HAL
open science

Development of the ATOS concept, analysis of technical and organisational safety

Jean-Christophe Le Coze, Emmanuel Plot, Franck Prats, Olivier Salvi, A.S. Vince

To cite this version:

Jean-Christophe Le Coze, Emmanuel Plot, Franck Prats, Olivier Salvi, A.S. Vince. Development of the ATOS concept, analysis of technical and organisational safety. Congrès ESREL 2002 "Aide à la Décision et Maîtrise des Risques", Mar 2002, Lyon, France. pp.NC. ineris-00972363

HAL Id: ineris-00972363

https://ineris.hal.science/ineris-00972363v1

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.

Development of the ATOS concept, analysis of technical and organisational safety

J.C.LE-COZE. A.S.VINCE, **O.SALVI, F.PRATS,** E.PLOT.
INERIS - Institut National de l'Environnement Industriel et des Risques
Parc Technologique ALATA
BP 2
60550 Verneuil en Halatte
Tél. : +33.3.44.55.66.77
Fax. : +33.3 44 55 66 99

Summary

ATOS is an experimental project based on 3 simple guiding principles aimed at integrating several disciplines for a risk analysis. The three guiding principles are:
- a vision of the organisation with a balance between an formal **(centralised,** or what is written) and an informal (decentralised, or unwritten rules) part,
- "you do not manage what you cannot measure",
- a focus on the quality of the barriers for the risk control.

The disciplines involved in this project are, respectively to these principles, the organisational sociology, quality management and engineering. In this paper, the approach is explained and the result of a first application is presented. ATOS is designed to be a transferable tool for managers who have in charge the management of major hazard prevention.

1 Introduction

The ATOS project, Analysis of Technical and Organisational Safety, has been developed following the European Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. Indeed, the directive contains a specific requirement in its annexe 3 for the risk control through the implementation of a safety management system (SMS). This SMS spécification has been included in accordance with the high rates of organisational root causes admitted to be at the origins of the accidents **[1].**

This new requirement of the directive introduces a dynamic dimension of prevention. The risk analysis is therefore not anymore a static approach (like a photograph) of the installation that includes only the safety design of **it,** but includes also now the interaction with its environment. The people and groups of people working on it constitute its direct environment, within the limits of the plants.

Thus, the new SMS requirement raises directly the question about the impact of this environment on the technical system. These people and group of people, within the limits of the plants, are ruled in their activities by management systems (like does a SMS) but as well as by the interactions they have each other.

This complex environment within the boundary of the plant needs to be addressed and introduced in the risk analysis.

This document describes an attempt to create a method integrating this dynamic dimension between technical and organisational issues. One question raised is therefore how can the link between the technical and the organisational approach be made explicit.

2 ATOS objectives and associated concepts

The project ATOS has several objectives:

2.1 Creating a frame where people from different disciplines could integrate their knowledge.

An objective of ATOS is to allow people with different background to work together. It means that these people must share a common understanding of the risk analysis and risk control; and the role they play in that analysis. This requirement can be met through a common vocabulary and concepts associated with it, and with a model of the approach that can bring a shared vision of the project. These steps are the elementary phases **of** the process of disciplines integration for a common objective.

The common objective here is indeed to include a dynamic dimension to the risk analysis. For that, three competencies are integrated in ATOS:

- Engineering, for the technical risk analysis of the installation (engineering science),
- quality auditing for the SMS structure (management science),
- organisational sociology for the study of interactions between people within a defined system (social science).

ATOS is really an experimental project because the dimensions, the concepts, the ideas that each discipline brings in the project do not match immediately. A lot of working-group work has to be done to start to apply specific tools from the different approaches in a common frame, where they can all **"fit".** This is what we could call a process of integration of disciplines (figure 1).

2.2 Integrating a human approach in the SMS through the organisational sociology angle.

The ATOS concept is based on the SMS specifications described in the annexe 3 of the SEVESO II **[2].** This is therefore the starting point of the approach.

A SMS is seen as a structure of the organisation that rules the work processes of different levels of people working in chemical plants for the major hazard prevention; from the director, to the manager to the operator. The SMS is traceable, in the sense where an auditor can check the activities through formal documents (formal is defined as something written). This **traceability** is the support of the principle of assurance.

Assurance implies that you can proof through tangible traces that things are carried out against defined rules. It can be therefore a procedure, a record of an action performed against a procedure, a work maintenance planning **etc...The** directive gives 7 main chapters that must be implemented through these principles of assurance and traceability.

It is argued that this approach has its limits. A description of two obvious limits is presented here.

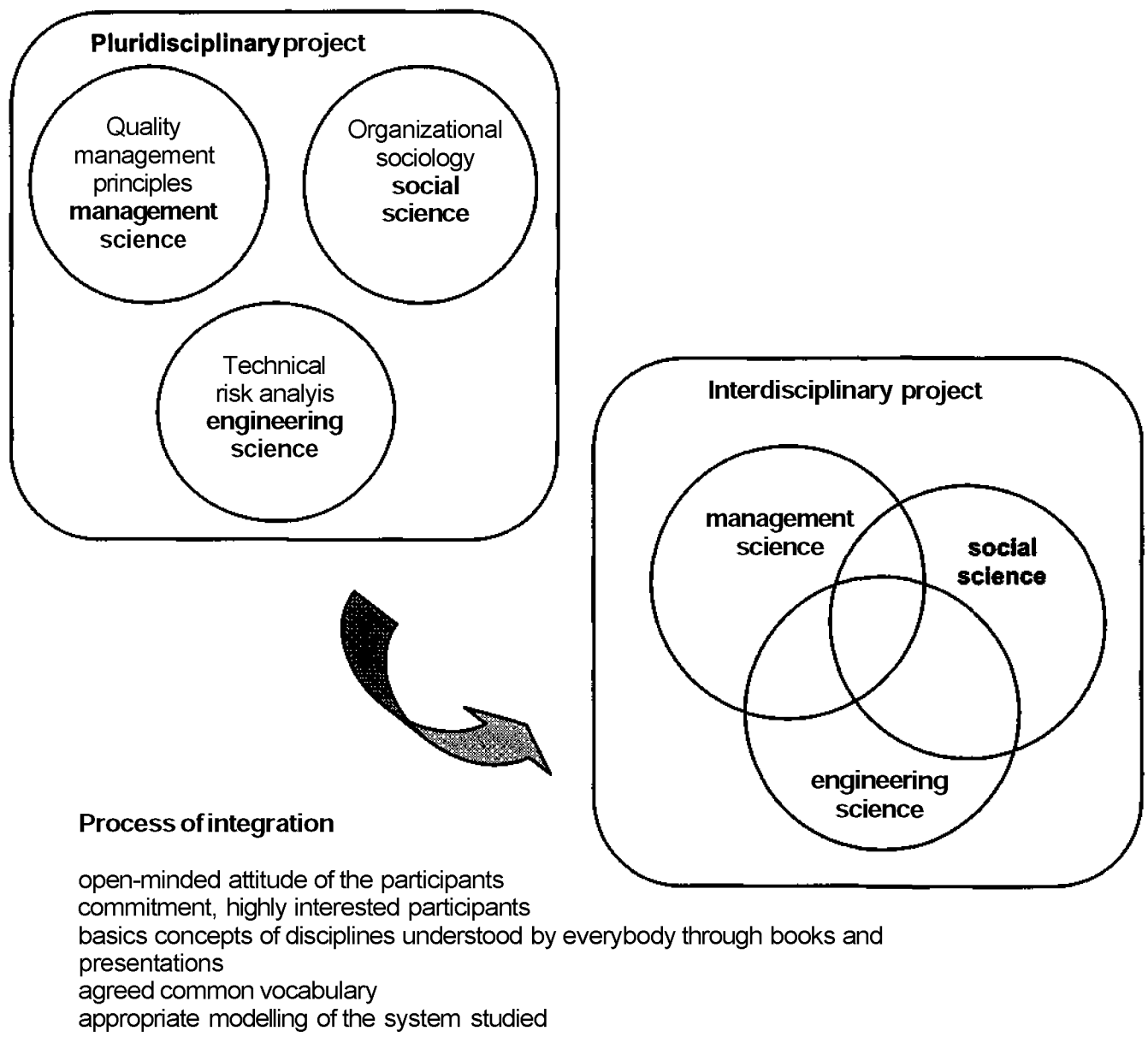

Figure 1 : Process of integration from **pluri** to interdisciplinary approach

2.2.1 Everything can't be written

First of all, everything (in relation with the risk control) can't be written. All situations can't be foreseen and described in procedures.

That point has been identified as an important feature in organisational approaches in general. Centralisation (everything has to be **written)** versus decentralisation (everything has not to be written) is a core concept which has been widely issued. James Reason [3] identified two types of organisations:

"Administrative controls range from the mainly prescriptive to the largely discretionary. The former depend primarily upon external procedures, while the latter are provided by internalised knowledge and ***experience-or*** *in a word, training. Between the two are various blends and mixtures. "*

Here the terms prescriptive - discretionary are used. James Reason imagined a continuum on which organisations would move along, depending on their style, more prescriptive, or more discretionary. This is an interesting concept.

C.Perrow in his "Normal Accident" book [4] wrote about this idea of the organisation position between centralised (prescriptive) and decentralised (discretionary) style, when participating in some discussions about nuclear power plants organisation:

"we *cycled endlessly through the problem of insuring rapid, unquestioning response to orders from high (or orders in the procedures manual), and at the same time allowing discretion to operators. Regarding discretion, the operators would have the latitude to make unique diagnoses of the problem and disregarded the manual, and be free of orders from remote authorities who did not have* ***hands-on*** *daily experience with the system. We could recognise the need for both, we could not find a way to have both"*

This is an issue that needs to be explicitly questioned. What sort of organisation could comply with both needs? How to measure that position along the Reason's imaginary continuum. Centralisation (everything under formal activities) is necessary but not sufficient, because of the unpredictable. The unpredictable implies decentralisation to cope accordingly and independently in real time with a situation of potential disaster, individually but also within a group. How to describe this balance is a key issue (figure 2).

During the daily life of an organisation, they are things done in relation with the prevention of major hazard which are not formal. These things are an organisational answer to unpredicted events, in the sense where they are not and won't be covered by any procedures. These situations arise under constraints and changes of the technical environment (the installation and technical system itself that designers **can't** totally cover) but as well as changes and constraints of the organisation itself (people interactions, changes in the organisation structure **etc...).** That will always be the **case,** there will be always unpredicted situations.
So rather than expecting of a system to write everything, it is important to consider right from the start that everything won't be written. That is important to integrate the aspects in the SMS assessment approach.

2.2.2 Everything can't be tangible through paper traceability

The SMS features covers 7 areas of management, most of them directly safety related:

Identification and evaluation of major hazards.
Management of change.
Operational control.

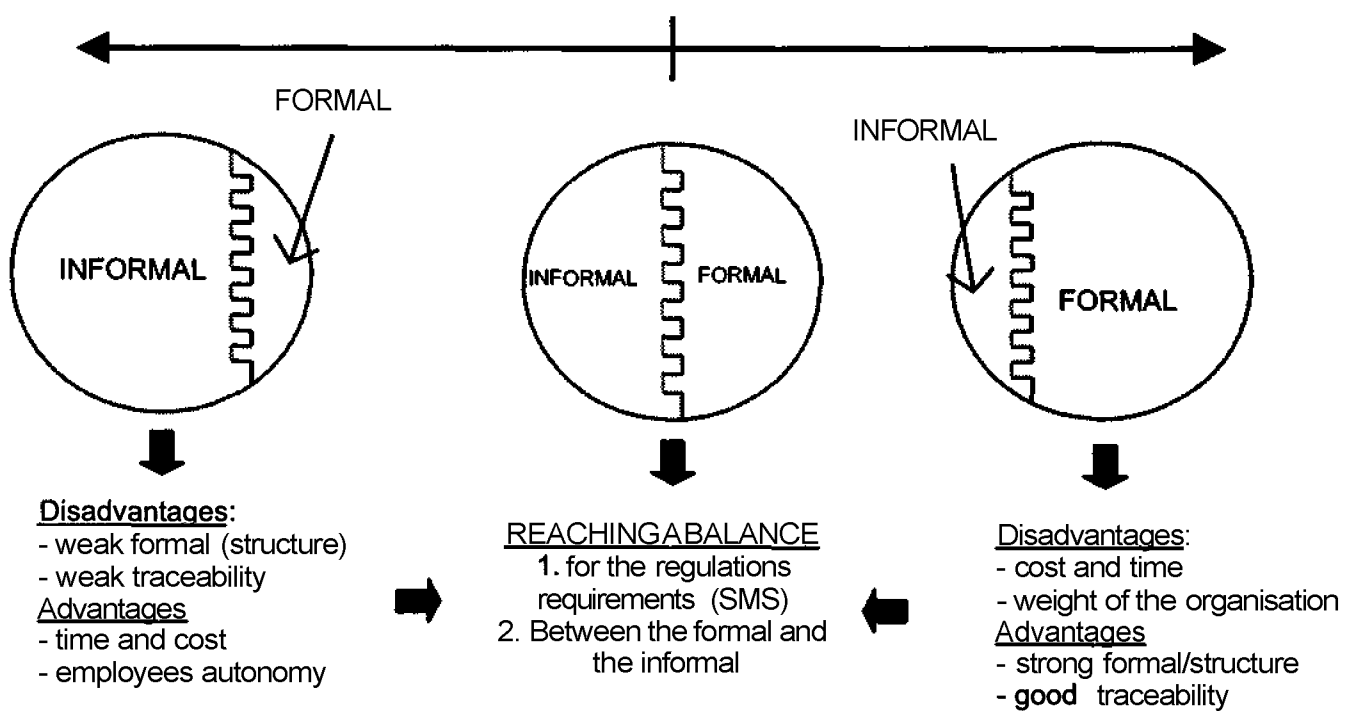

Figure 2. Balance between formal and informal aspects of organisations

Emergency preparedness.
Learning from experience.

The 2 others are general requirements of management systems in general **(quality,** environment **etc...):**

Organisation and personnel.
Audit and review.

These chapters cover a range of organisational features that however do not give a complete picture of what is the organisation. As written previously, again, one need to go beyond what is written.

These chapters and their implementations becomes formal and therefore tangible aspect of the organisation, related to safety. They are "**written** rules" that shape the structure of the organisation. It is not a discovery for anybody to say that some "unwritten rules" do exist too **[5].** They are actually never explicitly mentioned in any management system because they are the result of interactions between people **[6], [7].** These unwritten rules are developing as a result of interaction between people at several levels of the organisation.

These unwritten rules have an impact on features of the organisation like **communication,** co-ordination, leadership, decision making, learning... These organisational features are not explicitly formulated in the SMS but they are acknowledged to be important characteristics of an effective organisation, according to a sociological perspective.

It is actually understandable that no formal traces exist of these features. How could you rely on paper to say that you have a good leadership in the company? How could rely on paper to assure that you have an appropriate co-operation?

2.2.3 Consequence for the ATOS concept.

As a consequence, the concept acknowledges two dimensions of the organisation. There is a formal side described as a written part of the organisation, covered by a management system, and there is an informal described as the not written part of the company.

It is argued in ATOS that both an auditing **technique**[1] (assessment of the formal side of the organisation in relation to the major hazard prevention) and a sociological approach of the organisation (assessment of informal features of the organisation) must be complementary. This sociological approach is based on the strategic **analysis**[2]**.** Together, these two approaches must give a more comprehensive picture of the organisation (figure 3).

[1] The technique of auditing consists of checking compliance against formal standards and records, through the auditing loop including for steps: asking, looking, checking and recording.

[2] The stategic analysis [6] is aimed at understanding the unwritten rules, the underlying structure of an organisation, using a system approach based on the power, bounded rationality and culture to define the relationships between the actors of the organisation. This allows to give a more dynamic picture of the organisation and is a good tool for driving the change if necessary.

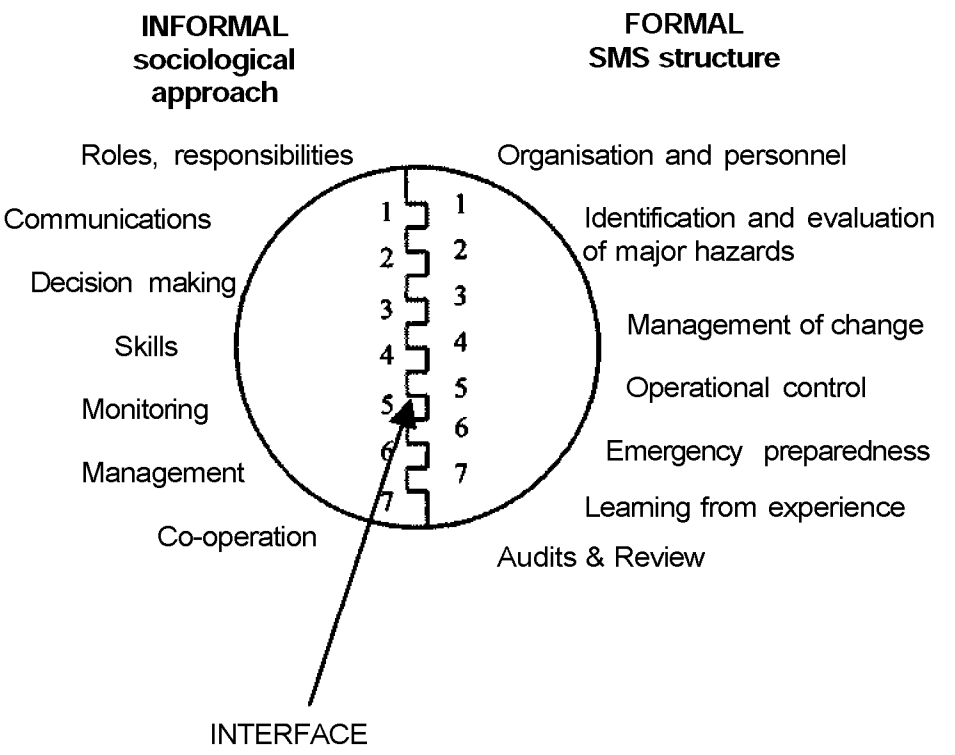

Figure 3: 2 complementary approaches of the organisatior

It is suggested in ATOS that the two approaches will be used for the risk analysis. The problem of their interface is therefore clearly raised.

2.3 Creating a set of safety indicators based on this specific approach.

2.3.1 The SMS performance measurement system

A SMS is based on the principle that "you do not manage what you cannot measure". For that a performance measurement system is built within the SMS. This system is based on indicators.

These indicators give a picture of the state of the SMS. The indicators must be therefore closely related to the prevention of the major hazard. Two alternatives are possible at this stage: trying to eliminate all initiating events and therefore put some indicators on these practices or trying to assess the defences that prevent the risk [2], **[8].**

The later proposition is more relevant since the complexity of the systems (a chemical plants) make the search for the initiating event a rather difficult task **[4].**

It is suggested in ATOS that the performance measurement system must show how the risk control is assured bya high quality of the barriers, or in other words, in accordance to the quality **approach,** by the assurance of the barriers effectiveness.

Basically, these line of defences can be described as technical equipment (a pressure valve system) or as a

human operation (an operator who must shut down the installation under defined criteria).

The seven chapters of the annexe 3 of the SEVESO II directive describing the SMS are the organisational mechanisms that give support to the quality of the barrier. For example, the management of change is implemented in order to assure that any technical modifications on the installation will be assessed in terms of its impact on the safety on the installation, and therefore on its impact on the effectiveness of the barriers. The organisation and personnel chapter will assure that the people (at any levels) will receive the appropriate training terms of safety issues related to their **work...etc...**
So in terms of indicators there are outcome indicators which describe the level of assurance of the barriers and the activities indicators which describes how the organisational mechanisms are working and implemented. Both can be checked through the auditing technique (see figure 4).

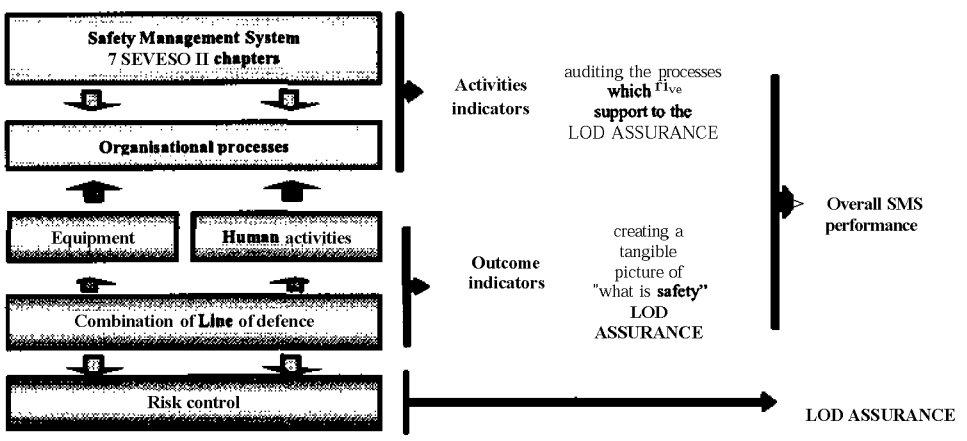

Figure 4. Representation of a safety performance measurement system SMPS

The auditing technique is based on the traceability, every questions related to the system must found its justification on paper.

It is the easiest way to create tangible indicators that anybody can ask for to check the compliance (subjectivity is eliminated- it is here or it is nor here). Does the record of the last preventive maintenance on this equipment according to the maintenance plan exist? Yes or No? This is a good example of tangible indicator (that can be even use for quantification).

Sometimes however a judgement is required too. For example, there is an emergency procedure for an unusual situation at work during the process. How do you know if that emergency procedure is relevant for other unusual situation that may arise (see 2.2.1 everything **can't** be **written)?** These more intangible indicators of compliance need to be clearly address when it comes to audit a system at the operational level. Often the solution is to rank the judgement on a semi-quantitative scale from bad to good.

2.3.2 Adding the informal part in the performance measurement system

This measurement performance system is therefore based on a formal aspect of the organisation. What is suggested here is to add the informal features described earlier (see 2.2.2 everything can't be tangible through paper traceability), through the same indicators classification between tangible and intangible. This work would be done through a different approach of the organisation than the auditing one, a sociological approach. This sociological approach will be based on the strategic analysis [6], **[7].**

This figure (figure 5) includes the informal aspect of the organisation in the safety performance measurement system of the SMS described previously:

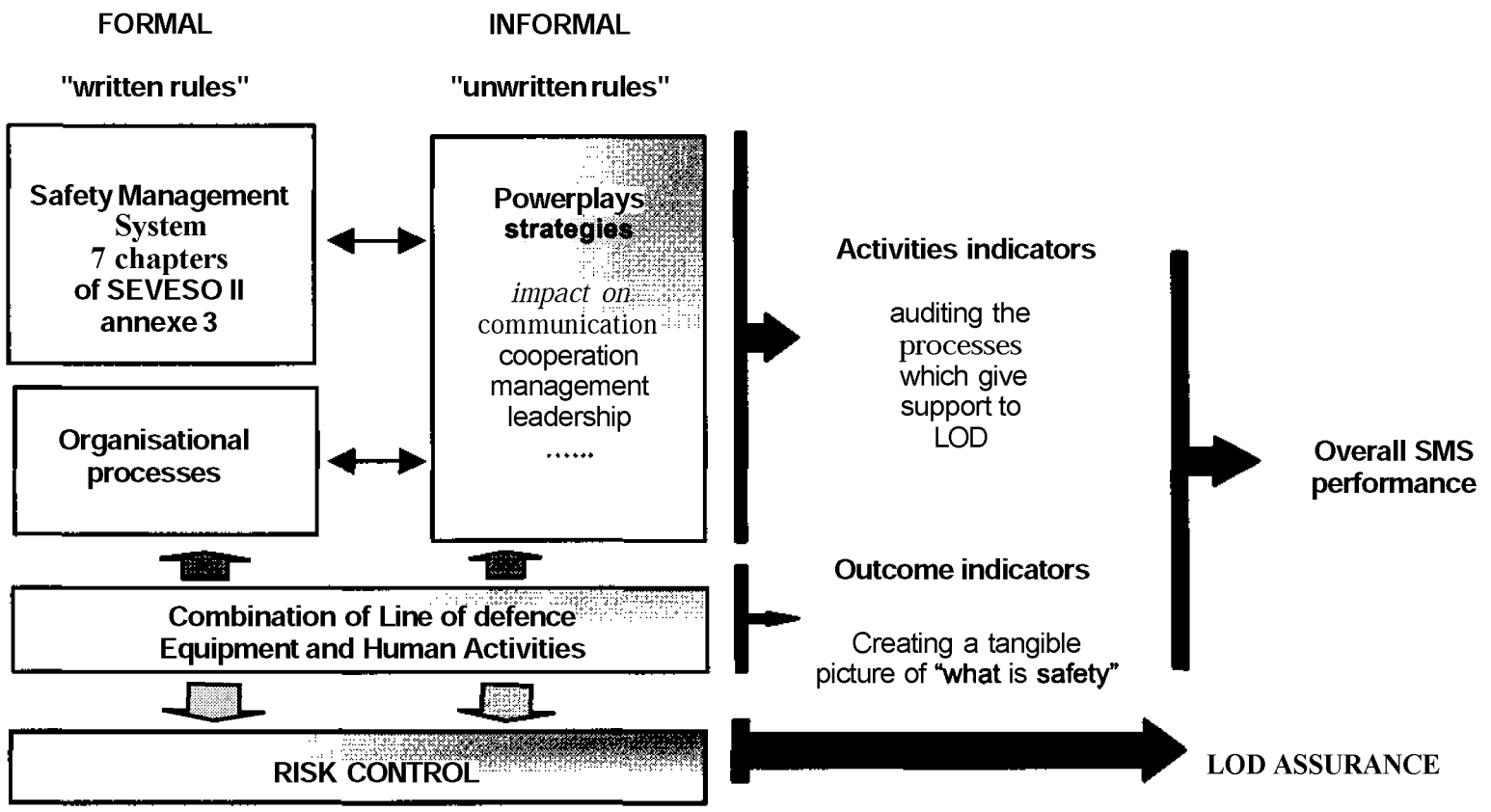

Figure 5. Adding the informal dimension to the representation of SPMS

3 Site tests

3.1 Methodology

For the site experimentation, the following steps have been applied.

First a technical risk analysis that allows to identify the scenarios and the **barriers** for the risk control. These barriers are technical equipment as well as human operations.

Secondly all the formal aspects that could be related through the assurance of this barriers is checked through the audit technique with the 7 points of the SMS.

And finally the sociological approach is carried out.

In certain cases, the company does not have a formal SMS. In that situation an initial review is carried out to identify the practices linked to the major hazard prevention as a starting point, and therefore can address the formal activities that need to be written. The sociological assessment evaluates how to implement as best as possible the formal SMS based on the initial review, to map the informal features of the organisation.

These three steps are represented in figure 6.

3.2 First tests

The first application of this method is currently carried on a SME chemical plant.

4 Conclusion

The ATOS method is an innovative concept trying to merge different relevant approaches for the risk assessment. The angles selected for that assessment, namely engineering, management and sociology, have been integrated in ATOS. This integrative process led to the **interdisciplinarity,** where different specialists can communicate and build a common frame for the risk assessment.

The ATOS method consists in three steps: a technical risk analysis, an audit of a formal SMS and a sociological approach revealing the informal side of the organisation.

The application of that method on site showed the difficulty for one person to encompass the whole method, and it is definitely a complementary work between specialists that has to be done for the moment. The quality of the link between the technical analysis and the organisation assessment depends on this.

Finally, to be transferable to managers, the method must be further described and worked out, particularly through the development of a set of appropriate indicators.

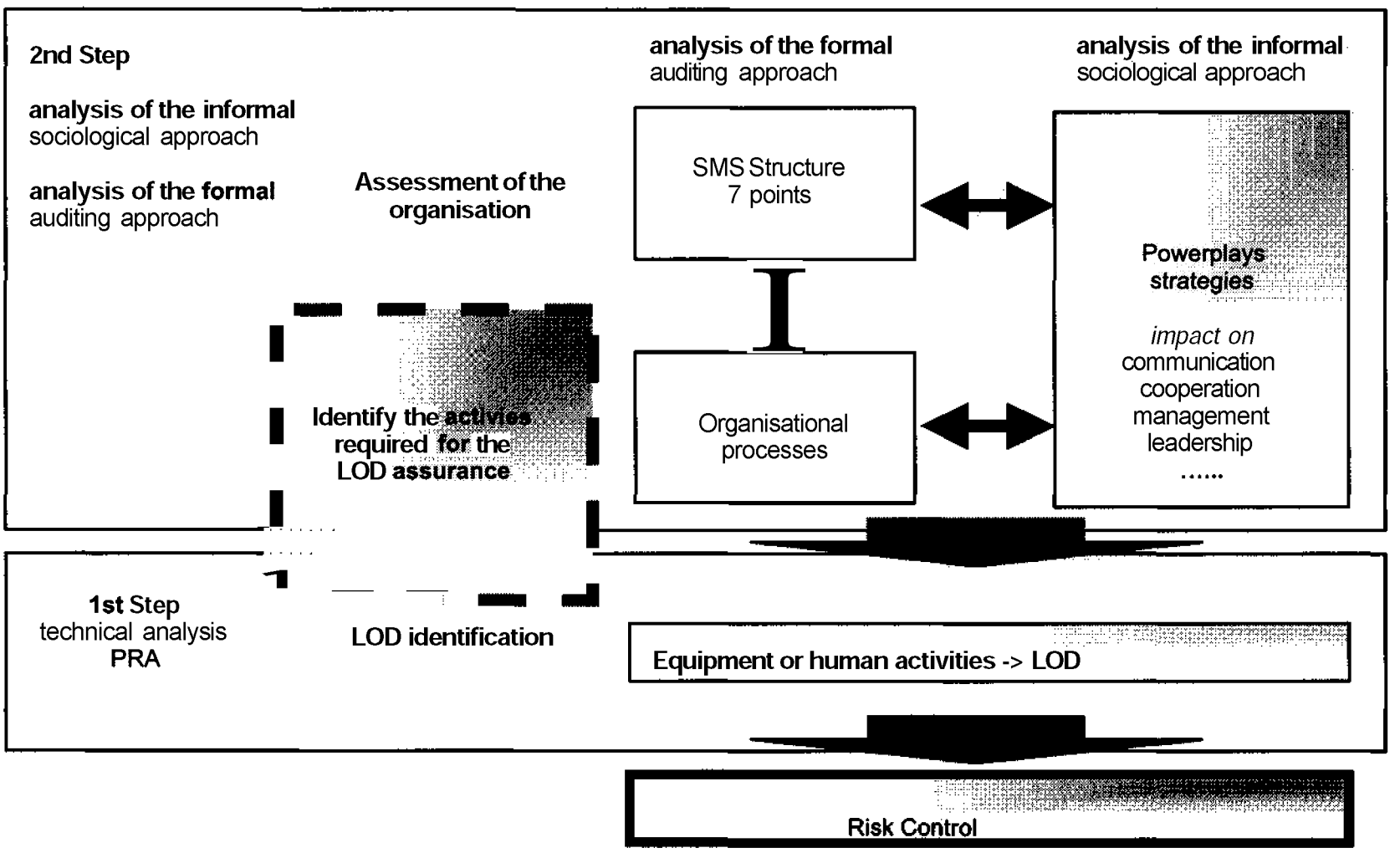

Figure 6. ATOS method

References

[1] Papadakis.G.A, **Porter.S,** Guidance on inspections as required by article 18 of the council directive 96/82/EC **(SEVESO** II), **DGXI** of the European Commission, Institute for systems **informaticsa** nd **safety,1999.**

[2] European Council Directive **96/82/EC** of 9 December 1996 on the control of major-accident hazards involving dangerous substances, annexe 3.

[3] Reason.J. Managing the risks of organizational accidents. Ashgate. 1997. 252p.

[4] **Perrow.C,** *Normal accidents, Living with High-Risk technologies,* second edition **1999,** Princeton University Press.

[5] Scott- **Morgan.P,** The unwritten rules of the game, **Mc Graw-Hill,** 1994.

[6] Crozier.M, **Friedberg.E,** "L'acteur et le système : Les contraintes de **l'action** collective" Editions du **Seuil, 1981.**

[7] Friedberg.E, Le pouvoir et la règle, Edition du seuil, **1993.**

[8] Reason.J. *L'erreur humaine.* Presse Universitaire de France. Collection Le Travail Humain. **1993.** 366p.