

# Risk control through Resilience Design

**Erik Hollnagel**

**Responsable de la Chaire “Sécurité Industrielle”**

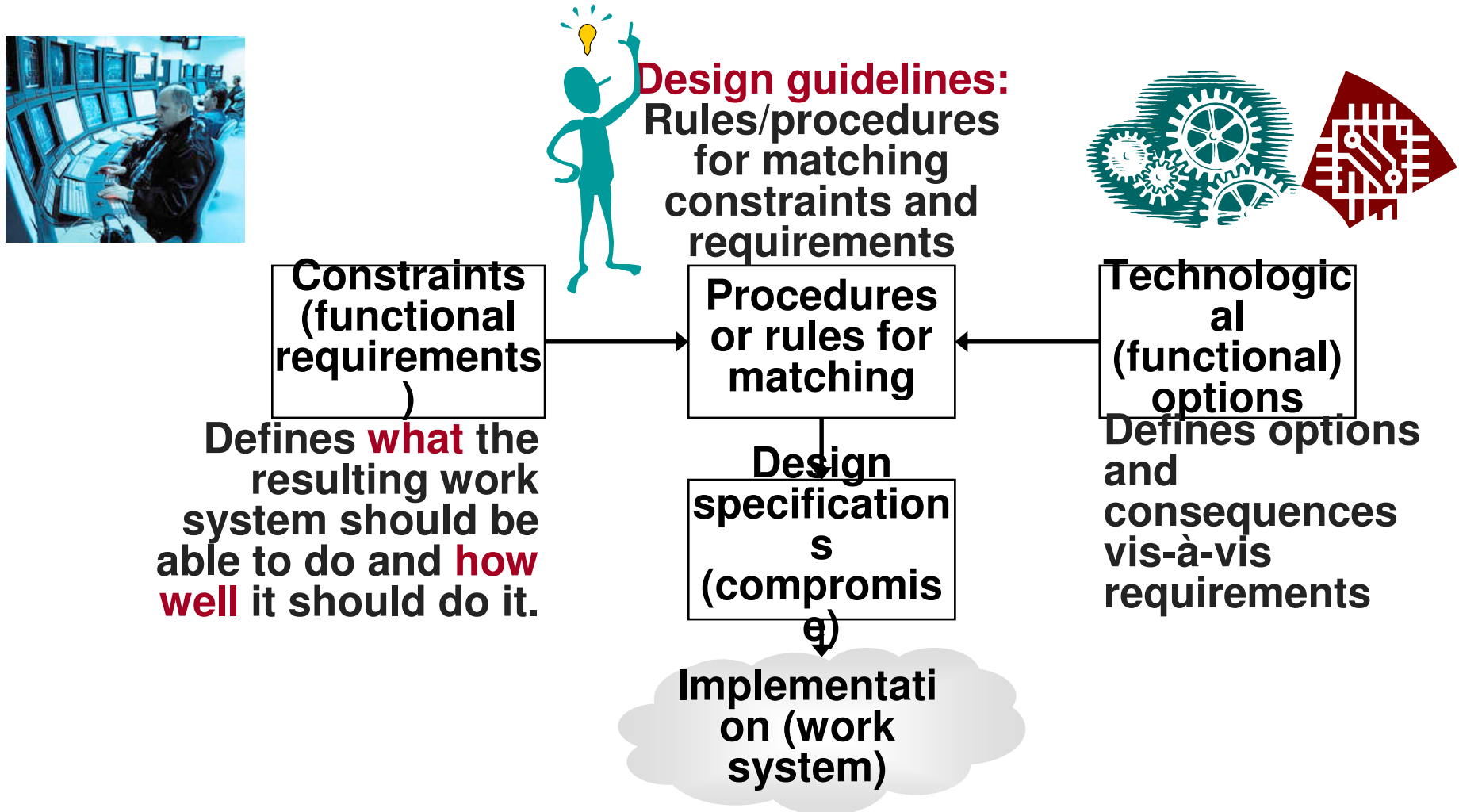
**ENSMP, Pôle Cindyniques**

**Sophia Antipolis, France**

**E-mail: [erik.hollnagel@cindy.ensmp.fr](mailto:erik.hollnagel@cindy.ensmp.fr)**

# The Art – and Purpose – of Design

**Design is the art of finding an effective compromise between constraints (functional requirements) and technological options.**

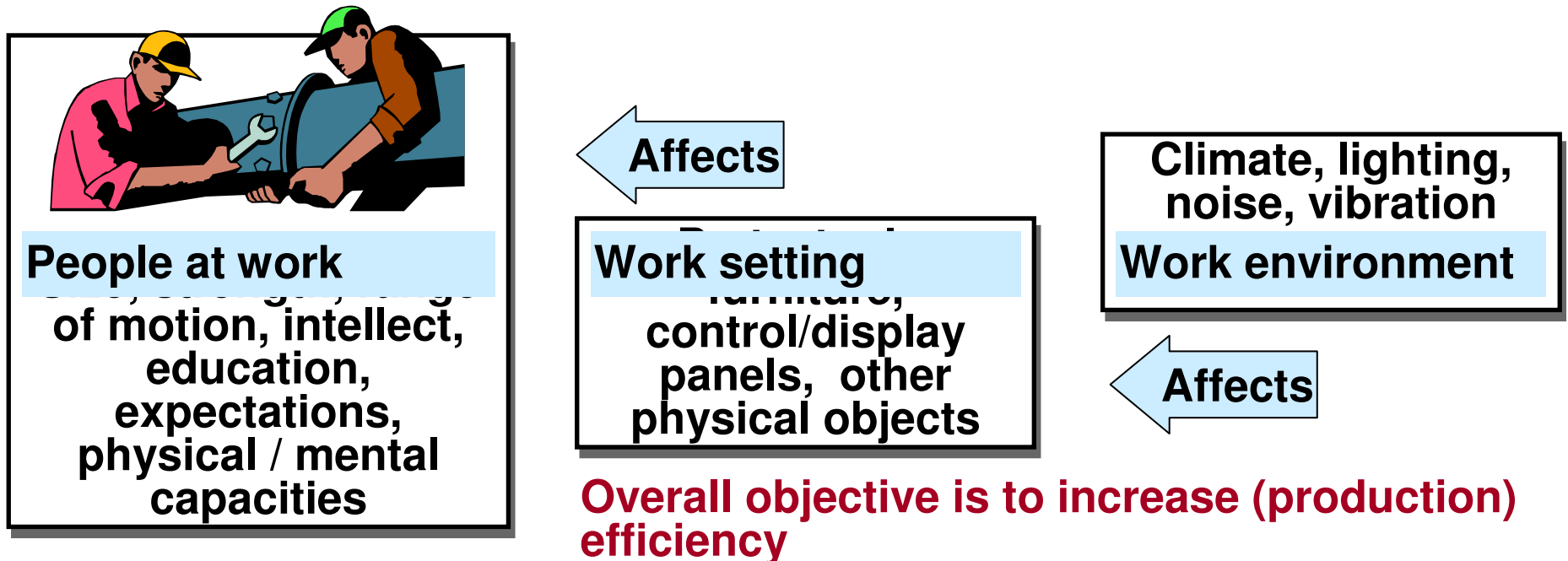


# Concerns of classical ergonomics

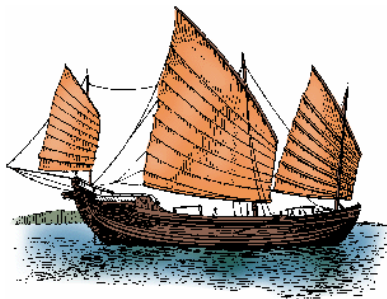
When humans are an explicit part of sharp-end operations the design must take into account the functional and structural characteristics of humans.

HFE has traditionally relied on a mechanical analogy and considered the human as a kind of complex machine (information processing system).

The focus has mostly been on the limitations of important capabilities such as speed, precision, endurance, etc. The best known example of that is Fitts' list, which is the basis for the compensatory approach to human-machine system design (MABA-MABA).



# System complexity is ever increasing



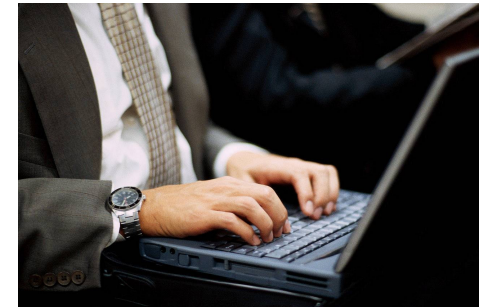
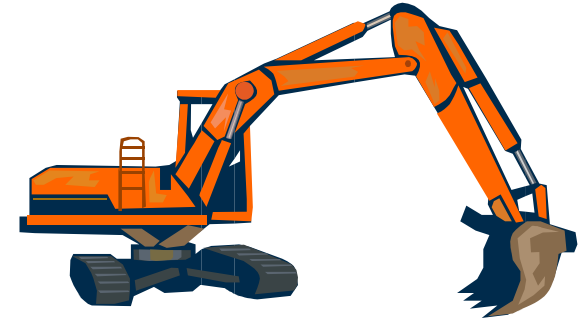
**Working  
directly  
(efficiency)**



**Humans have  
always made use of  
artefacts to do their  
work ...**



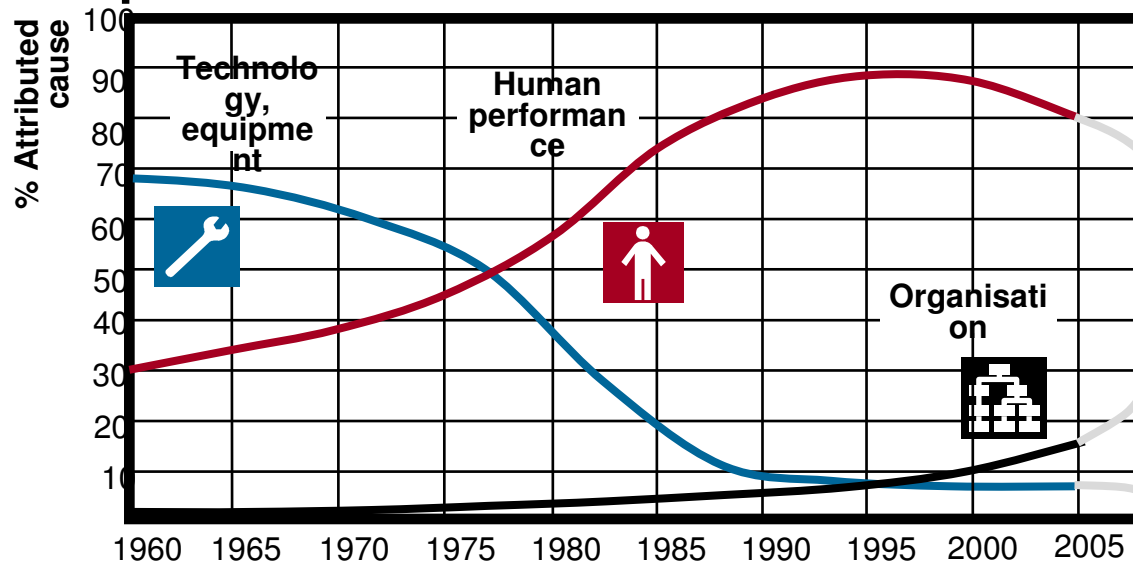
**... but since the  
1970s, artefacts  
have become  
exceedingly  
complex.**



**Working  
indirectly  
(usability)**

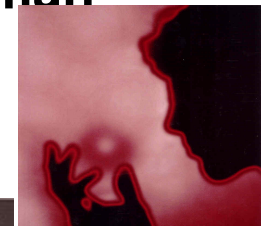
# Humans as the “weak” link

As systems have become more complex, the need to reduced or eliminate risks has increased. While technology (hardware) initially was the most unreliable part of the system, “out-of-range” human performance is now seen as the main source of risk.

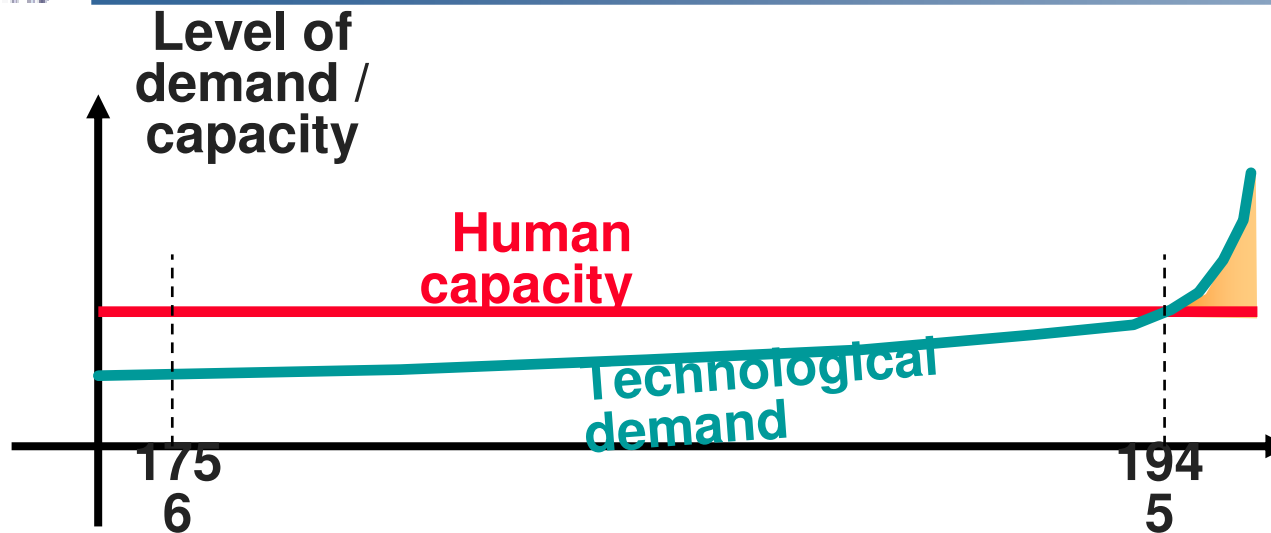


Focus on human limitations led to an emphasis on “human errors” in design and analysis. Technology and automation was used to increase efficiency – and to overcome human “limitations”.

Variability of human performance was seen as a necessary evil. Design, procedures, and work routines were used to constrain human performance to match the demands (“designing for simplicity”).



# Demand-capacity gap



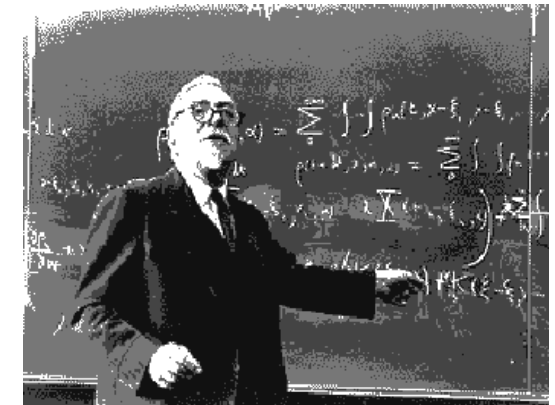
## Consequences of demand-capacity gap

Humans are too imprecise, variable, and slow.

Automation is used to overcome specific limitations

Human performance variability is cause of accidents.

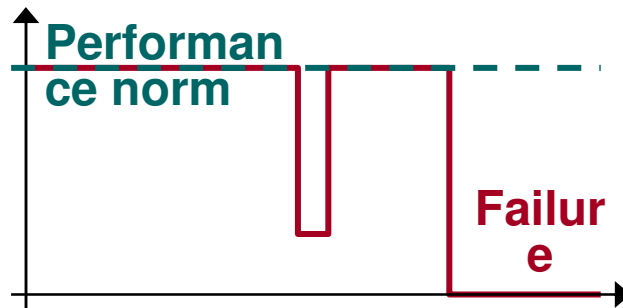
Automation is used to take over human tasks



**Gadget worshippers**, who “regard(ed) with impatience the limitations of mankind, and in particular the limitation consisting in man’s undependability and unpredictability”  
Norbert Wiener, 1964.

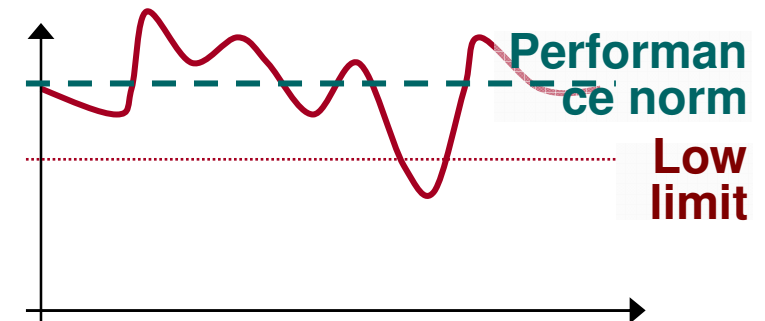
# Principle of bimodal functioning

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, although some failures may be intermittent (SW). Performance is bimodal: the system either functions correctly or it does not.

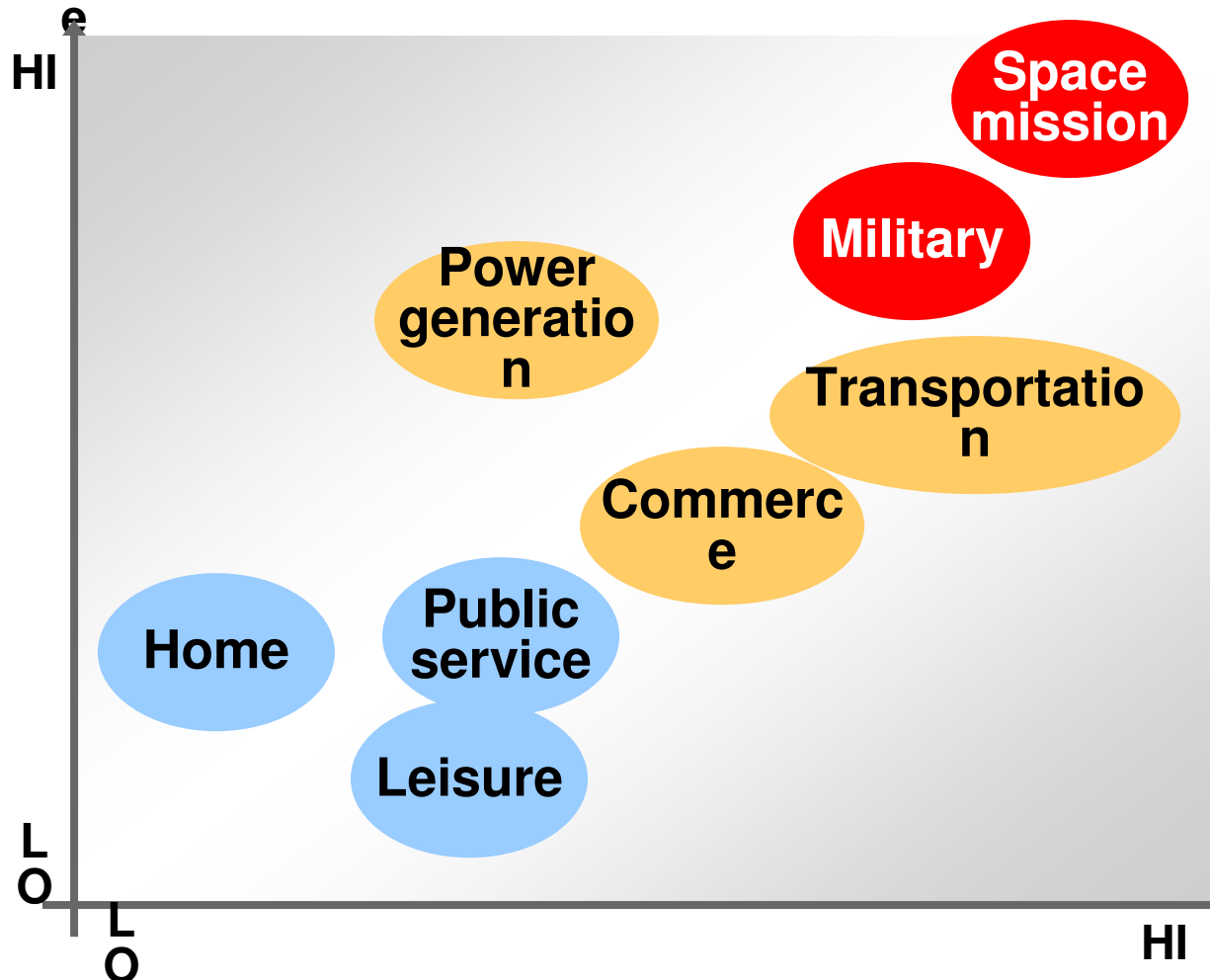
Humans and social systems are not bimodal. Normal performance is variable and this – **rather than failures and 'errors'** – is why accidents happen. Since performance shortfalls are **not** a **simple** (additive or proportional) result of the variability, more powerful, **non-linear** models are needed.



# Compliance as a solution?

One solution is to reduce risks by introducing constraints (barriers or limitations)

Need of  
compliance



**Compliance techniques:**  
**standardisation, procedures & regulations, formal methods, interface & interaction design**

**Effective compliance requires that work situations can be accurately predicted.**

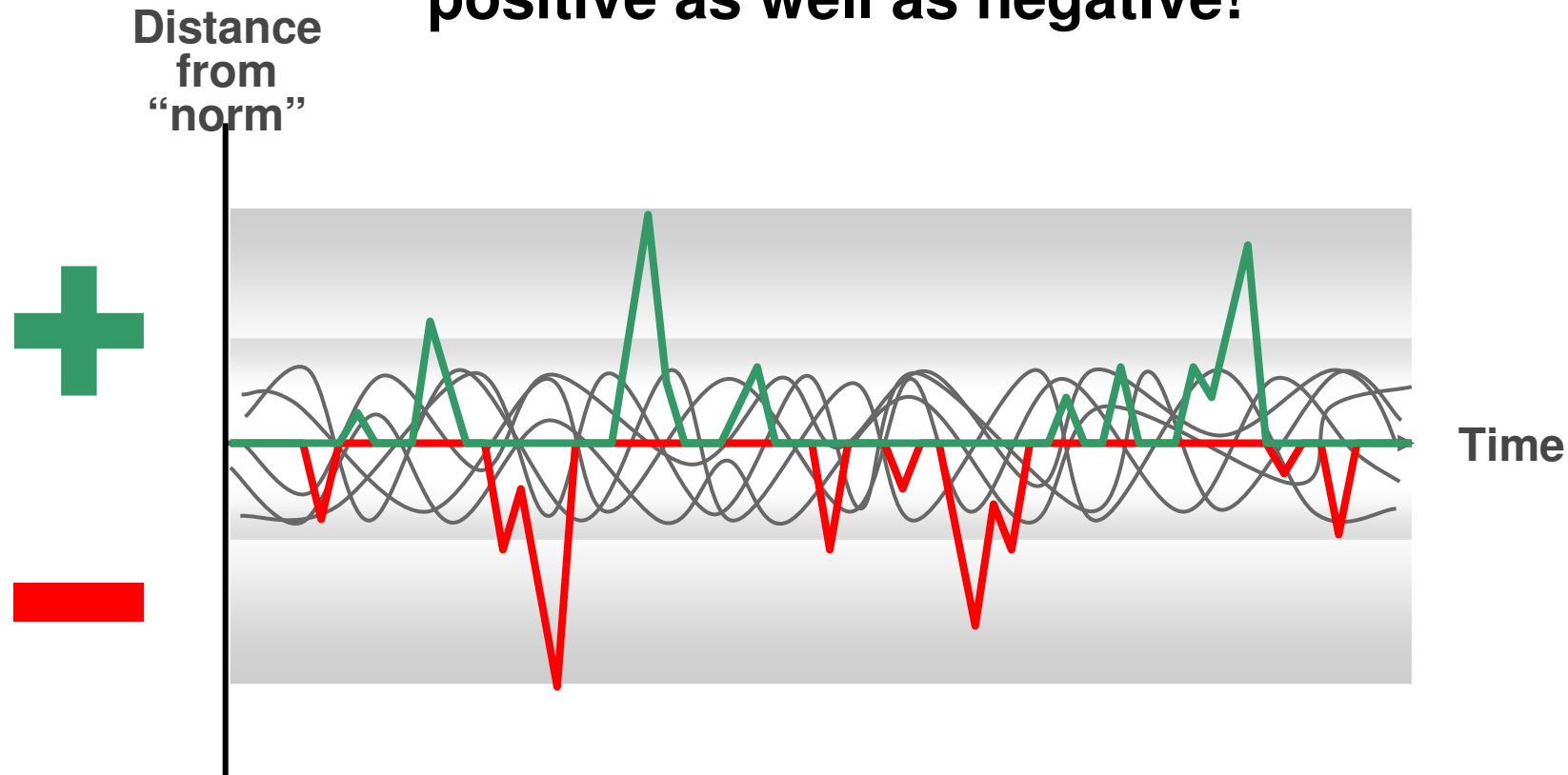
**Absolute compliance is therefore impossible**

Level of  
risk  
(operation)



# What should we be looking for?

**But performance variations can be positive as well as negative!**

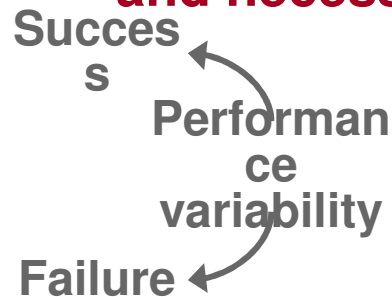


**Human factors has tended to look for negative aspects of performance - deviations or "errors"**

# All work systems are underspecified

Work systems are so complex that situations always are **underspecified** – hence partly **unpredictable**

Work systems are open and tightly coupled. 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 of this the problems cannot be solved by **eliminating** variability, since this will also eliminate the basis for effective work

The challenge is instead to **understand** the nature of variability (why, when, how) and how to **limit** it when it can be dangerous.

Limiting performance variability should not be achieved by constraining how people work, but by **addressing** the reasons for variability (why), monitoring (when), and understanding the possible consequences (how)

Humans and technology should not be described as two interacting “components”, but as constituting a **joint** (cognitive) system

# Variable behaviour is normal

Human failures **cannot** be modelled as **deviations** from designed and required performance:

humans are not designed and the “laws” governing human performance are imprecise.

conditions of work are usually underspecified; “correct” performance is ill-defined

humans are multifunctional and multitasking

Performance variability is **natural** in socio-technical systems, and a necessary 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.

**The ETTO principle:** Effectiveness-Thoroughness Trade-Off



# Changing of perspectives

## Human factors perspective (technological optimism)

Things go  
right  
because:

- Systems** are well designed and scrupulously maintained,
- Procedures** are complete and correct
- People **behave** as they are expected to – as they are taught
- Designers** can foresee and anticipate every contingency.

Humans are a **liability** and variability is a **threat**. The purpose of design is to constrain variability, so that efficiency can be maintained

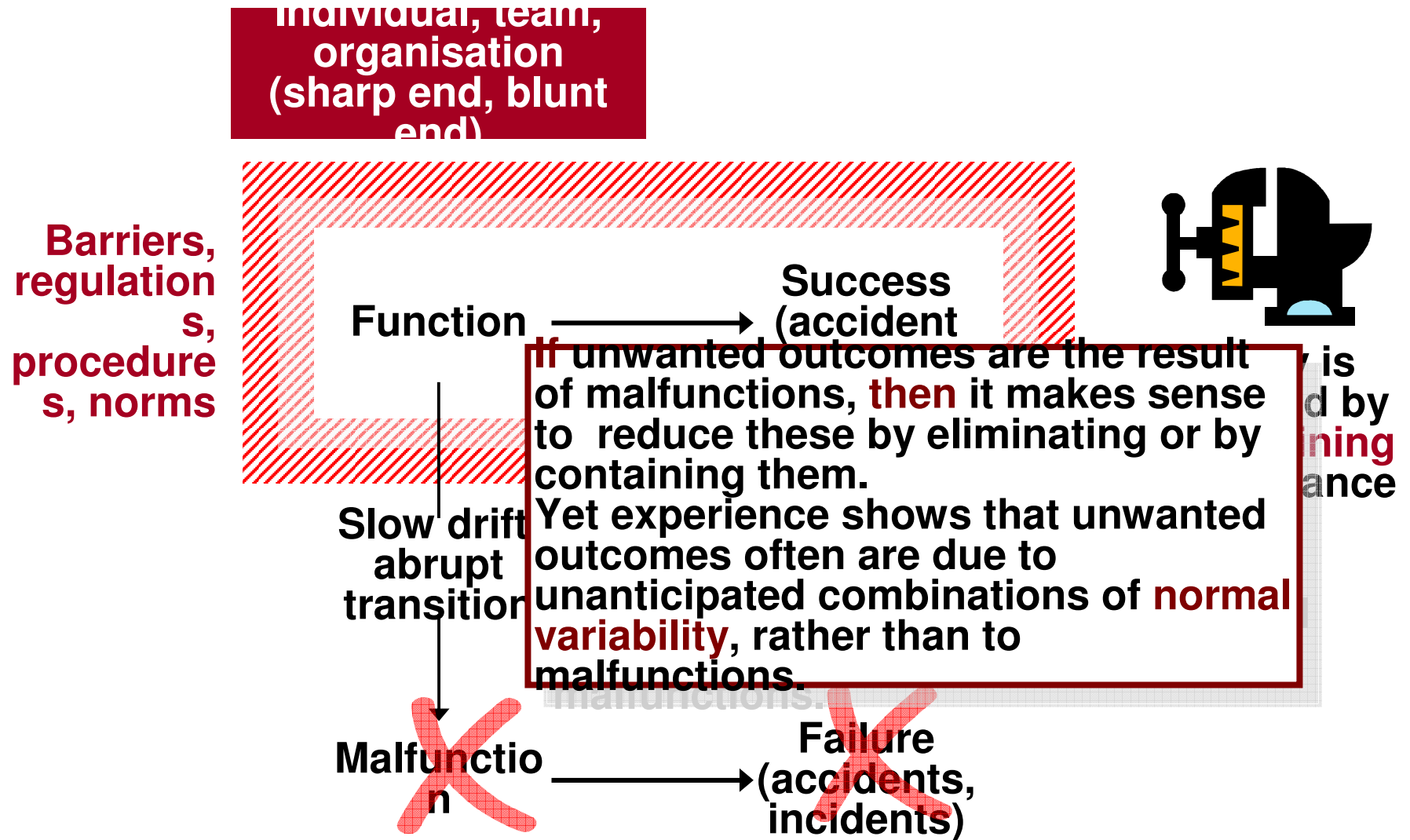
## Cognitive systems (resilience) perspective (technological realism)

Things go  
right  
because  
people:

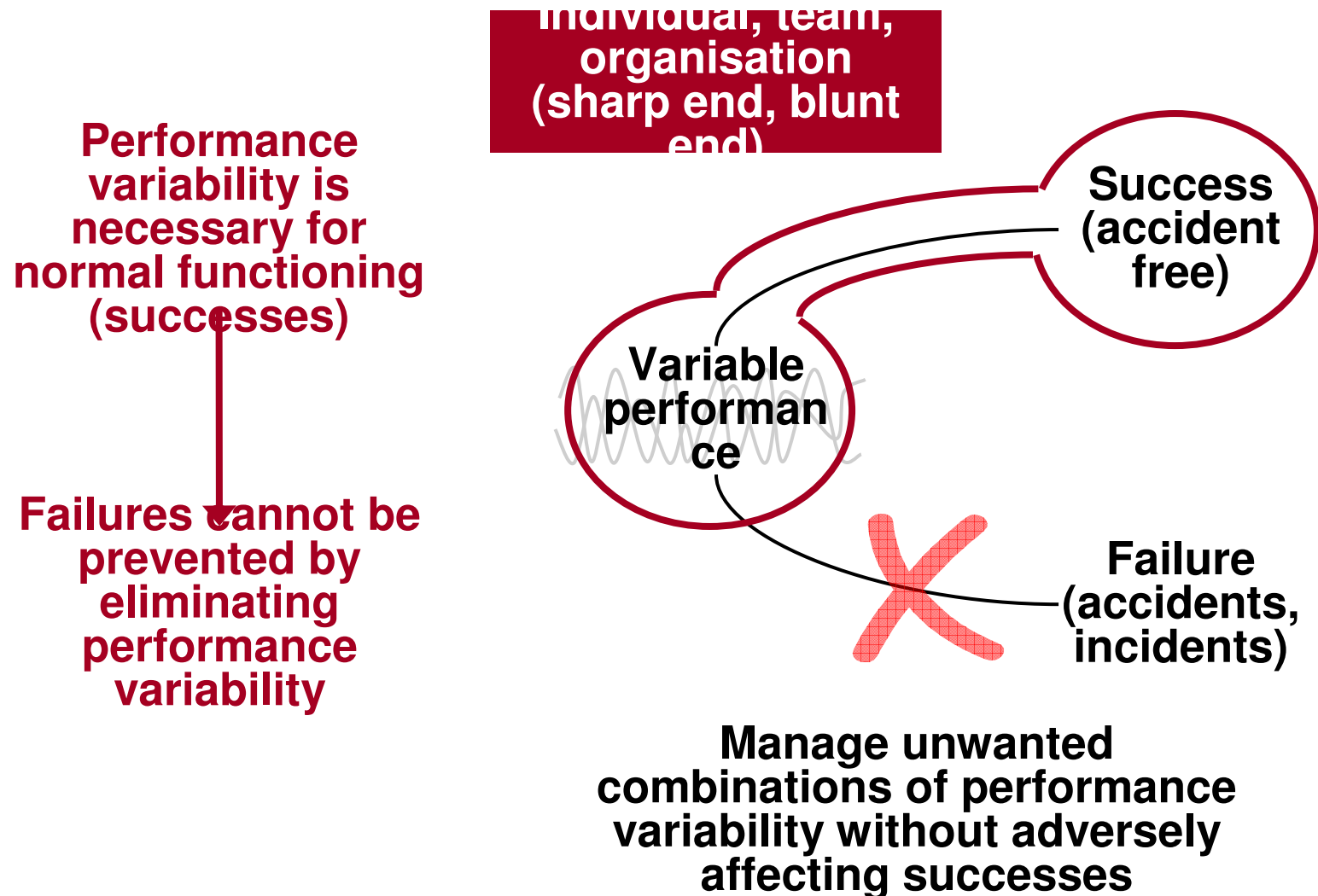
- Learn to **overcome** design flaws and functional glitches
- Adapt** their performance to meet demands
- Interpret** and **apply** procedures to match conditions
- Can **detect** and **correct** when things go wrong

Humans are an **asset** without which the proper functioning of modern technological systems would be impossible.

# Traditional view of failures



# Systemic view of failures



# Resilience design

The design of a safe and effective work system cannot be accomplished only by the **reduction** of something but must also comprise the **increase** of something, namely a capability to anticipate and compensate for large and small disturbances. One proposal for this is **resilience**, defined as the intrinsic ability of a system to adjust its functioning in the face of changes and disturbances so that it can sustain operations even after a major mishap or in presence of continuous stress.

- ➔ Resilience engineering changes the basis for design and operations from an over-reliance on analysis techniques to adaptive and co-adaptive measures and models.
- ➔ Humans are seen as a source of innovation that can adjust ways and means to match working conditions. The purpose of design is therefore to harness this variability to enhance both safety and efficiency.
- ➔ Performance variability should therefore only be eliminated when it is certain that it will never be needed.

The design target consequently changes from the prevention of risk to the creation of resilience



# Merci de votre attention

