System requirements control and risks control: mind the gap

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

Abstract

This paper sets out to analyze, within the framework of a development or of an upgrade of a system, how the logic of requirements definition impacts on the relevance of identification and evaluation of the risks.

This is true all the more as the system is complex and questions raised by the relation between requirement and level of safety and security are numerous:

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

The paper suggests showing, on the basis of an example, how a rigorous systemic and functional approach and concepts of defence in-depth allow wider points of view, structure the requirements and facilitate the identification of the risks.

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

WIT Transactions on Ecology and the Environment, Vol 142, © 2010 WIT Press
www.witpress.com, ISSN 1743-3541 (on-line)
doi:10.2495/SW100491

1 Classic approaches

Do classic approaches allow one to answer these questions? The answer is "partially".

First of all, because the "customer" (contractual and restrictive notion), as an operator or representative of the operator of the future system, has a different vision compared to designers and manufacturers. The expression of needs and constraints of stakeholders on the customer side (or from the customer terms of reference), is going to be translated, on the basis of results of preliminary studies and a choice of concepts, by formulated specifications in the form of requirements.

The expression "capture of requirements" evokes not the reasoning on needs and constraints, but the almost documentary analysis of their textual formalizations, which does not guarantee at all their relevance and, even less, their exhaustiveness.

Requirements Engineering is then going to allow drawing, from these "reference tables" of requirements, their consideration by the gradually developed solutions, as well as their evolution. The satisfaction of the requirements will be established under the base of conformity matrices between performances reached by the solutions and specified requirements.

These approaches becoming very quickly attached to technical solutions (the project owners and contracted entities for construction having, for different reasons, some difficulties to express real needs, which suppose a prospective and objective logic), there is mostly confusion between the notions of requirements (needs and operational constraints) and the performances (reachable results by the possible solutions).

So it will be easier to specify such performance of a given radar, instead of taking the risk of expressing that on such horizon it will be essential to detect such group of persons walking in a forest close to a city where will be held international summits ….

Only the real need is source of innovation of break (in the previous example, the requirement will imply the search for data merging from miscellaneous sensors).

These classic approaches limit besides the point of view by being only interested in the environment in terms of interfaces and constraints, and therefore by losing the global vision on the system and on "systems of systems" to which it contributes: Now, only the notions such as "finality" and "global vision" can pretend to go to the sense of a justification and a validation of the exhaustiveness of the requirements. Finally, risks analyses (PDA, PRA, FMEA), are carried out by specialists, experts in their domains, during project development to secure the envisaged system: choices of conception being almost made, those analyses treat essentially risks generated by dysfunctions of the technical solutions.

What succeeds to add "firewalls", that complicates, even weakens the final system, while it should be the efficiency of the conception that allows to make from the upstream, the choices which guarantee the targeted levels of safety and security.

2 Relevance of requirements and control of risks

Why and how should relevance of requirements and the control of risks be correlated?

"If we do not change our way of thinking, we shall not be capable of resolving the problems which we create with our current modes of thought" (Albert EINSTEIN)

A systematic approach is proposed which replaces the requirements at the functional level, by anticipating, from start-up, the consideration of the services in the various modes and the states of the system. Only a structured and prospective method of study of need, then rigorous declension of this need in term of functions and constraints can supply the development frame. It is then a question of encircling the real justification of the system or its component, while leaving free the field of the possible in terms of solution: needs, functions and constraints are independent from solutions, and more stable than them, on the condition of approaching them with a systematic approach. The risk control is therefore developed on a systemic and functional background which is supported by a "Defence in Depth" approach.

2.1 The term "holistic"

Is the term "holistic" not often wrongly used?

The "theory of the systems", which refers to a scientific context, and formulates in terms of mathematics and physical appearance (physics) (Wiener, Channon)

The Systemic approach, or "science of the systems", which refers to a way of modelling a reality perceived or conceived as complex, in order to lead the thinking towards the efficiency of the decision and the action (H. Simon, J. de Rosnay, J. Mélèse, J-L Lemoigne).

The System Engineering, which refers to some form of collaborative interdisciplinary processes during a system definition, which satisfies an identified need, by trying to balance the global economy of the solution on all the aspects of the problem, and in all the phases of system life,

The System analysis, which is only one among others of the processes of the system life cycle (refer to the EIA 632), and which has for purpose to replace at the global level the study of the conflicts (contradictory requirements, alternative solutions) and to propose compromises in order to optimize quality, costs and deadlines of a program or a project.

2.2 The expression "functional analysis"

The same confusion applies for the expression **"functional analysis"** which recovers miscellaneous approaches. In System Engineering, this term concerns mostly the function breakdown in sub-functions and interfaces (within the framework of an essentially Cartesian approach), and is more similar to system operations analysis (what makes the system):

In creativity, it is sometimes associated to a brainstorming process, which can turn out perfectly unsuitable for the study of a complex system, in particular when the rigor of reasoning and the control of tools are not there …

Anyway, in systematic approach and value analysis, this term also covers:
The earlier phases of identification and structure of the finalities, the environments, the interactions with these environments, needs and constraints then their declension in functions and constraints that must be satisfied by the system (services to be returned - or " sub-system of finalization" in the sense of the systemic).

The design phases, through creative research of principles and a field of what is possible, the traceability between the purposes/functions/requirements, and their breakdowns, and through the choices of eligible or retained principles.

2.3 The defence in depth concept

Risk control must itself be replaced in this global framework and not be restricted to system safety, which referring to the capacity of a system to return without failure the services specified for an interval of given time and in fixed conditions of use, limits itself generally to the notions of reliability, maintainability, availability of the system components and to the safety and security. The concept of defence in depth proposes this global vision by integrating:

- all the potential final effects, that they are connected to the environments, to the provided services, to the property and personal integrity, to the company corporate image, etc...
- the processes of prevention and protection, as well as those of safeguard, of crisis management, of recuperation and system recovery.

The defence system identification and analysis approach which is developed by the Authors of this presentation is clearly embedded in this "Holistic process for Risk Control".

- Defence in depth is focused on the control of final effects within the limits of acceptability defined with regard to elements considered as sensitive.
- Dangers and therefore the risks of exposure to such dangers are inherent to the system and its environment. The levels of acceptability for final effects are duly part of decisions made at a "political" level.
- The notion of depth takes its entire meaning in the structured and hierarchic implementation of defence actions to avoid or limit the consequences and prevent the combined creation of other effects on one or more sensitive elements.

The defence functions result from system functional analyses, and are expressed according to systems and implied entities: attackers, potentially aggressive flows, sensitive elements, whether they belong truly or partially to the system or are fully external.

The rigor of system functional analysis does guarantee to get an exhaustive list of undesired contexts and thereby structures the initiating events that classical risk analyses do not allow.

The defence system architecture is supported by a systems engineering process and includes three levels:

- A first level of structure by lines of defence, comparable to the definition of functional architecture at a subsystem level,
- The second level of structure by principles of action, comparable to the definition of logical architecture of the defence system,
- The third level of structure by means of action, comparable to the definition of technical architecture of the defence system.

The features of the system can be so specified then declined at the level of the defence elements: autonomy, activation, sequence of events, success or failure, elementary functions, for highlighting indicators of efficiency and precursors.

3 Development and illustration

A typical function of a rail transportation system as the public address system (message for the passengers aboard trains) will serve here as a base to illustrate these approaches and bring answers to the questions raised in the introduction.

On board PAS generally includes miscellaneous components such as public address units, amplifiers, loud speakers, which are all scattered along the various cars. The on board PA system is activated by the train driver when setting up his driving cab ready for departure. The second public address unit located in the other cab is then disconnected.

The communication link is one way, from “train driver to passengers”. The functioning check is done at the time of preventive maintenance. Checks are equally carried out online to assess the “quality” of the announcement and feed an indicator monitoring process. When a failure occurs during a journey, the train can be changed at the end of his journey according to the availability of spare train.

3.1 A first approach for a functional and risks analysis

The technical system has for object the one-way communication between the driver and the passengers. The main function may be defined as follows:

- FP1: To allow the driver to deliver messages (sound) of service to the passengers inside the train.
- This function must be fulfilled while respecting the other functions of the train (FC1) while ensuring protection against external aggressions (FC2).

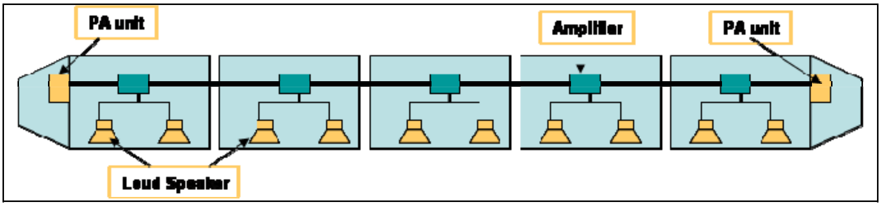

Figure 1: Generic configuration of PAS.

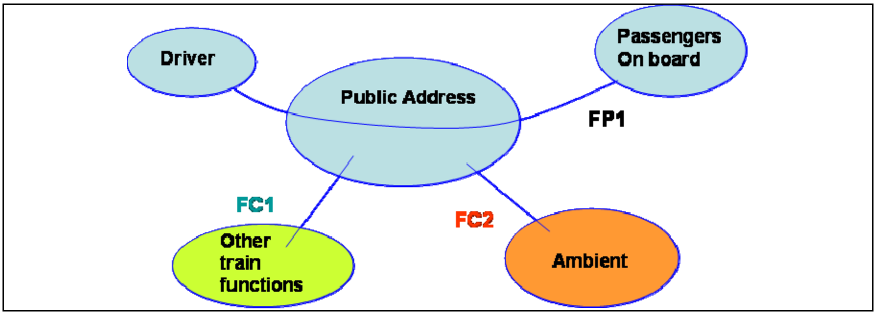

Figure 2: First representation of the on board public address function.

The requirements attached to the function are going to integrate criteria such as:

- 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).

Note that evolutions have taken place on recent rolling equipment, especially the possibility to activate pre-recorded messages, either by the driver or via train-track communication. The driverless stocks can receive messages from the traffic control centre.

The dangers assessments **(FMECA type)** are based on identified components failure scenarios.

- the message is delivered by the driver but is not heard by the passengers (impact on the quality of service),
- the message is delivered by the driver but is not understood, or not partially understood, by the passengers (impact on the quality of service, impact on the image of the company, the impact in term of passengers' possible falls).

3.2 Second functional (more system oriented) approach

To adopt a systemic approach supposes a change of logic of thinking: we hereby shall develop some aspects in order to illustrate the analyses which it engenders.

3.2.1 First axiom in systems analysis: understand the ultimate goals

Applied to our example, the question becomes: in what purposes do we want "to allow the driver to deliver messages to the train passengers" (FP1)?

C1 – NOMINAL OPERATION WITH PASSENGERS

Besides the nominal mode of the system, the analysis also has to take into account needs:

- In the failure modes for each of the previously listed functions, and
- Also in environment degraded conditions while the concerned system is in nominal or failure mode.

Table 1.

Function		Principles	Requirement
F1	To provide passengers with information for their travels	By informing on the name of the next station, on the availability of lines in correspondence or the other means of transportation in interface, commercial information, or other	belongs to the quality of service and travel comfort
F2:	To prevent or resolve a passenger related undesired event during platform train transfer	Either by sending a message before train stops on the existence of "gaps" ("Mind the gap" practiced in the UK), or the opening side of doors, Or by suggesting interventions of other passengers.	belongs to the safety of passenger movement
F3	To protect passengers against aggressions during their travels	By addressing messages related to the presence on board of risky passengers (such as pickpockets for example)	belongs to the security of passenger movement.
F4	To protect passengers from invasion of non revenue operations areas	By addressing messages on the arrival at terminals	belongs to the safety of passenger movement and also to the infrastructures protection against potential passengers intrusions

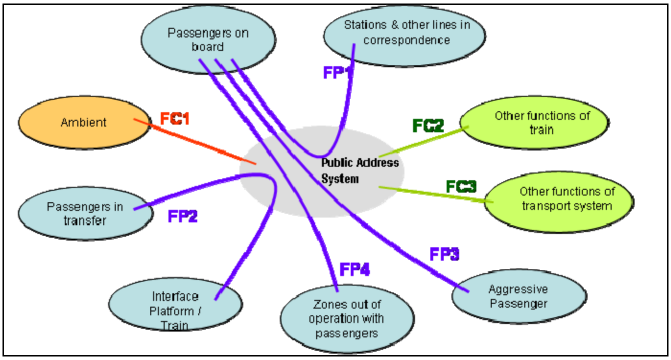
Passengers on board
Stations & other lines in correspondence
FP1
Ambient
FC1
FC2
Other functions of train
Public Address System
FC3
Other functions of transport system
Passengers in transfer
FP2
FP3
FP4
Interface Platform / Train
Zones out of operation with passengers
Aggressive Passenger

Figure 3: Representation of functions for the on board PAS in a nominal operating context with passengers on board (APTE® method).

CD2 – DEGRADED MODES OF OPERATION

FD1: In case of train evacuation in a station or in a tunnel, passengers must be informed and be given as precise as possible mandatory instructions.

FD2: In case of not availability of the local devices of treatment of the platform - train accessibility, inform the passengers of the non-opening of the train doors.

Clearly this category lies in the field of "safety passenger's movement"

This functional analysis, which is more rigorous than the previous one makes obvious that:

- The requirements attached to the on board Public Address System cannot be the same, depending on the functions to which it contributes (it is effectively very different to inform on the following station in normal operation or the station of correspondence and to deliver instructions in order to evacuate a train).
- In risk analysis, unavailability or the misunderstanding of a message delivered by the driver can have unacceptable impacts following the cases.

In these cases, PA functions, can take then the status of "Safety function". It will then become necessary to specify:

- The undesired contexts and the potential final effects (among which subsequent consequential effects),
- The acceptability levels for the final effects, and thereby the safety levels to be targeted.

Decisions made about those levels do determine the safety requirements.

3.2.2 Second axiom in systems analysis – understand the interactions with the environment

Applied to our example one might wish to ask the question: *Into which environments (functional, organisational and technical) does the onboard Public Address system integrate?*

Such subsystem previously considered and handled separately, also needs to be considered as part of a larger group of audiovisual media including functions related to:

- Passenger routes within the infrastructures,
- Passenger transfer between platforms and trains,
- Trains movements.

The need to communicate information to the passengers is not limited to the movement aboard the train. All the stages of the passenger progression inside the transport system are concerned, since its access to the system until its final destination. This global need of information to be supplied to the passengers is going to be analyzed according to a systemic approach and is going to lead to consider a system including audio and visual means which needs to serve both simultaneously needs for passengers and the operator's constraints, while taking into account the various ways of functioning (nominal mode, failure modes, degraded conditions of environment).

The functions become transverse and integrate all the interfaces. At the train level, the need of passenger's information will also include the following functions:

- To allow the passengers to communicate with the operator,
- To allow the passengers to communicate with the outside of the transport system,·
- To allow the station staff and line staff to communicate between themselves.

Communication becomes bidirectional and such functionalities are also required for platform operation. The onboard PA system will have to interface adequately with the other functionalities. This approach noticeably evidences:

- Interactions between the train PA and the platform PA, in particular during critical situations (train evacuation, station evacuation, passenger transfer problem, presence of aggressive passenger either within train or within platform),

What coherence between messages delivered aboard the train and on the platform do we have to guarantee and for which situation?

What priorities do we have to set up between types of messages, between the various sources?

- Interactions between the PA system and other audiovisual means, such as the interphone and the video in the train, etc.

The requirements will also have to take into account that the specified system must integrate into already existing equipments which is often the case due to programmed adjustments, and therefore specify interfaces with existing equipment in the various contexts of operations. According to the levels of safety and security defined by the operator, the functional analysis of the failure modes can lead to specify a "fallback" additional system with its own requirements in terms of services to be offered and of implementation.

The issue of resilience is effectively raised in similar terms.

In order to ensure the vital system functions continuity in crisis mode, in order to be able to restore the system stability when exiting the crisis, while limiting the final effects, imposes a culture and an anticipation of risks as soon as the first expression of finalities and needs within a combined system-environment approach.

So, a breakdown of PA system may oblige the operator to order unloading of the passengers at the next station and to replace the failed train by a spare train. That supposes that the operator has spare train. This solution may not seem very efficient, considering on one side improvements made on equipment availability and on the other side the economical constraints which incite the Operator to decrease strongly the spare rate of trains.

To improve the resilience potential it is mandatory to therefore consider other paths of solutions in regard to functions to fulfil, but also, to the final effect acceptability and risk of combination of effects: for example, the use of other information systems, the switching to the second PA unit located on the rear end of the train, other specific mode to be activated in those cases, etc, and at the origin, to be able to detect onboard PA failures.

4 How do these approaches bring elements of answers to the questions raised in the introduction?

We shall mention here the key points for those approaches compared to the questions put in introduction of the present communication:

Table 2.

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 he 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 using a rigorous method to formulate the needs, By helping the client to adopt a more prospective approach and considering the system or equipment studied as a black box interacting with various environments.
3	How to distinguish the safety functions?	First of all by clarifying the meaning of the term "safety function" By making sure that the "customer" expressed well the levels of acceptability of the final effects, and that he defined the priorities: • The expected level of safety for a function of a system or for one of its inner subsystems is directly linked to the level of risks acceptability and potential final effects, what comes from decision made by the project owner. • For the same function, the safety level will vary depending on the system context adopted as a standpoint: So, the communication between the driver and passengers may, depending on the various system states, recover from the simple quality of service or from the safety and security of the passengers.
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 standalone (each context is 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).

Table 2: Continued.

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 identified early in an independent way from the solutions because they are linked to: *interactions between the system (or subsystem) and its environments (system environment depending on operating contexts, or other subsystems in interaction), degraded situations within those environments at stake, and/or failure modes of functions expected in nominal situations for the element at stake.* • 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 wholesome method (such as Defence in Depth) with the intent to identify risk reduction dispositions, the related requirements and the ultimate goals. The analysis will thereby focus on the defence system and its characterization (typology of the elements of defence).

5 Conclusion

Why do these approaches meet difficulties in merging into the present organisations?

The single fact that rigorous processes are available for actors and keep improving just has a very evident interest only if they are actually applied to practical example. Today, the status of integration and the effective level of control of those approaches within the bodies remain very incomplete.

Why is it so? This question raises, for a conclusion, the thought on the roles, interests and responsibilities of the various actors: who should rather use these approaches? who can or has to use them? in what contexts, for which objectives? A first answer, which demonstrated its efficiency on a certain number of projects, is to use these approaches to understand, reformulate and so validate Terms of Reference (ToR) of a project owner, specifications or risks analyses. We then apply another logic of reasoning, other than that of specification writers and designers, which is going to allow one to bring to light the lacks, the errors or ambiguities of requirements and apprehension of the risks.

However, would not it be advisable to initiate that process earlier during the ToR specifications and risks analysis establishment? Should not we introduce into the programs additional files such as Justification of Needs, Justification of Risks, as well as Justification of Requirements, Justification of Definition?

However, bringing some rigor of reasoning, that implies sometimes deep doubting for envisaged solutions, and working practices.

By evidencing choices to be made, and thereby decisions to make and justify, such processes inevitably raise the question: “Who can decide what” and its subsequent question: “who wants to take the risk to decide what?”

References

[1] Jean-Louis Lemoigne, La théorie du Système Général, Version 2006 (www.mcxapc.org)
[2] Methodology of Defence Elements Identification within a Transport System (Alain Cointet - LAMBDAMU 14 Bourges) – Oct 2004,
[3] Defence-in-Depth & Human Factors (Jean Marion & Alain Cointet - ESREDA Ispra) Oct 2005,
[4] Risk Management Policy based on the Defence-in-Depth Concept (Jacques Valancogne & Alain Cointet - HKRMS Hong Kong) Dec 2005,
[5] Defence-in-Depth & Risk Analysis (Alain Cointet - SRA Orlando) Dec 2005,
[6] Risk Control, Defence in Depth, Indicators & Precursors (Alain Cointet & Gilles Foinant – ATEC Paris) Feb 2006,
[7] Catherine Laval & Alain Cointet, Defence in depth &System Engineering: A synergy for the benefit of a global approach of the risks and the responsibilities, - Congres λμ 15, October 2006.