CESAMES

Centre d'Excellence Sur l'Architecture, le Management et l'Economie des Systèmes

System Requirements Control & Risks Control: Mind the gap!!

October 27-29, 2010 – Cité Universitaire, Paris (France)

Alain COINTET – RATP
Catherine LAVAL – APTE System

Table of contents

6 questions to set the problem

Do classic approaches allow answering these questions?

Requirements and risk: to cross the gap
- **through a systemic and functional approach**
- **through the defense in depth concept**

…by avoiding the current confusions

Development & illustrations with an example

As a conclusion and to open the debate..
what answers against preliminary questions?

6 questions to identify the problem

The impact of the logic of requirements definition on the relevance of identification and evaluation of risks

1. How can we guarantee that the needs and constraints identified in the "customer" specifications constitute the complete set of requirements attached to the various functions?
2. How to help the "customer" to express the multiple aspects of needs by keeping distance with technical solutions?
3. How to distinguish the safety and security functions?
4. How to bring to light that the same function can have different safety and security levels, according to the contexts of system use?
5. How to deal with safety functions of segregated levels?
6. How to identify the risks connected to the non compliance with these requirements or to the inadequacy of requirements?

Do classic approaches allow answering these questions?

From side of requirements, …. partially because…

❑ Confusion between point of views (client, operator, designer)

The expression "***capture of requirements***" …..

… the almost documentary analysis of their textual formalizations more than the reasoning on needs and constraints

The « ***traceability of requirements*** »…

Logic of "conformity" with the specified requirements, but with the real needs?

❑ Frequent confusion between notion of requirements and performances…

needs and operational constraints … ≠ reachable results by the possible solutions ….!!!

Do classic approaches allow answering these questions?

… from side of risks, partially because…

Risk analysis (PHA, PRA, FMEA,…), performed within the project to secure the system, essentially treat risks linked to failures on envisaged technical solutions

→ And then by addition of "barriers", making the final system more complex and more fragile

From the beginning, design efficiency should allow to make choices which guarantee the expected safety levels

Do classic approaches allow answering these questions?

« If we do not change our way of thinking, we shall not be able of resolving the problems which we create with our current modes of thought " »

… Albert EINSTEIN …

Requirements & Risks: Gap via systemic and functional approach

Limits and confusions in methodology..

Improper use of word « systemic »…

The polysemy of term «functional analysis»…

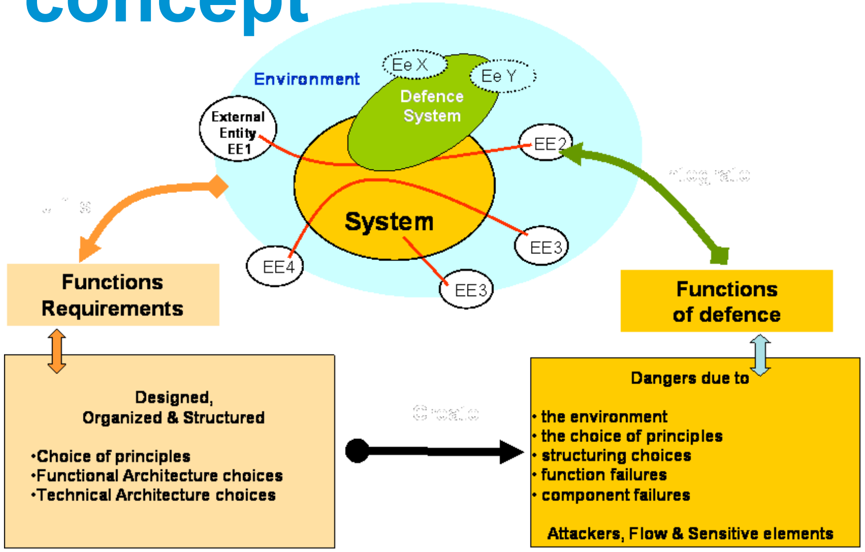
Too superficial control of methods..

… to be rigorous, a functional & systemic approach , should integrate…

- **<u>steps upstream</u>: identification & structuring of finality, environment, interactions with those environment, needs with justifications, then their breakdown into functions & constraints**
- **<u>steps of design</u>: creative research of principles & field of possibilities,**
- **traceability from goals, functions, requirements, & their breakdown through justified choice of principles**

Needs, functions & constraints are independents from solutions, more stables, on condition with reasoning with a systemic approach

Requirements & Risks: Gap via “defence in depth concept”



Functions Requirements

Designed,
Organized & Structured

- Choice of principles
- Functional Architecture choices
- Technical Architecture choices

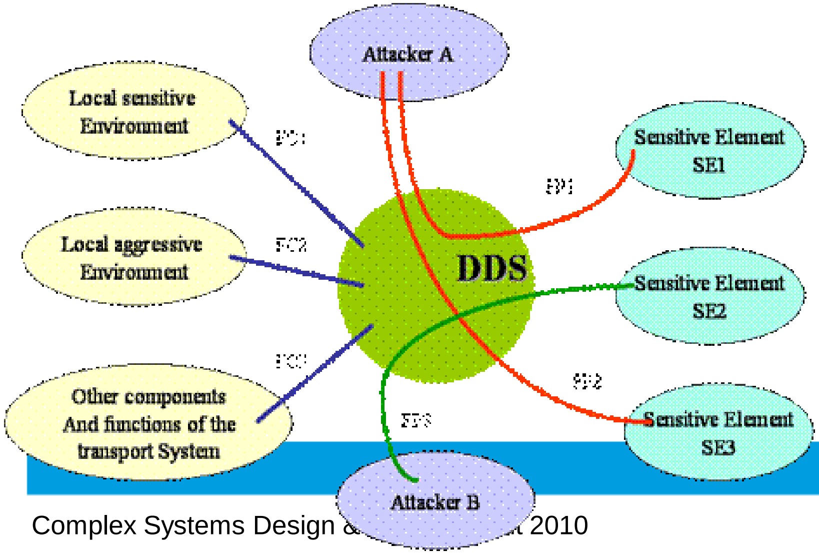
Functions of defence

Dangers due to

- the environment
- the choice of principles
- structuring choices
- function failures
- component failures

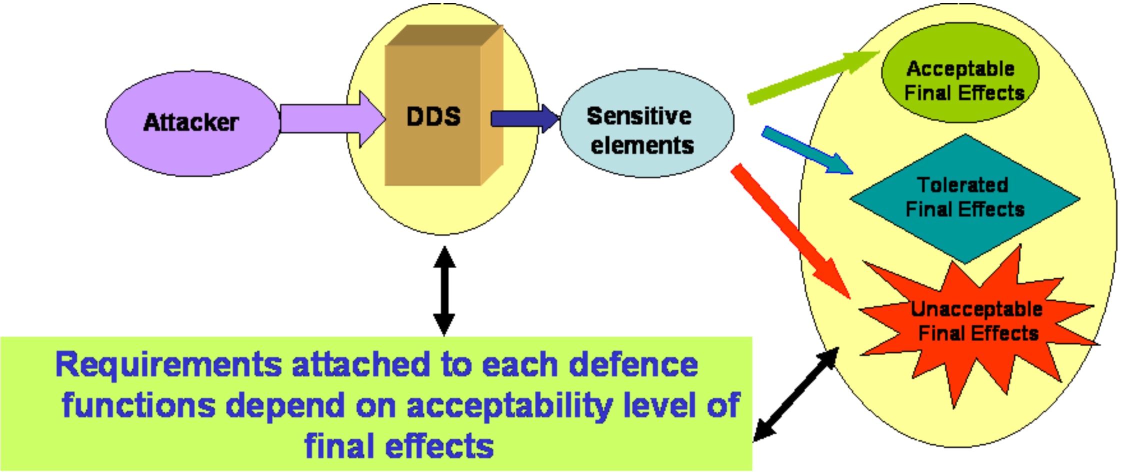
Attackers, Flow & Sensitive elements

The process of identification and analysis of a defence system is a part of the overall process of risk control.


Attacker A
Local sensitive Environment
Local aggressive Environment
Other components And functions of the transport System
FC1
FC2
FC3
DDS
FP1
FP2
FP3
Sensitive Element SE1
Sensitive Element SE2
Sensitive Element SE3
Attacker B

Defence functions derive from system functional analyses and expressed in term of involved entities such as attacker, aggressive flow and sensitive elements which can be internal or external

Requirements & Risks: Gap via “defence in depth concept”

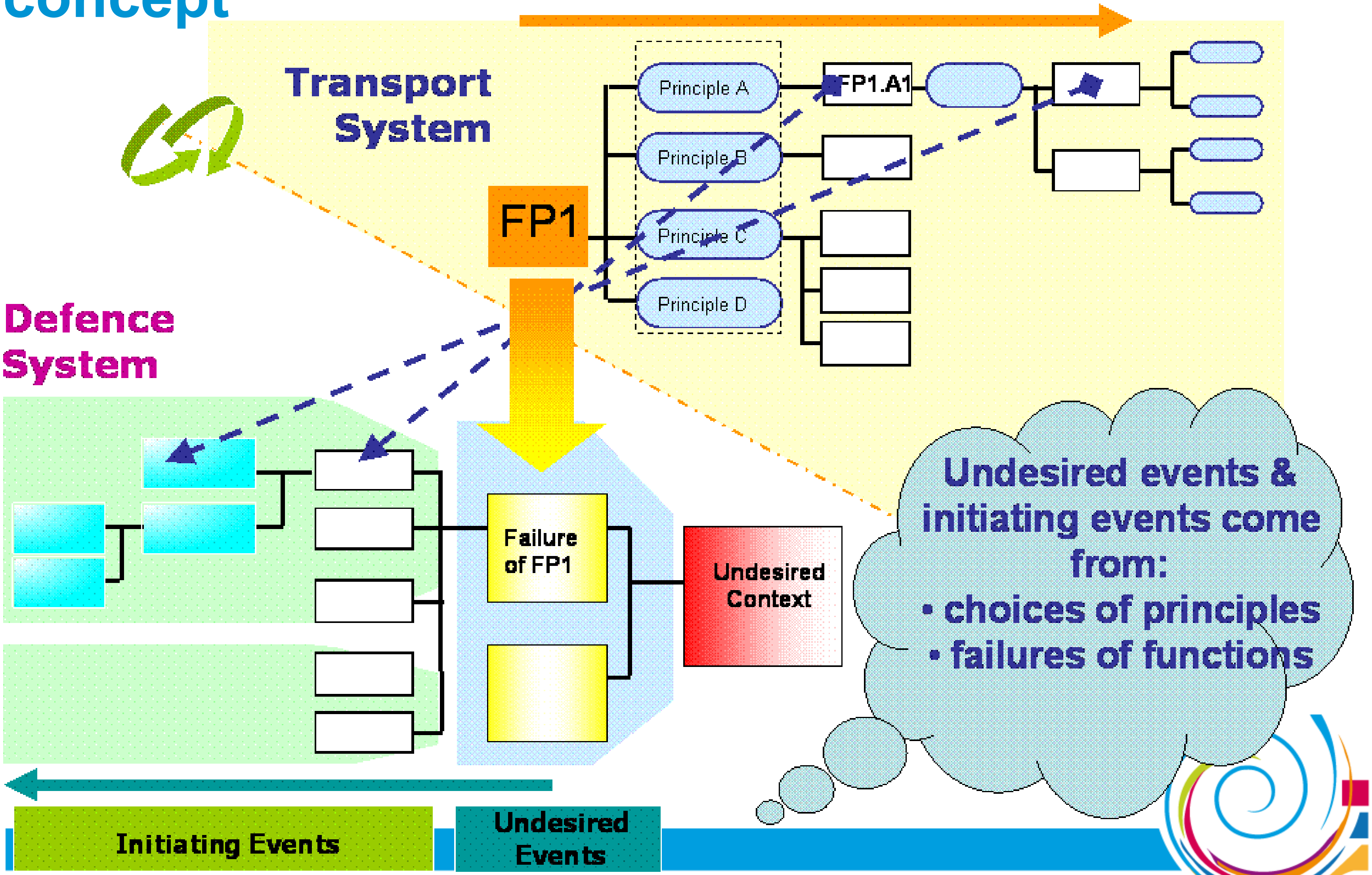


Requirements attached to each defence functions depend on acceptability level of final effects

- Physical integrity of people
- Physical integrity of system
- Quality of service offered
- Image of company
- Environment
- Financial contribution
- Company organization

Control of final effects

Requirements & Risks: Gap via “defence in depth concept”

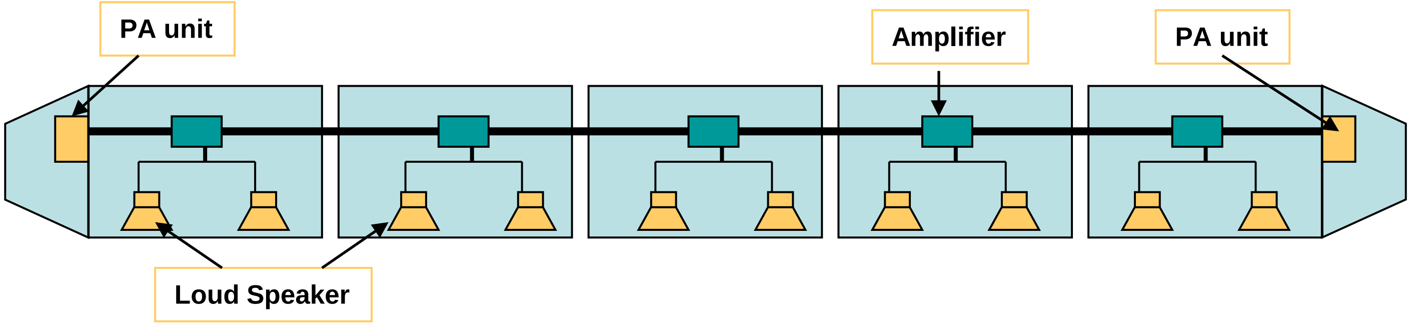


Undesired events & initiating events come from:

- choices of principles
- failures of functions

Functional approach ?

FP1: To allow the driver to deliver messages (sound) of service to the passengers inside the train.

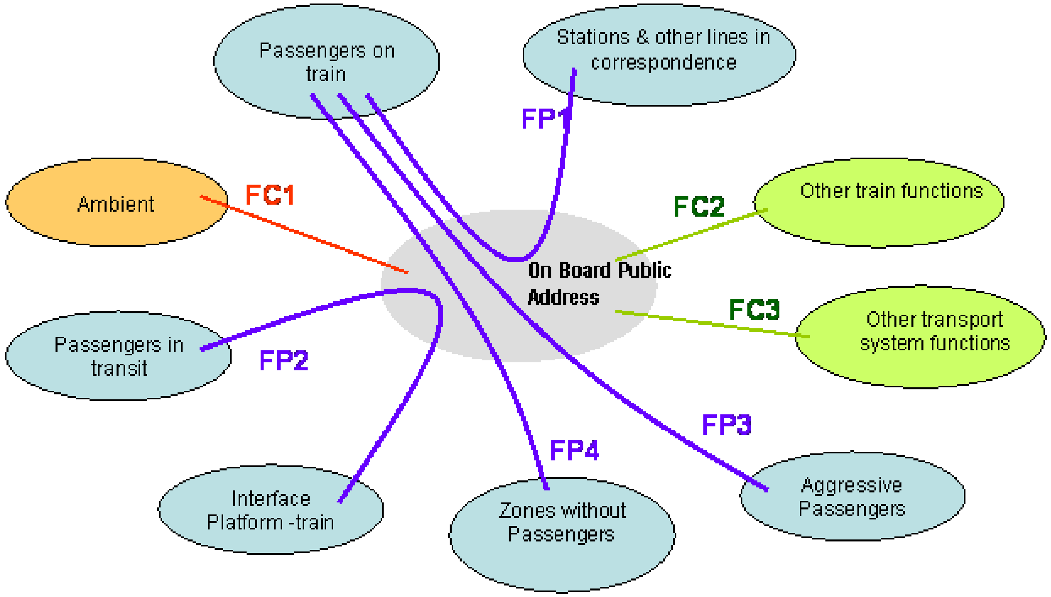


© RATP - MARGUERITE Bruno 243509 - 08/02/2000

<u>In term of Requirements</u>:
•the quality of the delivered message (content, speech, relevance, language),
•the sound level inside the cars (decibel, spatial distribution),
•the frequency of messages,
•system reconfiguration in case of failure (resiliency).

<u>In term of Risks</u>:
- ***quality of service***
- ***comfort of travel***

Functional & Systemic Approach Finalities of communication



Do not forget failures modes & degraded conditions :
- train evacuation in tunnel,
- non door opening

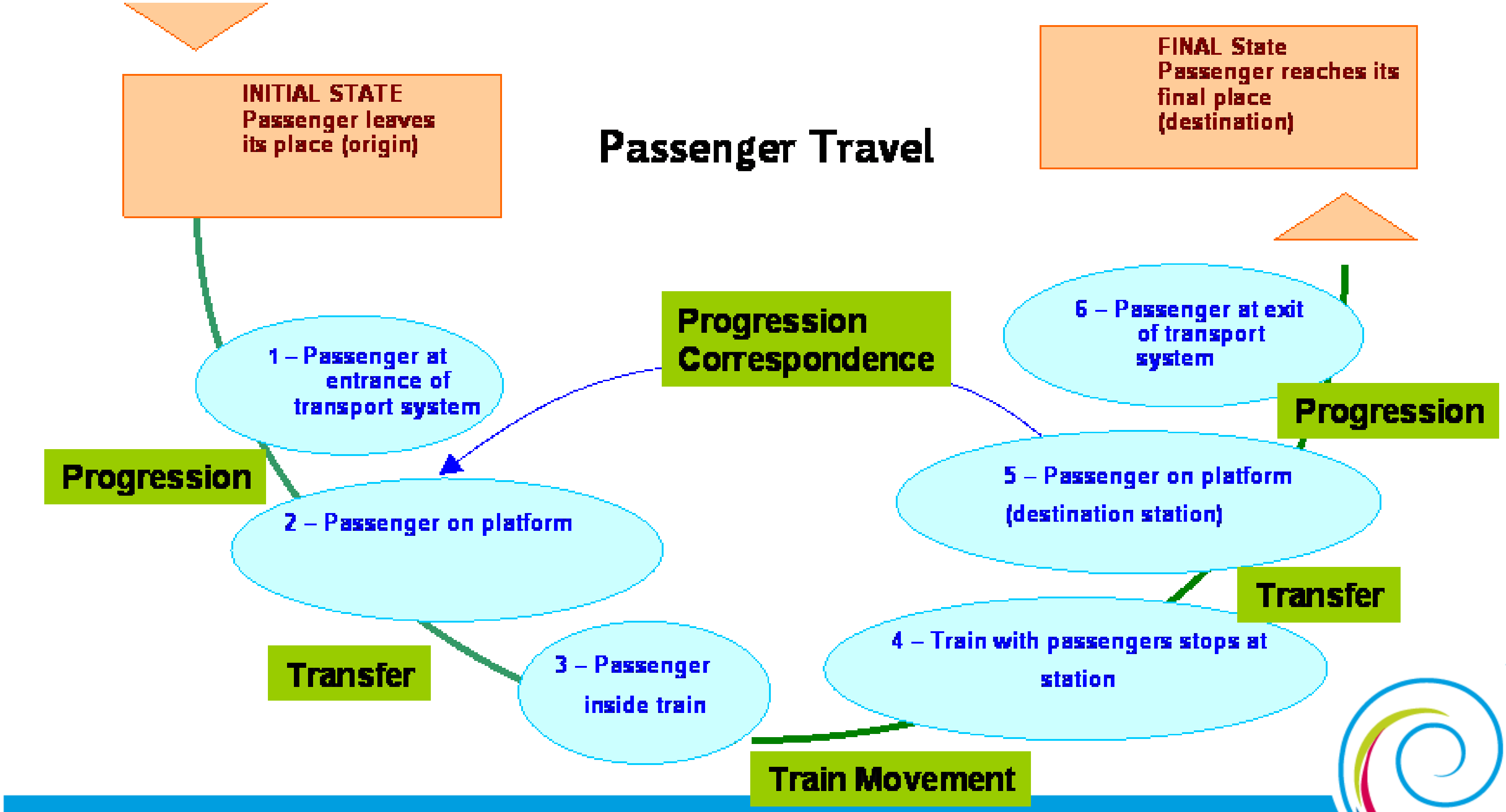
according context….
Function of Security

FP1: To provide passengers with information for their travels
FP2: To prevent or resolve a passenger related undesired event during platform train transfer
FP3: To protect passengers against aggressions during their travels
FP4: To protect passengers from invasion of non revenue operations areas

In term of Risks:
•quality of service, comfort,
•& security of travel,
•but also protection of infrastructures

Functional & Systemic Approach
Interactions with environment

Into which environments (functional, organisational and technical) does the onboard Public Address system integrate?



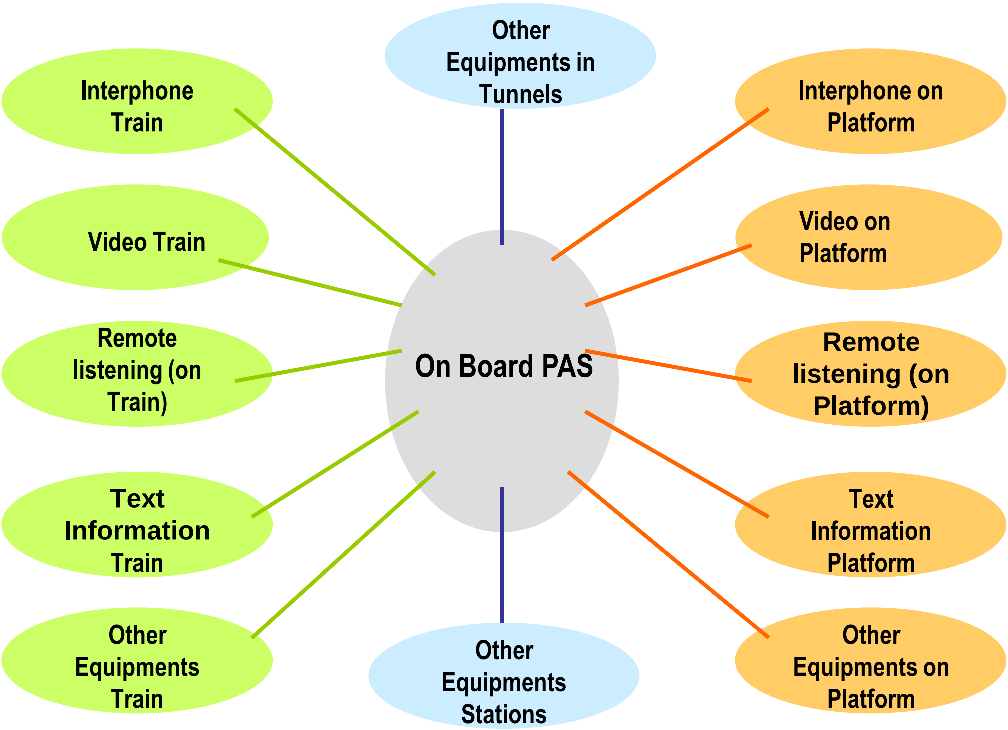
Functional & Systemic Approach
Interactions with environment

The need to communicate information to the passengers is not limited to the movement aboard the train:

- coherence of message between train & platform?
- priority of messages?

The functions become transverse and integrate all the interfaces

This global need of information to be delivered to passengers leads to consider a system gathering audio and visual means which need to serve both passengers and operator


Other Equipments in Tunnels
Interphone Train
Interphone on Platform
Video Train
Video on Platform
On Board PAS
Remote listening (on Train)
Remote listening (on Platform)
Text Information Train
Text Information Platform
Other Equipments Train
Other Equipments Stations
Other Equipments on Platform

<u>In term of Requirements</u>:

- Integration with existing sub systems
- failure modes (breakdown detection, resiliency, system "fall back")

<u>In term of Risks</u>:

•All final effects to be considered with a defence system approach

As a conclusion… to open the debate…

1 - How can we guarantee that needs and constraints identified in the client's « Terms of Reference » represent the set of requirements pertaining to the various functions? And that they are optimised for the benefit of the targeted needs?

By carrying out a real systemic functional approach to focus the object of the study in relation to:

- **finalities it has to contribute,**
- **envisaged context of operation**
- **interface with the external environment**
- **conditions and modes of functioning :*nominal mode and contexts of use, failure modes, degraded situations (related to the environment).***

By finding the design choices allowing passing from the needs to the functionalities of the object, and to dispatch those needs in requirements

By adopting an approach over passing the contractual point of view with a "client".

2 - How to help the « client" in expressing the multiple aspects of their needs while establishing the required distance with the technical solutions?

By avoiding pushing the customer towards solutions " on shelf " …

By helping the client into adopting a more prospective approach and considering the system or equipment studied as a black box interacting with various environments

As a conclusion… to open the debate…

3 - How to distinguish the safety functions?

By clarifying the meaning of the term “safety function”

By making sure that the "customer" expressed well the acceptability levels of final effects, and that he defined the priorities.

4 - How to prove that the same function can have different levels of safety according to the contexts of use?

By assessing each context as a standpoint and then to only make the synthesis

5 - How to deal with a function featuring different levels of safety according to the contexts?

By reasoning at first at general principles of solutions, which appear to be in a limited number:

- Then either in over sizing the solution with regard to the most constraining level of safety,
- Or in developing adjusted solutions to each context (to which one transition management function will be associated).

As a conclusion… to open the debate…

6 - How to identify risks linked to inadequate respect or the insufficiency of requirements? ?

By applying answers as per questions 1 to 6….!

The main sources of danger and their associated risks can be early identified in an independent way from the solutions because they are linked to:
•Interactions;
•degraded situations and/or failure modes of functions expected in nominal situations

They will then have to be completed by the risks which can be generated by choices of retained principles, choices of functional architecture and correlated interfaces, choices of technical architecture and correlated interfaces.

By applying a rigorous and global method (such as Defence in Depth) with the intent to identify risk reduction dispositions, the related requirements and the ultimate goals.

Thank you for your attention

Alain COINTET – RATP
alain.cointet@ratp.fr

Catherine LAVAL – APTE System
catherine.laval@apte-system.com