Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

A safety barriers-based approach for the risk analysis of socio-technical systems

A. Léger*. R. Farret¯. C. Duval°. E. Levrat*. P. Weber*. B. Iung*

* CRAN – Nancy-University – CNRS UMR 7039 – Faculty of Sciences – Boulevard des Aiguillettes – BP 239 – 54506 Vandoeuvre lès Nancy (e-mail: aurelie.leger@cran.uhp-nancy.fr, eric.levrat@cran.uhp-nancy.fr, philippe.weber@esstin.uhp-nancy.fr, benoit.iung@cran.uhp-nancy.fr)

¯ INERIS, Accidental Risks Division, Parc technologique ALATA – BP 2 – 60550 Verneuil en Halatte, France (e-mail: regis.farret@ineris.fr)

° EDF R&D, Industrial Risk Management Department, 1 avenue du Général de Gaulle – 92141 Clamart Cedex, France (e-mail: carole.duval@edf.fr)

Abstract: Usually, an efficient interaction between different resources of an industrial system (technical, human and organizational) leads to an efficient operation of this system. If this interaction is too weak due to missing or failing resources, the system can evolve to inoperative or risky situations, which can be hazardous for critical systems (as nuclear power plants and chemical processes). Thus methodologies are needed to support risk analysis by integrating together these system dimensions. Nevertheless few existing methodologies are able to perform this task and are mainly dedicated to partial or specific application domains. To face this gap, the paper presents a new methodology based on a system knowledge unification and its structuring in order to quantitatively estimate risks. Then the proposed approach integrates explicitly safety barriers, considered as key parts for risks prevention, and modeled by means of Bayesian networks. Finally a barrier example is depicted in the paper to highlight the feasibility of the methodology.

1. INTRODUCTION

Each industrial system has to manage risks, resulting from "the association of cause and consequence events characteristics of a given situation" (Gouriveau, 2004), and more specifically for critical systems (as for classified installations addressed in the SEVESO II directive). This management needs an adequate risk analysis, composed of a dangerous phenomena identification allowing a risk estimation (ISO 14121, 1999). Current developments on this subject are largely shared for the technical dimension of the system (Villemeur, 1992), but for the human dimension and more recently the organizational one (Le Coze, 2005), it is more partial. Furthermore several major accident analyses, such as the Columbia crash in 2003 (CAIB, 2003), have revealed deep causes (beyond technological failures) coming from organizational and human dimensions. In addition the database MARS (Nivolianitou *et al.*, 2006), listing major accidents which have occurred in the European Union, indicated (in 1998) that 64% of declared accidents implied human (11%) and organizational causes (53%) beyond immediate technological ones. Consequently, an integration of these aspects in a global approach is considered to be helpful to study risks under various points of view in an integrated way (i.e. in a same model). This problematic needs a knowledge unification, which has already been partially developed: qualitatively in (Svedung and Rasmussen, 2002), focused on learning processes in (Chevreau *et al.*, 2003), for the French railroad company in (Delmotte, 2003) and for chemical systems in (Papazoglou *et al.*, 2003). Considering unification concepts developed in these works, a methodology for the risk analysis of socio-technical systems is proposed in this paper. This research results from PhD thesis developments achieved in collaboration with a research and development center of the French Electricity Board nuclear branch (EDF) and the French National Institute for Industrial Environment and Risks (INERIS). This methodology should allow a probabilistic estimation of risky scenarios occurrence and safety barriers impacts (on the system and on its performances). Indeed, safety barriers are considered as key elements in the risks prevention field because of their critical position in the system operation (as it has been developed for the nuclear field with the "Defense-In-Depth" concept (INSAG, 1996)). Then human and organizational changes could be studied through these safety elements to identify and anticipate critical situations. The proposition of a probabilistic approach is possible by using Bayesian networks, which allow the merging of different kinds of knowledge (deterministic and probabilistic ones) in a same model. To highlight the interest and the development of the proposed methodology, the paper is structured as follows: principal stages of the methodology are defined in section 2, specificities of each dimension developed in this approach are described in section 3, a focus on safety barriers modeling is presented in section 4 and applied on an academic example in section 5. Finally, the last section gives some concluding remarks and perspectives.

2. METHODOLOGY STAGES

The aim of this research work is to propose a methodology for the risk analysis of socio-technical systems that consider the system as a whole (Von Bertalanffy, 1968) and in which different kinds of actors (technical, human, organizational, societal and environmental) have an influence (Transversal Risk Analysis in Fig.1). To address this kind of analysis in a

978-1-1234-7890-2/08/$20.00 © 2008 IFAC

10.3182/20080706-5-KR-1001.2413

convenient way, a knowledge extraction and its unification are needed. The first point defines which methods can be used for collecting information in each dimension and the second one, how to represent and organize this information in order to build and use the model to study different risky scenarios (Risk model construction in Fig.1). A risky scenario can be prevented by means of safety barriers. Thus it is essential to study these system component operations in order to anticipate safety problems. It is the reason why safety barriers are considered as key parts in the proposed methodology (Generic barrier models and Estimation of barriers effectiveness in Fig.1). A modeling tool is needed to support the methodology (a justification of the choice of Bayesian networks is given in (Léger *et al.*, 2006)), and some industrial applications are being carried out to validate it (Bayesian networks and Industrial scenarios in Fig.1).

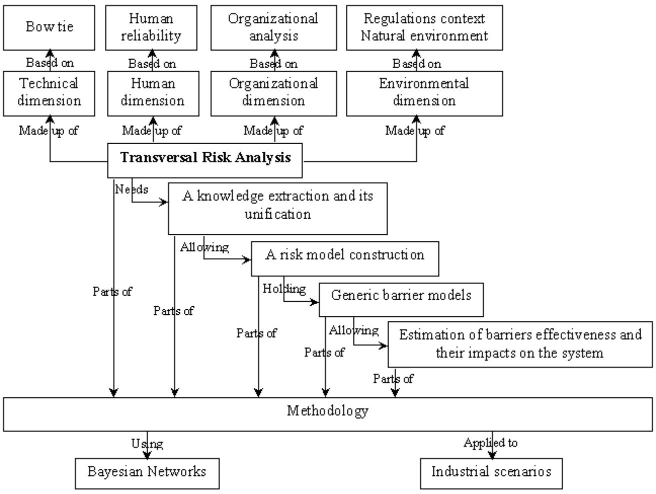

Fig.1: Methodological approach

3. APPROACH PRINCIPLES

The first point of our methodology consists in defining a frame (section 3.1) in which different dimensions are considered. This frame allows system characteristic descriptions, leading to the choice of adequate estimating and modeling methods (section 3.2).

3.1 Conceptual frame

Our conceptual frame (Fig.2) is based on those developed in the SAM approach (Paté-Cornell and Murphy, 1996) which considers that the organization influences human actions and, through these actions, the technical system operation (Fig.3).

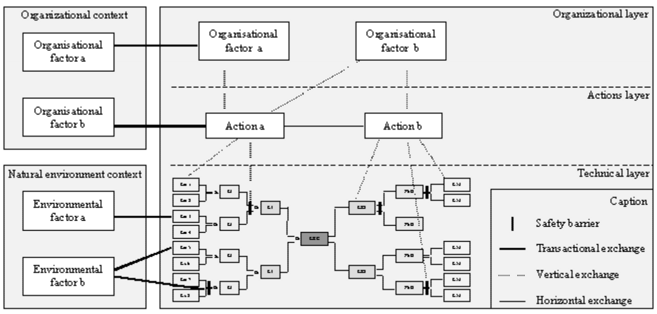

Fig.2: Conceptual frame

In our approach, the system is broken down into three representative layers interacting through horizontal and vertical exchanges (Fig.2): the technical layer, the human one and the organizational one. This system is then influenced, through transactional exchanges (Fig.2), by external constraints: the organizational and the natural environment contexts ((Léger *et al.*, 2006), (Duval *et al.*, 2007)).

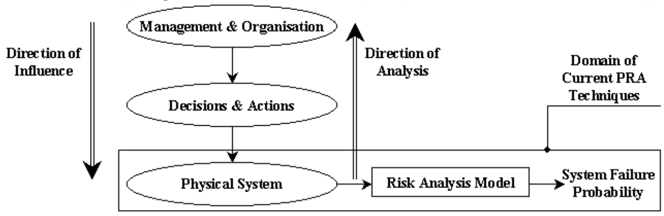

Fig.3: Structure of human and management effects on risk

This distinction has been made because system variables have different characteristics than contextual variables. Indeed, the first ones can be controlled, while the second ones influence the system but are undergone.

3.2 System dimensions

Technical dimension

The technical analysis is performed by using the "bow-tie" method (in the technical layer of Fig.2) developed in the European project ARAMIS (Andersen *et al.*, 2004). A bow-tie is composed of a fault tree and an event tree in which 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.

Human dimension

This layer characterizes the effectiveness of specific human actions, defined as the extent to which actual performances reach targeted ones. These actions are gathered into two categories: the "control actions" category, defining actions (supervision, diagnosis, …) which allows the system to continue in its operational conditions; and the "maintenance actions" category, defining the combination of all technical, administrative and managerial actions during the life cycle of an item intended to retain it in (or restore it to) a state in which it can perform the required function (EN 13306, 2001). Then in this dimension, the approach is focused on the collective behavior (and not on the individual one).

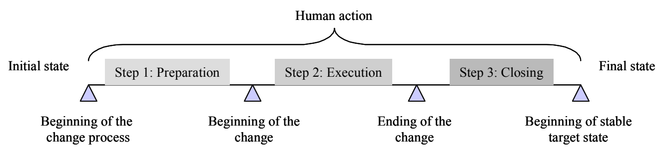

Fig.4: Change process representation

Each action can be seen as a local organizational change inspired by (Lewin, 1951) and depicted in Fig.4, and then divided into three generic steps: the Preparation step (enabling the planning, the specification and the characterization of all required conditions to the proper execution of an intervention), the Execution step (implementing this intervention in the system operation) and the Closing step (strengthening which ensures the proper integration of this intervention and confirms its continuity).

The proposed decomposition (Fig.4) allows a knowledge structuring and can be helpful during and after interviews to control the collection of information and organize this information.

Each action is characterized by indicators that impact its effectiveness. These indicators are specific of an action step and organized as follows: (1) delegation, (2) aids and (3) training for the Preparation step; (4) experience, (5) respect of work specifications, (6) contextual factors and (7) collective management and group dynamic for the Execution step, (8) real time control and (9) feedback experience for the Closing step. These indicators, established from our field knowledge, are characteristics of an action and have to be defined for each of them through interviews focused on their courses. This list aims at being exhaustive, but can be completed in specific contexts.

Organizational dimension

The modeling approach of this layer is focused on a global pathogenic view. It is based on (Pierlot *et al.,* 2007) depicting the organization in a global way and describing it by pathogenic organizational factors (because occurring in an accident). These factors are: (1) shortcomings in the organization culture of safety, (2) failure in daily safety management, (3) weakness of control bodies, (4) poor handling of organizational complexity, (5) difficulty in implementing feedback experience, (6) production pressures and (7) no re-examining of the design hypotheses. Such factors contribute to affect safety and to cause or precipitate the accident. They result of the aggregation of convergent signs that allow the characterization of a negative influence in the accident occurrence. Therefore from an organizational perspective, it constitutes a common cause failure (it summarizes a series of phenomena, processes, and effects on the organizational structure). They can be used to sum up a detailed description of events or to guide an investigation in an organizational structure in order to establish a diagnosis of overall (or partial) safety. Thus they have to be defined once for the studied system through an organizational diagnosis.

In the same way, the context dimensions (organizational and natural environment ones) will be described, analyzed and modeled in this methodology but not detailed in this paper. The organizational context represents processes linked with the situation in which the system evolves (social, regulations, competition), whereas the natural environment one represents processes linked with the evolution of the physical and natural climate (weather data, geographical implantation).

4. BARRIER MODELS

As defined in section 2, safety barriers have to be specifically studied because of their importance for the system safety. Indeed, human (indicators) and organizational (pathogenic factors) impacts on the technical (bow-tie) system dimension are studied through a modeling of safety barriers operation. To be able to propose an adequate modeling of these barriers according to our issues (sections 4.2 and 4.3), it is required to define their characteristics and propose a classification (section 4.1).

4.1 Classification

A classification has been proposed in (Léger *et al.*, 2006) based on barrier types (preventive or protective) and involved resources (technical, human and/or organizational). Further points are specified below.

A safety barrier can be composed of a Safety Instrumented System (SIS) or a Safety Device (SD, active or passive). Based on SIS ((IEC 61508, 2000), (IEC 61511, 2004)), a safety barrier can be broken down into three elements: a detection stage enabling a processing stage and then an action stage. In this approach, SD barriers are considered as a particularization of SIS ones (because it consists of one element, this point is studied in section 4.3). These different stages can be achieved through technical components and/or operators (Forest *et al.*, 2007).

A technical Detection consists of equipments, which convert a measure (temperature, pressure, flow) in another one, often electric (voltage, current, resistance), that can be directly used for the measurement or the control. A human Detection consists of getting one or more pieces of information allowing a failure identification (or detection), relieved (or not) by a technical device. The operator can be more or less active in this detection.

A technical Processing can consist of acquiring a measure by a sensor and displaying it, or activating a control of one or more actuators from a combinative function of sensors information. A human Processing consists of making a diagnosis from detection stage information and selecting the adequate security action.

A technical Action consists of equipments which convert a signal (electric or pneumatic) into a physical phenomenon, allowing it to control a pump moving off, a valve closing or its opening. A human Action consists of a manual action relieved (or not) by a technical device, countering the critical scenario.

4.2 Generic models

In our approach, a barrier can prevent a scenario occurrence if it is available. This availability is defined as the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or during a given time interval, assuming that the required external resources are provided (EN 13306, 2001). It is function of intrinsic data (which is purely technical and represented by manufacturer's data) and contextual ones (which represent human and organizational influences on this intrinsic data). In order to consider these correlated data in a probabilistic way, it is proposed to use the Bayesian network (which is an appropriate tool for the proposed risk model then for the safety barriers modeling (Léger *et al.*, 2006)).

As proposed in section 4.1, a barrier can be broken down into its technical components, in the same way its availability is broken down into "Detection Availability" (DA, scheme A in Fig.5), "Processing Availability" (PA) and "Action Availability" (AA) for SIS barriers type, or into "Technical Component availability" (TC, scheme B in Fig.5) for SD barriers type. These variables are modeled with Bayesian networks as described in (Weber and Jouffe, 2006) and are objects (holding an encapsulated Bayesian network, depicted in Fig.6 and Fig.7).

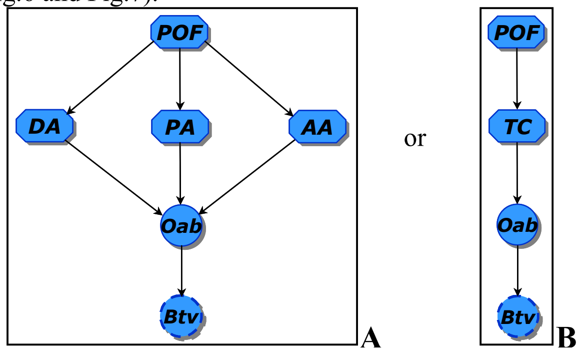

Fig.5: Global models for SIS (scheme A) and SD (scheme B) barrier types

In these models, variables have the following meanings: (POF) "Pathogenic Organizational Factors" which is an object depicting organizational factors states (presented in section 3.2), (Oab) "Operational availability of barrier" aggregates availabilities of its different components (DA, PA and AA, or TC in Fig.5) and (Btv) "Bow-tie variable" depicts an event, occurring in the scenario, prevented by a proper barrier operation.

Considering definitions given in the section 3.2 for maintenance and control actions classes, two kinds of impacts can be specified for each barrier component (Fig.6): an indirect impact (MAI, Mae), characterizing a maintenance action influence on the component (initial) availability (IA); and a direct impact (CAI, Cae), characterizing a control action influence on this component (operational) availability (OA).

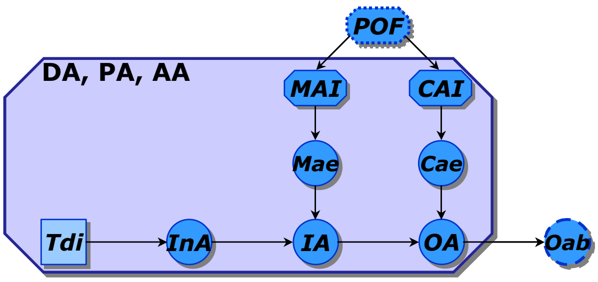

Fig.6: Model of a generic barrier component

In this model (Fig.6), variables have the following meanings: (Tdi) "Technical device installation" is a decision variable (without probabilities) modeling the physical presence of the component; (InA) "Intrinsic availability" describes manufacturer's availability considering its physical presence; (IA) "Initial availability" describes the component availability considering its intrinsic availability and specific maintenance action effectiveness; (OA) "Operational availability" describes the component availability considering its initial availability and specific control action effectiveness; (Mae, Cae) "Maintenance action effectiveness" and "Control action effectiveness" represent the probability of an action to be properly carried out considering the human (MAI, for Maintenance Action Indicators and CAI, for Control Action Indicators) and organizational (POF) contexts (in that way, a method for modeling these dimensions is proposed in (Léger *et al.*, 2008)).

Variables depicted in Fig.5, Fig.6 and Fig.7 have following modalities: "Present" and "Absent" for the variable Tdi; "Available", "Unavailable" and "Absent" for variables InA, IA, OA and Oab; "Effective" and "Ineffective" for variables Mae and Cae. Modalities of the variable Btv depend on the studied event (considered, in this paper, as a Boolean variable). Then associated Conditional Probability Tables (CPT) are defined below.

The "Oab" CPT (Fig.5) is defined by the following logical function: this variable is available if all of its components are also available, it is absent if one or more of its components are absent, and unavailable in the other cases.

The "InA" CPT (Fig.6) is depicted in Table 1.

Table 1: "Intrinsic availability" CPT

Technical device installation	Intrinsic Availability		
	Available	Unavailable	Absent
Present	x_1	$1-x_1$	0
Absent	0	0	1

$x_1 \in [0,1]$, depicts the manufacturer's availability.

The "Mae" and "Cae" CPT (Fig.6) are functions of human action indicator states (Léger *et al.*, 2008), whose influences on these actions effectiveness should depend on the considered action and component. Indeed human action indicators should not have the same influence on a sensor replacement and on a visual supervision of a valve (in this paper these indicators and organizational factors are considered favorable, i.e. action indicators are effective and the organizational situation is not pathogenic).

The "IA" CPT (Fig.6) is depicted in Table 2.

Table 2: "Initial availability" CPT

Intrinsic Availability	Maintenance Action Effectiveness	Initial Availability		
		Available	Unavailable	Absent
Available	Effective	1	0	0
	Ineffective	α_1	$1-\alpha_1$	0
Unavailable	Effective	$1-\alpha_2$	α_2	0
	Ineffective	0	1	0
Absent	Effective	0	0	1
	Ineffective	0	0	1

α_1 depicts an aggravation factor due to the ineffectiveness of the maintenance action, it decreases the component availability.

α_2 depicts an improvement factor due to the effectiveness of the maintenance action, it increases the component availability.

The "OA" CPT (Fig.6) is depicted in Table 3.

Table 3: "Operational availability" CPT

Initial Availability	Control Action Effectiveness	Operational Availability		
		Available	Unavailable	Absent
Available	Effective	1	0	0
	Ineffective	α_3	$1-\alpha_3$	0
Unavailable	Effective	$1-\alpha_4$	α_4	0
	Ineffective	0	1	0
Absent	Effective	0	0	1
	Ineffective	0	0	1

α_3 depicts an aggravation factor due to the ineffectiveness of the control action, it decreases the component availability.

α_4 depicts an improvement factor due to the effectiveness of the control action, it increases the component availability.

$\alpha_i \in [0,1]$, for $i = \{1,2,3,4\}$, will be established by experts' judgments and thanks to the feedback experience (leading to estimation uncertainties), through a semi-quantitative table (as those used in the application case).

4.3 Partial models

Three partial model types are proposed and classified through involved resources.

The first one is qualified as "Technical" due to the fact that all barrier components are technical devices (Detection, Processing and Action stages for SIS barriers). A human influence is present through the maintenance action for each component (Fig.7). This partial model is a convenient one to depict the variable "TC" for SD barriers type (section 4.1, passive: retention pool, active: safety valve), in which there are no direct human influences.

The second one is qualified as "Human" due to the fact that all technical components are influenced by indirect and direct human actions (Fig.6).

The third one is qualified as "Combined" due to the fact that each barrier component is composed of a technical device influenced (1) only by an indirect human action (Fig.7) or (2) by both indirect and direct human actions (Fig.6).

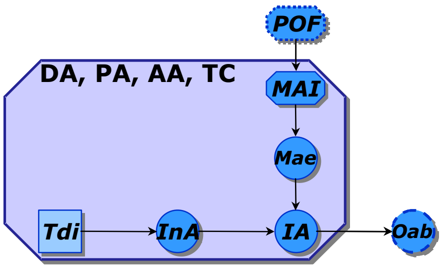

Fig.7: Model of a "technical" barrier component

Concerning SIS barrier types, different combinations can be proposed (Table 4).

Table 4: SIS barrier types

Detection	Processing	Action	Barrier type
Technical component	Technical component	Technical component	Technical
		Human action	Combined
	Human action	Technical component	Combined
		Human action	Combined
Human action	Technical component	Technical component	Not encountered
		Human action	Not encountered
	Human action	Technical component	Combined
		Human action	Human

For example, let us consider a barrier avoiding a tank overfilling:

- a technical barrier can be composed of a level sensor (Detection), an automatic order ("close the valve", Processing) and an automatic valve (Action).
- a human barrier can be composed of a visual supervision of a level (Detection), a human alarm activation (Processing), a manual valve closure (Action).
- a combined barrier can be composed of a level sensor (Technical Detection), an automatic alarm activation (Technical Processing) and a manual valve closure (Human Action).

5. APPLICATION - PARTICULAR MODELS

An example is presented in this section to illustrate previous points. The studied barrier corresponds to the third example presented in the previous section. Its global and component models are instantiations of these presented in Fig.5 (scheme A), Fig.6 and Fig.7.

It is considered that organizational and human contexts (i.e. variables POF, MAI and CAI) are favorable and that all technical devices (variables Tdi) are present in the system, then it allows the studying of maintenance and control action influences on barrier components and global barrier availabilities.

A specific scale for factors estimation has been defined: "No impact": 99%, "Little impact": 95%, "Impact": 75%, "Important Impact": 50%, "Total impact": 1% (sensitivity analyses have to be done to validate these rates, enabling thereafter its generalization).

Concerning the Detection component performance analysis (Table 5), data used to quantify CPT are the following ones: level sensor manufacturer's availability (99%), aggravation and improvement factors relating to the maintenance action state (a level sensor replacement, $\alpha_1 = 0.5$, $\alpha_2 = 0.75$).

Table 5: Level sensor operational availability

Level sensor presence	Level sensor replacement effectiveness	Level sensor operational availability (%)	
		Available	Unavailable
Present	Effective	99.25	0.75
	Ineffective	49.5	51.5

For the Processing component performance analysis (Table 6), data used to quantify CPT are the following ones: alarm manufacturer's availability (99.5%), aggravation and improvement factors relating to the maintenance action state (an alarm test, $\alpha_1 = 0.75$, $\alpha_2 = 0.95$).

Table 6: Alarm operational availability

Alarm presence	Alarm test effectiveness	Alarm operational availability (%)	
		Available	Unavailable
Present	Effective	99.53	0.47
	Ineffective	74.63	25.37

Concerning the Action component performance analysis (Table 7), data used to quantify CPT are the following ones: valve manufacturer's availability (98%), aggravation and improvement factors relating to the maintenance action state (a valve supervision, $\alpha_1 = 0.95$, $\alpha_2 = 0.95$) and to the control action state (a manual valve closure, $\alpha_3 = 0.01$, $\alpha_4 = 0.50$).

Table 7: Valve operational availability

Valve presence	Valve supervision effectiveness	Valve closure effectiveness	Valve operational availability (%)	
			Available	Unavailable
Present	Effective	Effective	99.98	0.02
		Ineffective	0.98	99.02
	Ineffective	Effective	96.55	3.45
		Ineffective	0.93	99.07

Finally the operational availability of this barrier is depicted in Table 8.

Table 8: "Avoid a tank overfilling" operational availability

Barrier components (Present)	Maintenance action effectiveness	Control action effectiveness	'Avoid a tank overfilling' operational availability (%)	
			Available	Unavailable
Level sensor	Effective	/	97.84	2.16
Alarm	Effective	/		
Valve	Effective	Effective		
Level sensor	Ineffective	/	48.80	51.20
Alarm	Effective	/		
Valve	Effective	Effective		
Level sensor	Effective	/	73.36	26.64
Alarm	Ineffective	/		
Valve	Effective	Effective		
Level sensor	Effective	/	95.37	4.63
Alarm	Effective	/		
Valve	Ineffective	Effective		
Level sensor	Effective	/	0.97	99.03
Alarm	Effective	/		
Valve	Effective	Ineffective		

These observations, Table 8, allow an ordering of actions considering their criticality (negative influence on the global barrier availability if they are ineffective) and this classification is confirmed by local performance analyses (Tables 5, 6 and 7): (1) manual valve closure, (2) sensor replacement, (3) alarm test, and (4) valve supervision. This study can be helpful for decision makers to anticipate critical situations and prioritize human actions and investments. This example points out the fact that influences on barrier components availabilities, then on the global barrier operational availability, are action specific (then action indicators influences on its effectiveness should be action specific).

6. CONCLUSION

The methodology proposed in this paper allows the user to get onto risk analysis of socio-technical systems by stages. Starting from an overall view of the system, and by defining adequate analyses and modeling methods for studied dimensions, it allows a handling of human and organizational impacts through safety barriers. In that way, a modeling method has been proposed to cover the whole barrier classes that can be encountered in these systems. It is focused on the fact that the component availability notion is influenced by some contextual data linked with maintenance and/or control processes. These works lead to conclusions, for which thorough investigations are required. The first one concerns the fact that action indicators are action and component specific. Further works will define influence classes according to these actions and components, modeled through Bayesian networks, which can be specialized on specific analysis. The second one is about the fact that organizational factors influences on human action indicators are indicator specific. Recent works, developed in (Léger *et al.*, 2008), propose a generic configuration using Bayesian networks, which can be particularized on specific organizational context analyses. The third one concerns uncertainties treatment in the proposed risk model. Further works will propose a modeling method, based on Bayesian networks, that would enable an explicit representation of these uncertainties. The last one is about the feasibility study of this methodology. This work is under development, collectively with EDF and INERIS, on an industrial case.

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*.

CAIB (2003). *Columbia Accident Investigation Board, Report Volume 1*. Government Printing Office, Washington, D.C.

Chevreau, F.R., J.L. Wybo and D. Cauchois (2006). Organizing learning processes on risks by using the bow-tie representation. *Journal of hazardous materials*, **130**, 276-283.

Delmotte, F. (2003). *A socio-technical framework for the integration of human and organizational factors in project management and risk analysis*. Master of science, Faculty of the Virginia Polytechnic Institute and State University.

Duval, C., A. Léger, P. Weber, E. Levrat, B. Iung and R. Farret (2007). Choice of a risk analysis method for complex socio-technical systems. *ESREL*, **1**, 17-25.

EN 13306 (2001). Maintenance Terminology. *AFNOR*.

Forest, C., E. Miché, V. De Dianous and S. Chaumette (2007). Probabilistic assessment of potential major industrial accidents: Estimating reliability of safety barriers. *ESREL*, **1**, 27-34.

Gouriveau, R. (2004). Risk Management, Dependability tools and Case-Based Reasoning integration using the object formalism. *Computers in Industry,* **55-3**, 255-267.

IEC 61508 (2000). Functional Safety of electrical/electronic/programmable electronic safety-related systems. *International Electrotechnical Commission*.

IEC 61511 (2004). Functional Safety, Safety instrumented systems for the process industry sector. *International Electrotechnical Commission*.

INSAG (1996). Defence in depth in nuclear safety. *International Nuclear Safety Advisory Group*, INSAG 10, Vienna.

ISO 14121 (1999). Safety of Machinery, Principles of Risk Assessment. *International Organization for Standardization*.

Le Coze, J.C. (2005). Are organisations too complex to be integrated in technical risk assessment and current safety auditing? *Safety Science*, **43-8**, 613-638.

Léger, A., C. Duval, P. Weber, E. Levrat and R. Farret (2006). Risk analysis of complex socio-technical systems by using Bayesian Network modeling. *Workshop on Advanced Control and Diagnosis*.

Léger, A., C. Duval, R. Farret, P. Weber, E. Levrat and B. Iung (2008). Modeling of human and organizational impacts for system risk analyses. *International Probabilistic Safety Assessment and Management Conference*.

Lewin, K. (1951). *Field theory in Social Science*. Ed. D. Cartwright, Harper & Row, New York.

Nivolianitou, Z., M. Konstandinidou and C. Michalis (2006). Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system. *Journal of Hazardous Materials,* **A137**, 1-7.

Papazoglou, I.A., J.L. Bellamy, A.R. Hale, O.N. Aneziris, B.J.M. Ale, J.G. Post and J.I.H. Oh (2003). I-Risk: Development of an integrated technical and management risk methodology for chemical installations. *Journal of Loss Prevention in the Process Industries,* **16-6**, 575-591.

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.

Pierlot, S., Y. Dien and M. Llory (2007). From organizational factors to an organizational diagnosis of the safety. *ESREL*, **2**, 1329-1335.

Svedung, I. and J. Rasmussen (2002). Graphic representation of accident scenarios: mapping system structure and the causation of accidents. *Safety Science*, **40**, 397-417.

Villemeur A. (1992). *Reliability, Availability, Maintainability and Safety Assessment – Volume 1: Methods and Techniques*. Wiley & Sons.

Von Bertalanffy, L. (1968). *General System theory*, G. Braziller, New York.

Weber, P. and L. Jouffe (2006). Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN). *Reliability Engineering & System Safety*, **91-2**, 149-162.