Complex system understanding back to basics! The functional analysis tracking a railway system case

A. Cointet[1] & C. Laval[2]
[1]*RATP Transport System Risk Control, France*
[2]*APTE System, France*

Abstract

It has been the tendency for some years, which is still confirmed today, to try to model complex systems by means of software, of successful languages and of algorithms in order to better understand, to optimize and even to develop them. However, in many cases, this modelling attempts to describe the functioning of the existing system. To analyze an existing system by its functioning description can present certain advantages but also inconveniences as for its complete understanding within the framework of objectives of diagnosis, optimization or evolution. To be able to visualize the system considered at different detailed levels, to act on parameters and to analyze diverse behaviours are, among others, part of the advantages. To develop a system by acting on functioning parameters in the aim of optimization does not guarantee a relevant result. This modelling hides the wide register of choices reserved or not reserved, and thus the logics of decisions which led to the existing solution. Furthermore, this modelling brings no proof that:

- performances of the system are strictly in a direct link with the initial requirements,
- all the interactions with the environments of the system are well taken into account.

Moreover, it becomes even more significant when we approach the management of the risks attached to the considered system. This paper suggests the consideration of functional analysis and a description to model the complex system considered.

Keywords: functional analysis, system engineering, risk management, defence in depth.

WIT Transactions on The Built Environment, Vol 128, © 2012 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT120471

1 Introduction

Based on RATP's experience related to railway complex system management, a part of risk management is supported by models and reference frameworks. RATP creates these supports by considering systemic and functional description of the transport system. The "complement to understanding" that offers a rigorous and opened functional approach, carried out upstream, can bring elements of answer more than useful in the frame of a complex system control. The paper will also show in which way the results of this approach improve the knowledge of the system and its environment, providing to different actors a better understanding of risks generated by the system and its environment.

2 Method

2.1 Objective

Three keys points appear, when an operator faces risks attached to the transport system and its environment, such as:

- Complexity: systems become more and more complex, interfaces between system components and constraints or interfaces with the environment of the considered system increase rapidly.
- Uncertainty: evolutions of an existing system are frequent, often implemented quickly without exploring all the interactions and consequences, creating a part of uncertainty regarding the capacity to guarantee the required safety level all the time. It must be taken into account evolutions coming elements of the environment (human, components, regulation…) in interaction with the system considered.
- Readability: the overall knowledge of the system is fundamental to maintain high level of risk control.

These key points underline the necessity to have a reference, a model that describes the system of transportation, translating the initial need by functions with the requirement levels which are expressed in terms of comfort, of speed and of safety and security. Attached to this model inherent dangers of the considered system, must be also hung. This model is generic and independent of the technical solution. This paper develops the diverse steps of model construction.

2.2 Process

In term of risk control, especially for complex system, a lot of questions regularly raises and points directly on the system knowledge. Among those questions, there are the following:

- Is our knowledge sufficient to operate such system?
- Is our knowledge sufficient to control risks attached to the system?
- Is our knowledge sufficient to anticipate what will happen?

- Is our knowledge sufficient to adapt the system (according to life cycle)?

RATP's approach relies on a functional description and aims to answer to those previous questions by providing experts and specialist with a set of views. Those combined views help to create at first a generic reference framework, then a reference framework according to the different transport modes and for each specific line a functional description which is directly connected with the existing line. The set of descriptions must be coherent.

It must be clarified in this approach that the term "function" does not mean "functioning" but must be associated with notions such as needs, expected service, usage.

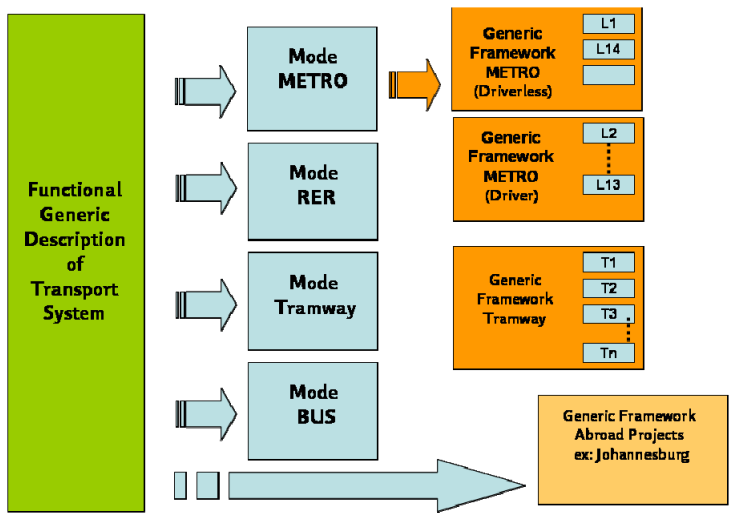

Figure 1: Set of generic and specific functional frameworks.

2.3 Generic description "top level"

This reference framework, based on functional model, traces the initial requirements [1], their successive allocations, the choices of principles reserved or not and, if the history allows it, the justifications of these choices.

In every stage of the functional breakdown it is possible to characterize functions and sub-functions by at once significant parameters of needs, constraints, upstream choices of principles, and associated risks.

It is possible at this stage to identify the safety functions and while examining the distribution of the requirements, to make obvious sub functions that will take charge of these safety requirements.

The functional description is built following a structured method called "APTE® method", which imposes for each step of the breakdown, to specify the function and the choices of principles which can be used to develop the cited function.

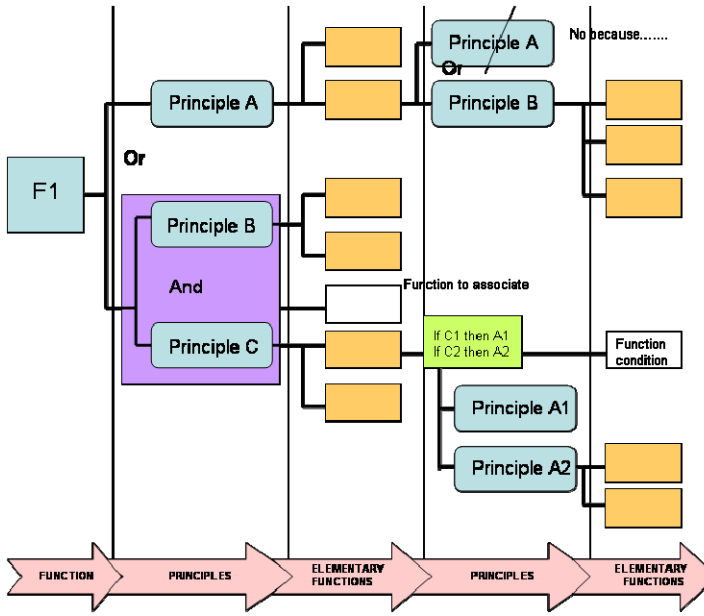

Figure 2: Function and choices of principles.

These choices of principle are gradually going to direct to the retained socio-technical solution. These choices represent:

- High level choices:
  - principles of physic: constitution of travellers groups, artificial strength for the mobiles movement, length of platforms and trains,
  - principles of organization: modes of recovering, periods of operation, principles of maintenance, social policy),
  - principles of integration in the site: infrastructures at surface, and\or underground,
  - principles of "calculations" modes: passenger's flows, capacities in term of interval of trains,
- And, via the function's breakdown, the more operational choices (according to the considered functional level),
  - technical principles: human action and\or automatisms, principles of train spacing control, platforms with or without screen doors, accessibility devices,
  - principles of organization: management of passenger's information, management of the drivers, presence of staff in stations, the on-line and in workshop maintenance.

In the system engineering framework, this "Top Down" approach, it means this systemic and functional description, also takes into account the environment,

and its interactions with the transport system. So, the constraints of adaptation to these environments are identified and attached to the various "main" functions.

In addition, the functional approach also includes:

- all contexts of life of the system, all needs and constraints attached to stakeholders: passengers, operator, third parties and,
- for each context, its diverse states according to failures (or hazards) which come from the system by itself or from its environment.

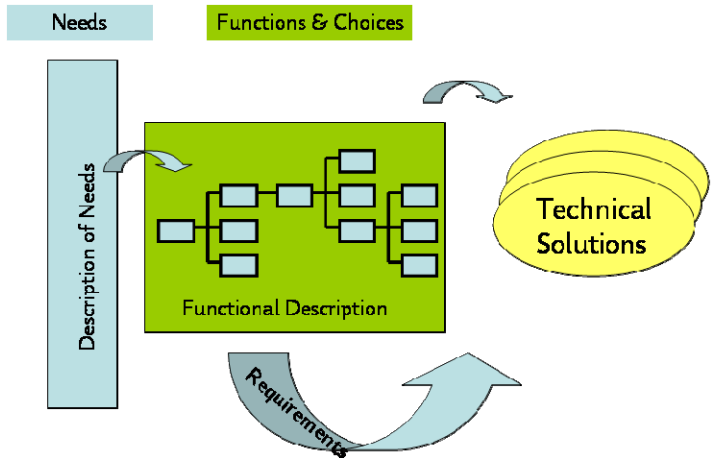

Figure 3: "Top down" approach.

The so created reference framework, at the top level brings to light the successions of functions, sub-functions, choice and requirements which could lead to several technical solutions. This is a generic model, gathering a first level of elementary information and providing a basic but fundamental knowledge of the transport system.

2.4 Generic description by mode

From that step, it is possible to create a second level of model which is related to a mode of transport, especially if there are different modes in the transport network such as metro, tramway, buses or express regional lines. The model, we are going to obtain from the generic one, results from selection of choice of principles and level of requirements. In term of choice of principle it is mentioned, as follows:

- Stop points (station): inside the city, underground or at surface, distance,
- Mobile: capacity, energy, speed,
- Operation: full or partial time, full driverless or drivers

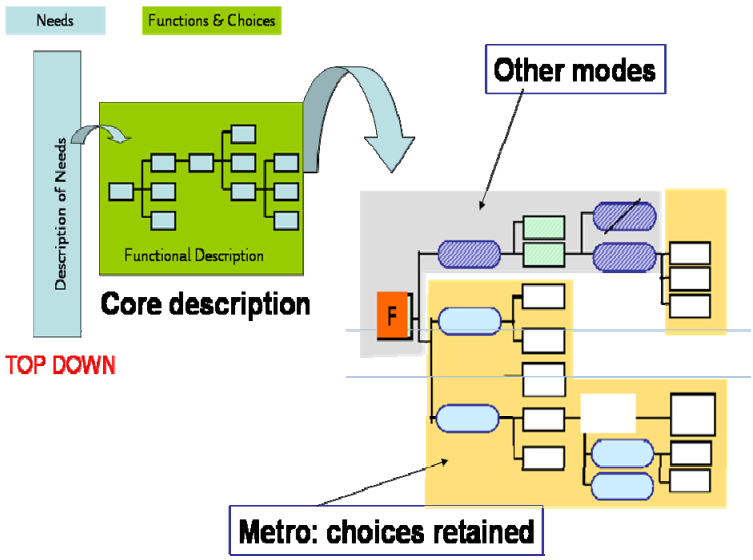

Figure 4: From core description to mode description.

2.5 From mode to existing system

The goal here is to establish an additional description, which is directly connected to the existing system and based on functions fulfilled. This is often the case when it is envisaged to describe an existing system with a functional view. The process used for that work is a kind of "Re Engineering". It starts to examine the existing system in details, by following several steps:

- Underlining the functions really fulfilled by sub system and equipments,
- Identifying the choices (of principles) really retained with justification,
- Highlighting the performances really reached to complete initial requirements.

The result is a "picture" composed of different layers connected together.

Links between layers are known and justified. It is possible to better characterize functions and choices with information coming from the existing system. This is the case of certain requirements which can be replaced by assumptions. This description provides also the principles which, for diverse but justified reasons, were pushed aside. This allows envisaging modifications of the system (optimization or evolutions) by a review of all the elements of the reference framework and to favour decisions of system adaptations.

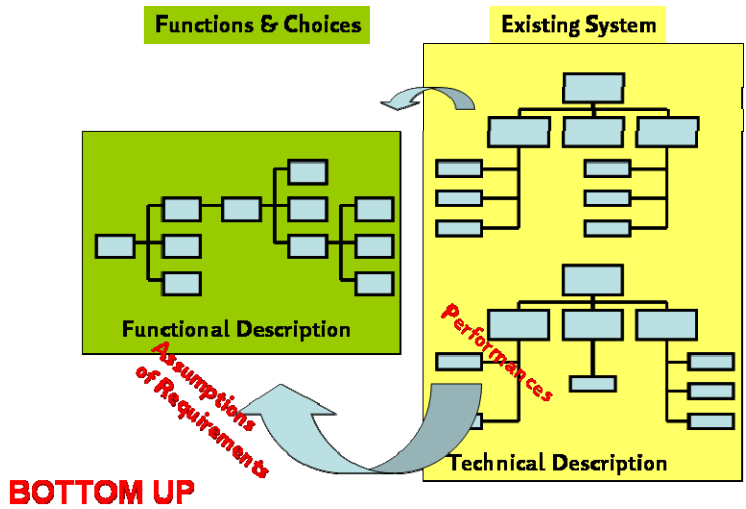

Figure 5: From mode description to existing system.

2.6 From functional description to risk control

By analysing the function failure it is also possible to draw up a first generic list of hazards attached to the transport system. At first, a hazard corresponds with a function failure. This is quite obvious taking into account that a failure of equipment provokes a change in function state and therefore function is partially or completely not fulfilled anymore.

Scenarios leading to accident can be built from this approach combining a "Bow Tie" representation and defence in depth (DEP) [2] concept appropriation. Since 2002, RATP has developed a specific appropriation of DEP concept in the Railway field in order to attach a defence system to the transport system. The defence system is characterized though the same functional approach.

The process to identify the "Undesired Context", which is considered here such as accident, takes origin within the functional description. The choices retained to build the transport system carry the source of accident. The following examples illustrate these links:

- Vehicles: collision with other vehicles, collision with infrastructures, collision with obstacles;
- Guides vehicles: derailment
- Platform: passenger fall onto the track
- Electricity (as energy to move vehicle): electrocution, fire

Both safety and security aspects are taken into account. The vulnerability of the transport system against terrorism or vandalism depends for a part on the choices which have been made during the design to consider constraints coming from the environment. This is strictly requirements attached to the constraint functions.

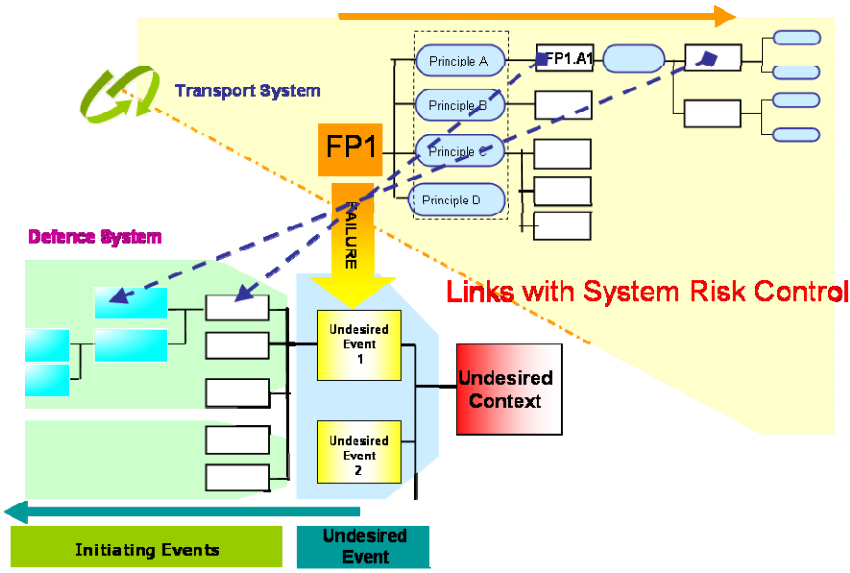

Figure 6: Links between transport system and defence system.

Therefore, based on functional description, a part of main accidents is identified and the associated failures located at functional level can be underlined. According to risk acceptability defined by the transport system operator, it is possible to adjust and allocate the safety and security requirements.

3 Benefits

Based on the systemic and functional approach, it is possible to create several views of a transport system providing materials to system engineering experts and specialists allowing them to know, to understand, to manage and to control different states, contexts of use, risks and evolutions of the considered system.

These views constitute a set of reference frameworks on which it is possible to rely because they translate the expression of needs and the level of requirements in a stable model independently of solutions. The generic model is usable for all kinds of transport systems. It constitutes the upper view. The others are developed from generic to specific following choices which orientate to specific solutions such as buses, metro or tramway.

These views also constitute a set of tools when evolutions are decided on existing system because new requirements can be placed at the right level of need expression. The development of functional model may retain choices which had been previously remote. Experts and specialists in different disciplines can analyse impacts and decide the best solution.

In corollary, such models allow to diagnose the relevance of a technical or organizational evolution, by bringing to light the possible functions not taken into account. Very often the technical experts become attached to a solution and

a given function (to improve an element of the system), without evaluating strictly:

- All functions (and the other principles) being able to be impacted by their solution, considering the strong functional interactions existing within any complex system,
- The possible consequences in all contexts and modes of system functioning,
- The potential effects on the environment.

In addition, these views constitute a bridge between design and risk management. The identification of dangers to the very first steps of system design allows involving several categories of experts including decision makers. The approach proposes to consider both transport system and defence system. The understanding of the system also implies the knowledge of the choices / decisions of risks acceptability levels, which constitute the initial requirements of security and safety and guide, through principal choices, the revealing of the elements of defence.

The knowledge of the transport system is then completed by knowledge of all functions which must be fulfilled to maintain the appropriate security and safety levels.

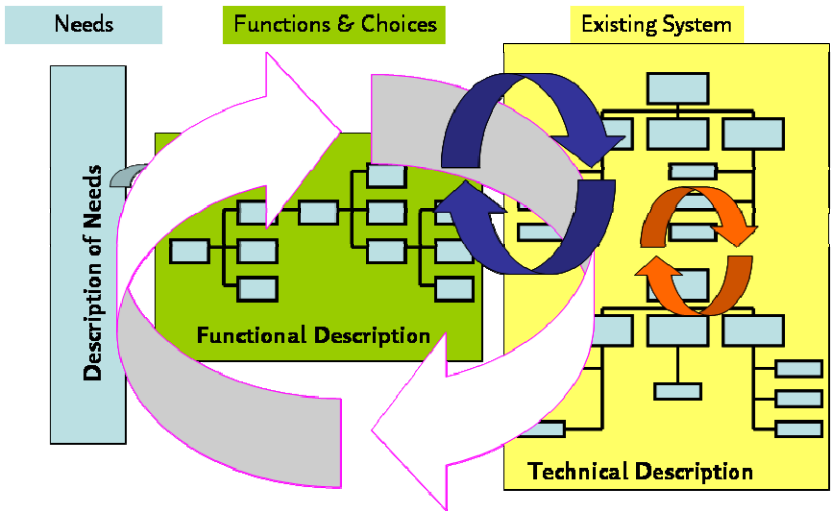

Figure 7: Several loops of evolutions.

Evolutions of the system can be treated by successive loops as follow:

- The loop is limited to the technical solution and improvement will certainly be only focused on equipment such as unique response,
- The loop includes a part of functional description (at least the function which is directly fulfilled by the equipment or group of equipment), it means that the purpose of evolution is translated into requirements,

choices of principles and the retained solution will merge from a panel of solutions,

- The loop includes a large part of functional description from the high level taking into account the system and its environment. New requirements are allocated and distributed differently leading to new solution.

4 Conclusion

A complex system, such a transport system, is evolutionary by definition. That is why, the models that we can propose have to take into account this dimension, by helping experts to differentiate invariants (attached to functions) and unstable elements (attached to choices of principle but also requirements). It is a fundamental contribution of the illustrated approaches here

Concerns of the System Engineering, and the existing standards, are often directed on aspects development and realization ("tactical" point of view). Now, half of the programs and projects failures are connected to a lack of control of the real services to be satisfied, evolutions of context, and, within the framework of an existing system modification, the lack of control of its impacts on the whole system.

Therefore it appears fundamental to widen the field of the System Engineering to consider also the processes which allow defining assumptions, declining the requirements and to master them in evolutionary contexts ("strategic" point of view).

The evolution of the requirements is not thus a defect in itself; it is their non-anticipation, their non-explanation and the absence of management of the associated risks that is one!

References

[1] Alain Cointet and Catherine Laval: System Requirements Control & Risks Control: Mind the Gap!!! (Urban Transport 2010).
[2] Alain Cointet: Defence-in-Depth & Risk Analysis (Seminar SRA - Orlando December 2005).