



**HAL**  
open science

**MAR-A-III-50-31**

Eunika Mercier-Laurent

► **To cite this version:**

| Eunika Mercier-Laurent. MAR-A-III-50-31. 2016. hal-03494165

**HAL Id: hal-03494165**

**<https://hal.science/hal-03494165v1>**

Submitted on 12 Jan 2022

**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**  
open science

## Connaissances et maitrise de risques

Eunika Mercier-Laurent, Avril 2016

► **To cite this version:**

Eunika Mercier-Laurent, Avril 2016. Connaissances et maitrise de risques. AFNOR, BIVI chapitre OUTILS ET BONNES PRATIQUES, 2016. hal-03494165

**HAL Id: hal-03494165**

**<https://hal.archives-ouvertes.fr/hal-03494165>**

Submitted on 12 Jan 2022

**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.

Réunir un ensemble de connaissances, souvent multidisciplinaires est indispensable dans la prévention et la maîtrise des risques. Cet article passe en revue les risques actuels et les principales approches du Knowledge Management afin de démontrer le lien vital entre les deux domaines. Cet article s'adresse aux personnes impliquées dans la maîtrise de risques et la sûreté de fonctionnement.

## Connaissances et maîtrise des risques

---

*MERCIER-LAURENT Eunika –*

### 1 Typologie des risques

L'humanité a toujours été exposée à toutes sortes de risques : naturels, industriels, réglementaires, alimentaires et autres. Ils se sont amplifiés suite à la mondialisation et au changement climatique.

Parmi les risques industriels, on peut distinguer ceux engendrés par l'activité humaine (dysfonctionnement d'une installation, déraillement d'un train, chute d'un aéronef...) et ceux provoqués intentionnellement (sabotage, terrorisme, faits de guerre...).

Les risques issus de l'activité humaine comme les accidents majeurs, les défaillances de systèmes sociotechniques, la pollution de l'air ou de l'eau, la destruction des écosystèmes naturels ou le changement climatique sont souvent le résultat d'une non-anticipation ou d'une absence d'analyse de risque mais aussi du non-respect de l'environnement, ou de motivations comme l'égoïsme et l'envie de s'enrichir vite, ou encore de l'absence de professionnalisme. Les causes liées à ces risques peuvent être directes (comme la rupture d'une digue lors d'une inondation ou la perte de sources électriques d'une installation industrielle...) et trouvent fréquemment leur origine dans des causes plus profondes, souvent liées à des facteurs organisationnel ou humain (comme par exemple une politique de maintenance déficiente ou des procédures d'exploitation mal adaptées).

La fierté et le pouvoir peuvent aussi mener à des décisions irresponsables (exemple du crash de l'avion du gouvernement polonais à Smolensk en avril 2010).

Lors de la résolution des problèmes, la perpétuation de mêmes schémas mentaux constitue un risque de ne pas trouver la solution adaptée ou alternative, prenant en compte les exigences de sécurité/sûreté, l'impact environnemental et l'impact technico-économique, et s'avère un frein à l'innovation. Ainsi, au lieu de reproduire la logique informatique arborescente utilisée dans certains ordinateurs de bord de voitures, on peut donner un ordre direct en parlant sans passer

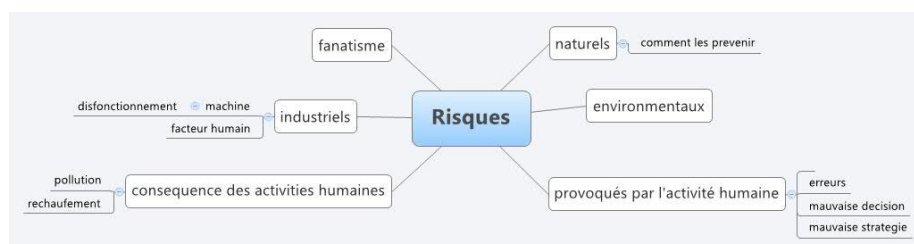
par des étapes intermédiaires. Une manipulation de l'arborescence à l'aide de la souris pendant la conduite peut entraîner un accident.

À ceci s'ajoutent des risques récents, qualifiés d'émergents et liés à l'utilisation des nouvelles technologies, à la numérisation, à la virtualisation, à la sécurité des données sensibles stockées sur des *clouds*, à l'impact des biotechnologies, des nanotechnologies et autres. Le principe de précaution est très souvent appliqué notamment quand le retour d'expérience sur l'impact (sur les éventuelles conséquences) n'est pas géré. Ce principe constitue cependant un frein à l'innovation.

Un autre risque peut venir des méthodes managériales, comme l'absence de management du capital intellectuel. En conséquence, certains savoir-faire ne sont pas exploités, car mal connus au niveau stratégique. Au sens de la norme **NF ISO 31000 :2010**<sup>1</sup>, tout risque de vol, de perte, d'obsolescence, de non-valorisation, de non-utilisation du savoir-faire apparaît de criticité élevée car amène une incertitude plus forte sur l'atteinte des objectifs.

La négligence de capitalisation de connaissances peut donc se trouver à l'origine d'accidents majeurs. On peut citer par exemple l'explosion d'un dépôt de carburant à Buncefield en 2005 (<http://www.buncefieldinvestigation.gov.uk/>), avec formation d'un nuage inflammable, allumage par une source confinée (*bang box explosion*), puis incendie important, comme si l'accident de Flixborough en 1974 se reproduisait et que ses enseignements n'avaient pas été pris en compte (Montmayeul, 2013).

La Figure 1.1 illustre les principaux types de risques.



**Figure 1.1** Une ontologie des risques

**Commentaire [gc1]**  
figure à traiter : en attente d'envoi par l'auteur

## 2 Le rôle des connaissances dans la maîtrise des risques

La connaissance des risques et de leurs causes possibles est primordiale dans la maîtrise des risques. Mais, de plus en plus, il s'agit d'aller au-delà de liens de causalité, prendre en considération la dimension humaine et la complexité grandissante dans une économie mondialisée. En effet, la mondialisation, renforcée par l'intensification des échanges commerciaux, grâce aux moyens de transport toujours plus variés et plus rapides, et par Internet et le commerce électronique a modifié la façon d'apprendre, de travailler et de faire des affaires et introduit de nouveaux risques.

À la recherche de la main-d'œuvre bon marché, les entreprises délocalisent leur production et le service client ce qui constitue un facteur de risque de pertes de connaissances et de non-satisfaction de clients. La production des pièces dans les pays où la main-d'œuvre est moins

<sup>1</sup> NE EN ISO 31000, Management du risque - Principes et lignes directrices, AFNOR, 2010

chère peut entraîner un risque de qualité des produits ou de services à cause du manque de savoir-faire local, du non-respect de spécifications ou de réglementations et l'utilisation de matériaux de remplacement pouvant dégrader les performances attendues. Produire à l'extérieur peut conduire en outre à une perte des connaissances sur le processus de fabrication, ce qui peut porter atteinte à l'existence même d'une entreprise. Une telle délocalisation peut en outre entraîner une perte d'emplois et donc de savoir-faire.

Les pertes de savoir-faire, de compétences clés pour l'entreprise ou les modifications d'organisation suite aux mutations internes, aux départs en retraite, aux démissions, au *turnover*, aux passages à la concurrence, à la délocalisation génèrent des impacts tels que la perte de temps à retrouver, réinventer et à refaire ce qui a été déjà fait, donc des surcoûts, une perte de compétitivité, de réactivité, des défauts de sécurité/sûreté, tous facteurs déterminants de différenciation dans une économie ouverte.

Face à la crise économique dans les pays développés, les gouvernements considèrent l'innovation comme le seul remède pouvant améliorer la croissance et impulser la création d'emplois. Mais l'entrepreneuriat exige la prise de risques et les connaissances nécessaires à la réussite d'une entreprise ne s'acquièrent pas qu'à l'école.

L'innovation porte souvent sur des parties techniques à haut degré de connaissances comme les réacteurs d'avion ou autres équipements complexes, tout en ignorant parfois l'ergonomie et l'intégration des facteurs humain et organisationnel en phase de conception, ainsi que les vrais besoins des utilisateurs et des clients. De ces failles, découle un risque de non-vente ou de non-utilisation.

Les technologies associées jadis à l'industrie sont maintenant présentes dans tous les domaines et leur développement s'intensifie. Elles sont de plus en plus embarquées. La vision des concepteurs des objets connectés, des équipements entièrement autonomes, de la communication M2M (*machine to machine*) ou des systèmes entièrement automatisés en support client peut entraîner un risque d'élimination de l'humain du circuit de la décision. Dans les systèmes semi-automatiques, le rôle de l'humain est de plus en plus réduit dans les phases d'exploitation. Si la machine pense pour nous, il y a un risque de perte de capacités cognitives (y compris le « savoir-penser »), d'incompréhension des processus et des phénomènes physiques.

Peut-on avoir une confiance totale dans ces systèmes et équipements entièrement autonomes ?

Internet, y compris les réseaux sociaux et autres services web 2.0, sont considérés désormais comme source de connaissances, mais la fiabilité des informations n'est pas garantie. Se reposer uniquement sur les connaissances glanées sur le web, et surtout sur les forums ou les réseaux sociaux, n'est pas suffisant. En outre, ces données, même sécurisées, sont exposées au risque d'intrusion et de piratage. Il convient de toujours vérifier leur justesse et leur pertinence avant toute utilisation.

### **3 Attendre et réagir ou prévenir et anticiper**

Il s'agit de deux attitudes bien différentes.

La première est une attitude réactive. Un événement indésirable survient et on s'efforce à agir le plus rapidement possible afin d'y remédier. Les connaissances sont alors indispensables pour résoudre au plus vite la crise et remettre le système en état de bon fonctionnement en toute sécurité/sûreté.

La seconde attitude est proactive et probabiliste, elle consiste à anticiper les événements indésirables avant qu'ils ne se produisent. Les connaissances sont alors nécessaires pour permettre la détection, le traitement et la mise en œuvre de solutions de prévention/protection.

Par exemple, pour faire face aux risques dans l'industrie, il est de rigueur de faire de la maintenance préventive, surveillance, inspections, et visites décennales pour les centrales nucléaires, les avions et autres équipements complexes, et de recueillir le retour d'expérience. Il est, en général, enregistré dans une base de données, validé au sens de la justesse et de la pertinence, traité, analysé et diffusé aux personnes concernées (Lannoy, Procaccia, 1994). Une telle base contient des données brutes. Les données analysées constituent des informations qui vont permettre de réaliser des études probabilistes de sûreté (*PSA : Probabilistic Safety Assessment*), d'optimiser les programmes de maintenance préventive ou de rédiger des bilans de comportement des équipements, d'analyser le vieillissement.

Ces informations sont-elles suffisamment fiables et permettent-elles de réduire les risques ? Est-ce que leur exploitation permet la découverte efficace de connaissances sur le comportement d'un équipement en exploitation dans un contexte donné ?

Dans quelques cas graves, comme par exemple, Fukushima, on gère la crise, alors que ce cas de figure aurait peut-être pu être appréhendé dans la phase de la conception. La gestion de crise traite les effets observés *a posteriori*, mais il est préférable de réunir toutes les connaissances associées en amont, afin de prévenir et anticiper d'éventuels accidents.

L'expérience pratique démontre que parfois un problème peut venir de signaux faibles souvent négligés. Il s'agit alors de glaner les connaissances, y compris celles du contexte, et vérifier leur cohérence, d'autant plus qu'elles proviennent souvent de plusieurs sources.

L'approche traditionnelle de la détection de signaux faibles associe des démarches expertes et de traitement de données, afin d'identifier le lien entre les données issues du retour d'expérience et un scénario de sensibilisation au risque défini comme signal faible. On représente ce dernier en s'appuyant sur des méthodes inductives ou déductives de la sûreté de fonctionnement, afin de comprendre les interactions entre les différents éléments du risque. Il faut y intégrer les dimensions facteurs organisationnel et humain aux dimensions techniques. L'identification des liens passe par les méthodes statistiques d'apprentissage ou par une mise en évidence par des experts ou des lanceurs d'alerte (Jouniaux et al, 2014).

Alors que la maintenance industrielle est en général organisée, celle des connaissances n'est pas de rigueur. Les connaissances jouent pourtant un rôle central dans nos activités. Mais quelles sont les connaissances, indispensables pour maîtriser les risques, comment les recueillir et modéliser dans l'ordinateur, quelles méthodes du raisonnement vont permettre à les exploiter efficacement ?

Tout dépend de la stratégie des organisations et des entreprises concernées. Ensuite, on utilisera des outils adéquats pour réaliser cette tâche. La démarche du *Knowledge Management* (KM) peut guider cette activité.

## 4 Qu'apporte le Knowledge Management ?

Au début des années 90, on a vu émerger une nouvelle méthode managériale – le *Knowledge Management* (KM) ou l'entreprise basée sur les connaissances (Drucker, 1992). Elle constitue le socle d'une nouvelle économie, celle de la connaissance (Amidon, 2005).

Le terme « Économie de la Connaissance » n'est pas récent. Bien qu'il ait été proposé dans les années 80, cette économie a toujours existé. Il s'agit de générer de la valeur à partir de connaissances telles que le savoir-faire et l'expérience. C'est un changement radical pour les entreprises qui doivent désormais comptabiliser l'immatériel, comme les compétences, l'image ou la réputation, entres autres (Mercier-Laurent, 2011).

Dans ce contexte, le *Knowledge Management* peut être défini comme l'ensemble des initiatives, méthodes et outils ayant pour objectif de construire un flux de connaissances

optimisé d'une organisation étendue aux partenaires, distributeurs et aux clients, afin de répondre à des enjeux de leadership, de performance industrielle, d'efficacité, de qualité et de sûreté.

Ce flux de connaissance comprend la création, la collecte, le traitement et le partage d'informations et de connaissances de façon organisée et optimisée, prenant en compte les différentes activités de l'entreprise étendue, les besoins, les motivations individuelles et collectives de tous les participants.

Deux principales démarches du Knowledge Management sont ascendante et descendante ou stratégique.

Une démarche ascendante commence en général par la résolution d'un problème donné, comme la capitalisation de connaissances pour un système d'aide à la décision en diagnostic, conduite de processus... et peut être ensuite étendue aux autres applications. L'objet de cette démarche est le savoir-faire applicable ou appliqué par l'entreprise ou l'organisation, pour son activité actuelle ou future. On s'intéresse aux savoir-faire importants ou critiques, détenus généralement par des experts et qui, dans la plupart des cas, ne sont pas formalisés. Alors que le transfert des connaissances a toujours été le champ d'action des formateurs, on ignore souvent que les connaissances peuvent être aussi « transmises » à l'ordinateur à l'aide d'interfaces et d'outils adaptés.

L'approche stratégique, peu utilisée en France, implique une réflexion au niveau du top management. Une comparaison de la situation courante et visée utilisant les KPI (*Key Performance Indicators*) élaborés à cet effet permet de définir les objectifs et les actions menant à leur accomplissement. Le management des connaissances associées aux risques fait alors partie des actions (Mercier-Laurent, 2011). Une telle démarche sera plus fructueuse, car elle associera les trois niveaux de management dans le même objectif.

Les différentes facettes du *Knowledge Management* pour la maîtrise des risques ont été abordées par l'IMdR (Institut pour la Maîtrise des Risques), entre autres dans le groupe « retour d'expérience technique » depuis le début des années 90 et dans deux colloques : « Knowledge Management et Maîtrise des Risques » du 5 juin 2007 (IMdR, 2007) et « Un enjeu pour aujourd'hui et demain : Maîtriser la connaissance » du 12 juin 2014 (Qualitique, 2014). Ce second colloque a été consacré aux enjeux de la gestion des connaissances et aux risques liés à la perte de connaissances (gestion absente ou déficiente des connaissances, perte de savoir-faire, non-identification de compétences clefs, non-utilisation, non-valorisation, mutations ou départs de personnel...) encourus par l'organisation. Quatre tendances principales ont été traitées dans ce colloque : la capitalisation des connaissances, les animateurs de communautés de pratiques, les méthodes et outils et enfin le retour sur investissement du **KM**.

L'étude prospective (Kahn et al, 2010) réalisée par l'IMdR insiste fortement sur la gestion des connaissances en matière de sûreté de fonctionnement et de maîtrise des risques. Il s'agit de garantir le maintien des connaissances et des compétences, malgré les difficultés citées ci-dessus et plus marquées actuellement : l'externalisation à cause des coûts de main-d'œuvre, la perte du métier d'ingénieur, le vieillissement du personnel. L'étude propose plusieurs types d'actions :

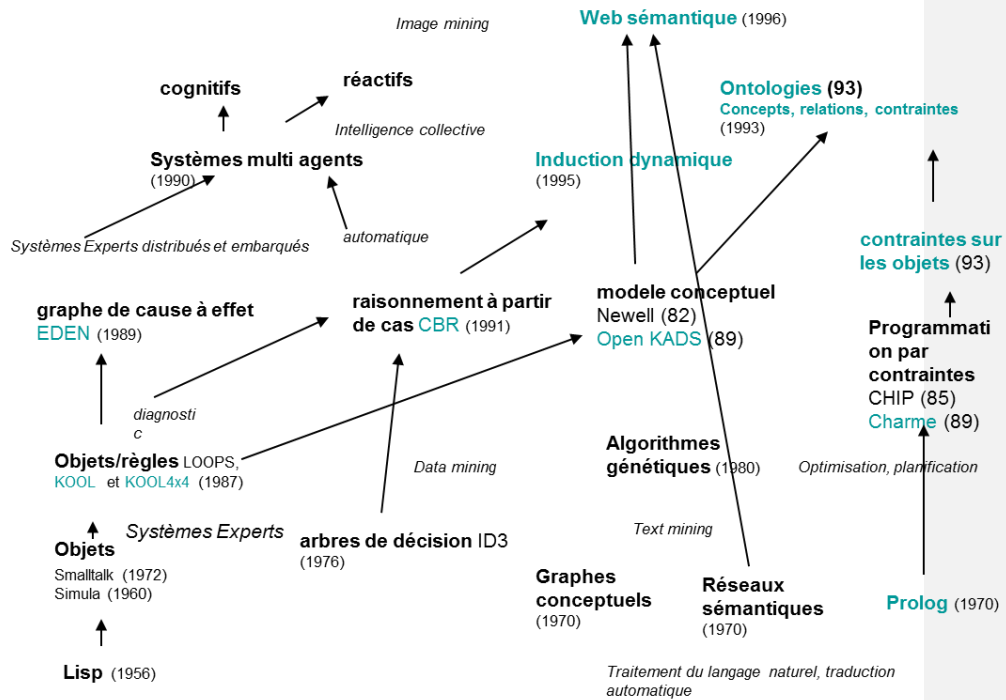
- développer un référentiel « sûreté de fonctionnement et maîtrise des risques » à partir des connaissances et de l'expérience acquises dans une entreprise donnée ;
- développer le concept de tutorat ou de compagnonnage dans les entreprises et une formation associée pour les futurs tuteurs ;

- développer l'investissement des entreprises dans le support de la formation et la R&D ;
- créer des modules de formation sur la sûreté de fonctionnement et la maîtrise des risques à mettre à disposition des entreprises, pour la formation ou la reconversion des personnels.

#### 4.1 Quelques techniques pour la modélisation et le traitement des connaissances

L'intelligence artificielle a inventé des méthodes et techniques pour traiter les connaissances par l'ordinateur. Ces méthodes et techniques de transfert, de modélisation de découverte et du traitement des connaissances ont été expérimentées avec succès depuis plus de 50 ans et sont désormais encapsulées dans les outils.

Une évolution dans le temps de ces techniques est présentée sur la Figure 4.1.



**Figure 4.1 Évolution des techniques de modélisation et du traitement des connaissances**

De nombreux systèmes d'aide à la décision ont été conçus pour assister les utilisateurs *via* les systèmes experts, d'aide à la conduite du processus, en diagnostic technique, médical ou organisationnel, d'aide à la conception, de raisonnement par analogie, de propagation des contraintes, de systèmes multi-agents et bien d'autres (AI4KM, 2014 et 2015). Ces techniques sont intégrées dans des outils facilitant la découverte, le transfert, la capitalisation et le traitement des connaissances par l'ordinateur. Les méthodes de modélisation des connaissances, comme des objets, des ontologies ou des cas facilitent non seulement leur préservation et partage, mais aussi une réutilisation pour une variété d'applications.



Rappelons qu'en maintenance industrielle, un diagnostic est un ensemble d'actions menées pour détecter une panne, la localiser et en identifier la cause (NF EN 13306, deuxième édition, 2010<sup>2</sup>). L'ensemble des connaissances acquises à partir de ce diagnostic, permet de pronostiquer un comportement futur. Le pronostic permet d'anticiper les situations potentiellement pénalisantes en termes de sûreté et de compétitivité, d'estimer une durée de vie résiduelle, de définir les actions de prévention/protection à prendre. Le pronostic dépend des informations disponibles du passé (le retour d'expérience, les inspections... mais aussi les connaissances disponibles), du présent (le diagnostic : le *health assessment*, l'état physique ou le bilan de comportement) et du futur (les conditions futures environnementales et d'exploitation - maintenance).

Le développement des méthodes basées sur les réseaux probabilistes en maîtrise des risques et sûreté de fonctionnement, dès le début des années 1990, a apporté une complémentarité dans le traitement de l'expertise. Les réseaux bayésiens, les réseaux de croyances, les réseaux évidentiels (VBS, Valuation Based Systems)... font appel à une représentation graphique des connaissances ce qui facilite leur compréhension. Elles sont bien adaptées au contexte d'incertitude (notamment l'incertitude épistémique) et généralisent des méthodes utilisées couramment par l'ingénieur en maîtrise des risques ou en sûreté de fonctionnement, comme l'arbre de défaillance ou le réseau bayésien. Les applications actuelles concernent l'analyse de risque, l'analyse de fiabilité, l'analyse du facteur humain (Sallak, 2013). Les réseaux bayésiens sont particulièrement utilisés en maîtrise des risques et leurs graphes sont une forme de représentation des connaissances. Il est possible d'introduire des variables d'action sur quelques nœuds critiques du graphe afin de mesurer les effets et donc l'efficacité. Les articles (Simon, Weber, 2013) publiés sur [Bivi\\*\\*http://www.bivi.maitrise-risques.afnor.org/\\*\\*](http://www.bivi.maitrise-risques.afnor.org/)<sup>3</sup> illustrent cette utilisation des connaissances.

Un dernier né de l'expérience et de la nécessité d'explorer de façon pertinente des gigantesques quantités de données est le *deep learning* qui connecte plusieurs techniques d'apprentissage automatique de machine (*machine learning*), comme le *data mining*, le *text mining*, utilisant les techniques de traitement du langage naturel (Blatter, Raynal, 2014) et *l'image mining*. Les techniques *Big data* permettent d'explorer les masses importantes de données générées, entre autres, par les services web, comme les réseaux sociaux, le commerce électronique, par les institutions publiques (par exemple Cordis), et par le *tracking* de joueurs ou autres navigateurs sur Internet (Jouniaux et al, 2014, Lejeune et al, 2014).

À ce stade une distinction entre la façon de penser « données » et « connaissances » doit être prise en compte. Alors que la première s'intéresse à la collecte de données et à leur validation, la seconde se concentre sur le recueil des connaissances indispensables à la résolution d'un problème donné dans son contexte. Elle permettra de choisir un outil adapté ou de construire une solution hybride pour traiter efficacement ce problème.

Le transfert de connaissances vers l'ordinateur *via* différents modèles de connaissances est maintenant maîtrisé et devrait être généralisé. De nombreuses bases de connaissances existent déjà en maîtrise des risques, mais le processus de capitalisation des connaissances n'est pas généralisé. Dans le domaine du vieillissement de systèmes, structures et composants de l'industrie de production nucléaire d'électricité, on peut citer la base GALL (US NRC, 2010) ou celles développées à l'heure actuelle dans le secteur nucléaire sur les propriétés des matériaux et en particulier sur les mécanismes de dégradation et leur cinétique (Qualitique, 2014). Dans le domaine de la fiabilité, il existe des bases de données de fiabilité (appelées aussi recueils de données de fiabilité) comme FIDES (2009) pour les composants électroniques, ou

<sup>2</sup> NF EN 13306, *Maintenance - Terminologie de la maintenance*, AFNOR, 2010

<sup>3</sup> Bibliothèque virtuelle Maîtrise des risques, AFNOR, 2016.

OREDA (6th edition, 2015) pour les composants mécaniques ou électromécaniques du secteur pétrolier.

Cependant le transfert de connaissances est très souvent mis sur le second plan, faute de temps ou sous-estimé par beaucoup d'entreprises. S'il paraît difficile pour certaines données et connaissances, comme les données d'inspection ou les connaissances d'experts, il peut être facilité par le choix judicieux des outils. Il demande néanmoins une motivation de la part de personnes concernées et notamment du décideur. La tendance du management des connaissances a remis la capitalisation au goût du jour.

## 4.2 Retour d'expériences des pratiques de management des connaissances

Depuis plus de deux décennies, des entreprises et organisations ont introduit des démarches du *Knowledge Management*, en partant de leurs motivations et de leur point de vue, soit intégrées dans leur stratégie, soit par le côté applicatif, comme le management du capital intellectuel, recueil et partage d'informations liées à l'Intelligence Économique ou encore par des applications métier ou informatiques (Mercier-Laurent, 2011).

De nombreuses entreprises ont entamé des démarches, mais, pour la plupart, sans prendre en compte le retour d'expérience de l'intelligence artificielle. Parmi les initiatives ayant pour objectif d'atténuer les risques liés à la connaissance et au retour d'expérience, on peut citer la création des réseaux d'experts (ou communautés de pratiques), le partage des bonnes pratiques, l'archivage et la sécurité des données notamment techniques.

Deux facteurs prépondérants freinent l'application du **KM** en tant que méthode managériale :

- l'envie de résultats rapides pour démontrer l'utilité de la démarche et le retour sur investissement ;
- l'incompréhension du rôle que le *Chief Knowledge Officer* doit jouer : il ne s'agit pas d'une position sociale, mais d'une animation transversale parfois à temps partiel et en parallèle avec d'autres activités.

Le **KM** intègre dans le processus les parties prenantes respectant une éthique dans un objectif de réussir ensemble. Il n'est pas facile à introduire car il implique de passer du temps à comprendre avant de faire, de penser « connaissances » et de modifier des attitudes : être plus à l'écoute au lieu de proposer des solutions « sur étagère », parfois sans avoir compris le problème. La collaboration à la place de la concurrence, le partage du retour d'expériences, l'estimation du retour sur investissement en termes d'immatériel, font partie des attitudes des « jardiniers de la connaissance ».

L'objectif initial du *Knowledge Management* reste cependant l'amélioration de la capacité à innover des entreprises et des organisations par une meilleure exploitation des talents, des connaissances, la détection d'opportunités, l'intégration du retour d'expérience et l'utilisation du meilleur des technologies.

## 4.3 Le management des connaissances appliqué à la maîtrise de risques

La prévention des risques implique une prise de conscience sur leur existence et leurs conséquences possibles, une aptitude en résolution de problèmes, une capacité de penser systémique pour comprendre des interactions et interinfluences dans des systèmes socio-techniques complexes et de réunir les connaissances indispensables pour prévenir, minimiser les causes, traiter en réduisant ou en supprimant l'impact. Si une telle approche avait été

appliquée dans le cas de Germanwings en mars 2015, on aurait pu éviter l'accident, car les connaissances sur la santé des employés et sur leurs relations font partie de la démarche globale.

Parmi les connaissances à préserver, il y a non seulement celles associées aux matériaux et équipements techniques complexes de longue durée de vie, comme les centrales nucléaires et leurs équipements, mais aussi celles liées à la capacité à résoudre un problème. Il s'agit de l'art de réunir les connaissances individuelles et collectives propres à la résolution d'un problème donné, tout en prenant en considération son contexte. La connaissance du contexte pèse toujours sur une décision. Prenons par exemple le risque de criminalité et de cybercriminalité. Résoudre ce problème ne consiste pas uniquement à trouver les coupables et les envoyer en prison, mais à comprendre les causes réelles et motivations des personnes concernées. Le récent colloque « Climat et défense : quels enjeux ? » organisé par le ministère de la Défense a démontré le lien entre le changement climatique et la criminalité. Par exemple, la sécheresse induite par le déboisement et les cultures intensifiées mène à l'épuisement de la terre, provoquant la famine, ce qui incite les plus vulnérables à revendre de la drogue ou à voler. Dans ce cadre, une modélisation conceptuelle des connaissances prenant en compte le contexte du problème à résoudre s'avère primordiale.

Une aide efficace peut être également apportée par les réseaux probabilistes qui stockent et traitent des informations de contexte et le retour d'expérience. Par exemple, en sciences humaines, en sociologie et en criminologie, la police de Zürich teste l'utilisation du logiciel Precobs (*Pre Crime Observation System*) pour prévoir les lieux probables de futurs cambriolages (Schindler, Wiedmann-Schmidt, 2015). En se basant sur 5 ans de statistiques policières, des données démographiques, des données des réseaux sociaux et quelques variables considérées influentes, le logiciel détermine les lieux de cambriolage les plus vraisemblables avec un taux de succès de 4/5. Ces statistiques complétées par les connaissances permettraient d'augmenter encore le taux de succès.

## 5 Que peut-on conseiller pour gérer les connaissances en maîtrise des risques ?

Finalement la démarche **KM** qui donne les meilleurs résultats en maîtrise de risques est celle qui commence par une application métier mais qui est élaborée avec une approche incrémentale : faire petit et penser grand. Elle permettra de construire un flux de connaissances composé de modules communiquant qui aideront efficacement les utilisateurs dans leurs activités en leur fournissant instantanément des connaissances pertinentes ou des suggestions de solutions déjà approuvées. L'accès pertinent aux connaissances et expériences collectives est particulièrement utile dans des cas d'entreprises mondialisées disposant de peu d'employés dans chaque filiale.

Dans le cas d'équipements à longue durée de vie, on assurera ainsi le bon fonctionnement en continu, même en cas de *turnover* et sans formation complémentaire des nouveaux arrivés.

En service client, plutôt que délocaliser et faire suivre par des employés une longue liste de questions à poser pour diagnostiquer le problème, on peut construire un système capable de répondre directement aux questions faciles et accompagner dans la résolution d'un problème faisant appel à l'expertise. Ceci assurera l'intégration du retour d'expérience d'une part pour une maintenance mieux adaptée ce qui diminuera le risque de perte de clients, d'autre part pour une utilisation future et donc ainsi anticiper les éventuels problèmes.

En conception, une démarche **KM** facilitera l'intégration du retour d'expérience pour éviter les risques de pannes. Elle facilitera aussi la gestion des différentes versions d'un système socio-technique et permettra l'optimisation de la logistique de soutien.

En maîtrise de risques, la capitalisation des connaissances ainsi qu'une prise en compte du contexte améliorera la détection des signaux faibles pertinents et d'autres facteurs non-techniques pouvant améliorer la décision, tout en renforçant la sûreté.

**En résumé**, une démarche adaptée du *Knowledge Management* renforcera la capacité à innover des entreprises, les rendra plus compétitives, plus durables, et moins vulnérables dans le contexte d'une hyperconcurrence mondiale.

Il reste à apprendre à évaluer les bénéfices de la démarche en termes de création de valeurs y compris immatérielles mais quelques propositions ainsi que des expériences sont déjà disponibles, comme l'évaluation du temps perdu à rechercher une solution déjà connue, de pertes de clients suite à un mauvais diagnostic, de fuites de compétences ou de détérioration de la réputation.

## 6 Quelques références

AI4KM (2014) Mercier-Laurent E., Boulanger D. (Eds), *Artificial Intelligence for Knowledge Management, Revised Selected Papers*, Springer IFIP AICT 422.

AI4KM (2015) Mercier-Laurent E., Owoc M.L., Boulanger D. (Eds), *Artificial Intelligence for Knowledge Management*, Springer IFIP AICT 469.

Amidon D., Formica P., Mercier-Laurent E. (2005), *Knowledge Economics : Emerging Principles, Practices and Policies*, Tartu University Press.

Blatter C., Raynal C., et al, (2014), *Méthodes d'analyse textuelle pour l'interprétation des rex humains, organisationnels et techniques*, Congrès λμ 19, Dijon, 21-23 octobre 2014.

*Climat et Défense : quels enjeux ?*, Conférence internationale de ministres et hauts responsables de la Défense, le 14 octobre 2015, Paris

*COP21 : Enjeux de la Défense*, Revue Défense Nationale, octobre 2015

Cordis, <http://cordis.europa.eu/>

Drucker P.(1992), *The New Society of Organizations*, Harvard Business Revue, September-October.

Duval C., Marle L., Paradowski V., Simon Ch., Weber Ph. (2014), *Exemples d'application des réseaux bayésiens*, AFNOR, MAR-A-III 10-82, janvier 2014.

IMdR (2007), Journée *Knowledge Management et Maîtrise des Risques*, 5 juin 2007, Paris, voir les actes de cette journée.

NF ISO 31000:2009, *Management du risque – Principes et lignes directrices*, AFNOR, 2010.

Jouniaux P., Hadida D., Dechy N., Marle L., et al, *Détection, pertinence et amplification des signaux faibles dans le traitement du retour d'expérience*, Congrès λμ 19, Dijon, 21-23 octobre 2014.

Kahn P., Lannoy A., Person-Silhol D., Vasseur D. (2010), *Anticipation, innovation, perception – Des défis pour la maîtrise des risques à l'horizon 2020*, Lavoisier, Editions Tec&Doc.

Lannoy A., Procaccia H. (1994), *Méthodes avancées de traitement et d'analyse des bases de données de retour d'expérience*, collection de la direction des études et recherches d'électricité de France, Eyrolles, 86.

Lejeune Y. (2014), *Big, fast & open data. Décrire, décrypter et prédire le monde : l'avènement des données*, Editions fyp.

Mercier-Laurent E (2011), *Les Ecosystèmes de l'Innovation*, Hermès Lavoisier, chapitres 4 et 5.

Montmayeul René (2013), *L'accident de l'usine chimique de Flixborough*, La mémoire vivante des catastrophes, Éditions Préventique, Bordeaux. Qualitique (2014), N° 256 p 6-7 et 9-53.

Sallak M. (2015), *Réseaux évidentiels (VBS, Valuation Based Systems) appliqués à la maîtrise des risques et à la sûreté de fonctionnement dans le domaine ferroviaire*, journée IMdR, Paris, 2 juin 2015.

Schindler J., Wiedmann-Schmidt W. (2015), *Im roten Bereich*, Der Spiegel 10/ 2015, <http://www.spiegel.de/spiegel/print/d-132040367.html>.

US NRC (2010), *Generic Aging Lessons Learnt (GALL) Report*, NUREG-1801 Revision 2.

Weber Ph, Simon Ch. (2013), *Réseaux bayésiens : méthodologies de modélisation en sûreté de fonctionnement*, AFNOR, MAR-A-III 10-81, octobre 2013.