



HAL
open science

De l'analyse préliminaire de risque au système d'aide à la décision pour le management des risques

Mohamed Habib Mazouni, Jean-François Aubry

► To cite this version:

Mohamed Habib Mazouni, Jean-François Aubry. De l'analyse préliminaire de risque au système d'aide à la décision pour le management des risques. 8ème Congrès international pluridisciplinaire en Qualité et Sécurité de Fonctionnement, Qualita 2009, Mar 2009, Besançon, France. pp.CDROM. hal-00377904

HAL Id: hal-00377904

<https://hal.science/hal-00377904v1>

Submitted on 23 Apr 2009

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

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

8^{ème} édition du congrès international pluridisciplinaire
QUALITA 2009 – Besançon (France)
Du 18 au 20 mars 2009

DE L'ANALYSE PRELIMINAIRE DE RISQUE AU SYSTEME D'AIDE A LA DECISION POUR LE MANAGEMENT DES RISQUES

MAZOUNI Mohamed-Habib ¹, AUBRY Jean-François ²,

¹ CRAN-UMR 7039, Nancy-Université, CNRS/ESTAS-INRETS, 2 Av Général M. Joinville, Arcueil -
94114, France, Tel : +33 147407305, Email : mohamed-habib.mazouni@inrets.fr

² CRAN-UMR 7039, Nancy-Université, CNRS, ENSEM, 2 Av de la Forêt de Haye, Vandoeuvre, 54516 –
France

Tel : +33 383595578, Fax : +33 383595565, Email : jean-francois.aubry@ensem.inpl-nancy.fr

Résumé:

La pratique du management des risques accuse une grande variabilité ainsi que de nombreux problèmes d'ordre méthodologique, terminologique, technique ou organisationnel. Cela rend fastidieuse l'élaboration du dossier de sécurité d'un système, surtout quand il s'agit de plusieurs sous-systèmes réalisés par des sous-traitants disposant chacun de ses propres terminologie, méthode et savoir-faire.

Pour remédier à ces problèmes, une méthode de Management Préliminaire des Risques (MPR) basée sur une ontologie du risque a été définie et implémentée avec un outil d'aide à la décision. Cette ontologie est fondée sur le principe de la distinction des entités sources et cibles de danger, des espaces de danger et des espaces de vulnérabilité, des états des entités et des événements provoquant les changements d'états. Chaque concept est abordé en fonction de son aspect sémantique et de sa contribution dans le processus accidentel générique. Cette ontologie peut être représentée sous forme d'un modèle état transition qui présente l'avantage de créer un lien vers des méthodes d'évaluation quantitatives probabilistes. Elle permet de modéliser de façon systématique tout processus d'évolution dangereuse d'un système associé à un risque donné, d'en analyser systématiquement toutes les phases et de mettre en évidence les potentialités d'effets domino.

Abstract :

The practise of risk management shows a great variability as well as many methodological, terminological, technical or organizational problems. This makes tiresome the development of the safety documents of a system, especially when it deals with several subsystems carried out by subcontractors laying out each one of its own terminology, method and know-how.

To deal with these problems, a Preliminary Risk Management (PRM) method based on risk ontology was defined and implemented with a decision-making tool. This ontology is founded on the principle of distinction of the hazardous source and target entities, of hazard and vulnerability spaces, of the entities' states and the events causing the changes of states. Each concept is approached according to its semantic aspect and of its contribution in the generic accidental process. This ontology can be represented in the form of a state transition model that has the advantage of creating a connection towards probabilistic quantitative evaluation procedures. It makes it possible to model in a systematic way any hazardous evolution of a system associated at a given risk, to analyse all the phases systematically and to highlight the potentialities of domino effects.

Mots clés: Risque, Entité source de danger, Entité cible de danger, Ontologie, Processus accidentel

Keywords: Risk, Hazardous supplier entity, Vulnerable Target entity, ontology, accidental process

1 Introduction

L'avancée technologique spectaculaire et la complexification des systèmes sociotechniques émergents semblent prendre une longueur d'avance sur les moyens disponibles d'évaluation de la sûreté de fonctionnement et plus particulièrement de ceux qui relèvent de l'évaluation de la sécurité des systèmes.

Ceci dit, malgré la richesse de la terminologie de la sûreté de fonctionnement, les concepts de base souffrent d'une inquiétante fluctuation d'usage. Ce problème prend une dimension impraticable quand un industriel s'apprête à élaborer le dossier d'analyse de risque du système global et qui se trouve contraint de rassembler un éventail d'analyses de risque hétérogènes relatives à des sous-systèmes réalisés par des sous-traitants.

En effet, les analyses de risque telles que l'APR, l'AMDEC, l'Arbre de Cause, l'Arbre d'Événement, se trouvent dissociées les unes des autres ; ceci nuit considérablement à la fluidité et à la continuité du processus de management des risques. En outre, il existe un clivage entre les analyses de risque qualitatives et les analyses quantitatives ; ceci astreint les industriels à adopter des techniques subjectives d'évaluation des risques à l'image de la matrice de criticité ou du graphe de risque.

2 Place de l'analyse de risque dans le processus de management des risques

L'analyse de risque est l'utilisation systématique d'informations pour identifier les entités sources et cibles de danger et estimer le risque. Le Guide ISO/CEI 51 [ISO/CEI Guide 51, 1999] précise qu'une analyse de risque est une : « *Utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer les risques* ». Le Guide ISO/CEI 73 [ISO/CEI Guide 73, 2002] généralise la phase d'identification à tous les facteurs de risque et non seulement les phénomènes dangereux. Un facteur de risque est un paramètre que l'on observe et dont on pense qu'il joue un rôle dans la séquence accidentelle sans qu'il puisse être prouvé qu'il en est une cause directe ou indirecte.

Le management des risques est un ensemble d'activités coordonnées visant à diriger et piloter en fonction de l'appréciation des risques, les différentes politiques possibles de maîtrise des risques, c.-à-d. de réduction (protection / prévention) et de transfert de risque.

Rappelons d'abord que le management des risques selon le guide ISO/CEI 51 est l'« *application systématique des politiques de gestion, des procédures et des usages, aux tâches d'analyse, d'évaluation et de maîtrise du risque* ». Le Guide ISO/CEI 73 évoque un ensemble d'« *Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque* ».

Selon le guide ISO/CEI 51, l'appréciation des risques est l'ensemble du processus d'analyse et d'évaluation des risques, tandis que le guide ISO/CEI 73 évoque plutôt l'évaluation de l'acceptabilité des risques et non pas des risques eux mêmes ; ceci nous semble plus cohérent et c'est bien cette dernière définition que nous adopterons dans la suite de ce papier.

3 Dix enjeux problématiques en matière de management des risques

Il existe plusieurs problèmes essentiels pénalisant la pratique d'analyse de risque et globalement l'ensemble du processus de management des risques. D'une manière synthétique, nous pouvons dire que malgré les divergences constatées dans l'emploi des termes, concepts et méthodes, les pratiques du management des risques se basent essentiellement sur 4 exercices: investigation sur les scénarios d'accident, estimation des risques (par référence aux indicateurs de sécurité), évaluation et acceptation des risques (en fonction des objectifs de sécurité), et enfin maîtrise des risques.

Cependant, en dépit de leur importance, plusieurs aspects sont malheureusement négligés. Ces derniers

peuvent être catalogués en 10 classes:

1. Spécification systémique des limites de l'étude (frontières Système/Environnement).
2. Spécification ontologique de l'ensemble des constituants du système global.
3. Prise en compte, lors de l'estimation de la gravité, des enjeux capitaux tels que techniques, financiers, commerciaux, juridiques, médiatiques et économiques, etc.
4. Estimation de la fréquence (ou probabilité) d'occurrence.
5. Estimation de l'exposition au danger.
6. Suivi des risques.
7. Interconnexion des scénarios d'accidents (effets domino).
8. Interconnexion des sous-systèmes (intégrabilité).
9. Interconnexion de systèmes similaires (interopérabilité).
10. Intégration dans la stratégie globale du SMS (système de management de la sécurité) afin de rendre les résultats profitables par les analyses ultérieures.

5 Modélisation ontologique du processus accidentel

Les ontologies occupent aujourd'hui une place pivot dans de nombreux domaines. De l'intelligence artificielle au Web sémantique, du génie logiciel à l'informatique biomédicale, désormais, l'architecture de l'information est considérée comme une forme de représentation de la connaissance.

L'ontologie est généralement employée pour raisonner à propos des objets du domaine concerné après avoir modélisé un certain ensemble de connaissances relevant du domaine en question. Donc, l'ontologie constitue en soi un modèle de données représentatif d'un ensemble de concepts dans un domaine, ainsi que les relations entre ces concepts. Néanmoins, il existe une nuance entre terminologie et ontologie. Il faut savoir que dans une terminologie on s'intéresse aux mots et au sens, c.-à-d., aux distinctions entre ces mots, tandis que dans une ontologie, on s'intéresse plutôt à la notion de concept et à leurs relations de dépendance. Dans le domaine d'ingénierie de la connaissance, le concept d'ontologie semble avoir été introduit dans les années 90 lorsque Grüber [Grüber, 1992] introduisit une définition devenue par la suite une référence consensuelle : « *Une ontologie est la spécification (description formelle) d'une conceptualisation (un choix quant à la manière de décrire un domaine) d'un domaine de connaissance* ».

5.1 Ontologie pour la modélisation du processus accidentel

Compte tenu de l'intérêt de définir une ontologie de management des risques, nous allons œuvrer à migrer d'un langage naturel vers un langage formel en introduisant les concepts d'entité, d'espace, de situation et d'événement.

5.1.1 Entités élémentaires

Nous avons adoptée la notion d'entité définie par la norme CEI 50(191) [CEI 50(191), 1990] de la manière suivante : « *Tout élément, composant, sous-système, unité fonctionnelle, équipement ou système que l'on peut considérer individuellement. Une entité peut être constituée de matériel, de logiciel, ou des deux à la fois, et peut aussi dans certains cas comprendre du personnel, de même un ensemble déterminé d'entités, par exemple une population ou par exemple un échantillon, peut lui-même être considéré comme une entité* ».

Entité Cible de Danger (ECD): Une ECD est une entité, telle une personne, un bien ou une composante de l'environnement, susceptible, du fait de l'exposition au danger, de subir, en certaines circonstances, des dommages.

On associe à l'ECD deux notions importantes : la vulnérabilité et l'espace de vulnérabilité. La vulnérabilité caractérise la susceptibilité d'une ECD exposée à un danger particulier, de subir un dommage. L'espace de vulnérabilité d'une ECD est caractérisé par la fragilité des mécanismes de défense

de cette entité vis-à-vis de tous les dangers auxquels elle peut être exposée ; il peut être multidimensionnel (non limité à l'espace) et évoluant dans le temps.

Entité Source de Danger (ESD) : Une ESD est une entité porteuse ou génératrice de danger. Il peut s'agir d'un système naturel (environnemental ou humain) ou créé par l'homme, ou d'une disposition adoptée et comportant un ou plusieurs dangers. Un espace de danger est tout espace à l'intérieur et/ou autour d'une ESD, dans lequel elle produit un ou plusieurs dangers ; il peut être également multidimensionnel.

5.1.2 Evénements élémentaires

L'événement est le concept associé au changement de situation d'une entité. Il peut être courant ou anormal, déterministe ou stochastique (aléatoire), interne ou externe à l'entité. Il est caractérisé par sa description et ses occurrences (dates, fréquence, probabilité d'occurrence, etc.).

Evénement d'exposition: Evénement susceptible de faire passer une ECD de la situation initiale à la situation d'exposition vis-à-vis d'un espace de danger ; il est antérieur à l'événement redouté.

Evénement Initiateur: Evénement ayant la capacité de provoquer le passage d'une ESD de la situation initiale à la situation dangereuse ; il est situé en amont de l'événement redouté.

Evénement redouté: Evénement entraînant une situation d'accident ; son occurrence peut avoir lieu dès qu'un espace de danger et un espace de vulnérabilité se recouvrent.

5.1.3 Situations élémentaires

La notion de situation est à rapprocher de celle d'état quand il s'agit de mettre en évidence les circonstances dans lesquelles se trouve une entité ou bien sa réaction à ces circonstances.

Situation Initiale: C'est la situation jugée fonctionnellement normale où tout est conforme aux spécifications fonctionnelles de l'entité.

Situation d'Exposition: Situation d'une ECD caractérisée par sa vulnérabilité vis-à-vis d'un espace de dangers, c.-à-d. vis-à-vis d'une ou de plusieurs sources de danger.

Situation Dangereuse: Situation d'une ESD caractérisée par sa dangerosité vis-à-vis des espaces de vulnérabilité, c.-à-d. vis-à-vis d'une ou de plusieurs cibles vulnérables particulières.

Situation d'Accident: Situation due au recouvrement d'un espace de danger d'au moins une ESD et d'un espace de vulnérabilité d'au moins une ECD et à l'apparition de l'événement redouté.

5.2 Modélisation de type état/transition du processus accidentel

Le modèle accidentel générique que nous proposons est basé sur le principe d'état/transition (voir Tableau. 1) ; c'est à dire que le passage d'une situation initiale à une situation d'accident passe à travers un processus causal à transitions entre différentes situations intermédiaires dues à l'apparition progressive ou simultanée d'un ensemble d'événements.

Code	Signification	Situation de départ	Situation d'arrivée
EvE	Evénement d'Exposition	Situation Initiale (SI)	Situation d'Exposition
EvI	Evénement Initiateur	Situation Initiale	Situation Dangereuse
EvR	Evénement Redouté	Situation Dangereuse (SD) + Situation d'Exposition (SE)	Situation d'Accident (SA)

Tableau 1. Alphabet du RdP étiqueté de modélisation du processus accidentel ontologique

amènent à deux situations d'accident différentes, respectivement SA1 et SA2. L'événement redouté EvR1 est similaire à l'événement d'exposition du scénario 3 EvE3; ceci explique que le scénario 1 peut entraîner le scénario 3 si l'entité source ESD3 se met en situation de danger (SD3). Donc, il existe un lien à effet domino entre le scénario 1 et le scénario 3. Pareillement, le scénario 2 peut entraîner le scénario 4, mais cette fois-ci la similarité est entre l'événement redouté du premier (EvR2) et l'événement initiateur du deuxième (EvI4). La modélisation proposée offre une meilleure visibilité permettant de mieux structurer les lignes de défense en profondeur en implantant des barrières appropriées à chaque situation élémentaire du processus accidentel. Ainsi concernant la situation d'exposition, il convient de réduire les fréquences et les durées d'exposition, tandis que la stratégie concernant la situation dangereuse serait d'éviter l'apparition des événements redoutés et enfin concernant la situation d'accident, l'enjeu ultime serait de minimiser les préjudices pouvant être portés au système global.

6 Processus de la méthode MPR

Dans une démarche de résolution des problèmes constatés en matière de management des risques, nous proposons une méthode de « Management Préliminaire des Risques (MPR) » basée sur le processus accidentel ontologique. MPR permet de canaliser les mécanismes de capitalisation et d'exploitation des connaissances relatives aux scénarios d'accident (causalité, entités, situations, événements, etc.).

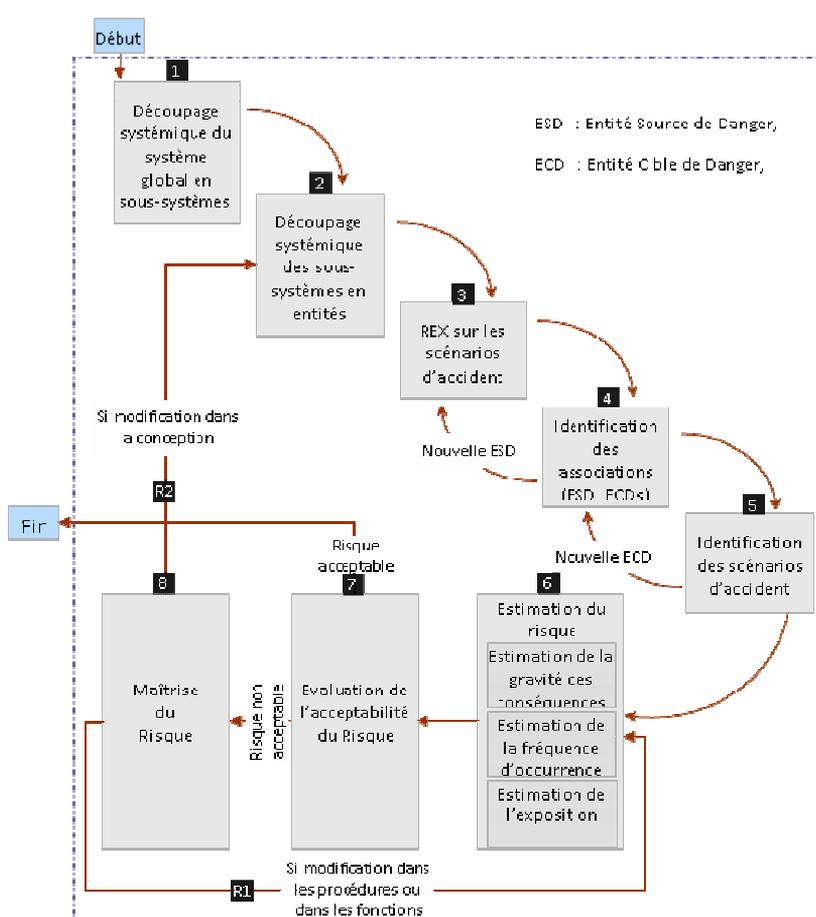


Figure 2. Processus de la méthode MPR

La méthode MPR se déroule en plusieurs phases (voir Figure 2) allant du découpage systémique du système global en des entités élémentaires [Mazouni & Aubry, 2007] jusqu'à l'identification inductive des scénarios d'accident en passant par une phase déductive d'identification des associations accidentogènes entre sources et cibles de danger, en se basant essentiellement sur le retour d'expérience et les bases de données d'expertise [Mazouni, Aubry, & El cours, 2008].

L'objectif final de notre étude est de concevoir un Système Interactif d'Aide à la Décision (SIAD) dédié à MPR. Par conséquent, il convient que le formalisme ainsi que la manière de présenter les données soient génériques et surtout adaptables aux différentes analyses de risque issues du monde industriel afin de pouvoir les capitaliser dans la base de données du SIAD [Mazouni, 2008].

Les résultats de MPR peuvent être regroupés dans un tableau ayant le format suivant (voir Tableau 2) :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Scénarios d'accident						Evaluation					Maitrise des risques					Décision		
ESD	EvI	SD	EvR	SA	ECD	Dom.	G.	O.	E.	Risque	Lib.	Type	Pilotage		Gains	Lib.	Motifs	Responsable
													Equipe	Manager	désirés			

Tableau 2. Présentation des résultats de la méthode MPR

MPR consiste à amorcer un processus itératif dans l'optique de converger vers les objectifs de sécurité préalablement énoncés. La démarche prend fin dès la réalisation de ces objectifs. Les deux boucles de rétroaction R1 et R2 (voir Figure 2) permettent de vérifier l'éventualité d'avoir généré de nouveaux dangers après mise en œuvre de certaines actions destinées à en contrôler d'autres. La première boucle correspond à une simple estimation a posteriori de la sensibilité des facteurs de risques vis-à-vis des modifications des fonctions d'une entité élémentaire ou bien à l'ajout de procédures de sécurité. La deuxième boucle, quant à elle, est plus complexe car elle correspond à un besoin d'opérer des changements dans l'architecture même du système global (ajout d'une nouvelle entité telle qu'une barrière de défense, modification de l'architecture d'une entité non élémentaire, etc.) ; ceci nécessite la reprise du processus MPR dès la deuxième phase, c.-à-d. la décomposition des sous-systèmes en entités.

La méthode peut idéalement accompagner le cycle de vie d'un système générique dès la phase de spécification jusqu'à la phase de démantèlement; ceci consiste à répéter le processus MPR depuis la seconde phase à chaque étape du cycle de vie (Initiative, spécification, conception, construction, exploitation, maintenance/modification, démantèlement).

7 SIGAR : Un outil d'aide à la décision en matière de management des risques

L'objectif principal de SIGAR est d'assister les évaluateurs dans la rédaction, la vérification et la mise à jour des dossiers de management des risques et particulièrement les dossiers d'Analyses Préliminaires de Risque [Mazouni, Aubry, & El kursi, 2008]. SIGAR (Système Informatique Générique d'Analyse de Risque) est un outil interactif d'aide et d'assistance au management des risques. Il est doté d'une interface graphique (GUI : Graphical User Interface) où les données introduites sont récupérées et ensuite composées sous la forme d'une requête informatique. L'extraction des données s'effectue à travers des sélections et des projections sur les tables correspondantes. Enfin, les résultats retournés par cette requête sont aussitôt récupérés et affichés de façon graphique agréable et ergonomique. Ces résultats affichés dans une forme tabulaire peuvent être triés par colonne afin de chercher les similarités des données. SIGAR est organisé autour de la base de données SIAD. Le modèle de données de SIAD se compose de plusieurs tables reliées entre elles par des liens relationnels ayant pour effet la génération de clés étrangères permettant de garder l'intégrité référentielle de la base de données. Cette notion d'intégrité référentielle est indispensable pour pouvoir vérifier la cohérence, la traçabilité et la complétude des données.

8 Conclusion

Les 10 problèmes que nous avons spécifiés expliquent en partie le manque d'outils fiables d'aide à la décision en matière de management des risques. Certaines méthodes comme l'APR n'ont jamais été outillées informatiquement. Enfin, les seuls produits qui existent ressemblent beaucoup plus à des interfaces de saisie d'analyses de risques qu'à des systèmes d'aide à la décision. MPR se présente sous une forme systémique et organisationnelle. En effet, les aspects organisationnels sont indispensables à la sécurité ; ceci a été affirmé par les résultats de la base de données Européenne MARS [INERIS-DRA,

2003] qui a réparti les causes des accidents majeures (déclarés survenus dans les pays membres) de la manière suivante (état au 05/1998): 53% liés aux dysfonctionnements de l'organisation, 29% à la fiabilité des équipements (au sens sûreté de fonctionnement), 11% imputable à un opérateur, 2% à l'environnement et 5% à d'autres causes. En outre, la démarche systémique de MPR permet de situer l'ensemble des entités du système global décomposé en plusieurs sous-systèmes, en l'occurrence le sous-système sociotechnique regroupant les acteurs et la technologie, et le sous-système environnement regroupant le public, la technologie et l'environnement naturel. Ces sous-ensembles sont à leur tour décomposés en entités plus élémentaires. Ainsi l'identification d'un scénario d'accident revient dans un premier temps à associer une entité source et une ou plusieurs entités cibles. L'outillage de la méthode MPR et la mise en place de la base de données SIAD permettent d'ouvrir un large champ d'étude et d'investigation en matière de traitement de données, car la base de données SIAD peut être accédée à partir de n'importe quel autre logiciel de base de données moyennant une autorisation d'accès délivrée par l'administrateur. La modélisation du processus accidentel ontologique est de type état/transition (spécification des états des entités, des événements, etc.), plusieurs extensions, telles que la génération automatique d'une version préliminaire d'AMDEC ou d'Arbre de Causes, sont possibles à travers l'exploitation directe de la base de données SIAD et aussi l'intégration directe de nouvelles fonctionnalités dans SIGAR.

Références

- [CEI 300-3-9, 1995] CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement*. CEI.
- [CEI 50(191), 1990] CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service*. CEI.
- [Grüber, 1992] Grüber, T.-R. (1992). *Ontolingua : A mechanism to support portable ontologies*. Stanford University, Knowledge Systems Laboratory.
- [INERIS-DRA, 2003] INERIS-DRA. (2003). *Outils d'analyse des risques générés par une installation industrielle*. INERIS, Direction des Risques Accidentels.
- [ISO/CEI Guide 51, 1999] ISO/CEI Guide 51. (1999). *Aspects liés à la sécurité – principes directeurs pour les inclure dans les normes*. ISO/CEI.
- [ISO/CEI Guide 73, 2002] ISO/CEI Guide 73. (2002). *Management du risque – Vocabulaire – principes directeurs pour les inclure dans les normes*. ISO/CEI.
- [Mazouni & Aubry, 2007] Mazouni, M.-H., & Aubry, J.-F. (2007, 26-29 Août). A PHA based on a systemic and generic ontology, Paper No. 166. *IEEE – ITS international conference SOLI'2007*. Philadelphia, USA: IEEE - ITS.
- [Mazouni, 2008] Mazouni M.-H. (2008, 13 Novembre). *Pour une meilleure approche du management des risques : de la modélisation ontologique du processus accidentel au Système Interactif d'Aide à la Décision*. Thèse de doctorat de l'Institut National Polytechnique de Lorraine.
- [Mazouni, Aubry, & El kursi, 2008] Mazouni, M.-H., Aubry, J.-F., & El kursi, E.-M. (2008, 4-5 juin). Méthode systémique et organisationnelle d'Analyse Préliminaire des Risques basée sur une ontologie générique. *1er Workshop du Groupement d'Intérêt Scientifique « Surveillance, Sûreté, Sécurité des Grands Systèmes » (3SGS'08)*. Université de Technologie de Troyes.
- [Mazouni, Bied-Charreton, & Aubry, 2007] Mazouni, M.-H., Bied-Charreton, D., & Aubry, J.-F. (2007, 18-21 Avril). Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport, Paper No. 98. *IEEE – SMC international conference SOSE'2007*. San Antonio, Texas – USA: IEEE – SMC.
- [SAMRAIL Consortium, Septembre 2003] SAMRAIL Consortium. (Septembre 2003). *Analysis of existing approaches, D 2.1.1 report*. European Commission and SAMRAIL partners.