Defence in depth: transport system and defence system

A. Cointet
RATP, System Risk Control, Fontenay Sous Bois, France

Abstract

In a competitive context and strongly regulated, the stakes for a mass transport company are strong: to perpetuate the confidence of its clients, or Transport Authorities, to establish a national and international public image, to guarantee technical and economic performances.

The increasing complexity of the transport systems and the reports carried out from incidents justify that a company such as RATP acquires and develops methods and tools to improve the control of the risks related to its activity, and to ensure a better knowledge of its system, by taking into account evolutions of this system since its creation.

Showing a high level of safety, which is recognized by all the actors of the transport field, RATP wants to maintain this safety level, even to improve it. But, it keeps facing problems related to the complexity of transport system, requirements and constraints.

Safety barriers have been progressively installed within the system, procedures have been written and applied, inspections and audits have been carried out. In addition, experts gathered within a system safety network examine incidents, taken into account human factors (ergonomic, formalized experience feedback). Despite these measures, serious breakdowns still appear but less often and their consequences are better controlled.

Keywords: defense, typology, flow, sensitive element, aggressive element, lines.

1 Introduction

To take into account these various factors which could question safety, RATP has established its Risk Management Policy based on principles, which are destined to help the leading of Railway System Safety Studies.

WIT Transactions on The Built Environment, Vol 101, © 2008 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT080091

- No regression of safety level: New system are design to reach at least the same safety level as existing system;
- Evolutions of system are mandatory: Balance between efficiency expected and cost.

This policy is declined in several objectives. One comes from the "Defence in-Depth" concept and aims:

- to identify elements of defence within the existing system;
- to measure their efficiency and then to propose evolutions;
- to constitute a reference framework of defence.

2 Transport system and defence system

2.1 Context

As mentioned before, a transport system is a complex system, subjected to a lot of constraints. Among them one can list:

- Passenger requirements;
- Transport authorities requirements;
- Rules and regulation;
- Inevitable evolutions;
- Cohabitation of various technologies;
- Environment constraints.

Consequences on the system are also numerous in terms of:

- Staff and knowledge;
- Equipment;
- Documentation;
- Organization.

The set of constraints and consequences generate more risks and it becomes highly difficult to guarantee the appropriate safety level of the transport system. With regard to the wide aspects of this problem, it is necessary to develop:

- A systemic approach to guarantee the global coherence between the system components and environment;
- A model of the system of defence.

A transport system fulfils at least one function: "To transport passenger from one point to another" with criteria such as comfort, journey duration, safety, etc…
Designing and building a transport system from this function impose to make choices and to decide what functional and technical organization the transport system will have. Those choices may create danger. For example:

- To decide using electrical motor cars creates electrical power dangers.
- To decide that trains will run on the same track with a minimum of headway creates danger of collision.

To face identified dangers, the risk engineers provide safety devices to prevent and/or to reduce consequences. The presence of these safety devices explains the existence of a set of defence functions which constitute a system of defence. It is

possible to illustrate the transport system and its defence system based on a functional approach as follow.

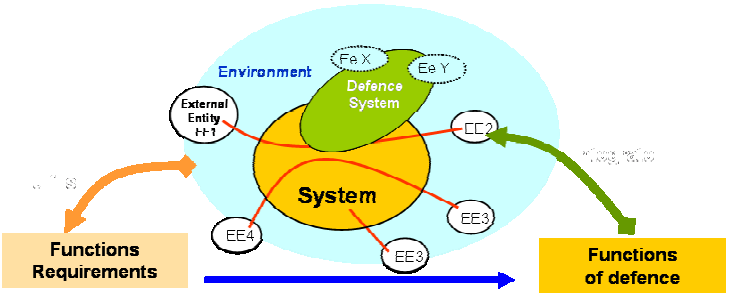

Figure 1: Functional approach.

Note: This kind of approach aims to highlight the importance of requirements attached to functions. It will be extremely difficult to measure the efficiency of a defence system without the expression of safety or security requirements

2.2 Basic history and concept of "Defence in Depth"

Defence in Depth is an old concept (2900 years / bc) mainly used by different army in the past. It was at that time, only question of protecting of civil and military sites, with several dispositions which were placed around the site.

From years 1960s, the concept has been used and applied in the nuclear field to define protection against radiations.

The notion of "lines of defence" is directly associated with the concept of "Defence in Depth". Each industrial field which applies this concept, stresses certain properties of defence:

- In the nuclear and industrial fields, one insists on the independence of the lines (or means of defence);
- In the military field, one sticks to the notion of global defence: "comprehensive" lines in the sense of capacity to deal with all the threats and "co-operating" lines the force of defence of the system is higher than the sum of the forces brought by each line;
- In the field of the data processing systems, one especially puts forward the unit treatment of each threat, regarding their diversity and difficulty of their expectation.

2.3 Goals and definitions of a "Defence in Depth" system

The defence of a transport system has the aim of insuring all the time, in all circumstances and against all forms of aggression, the necessary safety and the integrity of men, system, company and its environment.

"Defence in-Depth" is a global and dynamic defence, implementing several coordinated lines of defence, against internal and external aggressions, potential or proven - and that on all the cycle of life of the transport system.

A "Defence in-Depth System" (DDS), is the set of the provisions and means organized, implemented to satisfy, at the required levels, the finality of defence defined for a given transport system.

3 Modelling process of a defence system

Approach presented here, is based on a hierarchical modelling of a defence system, with an engineering system approach integrating the functional analysis. Engineering system brings its rigour of representation; functional analysis its resolutely systemic step and its relevance to build any modelling on perennial referents, which are finalities and functions of system. Four steps structure the modelling.

3.1 A precondition, the expression of the finalities of defence

According to the definition of Defence in Depth System and in a given context, finalities of defence are expressed in regard with:

Three types "of involved actors":

- Potential attackers;
- Aggressive flow emitted by these attackers;
- Sensitive elements which could suffer damage from these aggressions.

Direct or combined final effects, that one wishes to control, according to the types of elements and their sensitivity.

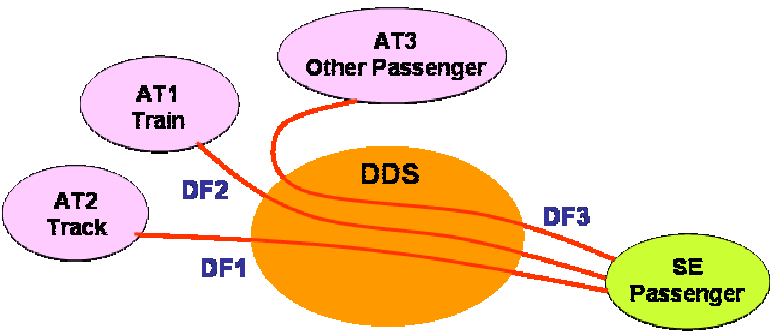

Figure 2: Defence functions.

The definition of DDS forces to quantify the acceptability levels associated for each final effect (on the system, its users, the implied organizations and the environment):

- What are the acceptable effects?
- What are the unacceptable effects? But also,
- What are the tolerated effects?

These levels of acceptability are independent regarding dreaded situations and events being able to lead to the considered final effect; They strictly depend on

the system of values retained and clearly concern the company level political choices and expressed within the Risk Control Policy.

The proposed approach is then coherent with logics of decision of the decision makers:

- Final effects treat consequences in the domain attached with their field of responsibility: awaited services of the system of transport, safety of the people, environmental protection, financial permanence of the company, image of the company.
- Notion of acceptability integrates a multi-criterion reasoning, characteristic of any decision-making process.

EXAMPLE: for a final effect on the person, will be considered the physical integrity, but also their own acceptance of the undergone risk, on an individual or collective level, and in the case of combined effects, the impact on the company image...

The chosen "target" of defence at the political level provides then the requirement reference framework to be satisfied for any design, management or improvement of the system. The three following levels are based on a system engineering approach:

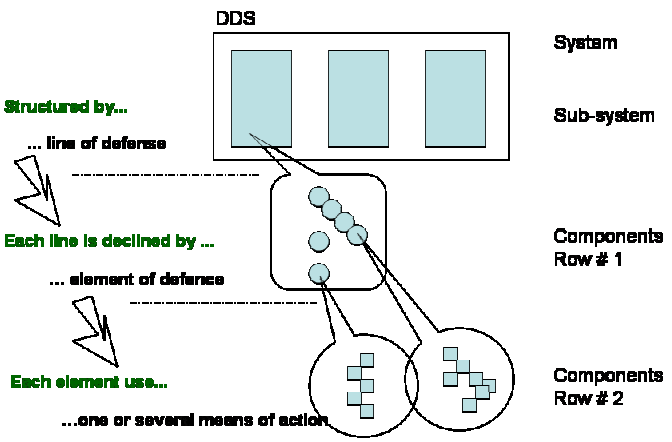

Figure 3: Structure proposed.

3.2 A structuring by lines of defence, in response to the finalities of defence

The "Defence in Depth" implements successive and autonomous parades, with respect to internal or external aggressions, potential or proven and that, on all the life cycle of the system.

The suggested structuring declines each finality of defence by specifying it under three complementary principles, which correspond to choices of action strategies to meet requirements previously characterized:

- A principle of prevention, consisting in acting on the probability of appearance of a dreaded event.

- A principle of protection, having to maintain the final effects within acceptable limits defined within the defence policy.
- A principle of safeguard, intended to limit the extent of the consequences whenever the accident cannot be avoided, and therefore to act at the same time on the gravity of the final effect and the not-combination with other final effects.

These three principles induce architecture of the defence system in 3 "lines of defence". The modelling, which results from this breakdown, is comparable to a functional architecture of the defence system in system engineering approach.

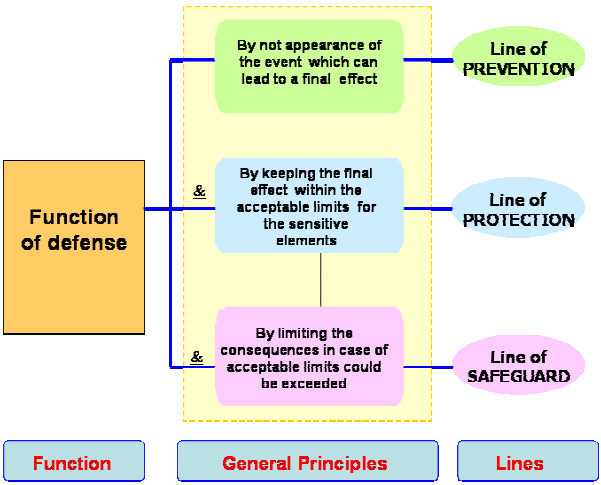

Figure 4: Choice of principle.

The concept of "depth" makes here more sense in "posting" the commitment to continue actions of defence beyond the traditional principles of prevention and protection, by integrating safeguard actions after accident, with internal means, total or partial transfer to external means.

3.3 An identification of defence elements constituting each line of defence

Elements composing each line of defence are defined via determination of "principles of action" choices in regard with the aggression, and interactions between defence elements of the same line and between lines.

This level of analysis, comparable to the definition of a logical architecture of the defence system in system engineering approach, imposes to justify each element regarding the relevance of the retained mode of action to satisfy the function of prevention, protection or safeguard:

- Action on the attacker;
- Action on the sensitive element or;
- Action on aggressive flow.

Note: It is also possible to combine several actions

The determination of this mode of action then makes it possible to define (or validate) the expected performances of the element, within the framework of its contribution to the considered line of defence.

A generic breakdown of principles of action allows locating the mode of action considered: An extract of this structure is provided hereafter.

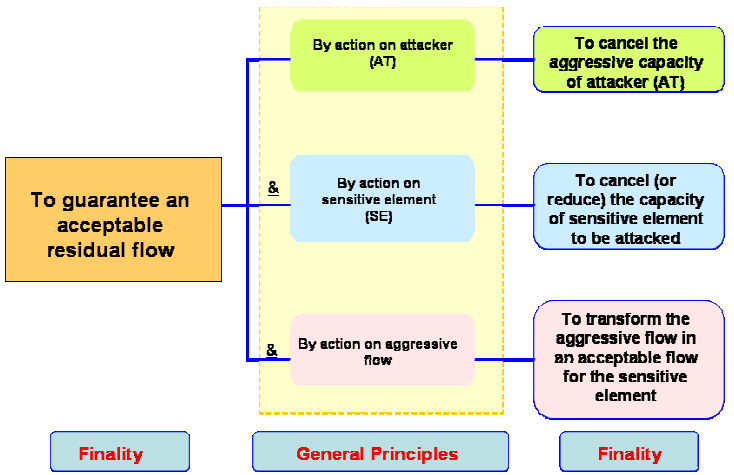

Figure 5: Choice of actions.

3.4 A Definition of each Defence Element

Each defence element is defined concretely through:

- Implemented means of action:
  - internal or external means with the system, even mixed;
  - equipment or automatisms, or man (group of men), or combination of these means;
- Activation and control mode of these means;
- Awaited functions of the defence element and associated requirements.

These definitions make it possible to model the technical architecture of the defence system. If necessary, these analyses can continue on finer levels: elementary functions of the means of action, technologies implemented...

Thus, the analyst can:

- Establish (or find) the traceability between the considered defence elements and the finalities of defence to which these elements contribute;
- Validate the relevance of the implemented means compared to the expected performances of the element.

A typology of each element can be shown as follow:

A part of the description results from the proposed structure. The second part of description which gives additional topics takes into account elementary functions that element could fulfil (detection, report,…), type of association of elements and status.

The set of properties constitutes a kind of "Identity Card" for an element or a group of elements and will be useful in case of measurement of defence efficiency.

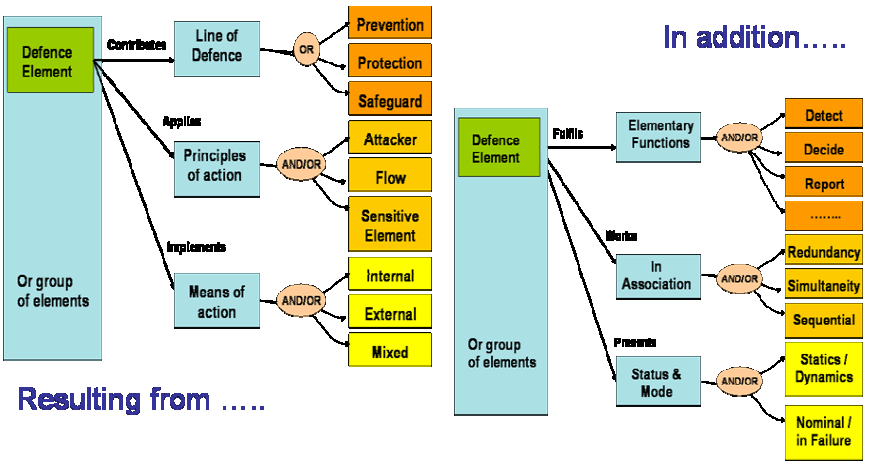

Figure 6: Typology of defence element.

3.5 Modelling of defence system

In addition to the detailed analyses of the lines and elements of defence, it is proposed the modelling of the system of defence for each defence function or a group of functions according to the perimeter of system analysed:

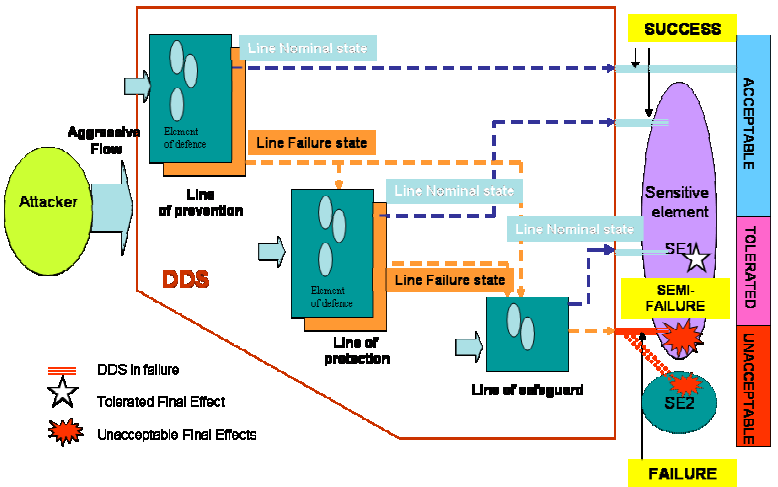

Figure 7: Generic model.

The model illustrates the different lines of defence, which are autonomous but contribute to the global defence. Links between lines, especially in case of failure, underline the necessity to take into account the global defence, while designing the transport system and its defence system.

4 System engineering and risk control

Systems are developed by a set of actors, in response to specified needs and constraints, part of them are translated into system safety requirements. This development calls upon various processes more structuring, which are related on system engineering and the risk control.

The process of system engineering, implemented by various experts and decision makers, is declined, in phase of definition of the system and its components, according to four main activities:

- Expression and understanding of the need;
- Choice of principles and functional breakdown;
- Choice of functional architecture;
- Choice of technical architecture.

Each activity constitutes a milestone for the definition and variation of the requirements.

In order to guarantee the correct operation of the system, a second process, the risk control, is implemented by other experts and decision makers. This process also covers the phases of system development; It is then very largely used during system operation to supervise its behaviour and to take into account its evolutions. This process calls upon cycles of activities including the following steps:

- Knowledge of the system and Identification of the dangers
- Quantitative or qualitative evaluations of the risks;
- Definition of risk reduction measures;
- Monitoring of the effectiveness of these measures.

Organizations generally implemented for these two processes are parallel and slightly inter-connected. Decision makers, experts but also methods and tools are specific to each one.

Taking into account points developed here, some questions can be raised.

- How to develop a synergy between these processes and for which finality?
- How to make communicate the experts and the decision makers according to their level of responsibility in the organization for the project?
- How to break the limits of the traditional tools for better apprehending of complex systems?

From our point of view, the concept of “Defence in-Depth” is an answer to these many questions and its appropriation structures the global step, supports the relation between processes and between actors, clarifies the role of the actors, contributes to a common vision of the objectives and provides representations allowing comprehension, control and improvement of the complex system concerned.

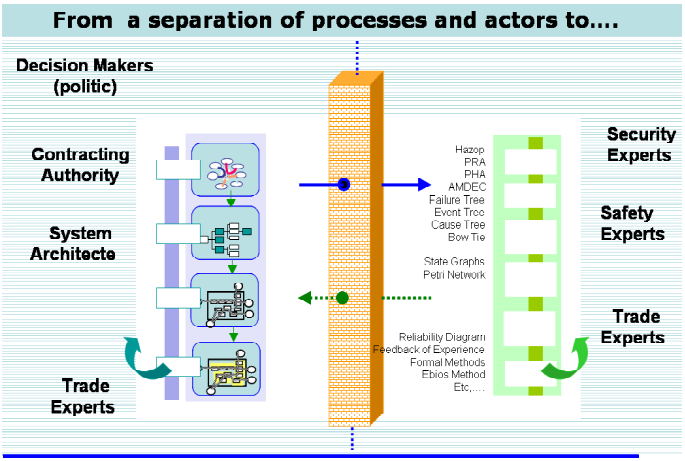

Figure 8: Separation between processes and actors.

5 Conclusion: Interest for RATP to appropriate the concept of "defence in depth"

5.1 Use of the model of DDS

The suggested logics to define the concept of "Defence in-Depth", as well as the principles of architecture of a DDS, provides a tool of reasoning to model an existing system of defence or to conceive it

The will of RATP, as regards the control of the risks, is translated firstly on the CONTROL OF WHAT EXISTS, to which the formalization of a reference frame of "Defence in-Depth" within the existing transport system contributes.

According to this framework, the logic of modelling of a "Defence in-Depth system" can be exploited for:

- To specify a system of defence (or coherent component of this system);
- To identify and characterize the elements of in-depth defence implemented for the existing system;
- To diagnose this system of defence existing compared to the requirements defined within the schedule of conditions;
- To establish, on these bases of the recommendations to improve the existing system of defence;

Approach, suggested here, of modelling of a "Defence in-Depth System" can be applied, in a fractal manner, at various levels, each one analyzes a complete system or a component of this system:

- DDS of a transport system or a subway line can be modelled by three lines of defence;
- DDS related to an operation of a train in maintenance workshop, or that related to the adherence of the trains on the rail (problem of pollution of the rail) can also be modelled by this principle of architecture.

5.2 Interest of concept appropriation

Taking into account the complexity of a transport system, its total coherence with regards to safety is very important.

The transport system (and its Defence in-Depth system) cannot be any more, only seen like an assembly of components: their understanding and their control impose a global solution.

Since a certain number of years, RATP has adopted a systemic approach to control the risks inherent in the system, not only technological but also human, organizational, economic and environmental. This approach also takes into account:

- The complete system in its environment, with all its interactions like their evolutions;
- The whole life cycle of the total system and its components.

The concept of "Defence in-Depth" is in perfect coherence with the systemic approach thus adopted by RATP: Its definition provides a logic of modelling making it possible to identify or design elements with very diverse nature contributing to the finalities of defence, to understand their interactions - that, in order to control the relevance and the effectiveness of it. This logic of modelling is based on steps of Engineering systems: functional architecture, logical and technical of the DDS, through the concepts of, lines of defence, element of defence and means of action.

An approach "Defence in-Depth" does not oppose to the traditional steps of: risk analysis, the system safety and experience feedback. At the same time, it supplements them, and it is nourished from them.

The purpose of "defence in-depth", is mainly the control of the final effects in regards to the elements declared sensitive. Its logic is centred on the control of the elements contributing to the maintenance of the final effects within the limits of acceptability fixed in a given system of values.

It is a question of supplementing the management of risks via the dreaded events and their causes (generally with a probabilistic approach), by a point of view of control of the effects and sensitive elements (more deterministic and systemic approach, by level of acceptability).

5.3 Interest for experts

Like any modelling, this proposed for a "defence in-depth system" makes it possible for the actors to have a common representation of the system. This modelling is finalized on the structured identification of the DDS:

- In order to constitute a reference frame on the DDS.
- In order to analyse the relevance of the means implemented compared to the awaited services of this system.

According to objectives of analysis, it can:

- Include one or more levels of representation (line, elements of defence, means of actions).

- Continue to take into account the steps of engineering systems from which it integrates, on finer levels: elementary functions of the means of action, technologies implemented.

The structuring suggested allows:

- To lay out (or find), permanently, of the traceability between the system requirements and the solution.
- To identify the interfaces between lines, elements of defence or means of defence.
- To distinguish the internal and external means from the transport system, operated by the DDS.
- To facilitate the analyses of impact in the case of evolutions of attacker, flow, sensitive elements or of their environment, principles and means implemented, contextual elements susceptible to lead to an event or a dreaded context.

It also makes it possible to distinguish the concepts of indicators and precursors: the first falling under an objective of follow-up of effectiveness of the implemented elements of defence, the second being centred on the appearance of contextual element being able to lead to an event or a dreaded context (susceptible to create unacceptable final effects on sensitive elements).

5.4 Interest for managers

Proposed modelling makes it possible to provide to the decision makers a synthetic representation of the system of defence.

This logic of structuring the defence elements by lines, principles and means of action is easily comprehensible by a non-specialist of the risks analysis.

Centred on the control of the final effects and the concept of acceptability, it is coherent with logics of decision of the decision makers:

- Final effects treat consequences in the fields concerned with their field of responsibility: awaited services of the transport systems, safety of the people, environmental protection, financial resources of the company, image of the company.
- Concept of acceptability facilitates a multi-criteria, reasoning specific to any decision-making process.

For this reason, the concept of "defence" is broader than the concept of safety:

- Determination of the final effects and the levels of necessary acceptability falls under a system of given values, and is integral part of the definition of the control of the risks policy.
- Distinction of the lines of prevention, protection and safeguard makes it possible to show the engagement of RATP, with regard to the safety of the transport system, and the company: to avoid any final effect, and even if certain situations occur for reasons being able to be external for him, to contribute to limit its consequences.

The concept of "Defence in-Depth" is very rich, but, in its current definition, it is insufficient to guide a control of the risks approach. The definition of a structured methodology only allows at the same time:

- To position it such as a base for control of the risks policy at the level of a system and a company.
- To transform it into real tool for all the chain of decision makers and actors intervening in the definition, the design, the implementation or the evolution of a defence system.

The appropriation of such a methodology passes by preconditions:

- Acceptance by the experts, of an evolution of the methods of safety analyses, new concepts and new terminology.
- Acceptance by the decision makers, of the responsibilities which fall to them and which are thus posted (determination of the acceptability levels of the final effects), and, in parallel, their comprehension of the advantage of new management tool which are proposed to them (modelling of the defence system, follow-up of indicators and precursors).

From these points of view, the formalization of a reference frame, of the defence system (or "database" of functions, lines and elements of defence), within the transport system, will constitute a real support:

- To refine the identification and the preliminary analysis of the risks.
- To facilitate the analyses of impact in the case of evolutions:
  - evolution of the objectives of defence;
  - evolution of the aggressions;
  - evolution of the sensitivity of the elements concerned;
  - evolution of average the techniques, procedural or organisational;
  - evolution of the environments.
- To ensure a common vision of the system of defence between the actors, the experts and the decision makers.

References

[1] SFEN, Introduction to nuclear safety, www.sfen.org/fr/intro/surete.htm,
[2] Analyse des risques et prévention des accidents majeurs (INERIS - DRA-07) June 2001.
[3] Et si les risques m'étaient comptés (Guy PLANCHETTE, Jacques VALANCOGNE, Jean Louis NICOLET – Editions Octarès) 2002.
[4] Important Elements for Safety (INERIS - DRA-35), May 2003.
[5] Defence in Depth applied to Data Processing System (SGDN/DCSSI) July 2004.
[6] Methodology of Defence Elements Identification within a Transport System (Alain COINTET - LAMBDAMU 14 Bourges) – Oct 2004.
[7] Defence-in-Depth & Human Factors (Jean MARION & Alain COINTET - ESREDA Ispra) Oct 2005.
[8] Risk Management Policy based on the Defence-in-Depth Concept (Jacques VALANCOGNE & Alain COINTET - HKRMS Hong Kong) Dec 2005.

[9] Defence-in-Depth & Risk Analysis (Alain COINTET - SRA Orlando) Dec 2005.
[10] Risk Control, Defence in Depth, Indicators & Precursors (A COINTET & Gilles FOINANT – ATEC Paris) Feb 2006.
[11] Defence in Depth and System Engineering – A Synergy for a global Approach of Risks and Responsibilities (Catherine LAVAL & Alain COINTET - LAMBDAMU 15 Lille) Oct 2006.