The Human role in ensuring and improving resilience

Alberto Pasquini – Deep Blue

Introducing myself

University Degree in Engineering (IT)

Background in safety assessment in the nuclear domain, than in software safety and safety in transportation

Research and professional interest in human reliability, and system safety

Several years (and now part time) with the Italian research body for Energy, Environment and New Technology

Now with Deep Blue, research and consultancy company in human factor, safety and validation in the transportation domain

Introducing myself (more informally)






Resilience in socio technical systems - I

Let's consider resilience as the ability of a system to continue safely its activity in spite of faults, mistakes, and attacks

Considering this simple definition, is your Personal Computer resilient ?

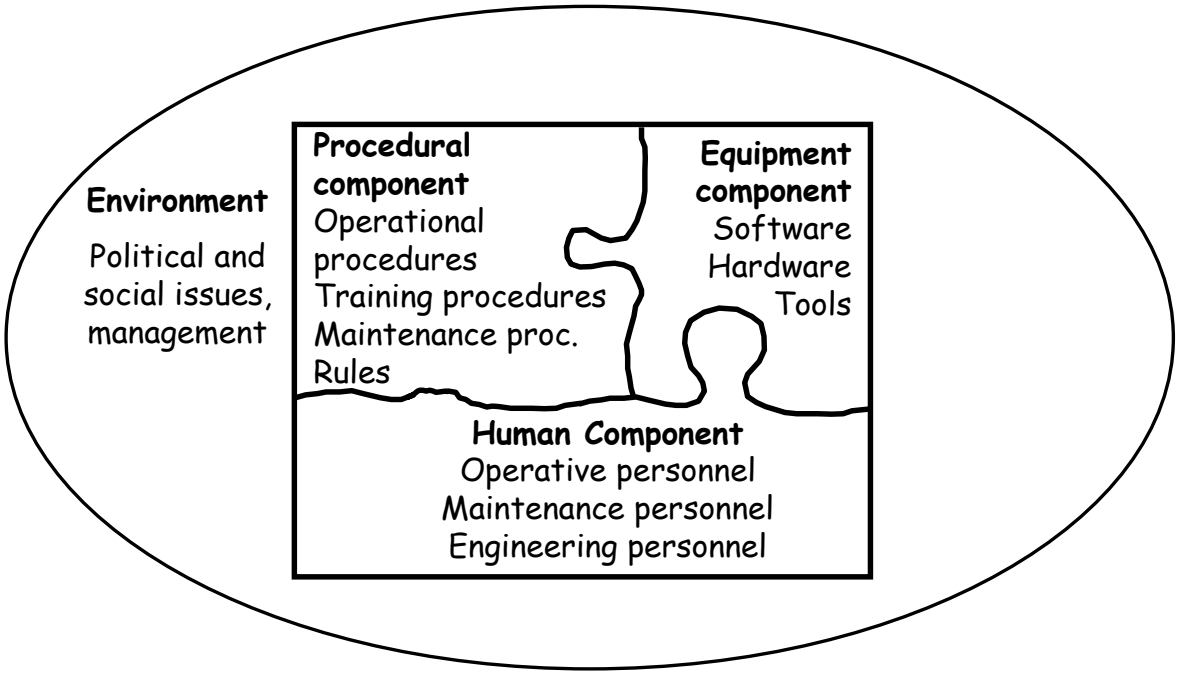
Resilience in a context

Non sense question, without the definition of:

- the objectives of the PC usage;
- the components with which the PC is interacting;
- all the other relevant contextual information.

A socio-technical system is a set of human, technical, and contextual components interacting to achieve a common goal

Components of a socio technical system



Socio technical system – An example

An example of problems originated from unsuccessful interactions with dramatic consequences:

The Uberlingen accident

Equipment component in Uberlingen

Notes:

Human component in Uberlingen

Notes:

Procedural component in Uberlingen

Notes:

Environment in Uberlingen

Notes:

Conclusions from Uberlingen

Socio technical systems can be very large and complex

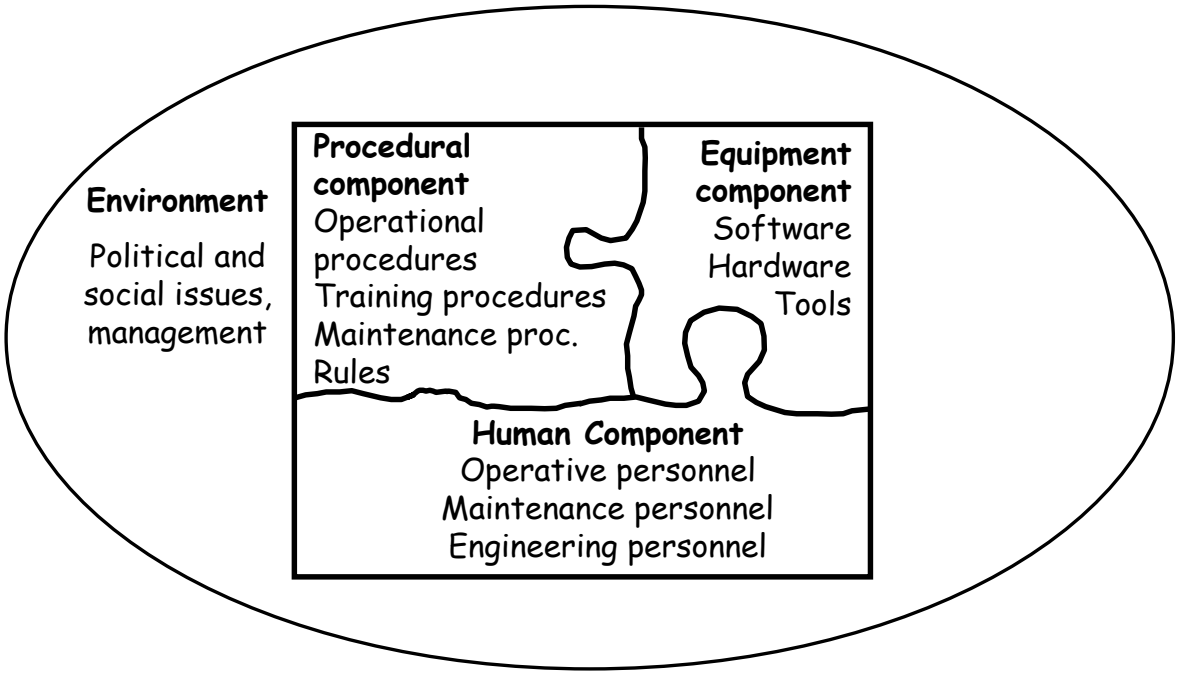
It can be extremely difficult to consider all the components and environmental elements that play a role in the performances (and resilience) of socio technical systems

Components can interact and influence each other in a complex and not forseable way

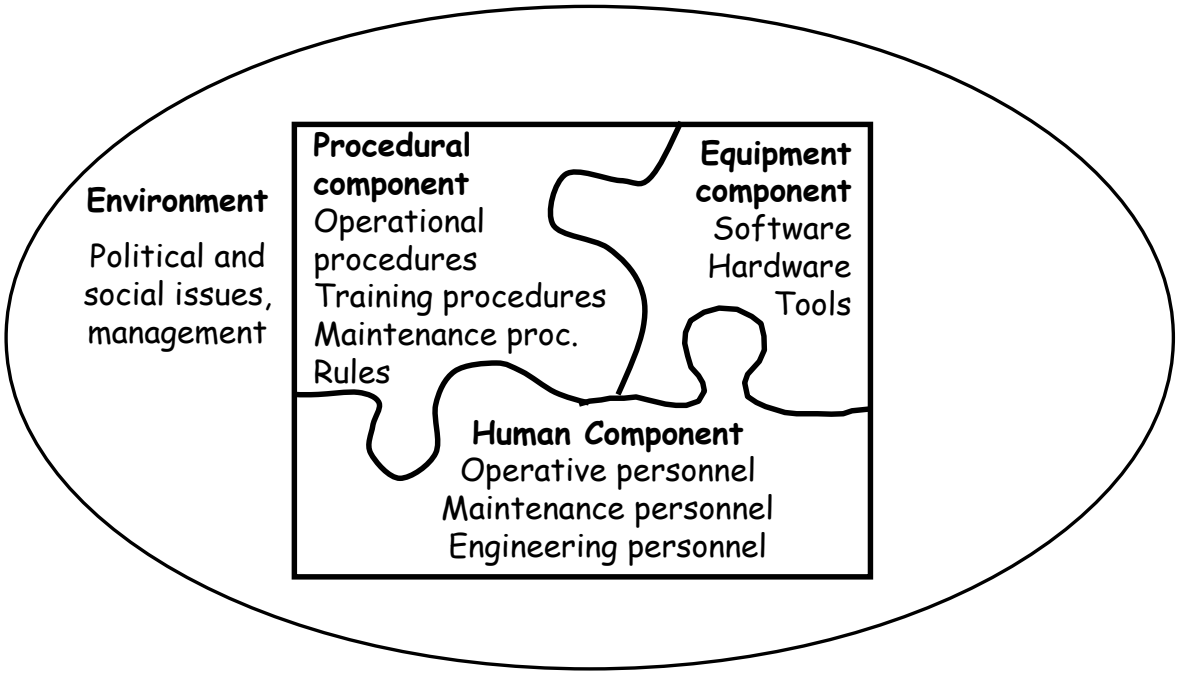
To study the resilience of a single component of a socio technical system in isolation is of limited usefulness

The way in which components interact evolve with time (socio technical systems are evolutionary systems)

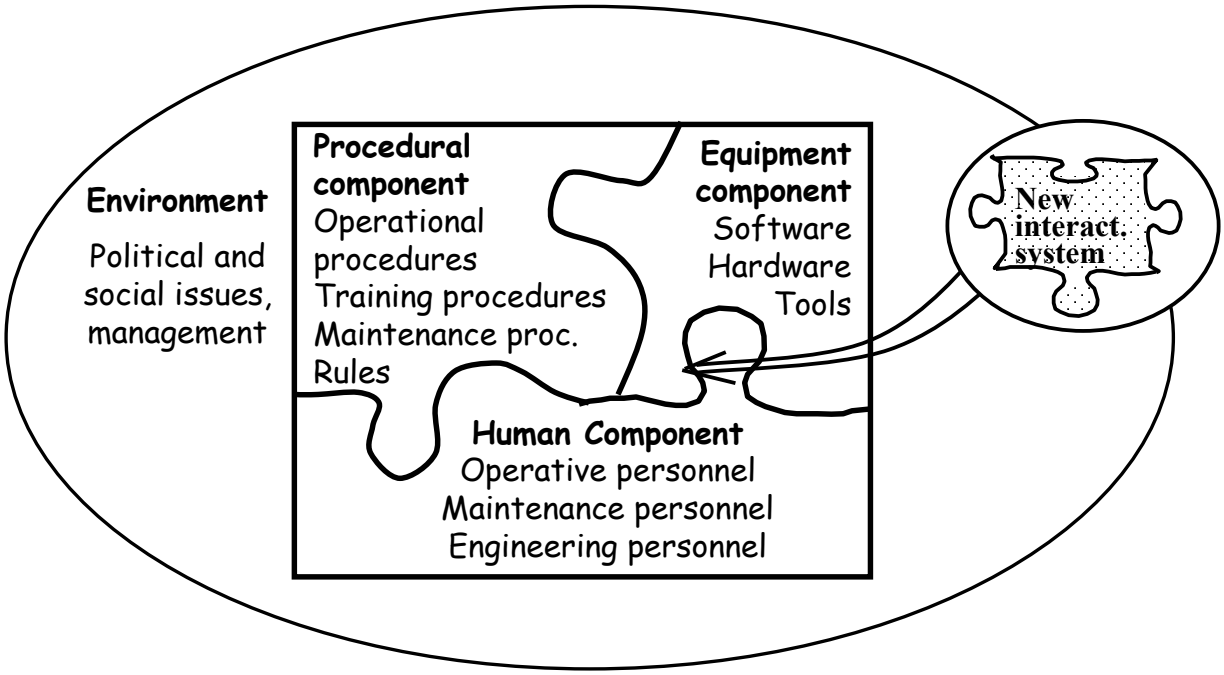
Evolution of socio technical systems



Evolution of socio technical systems



New components in socio technical systems



Main achievements of the Requirements Engineering Community

Modeling and analysis cannot be performed in isolation from the organisational and social context in which the system operates

Resilience of a system can only be properly understood through the analysis of the activity and focusing on the contribution of the system under design to the activity

Resulting Approach for Designing resilient socio technical systems

Activity at the center of the design

⇩

Understand and design the role of all the components contributing to the activity (task allocation)

⇩

Adequate consideration and integration of all the components (human centred design)

Distribution of resources and allocation of tasks

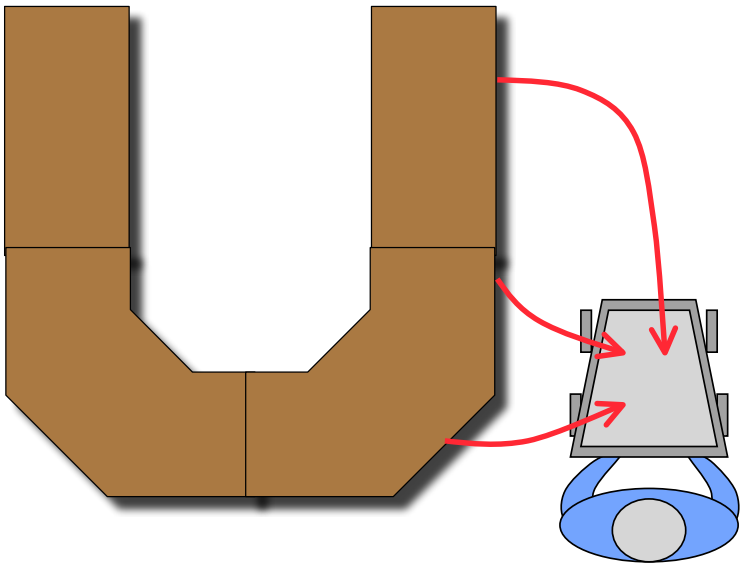
The resources needed for an activity can be distributed in different ways (e.g. document or help on line) and on different components

There is not a single exclusive combination of components to perform a specific activity

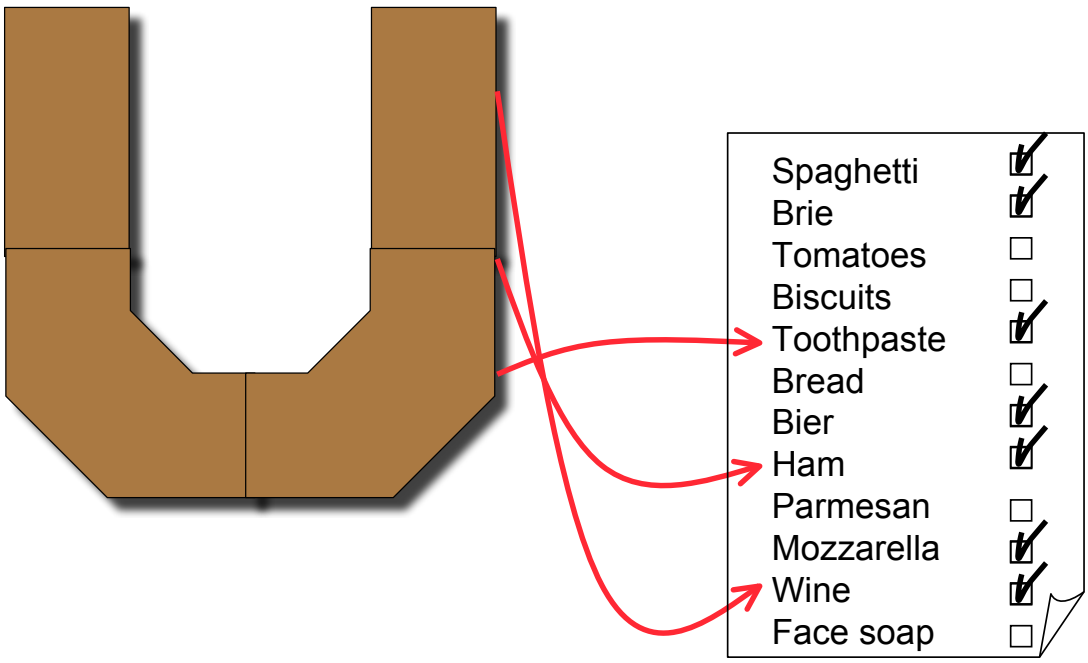
The distribution of resources results in an implicit assignment of tasks to components

Some distribution of resources and then some tasks allocation are more adequate than others to increase the system resilience

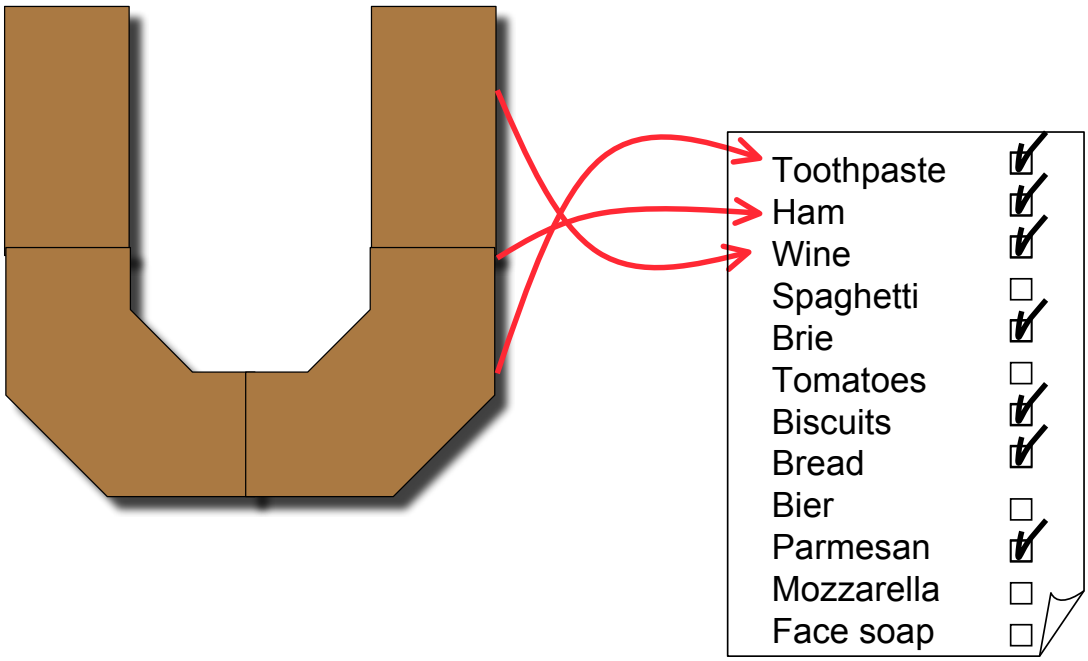
Example of Task Allocation (1)



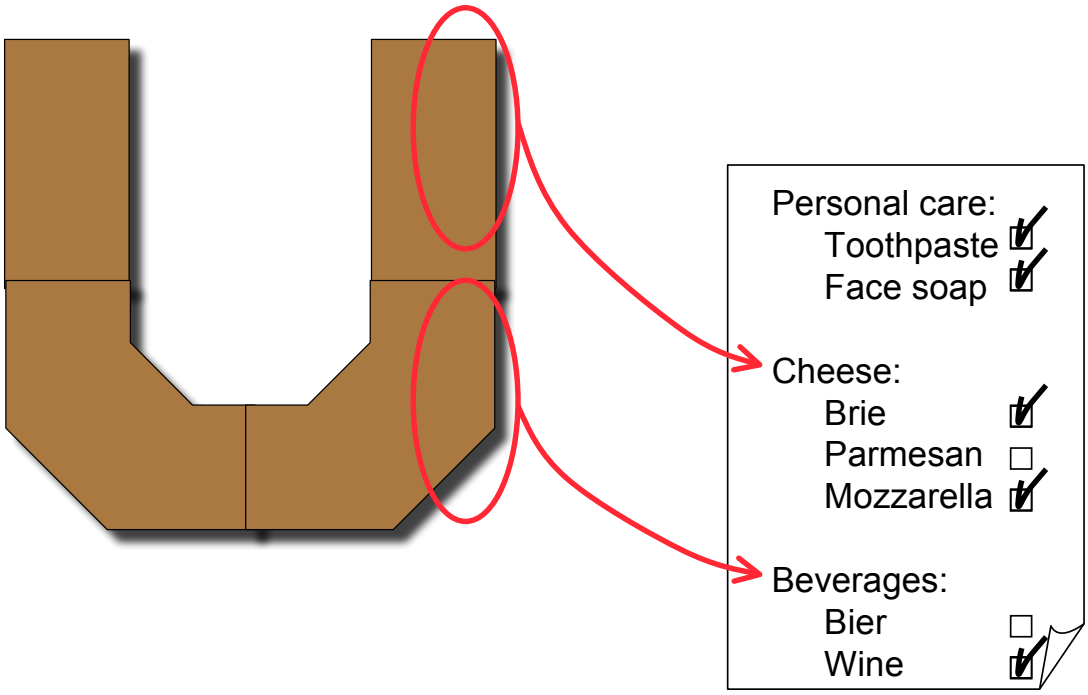
Example of Task Allocation (2)



Example of Task Allocation (3)



Example of Task Allocation (4)



Distribution of resources and allocation of tasks

The resources needed for an activity can be distributed in different ways and on different components

There is not a single exclusive combination of components to perform a specific activity

The distribution of resources results in an implicit assignment of tasks to components

Some distribution of resources and then some tasks allocation are more adequate than others to increase the system resilience

Resulting approach for designing resilient socio technical systems

Activity at the center of the design

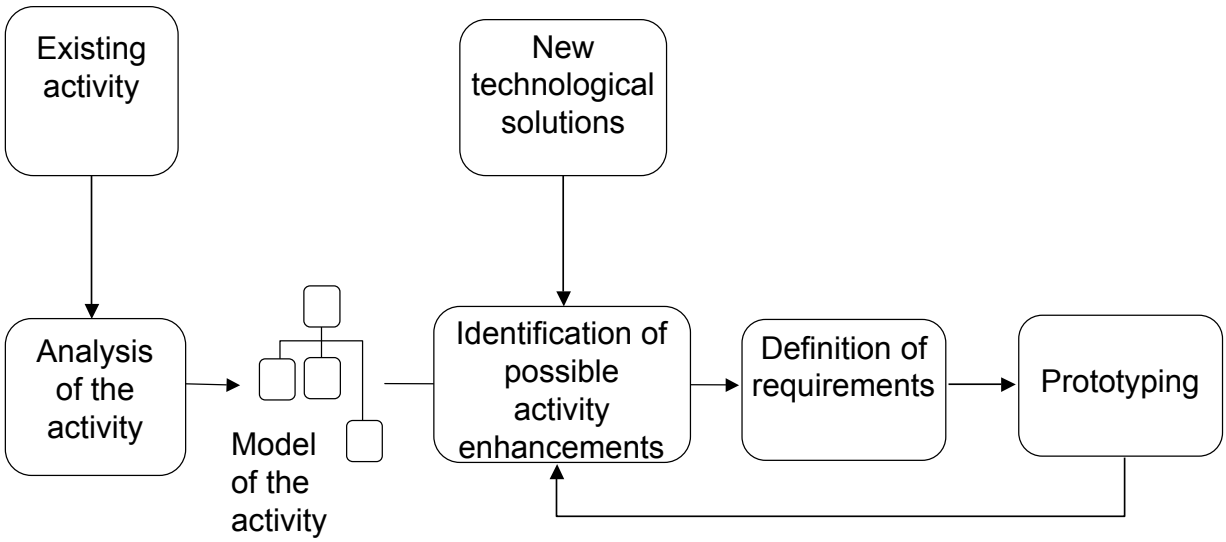
⇓

Understand and design the role of all the components contributing to the activity (task allocation)

⇓

Adequate consideration and integration of all the components (human centred design)

Requirement definition for socio technical systems



Suggested readings for this part

Socio technical systems:

- http://en.wikipedia.org/wiki/Sociotechnical_systems_theory
- Walker, G.H., Stanton, N. A., Young, M. S., Jenkins, D. & Salmon, P. Sociotechnical theory and NEC system design, HCII, Beijing, 2007

Uberlingen:

- http://www.bfu-web.de/cln_009/nn_53086/EN/Publications/Investigation_20Report/reports__node.html__nnn=true
- www.dcs.gla.ac.uk/~johnson/Eurocontrol/Ueberlingen/Ueberlingen_Final_Report.pdf

Task Allocation:

- J. Hoc, S. Debernard, From dynamic task allocation to function delegation in air traffic control, Procs of ECCE-11, September 8-11, 2002, Catania, Italy
- M. A. Sujan, A. Pasquini, Allocating Tasks between Humans and Machines in Complex Systems, 4th Conference on Achieving Quality in SW, Venezia, 1998

Human Centred Design:

- ISO13407, Human-centred design processes for interactive systems, 1999
- Trump Project: www.usabilitynet.org/trump/methods/index.htm
- Interaction Design, Inc. (2001) - Design does provide return on investment. http://www.user.com/transaction-anddesign.htm.

Humans and errors - I

We have seen that humans are an essential component of socio technical system, working in interaction with the other components

Shall we expect errors from humans ?

Let's look for the answer in this movie

As you can see humans make mistakes since the beginning, and not only by chance, they make use of mistakes to learn how to interact with the external word

Humans and errors - II

Humans make mistakes since the beginning, and not only by chance, they make use of mistakes to learn how to interact with the external word

The real world is too complex to evaluate, from a theoretical prespective, all the possible options

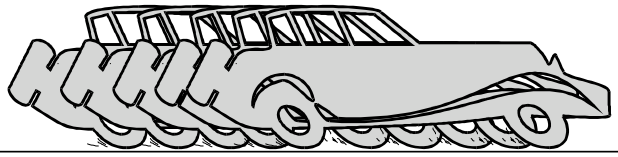
The human approach is to try the most promising options and choose on the basis of the results

Errors are the outcome of investigating non successful options

You experience of errors

Do you have a drive license ?

Do you remember when you tried to drive the car for the first time ?



Do you remember the "try and learn" process to find the just balance between gas pressure and clutch pressure release ?

Errors and successes - I

Humans explore different options in interacting with the external word

Learning from errors humans are able to identify and apply standard solutions in consolidated situations and to extrapolate possible solutions for new situations

Humans are essential to ensure resilience when systems have to afford the unexpected

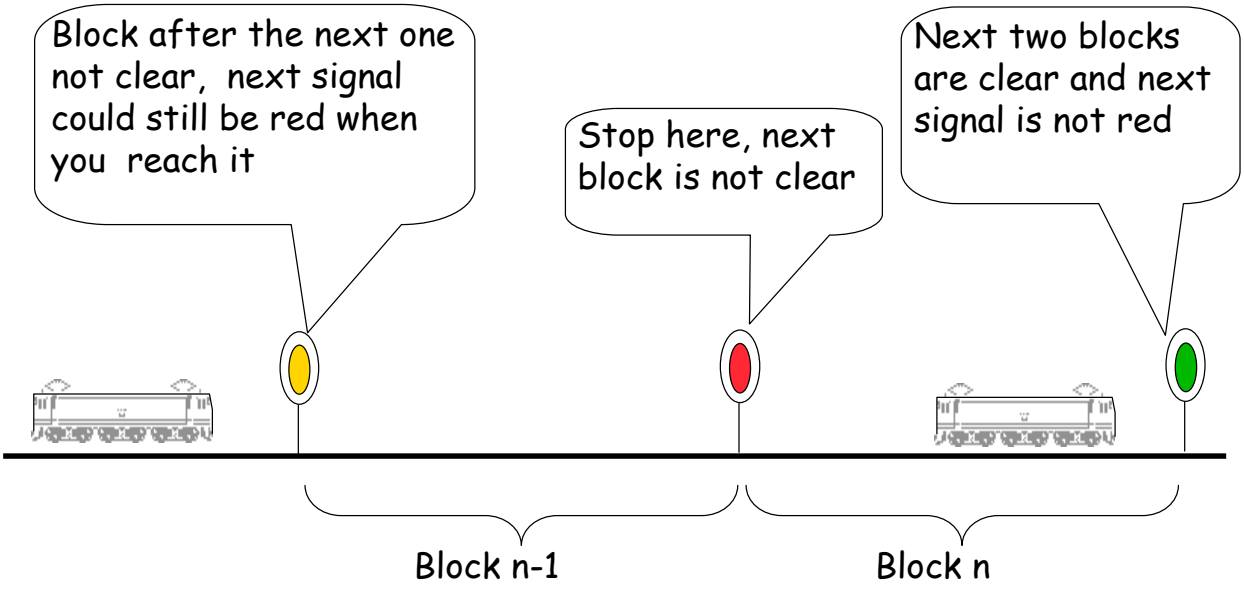
Errors and successes - II

To reason about different options requires an understanding and a model of the external world

Major problems are related with mismatches between this internal model and the real world

Let's analyse an incident in the transportation domain

The separation mechanism in the railways



What is a SPAD ?

SPAD = Signal Passed At Danger

Not allowed and potentially dangerous passage of a red signal by a train driver

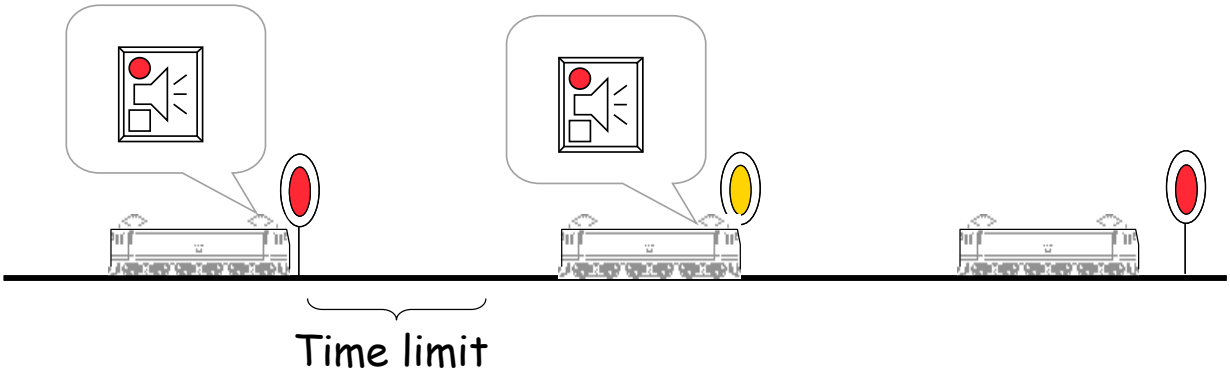
- Relatively frequent event (about 200 SPADs a year reported in the UK)
- Signal passed by few meters in most of the cases but extremely dangerous in a few situations
- SPADs considered as the main cause of severe incidents in the railways

The signal Repetition System - I

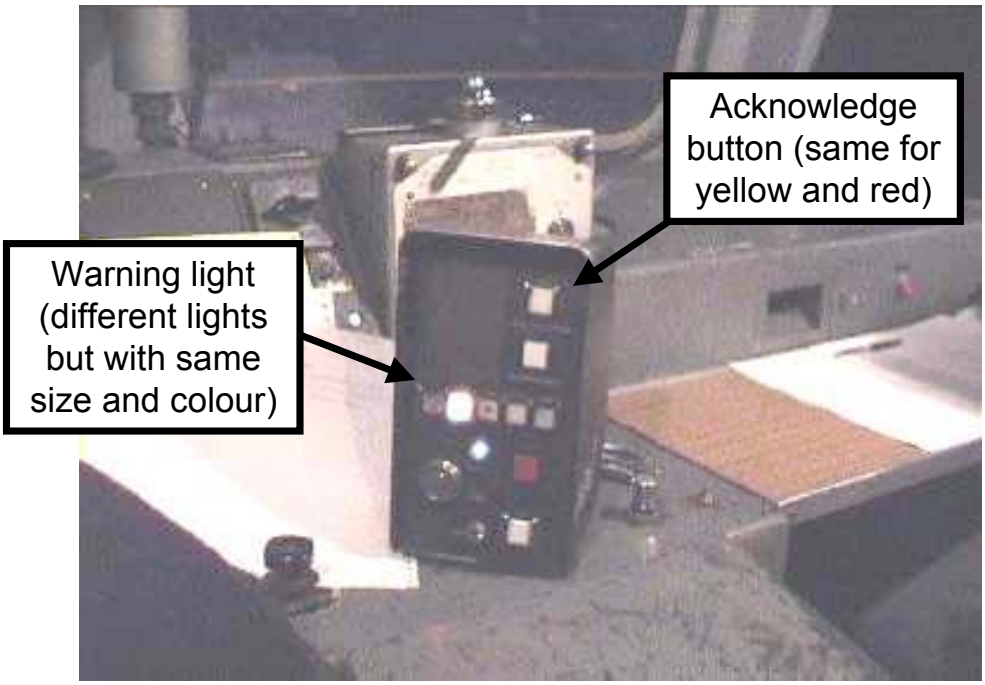
Control of the speed of the train and comparison with the line limits

Status of the signal the train is going to encounter (light and horn)

Acknowledge within a time limit for signals other than green otherwise automatic emergency break



The signal Repetition System - II



The supposed operative usage

Train position	Main resources involved in the process			
	Train driver	Signal repetition system	Signal	Braking system
Entering the block				
Running the block				
Approaching the signal				

However the final responsibility for breaking with red signal rests with the driver

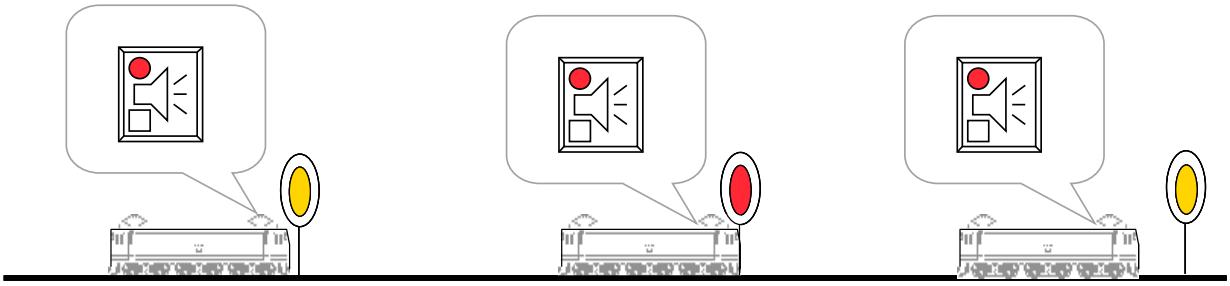
Accident analysis

Accident involving the system

- Train departing at 7:29 from station A with a yellow signal;
- Increasing speed while passing several green signals;
- Passing three yellow signals and then a red one when entering station B at 7:36
- No physical damages or injuries to humans;
- Perfect environmental conditions with good weather and good visibility;
- Two experienced drivers, not tired, with no physical problems
- Perfectly working Signal Repetition System

Frequent condition - I

- Experienced drivers do not perceive the system as a support but rather as a disturbance to be silenced as soon as possible
- This type of interaction is quite common
- Automatic habit perceived as a potential critical issue only when reviewing the activity with video



Frequent condition - II

The real operative usage

Train position	Main resources involved in the process			
	Train driver	Signal repetition system	Signal	Braking system
Entering the block				
Running the block				
Approaching the signal				

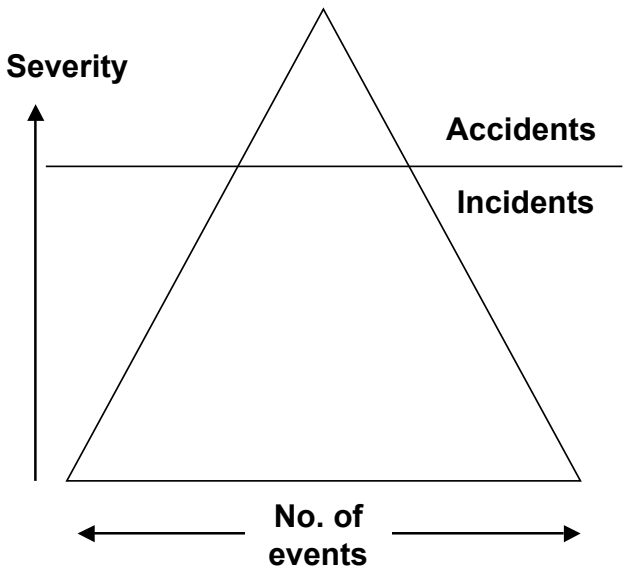
The positive contribution of humans - I

Learning from errors humans are able to identify and apply standard solutions in consolidated situations and to extrapolate possible solutions for new situations

Humans are able to provide unforeseen but adequate service and to provide expected service under unplanned conditions, anticipating incidents and accident prone situations

Humans are essential to ensure resilience when systems have to afford the unexpected

The positive contribution of humans - II



Increase resilience of socio-technical systems

Error prevention and removal

Error tolerance by designing system that are able to tolerate the human errors (not imparing the possible positive unplanned human contribution to resilience)

Exploit the human ability to afford the unexpected

Increase the overall system resilience by learning from problems and incidents, but also from successes

Suggested readings for this part

Understanding human errors:

- Wallace, B. & Ross, A. (2006). Beyond Human Error: Taxonomies and Safety Science. Boca Raton, Florida: Taylor & Francis.
- Reason, J.T. (1990). Human Error. Cambridge, UK: Cambridge University Press.

The railways incident:

- Pasquini, A., Rizzo, A., Save, L. (2004) A methodology for the analysis of SPAD. Safety Science. Vol. 42, 437-455.

Human as a resource for increasing system resilience:

- Reason, J.T. (1997). Managing the Risks of Organisational Accidents. Aldershot, UK: Ashgate.
- EUROCONTROL Success Case Approach (SCDM), Gilles le GaloSafety, Security and Human FactorsEurocontrol
- Clark, D. M., Human redundancy in complex, hazardous systems: A theoretical framework, Safety Science, 43, 655-677, 2005.

Porquerolles:

- Georges Simenon, My Friend Maigret, Penguin, June 2003.