Bayesian Network Modelling the risk analysis of complex socio technical systems

Aurélie Léger, Carole Duval, Philippe Weber, Eric Levrat, Régis Farret

Léger A., Duval C., Weber P., Levrat E., Farret R. "BAYESIAN NETWORK MODELLING THE RISK ANALYSIS OF COMPLEX SOCIO TECHNICAL SYSTEMS". Submitted to: 4th Workshop on Advanced Control and Diagnosis, Nancy - France, 16 et 17 nov., 2006.

BAYESIAN NETWORK MODELLING THE RISK ANALYSIS OF COMPLEX SOCIO TECHNICAL SYSTEMS

Léger A.[1-2], Duval C.[2], Weber P.[1], Levrat E.[1], Farret R.[3]

[1] Centre de Recherche en Automatique de Nancy (CRAN), UMR 7039, CNRS Nancy Université, 2 rue Jean Lamour 54519 Vandoeuvre les Nancy Cedex, France.
[2]EDF-R&D, Département 'Management des Risques Industriels', 1 avenue du Général de Gaulle 92141 Clamart Cedex, France.
[3]INERIS, Direction des Risques Accidentels, Parc technologique ALATA BP 2 60550 Verneuil en Halatte, France.

Abstract: The risk analysis of a system is a multidisciplinary process in constant evolution. Indeed, if a few years ago, analyses were limited at the technical level, it is today necessary to consider the system in a global way, by including Human beings and Organisations. But this involves an increasing complexity of the studied system, because of the widening of its limits and the diversity of considered disciplines. This article proposes a method to structure the knowledge in a decision-making model.

Keywords: Complex systems, Multilevel systems, Socio-technical system, Decision-making, Probabilistic risk assessment.

1. INTRODUCTION

In classified installations[1] (nuclear power plants, chemical plants …), the occurrence of a critical event (major accident) cannot be accepted. In May 1998, the database MARS[2], listing major accidents which have occurred in European Union, indicated that human failures represent 64% of deep causes of declared accidents (11% due to an operator failure, and 53% to a dysfunction of the organisation).
Thus, the risk analysis of these installations has to consider not only the technical dimension, but also human beings who influence it and organisations in which they evolve. By making this analysis, the risk of critical scenarios omission can be reduced and the real evolving of the system can be more easily understood.
It is also necessary to have a quantitative model allowing the simulation of the system evolving in order to help the decision-making (to compare several safety barriers impacts on system components …).
In these objectives, this article presents principles of a risk analysis at a technical level, specificities of the risk analysis of a socio-technical system, a method allowing to structure the knowledge and a method for the integration of safety barriers.

2. TECHNICAL RISK ANALYSIS

In this section, some characteristics of standard risk analysis are underlined in order to present the context of the problematic.

What is the risk and how can it be assessed?

Risk is a largely studied concept. Many authors have developed their own definition. For the standard ISO 14121 (1999) it is the combination of the occurrence probability of damage and its gravity. It can also be defined as an event or a sequence of events that can prevent achievements of entity (or group) objectives, or can reduce the organisation capacity to carry out its objectives (Deleuze, 2005).
In this problematic, the risk is defined as the association of cause and consequence events characteristics of a given situation (Gouriveau, 2003).

Risk assessment. This process is defined in the standard ISO 14121 (1999) as a series of logical steps that allow the expert to examine, in a systematic way, dangerous events associated to a machine. It consists of the risk analysis and the risk evaluation (fig.1).

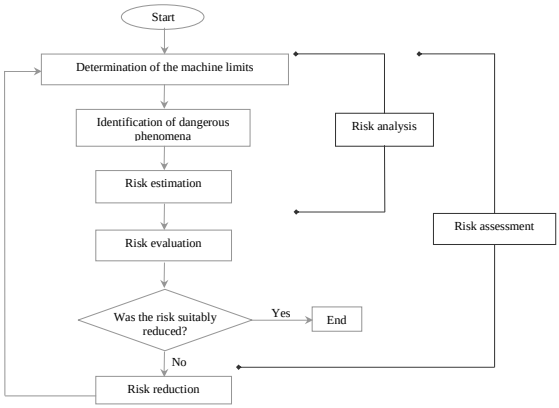

Fig.1. Risk assessment and risk reduction processes

The 'Bow-tie' risk analysis

In this problematic, the objective is the study of critical events (*ERC* in the technical level of the fig.2) which are characterised by a loss of containment (LOC, for fluids) or a loss of physical integrity (LPI, for solids) for a classified installation[3].

[1] It is a permanent installation of which the operating presents risks for the environment.
[2] Major Accident Reporting System.

[3] The risk of core fusion in a nuclear power plant for instance.

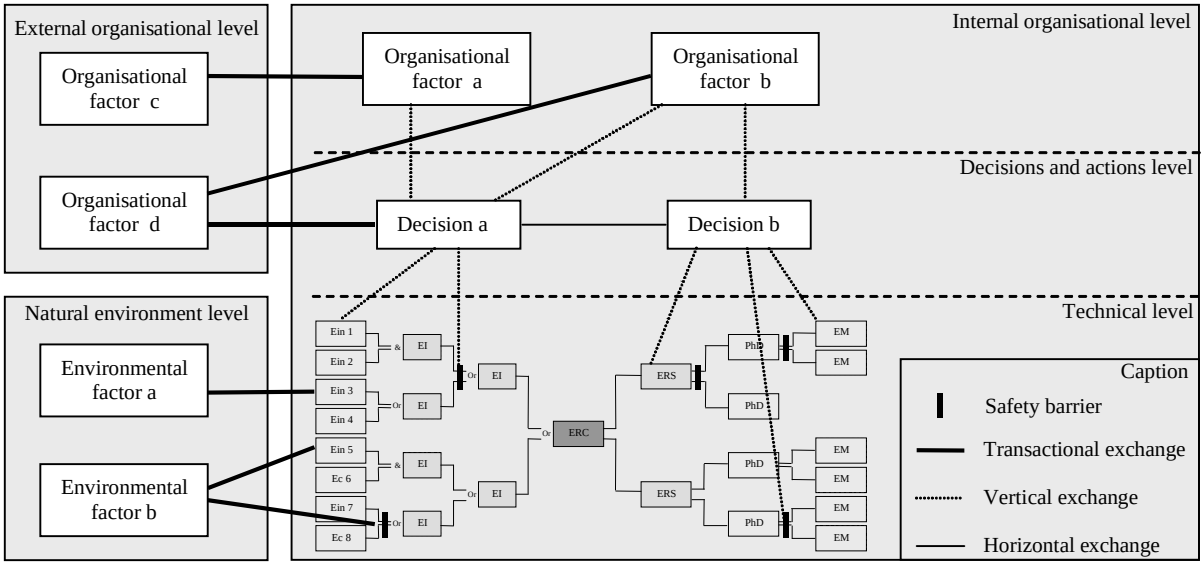

Fig.2. Conceptual diagram for a global risk analysis

The 'bow-tie' method (in the technical level of the fig.2) is a suitable one to compute a technical analysis. This is a method developed in the European project ARAMIS[4] (Andersen, *et al.*, 2001). It is composed of a fault tree (left part of the scheme) and an event tree (right part of the scheme).
In this method each path defines an accident scenario. Thus it allows the description of an accident scenario occurrence from initiators to final consequences by taking into account barriers operation.

Limitations and new needs

Unfortunately the method described above is only usable at a technical level, and recent studies have shown the implication of Humans beings and Organisations in the occurrence of major accidents: Tchernobyl explosion in 1986, Ladbroke Grove collision train in 1999 (Cullen, 2001a; Cullen, 2001b), Columbia crash in 2003 (Caib, 2003)… Consequently this method has to be modified in order to integrate these dimensions in the analysis.
Moreover, current methods are not adapted because they are limited to Boolean variables and uncorrelated relations and they do not include repairing notions and temporal dependencies.
And then, since 2003, it is necessary to take into account the law 2003-699 (JO 175, 2003). This law requests the introduction of the probability concept in any risk analysis.

3. GLOBAL RISK ANALYSIS

In this section the risk analysis principles of a complex socio-technical system taken in its environment are described.

Characteristics of the system

As presented in the first part, the starting point of the analysis is the technical system, which is constrained by external processes.

These processes are divided into four distinct categories (fig.2) inspired by the SAM[5] approach (Paté-Cornell and Murphy, 1996):
- The *Decisions and actions level* which represents processes linked with the decision-making at the individual level,
- The *Internal organisational level* which represents processes linked with the management of the enterprise (in which the individual evolves),
- The *External organisational level* which represents processes linked with the social climate (in which the enterprise evolves),
- The *Natural environment level* which represents processes linked with the evolution of the physical and natural climate.

This system can be qualified as complex because of its nature. This involves several abstraction levels, multiple elements by levels, a large number of relations between elements, a complexity of relations between elements (horizontal exchanges) and between levels (vertical exchanges and transactional exchanges, fig.2).

This architecture shows the need to establish relations between different kinds of levels in the model:
- The technical level, often qualified as a closed system (identified limits, causality relations and interactions relatively identifiable),
- The Human/Organisational level, often qualified as an open system (difficulties to determine limits, in permanent change, being adaptive and iterative).

Thus, this kind of system can be qualified as being quasi-isolated (it is influenced by its environment on its inputs and it influences this environment through its outputs) and partially broken down (it can be broken down into subsystems, linked together and with the environment, which are quasi-isolated) (Le Moigne, 1990). As a result, a modelling process is required to standardize the model building.

[4] Accidental Risk Assessment Methodology for IndustrieS in the context of the Seveso II directive.

[5] System-Action-Management.

Specificities of the global risk analysis

In a general way, an expert (or a working group) has to meet various needs to fulfil a risk analysis (fig.3).

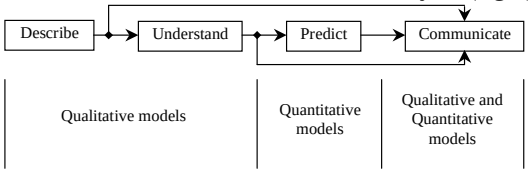

Fig.3. Needs met by the risk analysis

This scheme shows that the quantitative model is only needed in the predict step. This step is helpful for the decision-making because it allows, by studying the system evolving, the comparison of several strategies. But the prediction can be done only if the system operating has been previously described and understood (in order to represent influential factors). And finally the communication of results (or ideas) can be done after each step according to required objectives (Duval, *et al.*, 2006).

The main steps of a global risk analysis are described in fig.4.

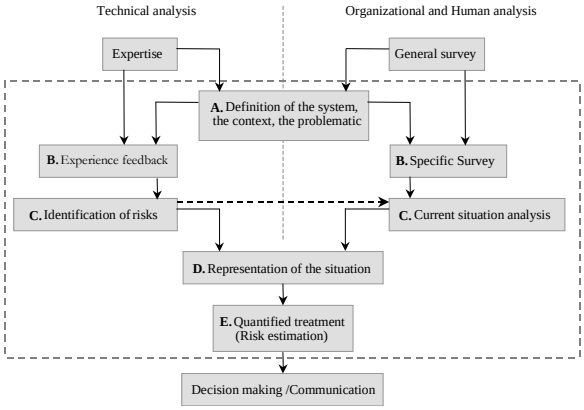

Fig.4. Steps of a global risk analysis in a perspective of decision-making support

This kind of analysis is composed of the aggregation of the technical analysis in one hand and the organisational/human analysis in other hand. Some similarities between these analyses can also be underlined:

- The *expertise* is considered as a source of data, often qualitative, and sometimes quantitative (Lannoy, Procaccia, 2001). In the organizational and human analysis, the *general survey* is a matter of listing human and organisational analyses of accidents, incidents, crises in any domains in order to build up a library of known cases.
- The *definition of the system* consists of an identification of variables, a definition of the level of detail and a definition of system limits.
- The *experience feedback* (EF) is a process including methods and procedures to draw lessons from known accidents and incidents so that they do not reappear. The *specific survey* is a matter of selecting among cases identified in the *generic survey* those which are most similar with the analysed situation.
- The *identification of risks* consists of determining influence links between significant variables of the technical system. The *current situation analysis* allows to determine influence links between significant variables of the human and organisational system.
- The *representation of the situation* is the step in which the qualitative model is built.
- The *quantified treatment* is the step of risk estimation. Two kinds of data are used: probabilities (for data with EF) and experts' judgments (for the others).
- The *decision-making* is the step in which risks are classified and different measures are proposed, and this information is presented to decision makers.

4. MODEL STRUCTURE

In this section the content of each abstraction level defined in the model is depicted (fig.2) and a formalisation of barriers integration is presented.

Conceptual diagram

The conceptual diagram proposed in fig.2 shows that the organisational level (internal and external) does not have a direct influence on the technical level because this level needs the intervention of the human resource to apply organisational changes.

The technical level. In this level, the approach to built a 'bow-tie' is composed of three steps: (1) a functional analysis is done to gather equipments by function, then (2) a dysfunctional analysis is carried out (an FMEA[6] is done to identify relevant failure modes of each material in order to determine their causes and effects on global performances) and (3) a list of sensitive components is established (from the previous FMEA, experts' judgments and experience feedback).

The decisions and actions level. This level characterise a confidence degree of specific human actions. Thus, a human action may be considered as a safety barrier, or an actor of this barrier (i.e. having a direct influence), or an initiator of this barrier (i.e. having an indirect influence). The objective is not to describe human behaviours in all situations implied by the system operating (ergonomics), nor to characterise all situations in which the human action is faulty (human reliability).

The organisational level (internal and external). The modelling approach of this level is dysfunctional because considering the good operating of this dimension needs to define a lot of variables which may limit data aggregation. It is based on Dien, *et al.* (2004) which depict the organisation in a global way and represent it by organisational factors[7] and associated indicators[8].

[6] Failure Modes and Effects Analysis.

[7] An organisational factor appearing in the occurrence of an accident will be described as 'pathogenic'. It results of the aggregation of convergent signs which allow the characterisation of an unfavourable influence in the occurrence of an accident.

[8] They are signs and elements characterising the situation (symptomatic of the presence of such a factor).

The natural environment level. It is composed of physical phenomena which affect the technical system (weather data, geographical implantation …).

The barriers integration

The conceptual diagram, depicted in fig.2, does not allow a clear representation of possible impacts of a barrier on system elements (specifically for human and organisational ones). In this objective, the study is focused on the integration of these safety barriers in the model.

Definitions. A safety barrier can be defined as an entity installed in the system to prevent the occurrence of a risky scenario. This barrier could be, according to its position in the scenario, a preventive or a protective one:
- A preventive barrier is located upstream of the critical event (it prevents or limits the critical event occurrence),
- A protective barrier is located downstream of the critical event (it reduces consequences of this event).

But according to resources it involves, a safety barrier can also be classified into one of the three following categories:
- The organisational barrier, composed of a management activity (regular follow-up of operator trainings according to activities fulfilled),
- The human barrier, composed of a human activity (visual monitoring of a technical process),
- The technical barrier, composed of a safety device or an instrumented system of safety (safety valve, sensor …).

A fourth category can also be defined: combined barriers. This type of barriers involves different sort of resources. Three kinds of combined barriers can be distinguished:
- the T-H barrier, with T for technical resources involved and H for human one (alarm in control room and associated actions done by operators in the workshop).
- the H-O barrier, with O for organisational resources involved (the realisation of a procedure with a regular control of the management: statement of temperatures in a warehouse and reports given to the HSE[9] director).
- the T-H-O barrier: the realisation of a procedure combining technical and human intervention with a regular control of the management (maintenance actions of technical equipments with control of directors in case of sensitive equipment replacements).

In this configuration, we cannot have a T-O barrier, indeed the human resource is necessary to achieve decisions taken by the management.

The formalisation of the barriers integration is then composed of four steps:
- Step 1: The modelling of the system (fig.2),
- Step 2: The identification of operating barriers and the new ones that could be established,
- Step 3: The classification of these barriers according to resources they involve,
- Step 4: The integration of their influences on the system (fig. 5).

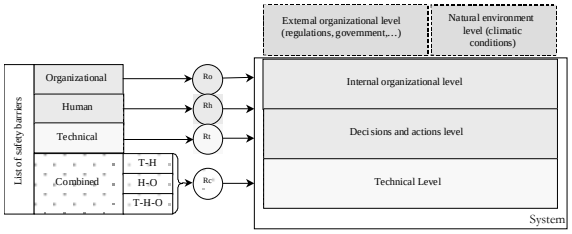

Fig.5. The integration of barriers in the model

The selection of one barrier defined in the list activates, at least, one of the three following variables (fig. 5):
- Ro, representing the realisation of an organisational safety barrier,
- Rh, representing the realisation of a human one,
- Rt, representing the realisation of a technical one,
- Rc, representing a combination of the three previous variables (Ro+Rh or Rh+Rt or Ro+Rh+Rt).

The definition of these variables allows an explicit representation of a barrier impact on the system.

5. BAYESIAN NETWORK MODEL

In this section, the justification of the modelling tool is done and then a generic modelling structure allowing the barriers integration is proposed.

Why Bayesian networks are used?

Many tools can be used to build the risk analysis model and the choice of an adapted one depends of aims sought by users (Villemeur, 1992).

A comparative study (relating to tree-based methods, network/graph-based methods, experts systems and fuzzy logic) was achieved to help the choice of an adapted tool.
According to its generic specificities, which allow the use of qualitative and/or quantitative models, Bayesian networks seem to be an adapted tool for this modelling problematic.
Concerning the technical level, Bayesian networks are a generalisation of trees formalism (thus, methods like fault trees, event trees … can be easily translated into Bayesian networks) (Bobbio, *et al.*, 2001). This formalism allows, for this abstraction level, the representation of system reconfigurations (they are a way of specifying a Markov chain) (Weber and Jouffe, 2003), the treatment of partially correlated failures (in opposition with fault trees which consider common causes failures, thus completely correlated failures), and the modelling and propagation of uncertainties in the model from initiators to output indicators (Weber and Jouffe, 2006).
Concerning organisational/human levels, they allow correlations between variables, the gathering and/or merging of various kinds of knowledge (experience feedback, experts' judgments), the structured

[9] Hygiene, Safety, Environment.

modelling of different abstraction levels (object oriented Bayesian networks) (Weber and Jouffe, 2006), and the use of multi-modal variables.
But two limitations can be underlined:
- the limit of the graphical model compared to the reality, and more specifically for human and organisational levels (which are generally presented in a textual form),
- the transposition of the qualitative model (the causal graph) to the quantitative model (the probabilistic representation).

However, it is necessary to exceed these limits to carry out a quantitative analysis in a decision-making objective.

Generic modelling structure

As described in part 2.2, a barrier is directly integrated in the scenario. But when the modelling tool is used, the representation becomes somewhat different. Indeed, in the Bayesian network, the barrier is integrated as a parent of the event it protects/prevents.

As defined in the Sam approach (Paté-Cornell and Murphy, 1996) and according to the part 3.1, the direction of influence goes from management to actors and then to the technical system (from the top to the down).
Moreover, ARAMIS principles request the independence of barrier components and control systems (for instance: redundancy barriers) in one hand, and other safety functions in other hand.
This implies that a safety barrier implementation (Ro, Rh, Rt) cannot impact directly another safety barrier implementation.
But this implementation needs some resources, which can be unavailable for another barrier implementation (in the case of an indirect influence, and particularly at decisions and actions, and organisational levels).
So, two kinds of generic configurations can be defined:
- The direct impact (fig.6): the barrier impacts directly the system and only it (elements in the same abstraction level than the concerned barrier).
- The indirect impact (fig.7a and fig.7b): the barrier impacts directly the system and indirectly other barriers implementation (elements in the same abstraction level or in an inferior one than the concerned barrier).

In this formalisation, a combined barrier is a specific case of direct and indirect impacts (fig.7c).

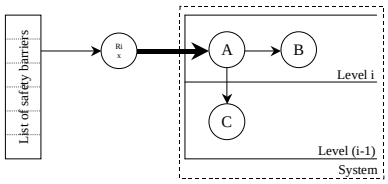

Fig.6. Direct impact

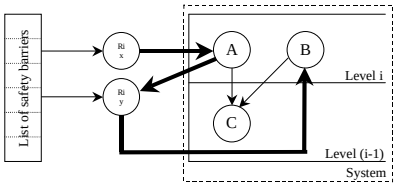

Fig.7a. Indirect impact (in the same abstraction level, x and y belong to the same level)

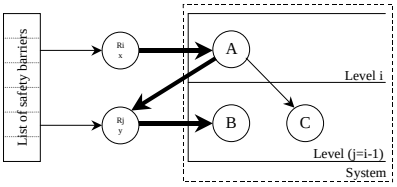

Fig.7b. Indirect impact (between different abstraction levels, x belongs to the level i and y belongs to the level j=i-1)

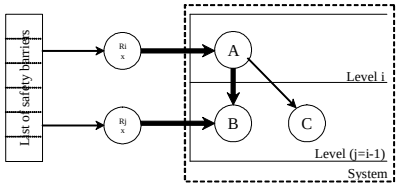

Fig.7c. Direct and indirect impact (in the specific case of a combined barrier)

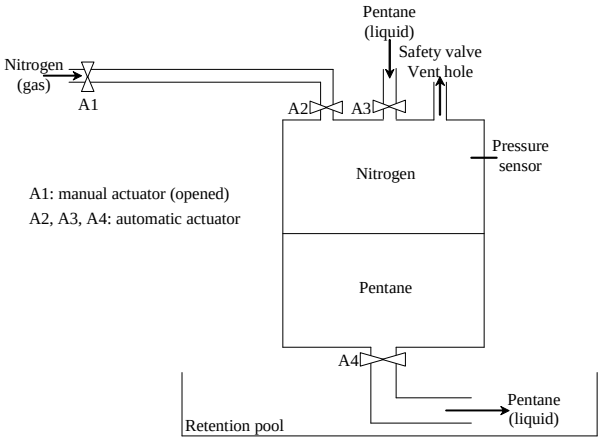

Fig.8. Storage tank

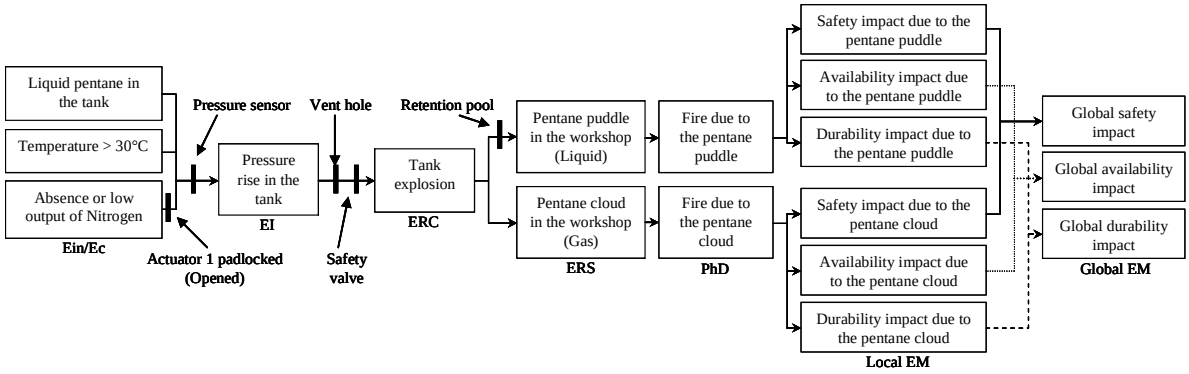

Fig.9. 'Bow-tie' of the tank explosion scenario (technical level)

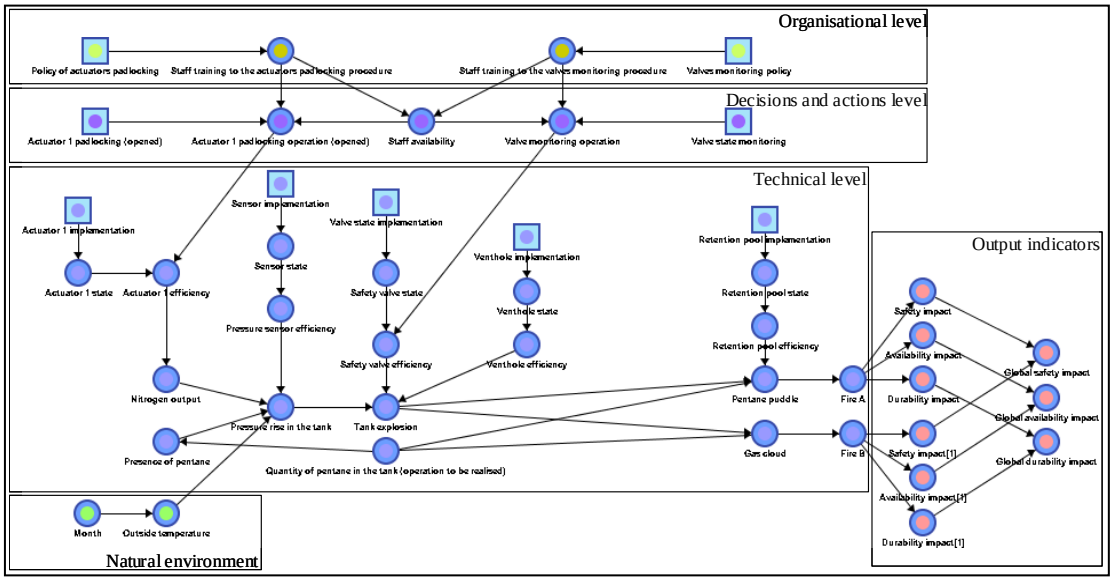

Fig.10. Bayesian network of the tank explosion scenario (global analysis)

6. APPLICATION

System Characteristics

The studied system (fig.8) consists of a transitional storage tank (the product, liquid pentane, is stored in the tank during a short period, from 30 minutes to 2 hours). This product is extremely flammable in air (its boiling point is 36°C). Thus, the storage operation is made in presence of gaseous nitrogen which prevent any reaction with air (ignition for example).
Different safety components are installed: a manual actuator (A1), a vent hole (for little pressure rises), a safety valve (for important pressure rises), a pressure sensor and a retention pool.
Two components need a regular and specific control: the actuator 1 and the safety valve.
These controls need human resources and specific formations (organised and implemented by the management):

- The actuator 1 has to remain open (to insure an optimal pentane output). The proposed solution is a padlocking and a regular follow-up (actions schedule).
- The safety valve has to be operational in case of important pressure rise. The proposed solution is a regular control of the good operating of this component.

The studied scenario is the risk of pressure rise in the tank which can lead to the tank explosion (and this event can produce a fire in the workshop). The proposed context is:

- a temperature upper than 30°C (in summer),
- liquid pentane in the tank,
- insufficient quantity of nitrogen in the tank.

In this context, the liquid pentane changes into gaseous pentane. This leads to a pressure rise in the tank which is evacuated by the vent hole and the safety valve (in a good operating).

The scenario modelling

The global risk analysis of this scenario needs several steps to be achieved. The first one consists of the technical analysis (thus the 'bow-tie' building). The second one consists of the 'decisions and actions' and 'organisational' variables identification (related to the barriers integration). And the last one consists of the Bayesian network building.

The 'bow-tie' building step (fig.9) allowed:

- The identification of the preventive barriers (actuator 1, pressure sensor, vent hole, safety valve) and the protective one (retention pool).
- The identification of two secondary dreaded events (a liquid pentane emission and/or a gaseous one). Thus, it implies different local impacts on output indicators (safety: human and environment, availability: productivity and durability: production material).

But this analysis does not allow the comprehension of staff and management influences on the barrier operating and on the scenario occurrence.
For this, it is necessary to define influential actions (which can be effective only if they have been accepted by the management and the staff):

- Concerning the organisational level, the management has to implement staff trainings to manual actuators padlocking and to safety valve monitoring procedures.
- Concerning the decisions and actions level, the staff has to achieve specific actions (actuator padlocking and valve monitoring) and these actions require availability.

Thus, in the Bayesian network (fig.10), barriers effectiveness is, at least, related to the physical state of the component (itself depending on the component implementation in the system, Rt). If the considered barrier is a combined one, it is also related to the operation fulfilment by the staff (itself depending on the staff decision acceptance, Rh) and indirectly to its training for the concerned procedure (itself depending on the management decision acceptance, Ro).
Concerning the probabilities tables quantification, it is necessary to carry out a combinatory logic analysis in one hand and an experience feedback analysis in

other hand (with the use of experts' judgments and databases).

Results analysis

In the first case, there is no preventive barriers implemented in the system (at the technical level), the considered month is august (thus the critical temperature risk is increased) and the quantity of pentane in the tank is important. In this context, the tank explosion can occur with a probability of 72%. The technical implementation of all preventive barriers allows to reduce the probability occurrence of the critical event to 0.67%.

If now, the tank explosion has occurred (all the preventive barriers were down), the protective barrier operating can be studied:

Global impact	*Retention pool implementation*	*Quantity of pentane*		
		Imp.	Med.	Lit.
Safety (%)	No	36.44	18.65	5.69
	Yes	23.53	12.23	3.45
Availability (%)	No	36.71	15.20	3.20
	Yes	20.44	7.61	0.90
Durability (%)	No	33.87	14.27	3.20
	Yes	18.09	6.90	0.90

In the second case, only the pressure valve is considered (all of other barriers are not implemented), the considered month is august and the quantity of pentane is important. Thus, this configuration allows the staff and management influences appraisal on the system and on the considered barrier efficiency:

	Valve implementation		
	Technical	*Technical + Decisions & actions*	*Technical + Decisions & actions + Organisational*
Barrier efficiency	87.88%	92.72%	96.64%
Tank explosion	9.36%	5.91%	3.12%
Staff training	40% (a) 10% (b) 50% (c)	40% (a) 10% (b) 50% (c)	80% (a) 20% (b) 0% (c)
Monitoring action (d)	43.85%	68.28%	88.06%

(a) for 'present and controlled', (b) for 'present but uncontrolled', (c) for 'absent' and (d) for 'realised'.

7. CONCLUSIONS

In this article an architecture allowing to structure the knowledge for a global risk analysis was defined and a method for the integration of safety barriers in an objective of decision-making was proposed.
The first point allowed to justify the need of a global risk analysis for hazardous installations, to propose a method to carry out this analysis, to determine different levels (and their components) that have to be considered in such an analysis and to justify the use of Bayesian networks in this context.

The second one allowed a generic modelling of the barrier integration (fitting a great number of applications) and a clear visualisation of safety barriers impacts.
But some points need to be studied more precisely:
- The modelling of decisions and actions and organisational levels (which degree of preciseness can we define? Is a probability quantification possible? …).
- The propagation of uncertainties (any risk analysis is subjected to measures and models uncertainties).
- The dynamic evolution of the system, …

REFERENCES

Andersen, H., J. Casal, A. Dandrieux, B. Debray, V. de Dianous, N.J. Duijm, C. Delvosalle, C. Fievez, L. Goossens, R.T. Gowland, A.J. Hale, D. Hourtolou, B. Mazzarotta, A. Pipart, E. Planas, F. Prats, O. Salvi and J. Tixier (2004). *ARAMIS User Guide*, http://aramis.jrc.it.

Bobbio, A., L. Portinale, M. Minichino, E. Ciancamerla. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety*, **71**, 249-260, Elsevier Science.

Caib (2003). *Columbia Accident Investigation Board*, Report volume 1.

Cullen (2001a). *The Ladbroke Grove Rail Inquiry*, Part I report. HSE books.

Cullen (2001b). *The Ladbroke Grove Rail Inquiry*, Part II report. HSE books.

Deleuze, G. (2005). Document associated to the MERIT training (Management of the industrial and technological risks). *ITECH (institute of technologies transfer)*.

Dien, Y., M. Llory and R. Montmayeul (2004). Organisational accidents investigation methodology and lessons learned. *Journal of Hazardous Materials*, **111**, pp. 147-153, Elsevier Science.

Duval, C., A. Léger, H. Bertin and R. Farret (2006). Choice of a risk analysis method for a complex socio-technical system. *15th congress on risks expertise and dependability*.

Gouriveau, R. (2003). *Analyse des risques-Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision.* Doctoral thesis of INP Toulouse.

ISO 14121 (1999). Safety of machinery-Principles of risk assessment. *International Organisation for standardisation*. First edition.

J0 175 (2003). *Law n° 2003-699 concerning the prevention of technological and natural risks, and to the repair of damage*. Official Journal of July 30, 2003.

Lannoy, A. and H. Procaccia (2001). *L'utilisation du jugement d'expert en sûreté de fonctionnement.* Tec & Doc editions.

Le Moigne, J.L. (1990). *La modélisation des systèmes complexes*, Dunod editions.

Paté-Cornell, M.E. and D.M. Murphy (1996). Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. *Reliability Engineering and System Safety*, **53**, 115-126, Elsevier Science.

Villemeur, A. (1992). *Reliability, availability, maintainability and safety assessment, Volume 1: Methods and Techniques*, Wiley and sons editions.

Weber, P., L. Jouffe (2003). Reliability modelling with dynamic Bayesian networks, *in 5th IFAC Symposium SAFEPROCESS'03*, 57-62.

Weber, P., L. Jouffe (2006). Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN), *Reliability Engineering and System Safety*, **91**, 149-162.