, disturbances, and uncertainty.

Drug handling – normal procedure



Drug handling - variation



Important announcement

EUROCONTROL

DFS Deutsche Flugsicherung

MINES PARIS ParisTech

Ph.D. Position
"A resilience based approach to evaluate the human contribution to system safety"

The position is part of a new project in a collaboration between Eurocontrol, Deutsche Flugsicherung (DFS), and École des Mines de Paris, Pôle Cindyniques.
The main place of work will be Sophia Antipolis, France

For further information please contact either:
erik.hollnagel@cindy.ensmp.fr
Oliver.Straeter@eurocontrol.int

Thank you for your attention