



De la gestion classique des risques industriels à la prédiction du danger en milieu industriel en Algérie ; une approche cyndinique

Salim Bouchentouf, Kheloufi Benabdeli

► To cite this version:

Salim Bouchentouf, Kheloufi Benabdeli. De la gestion classique des risques industriels à la prédiction du danger en milieu industriel en Algérie ; une approche cyndinique. 2021. <hal-03162310>

HAL Id: hal-03162310

<https://hal.science/hal-03162310v1>

Preprint submitted on 8 Mar 2021

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.



HAL Authorization

De la gestion classique des risques industriels à la prédiction du danger en milieu industriel en Algérie ; une approche cyndinique

From classical management of industrial risks to hazard prediction methods in Algerian industrial environment; a cyndinic approach

Par

Salim BOUCHENTOUF (auteur correspondant)

Doteur habilité à l'université Tahar Moulay de Saida et chercheur au laboratoire des substances naturelles et bioactives de l'université de Tlemcen, Algérie.

Adresse: Cité El-Nasr, boîte postale 138, Saida, 20000, Algérie.

Tel: +213557974407

E-mail: bouchentouf.salim@yahoo.fr , salim.bouchentouf@univ-saida.dz

&

Khéloufi BENABDELI

Professeur à l'université Mustapha Stambouli de Mascara et chercheur au laboratoire géoenvironnement et développement des espaces, Mascara, Algeria.

kheloufi.benabdeli@univ-mascara.dz

Résumé

La prévention des risques industriels reste une préoccupation majeure de tous les dirigeants d'entreprise sans pour autant qu'une intelligence cindynique soit réellement développée. Généralement c'est les outils classiques de prévention et d'évaluation du risque qui dominent la stratégie adoptée dans ce domaine, confortée par des Plans Particuliers d'Intervention et des Plan d'Organisation des Interventions.

Pourtant une nouvelle option est possible, celle de la science des dangers comme moyen de base permettant l'intégration combinée des différents outils. La finalité dans cette innovation se traduit par la mise en place d'un Plan de Prévention des Dangers Industriels ; elle constitue une nouvelle approche intégrée de gestion des dangers sources de risques industriels.

L'utilisation intelligente des outils classiques de gestion des risques (étude d'impact, audit environnemental, audit maintenance, gestion des ressources humaines, plan de gestion de la maintenance, étude de danger, évaluation préliminaire des risques) permet de développer une nouvelle approche. L'exploitation intelligente de tous ces outils combinée aux deux fondements du risque que sont le danger et la vulnérabilité permet la mise au point d'une stratégie intégrée d'identification des dangers et des aléas permettant une gestion prévisionnelle des risques en milieu industriel.

Ce document sera une ossature pour une meilleure maîtrise des sources de danger et permettant l'identification de leurs causes à travers des fiches de données cindyniques pour toutes les ressources en relation avec la gestion des risques en établissant la mise en place d'une intelligence cindynique.

Mots clés : industrie- outils- risques- dangers- intelligence cindynique.

Abstract

The prevention of industrial risks remains a major concern of all company leaders without developing real cindynic intelligence strategy. Generally, classic risk prevention and assessment tools are adopted in this field, supported by special intervention plans and intervention organization plans. However, a new option is possible, which is hazard science, representing a basic means permitting combination and integration of different tools. The purpose of this new method is reflected by the establishment of an industrial hazard prevention plan which constitutes a new integrated approach managing different sources of industrial risks. The intelligent use of conventional risk management tools (impact study, environmental audit, maintenance audit, human resources management, maintenance management plan, danger study, and preliminary risk assessment) allows the development of the proposed approach. The use of all cited tools combined with the two fundamentals principles of risk, namely danger and vulnerability, allows integrated development strategy of danger and hazards identification permitting predictive management of risks in industrial environment. The present paper constitutes a framework for better control of danger sources allowing identification of their causes through cindynic data sheets establishing cindynic intelligence.

Keywords: industry- tools- risks- dangers- cindynic intelligence.

Introduction

Le développement industriel imposé par l'activité pétrolière et gazière dans en Algérie nécessite, pour être en conformité avec la réglementation nationale et internationale, la mise en place d'une stratégie de l'intelligence des risques (*IR*) qui découle directement de l'intelligence économique (*IE*).

Avant de pouvoir prétendre à la gestion intelligente du risque, la compréhension de la terminologie et ses concepts clés est importante. Le terme «risque» lui-même est qualifié de nombreuses définitions, avec plus ou moins de détails et de précision. En combinant, assimilant et distillant plusieurs de ces approches ; le risque est le potentiel de perte ou de préjudice causé par un événement (ou une série d'événements) qui peuvent nuire à la réalisation des objectifs d'une entreprise. Cette définition tient compte à la fois de la protection des acquis et de l'amélioration des objectifs. La gestion intelligente des risques n'implique pas seulement le désir d'éviter quelque chose de négatif mais aussi la nécessité d'atteindre quelque chose de positif. La gestion cyndinique des risques ne considère pas le risque seulement comme une vulnérabilité mais aussi comme une préparation aux événements de réussites et de succès.

L'atout de la gestion intelligente des risques réside dans l'interaction entre la probabilité, la vulnérabilité et le risque lui-même. La probabilité reste importante et respectée dans les programmes traditionnels de gestion des risques. En effet, de nombreux événements à risque se produisent avec régularité et peuvent donc être efficacement modélisés en utilisant différents techniques de statistique. Mais cette dernière a moins de valeur pour les risques qui se produire en dehors des fluctuations normales, soit lorsque l'événement est rare, sans précédent, les règles sont inconnues ou changent rapidement, les causes sont motivées par des facteurs externes qui dépassent le contrôle de l'entreprise. Basée sur la prédiction, la gestion intelligente des risque reste difficile face à un environnement ouvert, où les connaissances sont généralement imparfaites et où plus de choses pourrait arriver que ce qui arrivera. Niels Bohr, le physicien danois et lauréat du prix Nobel est crédité de la citation «Prévenir est très difficile, surtout pour l'avenir » [1].

L'exploitation de différents outils disponibles mais très peu exploités constitue pourtant un volet déterminant pour une amélioration de l'approche en matière d'identification des dangers, source de risques industriels. Le recours permanent aux différents audits et études par une exploitation intelligente basée sur la capitalisation de l'information à travers un système de veille doit permettre la mise en place d'une stratégie de prédiction des dangers.

Une bonne élaboration et exploitation de ces outils permettent de concrétiser la progression suivante en matière d'identification et de localisation des dangers.

Outils classiques utilisés pour la gestion du risque et les problèmes rencontrés.

Les principaux outils disponibles au niveau des entreprises industriels sont imposés par la réglementation et peuvent être classés en trois catégories :

- Les outils majeurs qui regroupent la politique et l'organisation adoptée par l'entreprise dans le domaine HSE, les audits (environnement, sécurité, maintenance, organisation, gestion)
- Les outils secondaires qui ne sont que les outils de gestion courante comme les audits spécialisés, les audits internes, le système de gestion de la sécurité, le système de management intégré, la plan de gestion des risques, le management des ressources, le plan de gestion de la maintenance.
- Le retour d'expérience et la compétence des moyens humains qui constituent un volet de qualité reposant sur la capitalisation des enseignements tirés des accidents, des incidents, des erreurs commises et des dysfonctionnements constatés.

De ces outils il est possible de dresser un listing de toutes les sources de dangers constituant un potentiel risque pour l'entreprise (voir tableau 1).

Tableau 1 : Différents outils et leur utilité pour l'étude des dangers

Outils	Contenu	Utilité pour les cindyniques
Etude d'impact	Analyse des process et impact sur l'environnement	Localisation des sources de pollution
Audit environnemental	Localisation et évaluation des nuisances à l'environnement	Corrélation des nuisances avec les équipements
Etude de danger	Identification et évaluation des dangers potentiels	Hierarchisation des causes des dangers et des risques
P.O.I	Orientation en utilisation des moyens d'intervention	Capacité organisationnelle de l'entreprise à gérer ses risques a
P.P.I	Mobilisation des moyens et d'une stratégie	Capacité technique et moyen à gérer des risques
Plan Gestion Sécurité	Cartographie des sources de danger	Localisation des dangers dans le temps et dans l'espace
Plan Gestion Ressources	Evaluation du potentiel humain	Elaboration d'une Fiche de Données Humaines
Plan Gestion Maintenance	Prévision du maintien de fonctionnement des équipements	Localisation des zones vulnérables
Retour d'Expérience	Analyse de l'accidentologie et arbre des événements	Arbres des causes, volet très intéressant

Il a été constaté que la gestion des risques connaît beaucoup de problèmes et limites liées au facteur humain. A travers une analyse poussée, nous avons relevé les points suivants :

Un manque de structure de prise de décision sur les risques et un manque de responsabilité sur les décisions pour les risques dans une organisation. Presque tous les dirigeants d'entreprise sont à l'aise avec la prise de décisions en matière de risques, cependant, dans de nombreux cas, les bonnes personnes ne prennent pas ces décisions. Dans de nombreux cas, les décisions à haut risque sont prises à un niveau trop bas dans les organisations, avec des gens qui ne sont pas incités à prendre les bonnes décisions pour l'organisation.

L'absence d'un significatif de processus d'évaluation des risques. Certaines organisations considèrent la gestion des risques comme quelque chose à faire du point de vue de la conformité et effectuent des évaluations des risques superficielles. D'autres n'ont tout simplement pas les compétences nécessaires pour développer un processus d'évaluation des risques significatif. Un processus significatif permet d'identifier les risques en fonction des objectifs de l'organisation et décrit ces risques soit qualitativement, soit qualitativement à travers une taxonomie des risques commune.

Il y a une approche commune de «je me suis comparé à une liste de meilleures pratiques et tout ce qui me manque ne doit pas être un risque». Les meilleures pratiques doivent être adoptées en tant que contrôles pour gérer les risques que nous avons identifiés. Prendre une liste, et simplement l'appliquer, ne signifie pas que nous avons atténué les risques.

L'absence d'une culture du risque. Afin de créer une culture où les chefs d'entreprise sont disposés à être transparents vis-à-vis de leurs dirigeants, les dirigeants eux-mêmes doivent veiller à créer le type de culture qui favorise cette transparence. Les dialogues ouverts sur les préoccupations, les risques et les compromis nécessaires font souvent défaut dans les organisations qui ne disposent pas d'une gestion efficace des risques.

Les problèmes dans la pratique de la gestion des risques confirment que la gestion des risques est un système complexe [2].

Importance de la prédiction des dangers

3.1- Importance de la détection et évaluation des menaces cindyniques

Que cache l'expression détection des menaces ?

De la détection des menaces et des risques à la prédiction des dangers il n'y avait qu'un pas ; encore fallait-il le franchir ! En effet que cache cette expression ?

Tout doit dans un premier temps reposer sur un recensement le plus détaillé et précis possible des enjeux de l'entreprise et des aléas qui la menacent. Si les aléas et les dangers avec leurs sources sont connus, localisés et identifiés dans le temps et dans l'espace, leur prédiction est possible.

Concevoir une approche globale, intégrée et systématique des aléas et des dangers devient impératif managérial incontournable pour l'entreprise.

3.2- Utilisation des outils classiques pour une prédiction des dangers

Une analyse et exploitation professionnelle de tous les outils de gestion globale des risques industriels cités ci-dessus permet une maîtrise des sources de dangers. Les sources de dangers, unique moyen de bien identifier les risques industriels, peuvent être extraites des outils classiques et peuvent être regroupés en 4 catégories [3]:

- les enjeux
- les aléas
- les menaces
- les vulnérabilités

3.3- Les 4 sources de dangers

La maîtrise des dangers reste un volet déterminant dans la gestion globale des risques même si elle n'est issue que de l'étude de danger. Les paramètres à prendre en charge dans l'approche basée sur l'identification des dangers et de leurs sources qui se divisent en deux catégories : les enjeux et les aléas peuvent être récapitulés comme suit :

- *Enjeux* : utilisation des ressources, réalisation d'une production, commercialisation de la production, assurer une rentabilisation des ressources, stratégie de gestion
- *Aléas* : Carence professionnelle, mauvaise organisation, ressources humaines, dysfonctionnement, désorganisation.

A chacun de ces 2 niveaux de fonctionnement d'une entreprise il existe des dangers potentiels qu'il convient d'identifier et surtout de localiser leurs sources. La gestion des risques exige une clarté des informations, des données de qualité et leur quantification. Elle exige des analyses à partir des données pour soutenir le processus décisionnel. Les gestionnaires ne veulent plus simplement les données, elles veulent surtout pouvoir les utiliser de manière intelligente pour les aider à prendre de meilleures décisions. La finalité étant de maîtriser le domaine des dangers, mais aussi de soutenir les objectifs commerciaux de leurs entreprises. Les gestionnaires de risques sont passés une à approche beaucoup plus holistique de la gestion des risques.

Cet objectif ne peut être atteint qu'à travers la science des dangers. Les enjeux sur lesquels repose toute l'existence de l'entreprise constituent la principale source de danger.

La seconde catégorie se résume aux menaces et à la vulnérabilité de l'entreprise qui n'est que l'érosion ou l'absence de professionnalisme :

- *Menaces* : Externalisation d’actions structurantes, malveillance, mauvaise maintenance des ressources, exploitation des ressources

- *Vulnérabilités* : Sûreté des installations, surveillance perméable, suivi périodique, état des ressources, non détectabilité des risques

Comme le précise Ezell [4], «la vulnérabilité met en évidence la notion de sensibilité à un scénario, tandis que le risque se concentre sur la gravité des conséquences au sein du contexte d'un scénario ». Ainsi, les évaluations de la vulnérabilité ne sont pas les mêmes que les évaluations des risques

Les menaces et les vulnérabilités de l’entreprise tant dans son organisation que son fonctionnement constituent le référentiel et le creuset où doivent être trouvés toutes les sources de dangers.

Les gestionnaires des risques rencontrent d’autres difficultés comme les restrictions budgétaires et la complexité grimpante du paysage des risques auquel ils sont confrontés. Ils ont désespérément besoin de reconsidérer les méthodes classiques dans le but d’un changement fondamental des mentalités aboutissant à différentes compétence pour les gestionnaires des risques. Il est toujours important de considérer l'impact des nouvelles technologies sur l'élément humain pour une meilleure gestion des risques.

L’exploitation détaillée de chacune de ces 4 phrases de sources de dangers permet d’identifier et de localiser dans un premier temps les sources de dangers qui pourront être par la suite hiérarchisés suivant une matrice de criticité multicritères pondérés (voir tableau 2).

Tableau 2 : matrice combinée de criticité

Sources	Dangerosité	Fréquence	Détectabilité	Total
Enjeux				
Aléas				
Menaces				
Vulnérabilité				
Organisation				
Gestion				

4.1- Vers une nouvelle définition du risque : Sécurité, sûreté, dangers

A ce sujet Possin [5] note : « L’Intelligence du Risque ne relève pas d’une quelconque phobie, paranoïa ou d’une « obsession sécuritaire » pour l’entreprise, c’est au contraire une approche raisonnable et maîtrisée des menaces et risques qui accompagne un développement rationnel et harmonieux de celle-ci adaptée à la culture de l’entreprise ».

Déjà en 1916 Henri Fayol identifie 6 fonctions principales dans l’entreprise dont celle de « directeur sécurité et stratégie ». C’est le point de départ d’une véritable prise de conscience et de celle de la fonction de Responsable de la Gestion des Risques (RGR).

Il en découla une définition élargie de la notion de risque qui prend en charge les causes des risques : le danger. Il est « acceptable ou inacceptable ». Sur la base d'un audit sécuritaire préalable et de formules mathématiques simples *l'IR* permet de calculer la criticité pondérée de chaque risque décelé.

La criticité pondérée d'un risque est égale à la fréquence pondérée que multiplie la gravité pondérée selon la formule proposée par Geiben et Nasset [6] : $Cp = Fp \times Gp$.

Dès lors il devient possible de calculer et de visualiser le Risque Sécuritaire Global (*RSG*) d'une organisation. Les risques ayant été identifiés et calculés il est aisé de les hiérarchiser pour mieux les réduire (sensibilisation, prévention, réduction ou éradication).

Le monde industriel ne se reconnaît que dans l'intelligence des risques (IR) et le risque sécuritaire global (RSG). Après la gestion classique du risque est venue le concept de l'Intelligence du Risque (IR ; c'est un concept global de sécurité à double finalité. *L'IR* procède d'une stratégie sécuritaire globale allant de l'identification (dans et hors des murs de l'entreprise) au calcul et à la hiérarchisation du risque *jusqu'à* l'élaboration d'une capacité de réplique par la mission protection [7].

L'intelligence des risques combine l'identification des risques, l'analyse des risques et l'évaluation des risques. L'identification des risques est la première étape dans l'intelligence des risques et se concentre sur l'identification de la source des risques et des événements potentiels qui pourraient avoir un impact sur les objectifs d'une entreprise. L'identification du risque fournit également un aperçu de l'interaction entre le risque et la menace. Une telle perspicacité est un processus important car chaque entreprise a un contexte unique et, par conséquent, doit se concentrer sur différents risques [8].

L'IR assure la défense du « périmètre stratégique de souveraineté » ou « périmètre défendable » de l'entreprise préconisé par Clarke [7,9]. Cette notion de « périmètre défendable » vraie hier, l'est beaucoup moins aujourd'hui du fait de l'actuel nomadisme des cadres et *des* outils de travail collaboratif à distance.

Née de l'Intelligence Economique, l'Intelligence de risques (IR) devient aujourd'hui la modélisation proactive d'un outil de défense global conçu pour l'entreprise, *les* territoires comme les Etats mais qui doit découler de l'intelligence cindynique.

Les aléas et les ressources conjugués aux enjeux au sein d'une entreprise sont les sources principales de dangers générateurs de risques. Ainsi le danger devient global et permanent quelque soit la stratégie de gestion du risque mise en place. Effectivement, une fois le risque admis, sa gestion est déjà une carence et une fatalité [10].

Il est plus juste d'utiliser les termes de Gestion du Danger Global que celui de Gestion des Risques ; on ne peut gérer un risque que si l'on connaît sa source qui est le danger.

Le métier de Danger Manager doit remplacer celui de Risk Manager pour une instauration du concept de la prédiction des dangers. Ainsi la gestion du danger anticipe les crises au lieu

d'avoir à les gérer et contribue à rationaliser et diminuer les coûts de la sécurité et de la protection.

Dans l'entreprise, tout ce qui altère la performance pour une raison ou pour une autre relève désormais de la gestion des dangers *qui est plus préventive que l'Intelligence Risque*. C'est un concept nouveau de sécurité globale intégrant toutes les sources de dangers pouvant se traduire ou pas par des risques.

La gestion des dangers modélise et instaure une vigilance permanente et une protection compatibles avec l'activité des organisations et des systèmes de l'entreprise.

Ce concept de protection s'insère dans l'idée générale de vigilance qui ne peut se concrétiser qu'à travers une Intelligence Cindynique que se font nos sociétés de la protection des personnes et des biens matériels et immatériels, du tissu socio-économique et de l'économie en général.

4.2- Objectifs et avantages de la prédiction des dangers

L'obligation de prévention des risques, à la charge de la puissance publique, est polymorphe. Prévenir, c'est étymologiquement anticiper un événement pour empêcher qu'il se produise, mais c'est aussi informer les victimes potentielles de son existence. La prévention des risques s'appuie sur les notions communes que : danger, risques, dommage, évaluation, gestion.

La notion d'exposition d'une cible à un danger y est intégrée. Les nombreuses réglementations en la matière exigent que soit menée une évaluation des risques, laquelle va reposer sur une identification des dangers puis une analyse détaillée des risques. Dans ce volet, le recours à l'analyse des risques et leur évaluation consiste à améliorer la sécurité qui est l'aptitude des organisations à prévenir ou à éviter la survenance d'événements graves.

A titre non exhaustive, la prédiction intelligente des dangers permet :

Une capacité efficace et prouvée de prévenir, détecter rapidement, corriger et escalader les problèmes de risques critiques,

La réduction de la charge financière dans les opérations de normalisation et standardisation des procédures de gestion des risques.

Un meilleur partage de l'information sur les risques et intégration des risques existants,

Un meilleur moyen pour améliorer la flexibilité stratégique pour différents scénarios,

La fournir aux managers et aux différentes parties prenantes, un confort dans la gestion et la compréhension de différentes gammes de risque.

La prédiction des dangers livre une vision globale du panorama des sources donc des causes des risques et détermine le Risque Système Global soit sous la forme d'un panorama des risques, soit sous celle d'un histogramme. Elle repose sur deux volets plus exhaustifs et complémentaires que l'intelligence du risque. Le premier volet calcule puis hiérarchise les dangers et leurs sources c'est l'Intelligence risques.

Dans un second plan, elle s'attachera à bâtir l'épure d'une authentique mission protection apte à réduire les menaces les plus graves.

Ce second volet de l'IC traitera des points vitaux que sont :

- la Charte et le schéma directeur de sécurité/sûreté,
- la délégation de pouvoir,
- la mise en place d'un organigramme de sécurité et d'une cellule de gestion de crise.

Grâce à la prédiction des dangers l'entreprise sort de sa posture exclusivement défensive. Les barrières de protection physique ou immatérielle ne suffisent plus ; il convient d'aller au devant du risque, de débusquer les menaces et les dangers ainsi que la vulnérabilité très en amont avant qu'ils ne se concrétisent. L'entreprise bunker a vécu un certain temps, elle ne le peut plus actuellement que dans un périmètre défendable bien défini et maîtrisé [7].

Cette nouvelle approche cindynique préconise la mise en place de structures et de procédures de contrôle, d'alerte et de suivi dans le cadre d'une gouvernance efficiente de la gestion des risques et institue une véritable cartographie sécuritaire de l'organisation. Toutes les occurrences de dangers-risques confirment aujourd'hui la nécessité d'une réflexion globale et pluridisciplinaire. Seul le découplage des compétences et des risques permet d'envisager l'inconcevable, et de donner libre cours à l'imagination de scénarii improbables mais possibles.

L'entreprise ne prend généralement en compte que les risques liés à la sécurité (Safety) au sens industriel du terme (celle-ci intègre généralement la sécurité industrielle, l'incendie, l'environnement, l'hygiène et la santé au travail ainsi que les risques de Sûreté (Security) liés à la malveillance humaine. Les risques de management ne font pas l'objet d'une prise en compte systématique mais généralement d'un « traitement » au cas par cas en fonction des besoins ou dans le cadre d'une gestion de crise.

Conclusion

L'établissement d'une véritable gestion intelligente des risques est basée sur des objectifs, où l'entreprise examine ses stratégies et ses objectifs à long terme ainsi que ses besoins opérationnels et identifie les menaces susceptibles de créer de l'incertitude. Cependant, avant de pouvoir le faire, un cadre de gestion des risques approprié doit être mis en place. Cela comprend une structure de gouvernance et de surveillance des risques, un univers de risques commun utilisé pour catégoriser et délimiter une taxonomie des risques commune pour décrire les dangers et leurs impacts.

Plusieurs spécialistes sont persuadés que le "Risque Zéro" est non seulement possible mais que c'est une nécessité qui impose une prévention permanente des dangers, générant des risques qui ne soit pas seulement traduite dans les consignes affichées, mais aussi et surtout, qu'elle soit intégrée dans les comportements quotidiens et les esprits de chacun suivant son niveau et son degré de responsabilité.

Le risque zéro ne peut être atteint que s'il repose sur une maîtrise des dangers et de leurs diverses sources à travers une prédiction cindynique.

Un audit complet duquel découle un audit spécialisé mais à forte périodicité permet d'appréhender avec plus de certitude les sources de dangers induisant les Scénarios Maximum Physiquement Possibles. Le volet audit périodique des moyens humains constitue également un atout déterminant dans l'identification prévisionnelle des sources de dangers à travers les Scénarios Maximums Humainement Possibles [11].

Il ne fait nul doute que cette démarche volontaire qui n'en est encore qu'à ses débuts en Algérie dans le milieu industriel puisse se généraliser progressivement en se basant sur une combinaison de toutes les études. Il est temps de mettre fin à la banalisation des audits et d'en faire un instrument de référence pour vaincre la situation d'insécurité imposée par un risque permanent d'incidents.

Cette nouvelle approche axée essentiellement sur l'étude des dangers qu'est la cindynique [12] se traduira à très court terme comme :

- un moyen sûr d'amélioration de leur compte d'exploitation, par réduction ou élimination des coûts liés à la sécurité et sûreté,
- un élément prépondérant de leur stratégie commerciale.

Pour ceux, enfin, qui sont conscients des enjeux pour le devenir de leur entreprise face à un incident ou un accident à fort impact environnemental, la démarche, que nous venons d'examiner succinctement, permet à l'entreprise de mieux adapter sa stratégie à l'univers incertain, mais plein de promesses, dans lequel nous évoluerons désormais.

Références bibliographiques

[1] Hillson, D. and Murray-Webster, R., *Understanding and Managing Risk Attitude*, Gower, 2005.

[2] Stulz, R. M. (2008) 'Risk Management Failures: What Are They and When Do They Happen?', *Journal of Applied Corporate Finance*, 20(4), 58-67.

[3] K. Benabdeli., *Apport de la politique environnementale à l'amélioration de la gestion du risque industriel*. 1^{ères} journées nationales sur la sécurité industrielle et la gestion des risques majeurs Hassi Messaoud 26-27 mars 2007.

[4] Ezell, B.C., 2007. Infrastructure vulnerability assessment model (I VAM). *Risk Anal.* 27 (3), 571–583.

[5] B. Besson et J.C. Possin., « L'audit d'intelligence économique » - Mettre en place et optimiser un dispositif coordonné d'intelligence collective- Dunod 2^e édition août 2002.

- [6] *Geiben B, Nasset J J* Sécurité, Sûreté, la gestion intégrée des risques dans les organisations. *Éditions d'organisation* 1997.
- [7] R.V. Clark., L'expression espace défendable dans les technologies de la prévention situationnelle. Les « cahiers de la sécurité intérieure » N° 21 du 3 ième trimestre 1995.
- [8] Fischer, R.J., Halibozek, E., Green, G., 2008. Introduction to Security, eighth ed. Butterworth-Heinemann, Boston.
- [9] K. Benabdeli., Réhabilitation de quelques outils pour une amélioration des aspects environnementaux et cindyniques et impact sur la certification. Journée Scientifique : Les processus de certification et impact de l'environnement sur la santé. SH-HSE- Ain El Bya le 3 juin 2007
- [10] K. Benabdeli., L'audit environnemental en milieu industriel et son impact sur l'amélioration de la gestion des risques ». Journées Internationales sur les Risques Industriels Technologiques et Environnementaux. Skikda. 2006.
- [11] Rapport INERIS n° 46036 -02996A 20/12/2006 - Programme EAT-DRA 34 - Opération j -Intégration de la dimension probabiliste dans l 'analyse de risque - Méthode de quantification probabiliste dans l 'analyse de risques
- [12] G.Y. Kervern, P. Rubise P., L'archipel du danger : introduction aux cindyniques. Paris : Economica, 444 pages. 1991