Methodological developments for probabilistic risk analyses of socio-technical systems

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

Methodological developments for probabilistic risk analyses of socio-technical systems

Léger A.*[1], Weber P.*, Levrat E.*, Duval C. °, Farret R.˜, Iung B.*
* CRAN, Nancy-University, CNRS UMR 7039, Faculty of Sciences, Boulevard des Aiguillettes, BP 239, 54506 Vandoeuvre lès Nancy, France
° EDF R&D, Industrial Risk Management Department, 1 avenue du Général de Gaulle, 92141 Clamart Cedex, France
˜ INERIS, Accidental Risks Division, Parc technologique ALATA, BP 2, 60550 Verneuil en Halatte, France

Abstract
Nowadays, the risk analysis of critical systems cannot be focused only on a technical dimension. Indeed last well known accidents in nuclear or aerospace areas underlined initiating causes also related to technical and organisational viewpoints. It led to the development of methods for risk assessment considering three main aspects on the system resources: the technical process, the operator constraining the process, and the organisation constraining human actions on the process. However, only few scientific works tried to federate these methods in a unique and global approach. Thus this paper is focusing on a methodology aiming to achieve the integration of the different methods in order to probabilistically assess the risks. The integration is based on (a) system knowledge structuring and (b) its unified modelling by means of Bayesian Networks supporting also quantification and simulation phases. The methodology is applied to an industrial case to show its feasibility and to conclude on the model relevance for system risk analysis. The results of the methodology can be used by decision makers to prioritise their actions in face with potential or real risks.

Keywords
Risk analysis, Socio-technical systems, Bow-tie method, Human reliability, Organisational factors, Bayesian Networks

Introduction

Risk and more particularly the Accidental Risk is an inherent notion of all operating industrial systems. It is studied from many years and the identification of its causes tends nowadays to a diversification. Indeed, until seventies, the risk studies were centred on technical aspects of systems **[1]**. Then several major accidents, such as the Three Miles Island nuclear accident and the Bhopal catastrophe, have underlined complementary causes addressing operator errors and organisational dysfunctions. These accidents allowed the scientific community to propose, in eighties, first methods centred on the analysis of these human errors. It led to enlarge the Human Reliability Analysis area with methods such as THERP **[2]**, CREAM **[3]**, ATHEANA **[4]** … In addition, in nineties, other accidents (Challenger explosion, Chernobyl nuclear accident …) have emphasised the importance of organisational dysfunctions in accident occurrences. In that way, they contributed to the emergence of different theories for the organisational issue study such as the Normal Accident **[5]** and the High Reliability Organisations **[6]**. One main consequence has been that the risk analysis evolved to cover the whole of these causes (technical, human and organisational). It is particularly true for critical installations (such as nuclear power plants, chemical processes …) for which regulations become more and more drastic according to safety rules. Nevertheless these types of analyses are often difficult to achieve due to the volume of the required resources to be developed and the management hesitation. Therefore the well deployment of such analyses is mandatory correlated with an adapted methodology. This methodology has to propose knowledge structuring, knowledge unification and also demonstrative aspects (for decision makers). Recent scientific works hold this issue but generally in a partial way (i.e. focused on specific system resources) or for specific industrial sectors. It has been demonstrated qualitatively in **[7]**, focused on learning processes in **[8]**, for the French railroad company in **[9]**, for chemical systems in **[10]**, for nuclear power plants in **[11, 12, 13]**, and focused on the workload prediction in **[14]**. To face these gaps, it is proposed to develop a methodology based on

[1] Corresponding author: aurelie.leger@cran.uhp-nancy.fr, aurelie.leger@edf.fr

generic concepts (i.e. not sector-based) with an emphasis on knowledge structuring and unification to handle technical, human and organisational aspects in a same and unique model. This methodology aims to enable a probabilistic estimation of risky scenarios occurrence by considering safety barriers impacts on the system and on its performances. Indeed, safety barriers are defined as key elements in the risks prevention field because they are playing a critical position in the system operation **[15]**. Then human and organisational changes can be studied by means of these safety elements in order to identify and anticipate critical situations. The proposition of a probabilistic approach is done by using Bayesian Networks **[16]**. This modelling tool allows the merging of different kinds of probabilistic knowledge with no Boolean variables and uncertainties propagation in a same model.

This innovative methodology results from collaboration between a research centre (CRAN), a French end-user operating conventional and nuclear power plants (EDF) and the French National Institute for Industrial Environment and Risks (INERIS).

The methodology proposed in the paper is addressing as follows: the section 1 defines methodology phases, principles and characteristics. Subsequently, methods for knowledge collection and extraction are developed for each system dimension. Then the section 2 proposes techniques for system knowledge identification and extraction, leading in section 3 to unify this knowledge by means of Bayesian Networks. The methodology feasibility is illustrated in section 4 with an application on a risky scenario resulting from the operation of a chemical process. Finally some conclusions and perspectives are developed.

1. Methodological approach

Based on systemic principles **[17]**, the proposed methodology is organised with the following phases **[18]**:

- *Definition of system limits*. It consists in specifying the system characteristics and the contextual ones to be studied in this analysis.
- *Knowledge extraction*. It leads to an identification of adequate methods to be used to collect information in each dimension identified in the previous stage.
- *Knowledge unification*. It aims to define a shared representation of these different kinds of information that enables thereafter their aggregation in a risk model.
- *Risk model construction*. It consists in building a model based on the right modelling technique and allowing the studies of risky scenarios. In the proposed approach, different kinds of knowledge should be merged in a same risk model by means of Bayesian Networks.

Considering the key role of safety barriers to prevent risky scenarios occurrence **[19]**, it is also required to model the operation of these system safety components:

- *Definition of barrier models*. It enables to depict a convenient modelling of these safety elements, based on generic and partial models.
- *Estimation of barriers effectiveness and their impacts on the system*. It consists in using the model to simulate scenarios in order to classify risks, to prioritise strategies and investments.

1.1. System dimensions

In the way to well identity the limits of the studied system, it is proposed to define a conceptual framework (Figure 1). This framework enables the characterisation of studied system dimensions and their interactions. It is based on principles developed in **[20]** which specify that “an important feature of this model is that management factors affect the physical system only through human decisions and actions”.

In the proposed framework (Figure 1, **[21]**), the system is broken down into three representative layers and influenced by two contextual layers **[22, 23, 24]**: *the technical layer*, *the actions layer*, *the organisational layer*, *the organisational context* (context in which the system is evolving in relation to factors such as social, regulations, competition), and *the natural environment context* (such as the evolution of the physical and natural climate depending on weather data, geographical implantation …).

These layers interact through three kinds of exchanges defined as follows:

- *Horizontal exchange* - in a same abstraction layer,

- *Vertical exchange* - between two contiguous abstraction layers,
- *Transactional exchange* - between a system abstraction layer and a contextual one (Figure 1).

The transactional exchange is defined because system variables have different characteristics than contextual variables. Indeed, the first ones can be controlled while the second variables influence the system but are undergone.

2. Knowledge collection and extraction

On the basis of the system dimension definition, it is needed to select adequate methods to represent them in a risk analysis objective. Thus, in the scope of risks estimation (step E), an identification of similarities between technical risk analyses (defined in **[53]**) and human/organisational ones (Figure 2) underlines that it is required to define goals to be reached (steps A and B). Then field theories need to be identified to use the adequate methods to collect information (step C) and to propose a shared representation of the studied system (step D). These items are addressed in this section to characterise each system dimension, through a bottom-up approach as depicted in Figure 1.

2.1. The technical dimension

2.1.1. The bow-tie representation

Many methods can be used to study technical failures (FMEA, HAZOP, fault trees, event trees, reliability diagrams …). The choice of one between them depends mainly of the study aims **[1]**. Thus, in this approach, it is proposed to use the bow-tie method (Figure 3 and Table 1, developed in the European project ARAMIS **[25]**). Indeed, the bow-tie method enables the description of an accident scenario occurrence by each path from initiators to final consequences. It is done by graphically aggregating a deductive method through a fault tree and an inductive one through an event tree **[12]**. Moreover for assessing the risk level of events (CE, ME ... in Table 1), this aggregation is achieved in a probabilistic computation. Concerning safety barriers, they are represented by means of vertical bars (Figure 3) in order to materialise an opposition to the accident scenario development. The barrier depiction proposed in this method has to be specified for the global issue considering the study of their operation and impacts on the system.

UE	Undesirable Event	Drift or failure apart from usual conditions of operation, supposed to occur exceptionally
CUE	Current Event	Accepted event that can occur more or less frequently in normal conditions of exploitation
IE	Initiating Event	Direct cause of a loss of containment (LOC, for fluids) or a loss of physical integrity (LPI, for solids)
CE	Critical Event	Represented by a LOC or a LPI
SCE	Secondary Critical Event	Direct consequence of the critical event and at the origin of the accident/incident occurrence
DP	Dangerous Phenomenon	Physical event that can lead to major damages
ME	Major Event	Effect on targets (human beings, structures, environment) issued from the dangerous phenomena

Table 1: Definition of bow-tie variables

2.1.2. The barrier notion

A safety barrier is an entity implemented within the system to avoid the occurrence of a risky scenario by preventing/limiting the critical event occurrence (prevention barrier) or by reducing consequences of this event (protection one) **[22]**. These entities are composed either of a Safety Instrumented System (SIS) or of a Safety Device (SD, active or passive). A SIS is a barrier needing external activation. This barrier type is composed of three sub-systems **[19]** (as defined in **[54]**): Detection (sensors), Processing (logic solvers), and Action (final elements). These sub-systems can be composed of technical components and/or operators (Table 2).

Technical component	Detection	It consists of equipment, which converts a measure (temperature, pressure, flow) in another one, often electric (voltage, current, resistance), that can be directly used for the measurement or the control.
	Processing	It 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.
	Action	It consists of equipment, which converts a signal (electric or pneumatic) into a physical phenomenon, allowing it to control a pump moving off, a valve closing or its opening.
Action of operators	Detection	It consists of getting one or more pieces of information allowing a failure identification (or detection), relieved by a technical device. The operator can be more or less active in this detection.
	Processing	It consists of making a diagnosis from detection stage information and selecting the adequate security action.
	Action	It consists of a manual action relieved by a technical device, countering the critical scenario.

Table 2: Definition of SIS sub-systems

An active SD is a barrier needing a mechanical system to develop an action (safety pressure, valve) but without external source of energy. In addition, a passive SD is a permanent barrier without human action, energy source, or information source. In this approach, SD barriers are considered as a particularisation of SIS ones because they are usually composed of one technical sub-system.
Considering the fact that these barriers (SIS and SD ones) are composed of, at least, a technical device, they can then prevent a scenario occurrence if they are available **[12]**. The availability is defined in **[55]** 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". It is function of intrinsic data (which is purely technical and represented by manufacturer's data) and contextual data (which represent human and organisational influences on this intrinsic data).

2.2. The human dimension

2.2.1. Action classes

During the study of the system functioning, it has been observed that the availability of any technical component is acted upon human actions. These actions are gathered into two categories:

- the maintenance actions (defined as 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" **[55]),**
- the control actions (allowing the system to properly operate).

In this methodology, indirect influences are characterised by maintenance actions and direct ones by control actions **[21, 26]**. This configuration is justified because the system availability, ensured by the effectiveness of maintenance actions, depends on its production capacity (or operability), ensured by the effectiveness of control actions. These actions effectiveness have to be quantitatively assessed according to principles developed in the Human Factors field.

The human factors can be studied through two fields which have different characteristics and aims: Ergonomics and Human Reliability[2]. However in relation to the aim of estimating the effectiveness of specific human actions, the objective is not to characterise the human-system interaction and its influence on the action effectiveness but mainly to qualify the impact of the organisation on the action effectiveness. This system configuration implies to identify human reliability concepts.
Human reliability can be defined as the ability of a human operator to perform a required mission under given conditions during a given time interval. It concerns the analysis and impact of humans on the reliability and safety of systems [27], by considering human actions not only as a source of error [28] but also as a source of performance [29]. It leads to enlarge the classical human task analyses area [30] in which the details of individual behaviours mechanisms are not considered. This expansion is done by focusing on collective behaviours through an aggregation of the different individual

[2] The International Human Reliability Analysis Empirical Study (www.ife.no/main_subjects_new/mto/) proposes several relevant research works.

behaviours acting together for the mission effectiveness. Thus, the proposed developments (representative variables, quantification method …) are more based on principles developed in the Human Reliability field with a collective and quantitative point of view.

2.2.2. Representative variables

In the industrial context of this work, a comparison of methods used by the French Electricity Board nuclear branch (EDF) and the French National Institute for Industrial Environment and Risks (INERIS) has led to select the variables defined hereafter. Some of these indicators are related to the collective characteristics:

- (De) *Delegation*, defined as transferring a task responsibility to another person, generally a subordinate. It can be introduced by the management (formal delegation) or not (informal one).
- (Ex) *Experience*, defined as knowledge acquired by practice, completed by thought on this practice.
- (Tr) *Training*, defined as the whole of the activities aiming at ensuring the acquisition of skills, knowledge and required behaviours to hold down a job.
- (Cmgd) *Collective management and group dynamic*, which is composed of rules (formal and informal) and work skills used by the collective to reach goals. It can be defined as the ability of a collective to fit a specific situation and to balance a potential drift.

In addition, other variables are specific with the tools and procedures that are used by the collective to achieve its actions:

- (Ai) *Aids*, which represent the whole of the procedures (prescriptive and non-prescriptive documents) and tools (other documents and equipments) used by operators in support with their activity.
- (Rws) *Respect of work specifications*. Work specifications hold information concerning the system, objectives to be reached and means making it possible to reach these goals. Their fulfilments are possible if this information has been correctly defined and if these objectives are achievable.
- (Rtc) *Real-time control*, defined by controls (conformity evaluations by observations and judgments completed if necessary by measurements, tests or calibrations) and goals achievement (means used to appraise the visibility of action issues without considering means used to reach these issues).
- (Fe) *Feedback experience*, which consists in capitalising and exploiting information resulting from the analysis of positive and/or negative events.

And the last variable is about external factors that can influence the collective during actions achievement:

- (Cf) *Contextual factors*, characterised by external elements influencing the studied action (lights, smog, other human actions in progress ...).

Considering differences between technical process operation and collective behaviours, it is proposed to study human influences on the technical process as external disturbances, in the sense that the technical system moves from a stable state (valid before the human intervention) to another stable state (valid after this human intervention). Between these stable states, the technical process evolves in a changing state **[21, 26]**.

2.2.3. Local features of studied systems

In relation to the technical process, this changing state principle is characterised by the fact that the subject (the collective) consider its action with the change of the object state (the safety component) and takes temporally control of it **[31]**. This control is materialised by a physical contact (through instruments, tools) between subject and object. As a consequence, this contact brings to the subject the energy required for the object transformation. It leads to define, in the proposed approach, that each action is related to a specific component. Therefore it means to clearly identify the technical component which is influenced by human actions. For example, an action cannot impact directly a physical phenomenon such as a tank explosion. This relationship has to be first represented with the tank availability (as defined in section 2.1.2) and then, by adding human influences.

Concerning the human action, this change can be seen as a local organisational change, inspired by **[32]** and divided into three generic steps (Figure 4): the Preparation, the Execution, and the Closing.

This representation allows a knowledge structuring and can be helpful during and after interviews to control the information collection and to organise this information (Table 3).

Action step	Definition	Associated action indicators
Preparation	It enables the planning, the specification and the characterisation of all required conditions to the proper execution of an intervention.	Delegation Aids Training
Execution	It allows the implementation of this intervention in the system operation.	Experience Respect of work specifications Contextual factors Collective management and group dynamic
Closing	It is a strengthening which ensures the proper integration of this intervention and confirms its continuity.	Real time control Feedback experience

Table 3: Definition of action steps and associated action indicators

Some comments can be developed on the indicators defined in this section:
- They are specific of an action, and must be defined for each action through activity analyses.
- The whole of these characteristics aims at being exhaustive but can be adapted. Indeed, variables can be added or deleted for specific contexts.
- Their achievements are constrained by the organisational climate in which operators are evolving. It is thus required to define how to study and represent this dimension regarding needs of the proposed approach.

2.3. The organisational dimension

2.3.1. The concept of Organisational Factor

Two theories are at the root of the development of organisational factors for hazardous systems. They are named the “Normal Accident Theory” (NAT) and the “High Reliability Organisations” (HRO). The first one is based on the “idea that in some technological systems, accidents are inevitable or normal” due to the combination of “interactive complexity and tight coupling” which “determine a system susceptibility” to unforeseen or prevented accidents. The second one is defined “as the subset of hazardous organisations that enjoy a record of high safety over long period of time” **[33]**. These fields define basically different views concerning socio-technical systems evolution leading to different representations for organisational factors.

Nowadays, there exist different scientific contributions that propose to define these factors **[34]**. From a first survey based on **[35, 36, 37, 38, 39]**, over thirty different factors can be identified. Nevertheless these factors are related “to the safe, normal, routine operation of an organisation that manages risk. At no time is the question of accidents and their teachings mentioned, although they are clearly characteristic of the safety of which the aim is to avoid accident”. Thus, it is proposed to use (in the methodology) the medical metaphor **[34, 37]** defines as follow: “for determining if an organisation is in good health, it is far simpler to know the causes of the sicknesses … It is more accessible to define a set of pathogenic organisational factors than to exhaustively list the organisational factors required and sufficient to ensure a good safety level within an organisation”.

2.3.2. The chosen representation

In that way, a pathogenic organisational factor (POF) results of the aggregation of convergent signs that allow the characterisation of a negative influence on the system safety. Seven organisational factors, issued from industrial case and accident report analyses, have been defined in a generic way **[34]**.

Among the seven factors, four of them are defined as follows:
- (FDSM) *Failure in Daily Safety Management*. The daily safety management deals with the safety requirements implementation within the organisation. Its main goals are to ensure a good agreement between workers activities and competencies in order to give relevant training courses to teams and to ensure that the safety knowledge is always transferred to adequate operators. This daily safety management could be judged as inadequate when financial means and resources are not enough to

implement the daily activities. It failed when, in spite of dedicated means and resources, the objectives are not reached due to a failing assessment of the needs and activities.

- (WCB) *Weakness of Control Bodies*. Control bodies are those in charge of checking compliance with safety obligations by the operator of the high-risk socio-technical system. There are different types of control body knowing that they may be associated with the installation, at a corporate level of the company, or outside the company. The shortcomings of the control bodies refer to the inadequacy of their actions. It means that they do not play the role of counterweight or counter-power that they are supposed to play.
- (PHOC) *Poor Handling of Organisational Complexity*. The organisational complexity deals with items that complicate work, decision-making processes and communication relationships related to risks and safety issues. This organisational complexity is generally related to several origins. It could be linked to the technological complexity, to the building of organisational partitioning, or to the multiplication of stakeholders that complicates the coordination inside the organisation. A complex and inadequate organisation can also be seen at least by two phenomena: a failing organisational communication and a failing coordination. A failing organisational communication deals with situations where the transmission of major elements for each worker (e.g. new directive or a new way of organising) is not done or is not done totally. In this case, the efficient way of communication in the organisation becomes an informal one. A failing coordination deals with usual dysfunctions in organisations that are bureaucracy, organisational partitioning and isolation.
- (NRDH) *No Re-examining of the Design Hypotheses*. A system design is built on the definition and the integration of social and technical dimensioning hypotheses. These hypotheses are based on a description of the future system operation. Nevertheless some hypotheses could become out of date that is inadequate to a new way of functioning. These hypotheses could also become false because the actual operating is proved different from the design one.

The three last factors are: *Shortcomings in the Organisation Culture of Safety* (SOCS), *Difficulty in Implementing Feedback Experience* (DIFE), and *Production Pressures* (PP).

Each of these factors is characterised by markers, signs and symptoms that allow their identification during on-site investigations. Thus, they will be defined once for the whole studied system by means of an organisational analysis. This list of factors aims at being exhaustive but could be completed after further developments. Indeed, the definition of new (pathogenic or resilient[3]) factors needs to study different incident and/or accident report analyses.

3. Knowledge unification and integration

3.1. Safety studies with Bayesian Networks

The modelling technique selected for unifying the knowledge coming from the three previous dimensions (technical, human and organisational) is the Bayesian Networks (BN). BN are directed acyclic graphs in which each node represents a variable, and each arc encodes conditional dependencies between these variables **[41]**. This formalism, initially developed to represent uncertain knowledge in artificial intelligence, has nowadays various application fields[4] (e.g. marketing, industry, health, decision making, risk management ...). More precisely, and in relation to the area in phase with the proposed methodology (safety of complex systems, risk assessment …), different research works highlight that BN are particularly well-suited **[42]**. The first item is about considering BN as a generalisation of the tree formalism to deal with the complexity of studied systems. In **[43]**, the authors use the notion of polytrees, and in **[44]** the authors develop a method that allows the translation of fault trees into BN (by using multi-state variables). The second item underlines works that use Dynamic Bayesian Networks (DBN) to evaluate the reliability of complex systems. In **[45]** and **[46]**, it is demonstrated how DBN can represent Markov chains to model system availability and reliability. In **[47]**, an evaluation of the reliability of technical systems based on the DBN formalism is proposed, and in **[48]**, the authors use Dynamic Object Oriented Bayesian Networks (DOOBN) to

[3] "The resilience can be defined as the ability of a material or system to absorb change gracefully whilst retaining core properties or functions. For an organisation, it is about ensuring that this organisation is still able to achieve its core objectives in the face of adversity." **[40]**

[4] www.bayesia.com, www.norsys.com, www.hugin.com/cases

evaluate reliability of complex systems. The last item is about a synthesis of different stages that enable the modelling of complex systems through BN in a reliability objective **[42]**.

In addition, different approaches based on BN formalism are addressing the risk analysis of such complex systems. First, the considerations of exogenous variables allow the modelling to be closer to operating conditions of studied systems **[49]**. Second, **[50, 11**, **14]** are focusing on the integration of human factors in the risk analysis process. Finally, **[12**, **51]** propose an integration of organisational factors in the risk analysis process.

Thus, the choice of BN tool for the modelling aspect of the methodology is justified with the previous explanations but also in relation to the characteristics of the systems studied in this paper.
It means now to focus on the specifications of this technique knowing that **[14]**, "since Bayesian Networks precision is directly related to the prior knowledge embedded in them … it was imperative to provide a technique to accurately model the prior knowledge and the way is represented in the conditional probability tables (CPT)".

3.2. Risk model development: human and organisational dimensions

3.2.1. Model objectives

In relation to the human and organisational dimensions, the main modelling objective consists in estimating the human action effectiveness considering its organisational context in order to enable an assessment of safety barriers availability **[26]**. The proposed model should allow the study of different kinds of impacts according to available information (themselves depending on the main subject of on-site investigations) such as impacts of the organisation on the collective, impacts of the collective on action effectiveness and impacts of the organisation on this effectiveness. This model is also developed, in case of critical situation diagnoses, to identify the most influent variables (i.e. the knowledge of some variables state allows to isolate the most influent causes in the studied situation). Then, information concerning an action can be obtained:

- by means of an analysis of the feedback experience and experts judgments for a yet-implemented action,
- by (direct or indirect) impacts of the organisation and/or other yet-implemented actions (through their specific indicators) for a new action (not yet-implemented in the system operation, and with no feedback experience).

3.2.2. Impacts identification method

Possible influences between POF and human action variables have been identified on the basis of their local characteristics (signs and symptoms for POF, indicators and actions stages for human action variables). The approach (cf. Figure 5) is defined in several steps as follow: identification of influences between indicators and signs/symptoms in one hand and between action stages and signs/symptoms in other hand (links 1 and 1'), justification of the presence (or absence) of influences between indicators and POF in one hand and between action stages and POF in other hand (links 2, 2', 3 and 3'). If the presence of influences can be justified, then links 4 and 4' are considered in the generic model.

The method implementation which consists in combining knowledge and experience of organisational and technical experts to identify and justify all the possible influences, leads to a generic configuration depicted in Table 4. Indeed, experts involved in these analyses are considered as referent in their field domains due to their theoretical and industrial backgrounds. This configuration is considered as generic because it has been defined in a general way (not dedicated to a specific range of applications) with the help of organisational experts addressing all the possible configurations. Some examples of the justification of the absence/presence of these influences in the generic model are given hereafter:

- Absence of influence (a blank cell in Table 4) between "NRDH" and "Ex". Experience is gained by observing the real system operation. Design hypotheses, defined during the system design or re-design, are not considered in this learning process.

- Presence of influence (a cross in Table 4) between "PP" and "Execution". If time, budgets, means and resources are revised downwards with constant objectives, the execution stage might be hurriedly performed, by ignoring some critical steps. It can lead to risky situations.

	Pathogenic Organisational Factors						
Indicators	SOCS	FDSM	WCB	PHOC	DIFE	PP	NRDH
De				X		X	
Ai	X		X		X	X	X
Tr		X	X	X	X	X	
Ex		X				X	
Rws	X	X	X	X		X	
Cf				X	X	X	X
Cmgd	X	X		X	X	X	
Rtc			X		X	X	X
Fe	X	X		X	X	X	

Action stages							
Preparation	X	X	X	X	X	X	X
Execution	X	X		X	X	X	
Closing		X	X	X	X	X	X

Table 4: Generic influences between POF and (a) Action indicators, (b) Action stages

This influences identification allows the following observations:
- all the POF do not impact all the action indicators and stages,
- all of these factors have at least an influence on one of the action indicators (or one of the action stages), i.e. all of these factors are represented in the model,
- a limit of this method lies in meanings given to indicators, actions stages and POF. Indeed, different meanings could lead to different configurations. This generic configuration is simplified for specific applications by removing influences.

3.2.3. Quantification method

At this stage, the Bayesian risk model (presented in Figure 5b) has to be up-graded with (a) information concerning variables modalities, (b) associated quantification method and (c) conditional probability tables (CPT) structuring. In that way, two modalities have been defined for each group of (Boolean) variables.
- For POF: *"Absent"* (A) and *"Present"* (P). It means that the pathogenic feature of the considered organisational factors (A) has not been proved; (P) has been proved.
- For human action indicators: *"Present"* (P) and *"Damaged"* (D). It means that the considered indicator (P) meets action requirements; (D) does not meet (or in a partially way) these requirements.
- For human action effectiveness and its stages: *"Effective"* (E) and *"Ineffective"* (I). It means that the considered variable (the human action or its stage) (E) fulfils the function for which it has been implemented in the system operation, (I) does not fulfil (or in a partially way) this function.

Then the associated quantification method is integrated in the model. It leads first to consider an initial configuration, for which the context is completely favourable. The probability of a variable Y to be in non-degraded state ("Effective" for action stages), knowing the non-degraded state of all of its parents, is settled at $a_0 \in [0,1]$. If one of its parents (X_1) is in degraded state ("Damaged" for human action indicators), then the probability of the variable Y to be in non-degraded state moves from a_0 to $(a_0 \times \alpha_{1-Y})$, with $\alpha_{1-Y} \in [0,1]$ an aggravation factor representative of the worsening influence of the parent X_1 on the variable Y. If a second parent (X_2) is also in degraded state then the probability of the variable Y to be in non-degraded state moves from $(a_0 \times \alpha_{1-Y})$ to $(a_0 \times f(\alpha_{1-Y}, \alpha_{2-Y}))$, with $\alpha_{2-Y} \in [0,1]$ an aggravation factor representative of the worsening influence of the parent X_2 on the variable Y, and $f(\alpha_{1-Y}, \alpha_{2-Y})$ a function allowing the accumulation of worsening influences of parents X_1 and X_2 on the variable Y. It is proposed to consider $f(\alpha_{1-Y}, \alpha_{2-Y}) = \alpha_{1-Y} \times \alpha_{2-Y}$, which can be generalised by using the Noisy-Or gate principles because these variables are Boolean **[12, 52]**.

Thus, let Y a node and $X = \cup X_i$, the set of parents of Y (with $i = 1,2,3,...n$). Instead of defining the initial probability of the non-degraded modality of Y as (1) (as it is done in the binary Noisy-Or gate), it is proposed to introduce an uncertainty (due to considered variables, which are related to human actions and/or the organisational context) and then to define this probability by (2).

$$P(\overline{y}\,|\,\overline{x_1}, \overline{x_2}, \overline{x_3},..., \overline{x_n}) = 1 \qquad \text{Binary Noisy-Or} \qquad (1)$$

$$P(\overline{y}\,|\,\overline{x_1}, \overline{x_2}, \overline{x_3},..., \overline{x_n}) = a_0 \qquad \text{with } a_0 \in [0,1] \qquad \text{Leaky Noisy-Or} \qquad (2)$$

where, $\overline{y}$: the non-degraded modality of Y, and y: its degraded modality; $\overline{x_i}$: the non-degraded modality of the parent X_i, and x_i: the degraded modality of this parent.

Moreover the probability of the non-degraded modality of Y, given that the i^{th} parent is degraded, is defined in (3).

$$p_i = P(\overline{y}\,|\,\overline{x_1}, \overline{x_2}, \overline{x_3},..., x_i,..., \overline{x_n}) = a_0 \times \alpha_{i-Y} \qquad (3)$$

where $\alpha_{i-Y} \in [0, 1]$ is the influence of the degraded state of the parent X_i on the non-degraded state of Y.

Finally, the probability of the non-degraded modality of Y, given $X_k \subseteq X$ the subset of parents of Y that are in their degraded state, is specified in (4) with an innovative semantic (from the formula presented in **[52]**, p.169).

$$P(\overline{y}\,|\,X_k) = a_0 \times \prod_{i:X_i \in X_k} \left(\frac{p_i}{a_0}\right) = a_0 \times \prod_{i:X_i \in X_k} \alpha_{i-Y} \qquad (4)$$

The "$\times$" operator is used in this approach to support the consideration of the accumulative effect of different parents on a variable (i.e. if one parent is in its degraded state, it leads to a less critical situation than if two parents are in this state). Thus, the method enables a particularisation of each influence identified between two variables. It means that the non-degraded modality column of the CPT relative to a variable Y (which can be an action indicator, stage or effectiveness) can be built by means of the following principle: for each n parents of the variable Y, all the previous combinatory is multiplied by the corresponding aggravation factor (in order to represent all degradations rules related to the parent).

3.3. Risk model development: technical and human dimensions

3.3.1. Model objectives

In relation to the technical and human dimensions, the main modelling objective consists in estimating the availability of safety technical components considering human and organisational contexts, and an evaluation of their impacts on the system (event occurrences, safety impacts, environment impacts, facilities impacts …). In that way, the proposed model allows to represent impacts of human actions (maintenance and control actions) on the component availability. As defined previously, this model also enables, in case of critical situation diagnoses, an identification of most influent variables (i.e. the knowledge of some variables state would allow to identify the most influent parents in the studied situation). Then, information concerning a safety technical component can be obtained by means of manufacturer's data, analyses of the feedback experience and experts' judgments.

3.3.2. Generic models

As proposed in section 2.1.2, a barrier can be broken down into its technical components. It leads to decompose its availability into "Detection availability", "Processing availability" and "Action availability" for SIS barriers type, or into "Technical Component availability" for SD barriers type (Figure 6).

These variables (Figure 6) are modelled with object oriented BN as described in **[48]** (holding an encapsulated BN). The generic models and associated quantification methods are developed in **[21]**

and have been particularised for different applications as illustrated in section 4 (Figure 11 and Figure 13). The variable meanings are defined in the following table:

POF	Pathogenic Organisational Factors	Object depicting organisational factors presented in section 2.3.2
DA	Detection Availability	Object depicting the availability of the detection component of the considered SIS
PA	Processing Availability	Object depicting the availability of the processing component of the considered SIS
AA	Action Availability	Object depicting the availability of the action component of the considered SIS
TC	Technical Component availability	Object depicting the availability of the safety device component
Oab	Operational availability of barrier	Variable depicting the aggregation of different component availabilities (Detection, Processing and Action, or Technical Component)
Btv	Bow-tie variable	Variable modelling event, occurring in the scenario, prevented by a proper barrier operation

Table 5: Definition of global barrier objects and variables

4. Industrial application

4.1. Industrial context of the studied installation

The studied system is a part of a chemical process which belongs to a classified installation. It produces plastic goods and it employs less than 100 people for a production capacity of 200 million pounds per year. This industrial site is ISO 9001 **[56]**, ISO 14001 **[57]** and OHSAS 18001 **[58]** certified. On-site investigations have emphasised:

- Competitions between production shifts in one hand, and with other companies in other hand.
- The subcontracting, due to a workforce cutting (and especially for executives) and an increasing of the workload which could lead to “know-how” losses.

These observations result from reorganisation strategic decisions made in the firm. For these reasons, organisational experts have identified three main POF potentially impacting the functioning: “SOCS” (Shortcomings in the Organisational Culture of Safety), “PP” (Production Pressures) and “NRDH” (No Re-examining of the Design Hypotheses). These factors may contribute to the weakening of the system which could eventually lead to a higher probability of risky situations in the future.

The studied installation consists in the end product storage in silos (Figure 7), in which main components are: a nitrogen sensor, two level sensors, two temperature sensors, a water system, a filter, a hydraulic protection, and shielding braids.

4.2. Studied scenario

The modelling of this scenario requires information related to the dreaded physical phenomenon and the human and organisational specific configuration.

4.2.1. Technical dimension

In this installation, the main critical event is the silo explosion. Indeed, the remaining solvent that was used in the process can evaporate, leading to a flammable cloud. Besides, suspended combustive dusts (in this case: plastic dusts) may be disseminated. Hence, an explosion can occur since six conditions are simultaneously present (Figure 8). Three of them concern the product and the three last ones are related to the environment. When one of these conditions is missed (expect for ones of the fire triangle), the explosion does not occur but the resulting ignition and fire will not be prevented.

4.2.2. Human and organisational dimensions

The information on this specific system has been gathered during on-site investigations. The investigations consist in developing interviews of executives and operators, achieved by technical and organisational experts. The information is used to depict the specific human and organisational configuration (Table 6 and Table 7) which is obtained by particularising the generic configuration

depicted in Table 4 (in section 3.2.2). Thus, in Table 6 and Table 7, the simplified configuration is described from keeping only the influences that are assigned a qualification (LI, I, II, TI). It means that 22 relations from the 37 initial ones are selected in Table 6, and 15 relations in Table 7. The following qualitative scale is used to assess each influence:

- LI (Little impact). The effectiveness is slightly impacted by this pathogenic feature.
- I (Impact). The effectiveness is significantly impacted by this pathogenic feature.
- II (Important impact). It materials a tightly impact of this pathogenic feature on the effectiveness.
- TI (Total impact). It represents a total impact of this pathogenic feature on this effectiveness.

	Pathogenic organisational factors						
Indicators	SOCS	FDSM	WCB	PHOC	DIFE	PP	NRDH
De							
Ai	**LI**		**I**		**LI**	**LI**	**I**
Tr		**LI**			**LI**	**LI**	
Ex							
Rws	**LI**					**I**	
Cf					**LI**		**II**
Cmgd	**LI**	**LI**			**LI**	**LI**	
Rtc					**I**	**LI**	
Fe	**II**	**I**			**II**	**LI**	

Table 6: Human and organisational configuration for the sensor calibration

	Pathogenic organisational factors						
Indicators	SOCS	FDSM	WCB	PHOC	DIFE	PP	NRDH
De							
Ai							
Tr		**LI**			**I**	**LI**	
Ex						**I**	
Rws		**II**				**I**	
Cf					**LI**	**II**	**LI**
Cmgd							
Rtc					**LI**	**I**	**I**
Fe		**I**			**II**	**I**	

Table 7: Human and organisational configuration for the braid supervision

As it is defined in Table 3, the relationships between action indicators, its stages and its effectiveness are depicted in Table 8 and Table 9.

	Indicators									*Action effectiveness*
Action stages	De	Ai	Tr	Ex	Rws	Cf	Cmgd	Rtc	Fe	
Preparation	**I**	**II**	**I**							**II**
Execution				**II**	**I**	**II**	**TI**			**TI**
Closing								**I**	**II**	**I**

Table 8: Quantification of sensor calibration influences

	Indicators									*Action effectiveness*
Action stages	De	Ai	Tr	Ex	Rws	Cf	Cmgd	Rtc	Fe	
Preparation	**LI**	**LI**	**LI**							**LI**
Execution				**I**	**I**	**II**	**LI**			**II**
Closing								**II**	**II**	**I**

Table 9: Quantification of braid supervision influences

4.3. Scenario modelling

The scenario modelling is made up of three steps. The first one consists in the bow-tie construction, the second one is about its formalisation with Bayesian Networks, and the last one concerns the Bayesian model quantification.

4.3.1. Bow-tie representation

Risk analyses sessions have led by means of the ARAMIS method **[25]** to the bow-tie diagram shown in Figure 9 and Figure 10. Safety barriers identified in this diagram are the following ones: (a) respect of procedures or maintenance operating modes, (b) continuous measurement of nitrogen concentration,

(c) respect of ATEX equipment, (d) grounding (shielding braids), (e) elaboration and respect of fire permit, (f) filter.

4.3.2. Bayesian Risk Model

The resulting Bayesian Network modelled by means of the BayesiaLab software (www.bayesia.com), is depicted in Figure 13. Within the model, the barriers 'a', 'c' and 'e' (Figure 9 and Figure 10) are not directly represented. They are implicitly present in the characteristics (action indicators in Figure 11) of barriers 'b' (SIS type), 'd' (SD type) and 'f'. Concerning the last barrier ('f'), its human and organisational contexts are not studied in this application. Indeed, on-site investigations have underlined the criticality of the barriers 'b' and 'd' but not of the barrier 'f' (no information was obtained concerning this barrier except for its presence in the system).

The objects depicted in Figure 11 (according to generic concepts developed in **[21])** model the following system features:

- "POF", for Pathogenic Organisational Factors,
- "BC", for the Barrier Component models, which contain the technical component availability and influences of human actions on this availability,
- "AC", for Actions Characteristics, which contain indicators, stages and action effectiveness.

4.3.3. Quantification

The qualitative construction of the risk model has to be assessed in order to make simulations and diagnoses.

(1) Human and organisational dimensions

The quantification of this model part is structured in two stages:

- Quantification of the initial situation (initial distributions of variables, i.e. in a favourable context): It concerns action effectiveness, action stages, action indicators and POF. Their initial distributions have been settled at 99% for their non-degraded state ("Effective" modality for action effectiveness/stages, "Present" one for action indicators and "Absent" one for POF).
- Quantification of the CPT: This item is addressed with an estimation of aggravation factors which are specific of the situation and obtained by experts' judgments and/or feedback experience analyses.

The qualitative scale assessing each influence in Table 6, Table 7, Table 8 and Table 9 is used to compute α_{i-Y} . For this application, the following specific scale is used: 'LI' (Little Impact, 95%), 'I' (Impact, 75%), 'II' (Important Impact, 50%), 'TI' (Total Impact, 1%).

(2) Technical dimension

The quantification of this model part is carried out by four stages:

- Quantification of initiators (by using experts' judgments and feedback experience analyses).

Initiator		Value (%)
Air presence		99
Assembly/re-assembly errors		90
Breaks of piping or tank		99.99
Cloud of explosive dust		99
Electrostatic discharge	Lightning	99.97
	Static electricity	1
	Vagabond currents	0
Explosive atmosphere		0.1
Failure of the nitrogen production		99

Initiator		Value (%)
Hot spots (extern)		99.9
Hot spots (intern)	Level sensor (Low)	99
	Level sensor (High)	
	Nitrogen sensor	
	Temperature sensor (High)	
	Temperature sensor (Very high)	
Hot spots works		99.9
Release of liquid (hydraulic protection)		99
Wear of joints		99

Table 10: Quantification of the "event absence" modality of initiators

- Quantification of barrier components CPT (through the method developed in **[21]**).

Barrier component	Intrinsic availability (%)	Maintenance action (%)				
		Type	α_1		α_2	
Nitrogen sensor	98	Calibration	II	50	I	75
Shielding braid	99.9	Supervision	LI	95	II	50

Table 11: Quantification of barrier component availabilities (1)

Barrier component	Operational availability (%)		
	Available	Unavailable	Absent
Processing	99	1	0
Action (5%)	99.9	0.1	0
Action (7%)	99	1	0
Filter	50	50	0

Table 12: Quantification of barrier component availabilities (2)

- Quantification of intermediate variables CPT. These CPTs are generally defined through logical functions (such as AND, OR functions as defined in Figure 9 and Figure 10).
- Quantification of event tree variables CPT (from experts' judgments) such as:
  - *Silo destruction:* If the event "silo explosion" has occurred, it is present in 98%. It is absent in the other cases.
  - *Dangerous phenomena (pressure effects, missile ejection):* If the event "silo destruction" has occurred, it is only pressure effects in 2%, only missile ejection in 3%, and a combination of pressure effects and missile ejection in 95%. It is absent in the other cases.
  - *Safety impact:* If the Dangerous phenomenon is a pressure effect, then this impact is present in 70%; if the Dangerous phenomenon is a missile ejection, it is present in 80%; if the Dangerous phenomenon is a combination of pressure effects and missile ejection, it is present in 99.99%. It is absent in the other cases.

4.4. Simulations and diagnoses

On the basis of the quantified risk model, different configurations can be studied with the following hypothesis: it is considered that the nitrogen sensor and the shielding braids are present in the system, i.e. the decision variables "Nitrogen_sensor_installation" and "Shielding_braid_installation" (in Figure 11) are settled at "Present".

The first studied configuration concerns the *a priori* results for "Sensor calibration effectiveness" (93.7%), "Shielding braid supervision effectiveness" (97%), "Operational availability of 5% oxygen detection barrier" (94.3%), "Operational availability of 7% oxygen detection barrier" (93.4%), "Operational availability of shielding braid barrier" (99.8%) and "Safety impact" (99.9%). These data are in coherence with those used to build the model. These results globally qualify the model in a favourable situation, i.e. with no pathogenic organisational factors.

The second configuration is obtained by using conclusions issued from on-site investigations to make simulations. Thus the presence of the pathogenic organisational factors "SOCS", "PP" and "NRDH" (cf. Table 13) are considered. These cases stress that:

- If availabilities of barriers are considered, both "production pressures" (for shielding braids) and "no re-examining of the design hypotheses" (for oxygen detection barriers) have to be handled in priority. This configuration is due to the fact that operators in charge of the calibration action are dedicated to this activity (maintenance staff), but the operators in charge of the supervision action have to accumulate this action with other ones (production staff).
- But if safety impacts are considered, no priority can be given for the handling of these organisational factors.

	SOCS	PP	NRDH	SOCS+PP+NRDH
Sensor calibration effectiveness	81.7	81.5	66.5	51.1
OA of 5% oxygen detection barrier	88.5	88.3	81	73.5
OA of 7% oxygen detection barrier	87.7	87.5	80.3	72.8
Braid supervision effectiveness	97	76.3	93	74.2
OA of shielding braid barrier	99.8	98.8	99.6	98.6
Presence of safety impacts	0.04	0.05	0.07	0.11

Table 13: Influences of the organisational situation on specific parts of the system

The third configuration is obtained by considering safety impacts as being "Present" to make a diagnosis and then to identify most influent variables. These variables are the following ones: "OA of 7% oxygen detection barrier" (0%), "OA of filter barrier" (0%), "OA of 5% oxygen detection barrier" (0.01%), "assembly/re-assembly errors" (25.4%), "presence of internal hot spots" (81.1%) and "OA of shielding braids" (95.8%).

It implies to study more specifically these different components. In that way, a first study can be achieved to identify major contributors of the unavailability of oxygen detection barriers, and more particularly on those related to the ineffectiveness of the sensor calibration. The results of this diagnosis situation, focused on the ineffectiveness of the sensor calibration, are presented in Table 14. In this case, it is required to pay attention in priority to the execution stage (E), the collective management and group dynamic (Cmgd), and the no re-examining of the design hypotheses (NRDH).

Group of variables		Modality	Probability (%)
Action stages	**E**	Ineffective	**58.5**
	P		19.8
	C		11.9
Action indicators	**Cmgd**	Damaged	**18.6**
	Fe		13.1
	Ai		8.5
	Ex		8.3
	Cf		7.7
	Rws		6.3
	Tr		3.4

Group of variables		Modality	Probability (%)
Action indicators	Rtc	Damaged	3
	De		2.8
Pathogenic organisational factors	**NRDH**	Present	**5.3**
	DIFE		3.3
	PP		**2.9**
	SOCS		**2.9**
	FDSM		2.2
	WCB		1.9
	PHOC		1

Table 14: Contributors of the sensor calibration ineffectiveness

4.5. Sensitivity analysis

The results obtained with the proposed model need to be validated in order to conclude on the relevance and quality of the model. In that way, a first step within validity procedure (first static step) is implemented with the methodology development because the model structure and its building are issued from systemic principles and experts' knowledge. It means that the modeling mechanisms are not only syntaxic but also semantic.

Moreover, the validation study concerns also the model variables and parameters, and can be achieved through a sensitivity analysis as proposed in **[59]**. Indeed in **[59]**, it is shown a methodology for Knowledge Engineering of Bayesian Networks in which the sensitivity analysis is used to "measure the sensitivity of changes in probabilities of query nodes when parameters and inputs are changed".

Concerning the industrial application selected here, the focus is on sensitivity to findings which considers "how the Bayesian Network's posterior distributions change under different conditions". A part of this analysis is depicted in Figure 12 (the endpoint node considered is the sensor calibration effectiveness).

In the Figure 12, nodes are listed from the least influential to the most influential. Horizontal bars highlight the variations of the sensor calibration effectiveness when the probability of its direct and indirect parent nodes is varied from 0 to 100%.

This analysis confirms observations presented in Table 14 for the most important contributors of the action ineffectiveness, and for the overall classification of action stages and pathogenic organisational factors, but for items the prioritisation is slightly different.

Indeed, variables identified as being highly sensitive to change (the most critical ones) are for each system dimension: the Execution action stage, the item 'Cmgd', and the organisational factor 'NRDH'.
Concerning the overall classification, different items have to be underlined:
- The ineffectiveness of the sensor calibration can be explained by a combination of its direct and indirect parents (action stages, items, and organisational factors).
- The prioritisation of action stages and organisational factors are similar in Table 14 and Figure 12.

These points confirm that the proposed BN accurately model the prior domain knowledge.
The difference observed in the classification of items is due to the important number of correlations, which make these variables more sensitive to changes. It highlights the needs of further developments concerning sensitivity analyses problems in order to eventually propose a dedicated method (based on behaviour analyses, mathematical approaches and/or experts' judgments) for the analysis of the formalised model.

4.6. Conclusions on the application and its modelling

The application step leads to the following comments:
- The organisational factors "PP" and "NRDH" have to be handled in priority. "SOCS" should be studied thereafter.
- About the sensor calibration, it is required to pay attention in priority to its execution stage and its collective coordination.
- A detailed study has to be conducted on filter barrier to identify human and organisational major contributors of its unavailability.
- Specific studies must be done on initiators for assembly or re-assembly errors.

More generally, the proposed risk model enables to identify, in one analysis, major contributors (initiators, safety barriers, human and organisational weaknesses) for a specific target (e.g. the safety impact in section 4), and to be able to offer a complete set of solutions. In other words, it allows:
- To demonstrate that direct causes of an accident occurrence can be explained by other ones (indirect), and that their treatment have to be addressed collectively (i.e. by considering the whole causes and not only parts of them).
- An ordering of technical and human events considering their criticality for the system safety, and then to make a choice for the events that have to be detailed.

These characteristics can help decision makers to anticipate critical situations and to prioritise their investments (economical, human, technical …).

Conclusion

The methodology presented in this paper allows a handling of a socio-technical system risk analysis in an integrated way. The integration is done step by step, due to the complexity degree of considered systems. The first one consists in identifying the system limits, allowing in a second step, to define adapted methods relative to knowledge collection of each system dimension (technical, human and organisational). The method choice can be done only after a theoretical study because the way of analysing, representing and quantifying all the considered dimensions can be really different. The third item is about the proposition of methods that handle the unification issue in order to integrate these different dimensions in a same risk model. This proposal cannot be uncorrelated of the selected modelling tool which is the Bayesian Networks in this methodology (owing to its characteristics: it deals with probabilistic and deterministic data, correlated variables, uncertainties ...). Then, it becomes possible to develop, in a generic way, models and associated quantification methods. The generic characteristics cover different activity sectors but require knowledge on the proposed methodology mechanisms and underlying concepts to be in a position to apply it on a particular case.
Finally, the application on a specific industrial system demonstrates the methodology feasibility and validity. Indeed, observations of recurrent behaviours stress the robustness of the obtained results. Moreover, these results are in coherence with observations made on the field.

The thus-built model highlights major contributors by means of simulations and diagnoses, of a safety problem. It enables to propose solutions and/or further studies for these specific system elements (technical components, human actions, organisational factors). This tool can thus be useful for decision makers to anticipate critical situations, and to conclude on strategies and investments prioritisation.

Nevertheless the methodology requires times and resources to collect data and to build the associated model. It leads to consider its efficient development only for critical systems (nuclear power plants, chemical processes ...).

Currently, the proposed approach has several limitations needing further developments. These developments concern mainly the automation of the model building, the modelling of resilient characteristics of studied systems, and the consideration of model and measure uncertainties.

Some other items have to be thoroughly investigated in order to complete the proposed approach, which are namely: the definition of influence and quantification classes according to specific studied actions and components; the definition of influence and quantification classes according to specific organisational structures, actions and processes; the consideration of human and organisational impacts not only through safety barriers but also as bow-tie initiators or events; the development of methods that allow a generalisation of semi-quantitative scales used in such analyses; the development of methods for model validations (such as sensitivity analyses); and the application of the proposed methodology to other industrial cases in order to identify possible adaptations and simplifications (according to the activity for example) and to build a dedicated feedback experience.

Concerning the last point, EDF currently applies the methodology on several specific cases (for the analysis of nuclear systems and hydraulic ones).

Acknowledgments

This research results from PhD thesis developments and was achieved in collaboration with the Research Centre for Automatic Control (CRAN), a research and development centre of the French Electricity Board nuclear branch (EDF) and the French National Institute for Industrial Environment and Risks (INERIS).

The authors thank Yves Dien (EDF) and Jean-Christophe Le Coze (INERIS) for their help in the definition of the human and organisational models of the proposed methodology.

References

[1] **Villemeur, A.** Reliability, Availability, Maintainability and Safety Assessment - Volume 1: Methods and Techniques. Wiley & Sons, 1992.

[2] **Swain, A.D.** and **Guttman, H.E.** Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278, US Nuclear Regulatory Commission, 1983.

[3] **Hollnagel, E.** Cognitive reliability and error analysis method (CREAM). Elsevier, 1998.

[4] **Barriere, M., *et al.*** Technical basis and implementation guideline for a technique for human event analysis (ATHEANA). NUREG-1624, Rev.1, US Nuclear Regulatory Commission, 2000.

[5] **Perrow, C.** Normal Accidents: Living with High-Risk Technologies. Princeton University Press, 1990.

[6] **Roberts, K.H.** Managing High Reliability Organizations. In California Management Review, 1990, 32-4, pp.101-114.

[7] **Svedung, I.** and **Rasmussen, J.** Graphic representation of accident scenarios: mapping system structure and the causation of accidents. In Safety Science, 2002, 40, pp.397-417.

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

[9] **Delmotte, F.** 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, 2003.

[10] **Papazoglou, I.A., *et al.*** I-Risk: Development of an integrated technical and management risk methodology for chemical installations. In Journal of Loss Prevention in the Process Industries, 2003, 16-6, pp.575-591.

[11] **Kim, M.C.,** and **Seong, P.H.** A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. In Reliability Engineering and System Safety, 2006, 91, pp.580-593.

[12] **Galán, S.F., Mosleh, A.,** and **Izquierdo, J.M.** Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. In Reliability Engineering and System Safety, 2007, 92, pp.1131-1138.

[13] **Lee, S.J., Kim, M.C.** and **Seong, P.H.** An analytical approach to quantitative effect estimation of operation advisory system based on human process using the bayesian belief network. In Reliability Engineering and System Safety, 2008, 93, pp.567-577.

[14] **Gregoriades, A.** and **Sutcliffe, A.** Workload prediction for improved design and reliability of complex systems. In Reliability Engineering and System Safety, 2008, 93, pp.530-549.

[15] **Preckshot, G.G.** Method for performing diversity and defense-in-depth analyses of reactor protection systems. Division of Reactor Controls and Human Factors, US Nuclear Regulatory Commission, 1994.

[16] **Jensen, F.V.** Bayesian Networks and decision graphs. Springer, 2001.

[17] **Von Bertalanffy, L.** General System Theory. G. Braziller, 1968.

[18] **Léger, A., *et al.*** Methodology for a probabilistic risk analysis of socio-technical systems. In INSIGHT, The Best of France – Forum Académique et Robafis, 2008, 11, pp.25-26.

[19] **Forest, C., *et al.*** Probabilistic assessment of potential major accidents: Estimating reliability of safety barriers. In European Safety and Reliability conference, Stavanger, Norway, 2007, T. Aven & J.E. Vinnem, Eds., Taylor and Francis Group, 1, pp.27-34.

[20] **Paté-Cornell, M.E.,** and **Murphy, D.M.** Human and Management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. In Reliability Engineering and System Safety, 1996, 53, pp.115-126.

[21] **Léger, A., *et al.*** A safety barriers-based approach for the risk analysis of socio-technical systems. In 17th IFAC World Congress, Seoul, South Korea, 2008.

[22] **Léger, A., *et al.*** Risk analysis of complex socio-technical systems by using Bayesian Network modeling. In 4th Workshop on Advanced Control and Diagnosis, Nancy, France, 2006.

[23] **Duval, C., *et al.*** Choice of a risk analysis method for complex socio-technical systems. In European Safety and Reliability conference, Stavanger, Norway, 2007, T. Aven & J.E. Vinnem, Eds., Taylor and Francis Group, 1, pp.17-25.

[24] **Farret, R., *et al.*** Epistemological perspective in the modelling process of an industrial system integrating technical and organisational dimensions. In the 15th annual conference SRA-Europe, Innovation and technical progress: benefit without risk?, Ljubljana, Slovenia, 2006.

[25] **Andersen, H., *et al.*** ARAMIS User Guide. The European Commission - Community Research - Energy, Environment and Sustainable Development - Project under the 5th framework programme, 2004.

[26] **Léger, A., *et al.*** Modeling of human and organizational impacts for system risk analyses. In 9th International Probabilistic Safety Assessment and Management Conference, Hong Kong, China, 2008.

[27] **Hollnagel, E.** Human Reliability Analysis: Context and Control. Academic Press, 1993.

[28] **Reason, J.** Human Error. Cambridge University Press, 1990.

[29] **Hollnagel, E., Woods, D.D.,** and **Leveson, N.** Resilience Engineering: Concepts and Precepts. Ashgate, 2006.

[30] **Research and Technology Organization.** The Human factor in System Reliability - Is Human Performance Predictable? In Human Factors and Medicine Panel (HFM) Workshop, 2000, p. iii.

[31] **Schank, R.C.** Conceptual information processing. Elsevier, 1975.

[32] **Lewin, K.** Field theory in Social Science. Ed. D. Cartwright, Harper & Row, 1951.

[33] **Marais, K., Dulac, N.,** and **Leveson, N.** Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems. In Massachusetts Institute of Technology - Engineering Systems Symposium, 2004.

[34] **Pierlot, S.,** and **Dien, Y.** From organizational factors to an organizational diagnosis of the safety. In European Safety and Reliability conference, 2007, T. Aven & J.E. Vinnem, Eds., Taylor and Francis Group, 2, pp.1329-1335.

[35] **Turner, B.A.** and **Pidgeon, N.F.** Man-Made Disasters - Second edition. Butterworth Heinemann, 1997.

[36] **Sagan, S.D.** The limits of safety, Organisations, Accidents and Nuclear Weapons. Princeton University Press, 1993.

[37] **Reason, J.** Managing the risks of organizational accidents. Ashgate, 1997.

[38] **OECD.** Identification and assessment of organizational factors related to the safety of NPPs. State of the art report, 1999.

[39] **Beaumont, G. *et al.*** Organizational factors - Their definition and Influence on Nuclear Safety - Final report. Commission of the European communities, Fourth framework program on nuclear fission safety, Report AMM-ORFA (99)-R06, 2000.

[40] **Seville, E., *et al.*** Building Organisational Resilience: A summary of key research findings. Research report - Resilient organizations programme, 2006.

[41] **Jensen, F.V.** An introduction to Bayesian Networks. London, Editions UCL Press, 1996.

[42] **Langseth, H.,** and **Portinale, L.** Bayesian networks in reliability. In Reliability Engineering and System Safety, 2007, 92, pp.92-108.

[43] **Torres-Toledano, J.G.,** and **Sucar, L.E.** Bayesian networks for reliability analysis of complex systems. IBERAMIA'98, LNAI 1484, 1998, pp. 195-206.

[44] **Bobbio, A., *et al.*** Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. In Reliability Engineering and System Safety, 2001, 71, pp.249-260.

[45] **Weber, P.** Dynamic Bayesian Networks model to estimate process availability. In 8th International conference on Quality, Reliability, Maintenance (CCF2002), Sinaia, Romania, 2002.

[46] **Weber, P.,** and **Jouffe, L.** Reliability modelling with dynamic Bayesian networks. In 5th IFAC Symposium SAFEPROCESS'03, 2003, pp.57-62.

[47] **Boudali, H.,** and **Dugan, J.B.** A discrete-time Bayesian network reliability modeling and analysis framework. In Reliability Engineering and System Safety, 2005, 87, pp.337-349.

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

[49] **Weber, P., Munteanu, P.,** and **Jouffe, L.** Dynamic Bayesian Networks modeling the dependability of systems with degradation and exogenous constraints. In 11th IFAC symposium INCOM'04, Salvador-Bahia, Brazil, 2004.

[50] **Embrey D.** Using influence diagrams to analyse and predict failures in safety critical systems. In 23rd ESReDA Seminar - Decision Analysis: Methodology and Applications for safety of Transportation and Process Industries, Delft, The Netherlands, 2002.

[51] **Trucco, P., *et al.*** A Bayesian Belief Network modeling of organizational factors in risk analysis: A case study in maritime transportation. In Reliability Engineering and System Safety, 2008, 93, pp.845-856.

[52] **Onisko, A., Druzdzel, M.J.,** and **Wasyluk, H.** Learning Bayesian network parameters for small data sets: application of Noisy-OR gates. In International Journal of Approximate Reasoning, 2001, 27, pp.165-182.

[53] **ISO 14121.** Safety of Machinery, Principles of Risk Assessment. International Organization for Standardization, 1999.

[54] **IEC 61511.** Functional Safety, Safety instrumented systems for the process industry sector, all parts. International Electrotechnical Commission, 2004.

[55] **EN 13306.** Maintenance terminology. AFNOR, 2001.

[56] **ISO 9001.** Quality management systems - Requirements. International Organization for Standardization, 2000.

[57] **ISO 14001.** Environmental management systems - Requirements with guidance for use. International Organization for Standardization, 2004.

[58] **OHSAS 18001.** Occupational health and safety management systems - Specifications. Occupational Health and Safety Assessment Series, 1999.

[59] **Pollino, C.A., *et al.*** Parameterisation and evaluation of a Bayesian network for use in an ecological risk assessment. In Environmental Modeling and Software, 2006, XX, pp.1-13.

Annex 1

Bayesian Network of the scenario studied in the application part of the paper