How to reconcile operator and manufacturer risk control points of view during the construction of a transport system

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

Abstract

In a project of building a transport system, the risk control part is a key element of the system in front of the requirements of the authorities which have to deliver the licence to operate to the appointed operator. This proof to supply relies mainly on two aspects:

- The designed, built, tested system is in compliance with the requirements specified by the client.
- The operator set up the organization, the skills and the documentation which allow it to master the system operation, to maintain it at its nominal level of functioning and to assure the expected safety level from day to day and for the duration of the contract.

These two aspects are strongly bound, even if they result from two different points of view.

- The vision "Manufacturer" on the one hand, with whom the main objective is to supply a integrated safe and secure system, in compliance with the requirements specified within the framework of the term of references with the project owner and with the rules of the art,
- The vision "Operator" on the other hand, from whom the objective is to guarantee throughout the contract of transport a safe and secure operation for the passengers and employees.

How to reconcile these two visions which integrates all the requirements of integration, use and durability from the beginning of the project in order to present to the Railways Authorities a coherent transport system?

WIT Transactions on The Built Environment, Vol 128, © 2012 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT120171

And as regards the risk control, how to connect between them the undesired events identified for every part of the transport system life cycle, for every subsystem, and demonstrate that the measures of reduction constitute a homogeneous set, a perfectly adapted and efficient "defence system" towards the desired global safety level?

Furthermore, a report can be made, in view of various projects of transport in France and abroad that manufacturer approaches towards the risks analyses are very diverse, the choices of representation highly varied and terminologies not precise even contradictory. That creates, for the operator, an increased difficulty to validate these analyses and to finally make sure of the obtaining of the proof of the safety objectives achievement.

The communication suggests developing how a global and systemic approach of risk control can:

- associate all the actors of the project,
- create synergies between the experts of risk control and,
- facilitate the decision-making for the significant cases to be examined towards the expected level of safety.

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

1 Context of PPP projects

The PPP projects (partnership public and private) for the realization of a transportation system include a significant number of actors who are going to divide up the roles in the various phases of the project. The project is often articulated around two founding axes, as follows:

- the development of a system, and
- the operation of the realized system.

Among the various partners, at least one is going to be in charge of operating the realized system and ensuring the desired level of performances in terms of service but also in terms of safety and security. This must be done for the duration of its contract. The operator is thus obliged to control the risks of the complete system, in a given environment, from elements (data, information) supplied during the development and during the realization by the other partners.

According to the initial assemblies in term of relations between partners, specific structures, diverse committees, the "sum" of collected information does not allow the operator to directly achieve the objectives of safety and security without a preliminary formalization of these data, stemming from methods and from strategies or proper visions for each of the partners. Considerable work is then necessary to appropriate these data, understand them, to integrate them into *the risks management system*.

2 The control of the risks at the end of the chain

From the "safety and security" side of the transport system, it is the "system safety assurance" which prevails with all the tools attached to this discipline.

From the manufacturer's side, every actor of the project is going to implement these varied techniques on one or several sub-systems for which he is responsible by adapting, even by reusing, existing risk analyses performed on similar equipment. The results of these works are produced under a form which can be specific for every partner.

A structure called "System Integration" is often created in this type of project. During the phase of realization, it is in charge of verifying that every supplier respects the schedule of elaboration of documents "safety and security", in order to constitute a safety file and to prove that the system fulfilled the specified safety and security requirements. It is also a part of the safety file required by the Railways Safety Authorities to deliver the license to operate. This structure disappears when the project passes in the operation and maintenance phase.

From the operator side, risks analyses must be supplied to prove that a set of measures (including organization) are going to be activated to guarantee the level of safety and security. This logic of risk control development is illustrated by the following figure.

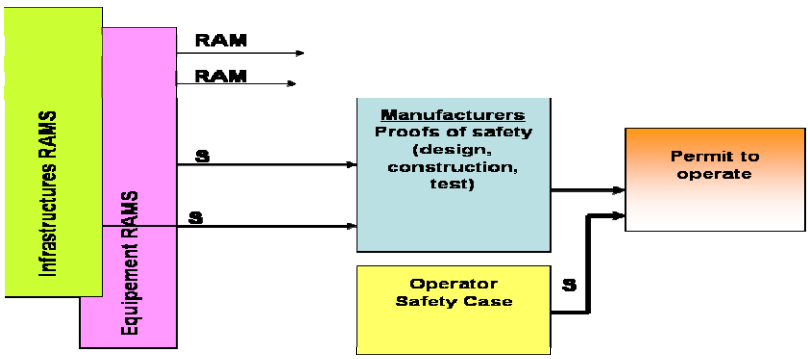

Figure 1: Logic of safety chain development.

Regarding the risk analysis, the hazard database constitutes an essential element of this safety file and an objective for the structure called "System Integration". The database includes all the risks identified by each of the suppliers, risks attached to equipment supplied and stemming from classic analyses of system safety assurance.

The compilation of these data with the risks identified by the operator gives a pile of records, the coherence of which is not guaranteed. It reflects only different points of view. Figure 2 illustrates this report.

Concerning this situation, what can we propose so that the risk control of the transportation system, results from a logic guaranteeing the maximum of coherence and comprehensiveness in the risks identification and in the measures of treatment of these risks?

What can we propose in terms of organization so that synergies appear between the various actors, in the various stages of the project, contributing to

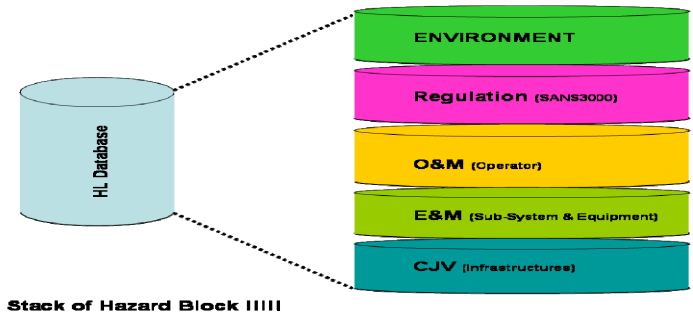

Figure 2: Pile of hazards.

supply of a solid foundation to the operator to guarantee the level of safety and security?

3 Systemic approach

"*Imagine that we try to understand the functioning of the Ariane rocket by reading the catalogue of its spare parts. And nevertheless the rocket is of a surprising simplicity with regard to a living cell!*"
Andràs Paldi (geneticist).

A global and systematic approach can allow answering the problem of coherence between the manufacturer's vision and the operator vision, by implementing a structured methodology leaning on system engineering principles such as functional analysis, the requirements of safety and security, and by appropriating innovative concepts such as defence in-depth for a common clarification of finality of defence.

This approach also brings to light the necessity of integrating the transportation system environment by taking into account:

- the functions of adaptation of the system to the environment, among which attacks coming from the outside from the system, but also,
- the respect for this environment, by avoiding or by reducing attacks resulting from choices of design or from system failures.

3.1 Project development

The approach being validated by all the actors in the beginning of project, the risks analyses performed by the manufacturers (or group of manufacturers) are then driven under a form defined before. It ensures the logical traceability between:

- the system analysis led from the beginning of the project by the operator (from a generic transport system analysis) bringing to light all the undesired events and dreaded contexts attached to the failures of the

system and its environment, and defining the levels of risks acceptability.
- the system and sub-systems risk analyses, led by the manufacturers and that must be validated by the operator.

It is also fundamental to clarify certain definitions in particular as regards:

- the security and the system safety assurance (deliberate, not deliberate),
- the undesired events,
- the final effects,
- the levels of acceptability of these final effects.

This clarification is all the more useful in the international projects where international and national standards can be used as references, without giving however the same definitions.

From the operator side, the vision cannot be focused on every component of the transportation system. It is the system in its entirety that it has to understand.

From the beginning of the project, in term of organization, the operator is a "stakeholder" in the structure in charge of federating the safety studies and verifying that the safety performances of the system will be in accordance with the requirements. A review of the safety and security requirements of the customer is a key point.

3.2 The method

The proposed methodology for this particular context of project arises from an implemented approach called "System Safety and Security Approach)" for the Paris Public Transport System. It consists at first in developing a risks analysis at the level of the transport system including its environment with an operator view, then to find the existing links between the system and sub-systems by means of the risks analyses performed by the manufacturer.

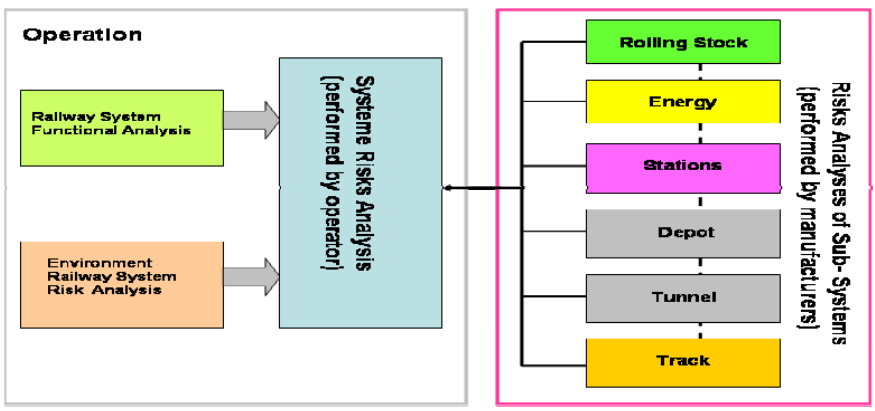

Figure 3: Links between the system and sub-systems.

3.2.1 Risk identification

The consideration of:

- the states of the system in terms of use (operation with or without passengers) brings to light risks which it is difficult to identify during an analysis with the sub-system level,
- the running modes and degraded conditions bring to light risks connected in particular to the outside elements of the system which are not treated when the sub-system is taken separately.

The proposed method to guarantee a much bigger exhaustiveness in the risks identification declines in 5 steps as illustrated hereafter:

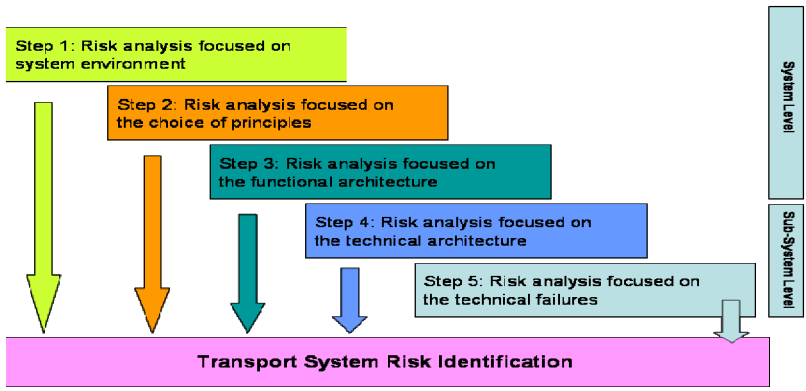

Figure 4: Main steps of approach.

This system analysis is also going to underline the existing links between the domain of the security and the domain of the system safety assurance by the identification of contexts, causes of which can be technical failures or human errors, but also acts of vandalism or diverse attacks.

Finally, the impacts on the various categories of final effects will be examined so as to prepare the evaluation of the risks and facilitate the decision for the measures to be taken in terms of reduction.

Therefore, at this step, it becomes possible for a given undesired context (UC), for example "passenger's fall onto the track", to visualize the technical and human causes which lead to the failure of the functions and sub-functions that the part of the system concerned has to fulfil.

3.2.2 Risk reduction measures

The links between the "system" risks analysis and the "sub- system" risks analyses are mainly translated on the reduction measures by references to documents (design, calculations), procedures, training programs, equipment), acting in a sequential or simultaneous way, to achieve the level of acceptability of every risk.

The application of the concept of defence-in-depth (DEP) [1], following an appropriation also developed for the Paris Public Transport System (by the authors), is going to allow us:

- to organize all the devices following finality of prevention, protection and safeguard,
- to attribute them characteristics in terms of principle of action, means of action, but also in term of functions and ways of functioning,
- to model the defence system in order to measure its robustness.

It is thus possible for a given undesired context (UC), for example "passenger's fall onto the track", to visualize the various defence elements which are expected to avoid or control the failures of the functions and sub- functions that the system has to fulfil.

3.2.3 Evaluation

When the links are established between the system analysis and the risks analyses at the sub-systems level, it is possible to assess the complete scenarios by taking into account the levels of acceptability beforehand defined on the various final effects. In that case, the undesired "contexts" leading to unacceptable final effects will first be estimated.

In addition, it is thus possible for a given undesired context (UC), for example "passenger's fall onto the track", to estimate the various probability of appearance of the undesired events (UE) and of the undesired context (UC) in order to measure "the distance" that exists between an event on which the actions stay possible and an event about which we know that it will lead to unacceptable consequences. This distance expressed by a difference between Pn(UE) and P(UC) is in a certain way an illustration of the efficiency of the line of protection but it is also a factor of decision to strengthen globally the defence system.

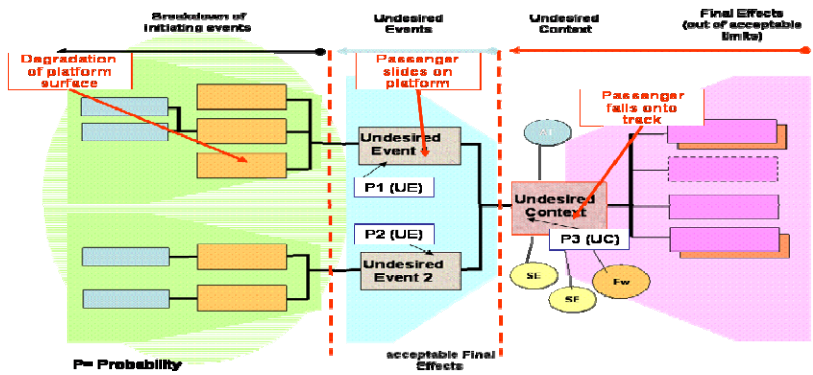

Figure 5: Causes–effects scenarios.

4 The results

The objective is to provide the Railways Safety Authorities with a coherent and complete safety file of the risks attached to the transportation system bringing to light at the same time the exhaustiveness of the risks analyses, the comprehensiveness of the reduction measures and their finalities.

The same file is used by the operator within the framework of its safety and security management system (SMS) to guarantee the preservation of the safety and security level, the correction of the new situations, the implementation of precursors follow-up [2], the monitoring and the improvement of the efficiency of the defence system.

The adoption of the proposed approach, within the framework of the creation of a new transport line, allows:

- taking into account the role of actors, according to the institutional and industrial assemblies, and to their respective responsibilities,
- avoiding the stumbling blocks of the classic approaches making parallel even opposite the operator and manufacturers points of view,
- improving the driving of the project, but also the control of the future operation of the system.

The proposed system approach has impacts on the management of the project, by the fact that it:

- ensures the stake in coherence of points of view and the used terminologies,
- ensures especially the stake in coherence of the data (needs, safety and security functions, requirements, risks, measures of reduction), and their structuralization necessary for the decisions of validation and for the constitution of proofs of the transportation system safety and security,
- allows the operator to finally build, in a progressive and rigorous way, databases for its safety and security management system.

References

[1] Alain Cointet Defence-in-Depth and Risk Analysis (SRA Orlando) Dec 2005.
[2] Gilles Foinant and Alain Cointet, Défense en Profondeur et Précurseurs de dangers, Communication ATEC, février 2006.