An integrated approach to organise major risks control in hazardous chemical establishments

Emmanuel Plot, Jean-Christophe Le Coze

▶ **To cite this version:**

Emmanuel Plot, Jean-Christophe Le Coze. An integrated approach to organise major risks control in hazardous chemical establishments. 23. ESReDA seminar "Decision analysis : methodology and applications for safety of transportation and process industries", Nov 2002, Delft, Netherlands. pp.29-41. ineris-00972443

HAL Id: ineris-00972443

https://ineris.hal.science/ineris-00972443

Submitted on 3 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

An integrated Approach to Organise Major Risks Control in Hazardous Chemical Establishments

E. Plot, J.C. Le-Coze
INERIS - Institut National de l'Environnement et des Risques Industriels
Parc Technologique ALATA, BP 2
F-60550 Verneuil-en-Halatte, France

Abstract

In the field of risk prevention, research is often divided or partial. Research work - achieved or in progress - focuses on topics like technical risk assessment, organisation management or human factor: ergonomics, sociology, etc. But little work is dedicated to an integration of all these disciplines into a same methodology.

It is yet obvious that an effective control of major accident risks depends on the ability of an organisation to consider and integrate every aspect of prevention. A separate control of either human factor, or safety technical barriers, or safety management is of course necessary, but does not guarantee a sufficient prevention level on its own. Effective prevention requires the control of every means available.

From this statement, INERIS has started developing an original integrated method to control major accident risks of hazardous establishments under the scope of Seveso II directive. The method is currently tested with voluntary French SEVESO II establishments.

1. Introduction

In January 2002, the European commission released the following statistics: the probability of an accident is 3 x 10" y^{-1} in industrial installations under the SEVESO II directive. It means concretely that for approximately 300 hundred installations, there is an accident per year. In most of the cases, accidents are described as having a close human or organisational components into it.

Indeed, in May 1998, the MARS database, in charge of collecting major hazard within the European community indicates that the human contribution represents 64% of root causes of the declared accidents. These causes can be divided among operational errors or organisational issues. These cover different origins: inappropriate or non existing procedures (13%), bad design of interface (12%), lack of analysis or bad knowledge of the product in use (10%), error due to bad contractors management (10%), device failure following a maintenance operation (9%). These data clearly indicate the weight of human and organisational factors for the major hazard control.

The major accident analysis like the researches done on Bhopal, Flixborough already pointed out these factors, and this has been again recently emphasised after the AZF chemical installation that exploded, in Toulouse, France, in September 2001. The official commission concluded that, among many other propositions, the defence in depth concept could be applied to chemical plants and that the human factors and the organisation were key elements of this principle.

Today industrialists et authorities need methodologies and new tools, integrating the human factors, the organisational issues as well as the technical aspects in order to identify the major hazard risks, to design and improve sociotechnical systems they have in charge, assess their performance and learn from incident and accidents.

2. Meeting the requirements of regulations and facilitate the application of the law

2.1 Linking technical risk analysis and organisational features for the compliance

The first objective of that project is to suggest a method that meets the legal requirements of the so called European SEVESO n directive, translated in the French system through the "arrêté du 10 mai 2000", concerning the installation that have the potential for major hazards. That document requires the industrialists to implement a safety management system, depending on threshold of dangerous chemical products. The safety management system must contain several items:

- Structure and training;
- Identification and evaluation of major hazards;
- Control of process and operation;
- Management of change;
- Emergency planning;
- Learning from experiences;
- Inspection; audit and management review.

This method describes the activities required for major hazard prevention. It is believed that such a representation can facilitate the design, the implementation and the assessment of a safety management system that will meet the SEVESO II criteria. The way these activities are combined is shown in the next figure (Figure 1).

There are 3 levels:

1. The starting point is the risk analysis activity. It identifies and assesses the major hazard scenario to be controlled.
   Along with the identification of the major hazard scenarios, there are the related functions that ensure their prevention and mitigation, they could be described therefore as *criticalfor safety,* and therefore be identified as barriers.
   These critical functions can be met by *critical technical devices* (like an automatic shut down valve) or by *critical activities* (like the action of an operator who pushes a button).

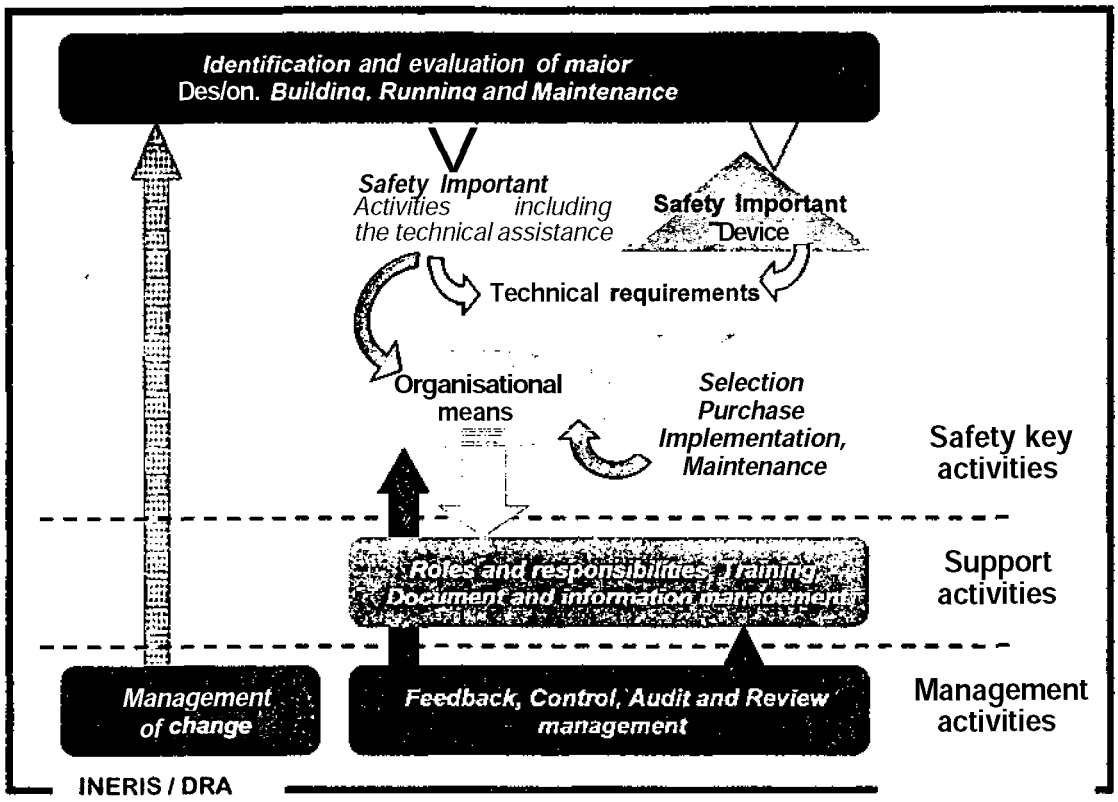

Figure 1. Safety **management** representation.

The device chosen for the critical functions are specified by *technical requirements* that describe their specifications.

The critical activities depend as well on *technical* ***requirements.*** "Technical" because the actors in charge of ensuring the fulfilment of the critical activities always make use of methods and tools, like the procedures describing the way operations should be carried **out,** like the action of pushing a button, and these are, in that sense, considered as depending on technical requirements. The pushing button and the method here are seen as a *technical assistance* for the activity of the actor.

These technical requirements rely on the ability of the organisation to properly buy, install, implement, operate, and maintain them. This ability is seen as the activity of *technical requirement management.*

Along with the technical requirements, there is the ability of the organisation to provide appropriate means for the *co-ordination* and the *competence* for the critical activity. The co-ordination is defined as the distribution of role and responsibilities, the communication and the decision making process at the level of the activity. The competence is described as the knowledge and know-how, and the behaviour (related to safety culture and risk sensibility). In an organisational perspective, the co-ordination and competence are seen as risk and performance factors.

They both rely on the *organisational means,* as distinguished on the figure from technical requirement and technical requirement management.

2. The second level is under the dependence of what has been defined as the *support activities.* These indeed provide all the necessary inputs for ensuring

appropriate level of co-ordination, and of competence as well as for ensuring the activity of technical requirement management. It implies the definition of role and responsibilities, the training, the document and information management.

3. The last level contains the learning from experience, the monitoring, the auditing and reviewing activities. These are seen as the *overall management activities.* At the left bottom of the figure there is the management of change activity. This is a crucial activity as the change can affect the initial risk analysis, and imply new barriers implementation like new activities or devices.

The Level 2 and 3 ensure the continuous improvement of the safety management system.

Such a method couldn't be complete, as it describes a really complex system, and it is acknowledged that some points are missing:

- The support activities ensure for themselves, for the management of change and for the overall management activity, the organisational means;
- The overall management activity ensure the continuous improvement for themselves, for the support activities and for management of change activity;
- The overall management activity and management of change use technical assistance that needs to be managed, by technical requirement management.

For implementation purposes, the first level is described through the use of matrixes. The first matrix divides the critical (safety) function into the chosen activities or/and devices. The second one introduces the technical requirements, as described earlier, associated with the activities and devices selected. The third one can for example put together the critical activities along with the organisational means required to fulfil the activity. These three examples (tables I, II, III) illustrate this.

Table I: Critical functions/activity or device.

Critical functions **Activity or devices**	**Function 1**	**Function 2**
Activity 1	**X**	**X**
Activity 2	**X**	
Device 1		**X**
Device 2	**X**	

Table II: Technical requirements/technical assistance or device.

Technical requirements technical assistance or devices	specification	Time for response	Backup when emergency situation
Technical assistance 1			
Device 1			
Device 2			

Table III: Critical functions/activity or device.

Critical functions Activity or devices	Procedure	Training
Activity 1	Who, what, when, where, how and checking points	Compliance with training specification
Activity 2	Who, what, when, where, how and checking points	Compliance with training specification

The following picture (figure 2) represents an example included in the figure 1.

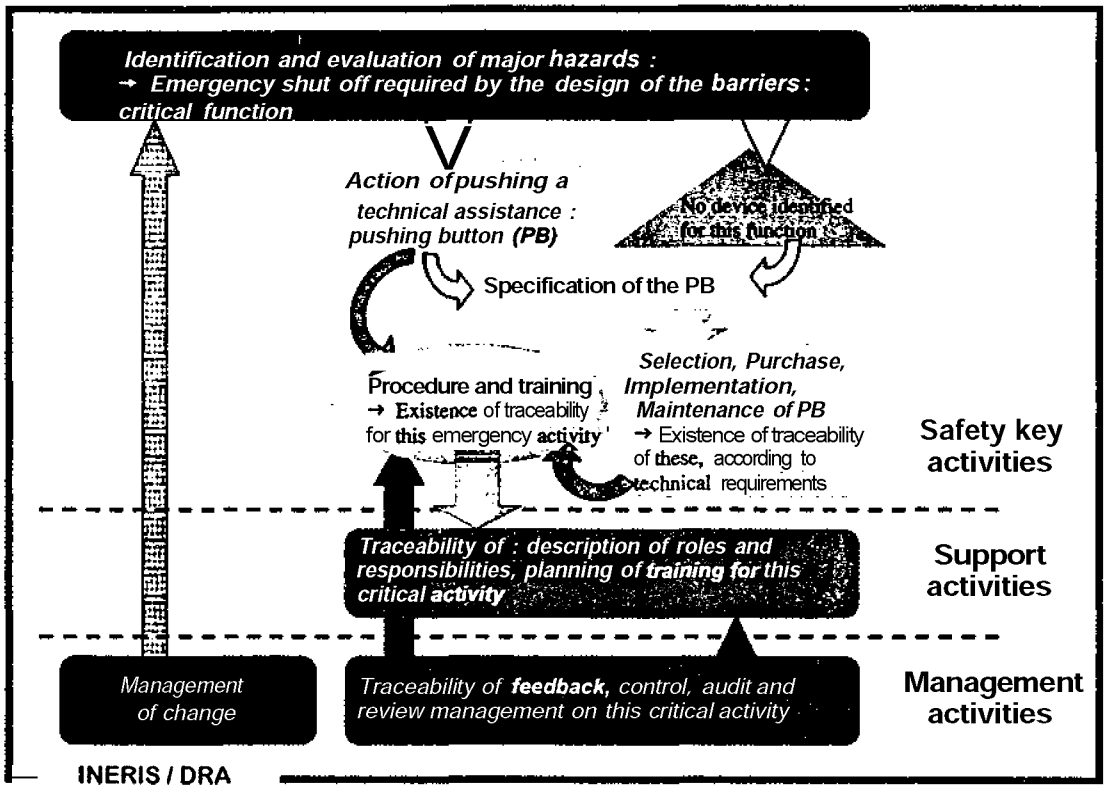

Figure 2. Application of the method to a critical **activity.**

Remarks: First, this method is not based on health and safety approaches that consist in analysing risks at the level of the operator. The method starts with the risk analysis made in a major hazard perspective, namely based on combined risk analyses approaches like HAZOP for Hazard operability study, and PRA for preliminary risk assessment for example. Secondly, it is based on a process approach that consists in decomposing the activities of the organisation. A process is seen as a system of activity that transform inputs into outputs using resources and constraints. The final outputs are hence in our case, the critical functions defined by the risk analysis.

One of the objectives of this method was to provide a structured way of implementing a safety management system, for the compliance with the SEVESC II requirement. This table (table IV) shows how the method fits in the SEVESO requirements.

Table IV: Comparison method/SEVESO II requirements.

INERIS method	SEVESO II requirements
Risk analysis activity	Identification and evaluation of major hazards
Critical functions (all life cycles)	Control of process and operation Planning for emergencies
Management of technical requirements (buying, designing, maintenance)	
Support activities	Organisation and personnel
Overall management activities Overall management activities	Learning from experience Monitoring performance Audit and review
Management of change activity	Management of change

2.2 Different uses

Actually the MIRIAM model can be applied for three different uses:

- It provides a guide for the implementation of a safety management system by visualising the combination of activities that are required to build the system. From the risk analysis defining the critical functions decomposed in critical activities (including technical assistance) and critical devices. The technical requirements and organisational means both specify what are the specification of these. The technical requirements rely on the activity of technical requirement management. All these are ensured by appropriate support activities and by the overall activities management.
- It defines the activities linked with the risk analysis that need to be checked through a external or internal audit.
- It provides a frame for learning from experience, as it describes what are the activities that must be implemented to ensure the risk control, from a risk analysis focused on major hazard prevention. Indeed, once the accidental scenario has been described, it is possible to search for what activities have been inappropriate. In order to do so, it is possible to follow the modelling and see what went wrong. A basic first representation is proposed (figure 3)

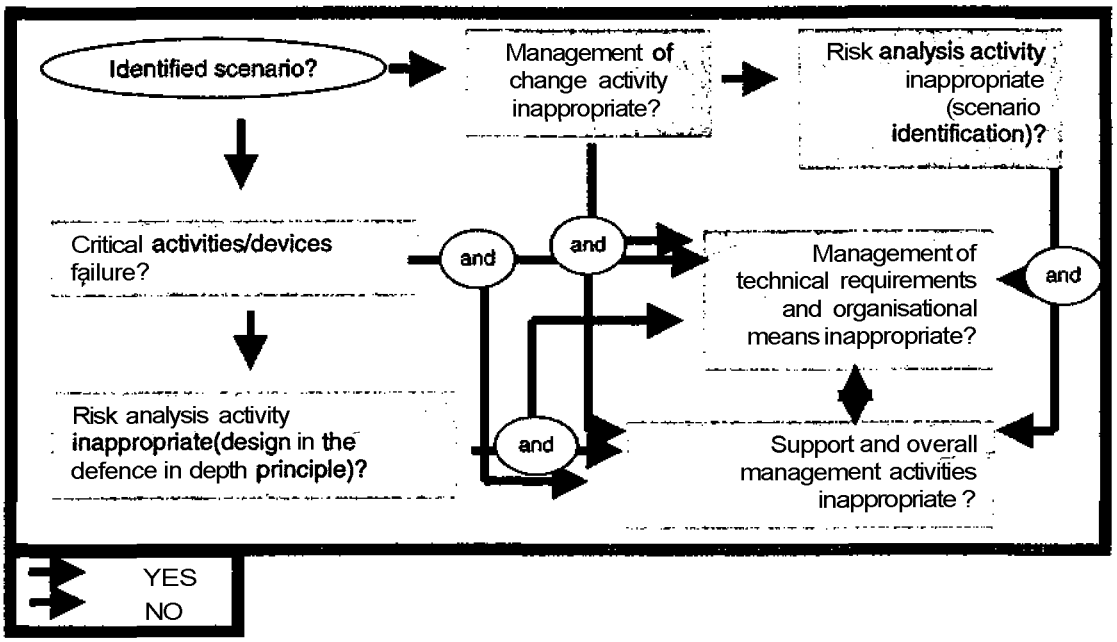

Figure 3. Learning from experience application of the method.

3. Integrating the human behaviour

3.1 Why integrating human behaviour?

The research works on organisational reliability describe that the core issue is the complexity of the **sociotechnical** systems, that must be controlled. What is complexity? There is a wide range of definitions, it is possible to simplify by saying that a system is complex because there are unpredicted events or even unpredictable events. These unpredicted events are **significant** events for safety as there is no designed alternative built to take into account the unpredicted event. This is a problem for safety as their treatment needs to be **ensured,** especially in hazardous installations.

The factors influencing the presence of unpredicted events are numerous. They are linked to the features of socio technical systems.

The consequence of this is that compliance with safety management system is a first requirement, but because of these unpredictable events generated by the complexity of the systems, more is needed. It is argued here, for this precise reason, that compliance **doesn't** always guarantee effectiveness.

3.2 How integrating human behaviour?

The unpredictable events lead to the following findings.

First, automation requires the human intervention for these unpredicted situations, so that the automation can't be seen as the solution for safety. It could be said in that

sense that the human activity allows to make work technical systems that do not work always as intended, and therefore that shouldn't be completely automated.

Secondly, the procedures do not cover all the situations that can arise. It must be acknowledged that working instructions won't be exhaustive, as the context and problems widely vary due, for example, to unpredicted events described here.

The unpredictability of events puts the supervision in a difficult situation, as everything can't be written. All situations can't be described and the supervision is therefore not able to foresee exactly what will be done by the operator. Everything can't therefore be centralised, and a sort of decentralisation is necessary. It implies that in order to find the solutions to the various situations that can be encountered due to unpredicted events, the autonomy of the actors is necessary.

It doesn't mean that the work is considered as being free from planning and monitoring, this remains an important feature of the will to make as rational as possible the way an organisation works. However it is stated that in a complex environment like an organisation in a chemical plant, the supervisors can't control all situations.

The level of safety is based on the co-operative behaviour of the actors who create the necessary synergy to treat and combine information, mental representations, and skills ... for managing this complexity and react accordingly to unpredicted events. A temptation and mistake would consist in trying to rationalise and structure the work through a theoretical frame that would be too general, how much precise it could be. More over, it would be wrong, in such a context to think that every organisational problem comes from the personnel attitude.

This necessary autonomy is implicitly acknowledged by industrialists when in very prescriptive companies, the actors have still a freedom margin and more over, have been asked to use their autonomy to adapt to situations that procedures can't describe. The actors who play a role in safety must comply with procedures but must apply them cleverly. This type of autonomy raises however the question of how to, somehow, "control" it for safety purposes.

The solution consists in implementing performance factors, tailored to the human behaviour (which is free by definition). The method suggests to read each critical activity of a safety management system as described in the following figure (figure 4):

This figure intends helping to frame the autonomy that is implied by the safety.

The entering point is the strategy that can explain the behaviour of the actor. A strategy is namely that an actor is able to find some solutions to the problems he encountered, the result of this being its behaviour. The strategy means that humans are free and is therefore opposed to the idea of a "programme". Thus, their behaviours must be understood through the solutions they found for solving their problems (the sources of this strategic approach is found in sociology and especially in the works of J. Baechler, "Nature et Histoire", 2000, PUF).

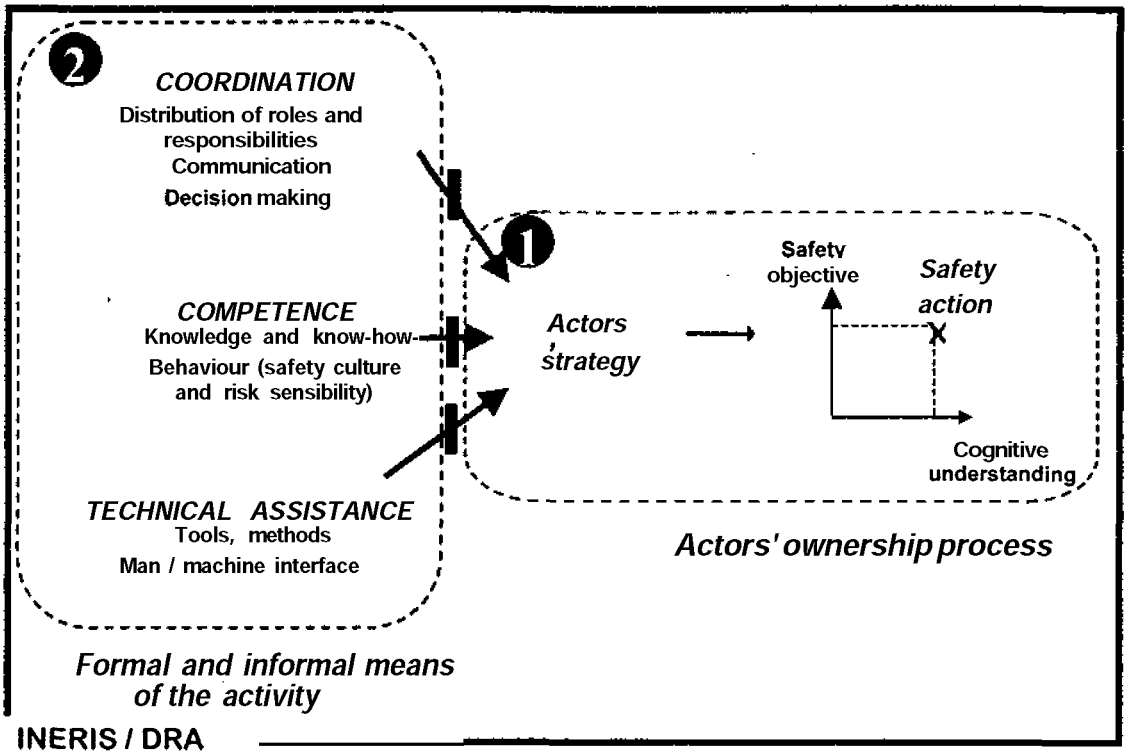

Figure 4: A human behaviour analysis approach.

This is a fundamental point. Thinking about actors not as "programmed" or "determined" is important. It implies that what is required is to look for the factors which influence their behaviour, but without pretending that it is possible to predict them, it is an inductive approach.

Such a way of looking at the organisation leads to find solutions of constraints and resources which defines these unwritten rules of the game of the organisation. If they create appropriate safety practices (represented on the right of the figure), they are described as performance factors, and if they lead to unsafe practices they are called risk factors.

The first part is therefore to qualify the part 1 of the figure. It corresponds to a safety action identification along with the strategy that led to the safety action. The safety action is appraised according to the level of compliance with the critical activity (as defined in figure 1) but as well with the level of safety margin (autonomy) that is required for the unpredicted events that can arise.

The performance and risk factors are represented on the left of the figure 4, in the part 2. However, given the freedom of the actors, it is impossible to predict which are the risk and performance factors. Consequently, the identification of these factors, and thus the organisational solutions, must go back from the observed practices (good or bad with the safety action description) to the influencing factors, through the understanding of the strategy of the actor (from part 1 to part 2)

It is impossible to find the factors (the rules of the game defined by the resources and constraints) without looking first at the strategies developed by the actors that define the safety action.

Consequently, the method suggests three tools made of check list and methodological guidance for, in a first step:

- Identifying the safety practices;
- Analysing the actors strategies that could explain the practices.

and in a second step:

- Identifying the risk and performance factors that influence these strategies.

A global assessment would therefore consist in applying this type of analyse of human behaviour to the three levels of the model (figure 1 and 2), from the risk analysis activity, through the critical functions to the support activity and overall management activity. IT should give a better understanding of how well the system works.

This could be illustrated by the following representation (figure 5), as a help to visualise what the method intends to do.

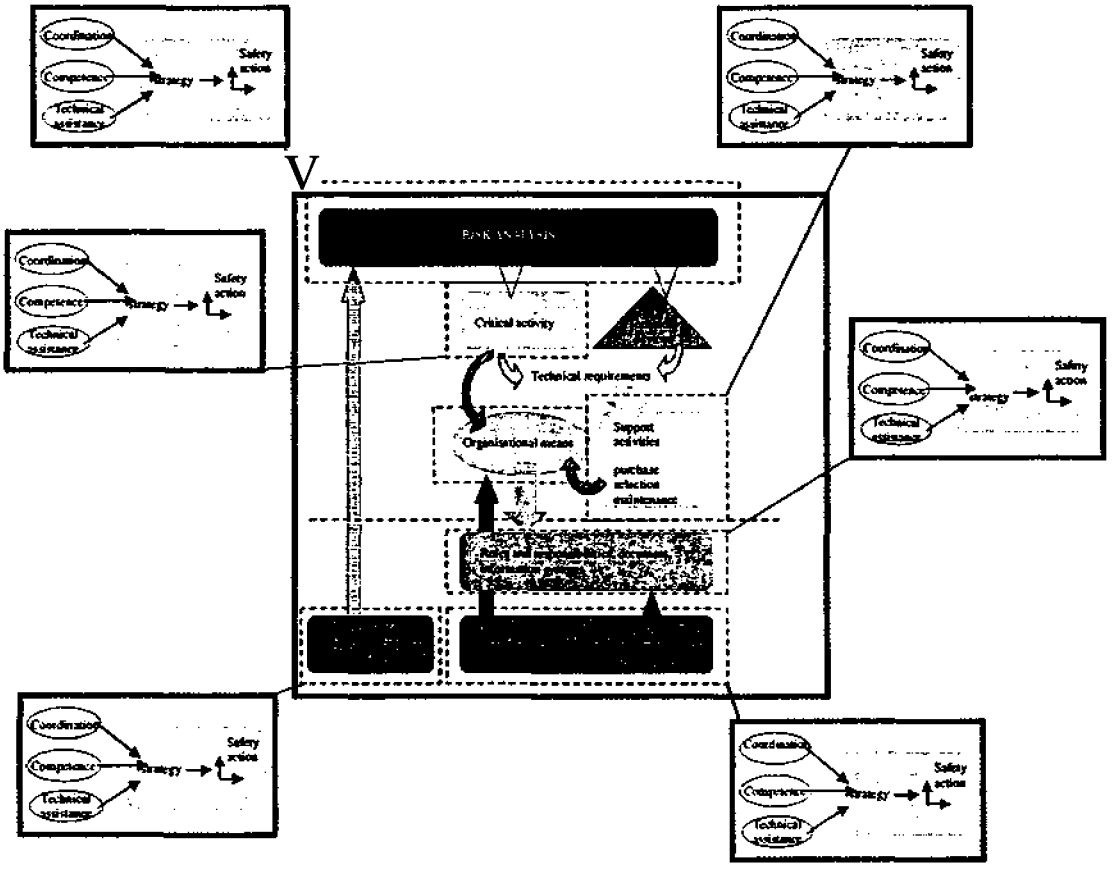

Figure 5. the human behaviour analysis for all activities of the safety management system.

4. Example

An example, which is summarised, is exposed here.

This example is extracted from a real situation where operators are in charge of the control of chemical reactions. In that activity the main risk is the runaway reaction.

- **First step: safety actions and rules associated with the strategies:**

The rules in that organisation are:

Rule 1: Strict respect of procedures. Everything is written in the documents that describe the safety related activities. This documents can be procedures, but checklist too, that allows to strictly follow how to proceed. The enquiry shows that all this is well classified and that traceability of this activity is ensured. The company invested time and resources to achieve such a result. As the operational manager noted: "the safety principle of safety here is based on the existence of procedures and checklists. If these are followed, there is problem".

Rule 2: Four monitoring levels of compliance with procedures. The rule 1 is assured by a monitoring of the operations in real time. This first type of control is allowed by the presence of a second person who checks what an operator does. That's the case for the chemical loading phase, where the quantities manipulated have to be precise. The second type of control is ensured by the traceability provided by the checklist filled through tthe first monitoring, and checked by the team leader (first supervisor). The operational manager (or second supervisor) reads them too, and that's the third type of monitoring. Finally, there are process parameters, which are used for the monitoring of the reaction, like temperature, pressure. The monitoring of products storage level against criteria defined by the quantity that should be used for the reaction, if there is a low quantity of product remaining at a certain point, it is probably that they used too much of these

Rule 3 : The operational manager is the only one able to decide the solutions to bring to problems that were not planned in the procedures. The decisions are centralised. The operators must validate the action that does not comply with the checklist, exepted in emergency situation. The team leaders must validate their decisions with the operational manager before modifying the written practices.

Rule 4 : These three first rules do not cover every single situations, even if they seem appropriate enough for everyone. The real activity is not totally covered by the three rules described, and the operators find solution in such cases. This fourth rule gives the operators the right to organise their work. This situation is seen as a normal due to the necessity of the real activity. But obviously, some actors use this in a way that does not follow the "spirit" of the written rules, but still comply with the traceability requirement of the written rules (a good example here is the act of filling the checklist without actually doing it in real). Everybody knows this, though they don't like talking about it (especially the managers).

What can be said from his enquiry is that there is a good compliance in respect with safety needs and requirements:

1. Procedures are articulated according to risk analyses;
2. Procedures are applied.

But, the safety margin could be considered as insufficient because:

3. Procedures do not describe all the decisions / actions necessary to comply entirely with safety requirements;
4. Controls can easily fail or be enforced;
5. The operational manager must be warned on time, be given the right information, be available when necessary, and competent at any time (no redundancy)...
6. Team leaders and operators are not given the competence neither the right technical means to make their own careful decisions and then arrangements.

- **Second step: identifying the risk and performance factors**

The first part describing the rules leads to put in light the following performance and risk factors:

Factors linked to co-ordination :

1. Range of production limited can be controlled by only "one brain";
2. Hall of production easy to walk across, next to operational manager's office;
3. Lack of a real structure of responsibilities, lack of official acknowledged delegations, culture of intrusion into the delegations;
4. Very little communication between production unit and other directions of the establishment;
5. No place or structure dedicated to dialogue nor exchange of information and opinion.

Factors linked to competence :

6. Operators' competence is adapted to the detail of procedures;
7. Operators and team leaders lack of knowledge and information on the substances used onsite, the dangerous runaway reactions and the existing safety barriers chosen to assure safety (agitator in reactor...);
8. Lack of competence for the operational manager about the way to organise and control the actors' autonomy;
9. Lack of a safety culture : everyone seems satisfied with a situation not very careful.

Factors linked to hardware interface :

10. Procedures and control means are totally operational (use of specific checklists for each batch reaction);
11. Methods and procedures don't help operators make their own analysis of the situation and know their autonomy of decision.

The identification of these factors suggests some improvement proposals:

- **Developing the competence of team leaders and operators through:**

1. The explanation of the decisions of operational manager (namely the definition of daily production planning);
2. Asking each operator to communicate two near misses per week. The most critical events should be tackled within the following month;
3. The contribution of each actor alternatively to a risk analysis;
4. Asking each actor to propose two ways of improvement per month ... They should be considered the same way as near-misses;
5. Setting up a training programme with exercises about employed substances, accidents scenarios and safety barriers implemented;
6. The communication on safety, the necessary autonomy of the actors and the limit of this autonomy;
7. Re-placing to other functions the actors who are not able to develop enough their competence.

- **Decentralising the decision-making and develop new kind of procedures through:**

8. The evaluation of the actors on defined results instead of the strict respect of procedures (new kind of controls);
9. Weekly «mini collective risk analysis» to account for all possible change in production, etc...
10. The development of new kind of procedures : operational procedures defining the limits of operators' autonomy, etc...

5. Conclusion

The aim of such a method is to be integrative, and to embrace several layers of analysis required by the multi dimensional origins of the accident, from the technical failure, to the human behaviour and the organisational context.

From a technical approach with the risk analysis of the technical installation to the organisational side of the assessment with the models developed here, this theoretical work carried out has proved so far to be efficient when it came to apply it on real cases.

The next step is to develop further and enhance the validity and usefulness of the method for various users. This will be done through the testing of the method and through the opportunity of comparing the approach with other safety management models.