Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision

Mohamed Habib Mazouni

▶ **To cite this version:**

Mohamed Habib Mazouni. Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision. Automatique / Robotique. Institut National Polytechnique de Lorraine - INPL, 2008. Français. NNT : . tel-00338938v1

HAL Id: tel-00338938

https://theses.hal.science/tel-00338938v1

Submitted on 14 Nov 2008 (v1), last revised 16 Feb 2009 (v2)

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.

Nancy-Université INPL

Ecole doctorale IAEM Lorraine

Département de Formation Doctorale en Automatique

Thèse

Présentée et soutenue publiquement le 13 Novembre 2008 pour l'obtention du :

Doctorat de l'Institut National Polytechnique de Lorraine

Spécialité Automatique, Traitement du Signal et Génie Informatique

Pour une Meilleure Approche du Management des Risques :

De la Modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision

Par :

Mohamed-Habib MAZOUNI

Composition du jury :

Rapporteurs : SCHON Walter Professeur Université de Technologie de Compiègne

BAYARD Mireille Professeur Université des Sciences et Technologies de Lille

Examinateurs : AUBRY Jean-François Professeur INPL

EL-KOURSI El-Miloudi Directeur de recherche INRETS-ESTAS

PETIN Jean-François Professeur Université Henri Poincaré Nancy 1

Membre Invité :

CAMBOU Bernard Directeur scientifique de l'INRETS

CRAN

Centre de Recherche en Automatique de Nancy

UMR 7039 - Nancy Université - CNRS

2, Avenue de la Forêt de Haye 54516 Vandœuvre-Lès-Nancy

Tél. +33 (0)3 83 59 59 59 Fax +33 (0)3 83 59 56 44

INTRODUCTION GÉNÉRALE

Contexte des travaux de recherche

Cette thèse a été engagée par l'Institut National de Recherche sur les Transports et leur Sécurité (INRETS) dans le cadre d'une collaboration entre l'Unité de Recherche « Evaluation des Systèmes de Transport Automatisés et leur Sécurité (ESTAS)» et le « Centre de Recherche en Automatique de Nancy (CRAN) » par l'intermédiaire du professeur J-F. Aubry, Directeur de nos travaux de thèse.

Le sujet était relatif au problème d'« Analyse Préliminaire de Risque (APR) », qui ne fait l'objet d'aucune norme générique, qui est déployée avec une grande variabilité dans les industries et qui pourtant est rendue obligatoire par certains règlements en vue de la délivrance d'autorisations d'exploitation. Ainsi, elle est un préalable à l'étude fiabiliste des systèmes instrumentés de sécurité qui est une des cibles de l'équipe projet « Systèmes Automatisés Contraints par la Sûreté et la Sécurité (SACSS) » du CRAN.

Après une année de recherche, le sujet a été revu et élargi de « l'analyse de risque dans le domaine ferroviaire » au « management des risques appliqué dans différents domaines industriels ». Ce changement de cap est motivé par deux raisons. La première, relative à l'élargissement du champ d'investigation, est due au fait que nous avons constaté que la problématique industrielle autour des questions abordées est quasiment toujours la même. La deuxième, relative au fait d'avoir fait porter l'étude sur le management des risques, vient du constat que l'APR est indissociable du reste du processus global de management des risques. Ainsi, nous la considérons comme la pierre angulaire du management des risques et par conséquent du Système de Management de la Sécurité (SMS). Le SMS reste l'une des priorités de l'UR ESTAS depuis le lancement du consortium SAMNET (Janvier 2003 – Décembre 2005) fédéré par l'INRETS en la personne de Monsieur El-Miloudi El-Koursi, Directeur de l'UR ESTAS et codirecteur de nos travaux de thèse.

Avant propos

Le 20éme siècle était le théâtre de nombreux changements. Désormais l'euphorie de l'ère industrielle est retombée, et le monde entier est confronté à un certain chaos exprimé par de nombreuses guerres régionales et de multiples catastrophes naturelles qui frappent un peu partout dans le monde. Cette évolution a vu s'éloigner une

fois pour toute l'illusion d'un monde idéal et a vu les concepts de risque et d'incertitude, de fiabilité et de sécurité prendre une part significative dans les esprits.

L'avancée technologique spectaculaire et la complexification des systèmes sociotechniques émergeants 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.

En outre, la mondialisation économique a engendré de nouvelles facettes de risque jusqu'alors ignorées ! Désormais, la survie de toute organisation socioéconomique, indépendamment de sa taille et de son facteur d'impact, est une variable aléatoire dans un système d'équations trop complexe de par ses facteurs hétérogènes peu maitrisés. Ainsi, la société d'aujourd'hui est contrainte d'améliorer continuellement et en permanence sa performance par des idées innovantes et une qualité de service captivante pour subsister face à la concurrence locale, régionale, nationale et internationale. En effet, dans cette course vers la continuité et la pérennité, le moindre risque inopiné peut mettre l'intégrité de la société en péril.

Ceci dit, la prise de risque est nécessaire, car risquer c'est d'abord oser courir le hasard en s'engageant dans une action qui pourrait apporter un avantage, mais qui comporte l'éventualité d'un danger. Marcel PAGNOL aurait dit : « Si vous voulez aller sur la mer, sans aucun risque de chavirer, alors, n'achetez pas un bateau : achetez une île ! », ce qui signifie dans un langage plus clair : « qui ne risque rien n'a rien » !

Le risque ne se rattache pas forcément à l'occurrence d'un événement malheureux ; il peut être une opportunité pour apprendre à mieux connaître les lacunes de la stratégie suivie par une société qui évolue vers ses objectifs tout en préservant son image de marque, sa qualité de service, et intrinsèquement l'ensemble des enjeux sociaux, économiques, techniques, financiers, juridiques, médiatiques, etc. Justement, le retour d'expérience est une perception intelligente de la notion de risque qui consiste d'ailleurs à tirer profit de l'occurrence de certains événements indésirables.

L'information stratégique est l'un des carburants de l'innovation. Elle revêt un caractère stratégique, et doit être intégrée dans une démarche globale de management des risques. On parle alors de Système de Mangement de la Sécurité (SMS) supportant des actions coordonnées visant à fournir, d'une manière proactive, la bonne information de sécurité, au bon moment et à la bonne personne.

Toutefois l'absence de stratégies organisationnelles et systémiques de management des risques à travers un SMS global, et le manque de partenariats techniques entres les différents acteurs du système global, sont deux précurseurs forts à l'apparition de nombreuses facettes du risque telles que :

- Les problèmes de sécurité, si les objectifs, les méthodes et les indicateurs de sécurité ne sont pas énoncés clairement, ou s'ils sont moins exigeants que ceux adoptés par d'autres parties partenaires.
- Les problèmes de disponibilité et de fiabilité, si l'approche de « production à moindre coût » gagne du terrain sur les exigences de sécurité et de qualité.
- Les problèmes de maintenabilité, si des logistiques de maintenance ne sont pas négociées au préalable avec les différents sous-traitants, comprenant contrats d'intervention et surtout des plans de qualification pour avoir plus d'autonomie.

- Les problèmes de fiabilité humaine pouvant générer des erreurs d'origine ergonomique, s'il n'y a pas de prise en compte des facteurs humains dès la phase de conception des systèmes à risques.
- Les problèmes de qualité, si les rôles et les responsabilités ne sont pas clairement énoncés, et qu'un Système de Management de la Qualité (SMQ) n'est pas mis sur pied avant le démarrage d'une quelconque activité.
- Les problèmes écologiques, si l'environnement n'est pas pris en compte durant tout le cycle de vie des activités à risque.

Certes, un dysfonctionnement ne doit jamais être vécu comme une faute ou un échec qu'il faut absolument dissimuler, mais plutôt comme un message d'ordre et de progrès que le système global nous transmet, et il incombe aux gestionnaires du SMS de décrypter ce message et apporter les corrections nécessaires pour faire en sorte que cela ne se reproduise plus. Cela passe forcement par un engagement sans équivoque, depuis le sommet, dans une stratégie globale de management de la sécurité.

Problématique industrielle

La sécurité est définie comme l'absence de risque non acceptable. Depuis quelques années, on a vu naître en Suède et puis en Suisse et dans d'autres pays le concept « vision zéro » qui s'est substitué à celui de « risque zéro » qui s'est avéré utopique. Dans une optique « vision zéro » on s'efforce à éliminer le maximum de risques résiduels y compris ceux qui sont en dessous du seuil de l'acceptabilité. Le seuil d'acceptabilité est généralement imposé par la réglementation ou bien précisé dans les référentiels de sécurité.

Malgré la richesse de la terminologie de la sécurité, les concepts de base souffrent d'une inquiétante fluctuation d'usage. Nous considérons que les divergences dans l'emploi des termes et les nuances des interprétations qui en découlent sont un frein au partage de connaissances et de savoir-faire en matière de sécurité. 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 relatives à des sous-systèmes réalisés par des sous-traitants disposant chacun de ses propres terminologie, méthode et savoir-faire.

En effet, les analyses de risque telles que l'APR, l'AMDEC, l'Arbre de Cause, l'Arbre d'Evénement, 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.

De ce qui précède, nous pouvons expliquer 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 préalablement élaborées qu'à des Systèmes Interactifs d'Aide à la Décision (SIAD).

Problématique scientifique

Le souci de généricité nous a conduits à élargir notre champ d'investigation et d'étude à divers domaines autres que le transport fondant leur analyse de risques sur des relations de causes à effets. Cette ouverture a été fortement recommandée par le professeur Jean-François AUBRY (CRAN). En effet, « l'accident se développe sémantiquement selon le même processus, seule la spécificité des circonstances et des conséquences le caractérise différemment en fonction du domaine d'étude (nucléaire, transport, machine, etc.) ou de la perception des risques encourus » (Mazouni M.-H. , 2007).

Pour ce faire, il était indispensable de converger vers un formalisme adapté de par sa généricité et adaptable de par sa réutilisabilité. Un objectif supplémentaire est d'éviter de brusquer les spécialistes dans leurs usages des concepts et de trouver un consensus permettant de rendre possible l'adoption d'une ontologie commune entre les différents acteurs impliqués dans les études de sécurité (constructeurs, exploitants, experts, administration, etc.).

Certes, la connaissance préalable du concept d'accident, de ses mécanismes de causalité ainsi que son processus de matérialisation est un gage à une meilleure identification des scénarios d'accident et une manière forte de consolider la défense afin d'empêcher leur survenance ou de réduire leur impact ou leur fréquence d'occurrence.

La définition d'un processus accidentel et la proposition de typologie des différents événements survenant avant chaque phase de ce processus, permettent de concevoir des barrières de sécurité primaire (barrière de protection) et notamment des barrières de sécurité secondaire (barrière de prévention) avant l'occurrence de ces événements. La décomposition de type état/transition permet d'intégrer l'aspect cinétique[1] des scénarios d'accident.

Après avoir tenté de voir clair dans les dédales du vocabulaire et essayé de replacer l'APR dans le concept englobant de management des risques, nous avons procédé à l'étude systématique des méthodes d'analyse de risque, déployées par différents acteurs issus de différents domaines, et mis en évidence les insuffisances et les contradictions. La difficile réutilisabilité des APRs réalisées par les différents fournisseurs d'équipements dans une analyse globale d'un système ferroviaire par exemple pose de nombreux problèmes à son constructeur.

L'objectif du travail a donc été de définir une approche générique de l'analyse de risque, qui soit appropriable par tout acteur d'un projet industriel et qui permette d'emboiter facilement les différentes analyses de ces acteurs pour construire le dossier global d'analyse de risque du système.

Pour atteindre cet objectif, une ontologie du risque a été définie 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. Elle permet de modéliser de façon systématique tout processus d'évolution dangereuse d'un système associé à un risque donné. Sur la base de ce modèle, la méthode « Management Préliminaire des Risques » proposée permet d'analyser systématiquement toutes les phases d'évolution du processus dangereux. Chaque utilisateur a la possibilité de définir la table de correspondance entre

[1] Cinétique : Vitesse d'enchaînement des événements constituant une séquence accidentelle

son propre vocabulaire et le vocabulaire de référence proposé et retrouvera les phases de sa démarche habituelle dans celles proposées par la méthode.

Bien entendu, une telle méthode n'a d'intérêt que si elle est outillée informatiquement. Un des objectifs de la thèse était de proposer un prototype d'outil logiciel support à la méthode. Sur proposition de l'INRETS, cet outil devrait faire l'objet d'un dépôt de brevet.

Organisation du mémoire

Dans le premier chapitre nous allons bien situer les différents concepts associés à la sécurité en regroupant les concepts en sous-ensembles ayant une forte dépendance causale.

Nous suivrons une démarche inductive dans la présentation des différents concepts. Chaque concept sera défini par ordre de priorité: définitions issues de la littérature, définitions proposées par des groupes de recherche spécialisés, définitions proposées par les normes génériques ou sectorielles, nationales, européennes ou internationales et enfin, le cas échéant, les définitions données par les réglementations nationales ou européennes.

En vue d'éliminer les nuances subsistant entre certains concepts, nous adopterons la technique de confrontation « versus », par exemple sécurité vs. fiabilité, risque vs. danger, etc.

Dans le cadre du deuxième chapitre, nous essayerons principalement de lever certaines ambigüités relatives aux activités de management des risques (appréciation, maîtrise, analyse, estimation, évaluation, etc.). Nous proposerons un processus de management des risques sous la forme d'une concaténation des propositions formulée dans les normes, en l'occurrence les guides ISO/CEI n°73 (ISO/CEI Guide 73, 2002) et n° 51 (ISO/CEI Guide 51, 1999) et la norme générique CEI 300-3-9 (CEI 300-3-9, 1995).

En effet, pour une meilleure fluidité de ce processus, nous présenterons une typologie et un panorama synthétique des différentes méthodes applicables en continuité de l'APR que nous considérons comme une pièce maitresse qui conditionne le succès de l'étude de sécurité.

Nous déplorerons dans le troisième chapitre le fait que l'APR ne fasse toujours pas l'objet d'un projet de normalisation ; ceci a induit toutes sortes de divergence. Nous essayerons d'en montrer quelques unes à travers un panorama de méthodes d'APR élaborées par des spécialistes du monde industriel.

L'étude méthodologique que nous avons pu réaliser dans ce chapitre va nous permettre ultérieurement, dans le quatrième chapitre de déceler les problèmes majeurs régissant conjointement la pratique de l'APR et du management des risques. Essentiellement, nous allons identifier 10 problèmes majeurs que nous essayerons de traiter dans le cadre des 3 derniers chapitres.

En effet, le cinquième chapitre se présente sous la forme d'un continuum de proposition de définitions de concepts liés à l'analyse de risques. La solution que nous proposerons repose sur le principe d'ontologie. Pour ce faire, nous allons suivre la démarche suivante : une partie de définition, ensuite une partie de synthèse et le cas échéant une partie de proposition. En outre, chaque concept est abordé en fonction de son aspect sémantique et de sa contribution dans le processus accidentel générique que nous proposerons. Donc, il ne s'agira pas d'un glossaire de termes présentés par ordre alphabétique.

Dans une démarche de résolution des problèmes constatés en matière de management des risques, nous proposerons une méthode nommée « Management Préliminaire des Risques (MPR)». Cette méthode itérative est basée sur l'ontologie générique proposée dans le cinquième chapitre. Principallement elle se déroule en plusieurs phases allant du découpage systémique du système global en des entités élémentaires jusqu'à l'identification inductive des scénarios d'accident en passant par une phase déductive d'identification des associations accidentogènes des sources et des cibles de danger en se basant essentiellement sur le retour d'expérience et les bases de données d'expértise.

La démarche MPR est conforme aux définitions normatives du management des risques que nous allons aborder en détail dans le deuxième chapitre. Ainsi, nous retrouverons la phase d'identification des scénarios d'accident, la phase d'estimation des risques, la phase d'évaluation des risques, et la phase de maitrise des risques.

Enfin, la méthode MPR se rattache au Système de Management de la Sécurité (SMS) par le point d'ancrage essentiel qu'est la gestion des processus techniques et organisationnels.

Certes, la proposition d'un système interactif et ergonomique d'aide à la décision pour le management préliminaire des risques présente un intérêt incontestable. Justement, dans le cadre du septième et dernier chapitre, nous présenterons SIGAR (Système Informatique Générique d'Analyse de Risque). SIGAR est un outil générique dédié à la méthode MPR conçu sur une base de données dédiée. Il est doté d'une interface graphique permettant aux utilisateurs de naviguer à travers ses menus graphiques interactifs et d'exprimer en langage habituel leurs besoins en informations et données via la saisie de formulaires sans être obligatoirement spécialistes de l'informatique et des langages de requêtes.

Ce mémoire de thèse s'achèvera par une conclusion générale dans laquelle nous repositionnerons l'ensemble de nos développements en regard des objectifs initiaux de l'étude. Enfin, nous aborderons naturellement une discussion sur les perspectives de travail qui découlent de cette thèse.

TABLE DES MATIÈRES DU CHAPITRE 1: SÉCURITÉ DES SYSTÈMES

Chapitre 1

SÉCURITÉ DES SYSTÈMES

Depuis de nombreuses décennies, la sûreté de fonctionnement (Dependability) et plus particulièrement la sécurité (Safety) sont devenues des enjeux cruciaux à la survie des sociétés. Cette considération repose essentiellement sur le concept de risque.

L'évaluation de la sécurité est un exercice crucial qui ne peut être intègre sans l'apprentissage des mécanismes de matérialisation des risques car la compréhension du risque est une manière forte de consolider la défense et d'optimiser, d'organiser et de mieux orienter les études de management des risques.

Dans ce premier chapitre nous allons bien situer les différents concepts associés à la sécurité en regroupant les concepts en sous-ensembles ayant une forte dépendance causale, à l'image de danger et phénomène dangereux ou bien dommage et conséquence. Nous adopterons une démarche inductive dans la présentation des différents concepts. Chaque concept est présenté de la manière suivante :

- Présentation des différentes définitions en commençant par le sens littéraire (Larousse, Grand Robert, etc.), ensuite les définitions distinguées proposées par des experts de la sûreté de fonctionnement, suivie de celles proposées par des groupes de recherche (AQS-GT OORS, Mars 1996) (GT 7 - CEI) (GT Aspects sémantiques du risque, 1997) (GTR 55, 2000) (GT Méthodologie, 2003). Nous poursuivons avec les définitions proposées par les normes nationales françaises (NF) ou britanniques (BSI), européennes (NF EN, BSI EN, etc.) ou internationales (CEI, ISO, etc.) et enfin, le cas échéant, nous terminons avec les définitions issues de la réglementation nationale ou communautaire (directive européenne, loi, décret, arrêté, etc.).
- Synthèse visant à déceler les divergences et les points communs des définitions rapportées. Nous serons parfois amenés à commenter certaines incohérences ou contradictions.

- Proposition d'une définition si aucune des définitions rapportées ne mérite d'être adoptée pleinement.

1 Sécurité (Safety)

Définitions :

SOURCE	
(Larousse, 2006)	Situation, état dans lesquels on n'est pas exposé au danger. Tranquillité d'esprit inspirée par la confiance, pas le sentiment de n'être pas menacé.
(Larousse, 2005)	Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration : Cette installation présente une sécurité totale.
(AQS-GT OORS, Mars 1996)	La sécurité d'entreprise est l'état de confiance individuel ou collectif, raisonné, conditionnel, ressenti comme tel vis à vis des dangers encourus et des risques associés reconnus comme acceptable.
(GT Aspects sémantiques	La sécurité est l'ensemble des dispositions prises pour éviter ou réduire les risques.
(ISO/CEI Guide 2, 1986)	Absence de risque de dommage inacceptable.
(ISO/CEI Guide 51, 1999)	Absence de risque inacceptable.
(CEI 50(191), 1990)	La sécurité est l'aptitude d'une entité à éviter, dans des conditions données, des événements critiques ou catastrophiques.

Synthèse : D'après les définitions précédentes, la sécurité est en général associée à l'absence de risque inacceptable. Il y a 20 ans, en l'occurrence dans la norme ISO/CEI Guide 2, le concept de sécurité était associé à la gravité des dommages : « La sécurité est l'absence de risque de dommage inacceptable » (ISO/CEI Guide 2, 1986). Cette forte corrélation sécurité/gravité a été ensuite pondérée avec la probabilité d'occurrence : « La sécurité est l'absence de risque inacceptable » (ISO/CEI Guide 51, 1999).

Proposition : La sécurité est l'absence de danger ou de conditions susceptibles de créer un risque inacceptable. C'est aussi la mesure d'un niveau de confiance vis-à-vis de l'acceptabilité d'un risque.

Avant de revenir sur les concepts de danger et de risque que nous venons d'introduire, nous proposons de bien cadrer le concept de sécurité et les activités associées par rapport à d'autres et notamment la sûreté de fonctionnement (SdF).

1.1 Sécurité vs. Sûreté de Fonctionnement

Le fonctionnement d'une entité est le succès de la « mission » qui lui a été assignée. Souvent on parle de « fonction requise » qui se définit selon la norme CEI 50(191) (CEI 50(191), 1990) comme une fonction ou un ensemble de fonctions d'une entité dont l'accomplissement est considéré comme nécessaire pour la fourniture d'un service donné.

Citons quelques définitions de le SdF extraites de documents de référence :

Définitions :

SOURCE	
(AQS-GT OORS, Mars 1996)	Ensemble de dispositions concrètes (organisation, procédures, moyens...) visant à éviter la surprise vis à vis des dangers et à limiter les dégâts en cas de dysfonctionnements.
(GT 7 - CEI)	Ensemble de techniques et de méthodes permettant d'atteindre la sécurité.
(ISO/CEI Guide 51, 1999)	La Sûreté de Fonctionnement est la science des défaillances. Elle recouvre les concepts de fiabilité, disponibilité, maintenabilité et de sécurité.
(CEI 50(191), 1990)	Ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent : fiabilité, maintenabilité et logistique de maintenance.
(CEI 61069, 1996)	La sûreté de fonctionnement se décompose en disponibilité et crédibilité, la première comprenant fiabilité et maintenabilité et la seconde intégrité et sûreté. La crédibilité est la mesure dans laquelle un système est capable de reconnaître et signaler son état et de résister à des entrées incorrectes ou des accès non autorisés. Quant à l'intégrité, elle se définit comme l'assurance fournie par un système que les tâches seront correctement accomplies à moins que le système ne prévienne que l'un quelconque de ses états pourrait conduire à une situation contraire.

Synthèse: Ces définitions divergent relativement entre deux tendances. On peut dire d'une part que la sûreté de fonctionnement (Dependability) n'est pas un but en soi, mais un moyen ou un ensemble de moyens (démarches, méthodes, outils, etc.) permettant de maitriser les risques. Autrement dit, la maitrise des risques est le but, la sûreté de fonctionnement est un moyen permettant de l'atteindre. Selon Y. Mortureux (Mortureux, 2002): « C*'est un atout majeur du concept de la sûreté de fonctionnement de réunir des approches motivées par la fiabilité, la disponibilité, la maintenabilité et la sécurité, mais c'est un piège de vouloir réduire à une valeur le résultat de ces démarches* ». Selon Heurtel (Heurtel, 2003), la sûreté de fonctionnement (SdF) se définit comme une activité d'ingénierie qualitative et quantitative, une riche palette de méthodes et de concepts au service de la maitrise des risques.

D'autre part et plus formellement elle est présentée comme un ensemble de paramètres mesurables par des approches probabilistes. Parmi les plus connus, citons les espérances mathématiques (E.M) des variables aléatoires temporelles associées aux défaillances et réparations d'un système :

- **MTTF (Mean Time To Failure)** : E.M. de la durée de bon fonctionnement avant l'apparition de la première défaillance, Notons que le taux de défaillance λ (voir §1.2) lorsqu'il est constant est tel que MTTF = 1/λ
- **MTTR (Mean Time To Repair)**: E.M. de la durée de réparation,
- **MUT (Mean Up Time)**: E.M. de la durée de bon fonctionnement,
- **MDT (Mean Down Time)**: E.M. de la durée d'indisponibilité,
- **MTBF (Mean Time Between Failures)**: E.M. de la durée entre deux défaillances consécutives.

Proposition : Nous proposons de conserver le vocable SdF pour la caractérisation probabiliste et de parler d'ingénierie de la SdF à propos de l'ensemble des activités visant l'amélioration de la SdF.

1.2 Sécurité vs. Fiabilité

L'objectif des études prévisionnelles de fiabilité (Reliability) d'un système est d'évaluer différentes architectures possibles pour ce système en comparant leurs performances au moyen de données statistiques (Sallak, Simon, & Aubry, 2007).

Selon la norme CEI 50(191) (CEI 50(191), 1990), la fiabilité est l'« *Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné* ». Ceci en supposant que l'entité est en état d'accomplir la fonction requise au début de l'intervalle de temps donné. La cessation de cette aptitude est l'événement « défaillance » de l'entité.

La fiabilité est généralement mesurée par la probabilité R(t) que l'entité accomplisse ses fonctions requises de l'instant *0* à l'instant *t*:

R(t) = P(E non défaillante sur [0, t]), tel que : E : entité considérée, [0, t] intervalle de temps donné.

Par définition, le taux de défaillance est tel que λ.dt est la probabilité pour que la défaillance de l'entité intervienne entre les instants t et t+dt, sachant qu'elle n'est pas encore survenue à l'instant t. Si λ est constant, alors R(t) = exp (-λt). Cependant, le taux de défaillance λ varie en général avec le temps dans une forme dite en baignoire (voir FIG. 1) :

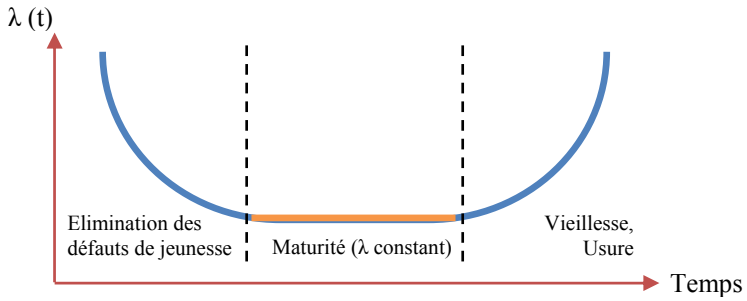


FIG. 1: Evolution du taux de défaillance d'un composant

Jusqu'ici, nous n'avons pas considéré la conséquence de la défaillance. Si la défaillance de l'entité est susceptible de produire un danger, alors on parle de défaillance dangereuse, dans le cas contraire, on parle de défaillance « sûre » (NF EN 61508, Décembre 1998). La sécurité étant l'absence de danger, la probabilité de

défaillance sûre peut donc être considérée comme caractérisant la sécurité de l'entité. Ainsi, la sécurité peut être considérée comme la partie de la fiabilité relative aux défaillances sûres. En pratique, on s'attachera plutôt à identifier exhaustivement et à évaluer les défaillances dangereuses.

1.3 Sécurité vs. Disponibilité : ou les effets pervers de l'ultra-sécurité

Selon la norme CEI 50(191) (CEI 50(191), 1990), la disponibilité (Availability) dépend de la fiabilité, de la maintenabilité et de la logistique de maintenance. C'est aussi l'« *aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée* ». Cette définition est conforme à celle de la norme CEI 61069 (CEI 61069, 1996). Y. Mortureux (Mortureux, 2002) ajoute que : « *La disponibilité est une synthèse de la fiabilité et la maintenabilité ; c'est la proportion du temps passé en état de remplir les fonctions requises dans des conditions données* ».

La disponibilité est généralement mesurée par la probabilité A(t) d'être en état, à l'instant *t*, d'accomplir les fonctions requises : A(t) = P(E non défaillante à l'instant t).

La sécurité et la disponibilité sont deux concepts souvent difficiles à concilier. En effet, comme il est impossible de garantir une probabilité nulle pour les défaillances dangereuses, on s'efforce de les détecter au plus vite et d'enclencher les moyens visant à empêcher leur propagation. Souvent, ces moyens ont pour effet de réduire la disponibilité de la fonction assurée, voir de l'interrompre (par principe de précaution par exemple).

Dans certains domaines tels que les transports guidés, l'application du principe de sécurité « Vision zéro » (voir introduction générale) oppose très souvent les équipes de sécurité et d'exploitation. La première cherchant à éviter le moindre risque, l'autre ayant pour vocation d'éviter les retards provoquant une concentration de masses de voyageurs sur les quais, ce qui peut être à l'origine de mouvements de foules, ou de panique, pouvant causer la chute de passagers sur la voie.

Certes, le concept de sécurité ne prime pas d'une manière triviale sur la disponibilité mais il est plutôt perçu comme une approbation ou un gage à une « disponibilité » optimale (respectant la contrainte sécuritaire) et non pas maximale.

1.4 Sécurité vs. Maintenabilité

La maintenabilité (Maintainability) est l'aptitude d'une entité à être remise, par une maintenance donnée, en état d'accomplir des fonctions requises dans des conditions données. Selon la norme CEI 50(191) (CEI 50(191), 1990): « *dans des conditions données d'utilisation, aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits* ».

La maintenabilité se mesure par la probabilité M(t) d'être en état, à l'instant *t*, d'accomplir ses fonctions requises sachant qu'elle était en panne à l'instant *0*:

M(t) = P (E est réparée sur [0, t]) E : entité considérée, [0, t] intervalle de temps donné.

Si le taux de réparation μ est constant, alors M(t) = exp (-μt).

La norme CEI 50(191) (CEI 50(191), 1990) donne une définition relative à la logistique de maintenance (Maintenance support performance) qui est : « *Aptitude d'une organisation de maintenance à fournir sur demande, dans des conditions données, les moyens nécessaires à la maintenance d'une entité conformément à une politique de maintenance donnée* ».

Une meilleure maintenabilité est un gage à une meilleure sécurité. Généralement, les équipements de sécurité sont conçus avec une bonne fiabilité et avec des capacités de tolérance aux fautes par recours à des redondances. Souvent, on retrouve des architectures « 2 parmi 3 » permettant de reconfigurer vers un état relativement moins sûr afin d'assurer un mode dégradé en cas de défaillance ou panne du composant principal. La restauration du mode nominal dépend de la maintenabilité de ce composant. Ainsi le concept d'intégrité de sécurité en sécurité fonctionnelle s'apparente à la disponibilité de la fonction sécurité et est donc largement tributaire de la maintenabilité (NF EN 61508, Décembre 1998).

Par ailleurs, dans un système de production, les procédures de maintenance se déroulent parfois avec précipitation sous l'influence du facteur de disponibilité ; ceci amène à shunter certaines consignes de sécurité et par conséquent prendre délibérément un risque inutile !

Il convient donc de veiller, dans le cadre du Système de Management de la Sécurité, sur le respect des procédures de sécurité de telle sorte que toute transgression soit réprimée.

1.5 Sécurité vs. Sûreté

Il ne faut pas confondre sûreté de fonctionnement (Dependability) et sûreté (Security) dans le sens large du terme.

Selon la norme CEI 61069 (CEI 61069, 1996), la sûreté est : « *l'assurance fournie par le système de sa capacité à refuser toute entrée incorrecte ou tout accès non autorisé et à pouvoir éventuellement en informer* ».

Pour les systèmes informatiques, J.-L. Laprie (Laprie, 1994) (Laprie, 2002) distingue entre sécurité innocuité (biens et personnes) et sécurité confidentialité. La première se rapproche du sens général de sécurité (Safety en anglais), alors que la seconde se rapproche du terme sûreté de la norme CEI 61069.

Dans le cadre des Installations Classées pour la Protection de l'Environnement (ICPE), on parle de sécurité des installations vis-à-vis des accidents et de sûreté vis-à-vis des attaques externes volontaires, des intrusions malveillantes et de la malveillance interne. Selon le GT méthodologie (GT Méthodologie, 2003), l'expression « sûreté de fonctionnement » dans les installations classées, se rapporte plutôt à la maîtrise des risques d'accident, donc à la sécurité des installations. Evidemment, ces nuances peuvent rendre difficile et atypique la définition des objectifs de sécurité et/ou de sûreté de fonctionnement.

2 Notions de danger et de phénomène dangereux

2.1 Danger

Définitions :

SOURCE	
(AQS-GT OORS, Mars 1996)	Etat ou situation comportant une potentialité de dommages.
(GT Méthodologie, 2003)	La notion de danger définit une propriété intrinsèque à une substance (ex : butane, chlore), à un système technique (ex : mise sous pression d'un gaz), à une disposition (ex : élévation d'une charge), à un organisme (ex : microbes), etc., de nature à entraîner un dommage sur un « élément vulnérable ». Sont ainsi rattachées à la notion de « danger » les notions d'inflammabilité ou d'explosivité, de toxicité, de caractère infectieux etc., inhérentes à un produit et celle d'énergie disponible (pneumatique ou potentielle) qui caractérisent le danger.
(BSI OHSAS 18001, 2005)	Situation, condition ou pratique qui comporte en elle-même un potentiel à causer des dommages aux personnes, aux biens ou à l'environnement. Une source ou une situation pouvant nuire à par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments.
(CEI 300-3-9, 1995)	Source potentielle de dommage.
(NF EN 61508, Décembre 1998)	Le danger désigne une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.
(Directive 96/82/EC (SEVESO II), 9 décembre 1996)	La propriété intrinsèque d'une substance dangereuse ou d'une situation physique de pouvoir provoquer des dommages pour la santé humaine et/ou l'environnement.

Proposition : Le danger se définit comme une propriété intrinsèque inhérente à un type d'entité ou un type d'événement qui a la potentialité de provoquer un dommage.

2.2 Phénomène dangereux

Définitions :

SOURCE	
(GT Méthodologie, 2003)	Libération d'énergie ou de substance produisant des effets susceptibles d'infliger un dommage à des cibles (ou éléments vulnérables) vivantes ou matérielles, sans préjuger l'existence de ces dernières.
(ISO 14971, 2000), (CEI 300-3-9, 1995), (EN 292/ISO 12100, 1995)	Source potentielle de dommage.

Synthèse : Dans la norme ISO 14971 relative à la « gestion du risque pour les dispositifs médicaux », le terme *phénomène dangereux* a été défini exactement de la même façon que la notion de *danger* dans la CEI 300-3-9.

Proposition : Un phénomène dangereux est un processus de matérialisation de danger. Cette concrétisation produit des effets (dispersion d'un nuage de gaz toxique, dérapage d'une voiture, etc.).

3 Notions de dommage et de conséquence d'accident

3.1 Dommage

Définitions :

SOURCE	
(Larousse, 2006)	Préjudice ou dégât causé à quelqu'un, à quelque chose.
(GT 7 - CEI)	Préjudice causé par un système à son environnement passif conduisant à une diminution de l'intégrité physique des personnes ou de la valeur initiale des biens ou des équipements.
(GT Aspects sémantiques du risque, 1997)	Effets néfastes d'un événement pour les personnes, la société, ou l'environnement.
(ISO/CEI Guide 51, 1999)	Blessure physique ou une atteinte à la santé des personnes ou dégât causé aux biens ou à l'environnement.

(NF EN 61508, Décembre 1998), (CEI 1050, Février 1991)	Blessure physique ou atteinte à la santé affectant des personnes soit directement soit indirectement comme conséquence à un dégât causé aux biens ou à l'environnement.

Synthèse : La notion de dommage (Harm) est relativement définie de la même façon dans la norme ISO 14971 (2000), la norme générique CEI 300-3-9 (1995), le guide ISO/CEI 51 (1999) et bien d'autres référentiels.

Proposition : La notion de dommage caractérise les préjudices matériels, moraux ou environnementaux, directs ou indirects, immédiats ou différés, involontaires ou délibérés.

NB. Les dommages différés sont généralement qualifiés de détriments. On parle par exemple de dommage sanitaire et de détriment écologique.

3.2 Conséquence

Définitions :

SOURCE	
(Larousse, 2006)	Conclusion déduite d'un principe, d'un fait.
(GT Méthodologie, 2003)	Combinaison, pour un accident donné, de l'intensité des effets et de la vulnérabilité des cibles situées dans les zones exposées à ces effets. Elles s'expriment en définissant la nature et la gravité des atteintes portées à celles-ci ».
(ISO/CEI Guide 51, 1999)	Résultat d'un événement. Il peut y avoir une ou plusieurs conséquences d'un événement. Les conséquences peuvent englober des aspects positifs et des aspects négatifs. Cependant, les conséquences sont toujours négatives pour les aspects liés à la sécurité. Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Proposition: Nous proposons que la notion de conséquence soit liée aux aspects négatifs contraires à la sécurité. Les conséquences d'un accident englobent l'impact des dommages qu'il a causés sur l'ensemble des enjeux socioéconomiques (techniques, financiers, commerciaux, juridiques, médiatiques, etc.).

4 Notions de gravité, de fréquence d'occurrence et d'exposition

4.1 Gravité

Proposition : Le terme gravité (Severity) se dit de l'importance des choses. C'est le caractère de ce qui est important, de ce qui ne peut être considéré avec légèreté, de ce qui peut avoir des suites fâcheuses. La gravité caractérise globalement l'ensemble des conséquences parmi différentes classes d'importance. Cette classification est effectuée généralement par des experts.

Il convient de définir un nombre pair de classes de gravité par soucis d'éviter la tendance de retenir la position médiane d'une classification impaire. Il convient aussi de choisir des termes révélateurs et distinctifs afin d'éviter les mauvaises interprétations en cas d'audit ou de demande d'avis d'experts. En effet, certains préfèrent tout simplement numéroter les classes de gravité (niveau 0, niveau 1, niveau 2, niveau 3).

Dans le domaine du risque professionnel, la gravité concerne essentiellement les préjudices portés à l'Homme. Ceci amène à définir des échelles de gravité dans la forme suivante (voir TAB. 1) :

TAB. 1 : Echelles de gravité selon la norme ISO 14971 (ISO 14971, 2000)

Gravité	Signification
Négligeable	Incident n'exigeant aucun acte médical
Minime	Légères blessures relevant des premiers soins (ne nécessitant pas un traitement médical)
Mineure	Blessures ou maladies mineures nécessitant un traitement médical
Majeure	Blessures ou maladies graves, infirmité permanente
Catastrophique	Décès d'une ou plusieurs personnes

Dans la majorité des domaines industriels, la gravité couvre aussi bien les dommages sur l'Homme et le Système, que les nuisances portées à l'Environnement. La norme ferroviaire NF EN 50126 propose quatre échelles de gravité (voir TAB. 2) :

TAB. 2 : Echelles de gravité selon la norme NF EN 50126 (NF EN 50126, Janvier 2000)

Gravité	Conséquences pour les personnes ou l'environnement	Conséquences pour le service
Insignifiant	Eventuellement une personne légèrement blessé	
Marginal	Blessures légères et/ou menace grave pour l'environnement	Perte d'un système important
Critique	Un mort et/ou une personne grièvement blessée graves et/ou des dommages graves pour l'environnement	Dommages graves pour un (ou plusieurs) système(s)
Catastrophique	Des morts et/ ou plusieurs personnes gravement blessées et/ou des dommages majeurs pour l'environnement	Dommages mineurs pour un système

Néanmoins, à l'image d'autres normes génériques voire même sectorielles, l'échelle de gravité de la NF EN 50126 ne fait pas l'unanimité auprès des spécialistes du monde ferroviaire qui ont tendance à l'adapter en fonction de leur propre perception du risque des enjeux majeurs les concernant. A titre d'exemple, l'échelle de gravité (voir TAB. 3) adoptée dans le cadre de l'APR du système de contrôle/commande ERTMS[1] (GTR 55, 2000), est une adaptation de la matrice de gravité proposée par la norme NF EN 50126 (voir TAB. 2):

TAB. 3 : Adaptation des échelles de gravité de la norme NF EN 50126

Gravité	Conséquences pour les personnes ou l'environnement	Conséquences pour le service
Insignifiant		Dommages mineurs au système
Marginal	Un blessé léger et/ou une menace significative de l'environnement	dommages sévères au système
Critique	Un blessé grave et/ou un dommage significatif à l'environnement	perte du système
Catastrophique	Un ou plusieurs morts et/ou blessés graves et/ou des dommages majeurs à l'environnement	

Pour mesurer la gravité d'un accident nucléaire, plus de cinquante pays ont adopté l'échelle internationale des événements nucléaires (INES, de l'anglais *International Nuclear Event Scale*). INES comporte 8 niveaux classés de 0 à 7 (voir TAB. 4) :

TAB. 4 Echelle internationale de gravité des événements nucléaire (Wikipédia, 2008) (Bouchet, 2001)

Type	INES	Incidence hors site	Incidence sur site	Dégradation de la défense en profondeur	Exemple
Accident majeur	**7**	Rejet majeur : effet étendu sur la santé et l'environnement.			1986, Explosion de la centrale de Tchernobyl en Ukraine.
Accident grave	**6**	Rejet important susceptible d'exiger l'application intégrale des contre-mesures prévues.			1957, Explosion à l'usine de retraitement de Kyshtym en URSS. 1969, fusion du cœur à la centrale nucléaire de Lucens.
Accident (entraînant un risque hors du site)	**5**	Rejet limité susceptible d'exiger l'application partielle des contre-mesures prévues.	Endommagement grave du réacteur ou des barrières biologiques.		1979, Fusion partielle du coeur du réacteur à Three Mile Island aux Etats-Unis. 1957, Incendie de Sellafield.
Accident (n'entraînant pas de risque important à l'extérieur	**4**	Rejet mineur: exposition du public de l'ordre des limites prescrites.	Endommagement important du réacteur ou des barrières biologiques, ou	(perte des défenses et contamination)	1999, Accident de criticité de Tokaimura au Japon. 1973, Rejet à

[1] ERTMS : *European Rail Traffic Management System*

du site)			exposition létale d'un travailleur.		Windscale. 1980, Endommagement du cœur de la Centrale nucléaire de Saint-Laurent.
Incident grave	**3**	Très faible rejet: exposition du public représentant une fraction des limites prescrites.	Contamination grave ou effets aigus sur la santé d'un travailleur.	Accident évité de peu. Perte des lignes de défense.	2005, Fuite nucléaire à Sellafield. Trois évènements ont été classés au niveau 3 en France (1981 à La Hague, 2002 à Roissy, 2008 à l'ONERA à Toulouse).
Incident	**2**	(pas de conséquence	Contamination importante ou surexposition d'un travailleur.	Incident assorti de défaillance importante des dispositions de sûreté.	(Quelques cas par an en France)
Anomalie	**1**		(pas de conséquence)	Anomalie sortant du régime de fonctionnement autorisé.	(Une centaine de cas par an en France)
Écart	**0**			Anomalie sans importance du point de vue de la sûreté.	(De l'ordre d'un millier de cas par an en France)

INES ne constitue pas une échelle d'évaluation de sûreté, mais elle est destinée à faciliter la perception par les médias et le public de l'importance des accidents nucléaires.

4.2 Fréquence d'occurrence

Proposition : La fréquence d'occurrence d'un événement est la mesure du nombre moyen d'occurrences attendues en un laps de temps donné dans des conditions connues. Cette fréquence est estimée sur une période de temps donnée (année, jour, heure, etc.).

Les classes de fréquence présentées dans la table suivantes (voir TAB. 5) sont proposées dans la norme NF EN 50126 (NF EN 50126, Janvier 2000):

TAB. 5 : Echelles de fréquence d'occurrence selon la norme NF EN 50126

Niveau	Description
Invraisemblable	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas
Improbable	Peu susceptible de se produire mais possible. On peut supposer que la situation dangereuse peut exceptionnellement se produire
Rare	Susceptible de se produire à un moment donné du cycle de vie du système. On peut raisonnablement s'attendre à ce que la situation dangereuse se produise
Occasionnel	Susceptible de survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne à plusieurs reprises

Probable	Peut survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne souvent
Fréquent	Susceptible de se produire fréquemment. La situation dangereuse est continuellement présente

La métrique de fréquences d'occurrence présentée dans la table suivante (voir TAB. 6) est adoptée dans le cadre de l'APR du système de contrôle/commande ERTMS (GTR 55, 2000). C'est une simplification de la métrique proposée dans la norme NF EN 50126 (voir TAB. 5):

TAB. 6 : Adaptation des échelles de fréquence d'occurrence de la norme NF EN 50126

Niveau	Description
Invraisemblable	Extrêmement invraisemblable à survenir durant la vie du système<=10^{-9} /h
Rare	Invraisemblable à survenir mais possible durant la vie du système > 10^{-9} /h
Occasionnel	Vraisemblable qu'il survienne plusieurs fois durant la vie du système
Fréquent	Vraisemblable qu'il survienne fréquemment durant la vie du système

Toutefois nous pouvons constater le caractère sommaire des significations données aux niveaux d'occurrence. Par exemple, il existe une forte nuance entre le terme « plusieurs fois » et le terme « fréquemment ». De surcroit, les deux termes renvoient à 2 comme à 1000 occurrences !

Une échelle de probabilités d'occurrence mieux élaborée (voir TAB. 7) est proposée en annexe 1 de l'arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation (Ministère de l'écologie et du développement durable , 29 septembre 2005) :

TAB. 7 : Echelle de probabilité d'occurrence appliquée dans le domaine des ICPE

Classe de probabilité / **Type d'appréciation**	**E**	**D**	**C**	**B**	**A**
Qualitative	« événement possible mais extrêmement peu probable » : *n'est pas impossible au vu des connaissances actuelles,*	« événement très improbable » : *s'est déjà produit dans ce secteur d'activité mais a fait l'objet de mesures correctives réduisant*	« événement improbable » : *un événement similaire déjà rencontré dans le secteur d'activité ou dans ce type d'organisation au niveau mondial, snas*	« événement probable » : *s'est produit et/ou peut se produire pendant la durée de vie de l'installation*	« événement courant » : *s'est produit sur le site considéré et/ou peut se produire à plusieurs reprises pendant la*

	mais non rencontré au niveau mondial sur un très grand nombre d'années et installations	*significativement sa probabilité.*	*que les éventuelles corrections intervenues depuis apportent une garantie de réduction significative de sa probabilité*		*durée de vie de l'installation, malgré d'éventuelles mesures correctives*
Semi-qualitative	Cette échelle est intermédiaire entre les échelles qualitative et quantitative, et permet de tenir compte des mesures de maîtrise des risques mises en place.				
Quantitative (par unité par an)		10^{-5}	10^{-4}	10^{-3}	10^{-2}

Les définitions données entre guillemets ne sont valables que si le nombre d'installations et le retour d'expérience sont suffisants Ces définitions sont conventionnelles et servent d'ordre de grandeur de la probabilité moyenne d'occurrence observable sur un grand nombre d'installations x années.

En effet, l'arrêté stipule que : « *si le retour d'expérience est limité, les détails figurant en italique ne sont en général que pas représentatifs de la probabilité réelle. L'évaluation de la probabilité doit être effectuée par d'autres moyens (études, expertises, essais) que le seul examen du retour d'expérience* ».

4.3 Exposition

La notion d'exposition en situation dangereuse à été définie par la norme européenne EN 292 (EN 292/ISO 12100, 1995) comme : « Situation dans laquelle une personne est exposée à un ou des phénomènes dangereux ».

Le facteur d'exposition est estimé en fonction des besoins d'accès à la zone dangereuse, de la nature de l'accès, du temps passé dans la zone dangereuse, du nombre de personnes demandant l'accès et de la fréquence d'accès.

L'exposition permet, entre autres, de mieux apprécier la gravité. Une échelle de gravité basée sur l'exposition des humains (voir TAB. 8) est donnée en annexe 3 de l'arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation (Ministère de l'écologie et du développement durable , 29 septembre 2005):

TAB. 8 : Echelle de gravité d'exposition des humains à l'extérieur des ICPE

Niveau de gravité Des conséquences	Zone délimitée par le seuil des effets létaux	Zone délimitée par le seuil des effets létaux	Zone délimitée par le seuil des effets

	significatifs		irréversibles Sur la vie humaine
Désastreux	Plus de 10 personnes exposées (1).	Plus de 100 personnes exposées	Plus de 1 000 personnes exposées
Catastrophique	Moins de 10 personnes exposées	Entre 10 et 100 personnes	Entre 100 et 1 000 personnes exposées.
Important	Au plus 1 personne exposée.	Entre 1 et 10 personnes exposées	Entre 10 et 100 personnes exposées
Sérieux	Aucune personne exposée.	Au plus 1 personne exposée.	Moins de 10 personnes exposées
Modéré	Pas de zone de létalité hors de l'établissement		Présence humaine exposée à des effets irréversibles inférieure à « une personne ».
(1) Personne exposée : en tenant compte le cas échéant des mesures constructives visant à protéger les personnes contre certains effets et la possibilité de mise à l'abri des personnes en cas d'occurrence d'un phénomène dangereux si la cinétique de ce dernier et de la propagation de ses effets le permettent.			

5 Facettes du risque

5.1 Risque

R. Flanagan et G. Norman (Flanagan & Norman, 1993) rapportent dans leur livre « Risk Management and Construction » que le mot « risque » est relativement moderne. Il provient du mot français « risqué ». Ce n'est qu'au milieu du 17éme siècle que les Anglo-Saxons ont adopté le terme « Risk », avant qu'il ne soit fort présent dans le jargon des Assurances.

Le risque est un concept diversement compris, représenté, identifié, estimé, interprété, perçu, évalué, maitrisé et géré !

Définitions :

Source	
(Larousse, 2006)	Eventualité d'un préjudice, d'un événement malheureux
(Larousse, 2005)	Possibilité, probabilité d'un fait, d'un événement considéré comme mal ou un dommage. Danger, inconvénient plus au moins probable auquel on est exposé : courir le risque
(HMSO, 1995)	Une combinaison de la probabilité, de la fréquence, de l'occurrence d'un aléa défini et de l'amplitude des conséquences de cette occurrence.

(GT Aspects sémantiques du risque, 1997)	Le risque est une mesure de l'occurrence d'un événement indésirable et/ou la mesure associée à ses effets et conséquences.
(GT Méthodologie, 2003)	Le risque est considéré comme la possibilité de survenance d'un dommage résultant d'une exposition aux effets d'un phénomène dangereux. C'est une espérance mathématique de pertes en vies humaines, blessés, dommages aux biens et atteinte à l'activité économique au cours d'une période de référence et dans une région donnée,
(BSI OHSAS 18001, 2005)	Combinaison de la probabilité et de la (les) conséquence(s) de la survenue d'un événement dangereux spécifié.
(NF EN 61508, Décembre 1998)	Combinaison de la probabilité d'occurrence d'un dommage et de sa gravité.
(ISO 14971, 2000), (ISO/CEI Guide 51, 1999), (CEI 300-3-9, 1995), (EN 292/ISO 12100, 1995)	Combinaison de la probabilité d'un dommage et de sa gravité.
(ISO/CEI Guide 73, 2002)	Combinaison de la probabilité d'un événement et de ses conséquences.
(NF EN 50128, Juillet 2001), (NF EN 50129, Mai 2003)	Combinaison de la fréquence ou de la probabilité, et des conséquences d'un événement redouté.
(NF EN 50126, Janvier 2000)	Le risque est la combinaison de deux éléments : - la probabilité d'occurrence d'un événement ou d'une combinaison d'événements conduisant à une situation dangereuse, ou la fréquence de tels événements. - les conséquences de cette situation dangereuse.
(Directive 96/82/EC (SEVESO II), 9 décembre 1996)	Probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées.

Proposition : Le risque est une propriété intrinsèque à toute prise de décision. Il se mesure par une conjonction entre plusieurs facteurs (Gravité, Occurrence, Exposition, Possibilités d'évitement, etc.), quoique généralement on se limite aux deux facteurs : gravité et fréquence d'occurrence d'un accident potentiellement dommageable en intégrant dans certains cas le facteur d'exposition.
Cependant, il ne faut pas confondre le concept de risque avec sa mesure.

5.2 Classification du risque

Généralement, les niveaux de gravité et de probabilité d'occurrence sont croisés dans une matrice de criticité afin de positionner les zones de risque. La matrice Gravité/Occurrence ci-dessous (voir TAB. 9) est proposée par la norme NF EN 50126 (NF EN 50126, Janvier 2000):

TAB. 9 : Matrice de criticité (G/O) - NF EN 50126

	Insignifiant	**Marginal**	**Critique**	**Catastrophique**
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Occasionnel	Acceptable	Indésirable	Indésirable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Fréquent	Indésirable	Inacceptable	Inacceptable	Inacceptable

Proposition : Nous proposons de garder les qualificatifs de la norme NF EN 50126, tout en les répartissant sur 3 classes distinctes : « risque maitrisé » regroupant le risque négligeable et le risque acceptable, « risque maitrisable » regroupant le risque indésirable non résiduel et enfin « risque non maitrisable » regroupant le risque résiduel et le risque inacceptable. Toutefois nous définissons le risque indésirable comme une sous catégorie du risque tolérable et nous procédons de la même façon en ce qui concerne le risque inacceptable par rapport au risque résiduel (voir FIG. 2).

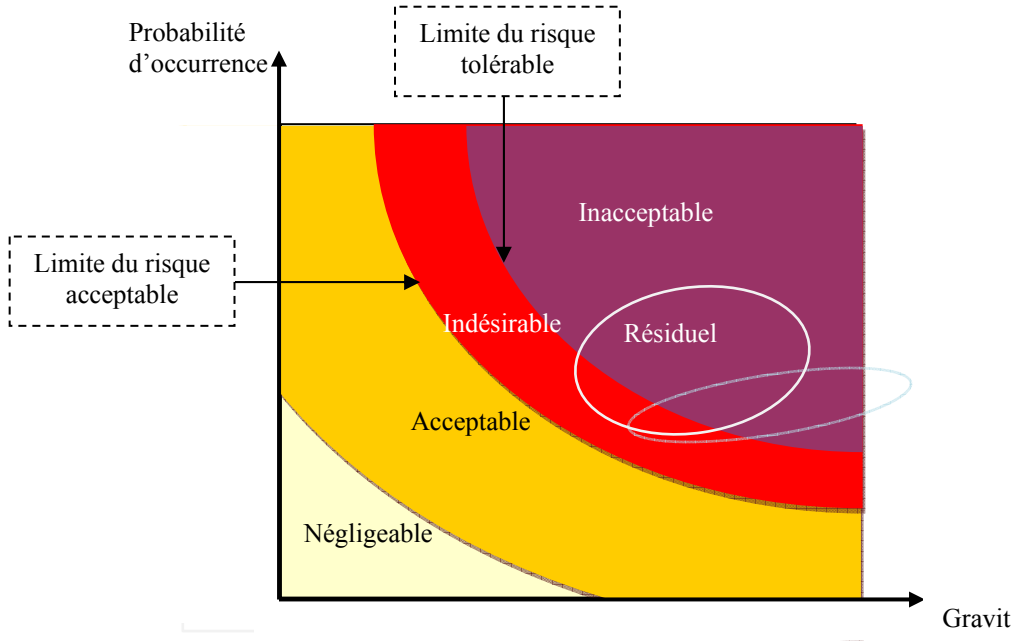


FIG. 2: Classification des risques

5.2.1 Risques maitrisés

5.2.1.1 Risque négligeable

Définitions :

SOURCE	
(GT Aspects sémantiques du risque, 1997)	Un risque est négligeable s'il est inférieur à un seuil (par exemple : 10^{-9} par an). Risque dont on ne se soucie pas de l'occurrence au quotidien.
(HSE, 1992)	Le risque négligeable fait référence à un niveau de risque dont l'occurrence est de l'ordre de 1 par million et par année et au dessous, et dont la possibilité de réalisation n'affecte pas la vie courante.

Synthèse : Les deux définitions du risque rattachent le risque à la probabilité d'occurrence évaluée au quotidien, et ce, quelque soit la gravité des dommages potentiels.

Proposition : Un risque négligeable n'est pas pris en compte dans l'évaluation globale du risque lié à un système.

5.2.1.2 Risque acceptable

Définitions :

SOURCE	
(Laurant, 2003)	Traduit la notion relative à un risque intégré tel que dans le contexte de la vie courante.
(AQS-GT OORS, Mars 1996)	Risque acceptable pour les personnes : un risque n'est accepté que s'il y a contrepartie ou/et s'il est inférieur au risque déjà encouru. Risque acceptable pour les entreprises : le risque acceptable ne se conçoit que dans le cadre résiduel, après la mise en œuvre des mesures de prévention et de Protection notamment celles imposées par la législation et la réglementation en vigueur.
(GT 7 - CEI)	Risque acceptable : valeur d'un risque résultant d'une décision explicite établie de façon objective. Il est parfois préférable pour certaines branches d'activité de parler du risque admissible ou du risque limite.
(GT Aspects sémantiques du risque, 1997)	un risque est acceptable en référence à un objectif de sécurité donné, un risque est acceptable s'il est inférieur à un seuil (par exemple : 10^{-5} par an), Risque avec lequel on consent à vivre en contrepartie d'un bénéfice et dans la mesure où il est contrôlé.
(ISO/CEI Guide 51, 1999)	Un risque accepté dans un contexte donné basé sur des valeurs courantes de notre société.

(ISO/CEI Guide 73, 2002)	L'acceptation du risque dépend des critères de risques retenus par la personne qui prend la décision.

Synthèse : Les définitions du risque acceptable peuvent être classées en deux catégories : celles dont l'acceptabilité est basé essentiellement sur les valeurs de la société, et celles dont l'acceptabilité est rattaché à la prise de décision (voir ISO/CEI Guide 73 et GT 7 – CEI).

Proposition : Un risque perçu comme insignifiant peut facilement être accepté. En d'autres termes, un accident potentiel caractérisé par une faible probabilité d'occurrence, peut facilement être accepté. En effet, nous continuons à prendre le train malgré les accidents possibles parce que la probabilité d'un déraillement ou d'une collision catastrophique est extrêmement faible.

5.2.2 Risques maitrisables

5.2.2.1 Risque tolérable (Tolerable risk)

Définitions :

SOURCE	
(Laurant, 2003)	Le risque toléré traduit, à l'effet d'en retirer certains bienfaits, la volonté de vivre avec les risques que l'on saurait ni ignorer, ni considérer comme négligeables, mais avec la confiance qu'ils sont correctement maîtrisés.
(HSE, 1992)	Risque que l'on ne peut pas considérer comme négligeable ou comme quelque chose que l'on peut ignorer mais que l'on doit garder présent à l'esprit et pour lequel on doit engager des mesures de réduction aussi tôt qu'il est possible.
(GT Aspects sémantiques du risque, 1997)	Risque que l'on doive considérer avec vigilance et chercher à réduire autant que raisonnablement possible. Risque inférieur à un seuil donné (par exemple : 10^{-9} par an).
(GT Méthodologie, 2003)	Le risque tolérable est le résultat de la recherche d'un équilibre optimal entre une sécurité absolue idéale et les exigences technico-économiques.
(NF EN 61508, Décembre 1998), (EN 292/ISO 12100, 1995)	Risque accepté dans un certain contexte et fondé sur les valeurs actuelles de la société.
(ISO/CEI Guide 51, 1999)	Risque accepté dans un certain contexte et fondé sur des valeurs admises par la société.

Synthèse : Selon le GT Méthodologie : « La tolérabilité du risque résulte d'une mise en balance des avantages et des inconvénients (dont les risques) liés à une situation, situation qui sera soumise à révision régulière afin d'identifier, au fil du temps et chaque fois que cela sera possible, les moyens permettant d'aboutir à une réduction du risque ». En effet, le risque serait toléré en attendant de pouvoir mieux juger, alors que le terme acceptable aurait un caractère d'acceptation plus définitif.

Proposition : Tolérer un risque signifie qu'on ne le voit pas comme négligeable et ce n'est pas vraiment l'accepter.

5.2.2.2 Risque indésirable (Undesirable risk)

SOURCE	
(NF EN 61508, Décembre 1998)	Risque indésirable, tolérable uniquement s'il est impossible de réduire le risque ou si le coût de la réduction est disproportionné par rapport à l'amélioration possible.

Synthèse : A l'égard de la définition donnée par la norme NF EN 61508, le risque indésirable est souvent lié au risque tolérable.

Proposition : Un risque indésirable est un risque qui peut être toléré moyennant des mesures appropriées de contrôle et de suivi.

5.2.3 Risques non maitrisables

5.2.3.1 Risque résiduel (Residual risk)

Définitions :

SOURCE	
(AQS-GT OORS, Mars 1996)	Risque qui subsiste quand on a fait « de son mieux » en fonction du « possible actuel ».
(GT Aspects sémantiques du risque, 1997)	Risque qui subsiste après avoir appliqué des mesures de réduction. Risque qui subsiste après avoir appliqué toutes les mesures de réduction disponibles.
(NF EN 61508, Décembre 1998), (CEI 1050, Février 1991)	Risque restant après que toutes les mesures de prévention ont été prises.
(ISO/CEI Guide 51, 1999)	Risque subsistant après que des mesures de prévention aient été prises.

(ISO/CEI Guide 73, 2002)	Risque subsistant après le traitement du risque.

Synthèse : Le GT OORS de l'AQS définit le risque résiduel de deux façons : la deuxième en l'occurrence concorde avec les autres définitions données ci-dessous, néanmoins la première ne met pas en valeur le fait que toutes les mesures possibles aient été prises avant que le risque subsistant ne soit qualifié de résiduel.

Proposition : Un risque résiduel est un risque subsistant après que les différentes mesures possibles aient été prises.

5.2.3.2 Risque inacceptable (non acceptable risk)

Proposition : Un risque inacceptable est un risque résiduel non tolérable.

5.3 Acceptabilité du risque

La mesure du risque peut rapprocher le degré de nuisance de deux situations dangereuses complètement dissemblables : l'une caractérisée par une pondération de fréquence et l'autre par une pondération de gravité.

L'acceptabilité concerne le risque et non la gravité du dommage ou la probabilité d'occurrence considérés séparément. En effet, la gestion des risques a pour objectif de consigner les aléas à l'intérieur de frontières jugées satisfaisantes. Un risque impossible à supprimer doit donc être réduit à un niveau acceptable fixé préalablement.

Le choix des actions de maîtrise des risques se fait en fonction de la fréquence et de la gravité des dommages relatifs à un accident potentiel. Les actions de protection (sécurité primaire) sont prioritaires par rapport aux actions préventives (sécurité secondaire) ayant objectif de réduire les conséquences d'événements dommageables tandis que ces dernières ont pour but de limiter la possibilité de récidive des événements redoutés.

5.4 Risque vs. Danger

Le risque est lié à la prise de décision qui a pour objet à soumettre une cible à un danger. Le danger est une propriété intrinsèque à une source de danger.

Le Groupe de Travail « Méthodologie » (GT Méthodologie, 2003) donne une définition intéressante aux concepts de risque et de danger : « Le risque constitue une potentialité. Il ne se réalise qu'à travers l'événement accidentel, c'est-à-dire à travers la réunion et la réalisation d'un certain nombre de conditions et la conjonction d'un certain nombre de circonstances qui conduisent, d'abord, à l'apparition d'un (ou plusieurs) élément(s) initiateur(s) qui permettent, ensuite, le développement et la propagation de phénomènes permettant au danger de

s'exprimer, en donnant lieu d'abord à l'apparition d'effets et ensuite en portant atteinte à un (ou plusieurs) élément(s) vulnérable(s) ».

5.5 Risque vs. Gravité

Beaucoup de personnes confondent risque et gravité et ne prennent en compte que les cas pour lesquels la gravité est importante sans aucune considération du facteur probabilité (c'est le cas des Analyses Préliminaires de Danger). Ce phénomène constitue ce que certains appellent « la fascination par le risque maximum ».

Le risque d'un scénario d'accident fréquent et peu grave peut être assimilé à celui d'un scénario rare et grave, quoiqu'il existe une certaine aversion pour ce dernier. Cependant, il convient de rappeler que **«** 1 x 1 n'est pas équivalent à 10 x 0 .1 ». La perception du risque du grand public vis-à-vis des crashs d'avions est beaucoup plus ferme de ce qu'elle est des accidents de la route, bien que ces derniers arrivent beaucoup plus souvent et fassent beaucoup plus de victimes.

5.6 Risque vs. Probabilité d'occurrence

Dans le domaine médical on définit plus généralement pour un risque la probabilité d'un dommage en exprimant, par exemple, la probabilité qu'il y ait un décès ou des complications ou des effets secondaires. Il convient de préciser que la notion de probabilité est associée aux événements et non pas aux dommages, le décès devrait être considéré comme un événement ayant une gravité et une probabilité d'occurrence estimée en fonction de l'espérance de vie et pondérée au cas par cas. Dans l'analyse de risques appliquée aux systèmes de transport, on ne s'intéresse pas à la probabilité d'un dommage mais plutôt à la probabilité d'occurrence d'un événement redouté. Cette probabilité d'occurrence est associée, au moins, à la gravité des dommages subis pour estimer le risque.

5.7 Risque vs. Incertitude

Le risque est inhérent à toute activité décisionnelle car ses racines plongent dans le futur et il se nourrit des décisions du présent (Bergadaà, Chandon, & Chebat, 1984).

Le contexte de toute prise de décision peut être représenté sur deux dimensions (voir FIG. 3): l'axe challenge (objectif à atteindre) et l'axe risque (prise de risque inhérente).

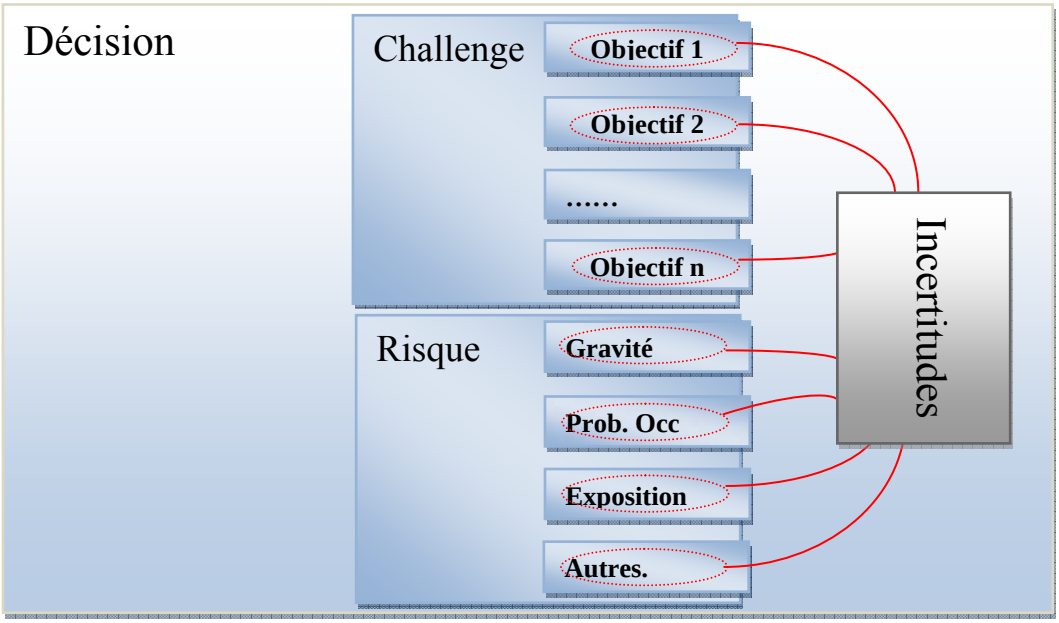


FIG. 3: Décision, challenge, risque et incertitude

Il est très difficile de spécifier avec certitude les objectifs et le risque d'une prise de décision. En effet, le mot incertitude est généralement employé quand il s'agit de situation non mesurable.

En fait, les spécialistes sont de deux avis : les premiers considèrent l'incertitude comme synonyme du risque. Ainsi par exemple, nous avons pris l'habitude de parler de risques naturels compte tenu l'aspect incertain et aléatoire des phénomènes naturels (inondation, foudre, etc.). Pour les autres une situation d'incertitude peut être considérée comme une situation à risque par l'affectation de probabilités subjectives !

5.8 Perception du risque

La perception du risque (Risk attitude) n'est nullement une appréciation objective des dangers, mais plutôt la conséquence d'une projection de sens et de valeurs sur certains événements, sur certaines pratiques.

Selon la norme ISO/CEI Guide 51 (ISO/CEI Guide 51, 1999), la perception du risque est l'« ensemble de valeurs ou préoccupations aux travers desquelles une personne, un groupe ou un organisme considère un risque ». Kerven et Rubise (Kerven & Rubise, 2001) soulèvent le paradoxe de la familiarité du danger en soulignant que : « *La fréquentation quotidienne d'un danger à forte gravité se traduit par une sous-estimation de ce danger qui décroît avec l'éloignement* ».

5.8.1 Perception de risque statique

Le risque statique (dit aussi risque pur) est le degré de vraisemblance que quelque chose de négatif se produise durant une période de temps donnée ou résulte d'une situation particulière. Ce type de risque relève essentiellement des décisions ne pouvant conduire qu'à des conséquences négatives (Flanagan & Norman, 1993).

Le suicide présente un risque purement statique, mais l'euthanasie est perçue différemment, elle est même légalisée dans certains pays Européens comme l'Allemagne et la Grande-Bretagne. Ce qui n'est pas le cas en France ou en Italie.

De même pour les entreprises industrielles, le risque d'incendie, de séisme, de tornade sont des risques statiques.

5.8.2 Perception de risque dynamique

Tous les domaines sociotechniques engendrent des risques dynamiques (dits aussi risques spéculatifs). Généralement, les entreprises dynamiques osent plus de risques dynamiques par la voie de l'innovation et du progrès.

On parle de risque dynamique quand la prise de décision engendre aussi bien une potentialité de gain que de perte (Flanagan & Norman, 1993). Le risque dynamique se présente comme un coup de poker et renvoie au fait de risquer la perte de quelque chose de certain afin de gagner quelque chose d'incertain. Par exemple, malgré les nombreux crashs (Tenerife (1977), etc.) on continue à prendre l'avion, et malgré les nombreuses catastrophes nucléaires (Three Miles Island (1979), Tchernobyl (1986), etc.) on continue à innover, construire et commercialiser des centrales nucléaires.

La typologie du risque (dynamique, statique) dépend de la perception des décisions. Ainsi les mouvements de grève sont perçus différemment par le patronat et le syndicat. La perception du patronat est pondérée essentiellement par les pertes financières engendrées par ces mouvements, ce qui présente un risque statique, tandis que les grévistes sont prêts à prendre un risque dynamique, celui de sacrifier plusieurs jours de salaire afin d'arriver à la satisfaction de leurs revendications. En outre, la perception du risque peut évoluer et changer de cap. Certes, le pire risque qui puisse exister est celui qu'on croirait spéculatif par un arbitrage préliminaire « gains versus pertes », mais qui s'avère avec l'affermissement de notre perception, un risque purement statique.

5.9 Prise de risque

Selon la norme ISO/CEI Guide 73 (ISO/CEI Guide 73, 2002) la prise de risque est : « l'acceptation de la charge d'une perte, ou du bénéfice d'un gain, d'un risque particulier.

5.9.1 Risque de ne rien risquer

La prise de risque est nécessaire à la survie d'une entreprise face à la concurrence et aux défis de la mondialisation. Risquer c'est d'abord oser courir le hasard en s'engageant dans une action qui pourrait apporter un avantage, mais qui comporte l'éventualité d'un danger (voir 5.8.2). Marcel PAGNOL aurait dit : « Si vous voulez aller sur la mer, sans aucun risque de chavirer, alors, n'achetez pas un bateau : achetez une île ! », ce qui signifie dans un langage plus clair : « qui ne risque rien n'a rien » !

5.9.2 Risque de trop risquer

La pratique du « risquer le tout pour le tout » comme un coup de poker, réserve trop souvent de mauvaises surprises. La prise de risque doit être sage, intelligente est réfléchie. A cet effet, trois facteurs clés méritent d'être situés avant toute prise de risque (voir FIG. 4) : les choses qu'on connaît (usage du REX), les choses que l'on ignore (usage des techniques d'analyse, de synthèse, de simulation et de test) et les choses qu'on croit connaître (usage inapproprié du REX) et c'est bien ce dernier facteur qui pose le plus de problèmes possibles:

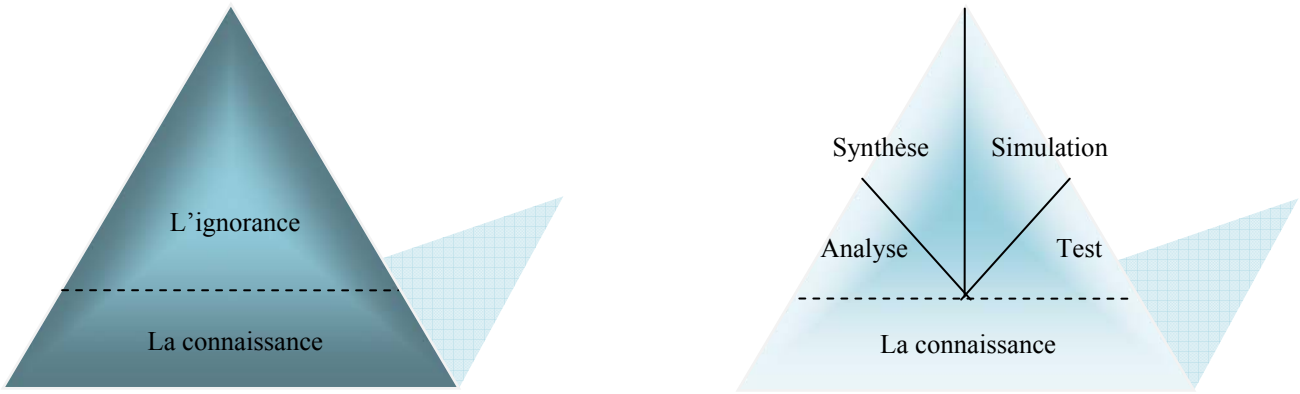


FIG. 4 : Remédier à l'ignorance avant de risquer (Flanagan & Norman, 1993)

Le risque est la balance qui permet de mesurer le poids d'une opportunité. Cette balance contient d'un côté le challenge et de l'autre la menace (Flanagan & Norman, 1993). Autrement dit, une opportunité se présente comme une menace pour ceux qui pensent perdre, et comme un challenge pour ceux qui prédisent le contraire.

En effet, le concept de risque permet de concilier les notions de challenge et de menace. Une fois qu'un risque est analysé, il tend à devenir un problème de management, même si on continue à parler de management des risques. Justement, la décision de prendre ou ne pas prendre un risque relève essentiellement du management.

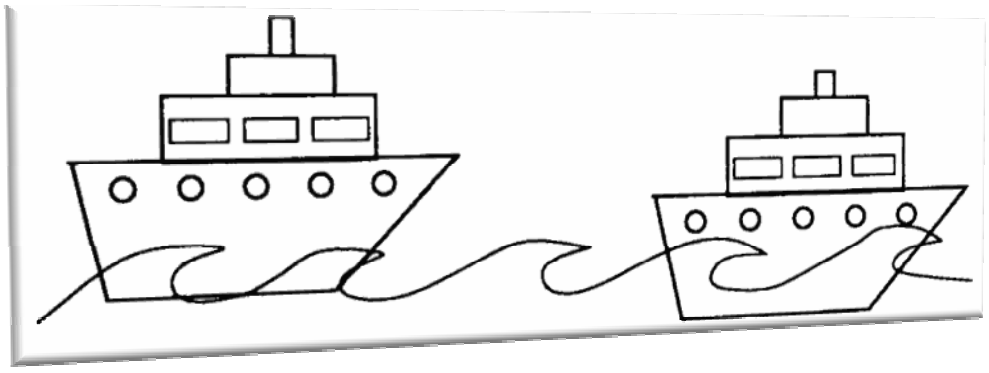


FIG. 5 : Place your waterline low (Peters, 1988)

La prise de risque possède naturellement une ligne rouge qu'il ne faut pas franchir. T. Peters (Peters, 1988) l'illustre avec une superbe métaphore « *Place your waterline low* » ou « Placer votre ligne de flottaison suffisamment en bas » (voir FIG. 5), ce qui signifie, vous pouvez tenter ce que vous voudrez du moment que cela n'affecte pas l'intégrité de votre organisation. R. Flanagan et G. Norman (Flanagan & Norman, 1993) dégagent dix critères permettant de poser un cadre propice à la prise de risque :

1. Ne pas risquer gros pour peu.
2. Ne jamais risquer plus qu'on est disposé à perdre.
3. Planifier avant d'agir.
4. Analyser toujours les sources et les conséquences du risque.
5. Agir, car l'inaction des autres ne justifie pas de rester immobile.
6. Eviter de prendre des risques purement pour des raisons de principe.
7. Eviter la prise de risque inutile juste pour ne pas perdre la face.
8. Prendre en considération les avis d'experts (regards exogènes).
9. Prendre en considération tout avis hétéroclite, qu'il soit basé sur l'intuition ou l'expérience (regards endogènes).
10. Considérer conjointement le côté contrôlable, et le côté incontrôlable du risque.

6 Conclusion

Dans le cadre du présent chapitre, nous avons commencé par clarifier les fondements de la sécurité d'abord en la définissant par rapport au danger et au risque et ensuite en la confrontant aux autres composantes de la sûreté de fonctionnement. Par conséquent, nous avons passé en revue le concept de risque et ses corollaires tels que danger, phénomène dangereux, conséquence, dommage, gravité, fréquence d'occurrence, en les regroupant selon les liens sémantiques qui puissent exister entre eux.

En vue de bien assimiler le chapitre suivant, qui sera consacré à l'étude de l'analyse de risque dans le processus de management des risques, nous avons consacré dans ce 1er chapitre une section entière à l'étude des facettes du risque, autrement dit, son concept, sa perception, sa prise, sa classification, son acceptabilité et ses différences avec d'autres concepts tels que gravité, probabilité d'occurrence, incertitude, etc.

En effet, après avoir cadré le concept de sécurité, nous allons aborder dans le cadre du 2éme chapitre l'essentiel des activités relatives à la sécurité en commençant par le management des risques et son processus général qui contient justement, entre entres, l'analyse de risque.

7 Travaux cités

AQS-GT OORS. (Mars 1996). *Management de la sécurité d'entrepreise, vocabulaire et concept.* Association Qualité-Sécurité (AQS) pour l'Observatoire de l'Opinion sur les Risques de la Sécurité.

Bergadaà, M., Chandon, J.-L., & Chebat, J.-C. (1984). Le temps comme intrant des attitudes á l'égard de la sécurité routière. *Revue d'Analyse Économique* , Vol 60, n°4, pp 495-513.

Bouchet, S. (2001). *Analyse des risques et prévention des accidents majeurs : Présentation des méthodes d'inspection TRAM, NIVRIM et AVRIM2.* INERIS, Direction des Risques Accidentels, Unité prévention.

BSI OHSAS 18001. (2005). *Occupational Health and Safety Management Systems – Specification.* England: BSI.

CEI 1050. (Février 1991). *Transformateurs pour lampes tubulaires à décharge ayant une tension secondaire à vide supérieure à 1 000 V - (couramment appelés transformateurs-néon): Prescriptions générales et de sécurité.* CEI.

CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement.* CEI.

CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service.* CEI.

CEI 61069. (1996). *Mesure et commande dans les processus industriels - Appréciation des propriétés d'un système en vue de son évaluation - Parti 5: Evaluation de la sûreté de fonctionnement d'un système.* CEI.

Cox, L.-A. (2008). What's wrong with risk matrices? *Journal of risk analysis* , Vol. 28, No. 2, pp 497-512.

Directive 96/82/EC (SEVESO II). (9 décembre 1996). *European directive on the control of major-accident hazards involving dangerous substances.* Brussels: Official Journal of the European Union, Commission of the European Communities.

EN 292/ISO 12100. (1995). *Sécurité des machines ; Notions fondamentales, principes généraux de conception.* ISO/CEN.

Flanagan, R., & Norman, G. (1993). *Risk Management and Construction.* Blackwell Science Ltd.

GT 7 - CEI. *Enseignement - Terminologie.* CEI.

GT Aspects sémantiques du risque. (1997). *Vocabulaire lié au risque à travers une analyse bibliographique.* Institut de Protection et de Sûreté Nucléaire (IPSN) - Observatoire de l'Opinion sur les Risques et la Sécurité.

GT Méthodologie. (2003). *Principes généraux pour l'élaboration et la lecture des études de dangers.* INERIS.

GTR 55. (2000). *Les analyses préliminaires de risques appliquées aux transports terrestres guidés.* Institut de Sûreté de Fonctionnement - Collège sécurité.

Heurtel, A. (2003). *La gestion des risques techniques et des risques de management.* CNRS - IN2P3/LAL.

HMSO. (1995). *A guide to Risk Assessment and Risk Management for Environmental Protection.* England: Her Majesty's Stationery Office.

HSE. (1992). *Generic terms and concepts in the assessment and regulation of industrial Risks.* UK: Health and Safety Executive.

ISO 14971. (2000). *Application de la gestion des risques aux dispositifs médicaux.* ISO.

ISO/CEI Guide 2. (1986). *Termes généraux et leurs définitions concernant la normalisation et les activités connexes.* ISO.

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). *Management du risque – Vocabulaire – principes directeurs pour les inclure dans les normes.* ISO/CEI.

Kerven, G.-Y., & Rubise, P. (2001). *L'archipel du danger - Introduction aux cindyniques.* Paris: Eyrolles.

Laprie, J.-C. (2002). *Guide de la Sûreté de Fonctionnement.* Cepaduès .

Laprie, J.-C. (1994). *La modélisation des systèmes informatiques : concepts de base et terminologie - , rapport n° 94448.* Toulouse: LAAS.

Larousse. (2006). Larousse Définitions.

Larousse. (2005). Larousse Expression.

Laurant, A. (2003). *Sécurité des procédés chimiques.* Lavoisier.

Ministère de l'écologie et du développement durable . (29 septembre 2005). *Arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des ICPE* . Journal officiel de la république française.

Mortureux, Y. (2002, Août). La Sûreté de fonctionnement: méthodes pour maîtriser les risques. *Techniques de l'ingénieur* .

NF EN 50126. (Janvier 2000). *Applications ferroviaires : Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).* Paris: AFNOR.

NF EN 50128. (Juillet 2001). *Applications ferroviaires : Systèmes de signalisation, de télécommunication et de traitement, Logiciels pour systèmes de commande et de protection ferroviaire.* Paris: AFNOR.

NF EN 50129. (Mai 2003). *Applications ferroviaires : Systèmes de signalisation, de télécommunication et de traitement, Systèmes électroniques de sécurité pour la signalisation.* Paris: AFNOR.

NF EN 61508. (Décembre 1998). *Sécurité fonctionelle des systèmes électriques et électroniques programmables relatifs à la sécurité.* Paris: AFNOR.

Peters, T. (1988). *Thriving on chaos.* London: MacMillan Ltd.

Sallak, M., Simon, C., & Aubry, J.-F. (2007). A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems* .

TABLE DES MATIÈRES DU CHAPITRE 2: L'ANALYSE DE RISQUE DANS LE PROCESSUS DE MANAGEMENT DES RISQUES

Supprimé : 38

Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38
Supprimé : 38

Chapitre 2

L'ANALYSE DE RISQUE DANS LE PROCESSUS DE MANAGEMENT DES RISQUES

Dans le cadre de ce chapitre, nous essayerons principalement de lever certaines ambigüités relatives aux activités de management des risques. En effet, il est très courant de confondre la notion de maitrise des risques à celle de management ou de gestion des risques. De même, les notions d'analyse, d'appréciation, d'évaluation ou estimation des risques doivent être précisées.

Compte tenu de la complémentarité des différentes méthodes d'analyse de risque réputées, il est inévitable, avant de porter l'étude sur l'Analyse Préliminaire de Risque, de présenter une typologie et un panorama synthétique des différentes méthodes applicables en continuité de l'APR. En outre, nous estimons indispensable, en préalable aux chapitres suivants consacrés au management préliminaire des risques, de bien fixer les limites et les interfaces des activités de management des risques (appréciation, maîtrise, analyse, évaluation, etc.).

1. Management des risques

Définitions :

SOURCE	
(Barbet, Mars 1996)	La démarche de gestion des risques consiste à : planifier, acquérir les informations, modéliser l'exposition du système aux risques et enfin conduire le système.
(CEI 300-3-9, 1995)	Application systématique des politiques de gestion, des procédures et des usages aux tâches d'analyse, d'évaluation et de maîtrise du risque.
(ISO/CEI Guide 73, 2002)	Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. Le management du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque. *Note : Le mot gestion a été remplacé par management.*

Synthèse: Rappelons d'abord que « management des risques » est une traduction directe de « Risk management », généralement employée dans la communauté francophone de la sûreté de fonctionnement.

Proposition : 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 maitrise de ces derniers (voir FIG. 1).

Rappelons que selon le guide ISO/CEI 51 (ISO/CEI Guide 51, 1999), l'appréciation des risques est l'ensemble du processus d'analyse et d'évaluation des risques, tandis que le guide ISO/CEI 73 (ISO/CEI Guide 73, 2002) 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 mémoire.

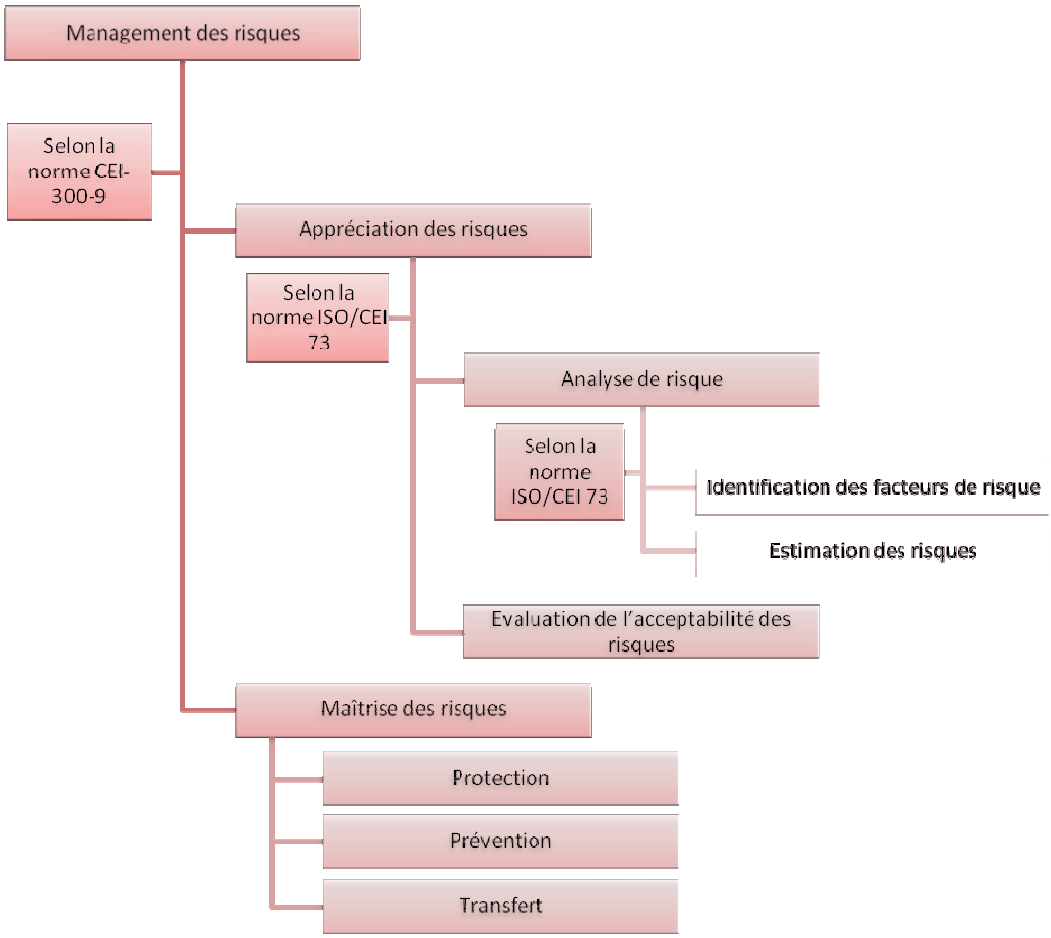


FIG. 1 : Processus de Management des risques

1.1 Analyse de risque

Définitions :

SOURCE	
(Larousse, 2005)	Analyse: Étude minutieuse, précise faite pour dégager les éléments qui constituent un ensemble, pour l'expliquer, l'éclairer : Faire l'analyse de la situation.
(ISO/CEI Guide 73, 2002)	Utilisation systématique d'informations pour identifier les facteurs de risque et pour estimer le risque
(ISO/CEI Guide 51, 1999)	Utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer les risques.

Proposition : L'analyse de risque est l'utilisation systématique d'informations pour identifier les entités de danger et estimer le risque.

1.1.1 *Identification des facteurs de risque*

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 (ISO/CEI Guide 73, 2002).

L'identification des facteurs de risque est un processus permettant de trouver, recenser et caractériser les phénomènes dangereux (ISO/CEI Guide 51, 1999). Selon le Guide ISO/CEI 73 (ISO/CEI Guide 73, 2002), c'est un « *Processus permettant de trouver, lister et caractériser les éléments du risque. Les éléments peuvent inclure les sources, les événements, les conséquences et la probabilité. L'identification des risques peut également concerner les préoccupations des parties prenantes* ».

1.1.2 *Estimation des risques*

L'estimation d'un risque se définit comme un : « *Processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque. L'estimation du risque peut considérer le coût, les avantages, les préoccupations des parties prenantes, et d'autres variables requises selon le cas pour l'évaluation du risque* » (ISO/CEI Guide 73, 2002).

1.2 Evaluation de l'acceptabilité des risques

Définitions :

SOURCE	
(Larousse, 2005)	Evaluation: Action d'évaluer, de déterminer la valeur de quelque chose : Faire l'évaluation d'une fortune, d'une distance.
(HMSO, 1995)	Traite de la détermination de la signification des risques estimés pour ceux qui en sont affectés.
(AQS-GT OORS, Mars 1996)	Attribution d'une valeur comparative à une grandeur complexe selon des modalités opératoires spécifiées. Note : la méthodologie d'évaluation constitue un amont incontournable des progrès du management de la sécurité d'entreprise car toute décision raisonnable exige des évaluations comparatives entre les voies possibles.
(GT Aspects sémantiques du risque, 1997)	Démarche formalisée qui comprend les étapes suivantes : Identification du risque, quantification du risque (probabilité et dommages), mise en perspective du risque.

(GT Méthodologie, 2003)	Signification ou "valeur" attribuée au risque estimé par les personnes concernées, en tenant compte de la perception qui en est faite ; cette estimation ou évaluation du risque est souvent réalisée selon deux composantes, la probabilité et les conséquences potentielles d'un risque, par exemple sur une grille de criticité.
(ISO/CEI Guide 51, 1999)	Processus de comparaison du risque estimé à des critères donnés pour déterminer l'importance d'un risque; jugement établi sur la base de l'analyse des risques qui permet de décider si le risque tolérable a été atteint.
(CEI 300-3-9, 1995)	Processus par lequel on juge le caractère tolérable du risque sur la base de l'analyse du risque et en tenant compte de facteurs tels que les aspects socio-économiques et environnementaux.
(ISO/CEI Guide 73, 2002)	Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance du risque. La comparaison peut être menée par rapport à un référentiel préétabli dans l'objectif de permettre la prise de décision vis-à-vis de l'acceptation du risque ou de la nécessité de son traitement. Elle peut considérer le coût, les avantages, les préoccupations des parties prenantes, et d'autres variables requises selon le cas pour l'évaluation du risque.

Synthèse: Il y a dans la définition du GT aspects sémantiques du risque (GT Aspects sémantiques du risque, 1997) des éléments de contradiction avec les définitions précédentes qui font confondre appréciation (analyse + évaluation) et évaluation des risques. De surcroit, selon le dictionnaire Larousse (Larousse, 2006), estimer c'est « évaluer la valeur, faire cas, présumer » et évaluer c'est « estimer la valeur, le prix d'une chose, calculer approximativement ». Nous constatons donc la contradiction avec les sens étymologiques des concepts d'évaluation (donner une valeur) et d'estimation (donner un avis sur une valeur). Ces contradictions proviennent probablement du manque de clarté des définitions linguistiques de certaines références, à l'image des deux définitions rapportées du dictionnaire Larousse où on peut constater que le verbe estimer est défini par rapport au verbe évaluer et vice versa, ainsi ces deux notions assimilées l'une à l'autre se trouvent complètement nuancées.

Proposition : L'évaluation des risques est une procédure de classification de l'acceptabilité de ces risques en fonction des fréquences d'occurrence, gravités, expositions, etc.

1.3 Maîtrise des risques

Définitions :

SOURCE	
(Larousse, 2005)	Maîtrise: Possibilité d'agir sur quelque chose; fait de le dominer techniquement, intellectuellement, scientifiquement. Sûreté de l'exécution dans un domaine technique ou artistique.
(GT Aspects sémantiques du risque, 1997)	Ensemble des disciplines concourant à la réduction et au contrôle du risque, incluant l'évaluation et la gestion du risque.
(ISO/CEI Guide 73, 2002)	Actions de mise en œuvre des décisions de management du risque. La maîtrise du risque peut impliquer la surveillance, la réévaluation et la mise en conformité avec les décisions.

Proposition : La maîtrise des risques (Risk control) est un processus conduisant à évaluer et choisir l'une des différentes possibilités de réduction des risques ; C'est d'une manière générale l'ensemble des actions de mise en œuvre des décisions de la gestion des risques visant à les ramener sous le seuil d'acceptabilité.

1.3.1 *Réduction du risque*

Définitions :

SOURCE	
(ISO/CEI Guide 73, 2002)	Actions entreprises en vue de diminuer la probabilité, les conséquences négatives (ou dommages), associées à un risque, ou les deux.

Proposition : La réduction des risques est l'ensemble des actions entreprises en vue de diminuer la gravité des conséquences (protection), les probabilités d'occurrence (prévention) ou les deux en même temps. Ça pourrait concerner la réduction des temps d'exposition et la multiplication des possibilités d'évitement des situations dangereuses.

1.3.1.1 Protection

Définitions :

SOURCE	
(Larousse, 2005)	Action de protéger, de défendre quelqu'un contre un danger, un mal, un risque: Réclamer la protection des lois. Prendre quelqu'un sous sa protection.

(AQS-GT OORS, Mars 1996)	Ensemble de méthodes, de techniques et de mesures destinées à réduire la gravité des risques et les conséquences d'un incident ou accident. On vise notamment à protéger les personnes et les biens contre des agressions de nature diverses.
(GT 7 - CEI)	Dispositifs, équipements mis en œuvre pour empêcher si possible, ou pour limiter l'importance des effets d'une attaque ou d'un accident.
(GT Aspects sémantiques du risque, 1997)	Ensemble de dispositions propres à réduire les conséquences d'un événement ou d'une situation néfaste
(GT Méthodologie, 2003)	Mesures visant à limiter l'étendue ou/et la gravité des conséquences d'un accident sur les éléments vulnérables, sans modifier la probabilité d'occurrence du phénomène dangereux correspondant. Elles peuvent être mises en œuvre « à titre préventif », avant l'accident, comme par exemple un confinement. La maîtrise de l'urbanisation, visant à limiter le nombre de personnes exposées aux effets d'un phénomène dangereux, et les plans d'urgence visant à mettre à l'abri les personnes sont des mesures de protection.
(CEI 300-3-9, 1995)	Mesures prises pour réduire les dommages causés par un événement.
(EN 292/ISO 12100, 1995)	Mesures de sécurité qui consistent en l'emploi de moyens techniques spécifiques, appelés protecteurs et dispositifs de protection, afin de protéger les personnes contre les phénomènes dangereux que l'application des techniques de prévention intrinsèque ne permet raisonnablement ni d'éviter ni de limiter suffisamment.

Proposition : Technique visant à limiter l'étendue et/ou la gravité des conséquences d'un accident sur les cibles vulnérables. Pour cela on peut soit renforcer la défense des cibles, soit réduire la dangerosité des sources de danger.

1.3.1.2 Prévention

Définitions :

SOURCE	
(Larousse, 2005)	Ensemble des dispositions prises pour prévenir un danger, un risque, un mal ; organisation chargée de mettre en place ces dispositions: Prévention routière. Prévention de la délinquance.
(GT 7 - CEI)	Ensemble d'actions permettant de diminuer la probabilité d'occurrence d'un sinistre, sans pour autant diminuer le montant maximum s'il se réalise.
(GT Méthodologie, 2003)	Mesures visant à prévenir un risque en réduisant la probabilité d'occurrence d'un phénomène dangereux. La réduction de la probabilité passe par l'amélioration de la prévention, par exemple par ajout ou fiabilisation des mesures de sécurité

(EN 292/ISO 12100, 1995)	Prévention intrinsèque: Mesures de sécurité qui consistent à éviter ou réduire autant de phénomènes dangereux que possible en choisissant convenablement certaines caractéristiques de conception, ou bien à limiter l'exposition des personnes aux phénomènes dangereux inévitables ou qui ne peuvent être suffisamment réduits ; ceci s'obtient en réduisant le besoin, pour l'opérateur, d'intervenir dans les zones dangereuses.

Synthèse : La prévention est généralement rattachée aux mesures de réduction de la probabilité d'occurrence d'un phénomène dangereux.

Proposition : Ensemble de méthodes, de techniques et de mesures prises en vue de réduire la probabilité qu'un événement redouté ne se produise. Ces méthodes relèvent de la surveillance, la formation, la réglementation, la répartition des responsabilités, etc.

1.3.2 *Transfert de risque*

Définitions :

SOURCE	
(ISO/CEI Guide 73, 2002)	Partage avec une autre partie de la charge de la perte, ou du bénéfice du gain, d'un risque.

Proposition : Hormis la réduction des risques, la maitrise des risques contient les actions de transfert de risque vers un autre acteur, par exemple, en faisant appel à un assureur qui, par effet de masse, est capable de supporter des risques forts.

2. Classification des méthodes d'analyse de risque

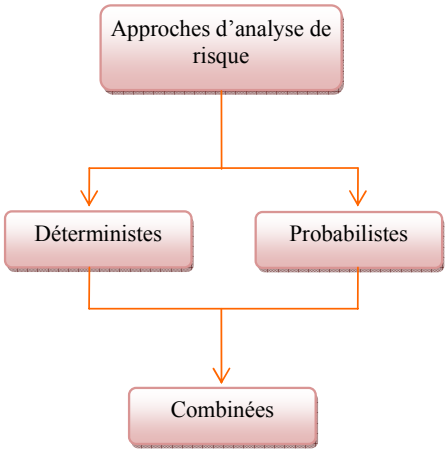


FIG. 2: Approches d'analyse de risque

2.1 Approche déterministe

L'approche déterministe a généralement été adoptée dans les domaines à haut risque tels que nucléaire, militaire, transports guidés, où le moindre risque significatifs est traqué et réduit à la source. Elle consiste à recenser les événements pouvant conduire à un scénario d'accident en recherchant le pire cas possible (*The Worst Case*) et en affectant une gravité extrême à ses conséquences potentielles. Par conséquent, les sous systèmes critiques (systèmes de sauvegarde, de protection et de prévention) sont dimensionnés pour éviter toute défaillance dangereuse et organisés rigoureusement selon une stratégie de défense en profondeur.

2.2 Approche probabiliste

L'approche probabiliste fait intervenir le calcul de probabilités relatives à l'occurrence d'événements faisant partie du processus de matérialisation d'un scénario d'accident donné.

Il s'agit d'une approche complémentaire qui permet d'analyser le dispositif de défense en profondeur décidé à l'issue d'une approche purement déterministe, ceci a été le cas dans le domaine nucléaire ou les techniques probabilistes viennent appuyer l'approche déterministe.

2.3 Méthodes qualitatives vs. Méthodes quantitatives

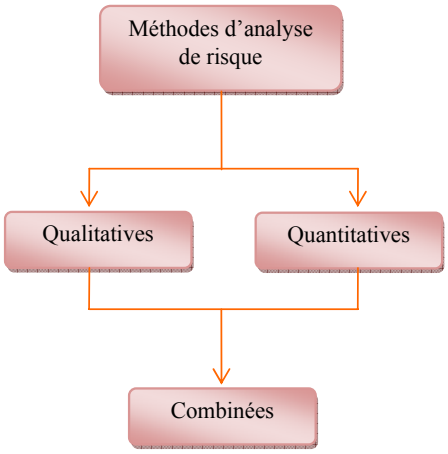


FIG. 3: Typologie des méthodes d'analyse de risque

2.3.1 *Méthodes quantitatives*

Les analyses quantitatives sont supportées par des outils mathématiques ayant pour but d'évaluer la sûreté de fonctionnement et entre autres la sécurité. Cette évaluation peut se faire par des calculs de probabilités (par exemple lors de l'estimation quantitative de la probabilité d'occurrence d'un événement redouté) ou bien par recours aux modèles différentiels probabilistes tels que les Chaines de Markov, les réseaux de pétri, les automates d'états finis, etc.

Les analyses quantitatives ont de nombreux avantages car elles permettent:

- D'évaluer la probabilité des composantes de la sûreté de fonctionnement.
- De fixer des objectifs de sécurité.
- De juger de l'acceptabilité des risques en intégrant les notions de périodicité des contrôles, la durée des situations dangereuses, la nature d'exposition, etc.
- D'apporter une aide précieuse pour mieux juger du besoin d'améliorer la sécurité.
- De hiérarchiser les risques.
- De comparer et ensuite ordonner les actions à entreprendre en engageant d'abord celles permettant de réduire significativement les risques.
- De chercher de meilleures coordination et concertation en matière de sécurité entre différents opérateurs (sous systèmes interagissant) ou équipes (exploitation, maintenance, etc.).

Quoique l'utilité des méthodes quantitatives soit indiscutable, ces dernières présentent tout de même un certain investissement en temps, en efforts et également en moyens (logiciels, matériels, financiers, etc.). Il peut s'avérer que cet investissement soit disproportionné par rapport à l'utilité des résultats attendus, le cas échéant

l'analyse quantitative est court-circuitée pour laisser la place aux approximations qualitatives (statistiques, retour d'expérience, jugement d'expert, etc.).

Un point très important mérite d'être clarifié, c'est que les résultats de l'analyse quantitative ne sont pas des mesures absolues, mais plutôt des moyens indispensables d'aide au choix des actions pour la maîtrise des risques. Nous citons par exemple l'évaluation par des techniques floues/possibilistes de la subjectivité des experts humains, ou la priorisation de certaines actions de maîtrise par rapport à d'autres par une analyse de type coût/bénéfices.

2.3.2 *Méthodes qualitatives*

L'application des méthodes d'analyse de risque qualitatives fait systématiquement appel aux raisonnements par induction et par déduction (Monteau & Favaro, 1990).

La plupart des méthodes revêtent un caractère inductif dans une optique de recherche allant des causes aux conséquences éventuelles. En contrepartie, il existe quelques méthodes déductives qui ont pour but de chercher les combinaisons de causes conduisant à des évènements redoutés.

L'APR, l'AMDEC, l'Arbre de Défaillances ou l'Arbre d'Evénements restent des méthodes qualitatives même si certaines mènent parfois aux estimations de fréquences d'occurrence avant la classification des risques.

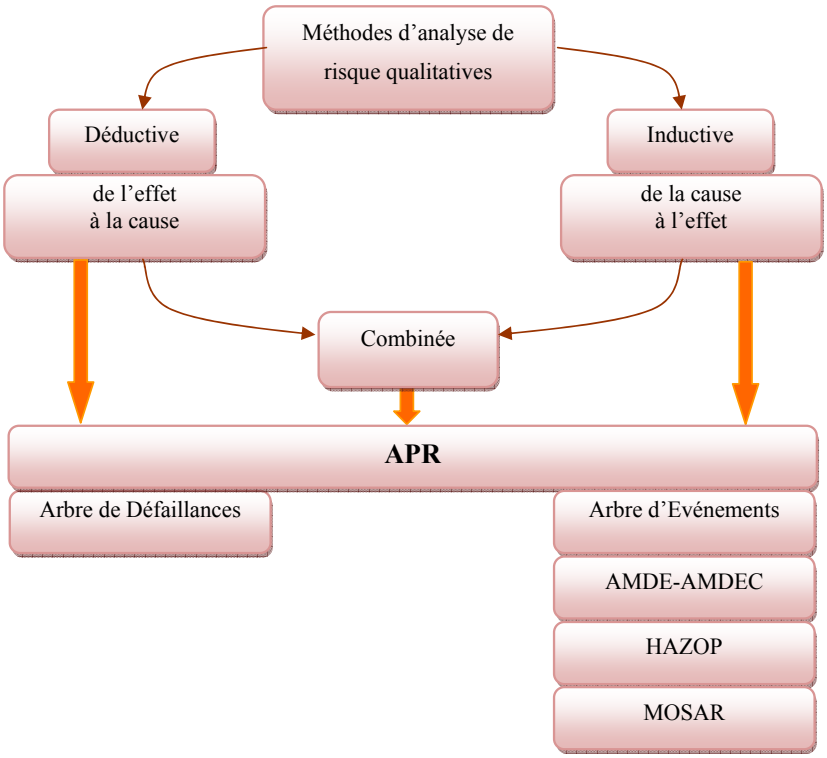


FIG. 4 : Classification des principales méthodes d'analyse de risque qualitatives

Méthodes inductives :

Le principe de ces méthodes consiste à partir d'une cause d'anomalie (défaillance, erreur humaine, agression externe, etc.) et à déterminer les scénarios d'évènements qui en résultent et/ou l'ensemble de ses conséquences possibles (RE. Aéro 701 11 , Novembre 1986).

La démarche inductive suppose la connaissance des causes et l'investigation des effets qu'elles sont susceptibles de provoquer.

Méthodes déductives :

Dans la démarche déductive, on se base plutôt sur la connaissance préalable des effets et on cherche justement à remonter causalement jusqu'aux origines de leur occurrence. Généralement, on part des événements redoutés, et on essaye de trouver leurs causes principales.

3. Panorama des méthodes d'analyse de risque

Nous allons présenter dans cette section un échantillonnage de l'ensemble des méthodes d'analyse de risque. Chacune d'entre elle sera présentée brièvement. Une description plus complète avec les références correspondantes se trouve en annexe A.

3.1 L'Analyse Préliminaire de Risque - APR / Analyse Préliminaire de Danger – APD (Preliminary Hazard Analysis –PHA)

L'analyse Préliminaire de Risque (Danger) a été développée au début des années 1960 dans les domaines aéronautique et militaire.

Selon la norme CEI-300-3-9 (CEI 300-3-9, 1995) *: « L'APR est une technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité* ».

Le but consiste à identifier les entités dangereuses d'un système, puis à regarder pour chacune d'elles comment elles pourraient générer un incident ou un accident plus ou moins grave suite à une séquence d'événements causant une situation dangereuse.

Pour identifier les entités et les situations dangereuses susceptibles d'en découler, l'analyste est aidé par des listes de contrôles (check-lists) d'entités dangereuses, de situations dangereuses et d'événements redoutés. Ces check-lists sont spécifiques au domaine d'étude concerné.

Comme son nom l'indique, cette méthode n'est pas destinée à traiter en détail la matérialisation des scénarios d'accident, mais plutôt à mettre rapidement en évidence les gros problèmes susceptibles d'être rencontrés pendant l'exploitation du système étudié.

Cependant, l'APR peut aussi et même doit être complétée par la plupart des analyses de risques fonctionnelles telles que l'AMDEC ou l'Arbre de Défaillances.

3.2 Analyse des Modes de Défaillances, de leurs Effets - AMDE /et de leur Criticité - AMDEC (Failure Modes, and Effects Analysis - FMEA / Failure Modes, Effects, and Criticality Analysis - FMECA)

L'AMDE a été employée pour la première fois dans le domaine de l'industrie aéronautique durant les années 1960. Son utilisation s'est depuis largement répandue à d'autres secteurs telle que l'industrie chimique, pétrolière ou nucléaire. L'AMDEC est l'extension de l'étude AMDE quand il est question d'évaluer la criticité des défaillances.

Selon la norme CEI-300-3-9 (CEI 300-3-9, 1995), l'AMDE est une technique fondamentale d'identification et d'analyse de la fréquence des dangers qui analyse tous les modes de défaillances d'un équipement donné et leurs effets tant sur les autres composants que sur le système lui-même.

Cette analyse vise d'abord à identifier l'impact de chaque mode de défaillance des composants d'un système sur ses diverses fonctions et ensuite hiérarchiser ces modes de défaillances en fonction de leur facilité de détection et de traitement.

L'AMDE(C) traite des aspects détaillés pour démontrer la fiabilité et la sécurité d'un système. Elle contient 3 (4) parties primaires :

1. Identification des modes de défaillance.
2. Identification des causes potentielles de chaque mode.
3. Estimation des effets engendrés.

S'il s'agit d'une AMDEC:

4. Evaluation de la criticité de ces effets.

L'analyse commence toujours par l'identification des défaillances potentielles des modes opérationnels. Elle se poursuit, par des inductions afin d'identifier les effets potentiels de ces défaillances (situation dangereuse, événement dangereux et dommages). Une fois les effets potentiels établis, on estime le risque on spécifie les actions de contrôle.

3.3 Hazard and Operability Study (HAZOP)

La méthode HAZOP a été développée par la société « Imperial Chemical Industries (ICI) » au début des années 1970. Elle sert à évaluer les dangers potentiels résultants des dysfonctionnements d'origine humaine ou matérielle et aussi les effets engendrés sur le système.

L'objectif de cette méthode est d'identifier les phénomènes dangereux qui mènent à des évènements dangereux lors d'une déviation des conditions normales de fonctionnement d'un système.

L'HAZOP n'a pas pour but d'observer les modes de défaillances à l'image de l'AMDE mais plutôt les dérives potentielles des principaux paramètres liés à l'exploitation de l'installation.

Lorsqu'une déviation est identifiée, l'analyse tente d'identifier les conséquences qui en découlent. Les déviations potentiellement dangereuses sont ensuite hiérarchisées en leur associant des actions de contrôle allouées. La méthode se termine par l'investigation des causes potentielles des déviations jugées crédibles.

De manière générale, les paramètres sur lesquels porte l'analyse sont observables, quantifiables et comparables. Par exemple la vitesse, la température, la pression, le débit, le niveau, le temps, etc.

La combinaison de ces paramètres avec des mots clés prédéfinis (plus que, moins que, pas de, etc.) se fait de la manière suivante :

« Plus de » et « Pression » = « Pression trop haute »,
« Pas de » et « Niveau » = « Capacité vide ».

Dans le cas où une estimation de la criticité est nécessaire, HAZOP est complétée par une analyse a priori de la criticité des risques sur les bases d'une technique quantitative simplifiée.

3.4 What-If Analysis

What-if est une forme dérivée de HAZOP, dont l'objectif est d'identifier les phénomènes dangereux régissant le fonctionnement d'un système.

La méthode consiste à réaliser un *brainstorming* partant généralement de situations dangereuses ou d'événements dangereux imaginés, en essayant de répondre à la question : « *qu'arrive-t-il si tel paramètre ou tel comportement n'est pas nominal ?* ». Ceci va permettre d'identifier les effets provoquant des dommages.

3.5 Analyse par Arbre de Défaillances, Arbre de Causes ou Arbre de Fautes (Fault Tree Analysis - FTA)

L'analyse par Arbre de Défaillances a été élaborée au début des années 1960 par la compagnie américaine « Bell Téléphone ». Elle fut expérimentée pour l'évaluation de la sécurité des systèmes de tir de missiles. Elle est employée pour identifier les causes relatives aux événements redoutés. En partant d'un événement unique, il s'agit de rechercher les combinaisons d'événements conduisant à la réalisation de ce dernier. L'analyse par Arbre de Défaillances peut également être poursuivie dans le cadre d'une reconstitution des causes d'un accident.

La méthode consiste en une représentation graphique des multiples causes d'un événement redouté. Elle permet de visualiser les relations entre les défaillances d'équipement, les erreurs humaines et les facteurs

environnementaux qui peuvent conduire à des accidents. On peut donc éventuellement y inclure des facteurs reliés aux aspects organisationnels.

L'analyse par Arbre de Défaillances se déroule généralement en 3 étapes :

- Spécification du système et de ses frontières.
- Spécification des événements redoutés préalablement identifiés par exemple par APR.
- Construction des arbres de défaillances : On cible les événements redoutés un par un et on essaye d'identifier les successions et les combinaisons d'événements de base permettant de les atteindre.

Toutefois, un événement de base doit répondre à un certain nombre de critères, en l'occurrence :

- Il doit être indépendant des autres événements de base.
- Il ne doit pas être décomposable en éléments plus simples.
- Il doit avoir une fréquence évaluable.

Le calcul de la probabilité de l'événement sommet se fait à travers la propagation des probabilités d'occurrence des événements de base vers le sommet. Le calcul des coupes minimales peut s'effectuer avec le même principe en essayant cette fois-ci de trouver les plus petits ensembles d'événements de base pouvant mener à un événement redouté. Ceci permettrait de hiérarchiser les événements et d'implanter stratégiquement les barrières de défense afin d'améliorer la fiabilité et la sécurité en même temps.

Une coupe minimale représente la plus petite combinaison d'évènements (chemin critique) pouvant conduire à un événement indésirable (intermédiaire) ou redouté (final). Plus l'ordre d'une coupe minimale est petit, plus l'occurrence de l'événement final suivant ce chemin critique peut paraître probable.

L'affectation des probabilités des événements de base se fait par extraction des bases de données, essais, retour d'expérience (REX), jugement d'experts, audits, etc.

3.6 Analyse par Arbre d'Evènements (Event Tree Analysis - ETA)

L'analyse par Arbre d'Evènements a été développée au début des années 1970 pour l'évaluation du risque lié aux centrales nucléaires.

C'est une technique d'identification et d'analyse de la fréquence des dangers moyennant un raisonnement inductif pour convertir différents événements initiateurs en conséquences éventuelles relatives au fonctionnement ou à la défaillance des dispositifs techniques/humains/organisationnels de sécurité.

À l'inverse de l'analyse par Arbre de Défaillances, l'analyse par Arbre d'Evènements suppose la défaillance d'un composant ou d'une partie du système et s'attache à déterminer les évènements qui en découlent.

L'analyse par Arbre d'Evènements se déroule en plusieurs étapes préliminaires :

- Considération d'un événement initiateur.
- Identification des fonctions de sécurité prévues pour contrôler son évolution.
- Construction de l'arbre.

- Description et exploitation des séquences d'évènements identifiées.

Il serait plus pertinent d'élaborer un Arbre d'Evènements à l'issue d'une première analyse identifiant les accidents potentiels à l'image de l'APR.

Les fonctions de sécurité doivent être assurées par des barrières ayant pour objectif d'empêcher le processus de matérialisation d'un accident provoqué par un événement initiateur.

La construction de l'arbre consiste à envisager soit le bon fonctionnement soit le dysfonctionnement de la première fonction de sécurité en partant de l'événement initiateur.

La suite de la méthode consiste à examiner le développement de chaque branche en considérant systématiquement le fonctionnement ou la défaillance de la fonction de sécurité jusqu'à l'atteinte d'un accident potentiel. La propagation des probabilités d'occurrence des évènements initiateurs permet de calculer la probabilité de l'évènement redouté.

3.7 Nœud papillon (Bowtie Model)

Le « Nœud Papillon » est une approche arborescente développée par SHELL. Il permet de considérer une approche probabiliste dans le management du risque.

Le nœud papillon est une connexion d'un Arbre de Défaillances et d'un Arbre d'Evènements, généralement établie lorsqu'il s'agit d'étudier des évènements hautement critiques.

Le point central du Nœud Papillon est l' « Evénement Redouté Central ». Généralement, ce dernier désigne une perte de confinement ou une perte d'intégrité physique (décomposition). La partie gauche sert à identifier les causes de cette perte de confinement, tandis que la partie droite du nœud s'attache à déterminer les conséquences de cet événement redouté central (INERIS-DRA, 2003) (Joly & Vallee, 2004).

Chaque scénario d'accident est relatif à un évènement redouté central et est représenté à travers un chemin possible allant des évènements indésirables ou courants jusqu'à l'apparition des effets majeurs.

Un Nœud Papillon est généralement précédé par une analyse de risque plus générique de type APR ou What-If..

3.8 Analyse de la fiabilité humaine (Human Reliability Analysis)

HRA traite l'impact des facteurs humains sur la qualité de fonctionnement du système. Elle peut être employée afin évaluer l'influence des erreurs humaines sur la sécurité.

De nombreux processus comportent un potentiel d'erreur humaine. L'erreur humaine (Mistake, Human error) est définie dans la norme CEI 50(191) (CEI 50(191), 1990) comme une : *« action humaine qui produit un résultat différent de celui qui est recherché »*. Selon la même norme: « une erreur est un écart ou discordance

entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte ».

L'humain est souvent perçu comme le maillon faible d'un système socio-technique malgré que l'action humaine dans certaines situations demeure la meilleure si ce n'est la seule défense permettant d'éviter qu'une défaillance n'entraine un accident.

La technique HRA comporte 3 étapes principales : l'analyse de la tâche, l'identification de l'erreur humaine et la quantification de la fiabilité humaine. La deuxième étape est la plus longue et nécessite le plus d'efforts.

J. Reason, psychologue d'origine, est l'un des précurseurs ayant considéré l'erreur humaine en tant que défaillance organisationnelle. Selon lui, les erreurs humaines peuvent être classées en trois catégories (Reason & Parker, 1993) : niveau comportemental, niveau contextuel et niveau conceptuel,

J. Reason (Reason & Parker, 1993) défend l'idée de focaliser sur la surveillance proactive des barrières de défense afin de traquer les erreurs latentes. Cependant, cette approche est intéressante pour des barrières techniques, car s'agissant de la 1éme catégorie (niveau comportemental), on passe de la psychologie proprement dite à la sociologie des organisations voire même à la psycho-sociologie (INERIS-DRA, 2003).

3.9 Modèle de danger MADS

Le modèle MADS (Méthodologie d'Analyse de Dysfonctionnement des Systèmes) est une conceptualisation d'une approche systémique du risque d'accident. Le danger est représenté comme un ensemble de processus conduisant à un processus principal représentant le flux de danger pouvant être généré par un système source de danger.

Selon B. Saoulé (Saoulé, 2002) : « *Le flux de danger peut être constitué d'énergie, de matière ou d'information. Il est généré par un événement (ou processus) initiateur d'origine interne ou externe. Ceci se déroule en plusieurs phases, d'abord l'occurrence d'un facteur de déclenchement (événement initiateur) qui génère un flux de danger entre les constituants du système global faisant de l'un d'eux une source et d'un autre une cible de danger. Un Evénement Non Souhaité (ENS) se produit alors et peut générer un dommage subi par la ou les cibles, qui peut être de surcroît accru par un processus renforçateur* ».

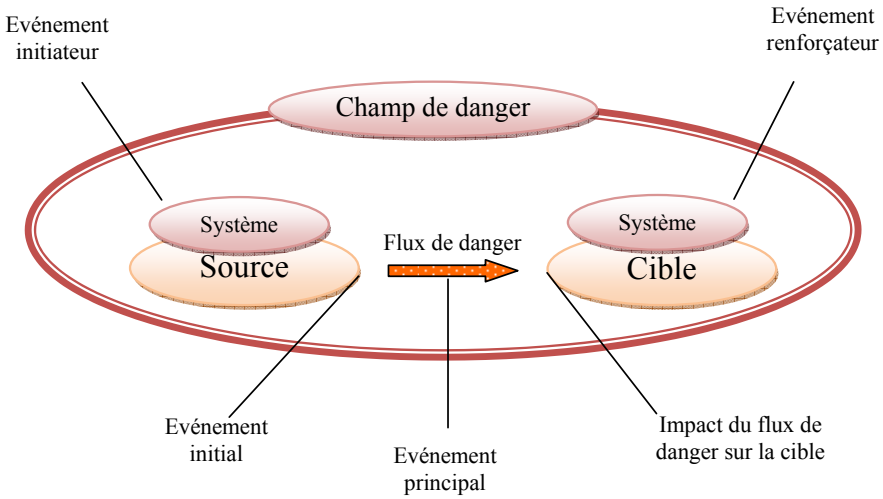


FIG. 5: Processus de danger du modèle MADS (Perilhon, 1999)

Le modèle MADS permet de mettre en relation un système source et un système cible par l'intermédiaire des flux de danger dans un environnement dit « champ de danger ».

Le modèle de référence du processus de danger permet de considérer 4 couples « source, cible ». Le tableau suivant regroupe les différentes possibilités d'interaction entre sources et cibles (Laurant, 2003):

TAB. 1: Classes d'interaction des sources/cibles de danger

Système source	**Système cible**	**Points de vue**
Installation (Système)	Installation (Système)	Sécurité des matériels Sûreté de Fonctionnement
Installation (Système)	Opérateur (Facteur Humain)	Ergonomie Sécurité des installations (systèmes)
Opérateur (Facteur Humain)	Installation (Système)	Fiabilité humaine Malveillance interne
Installation (Système)	Population	Hygiène et santé publique Epidémiologie, génie sanitaire Sécurité industrielle
Population	Installation (Système)	Malveillance externe
Installation (Système)	Ecosystème (Environnement)	Génie sanitaire, écologie Hygiène et sécurité de l'environnement
Ecosystème (Environnement)	Installation (Système)	Risques naturels

3.10 La méthode MOSAR

La méthode MOSAR (Méthode Organisée et Systémique d'Analyse des Risques) a été mise au point par Pierre PERILHON au CEA. Elle est utilisée dans divers domaines, en particulier dans l'étude des risques d'installations à hauts risques (nucléaire, chimique, etc.). En effet, la méthode à été effectivement appliquée dans le domaine nucléaire et notamment à EDF (Centres de recherches et d'essais) et au CEA (Installations d'essais).

MOSAR contient deux modules hiérarchiques, un module macro « module 'A' » et un module micro « module 'B' ».

Le module 'A' a pour but d'identifier les dysfonctionnements techniques et opératoires provoquant un événement indésirable. Les scénarios d'accident sont examinés d'une manière macroscopique, autrement dit, sans traiter en détail des aspects fonctionnels du système et de ses interfaces. Principalement, le module 'A' se décompose en 6 étapes :

- Modélisation de l'installation.
- Identification des sources de danger.
- Identification des scénarios d'accident.
- Evaluation des scénarios de risque.
- Négociation des objectifs.
- Définition des moyens de maîtrise des risques.

Le module 'A' s'appuie essentiellement sur le modèle MADS dans la phase d'identification des sources, flux et cibles de dangers ainsi que les différents événements du processus de danger.

Le module B de la méthode MOSAR qui se présente d'ailleurs comme une suite logique du module A. Il permet d'effectuer une analyse plus détaillée des dysfonctionnements techniques et opératoires et aussi de l'impact qu'ils pourraient engendrer sur le système global. Ce module se décompose en 5 étapes :

- Identification des risques de dysfonctionnement.
- Evaluation des risques en constituant des Arbres de Défaillances.
- Négociation des objectifs précis de maîtrise des risques.
- Affinement des moyens complémentaires de maîtrise des risque.
- Géstion des risques.

4. Propriétés des méthodes d'analyse de risque

4.1 Avantages généraux des méthodes d'analyse de risques

4.1.1 *Identification systématique des composantes du risque*

Les différentes situations dangereuses, évènements redoutés, causes, conséquences, ou accidents potentiels ; tous ces éléments sont identifiés d'une manière méthodologique et présentés dans une forme tabulaire à l'image de l'APR et l'AMDEC, ou arborescente à l'image de l'Arbre de Défaillances ou d'Evénements.

4.1.2 *Communication des risques*

La communication des risques englobe l'échange et le partage d'informations concernant les risques entre le décideur et d'autres parties prenantes. Les informations peuvent concerner l'existence, la nature, la forme, la probabilité, la gravité, l'acceptabilité, le traitement, ou d'autres aspects du risque (ISO/CEI Guide 73, 2002). L'analyse de risque représente un support très efficace d'étude et de communication des risques.

4.1.3 *Complémentarité*

Les méthodes d'analyse de risque sont complémentaires. On peut même interconnecter les résultats (sorties) des unes aux données (entrées) des autres à l'image du nœud papillon. Par exemple, l'APR peut être complétée par une AMDEC ou une étude HAZOP, en faisant porter l'étude cette fois-ci sur les éléments importants pour la sécurité (parties critiques) du système. Ensuite on peut procéder à des études encore plus fines des évènements critiques par Arbre de Défaillances ou d'Evénement ou des deux à la fois à travers un modèle en nœud papillon.

4.2 Lacunes des méthodes d'analyse de risque

4.2.1 *Non prise en compte des facteurs externes au système*

Les facteurs externes au système étudié (conditions climatiques, environnement, facteurs humains) sont rarement pris en compte ou alors pas suffisamment.

4.2.2 *Subjectivité dans l'estimation des risques*

Il est plus raisonnable de considérer que cette phase vise simplement à donner des indications sur les risques les plus significatifs en vue d'envisager des mesures de prévention et de protection. L'estimation des probabilités d'occurrence d'un événement redouté est souvent subjective. L'approche par intervalle, qui consiste à répartir les gravités et les occurrences sur une matrice de criticité avant d'attribuer les niveaux de risque à chaque zone de criticité (Gravité, Occurrence), semble être une technique discriminatoire étant donné qu'il

n'existe aucune règle permettant de définir les limites de ces zones précitées. A ceci s'ajoute aussi la subjectivité de l'analyste dans la désignation d'une zone plutôt qu'une autre. L.-A. Cox est revenu en détail sur les lacunes des matrices de criticité dans un papier intitulé : « What's wrong with risk matrices » (Cox, 2008).

Cepandant, il existe des approches d'évaluation de la subjectivité dans l'estimation des risques, telles que les approches par les théories des sous ensembles flous et la théorie des possibilités (Sallak, Simon, & Aubry, 2007).

Néanmoins, dans certaines méthodes, telles que l'analyse par Arbre de Défaillances, la propagation des probabilités de la base vers le sommet pour estimer la probabilité de l'évènement redouté est mathématiquement faisable. Cependant, la fiabilité des résultats dépend de l'estimation des probabilités affectées aux événements initiateurs (événements de base).

4.2.3 *Non-exhaustivité*

Il est quasiment impossible de tendre vers l'exhaustivité dans la phase d'investigation sur les causes et les conséquences des scénarios d'accident. Généralement, on se contente des causes et des conséquences les plus significatives.

La plupart des méthodes d'analyse de risque (HAZOP, AMDEC, What-if, etc.) visent l'exhaustivité par l'utilisation de mots clés qui évoquent les défaillances ou dérives à envisager. L'expérience montre qu'une utilisation rigoureuse de ces listes en groupe de travail, bien que nécessaire, peut s'avérer rapidement fastidieuse sans pour autant garantir la prise en compte de toutes les situations dangereuses : phases transitoires spécifiques, risque d'effet domino, perte d'utilités, etc. (INERIS-DRA ARAMIS, 2004).

4.2.4 *Non considération du fonctionnement des systèmes non-cohérents*

Selon KAUFMANN (Kaufmann, Grouchko, & Cruon, 1975) : « *un système est dit cohérent quand sa fonction de structure est monotone* ». Autrement dit, une nouvelle défaillance d'un composant ne remet pas en marche un système en état de panne, de même la réparation d'un composant défaillant ne remet pas en panne un système en marche.

Par conséquent, pour pouvoir analyser un système non-cohérent, il est impératif de considérer non plus des ensembles d'événements, mais plutôt des séquences d'événements.

4.2.5 *Non considération des défaillances en mode commun*

L'analyse causale d'un sous système ou d'un composant pris séparément n'est pas complète pour analyser le comportement de systèmes complexes caractérisés par des boucles fermées de rétroaction. Dans ce cas, le raisonnement causal linéaire devient circulaire (Rasmussen & Svedung, 2000).

La plupart des méthodes d'analyse de risque sont caractérisées par une causalité linéaire. Cependant, il existe tout de même un certain nombre de méthodes complémentaires telle que l'A*nalyse des Défaillances de Mode Commun* qui comme son nom l'indique permet d'examiner les défaillances simultanées relatives à des systèmes interagissant.

4.3 Comparaison des méthodes d'analyse de risques étudiées

TAB. 2 : Caractéristiques des méthodes d'analyse de risque

Méthode	Approche Systémique	Approche (D/P/DP) D : Déterministe, P : Probabiliste	Démarche (I/D/ID) I : Inductive, D : Déductive	Identification de scénarios	Estimation de fréquence d'occurrence	Phases du cycle de vie du système						
						R & D (faisabilité)	Conception	Test & validation	Réalisation	Exploitation	Modification	Démantèlement
APD	☺	D	ID	☺		☺	☺	☺			☺	☺
APR	☺	DP	ID	☺	☺	☺	☺	☺			☺	☺
AMDE		D	I					☺		☺	☺	
AMDEC		DP	I		☺			☺		☺	☺	
HAZOP		D	I					☺		☺	☺	
What-If		D	I			☺	☺	☺	☺	☺	☺	☺
AAD		P	D		☺			☺		☺	☺	
AAE		P	I		☺			☺		☺	☺	
Nœud Papillon		P	ID		☺			☺		☺	☺	
HRA			-		☺			☺	☺	☺	☺	
MADS	☺	D	I	☺	☺			☺		☺	☺	
MOSAR	☺	D	I	☺	☺			☺	☺	☺	☺	

What-if est dérivée de la méthode HAZOP qui est à son tour une forme de l'analyse AMDE. HAZOP est employée spécialement dans le domaine de l'industrie chimique. Elle permet de décider si les écarts de la spécification par rapport à la conception peuvent donner lieu à des dangers ou à des problèmes de faisabilité. Cette méthode est particulièrement utile pour identifier des dangers non prévus pouvant être induits lors de la phase de conception (manque d'informations, modifications des conditions de processus ou des procédures de fonctionnement).

L'AMDE est une approche descendante qui tient compte des modes de défaillances de chaque composant pris séparément. Cette méthode véhicule une certaine forme de redondance avant que sa réalisation ne devienne fastidieuse. De même, ses résultats peuvent être difficilement vérifiés par une personne ne maîtrisant pas le système. L'AMDEC, qui est une extension de l'AMDE intègre la notion d'estimation d'occurrence.

Les principaux inconvénients de ces deux dernières méthodes sont la difficulté de traiter la redondance et l'intégration des actions de remise en état. Ainsi l'accent est mis sur des défaillances de composant unique.

Une autre difficulté spécifique aux AMDEC concerne le calcul de la fréquence d'occurrence de la défaillance d'un composant faisant partie d'un système.

En ce qui concerne l'analyse par Arbre d'Evènements, elle peut être employée pour identifier les conséquences possibles, et si nécessaires, leurs fréquences du fait de l'apparition d'un événement initiateur. Cette méthode est fréquemment utilisée dans les installations munies de dispositifs de sécurité intégrés. La technique inductive de l'analyse consiste à répondre à la question fondamentale « qu'arrive-t-il si … ?». La difficulté majeure de cette technique est l'identification des événements initiateurs. En outre, les Arbres d'Evénements traitent uniquement des états de succès et d'échec d'un système et il est difficile d'y intégrer des événements de succès ou de récupération différés ; ce qui est indispensable s'agissant de systèmes non-cohérents.

4.4 Critères de choix d'une méthode d'analyse de risque

Nous avons retenu l'essentiel des critères pesant dans la mise en oeuvre d'une méthode plutôt qu'une autre dans l'étude d'un système donné:

- Domaine de l'étude.
- Stade de l'étude (spécification, conception, .., démantèlement).
- Perception du risque dans ce domaine.
- Culture de la Sûreté de Fonctionnement de l'organisation.
- Caractéristiques du problème à analyser.
- Niveau envisagé de la démonstration de la sécurité.
- Savoir-faire des intervenants.
- Nature des informations disponibles (spécifications du système et de ses interfaces, contraintes, etc.).
- Retour d'expérience et base de données disponibles.
- Moyens humains, logistiques et autres.
- Délais et autres contraintes de management de projet.

Toutefois, l'utilisation séparée d'une seule méthode d'analyse de risque peut ne pas apporter une démonstration définitive de la réalisation des objectifs de sécurité. En effet, il est nécessaire de combiner plusieurs méthodes pour une meilleure complétude et une bonne cohérence en termes de résultats.

4.5 Evaluation de la qualité d'une analyse de risque

La qualité d'une analyse de risque doit être réévaluée au fur et à mesure de l'avancement d'un projet. Pour ce faire, nous proposons un ensemble de critères qui serviront par la suite de repères à nos propositions qui seront formulées dans le cadre des chapitres 5 et 6.

4.5.1 *Cohérence*

La cohérence renvoie aux faits que :

- La démarche soit rationnelle et consensuelle.
- Les données et les résultats ne soient pas contradictoires, c.-à-d. qu'ils ne s'opposent ni entre eux ni avec les hypothèses de départ.

4.5.2 *Complétude*

La complétude peut être formalisée par les hypothèses suivantes:

- S'il existe un chemin causal inductif entre la cause A et la conséquence B, la cause A doit être déduite à partir de la conséquence B d'une façon immédiate ou différée (effet domino) suivant un chemin inverse déductif.
- Par analogie, pour tout chemin déductif, il doit y avoir un chemin inductif équivalent.

4.5.3 *Exhaustivité*

C'est la contrainte la plus difficile à satisfaire ou à démontrer, car l'analyste dans sa représentation de la réalité fait intervenir son intuition et son savoir-faire dans les limites de sa perception de cette réalité. Il peut donc porter un jugement disproportionné sur certains facteurs (cause, effet, probabilité, conséquence, etc.), comme il peut éventuellement manquer d'imagination par rapport à d'autres.

En effet, pour converger vers l'exhaustivité, il convient que l'analyse de risque soit :

- Elaborée au sein d'un groupe d'experts, idéalement en groupe pluridisciplinaire.
- Examinée par de tierces personnes externes.
- Assistée par des outils informatiques d'aide à la décision.

4.5.4 *Intégrité*

Assurance fournie par une organisation que l'analyse de risque est correctement accomplie à moins que les analystes, experts, ingénieurs ou autres, ne préviennent du manque de rigueur dans une quelconque étape, d'un désaccord sur un jugement, de la subjectivité dans l'estimation de paramètres telle que la probabilité d'occurrence, etc.

4.5.5 *Traçabilité*

L'analyse de risque n'est pas un but en soi, mais plutôt un moyen ayant pour but de démontrer le respect des exigences de sécurité. Chaque méthode est praticable dans un contexte particulier du cycle de vie d'un système. Chaqune fait appel aux données disponibles et fournit un certain nombre de résultats qui devraient être repris, en tant que données d'entrée, par l'analyse suivante. Ainsi, de fil en aiguille, on se retrouve entrain de concevoir la partie management des risques du plan général de démonstration et de maintien de la sécuritéen

l'occurrence le SMS pour *Safety Management System* traduit en français par Système de Management de la Sécurité.

5. Conclusion

Nous avons essayé tout au long de ce chapitre de mieux situer la notion d'analyse de risque par rapport aux autres activités du management des risques. Nous avons d'abord clarifié le lien indissociable entre ces deux notions à travers de nombreuses définitions issues principalement des normes et parfois des travaux de groupes de recherche. Ensuite, nous avons présenté rapidement les principales méthodes d'analyse de risque sachant qu'il existe d'autres méthodes moins utilisées dans un contexte industriel telles que : Analyse des Défaillances de Mode Commun, Modèles de Conséquences, Listes des contrôles, Technique de Delphi, Indice de danger, Comparaison par paires, Analyse transitoire, etc.

Après avoir essayé de déceler les points forts et points faibles de ces méthodes d'analyse de risque, nous avons trouvé intéressant de pouvoir les comparer les unes aux autres, et proposer ensuite des critères de choix de la méthode la plus convenable à une étude donnée, et enfin nous avons proposé un certain nombre de critères d'évaluation de la qualité d'une analyse de risque.

Dans le chapitre suivant nous reviendrons avec plus de détail à l'APR telle qu'elle est pratiquée dans différents domaines industriels.

6. Travaux cités

AQS-GT OORS. (Mars 1996). *Management de la sécurité d'entrepreise, vocabulaire et concept.* Association Qualité-Sécurité (AQS) pour l'Observatoire de l'Opinion sur les Risques de la Sécurité.

Barbet, J.-F. (Mars 1996). Maîtriser les risques. *Journal Préventique et Sécurité* .

CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement.* CEI.

CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service.* CEI.

Cox, L.-A. (2008). What's wrong with risk matrices? *Journal of risk analysis* , Vol. 28, No. 2, pp 497-512.

EN 292/ISO 12100. (1995). *Sécurité des machines ; Notions fondamentales, principes généraux de conception.* ISO/CEN.

Gouriveau, R. (2003). *Analyse des risques – Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision.* Thèse de Doctorat, Institut National Polytechnique de Toulouse.

GT 7 - CEI. *Enseignement - Terminologie.* CEI.

GT Aspects sémantiques du risque. (1997). *Vocabulaire lié au risque à travers une analyse bibliographique.* Institut de Protection et de Sûreté Nucléaire (IPSN) - Observatoire de l'Opinion sur les Risques et la Sécurité.

GT Méthodologie. (2003). *Principes généraux pour l'élaboration et la lecture des études de dangers.* INERIS.

HMSO. (1995). *A guide to Risk Assessment and Risk Management for Environmental Protection.* England: Her Majesty's Stationery Office.

INERIS-DRA ARAMIS. (2004). *ARAMIS: Développement d'une méthode intégrée d'analyse des risques pour la prévention des accidents majeurs.* Ministère de l'Ecologie et du Développement Durable - INERIS.

INERIS-DRA. (2003). *Outils d'analyse des risques générés par une installation industrielle.* INERIS, Direction des Risques Accidentels.

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). *Management du risque – Vocabulaire – principes directeurs pour les inclure dans les normes.* ISO/CEI.

Joly, C., & Vallee, A. (2004). *Analyse des risques et prévention des accidents majeurs: Synthèse vis-à-vis de l'étude de danger.* INERIS-Direction des Risques Accidentels.

Kaufmann, A., Grouchko, D., & Cruon, R. (1975). *Modèles mathématiques pour l'étude de la fiabilité des systèmes.* Masson & Cie.

Larousse. (2006). Larousse Définitions.

Larousse. (2005). Larousse Expression.

Laurant, A. (2003). *Sécurité des procédés chimiques.* Lavoisier.

Monteau, M., & Favaro, M. (1990). *Bilan des méthodes d'analyse à priori des risques.* INRS.

Perilhon, P. (1999). *Du risque à l'analyse des risques, développement d'une méthode MOSAR.*

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society.* Karlstad-Suède: Swedish Rescue Services Agency.

RE. Aéro 701 11 . (Novembre 1986). *Recommandations pour les études de l'industrie aérospatiale - Guide des méthodes courantes d'analyse de la sécurité d'un système missile ou spatial.* Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE).

Reason, J., & Parker, D. (1993). *Managing the human factor in road safety.* Maatschappij: The Hague: Shell International Petroleum.

Sallak, M., Simon, C., & Aubry, J.-F. (2007). A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems* .

Saoulé, B. (2002). *Les risques en station de ski alpin : d'une explication monocausale à une perspective d'analyse systèmique.*

TABLE DES MATIÈRES DU CHAPITRE 2: L'ANALYSE PRÉLIMINAIRE DES RISQUES

Chapitre 3

L'ANALYSE PRÉLIMINAIRE DES RISQUES

L'analyse Préliminaire des Risques (APR) a été développée au début des années 60 dans les domaines aéronautique et militaire (CEI 300-3-9, 1995) (SAMRAIL Consortium, Septembre 2003). C'est aujourd'hui la pierre angulaire des études de sécurité dans de nombreuses autres industries.

Après quasiment cinq décennies, la pratique d'APR accuse toujours un problème de compréhension (Mazouni, Aubry, & El koursi, 2008) (Mazouni & Hadj-Mabrouk, 2005). Une enquête[1] réalisée par l'INRS auprès de 220 experts de la sûreté de fonctionnement (Fadier, 2000), révèle que 81% des experts pratiquent l'APR, et seulement 9% d'entre eux considèrent qu'ils la maitrisent. En effet, cette révélation surprenante est justifiée compte tenu des nombreuses difficultés d'ordre méthodologique, terminologique, technique ou organisationnel que nous avons pu identifier. De surcroît, L'APR ne fait toujours pas l'objet d'un projet de normalisation, ce qui ouvre la porte à toutes sortes de divergence.

Notre objectif, dans ce chapitre, est de présenter des méthodes d'APR relatives à différents systèmes et sous-systèmes issues de plusieurs domaines industriels.

Nous avons recueilli les pratiques en usage dans un certain nombre d'entreprises de différents secteurs d'activité lors de rendez vous et par l'analyse de documents qu'elles nous ont prêtés. Par souci de confidentialité nous ne citerons pas les noms de ces entreprises mais seulement leur secteur d'activité.

[1] Les pratiques françaises en matière de sûreté de fonctionnement - Elie FADIER - INRS

1 Méthodologie d'APR dans le domaine des transports terrestres

1.1 Cadre réglementaire

1.1.1 Réglementation nationale

Au niveau national, l'Etat se préoccupe depuis longtemps de la sécurité du réseau ferroviaire et des systèmes de transport guidé. Il a élaboré, ces dernières années, des décrets relatifs à l'exploitation sûre des réseaux de transport guidé (GTR 55, 2000).

Le « décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national » (Secrétariat Général du Gouvernement, 2000) stipule que : « *l'exploitation et la maintenance des infrastructures, des installations techniques et de sécurité et des matériels roulants sont conçues et mises en œuvre de manière à permettre le maintien de leur niveau de sécurité pendant toute la durée de leur exploitation* ».

Le Dossier Préliminaire de Sécurité (DPS) est introduit pour la première fois dans le cadre du décret n°2000-286. En effet, il convient que le DPS prenne en compte les données techniques et fonctionnelles ainsi que les objectifs de sécurité énoncés au dossier de définition. La réalisation d'un nouveau système ne peut commencer qu'après que le ministre chargé des transports ait approuvé ce dossier. Ce dernier peut, si nécessaire, demander que soient apportés des compléments au dossier de sécurité (DS). Ce dossier est tenu à jour pendant toute la durée de l'exploitation du système considéré.

L'article 16 du décret n° 2003-425 stipule que : « *les travaux de réalisation ou de modification substantielle d'un système de transport ne peuvent être engagés qu'après l'approbation d'un dossier préliminaire de sécurité (DPS) par le préfet du département dans lequel doit être implanté le système, sans préjudice des autorisations éventuellement nécessaires au titre d'autres réglementations* ».

L'article 17 du même décret précise que : « *le dossier préliminaire de sécurité doit démontrer, à partir* ***d'une analyse des risques*** *résultant des options de conception des divers éléments constitutifs du système de transport, que les dispositions fonctionnelles, techniques, d'exploitation et de maintenance prévues pour le projet ainsi que le programme prévu d'essais et de tests, permettent d'atteindre l'objectif de sécurité tout au long de la durée de vie du système, de prévenir les différents types d'accidents étudiés, d'en réduire les conséquences, et de prendre en compte les risques naturels ou technologiques susceptibles d'affecter le système de transport*». L'article 17 évoque une analyse des risques, mais sans préciser qu'il s'agit d'une APR. Néanmoins ceci est dit implicitement par la précision « une analyse des risques résultant des options de conception… » (Mazouni & Hadj-Mabrouk, 2005). Enfin, l'objectif de sécurité préalablement défini repose généralement sur la démonstration du GAME par rapport à un système réputé sûr.

Dans l' « arrêté d'application du 8 janvier 2002 pris pour l'application du décret n° 2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national » (Secrétariat Général du Gouvernement, 2002), il est précisé en annexe 2 qu'une APR devrait contenir les documents suivants :

- Description du fonctionnement du système.
- Identification des événements redoutés liés à la sécurité du système.
- Evaluation et classement des risques associés.
- Liste des mesures de prévention et de protection à mettre en œuvre pour réduire ces risques.
- Guide pour les études de sécurité détaillées ultérieures éventuellement nécessaires.
- Proposition d'allocation des objectifs de sécurité entre les composants du système.
- Cadre de référence pour la validation du projet.
- Cadre de référence pour l'élaboration de la documentation du projet.

Ce même arrêté stipule que : « *dans le DPS on précise les objectifs de sécurité poursuivis et les méthodes qui seront appliquées pour les atteindre, les méthodes de démonstration et les principes dont le respect permettra le maintien du niveau de sécurité pendant l'exploitation du système. Le DPS comporte notamment un document relatif à l'organisation du projet et s'appuie sur les résultats d'une* ***analyse préliminaire des risques (APR)*** *».*

L'annexe 3 l'arrêté d'application du 8 janvier 2002 présente les documents constituant un DPS :

- Plan d'organisation du projet et de management de la sécurité.
- Présentation et justification des objectifs de sécurité.
- Présentation générale du système et de son environnement.
- Description fonctionnelle et structurelle du système et de son environnement.
- Identification des composants de sécurité.
- Documents de référence : textes réglementaires, documents normatifs.
- Liste des spécifications techniques et fonctionnelles du système de référence.
- Liste des spécifications techniques et fonctionnelles du système en projet.
- Liste des constituants possédant déjà des certificats.
- Présentation et justification des écarts éventuels avec le système de référence.
- Résultats de **l'analyse préliminaire des risques.**
- Justification des compétences de l'organisme ou service technique indépendant.
- Plan d'évaluation.
- Présentation détaillée des aspects novateurs du système.
- Présentation et justification des études et vérifications de sécurité.
- Présentation et justification des études de démonstration de la sécurité.
- Liste des documents, intéressant la sécurité et la qualité, à produire par le constructeur.
- Définition et programme prévisionnel des tests et essais.
- Principes d'exploitation et de maintenance envisagés.

Selon l'arrêté d'application du 8 janvier 2002 : « *Le Dossier de sécurité (DS) a pour objet de décrire le système tel que réalisé, d'apporter la preuve du respect des mesures de sécurité exposées dans le dossier*

préliminaire de sécurité. Il contient les conclusions des études de sécurité réalisées et attestation de ***la couverture des risques identifiés dans l'APR****, autrement dit, une démonstration de l'aptitude du système à être exploité et maintenu avec le niveau de sécurité requis* ».

L'annexe 4 de l'arrêté, contient une liste des documents contenus dans un DS :

- Documents descriptifs du système réalisé.
- Liste des composants de sécurité.
- Attestation du respect des méthodes de travail et des référentiels présentés dans le dossier préliminaire de sécurité.
- Présentation et justification des écarts éventuels.
- Objectifs de sécurité.
- Attestation, par la Société nationale des chemins de fer français, de la conformité de la réalisation aux engagements pris dans le dossier préliminaire de sécurité et, le cas échéant, aux prescriptions énoncées dans l'acte d'approbation de ce dossier.
- Rapport de l'organisme ou service technique indépendant.
- Conclusions des études de sécurité réalisées et attestation de **la couverture des risques identifiés dans l'APR**.
- Résultats des tests et essais.
- Plan de documentation et de gestion des modifications.
- Principes suivis pour la sélection, la formation et l'habilitation des personnels.
- Liste des règlements et consignes d'exploitation.
- Présentation et justification des principes de maintenance : liste des documents de référence.
- Présentation de l'organisation de l'exploitation en couvrant notamment les aspects : suivi de l'évolution du niveau de sécurité, statistiques, retour d'expérience, inspections, contrôles et audits.
- Plan d'intervention et de sécurité.

1.1.2 Réglementation Européenne

Malgré l'avancée remarquable en matière de réglementation (Directive 96/48/EC, 23 juillet 1996) (Directive 2001/16/EC, 19 mars 2001) (Directive 2004/49/EC, 29 avril 2004), l'interopérabilité du réseau ferroviaire européen se heurte à de sérieuses difficultés d'ordre procédural et matériel (El-Koursi, Mitra, & Bearfield, 2007). De surcroit, d'un pays membre à un autre, le concept de sécurité change de tenants et d'aboutissants : on retrouve par exemple des pays comme la France, où la sécurité prime sur tout le reste, d'autres pays comme la Grande-Bretagne, où la sécurité est contrebalancée par les surinvestissements qu'elle peut impliquer, et bien d'autres pays où le principe de sécurité est le contraire de ces deux approches française et britannique (Christian, 2002). Ceci complique sérieusement la tâche d'harmonisation des méthodes de sécurité communes, hélas promue par la Commission Européenne depuis le début des années 90. En outre, le problème se pose aussi par rapport à la reconnaissance mutuelle des certificats de sécurité entre les pays membres de la communauté européenne. Ces certificats sont délivrés par les agences ferroviaires nationales.

1.2 Méthode d'APR à « Entreprise 1 »

L'« Entreprise 1 » est spécialisée dans la construction de matériels ferroviaires. Elle peut intervenir en qualité de maître d'œuvre, fournisseur de système ou fournisseur de matériels.

L'analyse commence par l'identification des dangers en se basant principalement sur le retour d'expérience pour établir la liste préliminaire de dangers. Une fois la liste des dangers est arrêtée, on procède à un recensement des dispositions techniques permettant de garantir la sécurité. Ces dispositions peuvent être classées soit par sous-système soit par danger.

Ces résultats sont repris dans le cadre d'une analyse tabulaire (voir TAB. 1) déductive en vue de mettre en évidence :

- La liste des événements dangereux précurseurs d'accident potentiel.
- Les mesures de réduction de risques.
- L'allocation des responsabilités aux différents intervenants.
- La couverture des risques à travers l'évaluation a posteriori de la gravité et de la fréquence.

TAB. 1 : Présentation des résultats d'APR selon « Entreprise 1 »

1	2	3	4	5	6	7	8	9	10	11	12	13
Accident potentiel	**N°**	**phase**	**Evénements dangereux**	**causes**	**Conséquences**		**Mesures prises**			**Evaluation du risque**		
					Conséqu-ences	**Gravité**	**libellé**	**type**	**Resp**	**Grav**	**Fréq**	**Accept**

Les causes (colonne 5) entrainant les événements dangereux peuvent être des dysfonctionnements, des causes externes ou des problèmes opératoires.

1.3 Méthode d'APR à « Entreprise 2 »

L'« Entreprise 2 » est leader mondial en métro automatique et automatismes appliqués aux transports urbains.

L'APR fait partie intégrante des activités de sûreté de fonctionnement de cette entreprise. Elle sert généralement à identifier et évaluer la criticité des événements redoutés et ensuite proposer des mesures de prévention et de protection permettant de maîtriser les risques inhérents.

Il existe deux types d'APR hiérarchiques : l'APR système réalisée en début de projet et les APRs sous-systèmes.

La méthode d'APR suivie se décompose en plusieurs étapes :

1. Etablissement de la liste préliminaire d'événements redoutés.
2. Recherche des événements redoutés.
3. Recherche des situations conduisant aux événements redoutés.

4. Evaluation et classification des risques.

En effet, on part de l'établissement par retour d'expérience d'une liste préliminaire d'événements redoutés :

1. Collision du train avec un objet ou une personne

2. Déraillement du train

…

Pour compléter la liste préliminaire des événements redoutés et la rendre plus exhaustive, on cherche à identifier les conditions progressives de leur production :

1. Collision du train avec un objet ou une personne
   1.1. avec une partie mécanique pendant le mouvement des trains et les interventions sur site / hors site
      1.1.1. due à une partie mécanique d'un train tombée sur la voie
   1.2. avec un autre train arrêté ou roulant pendant le mouvement des trains
      1.2.1. due à un rattrapage
      1.2.2. due à une prise en écharpe
      1.2.3. due à une rencontre frontale
      …

L'analyse se poursuit par l'élaboration d'un arbre de défaillances pour rechercher les situations conduisant aux événements redoutés :

1. Collision du train avec un objet ou une personne
   1.1. avec une partie mécanique pendant le mouvement des trains et les interventions site / hors site
      1.1.1. due à une partie mécanique d'un train tombée sur la voie
         1.1.1.1. ayant pour origine une mauvaise fixation de la partie mécanique
            1.1.1.1.1. due à une erreur de conception ou de réalisation
            1.1.1.1.2. due à une opération de maintenance non-conforme
            …….

Pour chacune des situations identifiées lors de l'étape précédente, on évalue le risque associé. Il est défini par la jonction entre la probabilité d'occurrence de l'événement redouté et de la gravité des dommages qu'il est susceptible de provoquer.

Items	**Evénement redouté**	**Mode d'utilisation**	**Situation conduisant à l'événement redouté**		**Risque**	
			Origine	**Cause**	**Gr.**	**Niveau**

Items	Evénement redouté	Mode d'utilisation	Situation conduisant à l'événement redouté		Risque	
			Origine	Cause	Gr.	Niveau
1.1.1.1.1	Collision du train avec une partie mécanique d'un train tombée sur la voie	Pendant le mouvement des trains et les interventions sur site / hors site	Mauvaise fixation de la partie mécanique	Erreur de conception ou de réalisation	2	Inacceptable
1.1.1.1.2	Collision du train avec une partie mécanique d'un train tombée sur la voie	Pendant le mouvement des trains et les interventions sur site / hors site	Mauvaise fixation de la partie mécanique	Opération de maintenance non conforme	2	Inacceptable

La dernière étape consiste à proposer des mesures de protection et de prévention des risques classés inacceptables ou indésirables.

Les résultats de l'analyse sont présentés dans un tableau de la forme suivante (voir TAB. 2) :

TAB. 2 : Présentation des résultats d'APR selon « Entreprise 2 »

Items	Evénement redouté	Mode d'utilisation	Situation conduisant à l'événement redouté		Risque		Exigences de sécurité / Moyens de couverture	Domaine d'application
			Origine	Cause	Gravité	Niveau		

1.4 Méthode d'APR à « Entreprise 3 »

L'« Entreprise 3 » est leader en matière de transport terrestres de voyageurs.

L'analyse commence par l'élaboration de l'arborescence des dangers (voir TAB. 3). Cette phase s'appuie principalement sur le retour d'expérience pour déterminer la liste des accidents potentiels, ensuite on essaye de déceler par déduction les événements redoutés correspondants.

Les résultats sont mis dans un tableau d'analyse élémentaire qui a la forme suivante :

TAB. 3 : Arborescence des dangers

Accident potentiel		Evènement redouté
1. Collision	1.1 avec obstacles	1.1.2 Distance d'arrêt trop longue
		…….
	1.2 avec tiers	1.2.1 Présence d'un véhicule routier ou de service sur la voie

L'analyse continue suivant une démarche déductive afin d'identifier les causes et les origines des événements redoutés.

La dernière étape concerne l'allocation des mesures de réduction de risques qui en fonction de l'évaluation des conséquences relatives à chaque événement redouté. La précision des acteurs concernés par ces

mesures est un aspect organisationnel permettant de définir clairement les responsabilités et d'officialiser le suivi des risques.

Les résultats de l'analyse sont présentés de la manière suivante (voir TAB. 4) :

TAB. 4 : Présentation des résultats d'APR selon « Entreprise 3 »

1	2	3	4	5	6	7	8	9
Accident potentiel	**Événement redouté**	**Lieu**	**Cause potentielle**	**Elément en cause**	**classe de gravité**	**Type**	**Mesures en réduction du risque**	**Acteur concerné**

Les accidents potentiels (colonne 1) et les événements redoutés (colonne 2) correspondant sont décelés à l'issue de la phase d'élaboration de l'arborescence des dangers.

Un Elément en cause (colonne 5) de l'événement redouté peut être de différentes natures: voie, infrastructure, signalisation, etc.

Les classes de gravité (colonne 6) sont dérivées de la norme NF EN 50126 (NF EN 50126, Janvier 2000).

1.5 Méthode d'APR à « Entreprise 4 »

La méthode d'APR suivie à l'« Entreprise 4 », spécialisée dans les systèmes de transport à câble, se décompose en trois phases complémentaires :

1. Identification et évaluation des situations dangereuses.
2. Allocation d'un niveau de criticité aux sous-ensembles de mesures de maîtrise des risques.
3. Analyse détaillée par AMDEC des sous-ensembles pour s'assurer que le niveau de criticité alloué est atteint.

L'élaboration de liste préliminaire des situations dangereuses se déroule selon les étapes suivantes :

1. Elaboration d'une liste de phénomènes dangereux.
2. Identification des situations dangereuses.
3. Evaluation de la gravité et de la probabilité d'occurrence de l'accident.
4. Déduction du niveau de risque de chaque situation.
5. Détermination des actions de maîtrise des risques.

En se basant principalement sur le retour d'expérience, les situations dangereuses pouvant conduire à un accident sont hiérarchisées dans des listes préliminaires.

Les mesures de maîtrise des risques sont allouées en fonction de l'estimation du niveau de criticité de chaque situation.

La méthode se poursuit par une analyse détaillée des sous-ensembles lors de laquelle un niveau de criticité est attribué à chacun des composants en fonction de la criticité du sous-ensemble auquel il appartient et de la présence ou non de composants redondants.

Les composants sont analysés un par un à l'aide d'une AMDEC afin de s'assurer que le niveau de criticité requis par l'analyse préliminaire des situations dangereuses est atteint.

1.6 Méthode d'APR appliquée au « sous-système X »

Il s'agit d'un sous-système de contrôle commande visant l'interopérabilité des réseaux européens à grande vitesse.

La méthode consiste principalement à identifier les événements dangereux, les dangers associés, et les exigences de sécurité requises (voir FIG. 1) :

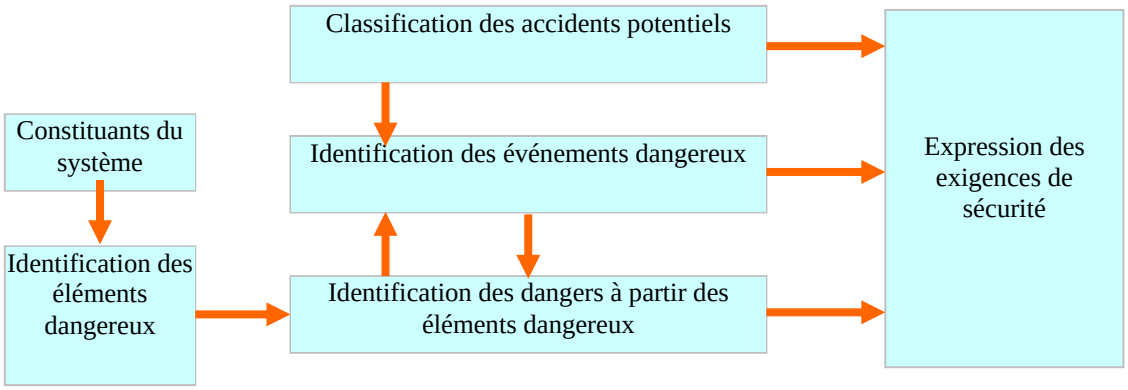


FIG. 1: Méthode d'APR appliquée au « S\Système X »

L'identification des événements dangereux commence d'abord par la classification des accidents par une analyse croisée entre l'emplacement des personnes (par exemple : dans le train ou sur le quai) et les situations possibles d'exploitation (par exemple : en évacuation).

Emplacement de la personne	Phase d'exploitation	Accidents

Ensuite, à partir de la liste des accidents potentiels, on procède à la recherche des dangers et à la détermination des événements dangereux pouvant conduire à ces dangers.

Cette étape permet de faire ressortir l'origine détaillée des accidents potentiels identifiés précédemment. Les dangers et les événements dangereux initiateurs sont alors déterminés.

Cette détermination se réalise en trois étapes inductives successives :

1. Détermination des conditions d'occurrence de l'accident potentiel
2. Détermination des dangers
3. Détermination des événements dangereux : pour chaque danger identifié on recherche les défaillances matérielles ou fonctionnelles qui peuvent l'amorcer

Accident potentiel	Conditions d'occurrence	Danger	Evénement dangereux

L'identification des dangers consiste à déterminer les éléments constitutifs du « sous-système X » considérés comme dangereux et à identifier ensuite les dangers induits pouvant conduire à des accidents potentiels.

Famille	Elément	Sous-élément n1	Sous-élément n2	Danger lié au « Sous-système X »	Evénement dangereux

A partir des événements dangereux, on détermine la criticité des accidents potentiels.

Item	Effet	Risque	Circonstance	Gravité	Occurrence	Criticité	Remarques

Finalement on détermine les critères de sécurité permettant de réduire les risques. Plusieurs classes de critères sont définies en fonction de l'impact sur l'exploitation, sur l'ensemble bord ou sur l'ensemble sol.

Réf.	Critère	Responsable

2 Méthode d'APR issue du domaine aéronautique

Selon C. Lievens (Lievens, 1976), l'APR a pour objet d'identifier les risques et leurs causes (éléments dangereux, situations dangereuses, accidents potentiels), ensuite de déterminer la gravité de leurs conséquences et enfin de définir les règles de conception et les procédures permettant de maîtriser les situations dangereuses et les accidents potentiels.

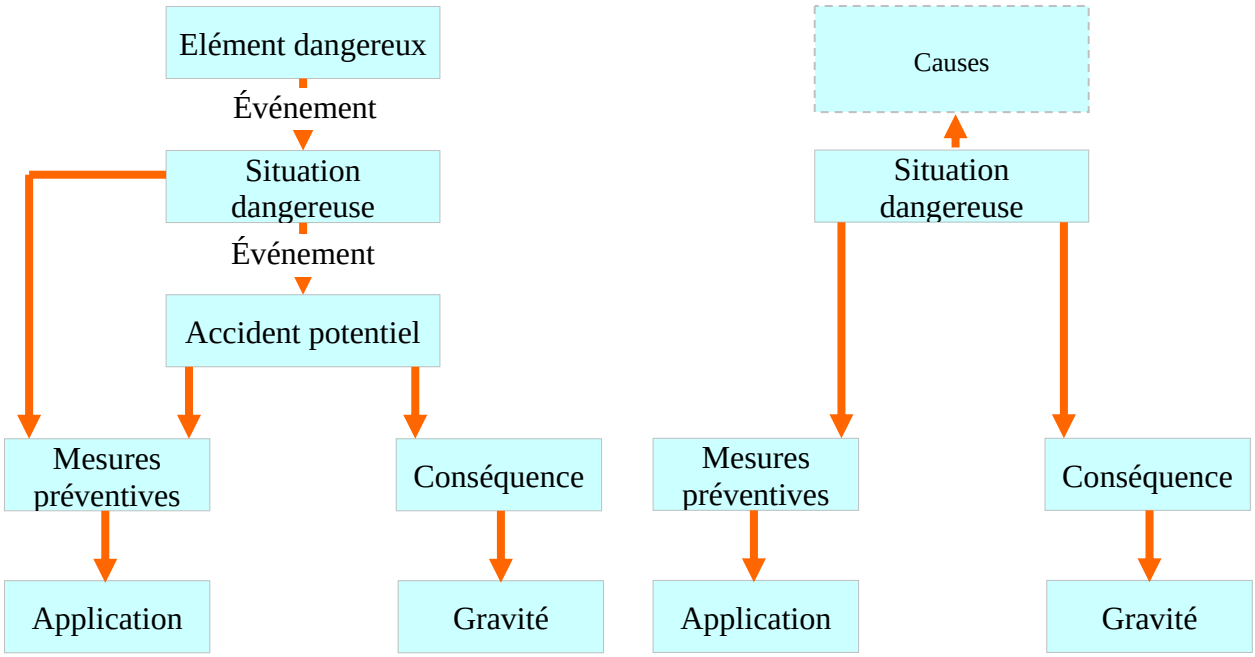


FIG. 2: APR, AER (Lievens, 1976)

L'analyse élémentaire de risques est une autre démarche simplifiée centrée cette fois-ci sur la situation dangereuse et non pas sur l'élément dangereux (voir FIG. 2).

Concernant la présentation des résultats, il existe deux manières de présenter les résultats d'APR : la forme tabulaire et la forme arborescente. Cependant, cette deuxième forme est rarement mise en œuvre.

Le tableau suivant (voir TAB. 5) ne contient pas l'estimation d'occurrence d'accident. C'est un prototype d'APD appliquée dans le domaine aéronautique (Lievens, 1976):

TAB. 5 : Présentation des résultats d'APR selon Lievens

1	2	3	4	5	6	7	8	9	10	11
Système ou fonction	**Phase**	**Elément danger-eux**	**Evénement causant une situation dangereuse**	**Situation dangereuse**	**Evénement causant un accident potentiel**	**Accident potentiel**	**Effets ou conséqu-ences**	**Classific-ation par gravité**	**Mesures Préven-tives**	**Application de ces mesures**

La démarche d'APR se déroule suivant les étapes suivantes :

1. Spécification de l'élément à étudier,
2. Identification des phases durant lesquelles une situation dangereuse est possible,
3. Identification des entités dangereuses,
4. Identification des conditions, événements indésirables, pannes ou erreurs mettant l'élément étudié en danger.
5. Identification des situations dangereuses,
6. Identification des conditions, événements indésirables, pannes ou erreurs mettant l'élément étudié en situation d'accident.
7. Identification des accidents potentiels
8. Estimation des dommages d'accident potentiel,
9. Estimation des gravités d'accident potentiel,
10. Proposition de mesures préventives,
11. Suivi de l'application de ces mesures.

Les mesures de protection n'ont pas été évoquées car le descripteur d'APR proposé est un prototype utilisé dans l'industrie aéronautique où la réduction de l'occurrence des accidents prime sur la réduction de leur impact.

3 Méthode d'APR issue du domaine de l'énergie

A. Villemeur (Villemeur, 1988) précise que l'Analyse Préliminaire de Dangers (APD) a deux objectifs principaux : d'abord identifier les dangers et les causes (entités dangereuses, situations dangereuses, accidents potentiels) et ensuite évaluer leur gravité.

A l'issue de l'identification et de l'évaluation, les moyens et les actions correctrices sont alloués afin de maîtriser les situations dangereuses et les accidents potentiels analysés (Villemeur, 1988).

L'auteur ajoute que l'APR est une extension de l'APD en introduisant l'estimation des fréquences d'occurrence des accidents potentiels. Cette particularité est un critère pertinent à définir les priorités dans l'allocation des mesures de prévention en fonction de l'occurrence des accidents potentiels les plus probables.

L'APR comme son nom l'indique est préliminaire aux études complémentaires de sécurité. Son objectif est de mettre en évidence les scénarios dangereux qui méritent une étude prévisionnelle plus approfondie par d'autres méthodes appropriées telles que l'AMDEC, l'Arbre de Défaillances, etc.

TAB. 6 : Présentation des résultats d'APR selon Villemeur

1	2	3	4	5	6	7	8	9	10	11
Système ou fonction	**Phase**	**Entités danger -euses**	**Evénement causant une situation dangereuse**	**Situation dangereuse**	**Evénement causant un accident potentiel**	**Accident potentiel**	**Effets ou conséque nces**	**Classific- ation par gravité**	**Mesures Préven- tives**	**Application de ces mesures**

On peut remarquer que A. Villemeur (Villemeur, 1988) et C. Lievens (Lievens, 1976) emploient quasiment le même formalisme de présentation tabulaire proposé par C. Lievens (Lievens, 1976) mais à une légère différence en ce qui concerne la colonne n°3, Villemeur emploie le terme entité dangereuse (voir TAB. 6) tandis que Lievens emploie le terme élément dangereux (voir TAB. 5):

Nous avons constaté que le terme danger est employé par A. Villemeur pour désigner en même temps l'accident potentiel et la situation dangereuse. Nous avons montré dans le premier chapitre que les concepts d'accident et de danger sont complètement différents.

4 Conclusion

L'Analyse Préliminaire de Risque se tient pour la première fois entre la phase de spécification et la phase de conception du système. Ce qui fait d'elle à ce stade la première étude de sécurité. Cependant le mot « Préliminaire » n'exprime pas le fait qu'elle se tient à un stade avancé dans le cycle de vie d'un système car l'analyse est itérative et son dossier doit rester ouvert pour accompagner l'étude de sécurité pendant tout le cycle de vie du système (Mazouni & Aubry, 2007) (Mazouni, Bied-Charreton, & Aubry, 2007). Aujourd'hui plusieurs centrales arrivent en fin de vie après plus de 30 ans d'exploitation (durée de vie moyenne). Par conséquent, le prolongement de toute activité d'exploitation se traduit par une nouvelle itération de l'APR ainsi que d'autres études de sûreté de fonctionnement afin de démontrer le maintien des objectifs de sûreté de fonctionnement pendant cette prolongation et également pendant la phase de démantèlement qui viendra inévitablement par la suite (NEA - OECD, 2005).

Qu'elle peut être donc la signification du mot préliminaire ? Notre point de vue est que l'APR n'est pas préliminaire dans le temps, mais l'est par rapport aux autres études de sécurité. Ainsi, ses résultats sont exploités par la plupart des analyses de risque (AMDEC, Arbre de Causes, Arbre d'Evénements, HAZOP, Nœud Papillon, HRA, etc.). A cet effet, nous avions bien voulu lui réserver un chapitre entier car nous pensons que c'est l'analyse qui pose le plus de problèmes au management des risques étant donné qu'elle n'est pas normalisée !

Nous pouvons dire que la pratique d'APR est très diversement perçue. Il faut d'abord remarquer que dans la majorité des cas, il s'agit d'Analyses Préliminaire de Danger (APD), car seule la gravité est prise en

compte ; on devrait donc parler d'APD, que d'ailleurs les anglo-saxons dénomment « Preliminary Hazard Analysis (PHA) ».

L'étude méthodologique que nous avons pu réaliser dans ce chapitre va nous permettre ultérieurement, dans le quatrième chapitre de déceler les problèmes majeurs régissant conjointement la pratique de l'APR et du management des risques. Nous essayerons de remédier à ces problèmes par le biai des solutions que nous développerons dans le cadre des 3 derniers chapitres de ce mémoire.

5 Travaux cités

CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement.* CEI.

Christian, P. (2002). *L'Europe ferroviaire est-elle sur la bonne voie ?* les documents d'information de l'assemblée nationale, n° 388.

Directive 2001/16/EC. (19 mars 2001). *Directive of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 2004/49/EC. (29 avril 2004). *Directive of the European Parliament and of the Council on safety on the Community's railways.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 96/48/EC. (23 juillet 1996). *Directive of the European Parliament and of the Council on the interoperability of the trans-European high-speed rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

El-Koursi, E., Mitra, S., & Bearfield, G. (2007). Harmonizing Safety Management Systems in the European Railway Sector. *Safety Science Monitor* , Issue 2, Vol 11, 1-14.

Fadier, E. (2000). Les pratiques françaises en matière de sûreté de fonctionnement. *Congrès Lambda Mu 12* .

GTR 55. (2000). *Les analyses préliminaires de risques appliquées aux transports terrestres guidés.* Institut de Sûreté de Fonctionnement - Collège sécurité.

Lievens, C. (1976). *Sécurité des systèmes.* Cépaduès.

Mazouni, M.-H. (2007, Avril). Modélisation générique des scénarios d'accident dans le but d'harmoniser les APRs. *Communiquer, naviguer,surveiller - Innovations pour des transports plus surs* , Actes INRETS n° 112, pp 17-27. Actes INRETS.

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, M.-H., & Hadj-Mabrouk, H. (2005, Avril). L'analyse des risques d'accidents dans les transports ferroviaires. Québec-Laval.

Mazouni, M.-H., & Hadj-Mabrouk, H. (2005, Décembre). Méthode et formalisme de base pour l'Analyse Préliminaire des Risques appliquée dans le transport ferroviaire. *6e Conférence internationale des sciences et des techniques de l'automatique (STA'2005)* . Sousse, Tunisie.

Mazouni, M.-H., Aubry, J.-F., & El koursi, 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, 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.

NEA - OECD. (2005). *Gestion des déchets radioactifs: Vers la réalisation d'un dossier de sûreté - Rapport de synthèse préparé au nom du WPDD par son Groupe d'étude sur l'analyse du dossier de sûreté de démantèlement. Rapport n° 6073.* Paris: Agence pour l'Energie Nucléaire - Organisation de Coopération et de Développement Économique.

NF EN 50126. (Janvier 2000). *Applications ferroviaires : Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).* Paris: AFNOR.

SAMRAIL Consortium. (Septembre 2003). *Analysis of existing approaches, D 2.1.1 report.* European Commission and SAMRAIL partners.

Secrétariat Général du Gouvernement. (2002, Janvier 8). *Arrêté d'application du décret n°2000-286 relatif à la sécurité du réseau ferré national*. Récupéré sur LégiFrance, Le service public de diffusion du droit: http://www.legifrance.gouv.fr

Secrétariat Général du Gouvernement. (2003, mai 9). *Décret n° 2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés*. Récupéré sur LégiFrance, Le service public de diffusion du droit: http://www.legifrance.gouv.fr

Secrétariat Général du Gouvernement. (2000, Mars 30). *Décret n°2000-286 relatif à la sécurité du réseau ferré national*. Récupéré sur LégiFrance, Le service public de la diffusion du droit: http://www.legifrance.gouv.fr/

Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels.* Eyrolles.

TABLE DES MATIÈRES DU CHAPITRE 2: 10 ENJEUX PROBLÉMATIQUES EN MATIÈRE DE MANAGEMENT DES RISQUES

Chapitre 4

10 ENJEUX PROBLÉMATIQUES EN MATIÈRE DE MANAGEMENT DES RISQUES

Dans le cadre de ce chapitre, nous allons recenser les problèmes essentiels pénalisant la pratique de l'analyse de risque et d'une manière générale du management des risques. Nous essayerons de les aborder synthétiquement avant de présenter rapidement les solutions envisagées permettant de rendre plus efficace la pratique du management des risques. Ces solutions seront longuement discutées dans le 5éme et le 6éme chapitre.

1 Difficulté de définition du système et de son environnement

Les spécialistes de la linguistique ont abordé le concept de système avec intérêt. Selon E. Morin (Morin, 1977) un système est une unité globale organisée d'interrelations entre éléments, actions ou individus. Ferdinand De Saussure (1857-1913) (De Saussure, 1913) enrichit cette définition en précisant que cette unité organisée,

faite d'éléments solidaires ne pouvant être définis que les uns par rapport aux autres en fonction de leur place dans cette totalité (unité). V. Bertalanffy (Bertalanffy, Décembre 1972) insiste lui aussi sur l'interaction de l'ensemble d'unités d'un système. De-Rosnay (De Rosnay, 1977) ajoute que cette interaction possède un aspect dynamique et organisé en fonction d'un but.

Cependant, dans la pratique, on peut considérer qu'un système est composé de deux parties: la partie structurelle et la partie fonctionnelle. En effet, il est difficile convient de spécifier clairement l'ensemble des entités structurelles et fonctionnelles et définir les interfaces entre ces entités et également entre elles et l'environnement.

2 Divergence des termes et des concepts

Malgré la richesse de la terminologie de la sécurité, les concepts de base du management des risques souffrent d'une grande fluctuation de définitions plus au moins semblables, parfois même opposées (El-Koursi, Fletcher, Tordai, & Rodriguez, 2006), (IAEA Safety glossary, 2007), (ISO/CEI Guide 2, 1986).

Nous avons de suite constaté, à la lecture des documents que nous avons empreinter des industriels, que les différents acteurs industriels ont de sérieuses divergences dans l'usage des termes relevant du management des risques voire même de la sécurité d'une manière générale.

Souvent les mêmes termes ne renvoient pas vers les mêmes concepts et vice versa. Par exemple, nous pouvons voir à partir du chapitre 3 (§1.2 et §1.4) que le concept de « cause » est employé différemment entre l'« Entreprise 1 » (voir Chapitre 3, TAB. 1, 5éme colonne) et l'« Entreprise 3 » (voir Chapitre 3, TAB. 4) dont d'ailleurs la 4éme colonne est nommée causes potentielles.

Les divergences dans les termes et les concepts représentent un frein à l'échange de connaissances et de savoir-faire en matière de management des risques. En effet, il faut donc converger vers un langage adapté aux différents acteurs (constructeurs, exploitants, experts, administration, etc.). De surcroit, ce langage doit être ouvert en vue de contenir de nouveaux concepts émergents et en même temps adaptable, c.-à-d. que chaque acteur se retrouve à travers ce langage à réaliser ses études de management des risques suivant sa propre méthode et son savoir-faire en la matière.

3 Divergence des Objectifs de Sécurité

Comme présenté au chapitre 1 §5.2.2.1, le risque tolérable est le résultat de la recherche d'un équilibre optimal entre une sécurité absolue idéale et les exigences technico-économiques (GT Méthodologie, 2003).

Justement, les approches de sécurité ont pour vocation de définir les objectifs globaux de sécurité, autrement dit, permettre de statuer si le risque global que présente un système est acceptable ou non, tolérable ou non, et surtout, le cas échéant, définir les limites de l'acceptabilité et celles de tolérabilité.

Dans le monde industriel, on retrouve 3 approches principales et un certain nombre d'approches dérivées. Ces approches sont désignées sous les termes GAME (français), ALARP (britannique) et MEM (allemand) :

- **Principe GAME[1]:** Tout système nouveau ou toute modification à un système en exploitation doit offrir un niveau global de sécurité au moins équivalent à celui de systèmes existants réputés sûrs et offrant des services comparables. L'article n° 3 du premier chapitre du décret du 20 mars 2000 (Secrétariat Général du Gouvernement, 2000) stipule que : « la modification d'un système existant ou la conception et la réalisation d'un nouveau système sont effectuées de telle sorte que le niveau global de sécurité obtenu soit au moins équivalent au niveau de sécurité existant ou à celui de systèmes existants assurant des services ou fonctions comparables, et ce, conformément aux règles, normes et prescriptions relatives, notamment, à la sûreté de fonctionnement, à la qualité et à l'accessibilité ».

  Selon P. Christian (Christian, 2002), une telle approche a en effet le mérite intrinsèque de maintenir une dynamique de progrès en minimisant le risque du « toujours plus ». Elle permet de tirer parti de l'existant, jugé satisfaisant, et donc de bénéficier de l'expérience acquise.
- **Principe ALARP[2]:** Tout système possède une certaine probabilité de défaillance. Le principe ALARP consiste à évaluer le risque (gravité, fréquence) que représente cette probabilité ; ceci en intégrant le coût de la mise en œuvre des actions de réduction. Selon P. Christian(Christian, 2002), ce principe est sans doute celui qui met directement l'accent sur le paramètre financier : « Le standard de sécurité se définit comme devant être 'aussi bas qu'il est matériellement raisonnable' (As Low As Reasonably Practicable). En pratique, l'approche britannique conduit à évaluer le standard de sécurité en le mettant directement en balance avec les surinvestissements qu'il peut impliquer. Le risque se trouve pondéré par le coût qui incomberait à l'entreprise ferroviaire qui voudrait se prémunir efficacement contre lui ».
- **Principe MEM[3]:** Il existe un « risque ambiant » que vit quotidiennement chaque individu, ce risque est calculé en fonction de l'espérance de vie. Le transport constituant une partie de ce risque. En effet, tout nouveau service mis à la disposition de l'usager ne doit pas faire augmenter notablement le risque ambiant, autrement dit, le risque doit alors s'établir à un niveau qui garantisse une « mortalité endogène minimale ».

4 Divergence des Indicateurs de Sécurité

Les niveaux de gravité et de probabilité d'occurrence sont croisés dans une matrice de criticité, un graphe de risques, ou toute autre forme permettant de modéliser une jonction entre la gravité et la fréquence. Généralement, ces classifications permettent de spécifier les différentes zones à risques.

[1] Globalement Au Moins Equivalent

[2] As Low As Reasonably Practicable

[3] Minimum Endogenous Mortality

L'approche de classification par intervalle des niveaux de risque permet d'engager des actions de management des risques portant sur les zones à risque jugés non acceptables, ceci avec une priorité sécurité primaire (voir chapitre 2, §1.3.1).

Les méthodes de classification véhiculent une forte subjectivité, et plus particulièrement en ce qui concerne l'estimation des risques(Cox, 2008). Ceci est dû au fait que les probabilités d'occurrence et les gravités sont regroupées dans des plages prédéfinies en donnant parfois une équivalence quantitative. Quoique, la norme ISO 14971 (ISO 14971, 2000) tempère cet avis en précisant qu'« *une bonne description qualitative est préférable à une inexactitude quantitative* »!

5 Divergences d'ordre méthodologique des analyses de risque

Comme présenté au chapitre 2 §2.3.2, l'approche causale est une manière de dire que rien n'est l'œuvre du hasard, et que derrière tout effet y a au moins une cause possible. En effet, il existe deux sens d'investigation des relations de « cause à effet » : l'approche inductive et l'approche déductive (voir FIG. 1):

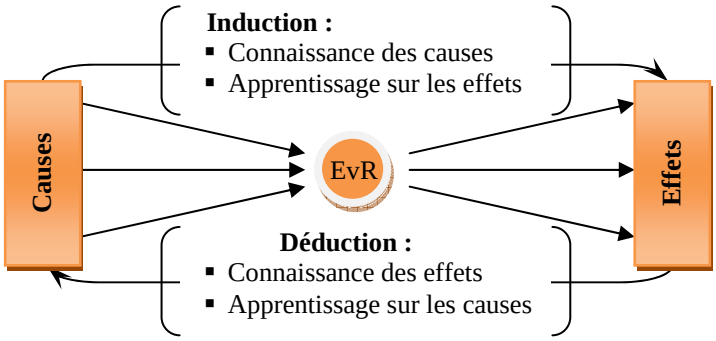


FIG. 1: Raisonnement causal : Induction et Déduction

Théoriquement, les ensembles de causes et d'effets sont divergents. Néanmoins, dans la pratique on se limite à considérer des ensembles représentatifs contenant les éléments les plus crédibles.

La qualité et la quantité d'informations dont on dispose sont des facteurs déterminants dans le choix qui sera porté sur la démarche d'analyse : inductive ou déductive (Mazouni, Bied-Charreton, & Aubry, 2007).

Dans le cas où ces informations portent essentiellement sur les conséquences, on peut donc procéder par déduction afin d'identifier les causes possibles. Les mécanismes de Retour d'Expérience sont largement utilisés dans cette démarche qui semble en parfaite harmonie avec l'exercice de reconstitution des accidents.

La démarche inverse nécessite une bonne connaissance des causes de l'accident. Logiquement, on se situe en amont de l'accident et on tente de dégager les conséquences possibles relatives à une cause donnée. Cette démarche consiste donc à extraire les différents scénarios d'accident potentiels.

Nous pouvons constater que quasiment toutes les méthodes d'analyses de risque permettent d'élaborer, que ce soit par induction ou par déduction, une liste d'événements redoutés et une liste de mesures de maîtrise des risques.

6 Enjeux organisationnels de la maitrise des risques

La connaissance préalable du concept d'accident, de ses mécanismes de causalité ainsi que de son processus de matérialisation permet de mieux identifier les scénarios d'accident et ensuite de placer les barrières de défense en profondeur.

La mise en œuvre des barrières de défense requises doit se baser sur des techniques scientifiques et organisationnelles de management des acteurs. Ainsi, la réalisation ou le contrôle de chaque barrière doit être assigné à une équipe nommée, et la responsabilité technique à un chef qualifié.

En plus de la responsabilité technique, se pose également le problème de la responsabilité hiérarchique. Cette deuxième forme consiste en l'approbation ou le refus des actions recommandées par l'équipe technique chargée de l'analyse et du suivi du risque.

7 Absence de suivi des risques

L'absence de modélisations sémantique d'ontologies d'analyse de risque, rend la maitrise des risques fastidieuse. Ce serait pourtant la meilleure manière permettant d'intégrer le management des risques au processus global du SMS ; ceci en identifiant les interfaces de l'analyse (les données en entrée, les résultats en sortie, les contraintes, etc.). Une fois le processus accidentel dûment conçu, il devient plus viable d'implanter un système de défense en profondeur en fonction des entités, situations et événements élémentaires.

L'estimation a postériori des risques permet d'apporter une assurance quant à l'efficacité des mesures de réduction envisagées. En effet, il convient de suivre l'évolution du risque et évaluer les gains obtenus après mise en œuvre des actions envisagées afin d'éviter que le niveau de sécurité obtenue ne soit pas pire que ce qu'il était avant.

8 Non-prise en compte des effets domino

Le terme « effet domino » se rapporte au fait qu'un accident génère ou enclenche un autre, autrement dit, à l'action d'un processus accidentel affectant une ou plusieurs entités qui pourrait déclencher un accident sur une entité voisine, conduisant à une aggravation générale des conséquences.

Cependant, en dépit de son importance, l'identification des effets domino ne fait pas l'objet d'études sérieuses. Admettons qu'un scénario d'accident 'A' évalué à un niveau de risque indésirable est susceptible

d'enclencher un autre scénario 'B' d'un risque inacceptable. Il convient dans ce cas là de majorer le niveau de risque du premier scénario 'A'.

En effet, il est très important d'identifier les conséquences des scénarios d'accident relatifs à toute entité source de danger et voir si éventuellement elles engendrent un événement dangereux vis-à-vis les autres entités (système global, sous-système, composant, procédure, etc.) situées dans son entourage que nous appellerons dorénavant espace de danger.

9 Enjeux d'interopérabilité : harmonisation des Analyses au niveau système

L'une des préoccupations majeures en matière de management des risques est le fait de rendre les analyses de risques interopérables, autrement dit, que des scénarios d'accident relatifs aux systèmes, soient rapprochés par les mécanismes de similarité, souvent connu en Intelligence Artificielle par RPC (Raisonnement à Partir de Cas, de l'anglais CBR : Case Based Reasoning). Ceci, est une manière forte pour consolider la pratique du principe de sécurité GAME.

10 Enjeux d'intégrabilité : harmonisation des Analyses au niveau sous-système

L'harmonisation a pour but de trouver une passerelle permettant de rendre intégrables les différentes analyses de risque relatives aux sous-systèmes. Ces analyses sont généralement élaborées par des sous-traitants, avant que l'intégrateur ne constitue l'analyse de risque du système global. Ceci permet, entre autres, d'identifier les effets domino entre sous-systèmes et entre sous-système et le système global. Autrement dit, déceler au niveau d'un sous-système les scénarios indésirables susceptibles de constituer des précurseurs à d'autres scénarios induits au niveau d'un sous-système adjacent, ou bien même au niveau du système global.

11 Conclusion et perspectives

D'une manière synthétique, nous pouvons dire que malgré les divergences constatées dans l'emploi des termes, concepts, approches, et autres, les pratiques du management des risques tournent essentiellement autours des quatre exercices suivants:

- Investigation des scenarios d'accident.
- Estimation des risques (par référence aux indicateurs de sécurité).
- Evaluation et acceptation des risques (en fonction des objectifs de sécurité).
- Maitrise des risques.

Cependant, en dépit de leur importance, plusieurs points sont souvent négligés, en l'occurrence :

- La spécification systémique des limites de l'étude (frontières Système/Environnement).
- La spécification ontologique de l'ensemble des constituants du système global.
- La prise en compte, lors de l'estimation de la gravité, des enjeux capitaux tels que techniques, financiers, commerciaux, juridiques, médiatiques et économiques, etc.
- L'estimation de la fréquence (ou probabilité) d'occurrence.
- L'estimation de l'exposition au danger.
- Le suivi des risques.
- L'interconnexion des scenarios d'accidents (effets domino).
- L'interconnexion des sous-systèmes (intégrabilité).
- L'interconnexion de systèmes similaires (interopérabilité).
- L'intégration dans une stratégie globale de SMS (système de management de la sécurité) afin de rendre les résultats profitables par les analyses ultérieures.

Le tableau suivant (voir TAB. 1) présente conjointement les principaux enjeux de la pratique de l'analyse de risques dans le domaine industriel et les solutions que nous proposons et développerons afin d'apporter des éléments de réponses aux problèmes posés:

TAB. 1: Solutions proposées pour améliorer la pratique du management des risques

<table>
<tr><th colspan="2">Quelques difficultés dans la pratique du management des risques</th><th>Solutions proposées</th></tr>
<tr><td colspan="2">Difficultés de spécification des limites et interfaces du système</td><td>Décomposition systémique du système global</td></tr>
<tr><td>Divergence des termes</td><td rowspan="3">Divergence des indicateurs de sécurité</td><td>Découpage des sous-systèmes en entités</td></tr>
<tr><td>Divergence des concepts</td><td>Modélisation d'un processus accidentel ontologique</td></tr>
<tr><td>Divergence des méthodes</td><td rowspan="8">Proposition de la méthode MPR

+

SIGAR (Système Interactif Générique d'Analyse de Risques):

Un outil d'aide à la rédaction, édition, vérification, capitalisation et pérennisation des analyses de risque</td></tr>
<tr><td colspan="2">Absence d'aspects organisationnels et de responsabilisation</td></tr>
<tr><td colspan="2">Absence d'interopérabilité</td></tr>
<tr><td colspan="2">Absence d'intégrabilité</td></tr>
<tr><td colspan="2">Absence de traçabilité des effets domino</td></tr>
<tr><td colspan="2">Absence de suivi des risques</td></tr>
<tr><td colspan="2">Absence de Complétude, cohérence, confidentialité, communication et de portabilité des données</td></tr>
</table>

En effet, il est primordial de stimuler une réflexion plénière dans le but de définir une stratégie globale de convergence vers une réelle compréhension du management des risques, de ses concepts élémentaires et de son processus avant d'aspirer à doter les experts d'outils d'aide à la décision. Nous essayerons d'aborder cette problématique dans le cadre des chapitres ultérieurs.

12 Travaux cités

Bertalanffy, L. (Décembre 1972). The History and Status of General Systems Theory. *The Academy of Management Journal* , Vol. 15, No. 4, General Systems Theory, pp 407-426.

Christian, P. (2002). *L'Europe ferroviaire est-elle sur la bonne voie ?* les documents d'information de l'assemblée nationale, n° 388.

Cox, L.-A. (2008). What's wrong with risk matrices? *Journal of risk analysis* , Vol. 28, No. 2, pp 497-512.

El-Koursi, E.-M., Fletcher, S., Tordai, L., & Rodriguez, J. (2006, February). Safety and interoperability. *SAMNET synthesis report* .

Gallou, G., & Bouchon-Meunier, B. (1992). *Systémique : Théorie & Application.* France: Lavoisier.

Goffin, L. (1976). *Environnement et évolution des mentalités.* Arlon, Belgium: Thèse de doctorat, FUL.

IAEA Safety glossary. (2007). *Teminology used in nuclear safety and radiation protection.* International Atomic Energy Agency.

ISO 14971. (2000). *Application de la gestion des risques aux dispositifs médicaux.* ISO.

ISO/CEI Guide 2. (1986). *Termes généraux et leurs définitions concernant la normalisation et les activités connexes.* ISO.

Le Moigne, J.-l. (1994). *Théorie du Système Général, théorie de la modélisation.* Paris: PUF.

Mazouni, M.-H. (2006, Avril). Concepts et terminologie de base pour l'Analyse Préliminaire des Risques dans le transport ferroviaire. *Communiquer, Naviguer, Surveiller-Innovations pour des transports plus sûrs, plus efficaces et plus attractifs* , Actes INRETS no. 109, pp 143-152.

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, M.-H., & Hadj-Mabrouk, H. (2005, Décembre). Méthode et formalisme de base pour l'Analyse Préliminaire des Risques appliquée dans le transport ferroviaire. *6e Conférence internationale des sciences et des techniques de l'automatique (STA'2005)* . Sousse, Tunisie.

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.

Morin, E. (1977). *La Méthode, 1 : la nature de la nature ; 2 : la vie de la vie.* Le Seuil.

Secrétariat Général du Gouvernement. (2000, Mars 30). *Décret n°2000-286 relatif à la sécurité du réseau ferré national*. Récupéré sur LégiFrance, Le service public de la diffusion du droit: http://www.legifrance.gouv.fr/

Senge, P. (1990). *The Fifth Discipline: The Art & Practice of The Learning Organization.*

TABLE DES MATIÈRES DU CHAPITRE 5 : MODÉLISATION ONTOLOGIQUE DU PROCESSUS ACCIDENTEL

Chapitre 5

MODÉLISATION ONTOLOGIQUE DU PROCESSUS ACCIDENTEL

Ce travail est le résultat d'une analyse des approches utilisées dans les domaines critiques. Il se présente sous la forme d'un continuum de proposition de définitions de concepts liés à l'analyse de risques.

Le langage de la sûreté de fonctionnement est en perpétuelle mutation. En effet, ni la réglementation nationale ou communautaire, ni les normes nationales, européennes ou internationales, ni les glossaires divers et variés n'ont pu unifier un langage consensuel pouvant servir de base universelle d'harmonisation.

Nous avons pu constater, en effet, toutes sortes de divergences terminologiques syntaxiques ou sémantiques. Nous pouvons citer, entre autres, les difficultés suivantes :

- Association d'un même terme à plusieurs concepts,
- Association d'un même concept à plusieurs termes,
- Nuance des liens entre les différents concepts,
- Définition sommaire des termes sous forme de glossaires, souvent présentés par ordre alphabétique,
- Confusion entre les notions d'état et de transition (événements),

- Absence de rattachement au processus accidentel, c.-à-d. à quelle phase se situe un concept donné et quelle peut être sa contribution à la réalisation de l'accident,
- Usage excessif du descriptif textuel, que ce soit à travers des définitions beaucoup plus littéraires que scientifiques, ou voire même l'introduction de sens figurés et d'images ambivalentes. En effet, une phrase compliquée ne fait que rendre le sens plus complexe et par conséquent sujet à diverses interprétations !
- Aléas de la traduction (anglais – français): des termes sont directement traduits en partant d'une compréhension superficielle. En effet, souvent, il existe deux ou trois termes en français pour un même terme en anglais. Ainsi, pour « risk management », on retrouve « gestion des risques » ou « management des risques » et parfois même c'est traduit à tort par « maitrise des risques » ! De même, pour « PHA (Preliminary Hazard Analysis) », on retrouve et « APD (Analyse Préliminaire de Danger) » et « APR (Analyse Préliminaire de Risque) » qui est le nom le plus répandu même s'il est le moins conforme aux normes, en l'occurrence ISO/CEI Guide 73 et Guide 51, précisant que dans une analyse de risque, on commence toujours par identifier les dangers et on finit par estimer les risques inhérents.

La solution que nous proposons, et qui fait l'objet de ce chapitre, repose sur le principe d'ontologie. Pour ce faire, nous allons suivre la démarche suivante :

- Une partie de définition : chaque concept sera présenté sous forme d'un tableau contenant les définitions issues de la littérature, réglementation, normalisation et aussi quelques définitions intéressantes issues des travaux de recherche.
- Une partie de synthèse : dans cette partie nous donnerons notre point de vue et nous commenterons, éventuellement, les différentes définitions.
- Une partie de proposition : nous proposerons des définitions dans le cas où nous ne trouverons pas de définition qui nous semble en harmonie avec l'ensemble des concepts de l'ontologie.

L'originalité de cette ontologie est fondée sur le fait que chaque concept est abordé en fonction de son aspect sémantique et de sa contribution dans la réalisation du scénario d'accident selon un processus accidentel (voir FIG. 3), contrairement à la littérature, où les termes sont souvent définis individuellement et présentés par ordre alphabétique.

1 Introduction aux ontologies

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. Compte tenu de l'intérêt qu'elles représentent, les ontologies ont fait l'objet de normalisation. On peut citer par exemple la norme ISO 21127 (ISO 21127, Août 2002) intitulée « Ontologies nécessaires à la description des données concernant le

patrimoine culturel ». Cette norme à été publiée en 2006 suite à la définition du patrimoine culturel immatériel effectuée par l'UNESCO. Elle décrit en particulier les métadonnées nécessaires à la structuration des ontologies.

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.

Toutefois, avant d'aborder en détail l'ontologie, il convient de dissiper la nuance qui puisse exister avec « Terminologie ». Dans une terminologie on s'intéresse aux mots et au sens, c.-à-d., aux relations entre ces mots; tandis que dans une ontologie, on s'intéresse à la notion de concept et aux relations entre eux.

1.1 Ontologie en tant que notion : une origine métaphysique

Selon Aristote (-384 – -322): « *Il y a une science qui étudie l'être en tant qu'être et les attributs qui lui appartiennent essentiellement* ».

L'ontologie est une notion philosophique grecque très ancienne qualifiée par Descartes et Kant de « *science du fondement de la connaissance* ». Le mot « Ontologos » étant lui même une composition de deux mots : « Ontos » pour dire « être », et « logos » pour dire « mot ». Une notion est toute unité de pensée utilisée pour structurer la connaissance et la perception du monde extérieur et n'est pas forcément exprimée (Charlet, Zacklad, Kassel, & Bourigault, 2000).

Selon le Petit Robert (Petit Robert, 1984) la notion d'ontologie remonte à 1646 (lat. philo. Ontologia, 1646) et elle concerne la « *partie de la métaphysique qui s'applique à l'être en tant qu'être, indépendamment de ses déterminations particulières* ». Le Petit Larousse (Larousse, 2006) évoque une « *Etude de l'être en tant qu'être, de l'être en soi. C'est aussi l'étude de l'existence en général, dans l'existentialisme* ».

Selon Socrate (-469 – -399) et son disciple Platon (-427 – -346) : « *La réalité se présente sous la forme d'individualités uniques et particulières qu'il faut aborder à partir de concepts généraux (tigre, animal, être vivant)* ». Porphyre (234 – 305), philosophe grec du troisième siècle eut insisté sur la catégorisation par identité et différence des êtres dans une forme taxinomique.

Du concept d'ontologie se déclinent plusieurs concepts dérivés, à l'image de « ontologisme » défini par Gioberti (1801 – 1852) comme étant « *une théorie métaphysique affirmant que la connaissance de Dieu directe et immédiate est naturelle à l'Homme* ».

1.2 Ontologie en tant que concept : un devenir « computationnel »

Un concept est une notion exprimée en général par un terme, un symbole ou autre, et qui sert à représenter un ensemble d'objets ou d'êtres ainsi que leurs propriétés communes.

Dans le domaine de l'ingénierie de la connaissance, le concept d'ontologie semble avoir été introduit dans les années 90 lorsque Grüber (Grüber, 1992) introduisit une définition devenue depuis 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* ». Cette définition fut aussitôt réajustée par Grüber (Grüber, 1993) (Grüber & Thomas, 1993) lorsqu'il insista sur les aspects formel et partageable : « *Une ontologie est une spécification formelle* (compréhensible aussi bien par les machines que par les humains) *explicite d'une conceptualisation partagée* (décrit des connaissances consensuelles) ».

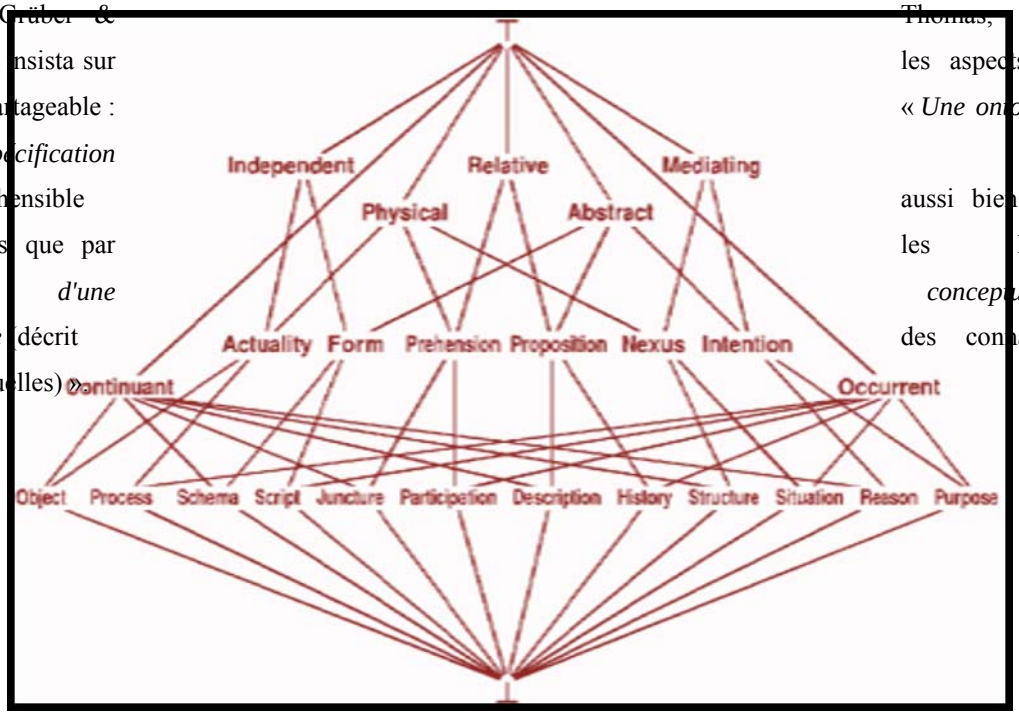


FIG. 1: L'ontologie Sowa (Sowa, 1984)

En effet, dans l'encyclopédie libre Wikipedia on a relevé que « *C'est naturel que le terme soit repris en informatique et en science de l'information, où une ontologie est l'ensemble structuré des termes et concepts fondant le sens d'un champ d'information, que ce soit par les métadonnées d'un espace de noms, ou les items d'un domaine de connaissances*».

En conséquence, on a donné une définition pragmatique plus proche de l'opérationnel que de l'abstrait : « *Une ontologie est un réseau sémantique qui regroupe un ensemble de concepts décrivant complètement un*

domaine. Ces concepts sont liés les uns aux autres par des relations taxonomiques (hiérarchisation des concepts) *d'une part, et sémantiques d'autre part* » (voir FIG. 1).

On peut retrouver aussi dans (Charlet, Zacklad, Kassel, & Bourigault, 2000) une vision plus orientée objet des ontologies : « *Une ontologie est un ensemble des objets reconnus comme existants dans le domaine. Construire une ontologie c'est décider de la manière d'être et d'exister des objets* ».

1.3 Typologie des ontologies

En fonction de leur usage, on distingue cinq catégories d'ontologies (Van Heijst, Schreiber, & Wielinga, 1997) en l'occurrence : générique, de domaine, d'application, de représentation et de méthode :

1. Ontologie générique : décrit des concepts généraux, indépendants d'un domaine ou d'un problème particulier. Il s'agit par exemple des concepts de temps, d'espace et d'événement.
2. Ontologie de domaine : spécifie un point de vue sur un domaine particulier à l'aide d'un vocabulaire lié à un domaine de connaissance générique. Les concepts d'une ontologie de domaine sont souvent définis comme une spécialisation des concepts des ontologies génériques. Une ontologie de domaine est constituée d'une description en extension du vocabulaire du domaine, d'une typologie, et d'une hiérarchie ou un treillis de classes.
3. Ontologie d'application : décrit la structure des connaissances nécessaires à la réalisation d'une tâche particulière (Van Heijst, Schreiber, & Wielinga, 1997). Elle permet aux experts du domaine d'utiliser le même langage que celui de l'application.
4. Ontologie de représentation : définit un ensemble de primitives de représentation des concepts des ontologies de domaine et des ontologies génériques.
1. Ontologie de méthode: décrit le processus de raisonnement d'une façon indépendante d'un domaine et d'une implémentation donnée. Elle spécifie des entités qui relèvent de la résolution d'un problème et fournit les définitions des concepts et relations utilisées pour spécifier un processus de raisonnement lors de la réalisation d'une tâche particulière.

1.4 Représentation des ontologies

Selon G. Diallo (Dialo, 2006): « *On peut distinguer entre les ontologies informelles, qui utilisent le langage naturel et qui peuvent coïncider avec les terminologies, les ontologies semi-formelles, qui fournissent une faible axiomatisation, comme les taxonomies, et enfin les ontologies formelles, qui définissent la sémantique des termes par une axiomatisation complète et rigoureuse* ».

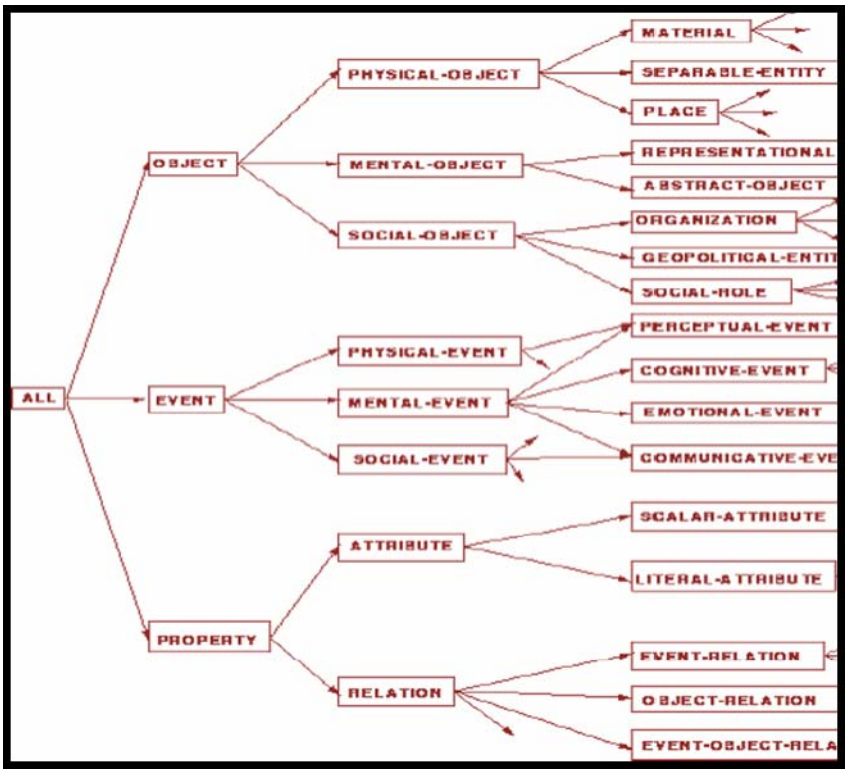


FIG. 2: L'ontologie générique Mikrokosmos (Manesh, 1996)

Les ontologies décrivent généralement les individus, les classes (ensembles, collections, ou types d'objets), les attributs (propriétés, fonctionnalités, caractéristiques ou paramètres des objets), les relations entre les objets, et les événements relatifs au changement d'attribut ou de relation (voir FIG. 2).

Les ontologies informatiques sont des outils qui permettent précisément de représenter un corpus de connaissances sous une forme utilisable par une machine. Une ontologie contient une description hiérarchique des concepts importants d'un domaine et une description des propriétés de chaque concept et ses relations avec d'autres concepts. Les concepts sont organisés dans un graphe dont les relations peuvent être sémantiques ou de subsumption. La « subsumption » organise les concepts par abstraction de caractères communs pour aboutir à une hiérarchie correspondant à une organisation taxonomique des objets (Roche, 2005).

1.5 Critères d'évaluation d'une ontologie

Grüber (Grüber, 1993) affirme que dans un processus de design d'ontologie, certains critères pour évaluer la qualité de cette ontologie doivent être appliqués. En effet, l'auteur établi 5 critères permettent de mettre en évidence des aspects importants d'une ontologie (Source : Wikipedia) :

1. *La clarté : La définition d'un concept doit faire passer le sens voulu du terme, de manière aussi « objective » que possible (indépendamment du contexte). Une définition doit de plus être « complète », c.-à-d., définie par des conditions à la fois nécessaires et suffisantes et ensuite documentée en langage naturel.*

2. *La cohérence : Rien qui ne puisse être inféré de l'ontologie ne doit entrer en contradiction avec les définitions des concepts y compris celles qui sont exprimées en langage naturel.*

3. *L'extensibilité : Les extensions qui pourront être ajoutées à l'ontologie doivent être anticipées. Il doit être possible d'ajouter de nouveaux concepts sans avoir à toucher aux fondations de l'ontologie.*

4. *Une déformation d'encodage minimale : Une déformation d'encodage a lieu lorsque la spécification influe la conceptualisation. Un concept donné peut être plus simple à définir d'une certaine façon pour un langage d'ontologie donné, bien que cette définition ne corresponde pas exactement au sens initial. Ces déformations doivent être évitées autant que possible.*

5. *Un engagement ontologique minimal : Contrairement aux bases de connaissances, on n'attend pas d'une ontologie qu'elle soit en mesure de fournir systématiquement une réponse à une question arbitraire sur le domaine. Une ontologie est la théorie la plus faible couvrant un domaine ; elle ne définit que les termes nécessaires pour partager la connaissance liée à ce domaine. Donc, le but d'une ontologie est de définir un vocabulaire pour décrire un domaine, si possible de manière complète.*

Enfin, en vue de répondre aux 5 critères de Grüber, il est important que soient fixés préalablement et précisément : les engagements ontologiques généraux, les catégories de haut niveau telles que les appellations et les significations, le processus de raffinement de ces engagements et définitions des catégories, et enfin la spécialisation de ces catégories (Guarino, 1998).

1.6 Conclusion

L'ontologie n'est pas un but en soi, elle fournit des moyens de construction pour d'autres modèles et systèmes. Le degré de formalisation (implantation des structures issues de la conceptualisation dans un langage formel) varie du langage naturel sans primitive et régis par des définitions circulaires, des énoncés imprécis, et des objets instables, au langage formel caractérisé par une sémantique, des expressions construites avec des primitives, des connecteurs, etc. Cela passe d'abord par chercher une stabilité référentielle et relationnelle en choisissant un contexte de référence aux objets afin de fixer et stabiliser leur interprétation, et ensuite par structurer et organiser les concepts créés.

Une formalisation optimale rend l'ontologie réutilisable. Bien que la réutilisabilité se confronte à l'utilisabilité. Autrement dit, plus une ontologie est réutilisable plus elle perd en précision et par conséquent s'éloigne du scénario d'application et perd de son utilité. Et plus une ontologie est spécialisée, plus elle est proche des préoccupations d'une application (Charlet, Zacklad, Kassel, & Bourigault, 2000).

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, de situation et d'événement.

2 Ontologie pour la modélisation du processus accidentel

La modélisation des scénarios d'accident à travers un processus accidentel générique permet de les décrire d'une manière spatio-temporelle. L'identification des scénarios d'accident sera basée sur le développement du processus accidentel en fonction de l'occurrence de trois types d'événements : Evénement d'Exposition (EvE), Evénement Initiateur (EvI) et Evénement Redouté(EvR). Ces événements ont la capacité de provoquer le changement de situation d'une entité entre: Situation Initiale (SI), Situation d'Exposition (SE), Situation Dangereuse(SD) et Situation d'Accident (SA).

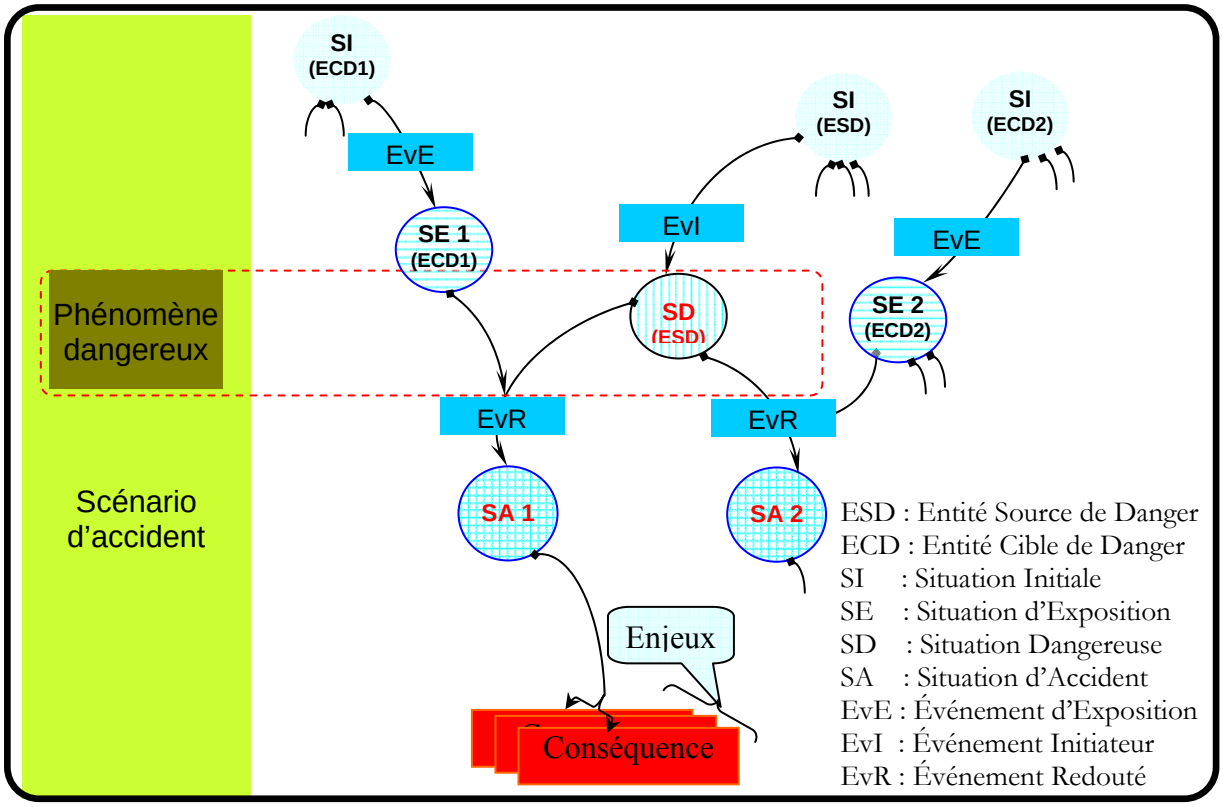


FIG. 3: Scénario d'accident avec une source et deux cibles à travers le processus accidentel

Nous avons modélisé cette ontologie en tenant compte des règles suivantes :

- L'accident est une réalisation qui se développe entre une entité source de danger (ESD) et une ou plusieurs entités cibles de danger (ECDs) en passant par plusieurs situations intermédiaires (situation dangereuse, situation d'accident). Le risque est la mesure assignée à cette réalisation.
- Le scénario de danger est une partie du scénario d'accident (cf. Figure 3) qui fait l'objet de l'analyse de danger, ce qui permettra d'élaborer une cartographie des espaces de danger et de préciser les intensités des phénomènes dangereux qui en résultent.
- La gravité des dommages potentiels d'un scénario d'accident est estimée en fonction des préjudices portés aux cibles exposées dans l'espace de danger d'une source. Les préjudices subits par cette source sont pris en considération dans l'estimation de la gravité globale.

- Une entité peut être en même temps source et cible dans un scénario d'accident.
- Tout système est situé par rapport à un environnement sensible à ses changements d'état.
- Le concept d'espace (de vulnérabilité, de danger) dépasse l'acception physique, il peut admettre plusieurs dimensions outre que spatiales à l'égard du risque éthique, culturel, mental (stress, harcèlement), médiatique (l'image de marque d'un organisme), etc.

2.1 Entités élémentaires

Il faut rappeler que le modèle MADS (voir chapitre 2 §3.9) permet de mettre en relation un système source avec un système cible par l'intermédiaire des flux de danger dans un environnement appelé champ de danger. Néanmoins, le modèle de référence permet de considérer quatre couples source/cible en l'occurrence : « installation, installation », « installation, opérateur » ou « opérateur, installation », « installation, population » ou « population, installation », « installation, écosystème » ou « écosystème, installation »(Laurant, 2003).

Une menace est un signe ou indice qui « fait référence à des conséquences implicites dans un aléa mais de manière à décrire plus précisément les circonstances de sa réalisation et de son imminence. Ainsi on peut dire qu'une menace s'approche, recule ou se réalise » (HSE, 1992). Justement, la notion de source et de cible permet de donner un sens à l'exercice d'une menace, et par conséquent donner plus de dynamisme aux mesures de protection des cibles et de prévention au niveau des sources.

Le modèle MADS permet d'avoir une vision Macro sur l'accident, ce qui permet de positionner la nature des études requises permettant de maitriser la menace en question (sûreté de fonctionnement, ergonomie, fiabilité humaine, épidémiologie, etc.) (Laurant, 2003).

Néanmoins, dans notre cas, nous ne nous limitons pas à considérer des systèmes comme sources ou cibles, mais plutôt des entités élémentaires, quelque soit leur niveau hiérarchique.

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* ».

Ainsi un flux de danger peut s'exercer entre un sous-système et le système global, entre plusieurs sous-systèmes ou composants élémentaires logiciels, matériels, humains ou environnementaux, etc.

2.1.1 Entité Cible de Danger (ECD)

La notion d'ECD est à rapprocher de la notion « d'intérêt à protéger » de la législation sur les installations classées (Code de l'Environnement: Article L. 511-1, 17 janvier 2001). Toutefois, on associe à l'ECD deux notions importantes : la vulnérabilité et l'espace de vulnérabilité.

Proposition : Entité telle qu'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.

2.1.1.1 Notion de vulnérabilité

Définitions :

SOURCE	
(Larousse, 2005)	Caractère vulnérable de quelque chose ou de quelqu'un: Qui est exposé aux atteintes d'une maladie, qui peut servir de cible facile aux attaques d'un ennemi : Une position vulnérable Qui, par ses insuffisances, ses imperfections, peut donner prise à des attaques
(GT Aspects sémantiques du risque, 1997)	Etat ou degré de fragilité d'un système.
(GT Méthodologie, 2003)	«Vulnérabilité d'une cible à un effet x» : facteur de proportionnalité entre les effets auxquels est exposé un élément vulnérable (ou cible) et les dommages qu'il subit.

Proposition : La vulnérabilité caractérise la susceptibilité d'une ECD être exposée à un danger particulier, de subir un dommage.

2.1.1.2 Notion d'espace de vulnérabilité

Proposition : 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 temporaire ou permanent.

2.1.2 Entité Source de Danger (ESD)

Un réservoir de liquide inflammable est porteur du danger lié à l'inflammabilité du produit contenu, à une charge disposée en hauteur correspond le danger lié à son énergie potentielle, à une charge en mouvement celui de l'énergie cinétique associée, etc.

Proposition : 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.

2.1.2.1 Notion d'espace de danger

Proposition : Tout espace à l'intérieur et/ou autour d'une ESD, dans lequel elle produit un ou plusieurs dangers.

2.2 Evénements élémentaires

Selon la norme ISO/CEI Guide 73 (ISO/CEI Guide 73, 2002): « un événement est une occurrence d'un ensemble particulier de circonstances. L'événement peut être certain ou incertain. La probabilité associée à l'occurrence de l'événement peut être estimée sur une période de temps donnée ».

Proposition : Un 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, etc.).

2.2.1 Evénement d'exposition

L'Evénement d'Exposition amorce le chronomètre de la situation d'exposition qui se termine normalement avec la disjonction de l'espace de vulnérabilité de l'ECD et de l'espace de danger de l'ESD, ou dangereusement par l'apparition d'un événement redouté.

Proposition : 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.

2.2.2 Evénement Initiateur

Proposition : 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.

2.2.3 Evénement redouté

Définitions :

SOURCE	
(GT Méthodologie, 2003)	Evénement conventionnellement défini, dans le cadre d'une analyse de risque, au centre de l'enchaînement accidentel. Généralement, il s'agit d'une perte de confinement pour les fluides et d'une perte d'intégrité physique pour les solides. Les événements situés en amont sont conventionnellement appelés « phase pré-accidentelle » et les événements situés en aval « phase post-accidentelle ».
(HSE, 1992)	L'événement redouté « fait référence à un aléa qui s'est réalisé ».
(GT Aspects sémantiques du risque, 1997)	Un événement redouté est « une situation très probable aux conséquences néfastes pour les individus ».

Proposition : Evénement entrainant une situation d'accident ; il décrit le moment où un espace de danger et un espace de vulnérabilité se recouvrent.

2.3 Situations élémentaires

2.3.1 Situation vs. état

Une situation résume la conjoncture que subit une entité. En d'autres termes, une situation est fonction des états, possibilités, actions et réactions de cette entité.

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. On peut dire aussi que la notion d'état est liée à l'aspect fonctionnel d'une entité, alors que la notion de situation renvoie plutôt à l'aspect cindynique[1]. Autrement dit, pour une entité donnée on peut parler en termes d'état de marche, d'arrêt ou de panne, voire de situation initiale, d'exposition au danger ou situation dangereuse.

2.3.2 Situation Initiale

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

2.3.3 Situation d'Exposition

Définitions:

SOURCE	
(Larousse, 2006)	Situation dans laquelle on est menacé d'un mal quelconque.
(Larousse, 2005)	Situation où l'on est exposé à quelque chose qui légitime une inquiétude ; ce qui constitue une menace, un risque, qui compromet l'existence ou le bon état de quelque chose, de quelqu'un.
(HSE, 1992)	Disposition d'une chose, d'une condition ou d'une situation à produire un tort. (Note. assimilé à aléa). Des mots comme danger, menace, péril, etc. peuvent être utilisés pour caractériser un aléa ou l'imminence de sa réalisation.
(GT Aspects sémantiques du risque, 1997)	Situation d'incertitude pouvant nuire à l'homme, à la société ou à l'environnement. Sa réalisation est un sinistre.
(NF EN 61508, Décembre 1998), (EN 292/ISO 12100, 1995)	Situation dans laquelle une personne est exposée à un (des) phénomène(s) dangereux.

[1] La **cindynique** (du grec ancien κίνδυνος / *kíndunos*, danger) regroupe les sciences qui étudient les risques. On les appelle aussi « ***sciences du danger*** » [Wikipedia].

Synthèse : L'événement d'exposition annonce l'entrée d'une ECD dans un espace de danger. Un individu se trouvant sur les rails est considéré comme une ECD en phase d'exposition à plusieurs dangers (électrocution, écrasement par un train, poursuite judiciaire (une autre dimension de l'espace de dangers)…). Un opérateur (ECD) travaillant dans un laboratoire à effets de radiation, est considéré en phase d'exposition dès lors qu'il se trouve dans le laboratoire.

Proposition : 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 plusieurs sources de danger.

2.3.4 Situation Dangereuse

Définitions :

SOURCE	
(HSE, 1992)	Disposition d'une chose, d'une condition ou d'une situation à produire un tort. Des mots comme danger, menace ou péril peuvent être utilisés pour caractériser un aléa ou l'imminence de sa réalisation.
(GT Aspects sémantiques du risque, 1997)	Situation d'incertitude pouvant nuire à l'homme, à la société ou à l'environnement. Sa réalisation est un sinistre.

Synthèse : La situation dangereuse se définit comme un contexte aléatoire à l'issue de l'occurrence d'un événement initiateur ayant la capacité de rompre le cours normal, ce qui provoque le développement d'un phénomène dangereux. Elle est aléatoire parce qu'on connaît ses conditions sans pour autant prévoir avec exactitude le cours de ce qui va arriver, mais tout en ayant la certitude qu'elle présente une potentialité d'atteinte à la santé, aux biens ou à l'environnement.

Proposition : 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.

2.3.5 Situation d'Accident (SA - Accident Situation)

La situation d'accident est la conséquence de l'événement redouté lorsqu'une situation dangereuse et une situation d'exposition sont réunies.

Cette situation est caractérisée par la production de dommages, qu'il s'agisse d'une perte d'intégrité au niveau système, de l'atteinte physique des hommes, de la nuisance à l'environnement, ou de la dégradation d'un enjeu important pour l'organisation (perte financière, perte de crédibilité, etc.).

La situation d'accident peut durer quelques secondes (accident de la route) comme elle peut durer des années (catastrophe nucléaire). On parle alors souvent d'effets immédiats et d'effets latents.

Proposition : 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.

2.4 Modélisation de type état/transition du processus accidentel

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

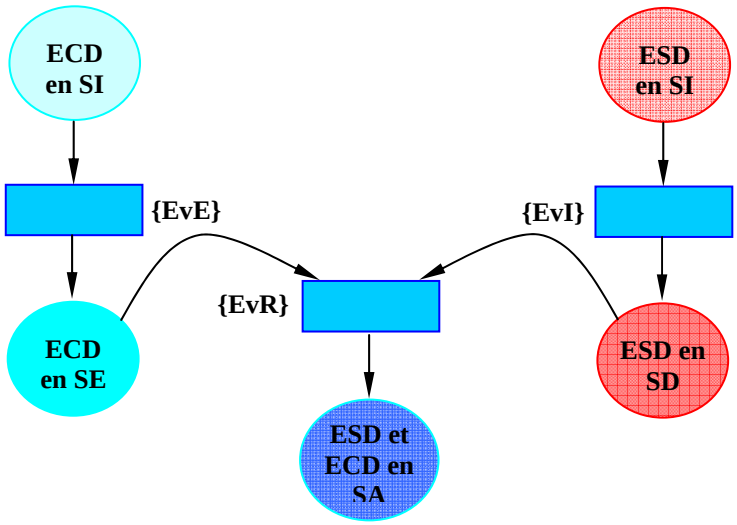


FIG. 4: Réseau de Pétri étiqueté (RdP) d'un scénario d'accident type

Nous devons retenir les événements ayant un potentiel à provoquer des transitions significatives dans l'état du système global ou de l'une de ses entités. Par exemple, un événement redouté entraîne la transition d'une situation dangereuse à une situation d'accident.

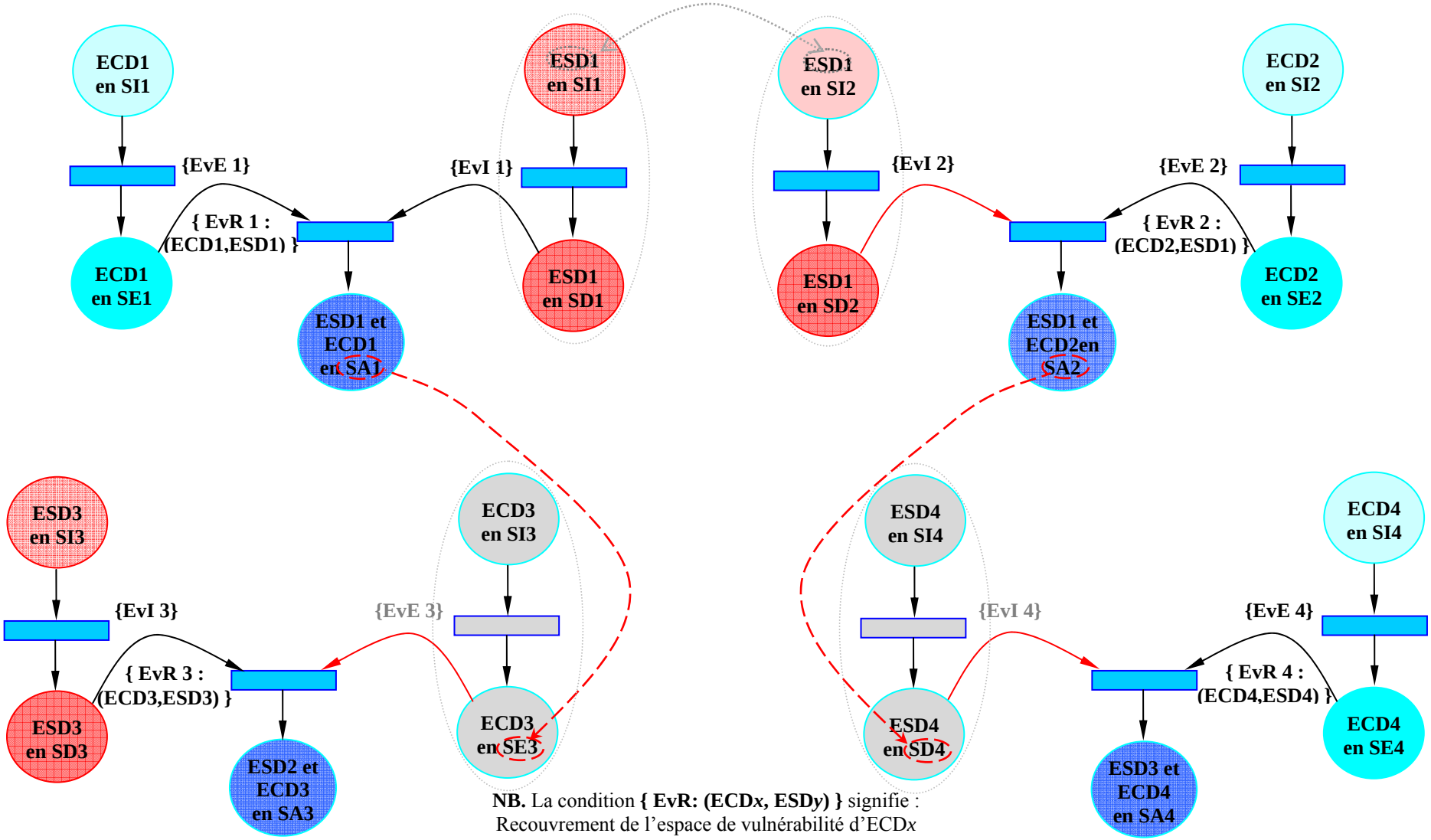
TAB. 1 : Alphabet du RdP étiqueté de modélisation du processus accidentel ontologique

Code	Signification	Situation de départ	Situation d'arrivée
EvE	Evénement d'Exposition	Situation Initiale	Situation d'Exposition
EvI	Evénement Initiateur	Situation Initiale	Situation Dangereuse
EvR	Evénement Redouté	Situation Dangereuse + Situation d'Exposition	Situation d'Accident

Une modélisation à l'aide d'un automate à états finis peut convenir pour représenter un processus accidentel. Les transitions entre états seront étiquetées par les différents événements précédemment définis. Cependant, le recours aux réseaux de Pétri (voir FIG. 4) nous semble plus intéressant en ceci que le modèle pourrait être construit progressivement sans connaître a priori l'ensemble des états potentiellement accessibles dans un processus complexe. Ainsi, le marquage permet de matérialiser les conditions nécessaires à l'initiation du processus dangereux. Il faut a minima une source et une cible de danger. Si l'on veut enrichir le modèle pour prendre en compte l'insertion de barrières de protection, de nouvelles places vont être introduites pour indiquer la présence de ces nouvelles entités qui vont imposer de nouvelles conditions au franchissement des transitions, en plus de l'occurrence de l'événement associé. La défaillance d'une barrière sera matérialisée par l'apparition d'un jeton dans une des places amont de la transition associée à l'événement qu'elle est sensée contrôler. La transition pourra alors être franchie si l'événement se présente.

En plus d'une clarté accrue dans la description des phénomènes, le réseau de Pétri apporte l'avantage d'un modèle formel dont on pourra exploiter les propriétés. De nombreux logiciels sont aujourd'hui disponibles pour éditer, vérifier, évaluer les propriétés ou simuler le fonctionnement de RdP. Certains sont orientés vers les besoins de la sûreté de fonctionnement et permettent d'accéder aux évaluations probabilistes des composantes de cette dernière. La modélisation du processus accidentel sous forme de RdP permettra un passage aisé vers ces outils d'évaluation quantitative (dans l'outil de mise en œuvre de la méthode, un fichier de description compatible pourrait être généré automatiquement).

Il faut noter en particulier que ce formalisme permet de construire à partir de la description de processus accidentels séparés, les scénarios menant à un effet domino lorsque différentes sources ou cibles interagissent en séquence.



NB. La condition **{ EvR: (ECD*x*, ESD*y*) }** signifie :
Recouvrement de l'espace de vulnérabilité d'ECD*x*
et de l'espace de danger d'ESD*y*

FIG. 5: Modélisation d'un scénario d'accident complexe à effets domino

La figure 5 (voir FIG. 5) présente une modélisation de 4 scénarios d'accident (scénario 1, 2, 3, 4) avec 3 entités sources (ESD1, ESD2, ESD3) et 4 entités cibles de danger (ECD1, ECD2, ECD3, ECD4).

La source ESD1 est associée aux deux scénarios 1 et 2 respectivement avec ECD1 et ECD2. Les deux scénarios en question amènent à deux situations d'accident différentes, respectivement SA1 et SA2.

La situation d'accident SA1 est similaire à la situation d'exposition du scénario 3 SE3 (voir §3, FIG. 6, scénarios 6 et 7) , 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 la situation d'accident du premier (SA2) et la situation de danger SD4 du deuxième (voir §3, FIG. 6, scénarios 1 et 2).

La modélisation proposée permet d'offrir une meilleure visibilité pour 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 est d'éviter l'apparition des événements redoutés et enfin concernant la situation d'accident, l'enjeu ultime est minimiser les préjudices pouvant être portés à l'homme, aux biens ou à l'environnement.

3 Illustration de l'ontologie

Dans cette section nous allons essayer d'illustrer comment l'ontologie proposée permet de répondre à plusieurs préoccupations majeures en matière d'analyse de risques, que nous avons soulevées dans le chapitre précédent (voir chapitre 4). En effet, la modélisation des scénarii d'accident à travers cette ontologie permet d'assurer une passerelle entre:

- Les scénarios en permettant de déceler de manière systématique les effets domino; ceci permet de répondre à l'enjeu de traçabilité.
- Les sous systèmes ; ceci permet de répondre à l'enjeu d'intégration
- Les systèmes semblables ; ceci permet de répondre à l'enjeu d'harmonisation des analyses de risques
- Les différents types de risques (la modélisation de l'affaire du Watergate entre risques politique, médiatique et ensuite juridique) ; Ceci permettra de mieux analyser les risques globaux pluridisciplinaires.
- Les différents domaines (ferroviaire, routier, machine, etc.) ; Ceci permet de répondre à l'enjeu de généricité, qui est sans doute le plus important de tous. Par exemple, s'agissant d'un train, quand il est en construction l'ontologie couvre l'aspect manufacturier. Une fois mis en circulation, elle couvre l'aspect ferroviaire, mais en cas de passage à niveau, elle permet

d'évaluer le risque routier. Quand le train passe à l'atelier de maintenance, il y est plutôt question de risque machine. De même quand le train transporte une matière dangereuse, l'ontologie couvre conjointement les aspects process et ferroviaire.

3.1 Risque ferroviaire

3.1.1 Scénario 1 : Présence d'un individu sur la voie

ESD: écran d'affichage des arrivées	**ECD**: personne autorisée (client)
EVI : panne de l'écran des arrivées	**EVE:** train aperçu à l'approche vers le quai opposé
SD : absence d'indication sur les arrivées	**SE** : précipitation pour rattraper le train
EVR: un individu traverse la voie	
SA : présence d'individu sur la voie	
Conséquences : RAS	
Gravité : Mineure	

Suite à une panne générale du système d'affichage des arrivées des trains. Un passager qui se trouvait sur le mauvais quai, aperçut un train à l'approche de la gare qui se dirigeait vers le quai opposé. Il se précipita donc en traversant les voies afin qu'il puisse rattraper le train.

3.1.2 Scénario 2 : immobilisation d'un train

ESD: personne autorisée (client)	**ECD**: train
EVI : un individu traverse la voie	**EVE**: train en mouvement entre deux stations
SD : présence d'individu sur la voie	**SE** : train à l'approche de la station
EVR: freinage d'urgence	
SA : immobilisation d'un train	
Conséquences : Panique générale dans le train	
Gravité : Mineure	

Un individu traversant la voie fut signalé, tandis qu'un train se dirigeait vers la gare. Un freinage d'urgence fut systématiquement actionné, immobilisant le train sur place en attente d'une ordonnance de circulation. Cet incident provoqua un mouvement de panique parmi les passagers.

3.1.3 Scénario 3 : évacuation d'un train entre deux stations

ESD: train	**ECD**: personnes non autorisées
EVI : freinage d'urgence	**EVE**: des passagers s'impatientent et/ou paniquent
SD : immobilisation d'un train	**SE** : passagers à bord d'un train immobilisé

EVR: des individus descendent du train
SA : présence d'individu sur la voie
Conséquences : Panique générale
Gravité : Significative

Suite à une longue immobilisation d'un train entre deux stations, quelques passagers impatients descendirent du train et se trouvèrent désormais sur la voie.

3.1.4 Scénario 4 : indisponibilité du Pilote Automatique

ESD: PA principal	**ECD**: le PA redondant
EVI : indisponibilité du PA principal	**EVE**: basculement sur le PA redondant
SD : panne de la redondance	**SE** : conduite en mode dégradé
EVR: défaillance du PA redondant	
SA : indisponibilité du PA	
Conséquences : panne du pilotage automatique	
Gravité : Significative	

Suite à une défaillance du Pilote Automatique (PA) principal, le système de contrôle/commande bascula sur le PA secondaire (redondant) en mode dégradé. Quelque temps après, le PA redondant tomba en panne à son tour, ceci provoqua une indisponibilité totale du pilotage automatique.

3.1.5 Scénario 5 : excès de vitesse

ESD: PA	**ECD**: Conducteur
EVI : défaillance des PA	**EVE**: dépassement du temps de travail autorisé
SD : indisponibilité du PA (conduite en mode manuel)	**SE** : baisse de vigilance
EVR: dépassement de la vitesse autorisée	
SA : excès de vitesse	
Conséquences : panne du PA	
Gravité : Significative	

Le PA étant en état de panne, le conducteur conduisit en mode manuel (marche à vue). Ce dernier ayant dépassé le temps de travail maximum autorisé par la loi, se trouve en situation de baisse de vigilance et de cumul de fatigue, ce qui l'emmena à dépasser la vitesse maximale autorisée.

3.1.6 Scénario 6 : distance d'arrêt trop longue

La distance de freinage fut trop longue à cause du dépassement de vitesse par le conducteur:

ESD: Conducteur	**ECD**: respect de la distance de freinage (procédure)

EVI : dépassement de la vitesse autorisée	**EVE**: dépassement de la vitesse autorisée
SD : excès de vitesse	**SE** : inefficacité du freinage
EVR: freinage d'urgence	
SA : distance d'arrêt trop longue	
Conséquences : RAS	
Gravité : Mineure	

3.1.7 Scénario 7: heurt d'un individu

ESD: personne non autorisée	**ECD**: train
EVI : l'individu traverse la voie	**EVE**: freinage d'urgence
SD : présence d'individu sur la voie	**SE** : distance d'arrêt trop longue
EVR: train heurte un individu	
SA : heurt d'un individu	
Conséquences : un décès	
Gravité : Critique	

Un individu traversant la voie fut perçut par le conducteur au moment où le train se dirigeait vers la gare. En conséquence, un freinage d'urgence fut systématiquement actionné par le conducteur. La distance d'arrêt était trop longue, l'individu fut heurté par le train, ce qu'il entraîne son décès.

3.1.8 Scénario 8 : déraillement

ESD: corps humain ou animal	**ECD**: train
EVI : un corps tombe (se met) sur la voie	**EVE**: freinage d'urgence
SD : présence de corps sur la voie	**SE** : distance d'arrêt trop longue
EVR: train écrase un corps	
SA : déraillement	
Conséquences : plusieurs décès, perte du système	
Gravité : Catastrophique	

Un corps (homme ou animal) s'est mis (ou est tombé) sur la voie alors que le train se trouvait à proximité. Le freinage d'urgence fut systématiquement actionné, mais la distance de freinage fut trop longue. En conséquence le passage du train sur le corps provoqua un déraillement.

3.1.9 Scénario 9 : Collision sur un Passage à Niveau (PN)

Un véhicule routier cale sur la voie au niveau d'un PN au moment où il s'apprête à passer juste avant l'arrivée du train signalé à l'approche (début de fermeture des barrières, activation des signaux d'alarme). Le train rattrape et heurte le véhicule. Ce qui provoque la mort de plusieurs passagers de ce dernier.

ESD: Véhicule routier	**ECD**: train
EVI : Véhicule cale en traversant le PN	**EVE**: : train en mouvement entre deux

	stations
SD : présence d'un véhicule sur la voie	**SE** : train à l'approche du PN
EVR: train heurte un véhicule	
SA : Collision	
Conséquences : plusieurs décès	
Gravité : Catastrophique	

Si on suppose qu'il y a eu un défaut de signalisation de l'approche du train, le système de signalisation devient la principale ESD et le véhicule quant à lui l'ECD.

3.1.10 Aide à la vérification de l'incomplétude, cohérence, traçabilité, harmonisation, intégration à travers la modélisation des effets domino

La réalisation d'un scénario d'accident peut amorcer la propagation de nouveaux scénarios. Une SA (Situation d'Accident) peut constituer une SD (Situation Dangereuse) ou une SE (Situation d' Exposition) dans la réalisation d'autres scénarios. Par exemple la SA du scénario 1 constitue une SD pour les scénarios 2, 7 et 8. Alors que la SA du scénario 6 constitue une SE pour les scénarios 7 et 8.

Comme le montre la figure, il existe plusieurs chemins de réalisation d'effets domino. Par exemple, la séquence : scénario 1, scénario 2, scénario 3, scénario 8, ou la séquence : scénario 4, scénario 5, scénario 6, scénario 7. Toutefois, il existe un scénario plus complexe :

(scénario 1, scénario 2, scénario 3) et (scénario 4, scénario 5, scénario 6), scénario 7, scénario 8.

Ce dernier scénario résulte en un déraillement en partant d'une panne ordinaire d'un écran d'affichage des arrivées des trains, et il se décrit comme suit :

« Suite à une panne générale du système d'affichage des arrivées des trains, un passager qui se trouvait sur le mauvais quai, aperçut un train à l'approche de la gare qui se dirigeait vers le quai opposé. Il se précipita donc en traversant les voies afin qu'il puisse rattraper le train. Il fut aussitôt signalé. Un freinage d'urgence fut systématiquement actionné et par conséquent, le train fut immobilisé sur place entre deux stations en attente d'une ordonnance de circulation. Cet incident provoqua un mouvement de panique parmi les passagers, et comme l'immobilisation du train fut trop longue, quelques passagers impatients descendirent du train et se trouvèrent désormais sur la voie.

D'autre part, un deuxième train se dirigeant vers la même station présentait quelques soucis. En fait, suite à une défaillance du Pilote Automatique (PA) principal, le système de contrôle/commande bascula sur le PA secondaire (redondant) en mode dégradé. Quelque temps après, le PA redondant tomba en panne à son tour, ceci provoqua une indisponibilité totale du pilotage automatique. Le PA étant en état de panne, le conducteur conduisait en mode manuel (marche à vue). En ayant dépassé le temps de travail maximum, par baisse de vigilance et cumul de fatigue, le conducteur dépassa la vitesse maximale autorisée.

Les passagers du premier train furent aperçus par le conducteur au moment où son train se dirigeait vers la gare. En effet, un freinage d'urgence fut systématiquement actionné, mais hélas, la distance d'arrêt était trop longue, et

par conséquent plusieurs individus furent heurtés, ce qui a causé leur décès. De surcroit, le passage des corps sous le train ait engendré un déraillement catastrophique ».

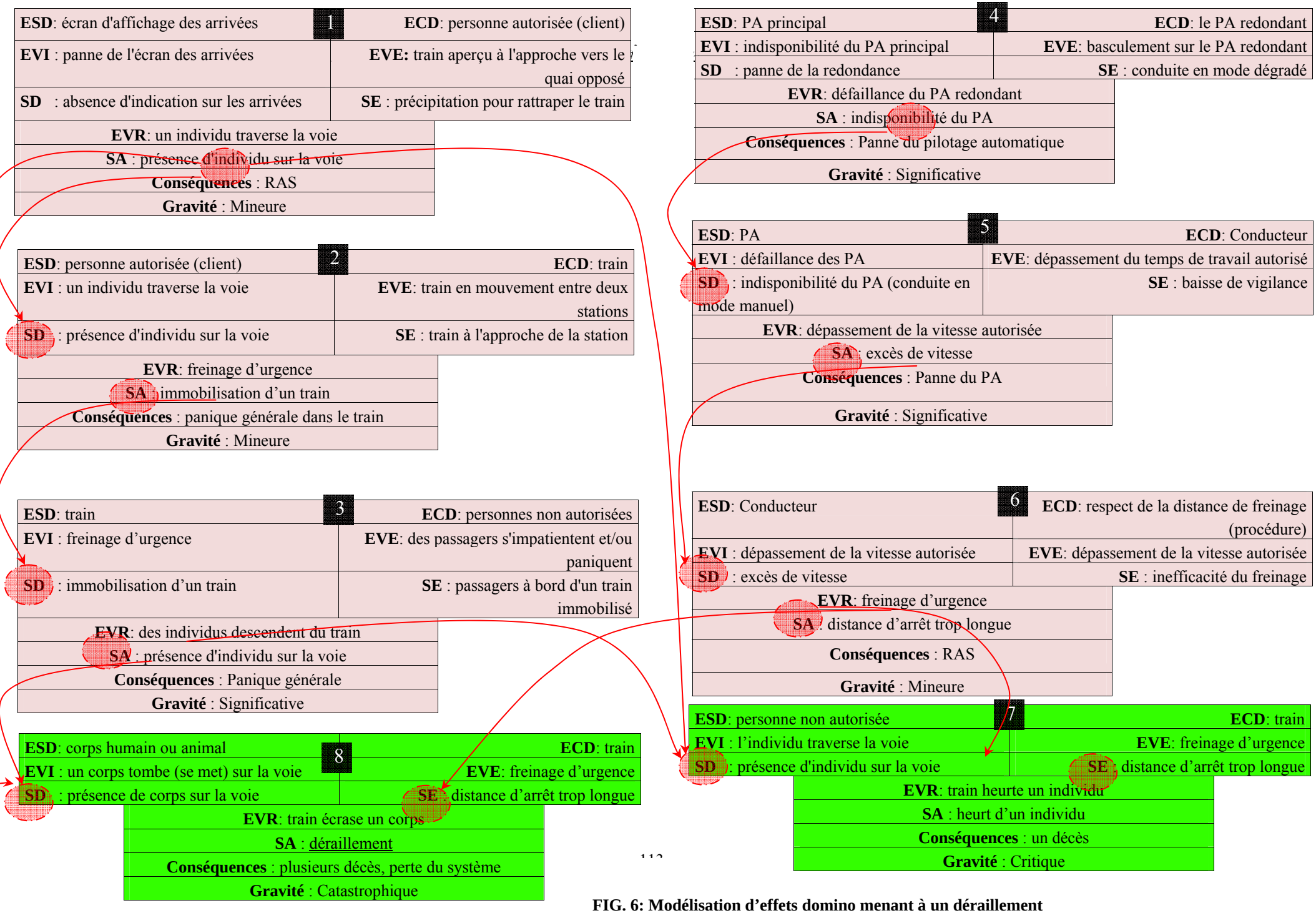


FIG. 6: Modélisation d'effets domino menant à un déraillement

3.2 Risque routier

Dans le domaine des transports, certains travaux de recherche à l'INRETS ont permis de proposer un modèle accidentel basé sur l'évolution chronologique des phases d'accident. La pertinence de l'analyse résulte de la superposition d'une logique d'enchaînement spatio-temporelle et d'une logique causale conditionnant les transitions entre phases.

« Le processus accidentel séquentiel se décompose (se déroule) en quatre situations (phases) : La situation de conduite, la situation d'accident appelée aussi situation de rupture pendant laquelle les acteurs sont confrontés à un problème à résoudre, la situation d'urgence est celle de la recherche hâtive d'une solution et en fin la situation de choc » (Brenac, Nachtergaele, & Reiner, 2003).

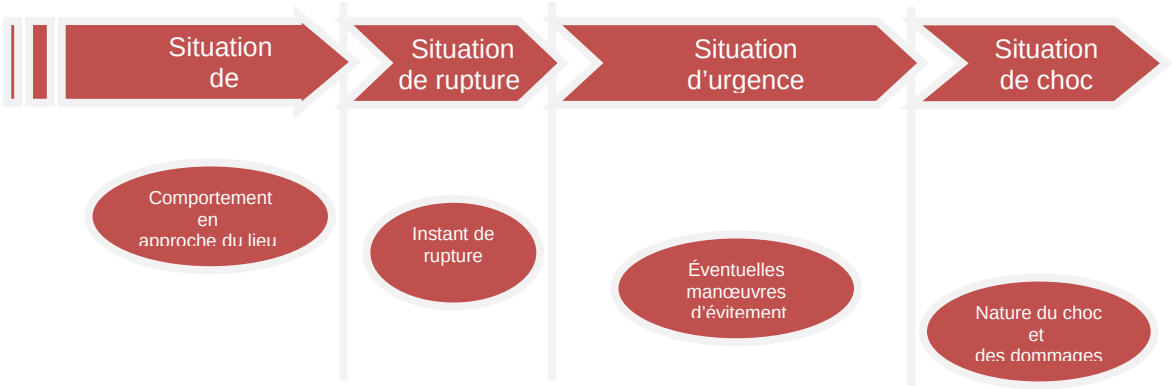


FIG. 7: Modèle accidentel séquentiel (Brenac, Nachtergaele, & Reiner, 2003).

Ce modèle est à l'origine dédié au transport routier, et dont l'objectif primaire est d'appuyer la discipline d'études détaillées des accidents et plus particulièrement la filière de reconstitution d'accident. Il a fait l'objet de nombreux travaux de modélisation de scénarios d'accident, en l'occurrence : **«** Scénarios types d'accidents impliquant des piétons et éléments pour leur prévention » (Brenac, Nachtergaele, & Reiner, 2003) ou **«** Scénarios types de production de "l'erreur humaine" dans l'accident de la route : problématique et analyse qualitative » (Van Elslande, Alberton, Nachtergaele, & Blanchet, 1997).

L'ontologie que nous proposons permet de contenir systématiquement le modèle accidentel séquentiel. Seulement, des aménagements doivent être opérés afin de l'inscrire dans un processus de type « état/transition » en intégrant les notions d'exposition (SE), de source (ESD) et de cible (ECD) de dangers, et mettre surtout l'accent sur les transitions événementielles (EvI, EvE, EvR).

3.2.1 Scénario 1 : heurt d'un piéton

Une voiture viola le feu rouge et heurta un piéton traversant le passage piéton :

ESD: voiture		**ECD**: piéton
EVI : voiture	**EVR**: voiture heurte un piéton	piéton) au vert
SD : passage d'une voiture	**SA** : heurt d'un piéton	**SE** : passage d'un piéton

Conséquences : un décès
Gravité : Critique

Supposons que la voiture passa au vert et c'est le piéton qui n'a pas respecté le feu violé le feu rouge. On peut constater que de par le fait que la voiture est une ECD cette fois-ci, les dommages qui peuvent lui être portés figurent parmi les conséquences :

ESD: piéton	**ECD**: voiture
EVI : piéton grille le feu rouge	**EVE :** passer au vert
SD : présence d'un piéton sur le passage piéton	**SE** : passage d'une voiture par le passage piéton
EVR: voiture heurte un piéton	
SA : heurt d'un piéton	
Conséquences : un décès, dommages importants portés à la voiture	
Gravité : Critique	

3.2.2 Scénario 2 : collision de trois voitures dans une intersection (feux rouges):

Une voiture A viola le feu rouge, tandis que d'autres voitures B et C passèrent dans le sens opposé. Aussitôt, elle rentra en collision avec ces deux dernières :

ESD: voiture A	**ECD**: voitures B et C
EVI : voiture A grille le feu rouge	**EVE**: Voitures B et C passent le feu au vert
SD : passage dans le carrefour	**SE** : passage dans le carrefour
EVR: voiture A rentre en collision avec voitures B et C	
SA : collision	
Conséquences : plusieurs décès, dommages importants portés aux voitures	
Gravité : Catastrophique	

Supposons maintenant qu'un disfonctionnement du système de signalisation a induits le véhicule en question à rentrer en collision avec les deux autres véhicules. Dans ce nouveau scénario, le système de signalisation est l'ESD, et les trois voitures sont considérées en tant que ECDs :

ESD: Système de signalisation	**ECD**: Voitures A, B et C
EVI : défaillance du système de signalisation	**EVE**: passage des feux au vert
SD : des feux opposés sont au vert	**SE** : engagement des voitures A, B et C
EVR: Voitures A, B et C rentrent en collision	
SA : collision	
Conséquences : plusieurs décès, dommages importants portés aux voitures	
Gravité : Catastrophique	

3.3 Risque machine

Afin d'illustrer l'applicabilité de l'ontologie dans le domaine machine, nous allons prendre pour exemple une Plate-forme Elévatrice Mobile de Personnel (PEMP).

Selon la norme EN 280, une PEMP (plate-forme élévatrice de personnel) est constituée au minimum par une plate forme de travail, une structure extensible et un châssis (voir FIG. 8).

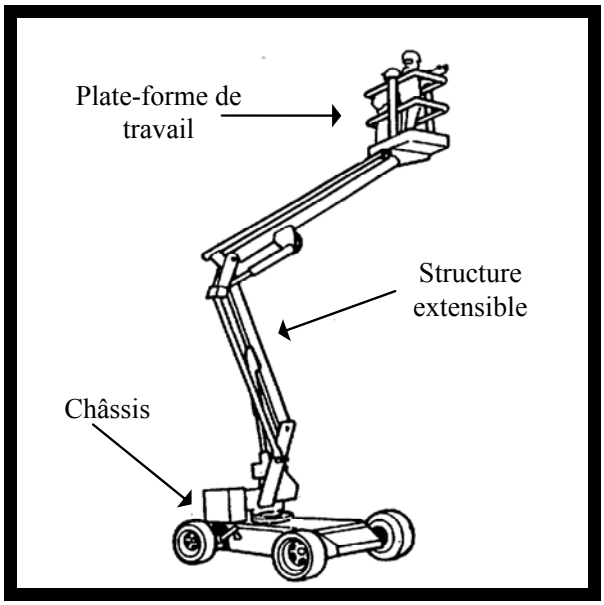


FIG. 8: exemple de Plate-forme Elévatrice Mobile de Personnel (Marsot, 1998)

« La plate-forme de travail est constituée soit d'un plateau entouré d'un garde-corps soit d'une nacelle qui peut être déplacée avec sa charge à la position permettant d'effectuer des travaux de montage, réparation, inspection ou autres travaux similaires. La structure extensible est la structure qui est solidaire du châssis et sur laquelle la plate-forme de travail est installée. Elle permet de mouvoir la plate-forme de travail jusqu'à la position voulue. Il peut s'agir, par exemple, d'une flèche ou d'une échelle simple, télescopique ou articulée, ou d'une structure à ciseaux, ou de toute combinaison de celles-ci avec ou sans possibilité d'orientation par rapport à la base. Enfin, le châssis est la base de la PEMP. Il peut être remorqué, poussé, automoteur, etc. » (NF EN 280, 2001) (Marsot, 1998).

3.3.1 Scénario 1 : chute, basculement

La fonction d'une PEMP est l'élévation de personnel à plusieurs mètres ou dizaines de mètres de hauteur.

Chute par basculement de la PEMP :

ESD: Structure extensible	**ECD**: PEMP
EVI : remonter la plate-forme	**EVE**: installer la PEMP
SD : présence d'une plate-forme à plus de 12 mètres de hauteur	**SE** : Présence d'une PEMP sur une pente

EVR: rupture d'un raccordement de la structure extensible
SA : basculement de la PEMP
Conséquences : RAS
Gravité : Mineure

ESD: PEMP	**ECD**: opérateur
EVI : rupture d'un raccordement de la structure extensible	**EVE**: accéder à la plate-forme
SD : basculement de la PEMP	**SE** : Présence d'un opérateur sur la plate-forme
EVR: déséquilibre d'un opérateur par le basculement de la PEMP	
SA : chute d'un opérateur	
Conséquences : un décès	
Gravité : Catastrophique	

Chute depuis la plate forme de travail :

ESD: Plate-forme	**ECD**: opérateur
EVI : conception non ergonomique du garde-corps	**EVE**: accéder à la plate-forme
SD : Présence d'une plate-forme à plus de 12 mètres	**SE** : présence d'un opérateur sur la plate-forme
EVR: l'opérateur appuie avec son dos sur le garde-corps	
SA : chute d'un opérateur	
Conséquences : un blessé grave	
Gravité : Importante	

3.3.2 Scénario 2 : choc, coincement, écrasement

L'utilisation d'une PEMP a pour but de rapprocher l'opérateur d'une structure extérieure. Ceci peut provoquer plusieurs types d'accident : choc, coincement, écrasement entre la plate forme et cette structure. De surcroit, si l'obstacle est un conducteur électrique, l'opérateur se trouve exposé à une électrisation ou une électrocution (Marsot, 1998):

ESD: Câble électrique	**ECD**: Opérateur
EVI : rupture d'un raccordement de la structure extensible	**EVE**: remonter la plate-forme
SD : basculement d'une PEMP	**SE** : Présence d'un opérateur à proximité d'un câble électrique
EVR: l'opérateur tient le câble pour éviter de chuter	
SA : électrocution	
Conséquences : un décès	
Gravité : Critique	

3.4 Risque manufacturier

Nous allons prendre un exemple simplifié d'une chaine industrielle de production de boules de pétanque. Cette chaine contient une unité de transport et deux unités de traitement : une cuve de zinc et une cuve d'acide.

La principale utilisation du zinc est la galvanisation des aciers : le dépôt d'une mince couche de zinc en surface de l'acier le protège de la corrosion. La corrosion désigne l'altération d'un objet manufacturé par l'environnement, telle que la rouille du fer et de l'acier, ou la formation de vert-de-gris sur le cuivre et ses alliages (bronze, laiton). Ces altérations chimiques sont regroupées sous le terme de « corrosion aqueuse ».

Une des principales propriétés des solutions acides est de pouvoir dissoudre un grand nombre de matériaux. Justement, le passage des pièces dans la cuve d'acide sert à les nettoyer.

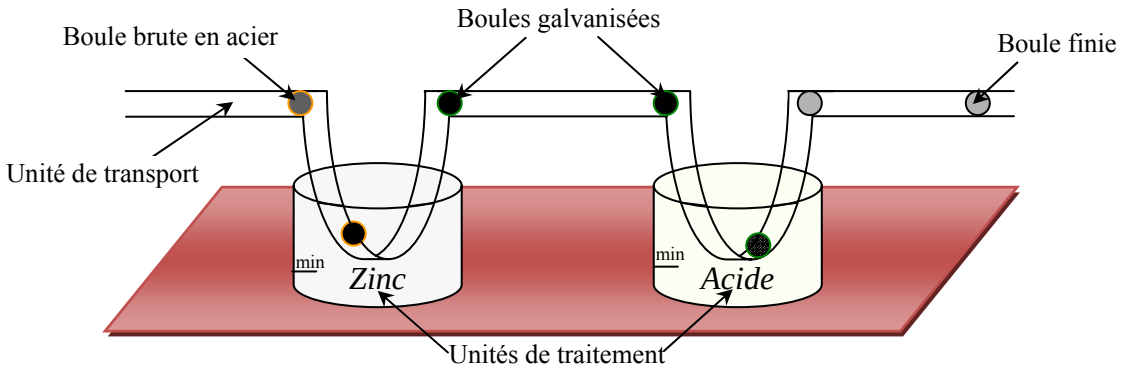


FIG. 9 : Chaine de production de boules de pétanque

Dans cet exemple, il y a deux sortes de contraintes à prendre en compte : d'abord le transport des pièces à travers les unités de traitement et ensuite les durées de passage. Cette durée peut être évaluée par les chimistes entre deux valeurs Min / Max. Autrement dit, si le séjour d'une pièce dans une cuve est inférieur à Min le traitement est considéré insuffisant, et si le séjour est supérieur à Max l'unité traitée subit une suroxydation.

3.4.1 Scénario 1 : rupture de la chaine de transport

ESD: Chaine de transport	**ECD**: Convoi de boules
EVI : Rupture d'un maillon	**EVE**: Passage des boules dans la cuve d'acide
SD : Rupture de la chaine	**SE** : Présence de boules dans la cuve d'acide
EVR: Séjours supérieur à la valeur Max	
SA : Suroxydation des boules	
Conséquences : Perte des boules, rupture de la chaine	
Gravité : Significative	

Effet domino : On peut lier, par exemple, la rupture de la chaine avec une mauvaise maintenance, ou un oubli de contrôle.

3.4.2 Scénario 2 : écoulement de l'acide

ESD: Cuve d'acide	**ECD**: Convoi de boules
EVI : le niveau du liquide passe en dessous du minimum (min)	**EVE**: passage dans la cuve d'acide
SD : Une cuve d'acide vide	**SE** : Présence de boules dans la cuve d'acide
EVR: passage des boules dans la cuve d'acide (vide)	
SA : indisponibilité du processus de nettoyage	
Conséquences : des boules galvanisées non finies	
Gravité : Mineure	

Effet domino : On pourrait établir un lien de ce scénario avec un autre scénario « amont » d'une erreur humaine d'approvisionnement de la cuve d'acide, et dont la SA de ce dernier est simplement la SD du scénario modélisé ci dessus, en l'occurrence « cuve d'acide vide ».

3.5 Risque professionnel

3.5.1 Scénario 1 : Tendinites et lombalgie

Troubles musculo-squelettiques (tendinites, lombalgie, etc.) lors de la manipulation de pièces lourdes et encombrantes. Ce scénario d'accident s'applique aussi bien au tôlier, menuisier, maçon ou autre métier physique :

ESD: pièce lourde	**ECD**: tôlier
EVI : la pièce a dû être posée dans un endroit encombrant	**EVE**: déplacer une pièce
SD : Présence d'une pièce lourde dans un endroit encombrant	**SE** : prise en main de la pièce
EVR: lever, porter et déplacer une pièce lourde d'un endroit encombrant	
SA : tendinites et lombalgie	
Conséquences : blessures graves	
Gravité : Significative	

3.5.2 Scénario 2 : allergie cutanée et respiratoire

Allergies cutanées et respiratoires suite à la préparation et la manipulation de produits toxiques :

ESD: réservoir de produit toxique	**ECD**: tôlier

EVI : ouverture du réservoir	**EVE**: peindre un réservoir
SD : **un** réservoir de produit toxique ouvert	**SE** : présence d'un tôlier à proximité d'un réservoir de produit toxique
EVR: respiration du produit toxique	
SA : Allergies cutanées et respiratoires	
Conséquences : blessures graves	
Gravité : Critique	

3.6 Risque épidémiologique

La transmission du H5N1 se fait par un contact étroit ou prolongé entre un humain et une volaille. Les oiseaux s'infectent aussi entre eux.

Les épidémiologistes craignent que le H5N1 mute de façon à passer facilement d'un humain à l'autre à l'égard de la pandémie de grippe espagnole de 1918 qui a tué entre 50 à 100 millions de personnes. Justement, un cas de transmission d'homme à homme a été confirmé en décembre 2007, mais le virus n'est pas hautement contagieux dans l'espèce humaine.

Prenons donc le scénario de transmission du H5N1 de l'animal (volaille) à l'homme (un éleveur) :

ESD: Volaille	**ECD**: Eleveur
EVI : la volaille reçoit le virus H5N1 de la part d'un oiseau migrateur	**EVE**: pénétrer dans le poulailler
SD : Volaille porteuse du H5N1	**SE** : Présence d'un éléveur à proximité des volailles
EVR: contact physique entre l'éleveur et la volaille	
SA : contamination avec le virus H5N1	
Conséquences : un décès	
Gravité : Critique	

Effet domino : on peut imaginer un scénario de contamination d'Homme à Homme.

3.7 Risque politique

Le scandale du Watergate ou affaire du Watergate a poussé le président des États-Unis Richard Nixon à démissionner en 1974. L'affaire commence avec le cambriolage des locaux du Parti Démocrate dans l'immeuble du Watergate à Washington en 1972, et se développe ensuite avec de nombreuses ramifications. Les investigations de journalistes et une longue enquête sénatoriale lèvent le voile sur des pratiques illégales à grande échelle au sein de l'administration présidentielle :

ESD: administration NIXON	**ECD**: Parti Démocrate

EVI : approche de l'échéance présidentielle	**EVE**: approche de l'échéance présidentielle
SD : Promouvoir une politique de déstabilisation à l'encontre du Parti Démocrate	**SE** : Statut du Parti Démocrate de principal parti d'opposition
EVR: cambriolage des locaux du Parti Démocrate	
SA : Prise en main de l'affaire dans le cadre d'enquêtes journalistique et sénatoriale	
Conséquences : Impact médiatique	
Gravité : Significative	

3.8 Risque médiatique

Deux journalistes du *Washington Post*, Carl Bernstein et Bob Woodward, enquêtent à partir des informations recueillies directement sur les cambrioleurs, ils parviennent à remonter les fils du financement occulte de la campagne électorale de Nixon en 1972, opéré notamment par le biais d'intermédiaires au Mexique. Ils sont aidés par un informateur inconnu se faisant appeler « Gorge Profonde » (« Deep Throat » en anglais), dont l'identité a été révélée 30 ans plus tard :

ESD: Woodstein (journalistes du WP)	**ECD :** administration NIXON
EVI : Révélations de « Deep Throat »	**EVE**: cambriolage des locaux du Parti Démocrate
SD : enquête journalistique	**SE** : Menace d'une fuite d'information sur les circonstances du cambriolage
EVR: accusation de l'administration NIXON d'être le commanditaire du cambriolage et dévoilement du financement occulte de la campagne électorale de Nixon en 1972	
SA : prise en main de l'affaire par la justice	
Conséquences : Perte de crédibilité politique de l'administration NIXON	
Gravité : Critique	

3.9 Risque juridique

Obsédés par l'affaire et suivis par leurs confrères, Woodward et Bernstein (surnommés Woodstein) parviennent à éclairer le sujet, qui est ensuite relayé par la justice américaine, puis par une commission d'enquête sénatoriale :

ESD: Loi juridique	**ECD :** administration NIXON
EVI : Accusation de l'administration NIXON	**EVE**: dévoilement du financement occulte de la campagne électorale de Nixon en 1972
SD : enquête juridique sur les révélations	**SE** : l'administration NIXON est la cible

des journalistes	d'une enquête juridique
EVR: confirmation des révélations des journalistes	
SA : prise en main de l'affaire par une commission d'enquête sénatoriale	
Conséquences : Démission de NIXON	
Gravité : Catastrophique	

4 Conclusion

Nous avons tenu lors de la construction de l'ontologie présentée dans ce chapitre à répondre aux 5 critères d'évaluation d'une ontologie définis par Grüber, en l'occurrence : clarté, cohérence, extensibilité, déformation d'encodage minimale, engagement ontologique minimal. En ce qui concerne le premier critère (clarté), nous avons tenu à suivre une démarche inductive et chronologique dans la présentation des différents concepts, et ce en les inscrivant dans un processus accidentel de type état/transition qui sert en même temps à garder la cohérence des définitions des concepts car chaque concept est associé sémantiquement à d'autres (événement – situation), (situation – événement), (événement – entité), (entité – événement), (entité – situation) et (situation – entité). Ces dernières classes de concepts sont aussi clairement définis que les concepts eux mêmes, ce qui garantit que l'ajout d'un concept (extensibilité) quelconque n'affecte pas les fondations de l'ontologie. Afin d'éviter les déformations d'encodage, nous avons tenu avant de définir un concept donné de voir d'abord son rôle et sa contribution dans le processus accidentel, afin d'éviter qu'une définition donnée ne corresponde pas au sens initial. Enfin, notre engagement ontologique est minimal afin que de nombreux acteurs puissent transcrire leurs scénarios d'accident en opérant juste quelques ajustements par rapports aux termes utilisés

L'ontologie proposée peut être considérée comme une passerelle permettant de lier les scénarios d'accident entre eux afin de déceler les effets domino, à l'égard de la modélisation des scénarios d'accident ferroviaire de la section 6.1, dans laquelle, nous avons imaginé un déraillement catastrophique en partant tout simplement d'une panne d'un écran d'affichage des arrivées des trains.

Cette ontologie permet, entre autres, de modéliser le transfert de danger entre entités sources et cibles, soit entre sous-systèmes d'un même système (cf. 3.1), soit entre sous-système et système global (cf. 3.3.1), soit entre systèmes (cf. 3.3.2), soit entre différents types de risques à l'image de l'affaire Watergate que nous avons étalée sur 3 domaines de risque différents : risque politique (cf. 3.7), risque médiatique (cf. 3.8), risque juridique (cf. 3.9).

Les effets domino allant d'une entité élémentaire tel qu'un écran d'affichage jusqu'à provoquer un déraillement catastrophique (voir Figure 6), et aussi les réactions de l'environnement de cette entité à la survenance d'un accident (les enjeux économique, médiatique, financiers, juridique et autres) sont deux contraintes auxquelles nous avons essayé de répondre dans le cadre de ce chapitre.

Une entité appartient à un quelconque système. Tout système est situé par rapport à un environnement sensible à son changement d'état. En effet, nous avons modélisé de nombreux scénarios d'accident dans les domaines : ferroviaire, routier, machine, manufacturier, professionnel, épidémiologique, politique, médiatique et juridique. De surcroit, l'ontologie proposée est adaptée aux risques aérien, maritime, spatial, militaire, nucléaire, chimique, NTIC[3], projet, financier, économique, commercial, social, éthique et théologique.

5 Travaux cités

Brenac, T., Nachtergaele, C., & Reiner, H. (2003). *Scénarios types d'accidents impliquant des piétons et éléments pour leur prévention, Rapport INRETS n°256.*

CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service.* CEI.

Charlet, J., Zacklad, M., Kassel, G., & Bourigault, D. (2000). *Ingénierie des connaissances, évolutions récentes et nouveaux défis.* Eyrolles.

Code de l'Environnement: Article L. 511-1. (17 janvier 2001). *Loi n° 2001-44 du 17 janvier 2001 art. 11.* Journal Officiel de la république française.

Dialo, G. (2006). *Une architecture à Base d'Ontologies pour la Gestion Unifiée des Données Structurées.* Grenoble: Thèse de doctorat, Université Joseph Fournier.

EN 292/ISO 12100. (1995). *Sécurité des machines ; Notions fondamentales, principes généraux de conception.* ISO/CEN.

Grüber, T.-R. (1993). *A translation approach to portable ontologies. Knowledge Acquisition.*

Grüber, T.-R. (1992). *Ontolingua : A mechanism to support portable ontologies.* Standford University, Knowledge Systems Laboratory.

Grüber, T.-R., & Thomas, R. (1993). *Towards principles for the Design of Ontologies Used for Knowledge sharing in formal Ontology in conceptual Analysis and Knowledge Representation.* Kluwer Academic Publishers.

GT Aspects sémantiques du risque. (1997). *Vocabulaire lié au risque à travers une analyse bibliographique.* Institut de Protection et de Sûreté Nucléaire (IPSN) - Observatoire de l'Opinion sur les Risques et la Sécurité.

GT Méthodologie. (2003). *Principes généraux pour l'élaboration et la lecture des études de dangers.* INERIS.

Guarino, N. (1998). *Some ontological principles for designing upper level lexical resources.* IOS Press.

HSE. (1992). *Generic terms and concepts in the assessment and regulation of industrial Risks.* UK: Health and Safety Executive.

[3] Nouvelles Technologies de l'Information et de la Communication

ISO 21127. (Août 2002). *Information and documentation — A reference ontology for the interchange of cultural heritage information.* ISO.

ISO/CEI Guide 73. (2002). *Management du risque – Vocabulaire – principes directeurs pour les inclure dans les normes.* ISO/CEI.

Larousse. (2006). Larousse Définitions.

Laurant, A. (2003). *Sécurité des procédés chimiques.* Lavoisier.

Manesh, K. (1996). *Ontology development for machine translation: Ideology and methodology. Memoranda in computer and cognitive science.* New Mexico State University, Computing Research Laboratory, Las Cruses, New Mexico.

Marsot, J. (1998). Nacelles élévatrices de personnel - Etude des schémas de commande. *Cahiers de notes documentaires - Hygiène et sécurité du travail - N°171, 2e trimestre 1998, INRS* .

NF EN 280. (2001). *Plates-formes élévatrices mobiles de personnel. Calculs, stabilité, construction. Sécurité, examen et essais.* Paris: AFNOR.

NF EN 61508. (Décembre 1998). *Sécurité fonctionelle des systèmes électriques et électroniques programmables relatifs à la sécurité.* Paris: AFNOR.

Petit Robert. (1984). *Dictionnaire.* Paris.

Roche, C. (2005). Ontologie et Terminologie. *Larousse - Revue* , n° 157, pp 1-11.

Sowa, J. (1984). *Conceptual structures: Information processing in mind and machine - The system Programming series.* Wesley Publishing Inc.

Van Elslande, P., Alberton, L., Nachtergaele, C., & Blanchet, G. (1997). *Scénarios types de production de l'erreur humaine dans l'accident de la route : problématique et analyse qualitative, Rapport INRETS n°218.* Paris: lavoisier.

Van Heijst, G., Schreiber, A., & Wielinga, B. (1997). Using explicit ontologies in kbs development. *International Journal of Human-Computer Studies* , 46(2/3), pp 183-292.

TABLE DES MATIÈRES DU CHAPITRE 6: MANAGEMENT PRÉLIMINAIRE DES RISQUES

Chapitre 6

MANAGEMENT PRÉLIMINAIRE DES RISQUES

Comme nous l'avons vu au chapitre 2 §1, selon la norme CEI 300-3-9 (CEI 300-3-9, 1995) l'APR est une technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité. Néanmoins, usuellement, l'APR ne se limite pas à la phase d'appréciation des risques (analyse + évaluation), mais elle fournit en sortie des directives de maitrise des risques, ce qui fait d'elle une méthode de management préliminaire des risques plutôt que d'analyse!

En effet, il est, aujourd'hui plus qu'hier, nécessaire de posséder une vision globale de son environnement, connaître les nouvelles réglementations en vigueur, être au courant des évolutions technologiques, et des facteurs socioéconomiques pour réagir, voir mieux, et ensuite agir.

Ainsi, toutes les parties responsables faisant partie du système global et concernées de près ou de loin par l'activité à risque, doivent contribuer à la mise en place et au maintien d'un SMS (Système de Management de la Sécurité) offrant un cadre propice à une meilleure préparation pour faire face aux scénarios de risque. Cela signifie fixer au préalable puis mettre en œuvre des actions coordonnées de maitrise permettant de réduire le risque global à un niveau acceptable.

1. 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 une ontologie générique permettant de canaliser les mécanismes de capitalisation et d'exploitation des connaissances relatives aux scénarios d'accident (causalité, entités, situations, événements, etc.). La méthode MPR se rattache au Système de Management de la Sécurité (SMS) par le point d'ancrage essentiel qu'est la gestion des processus techniques et organisationnels.

Notre démarche est basée sur l'ontologie générique développée dans le chapitre 4 dont le but est d'uniformiser les concepts de base et établir un lien sémantique à travers ces concepts afin de mieux maitriser la matérialisation des scénarios d'accident.

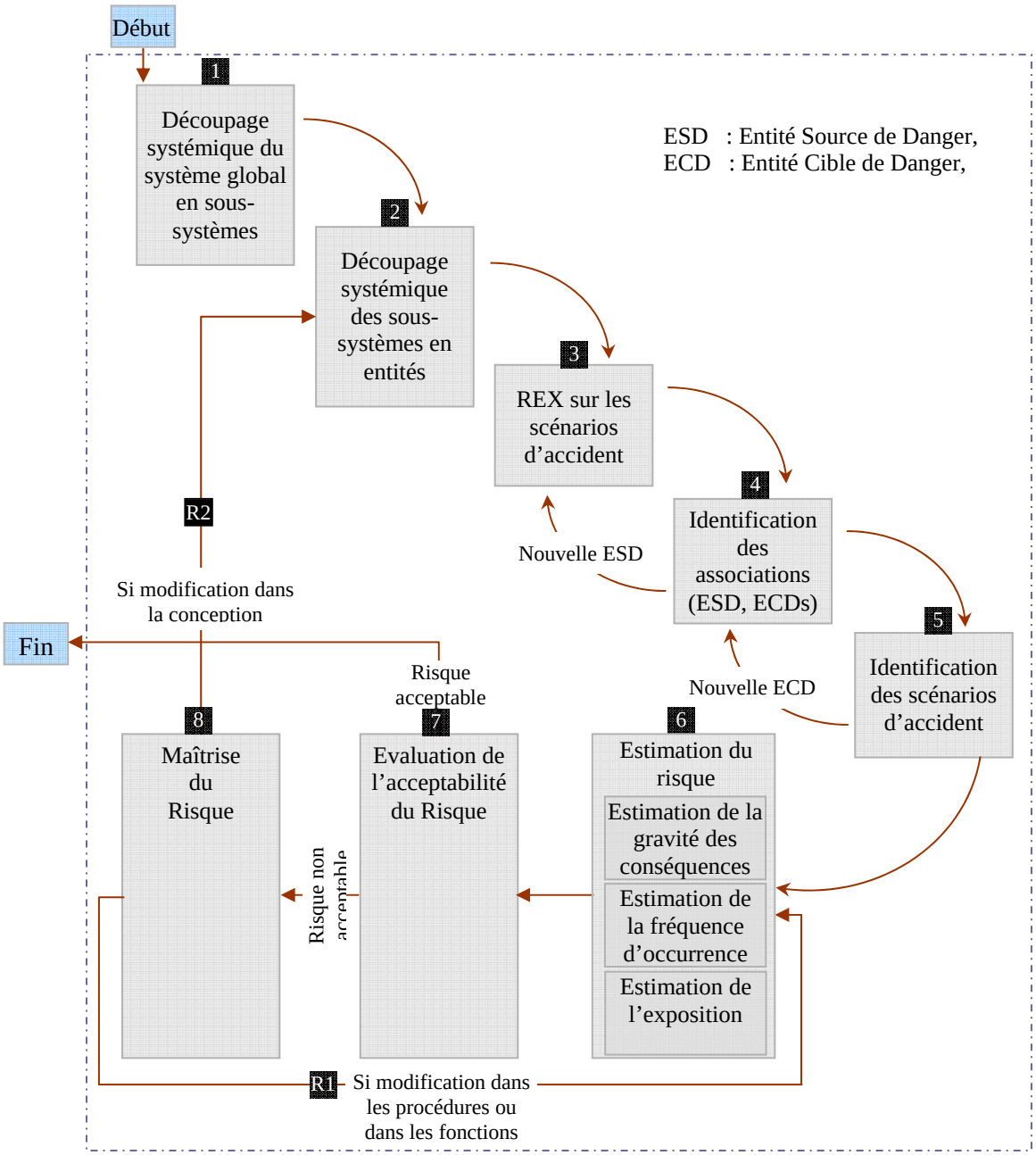


FIG. 1: Processus de la méthode MPR

Cependant, l'objectif final de notre étude est de concevoir un Système Interactif d'Aide à la Décision (SIAD) en matière de management des risques. 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 de notre outil (Mazouni & Aubry, 2007; Mazouni, Bied-Charreton, & Aubry, 2007).

1.1 Découpage systémique du système global

La systémique est une vision à la fois moderne et prudente du monde. L'avènement de l'ère industrielle nous avait incité à penser que nous nous dirigions vers une maîtrise totale et une connaissance exhaustive des systèmes technologiques ; Il nous faut maintenant déchanter et admettre que les limites de la science reculent au moins autant que ne progresse notre connaissance et que plus fondamentalement encore nous ne savons pas maîtriser correctement les problèmes que nous avons nous-mêmes créés.

Entre 1940 et 1960, une véritable explosion de concepts et notions nouvelles dans de nombreux domaines des sciences et des techniques a eu lieu (Gallou & Bouchon-Meunier, 1992). Ainsi, on a tenté de définir et introduire la notion de système, ceci dans un premier temps et puis la littérature atteint même la notion de systémique qui est devenue plus tard une approche très répandue dans plusieurs domaines mobilisant de nombreuses compétences scientifiques et techniques (biologie, écologie, économie, psychologie, psychanalyse, thérapies de groupe, sciences sociales, sciences politiques, informatique, robotique, sciences des organisations, ergonomie, sciences juridiques,..).

La systémique s'est développée d'abord par simple extension de la théorie des systèmes. Cette nouvelle discipline regroupe des démarches théoriques, pratiques et méthodologiques visant à préciser des frontières, des relations internes et externes, des structures, des lois ou propriétés émergentes caractérisant un système donné.

Le théorème de « l'indécidabilité » (appelé aussi théorème d'incomplétude) de Gödel démontre qu'on ne peut connaître entièrement un système en restant à l'intérieur de ses frontières.

Un système (global) n'est pas égal à la somme de ses constituants, car tout simplement, ces derniers sont indissociables. Justement, appliquée à un système complexe, l'approche systémique tient compte des interactions internes entre ces composantes.

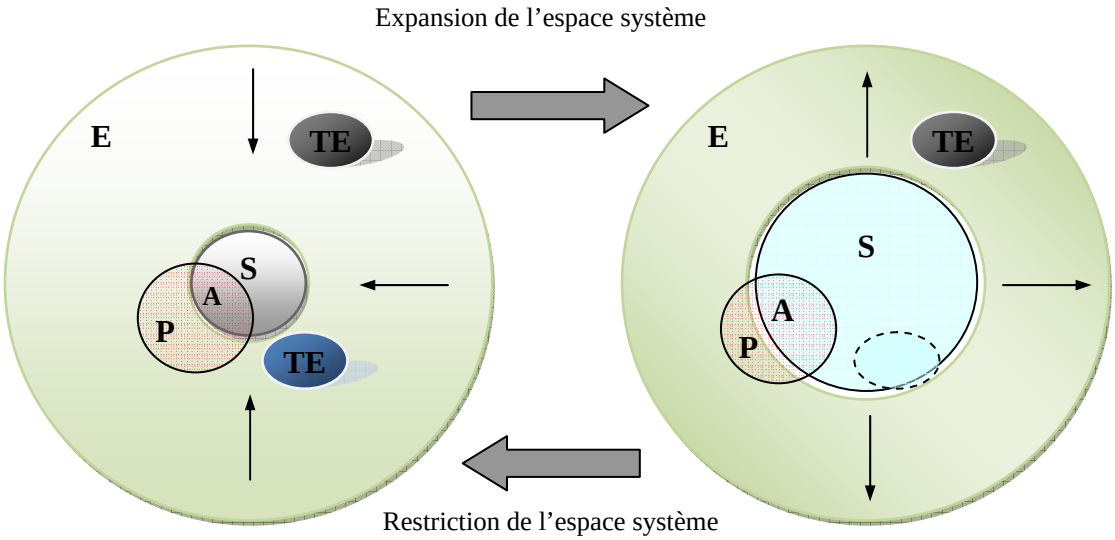
En effet, les interactions Système/Humain, Système/Environnement et Humain/Environnement doivent être étudiées avec prudence car il ne saurait suffire d'avoir un système technologique sûr de fonctionnement, des facteurs humains fiables et un environnement adapté pour se prononcer sur la réalisation des objectifs de sûreté de fonctionnement (RAMS).

1.1.1 *Découpage systémique du système global en sous-systèmes*

Notre vision systémique et générique d'un système industriel global, nous a amené à définir deux espaces hétérogènes : l'espace Système sociotechnique englobant la technologie et les acteurs, et l'espace Environnement caractérisé par les membres du public, les installations technologiques avoisinant le système sociotechnique et l'environnement naturel avec ses conditions météorologiques, hydrologiques et/ou géologiques, sismiques, etc. (cf. FIG. 2).

La composante humaine est donc divisée en deux grandes catégories hétérogènes :

- Les acteurs : l'ensemble des utilisateurs de l'espace système (opérateurs, agents de maintenance, etc.)
- Le public : l'ensemble des personnes se trouvant dans l'espace environnant (passagers, riverains, etc.)



***S** : Système sociotechnique. **E** : Environnement.*

***A** : Acteurs. **P** : Public. **TE** : Technologie de l'environnement.*

FIG. 2: Le système et son environnement

L'expansion de l'espace système (sociotechnique) sur l'environnement contraint à considérer autrement les facteurs humains et les sous-systèmes se trouvant, en effet, à l'intérieur des nouvelles frontières. Par exemple, les agents de maintenance intervenant sur les voies peuvent être considérés comme faisant partie du système, l'infrastructure peut être considérée comme faisant partie du système ou bien de l'environnement.

1.1.1.1 Le Système sociotechnique

(a) Le Système technologique

Le système technologique est l'ensemble des entités, matériels, logiciels et tous les aspects fonctionnels permettant de les gérer.

Définir un système générique renvoie systématiquement à considérer les aspects suivants :

- La description générale du système, de ses limites et de ses interfaces
- La description des différents profils de mission
- La description fonctionnelle en partant d'une décomposition structurelle.

Dans le domaine ferroviaire, conformément aux dispositions des directives européennes d'interopérabilité (Directive 96/48/EC, 23 juillet 1996)(Directive 2001/16/EC, 19 mars 2001)**,** le système ferroviaire générique doit être décomposé en deux sous-systèmes :

- Le sous-système structurel : c'est la partie physique du système ferroviaire. Cette partie englobe l'Infrastructure (réseau)' et les 'Trains':

- La voirie : heurtoirs, voies, postes d'aiguillage, croisements, station, génie civil (ponts, viaducs, tunnels, Passages à niveau, etc.).
- L'énergie : Source d'énergie électrique, caténaires aériens, pantographes, etc.
- La signalisation et les systèmes de contrôle/commande.
- Le matériel roulant.

- Sous-système fonctionnel :
  - La maintenance : procédures et actions correctives ou préventives nécessaires.
  - L'exploitation : mode normal et dégradé.

(b) Les Acteurs

Tout employé est sensé contribuer à l'accomplissement de l'objectif de sécurité. Les acteurs sont l'ensemble des équipes techniques, managériales et de formation impliquées tout au long du cycle de vie d'un projet, c.-à-d. de la spécification jusqu'au démantèlement.

Dans le domaine ferroviaire, on peut distinguer entre quatre classes d'acteur affectées aux opérations d'exploitation ou de maintenance :

- Les agents travaillant dans le train.
- Les agents travaillant dans les stations.
- Les agents travaillant sur ou près de la ligne.
- L'ensemble des sous-traitants.

De nombreux processus comportent un potentiel d'erreur humaine. L'erreur humaine (Mistake, Human error) est définie dans la norme CEI 50(191) (CEI 50(191), 1990) comme une : « action humaine qui produit un résultat différent de celui qui est recherché ». La norme donne la définition suivante à la notion d'erreur (Error) dans le sens le plus large du terme : « (Une erreur est) un écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte ».

Toutefois, l'analyse de l'erreur humaine devrait compléter d'autres analyses traitant des aspects techniques afin de donner une nouvelle dimension à l'étude de risques en intégrant l'impact du facteur humain sur le fonctionnement du système et d'évaluer l'influence de la fiabilité humaine sur la fiabilité globale.

Les erreurs humaines peuvent être classées en trois catégories :

- Erreurs au niveau comportemental : l'erreur est imputée directement à l'individu, selon J. Reason (Reason & Parker, 1993) ça peut être un acte de sabotage, violation routinière, violation exceptionnelle, mauvaise application d'une bonne règle, application d'une mauvaise règle, faute basée sur les connaissances déclaratives, etc.).
- Erreurs au niveau contextuel : ici on considère que l'erreur est humaine, mais jamais seulement humaine et on cherche à déduire son origine et son contexte qui peut être dans certains cas du à un manque de formation, problèmes d'ergonomie, complexité des tâches, etc.

- Erreurs au niveau conceptuel : on exploite des hypothèses sur les mécanismes cognitifs en distinguant les types d'erreurs (intentionnelles, non intentionnelles) et les formes d'erreurs (Violation/Faute, Raté/Lapsus).

1.1.1.2 Environnement

L. Goffin (Goffin, 1976) défini l'environnement comme « un système dynamique défini par les interactions physico-chimiques, biologiques et culturelles, perçues ou non, entre l'homme, les autres êtres vivants et tous les éléments du milieu, qu'ils soient naturels, transformés ou créés par l'homme ».

L'environnement possède plusieurs caractéristiques, nous insistons sur les trois suivantes (Goffin, 1976):

- L'environnement est « global ». Il se présente donc comme un système, c'est-à-dire un ensemble complexe d'éléments structurés et fonctionnels en interaction. Il s'établit une dynamique par les échanges continus entre les sphères « nature » et « humaine » selon un jeu perpétuel d'équilibres et de déséquilibres.
- L'environnement est « multidimensionnel ». Il se réfère à la fois aux dimensions physiques, chimiques, biologiques, techniques, économiques, sociales, politiques et culturelles de la vie humaine. Diverses disciplines sont donc nécessaires pour l'appréhender. Il est souhaitable de les travailler en interdisciplinarité.
- L'environnement « se délimite dans l'espace et le temps ». Il doit donc être localisé de façon précise, dans un cadre spatial et temporel. Chaque approche doit intégrer ces éléments mais ne pas les fermer. En effet, si nous délimitons un environnement, il est nécessairement influencé par celui qui l'englobe avec lequel il échange des interrelations ; de même, il s'inscrit dans une durée avec un impact du passé et une prévision du futur.

Dans le domaine industriel (nucléaire, transport, chimique, militaire), nous pouvons considérer comme faisant partie de l'environnement toute entité qui n'est pas sous le contrôle de l'entreprise, mais qui peut être une Entité Source de Danger (ESD) ou une Entité Cible de Danger (ECD) potentielle envers le système sociotechnique.

Enfin, nous considérons dorénavant que l'environnement est principalement caractérisé par trois types de risque : le risque humain véhiculé par le public, le risque technologique et le risque naturel.

(a) Environnement humain : membres du public

Personnes se comportant d'une manière légale ou illégale et qui ne sont pas sous le contrôle de l'autorité de l'organisation. Par exemple, dans le domaine ferroviaire, on peut différencier entre les groupes suivants :

- Les passagers situés dans le train.
- Les passagers se trouvant en station.

- Les tierces personnes se trouvant légitimement au sein de l'infrastructure, comme par exemple dans un passage à niveau.
- Les passagers se trouvant illégitimement dans certaines zones interdite au public, comme par exemple un passager qui traverse la voie dans une station.
- Les personnes vivant ou travaillant à proximité des infrastructures ferroviaires.
- Les services d'urgence et/ou d'intervention (pompiers, police, services d'urgence médicaux, etc.) peuvent être considérés comme faisant partie du Système quand il s'agit d'élaborer des plans d'interventions communes avec les agents de l'entreprise. Néanmoins, ils peuvent être affectés à l'environnement et plus précisément aux membres du public, s'agissant d'étudier cette fois ci leurs interactions avec le système étudié (accès et présence dans la zone d'intervention).

(b) Environnement technologique

C'est l'ensemble des systèmes technologiques environnants présentant une menace sur le système technologique, ou bien comportant une certaine vulnérabilité vis-à-vis des ESD appartenant au système technologique. Dans le premier cas, la technologie environnante est considérée comme ESD, dans le deuxième cas, elle se présente comme une ECD.

D'une manière générale, l'environnement technologique couvre les :

- Services de télécommunication, GPS (Global Positioning System), Galileo, les chaines d'électrification haute tension, etc.
- Bâtiments et installations comportant des processus de dangers (centrales nucléaires, raffineries, etc.).
- Routes, ponts et tunnels, passages à niveau, aéroports, ports, etc.
- Environnement électromagnétique.

(c) Environnement naturel

L'environnement naturel peut englober les (HMSO, 1995):

- Conditions écologiques : l'eau, l'air, le sol, ressources naturelles, faune, flore, etc.
- Conditions météorologiques : vent, pluie, neige, verglas, grêle, etc.
- Conditions hydrologiques : inondation, flots, marais, etc.
- Conditions géologiques/ hydrologique : glissements de terrain, les marécages, formation des poches souterraines, etc.
- Conditions sismiques.

1.1.2 *Découpage des sous-systèmes en entités*

Tout système global est chargé d'une mission qu'il doit accomplir à travers le fonctionnement en mode commun de ses constituants. Certes, pour chacun d'entre eux, on doit au moins connaître le profil de mission (ses tâches), ses frontières et ses interfaces directes, que ce soit avec l'entité mère ou avec des entités adjacentes du même niveau hiérarchique.

Nous avons adopté 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 ».

Ainsi un flux de danger peut s'exercer entre un sous-système et le système global, entre plusieurs sous-systèmes ou composants élémentaires logiciels, matériels, humains ou environnementaux, etc.

En effet, les entités globales sont, à leur tour, décomposées en des entités plus élémentaires, ainsi de suite jusqu'à l'obtention d'une représentation systémique globale. Cette représentation hiérarchique (voir FIG. 3) permettrait d'imaginer graphiquement la propagation du danger entre les différents niveaux hiérarchiques.

Mis à part l'entité (le rectangle) « système global » (voir FIG. 3), toute autre entité est susceptible de devenir une ESD ou une ECD. Justement, la phase 4 de la méthode MPR s'attache à déceler les associations de type (ESD, ECDs) pouvant donner lieu à un accident comme par exemple le système technologique en tant que ESD et l'environnement naturel en tant qu'ECD, à l'image des installations technologiques émettrices de gaz à effet de serre ou polluants (CO2, NOx). Dans cet exemple, l'association peut être raffinée, en travaillant sur l'unité d'incinération de déchets toxiques (ET1) appartenant à l'installation en ce cas là, il s'agit plutôt d'une association (ET1, Environnement naturel), voire même (ET1, Conditions écologiques) en propageant le danger vers les entités filles de l'environnement naturel.

Ainsi une situation d'accident relevant d'une entité donnée peut entraîner un effet domino sur une autre entité de voisinage appartenant au même ascendant (voir FIG. 3, ST11 et ST12), comme elle entraîner un effet domino sur l'ascendant lui même (voir FIG. 3, ST11 et ST1) ou bien sur un descendant (voir FIG. 3, equipe22 sur agent 221).

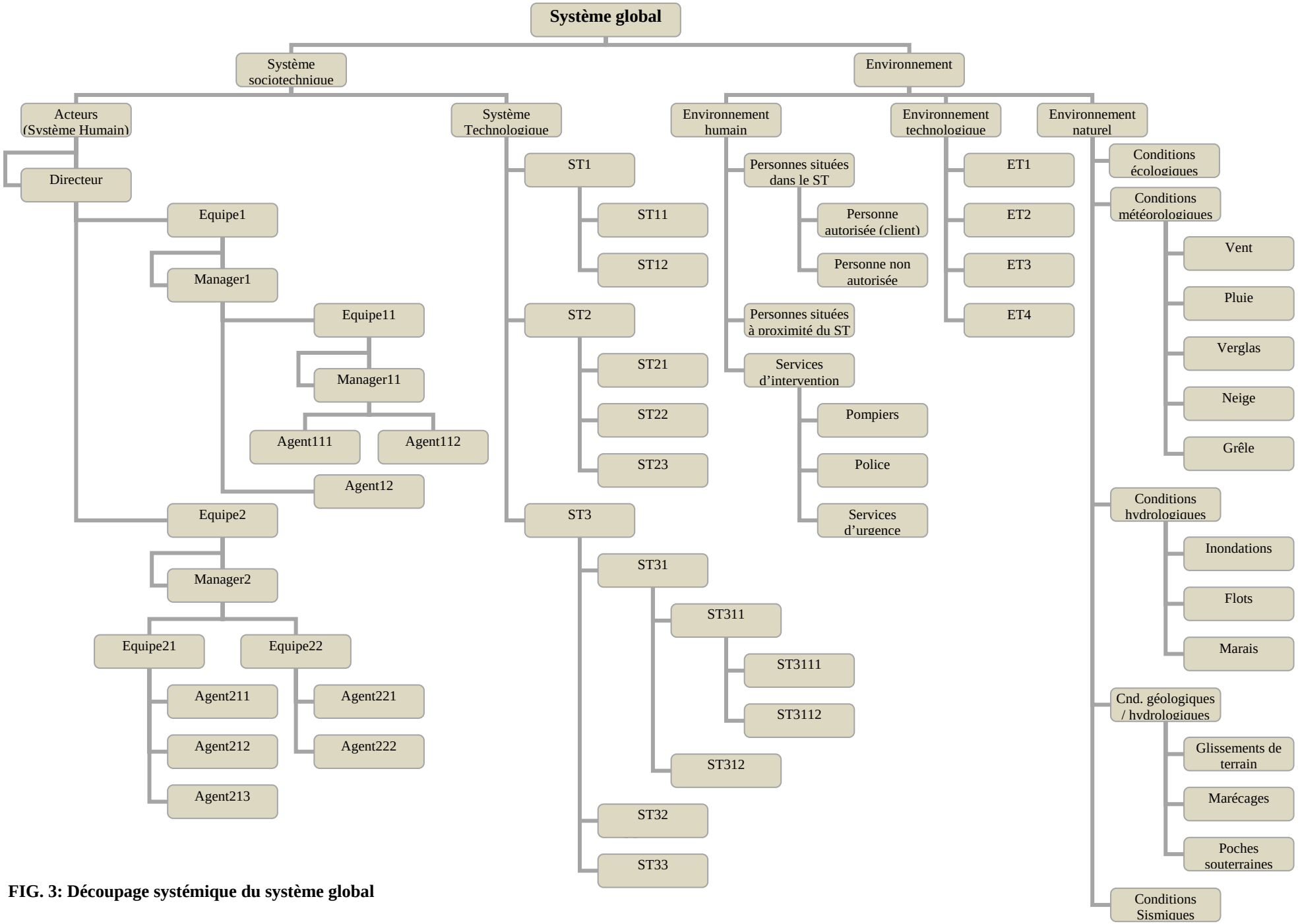


FIG. 3: Découpage systémique du système global

Le passage d'un train de transport de matière dangereuse à proximité d'une centrale nucléaire renvoie à considérer trois sous-systèmes sociotechniques différents (le train, la matière dangereuse et la centrale nucléaire) Ainsi, l'exploitant du train doit considérer dans son environnement et plus précisément sous la composante « Environnement Technologique » (voir FIG. 3) la matière dangereuse transportée (ET1) et aussi la centrale nucléaire (ET2). Ces deux entités du sous-système « Environnement Technologique » peuvent être raffinées en des entités plus élémentaires en fonction de la portée de l'étude et de la coopération entre les parties responsables de part et d'autre. Idéalement, la décomposition systémique s'arrêterait là où l'étude est reprise par un partenaire tel qu'un sous-traitant. La coordination entre les différentes parties passe à travers les canaux de communication des Systèmes de Management de la Sécurité afin d'augmenter le degré de confiance mutuelle en matière de sécurité.

1.2 Management des risques

Chaque partie responsable appartenant au système global doit mettre en place des procédures adéquates d'identification et d'évaluation des risques. Ces risques doivent être réduits à un niveau acceptable conforme aux objectifs de sécurité préalablement établis.

1.2.1 *Analyse des scénarios d'accident*

La phase d'identification des scénarios d'accident repose essentiellement sur un processus accidentel générique (Mazouni, Aubry, & El koursi, 2008). En effet, l'identification des scénarios d'accident sera basée sur le développement du processus accidentel en fonction de l'occurrence de trois types d'événements : Evénement d'Exposition (EvE), Evénement Initiateur (EvI) et Evénement Redouté (EvR). Ces événements jouent le rôle d'interrupteurs ayant la capacité de stimuler le changement de situation d'une ESD ou d'une ECD entre : Situation Initiale (SI), Situation d'Exposition (SE), Situation Dangereuse(SD) et Situation d'Accident (SA).

En effet, la démarche d'analyse de la méthode MPR consiste d'abord à identifier, principalement grâce au Retour d'Expérience, les accidents potentiels, les événements redoutés, et les associations sources (ESD), cibles (ECD) ayant amené à ces accidents. Ensuite analyser les ESD en vue d'identifier les différents scénarios d'accident.

Cependant, comme son nom l'indique, la méthode MPR n'est pas destinée à traiter en détail la matérialisation des scénarios d'accident, mais plutôt à mettre rapidement en évidence et se prémunir des gros problèmes susceptibles d'être rencontrés pendant le cycle de vie du système étudié. La démarche MPR peut aussi et même devrait permettre l'enchainement naturel des analyses de risque grâce au SIAD que nous étudierons dans le cadre du prochain chapitre.

1.2.1.1 Retour d'expérience sur les scénarios d'accident

Cette phase s'appuie principalement sur le retour d'expérience pour déterminer la liste des situations d'accident potentielles, et aussi des événements redoutés (EvR) correspondants. Les résultats sont mis dans un tableau d'analyse élémentaire ayant la forme suivante :

TAB. 1 : REX sur les scenarios d'accident

Situation d'Accident		Evénement Redouté
	1.1 avec obstacles	1.1.2 Distance d'arrêt trop longue
		…….
	1.2 avec tiers	1.2.1 Présence d'un véhicule routier ou de service sur la voie

1.2.1.2 Phase I : identification déductive des associations d'entités ESD/ECD(s)

En partant des résultats du retour d'expérience sur les Situations d'Accident **(**colonne **1** du tableau **2)** et les Evénements Redoutés **(**colonne **2** du tableau **2)** associés, on essaye, cette fois ci, d'identifier à froid l'ensemble des Situations Dangereuses **(**colonne **3** du tableau 2**)** préalables à l'apparition des EvR en question. Pour chaque SD, on identifie tout EvI **(**colonne **4** du tableau **2)** pouvant altérer la Situation Initiale d'une ESD, et enfin on élabore l'ensemble des associations (ESD, ECDs) **(**colonne **5** du tableau **2)** dont la proximité est accidentogène.

TAB. 2 : Identification des associations (ESD, ECDs)

1	2	3	4	5
Situation d'Accident	Evénement Redouté	Situation Dangereuse	Evénement Initiateur	ESD, ECD(s)

1.2.1.3 Phase II : identification inductive des scénarios d'accident

TAB. 3 : Identification des scénarios d'accident

1	2	3	4	5	6
Scénarios d'accident					
ESD	Evénement Initiateur	Situation Dangereuse	Evénement Redouté	Situation d'Accident	ECDs

Les ESDs identifiées lors de la phase 'I', sont reprises une par une dans cette nouvelle phase d'investigation inductive afin de déceler les aléas qu'ils sont susceptibles de provoquer. Ainsi, pour chaque ESD **(**colonne **1** du tableau **3)**, on décèle les EvI **(**colonne **2** du tableau **3**) significatifs ayant le potentiel de stimuler cette dernière qui devient alors génératrice de danger. De la même manière, on identifie les SD (colonne **3** du tableau **3**) qui en découlent de cette excitation de l'ESD, et pour chaque SD, on identifie les EvR (colonne **4** du

tableau **3**) pouvant se produire. Enfin, pour chaque EvR, on identifie les Situation d'Accident potentielles (colonne **5** du tableau **3**) et on liste l'ensemble des ECDs (colonne **6** du tableau **3**) atteintes par la SA.

1.2.2 *Evaluation des risques*

Cette partie consiste en l'évaluation des risques des scénarios d'accident identifiés lors de la phase précédente.

TAB. 4 : Evaluation du risque

7	**8**	**9**	**10**	**11**
Evaluation				
Dommages	Gravité	Occurrence	Exposition	Risque

1.2.2.1 Evaluation des dommages et estimation de la gravité

En effet, pour chaque scénario d'accident on fait une évaluation 'pire cas' (en anglais : *the worst case*) des conséquences pouvant être engendrées **(**colonne **7** du tableau **4)**, ensuite on estime la gravité correspondante **(**colonne **8** du tableau **4)** selon une grille systémique de gravité préalablement définie :

TAB. 5 : Grille systémique de gravité

Gravité	**Impact sur le Système**		**Impact sur l'Environnement**			**Enjeux de l'entreprise**
	Acteurs	**Technologie**	**Public**	**Environnement Technologique**	**Environnement Naturel**	
Mineure (G1)	Un blessé	Dommage mineur	Pas de blessés	Pas d'effets	Pas d'effets	Technique
Significative (G2)	Plusieurs blessés légers, ou un blessé grave	Dommage important	Pas de blessés	Dommage mineur	Menace significative	Commercial, Financier, Technique
Critique (G3)	Plusieurs blessés graves, ou un seul mort	Perte du système	Un ou plusieurs blessés légers, ou un blessé grave	Dommage important	Nuisance localisée	**(Crise localisée)** Juridique, Commercial, Financier, Technique
Catastrophique (G4)	Décès collectifs	(Sans importance)	Plusieurs blessés graves, un ou plusieurs morts	Destruction	Nuisance importante	**(Crise importante)** Economique, Médiatique, Juridique, Commercial, Financier, Technique

La notion de « nuisance » englobe divers aspects environnementaux, sociaux (bruit, pollution) susceptibles d'avoir une incidence sur le comportement ou la santé des individus qui y sont exposés. Le

dictionnaire Larousse (Larousse, 2006) défini littérairement le terme comme « tout facteur qui constitue un préjudice, une gêne pour la santé, le bien-être, l'environnement ». En effet, contrairement au concept de dommage à caractère aléatoire, brusque ou exceptionnel, le concept de nuisance peut être considéré comme une « détérioration souvent insidieuse de l'environnement et de la qualité de vie, généralement à caractère déterministe et continu ou permanent (AQS-GT OORS, Mars 1996). Le groupe de travail GT aspects sémantiques du risque (GT Aspects sémantiques du risque, 1997) évoque une « altération à caractère chronique ou permanent ». Cette définition correspond à ce que nous avons appelé « nuisance localisée », de surcroit la définition donnée par le GT OORS/AQS renvoie à la notion de nuisance importante étant donné qu'elle manifeste une détérioration.

1.2.2.2 Estimation de la fréquence d'occurrence

Après avoir estimé la gravité, on estime la fréquence d'occurrence **(**colonne **9** du tableau **4)** de l'EvR donnant lieu à l'accident.

A l'égard du projet ERTMS (voir chapitre 1 §4.2), nous adapterons, pour des fins de simplification, l'échelle de fréquences d'occurrence donnée par la norme NF EN 50126, en la ramenant de 6 à 4 niveaux (voir TAB. 6):

TAB. 6 : Echelle de fréquences d'occurrence adaptée de la norme NF EN 50126

Occurrence de EvR	Description
Invraisemblable (O1)	Extrêmement invraisemblable à survenir durant la vie du système<=10-9 /h
Rare (O2)	Invraisemblable à survenir mais possible durant la vie du système > 10-9 /h
Occasionnelle (O3)	Vraisemblable qu'il survienne plusieurs fois durant la vie du système
Fréquente (O4)	Vraisemblable qu'il survienne fréquemment durant la vie du système

1.2.2.3 Estimation de l'exposition

L'avant dernière étape de la phase d'évaluation du risque, est l'estimation du degré d'exposition au danger (colonne 10 du tableau 4) des cibles ECDs concernées par le scénario d'accident en question.

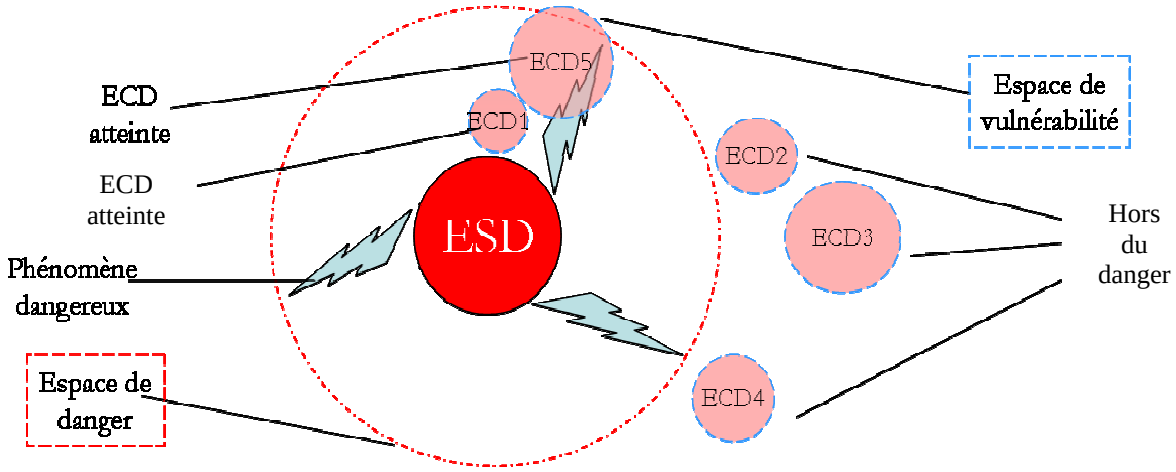


FIG. 4: Recouvrement des espaces de vulnérabilité avec l'espace de danger

L'exposition des ECDs est estimée en fonction des besoins de séjour dans l'espace de danger, de la nature des espaces de vulnérabilité, du temps passé, du nombre de cibles et de la fréquence d'accès.

Cependant, généralement l'exposition est fonction de deux variables : la durée et la fréquence d'accès (NF EN 60204, Avril 1998) (Whittingham, 2004):

- ECDs s'exposant rarement (**F1**).
- ECDs s'exposant fréquemment (**F2**).
- ECDs s'exposant durant de courtes durées (**D1**).
- ECDs s'exposant durant de longues durées(**D2**).

TAB. 7 : Estimation du degré d'exposition

	F1	F2
D1	**E1**	**E2**
D2	**E2**	**E2**

Dans le domaine de la « sécurité machine », la norme ISO 12100 (EN 292/ISO 12100, 1995) dans sa première partie, ajoute que l'estimation de l'exposition requiert l'analyse et la prise en compte de tous les modes de fonctionnement de la machine et de toutes les méthodes de travail.

1.2.2.4 Evaluation du risque

Une fois la gravité, la fréquence d'occurrence et l'exposition sont estimées, il ne reste qu'à évaluer le risque inhérent **(**colonne **11** du tableau **4)** à partir d'un graphe de risque, dont voici un prototype :

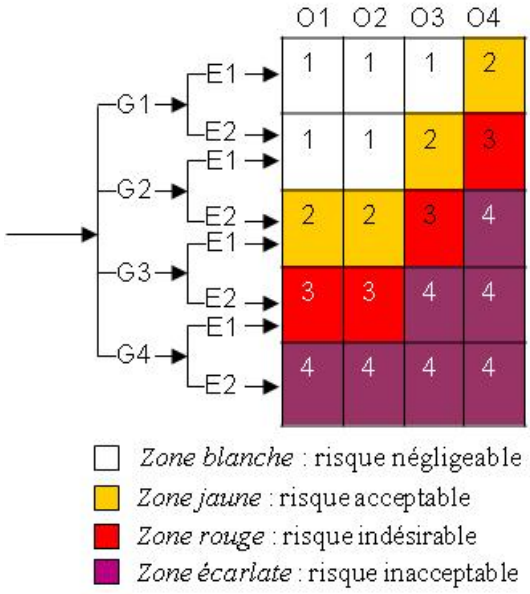


FIG. 5: Prototype d'un graphe de risque

Comme nous l'avions souligné dans le chapitre 5 (voir chapitre 5, §1.5), il convient de rappeler que notre engagement ontologique est minimal. Par conséquent, l'utilisateur peut soit accepter notre graphe de risque (voir FIG. 5), soit définir ses propres niveaux de gravité, et le cas échéant de fréquence d'occurrence et/ou d'exposition. Il peut aussi considérer seulement la gravité en vue de réaliser des analyses de danger telles que l'APD (Analyse Préliminaire des Dangers)**.**

1.2.2.5 Critères d'acceptabilité du risque

Le graphe de risque proposé (voir FIG. 5) est scindé en quatre zones de risque distinctes. En effet, chaque zone est caractérisée par des critères d'acceptabilité bien spécifiques (voir TAB. 8):

TAB. 8 : Critères d'acceptabilité du risque

Zone de criticité	Acceptabilité des risques	
Négligeable	**Acceptable**	Risques ne nécessitant pas l'accord de l'autorité de tutelle
Acceptable		Risques nécessitant un contrôle approprié et l'accord de l'autorité de tutelle
Indésirable	**Non acceptable**	Risques dont la réduction est impossible ou insuffisante et qui nécessitent un accord de l'autorité de tutelle
Inacceptable		Risques devant être réduits

1.2.3 *Maîtrise des risques*

1.2.3.1 Réduction des risques

Cette partie concerne toutes les actions de réduction de risque (Protection, Prévention, Transfert). Idéalement, ces actions devront être codifiées par des libellés **(**colonne **12** du tableau **9)** permettant de les décrire

clairement. Ces actions sont de natures différentes **(**colonne **13** du tableau **9)**, en l'occurrence il peut s'agir de disposition constructive, procédure ou mode opératoire, procédure et règles de maintenance, conception, dimensionnement, test, respect des référentiels de sécurité (norme, réglementation et autres).

TAB. 9 : Maîtrise des risques

12	13	14	15	16	17	18	19
Maîtrise des risques					**Décision**		
Libellé	Type	Pilotage		Gains potentiels	Libellé	Motifs	Responsable
		Equipe	Manager				

Nous avons insisté dans le chapitre 5 (voir §2.1.1.2, §2.1.2.1) que les espaces de danger et de vulnérabilité sont multidimensionnels. L'espace de danger est le même pour toutes les cibles. Donc, protéger une entité cible la rend insensible à certaines dimensions de l'espace de danger, c'est-à-dire que cela revient à réduire son espace de vulnérabilité de telle sorte qu'il n'y ait plus d'intersection avec l'espace de danger. Réduire un risque c'est donc réduire soit l'espace de danger soit l'espace de vulnérabilité pour diminuer voire annuler l'intersection.

1.2.3.2 Aspects organisationnels

Les actions de maîtrise des risques doivent être assignées à des équipes et des managers qualifiés à en assumer la mise en œuvre. Néanmoins, la plupart des industriels rencontrent des difficultés d'ordre organisationnel en matière de maîtrise des risques, à cause de l'encombrement du continuum de mesures de réduction des risques. En effet, nous consacrerons une partie organisationnelle relative au pilotage des actions de maîtrise des risques. Ainsi, chaque mesure est affectée à une équipe **(**colonne **14** du tableau **9)** sous la responsabilité technique d'un personnel expérimenté **(**colonne **15** du tableau **9)**.

1.2.3.3 La défense en profondeur

Le principe de défense en profondeur peut accompagner cette phase à travers les différentes situations et transitions du processus accidentel (voir TAB. 10):

TAB. 10 : Défense en profondeur par l'analyse du processus accidentel

Code	Signification	Situation de départ	Situation d'arrivée	Causes	Principe de défense en profondeur
EvE	Evénement d'Exposition	Situation Initiale	Situation d'Exposition	Internes ou externes aux	Réduire l'exposition et la

				ECDs	vulnérabilité des ECDs
EvI	Evénement Initiateur	Situation Initiale	Situation Dangereuse	Internes ou externes à l'ESD	Réduire la sensibilité de l'ESD et éviter l'occurrence des EvI
EvR	Evénement Redouté	Situation Dangereuse + Situation d'Exposition	Situation d'Accident	Dangerosité de l'ESD + Vulnérabilité des ECDs	Atténuation des effets + Limitation des conséquences

En effet, il convient de structurer les lignes de défense en profondeur en concevant des barrières appropriées à chaque phase élémentaire du processus accidentel. Ainsi concernant la situation d'exposition, il convient de réduire les fréquences et les durées d'exposition tandis que pendant la situation dangereuse il convient d'éviter l'apparition de l'événement redouté et enfin durant la situation d'accident, on cherche à minimiser les conséquences.

1.2.3.4 Décision

Avant l'approbation des actions de maîtrise des risques par le ou les responsables hiérarchiques **(**colonne **19** du tableau **9)**, on doit, toutefois, estimer les gains potentiels **(**colonne **16** du tableau **9)** résultant de l'application de ces mesures, en faisant un arbitrage Coût/Bénéfices entre le coût et la faisabilité de mise en œuvre et le taux de réduction du risque.

Par conséquent, une action peut être accordée ou bien rejetée **(**colonne **17** du tableau **9)**. Cependant, l'approbation ou la désapprobation d'une quelconque action doit être explicitement motivée **(**colonne **18** du tableau **9)**.

En effet, cette partie a pour vocation d'engager une politique de gouvernance des risques afin que les décideurs au plus haut sommet d'une organisation soient responsabilisés. Car le simple fait qu'un responsable porte sa mention quant à l'engagement ou non d'une action, peut représenter un frein à la politique du moindre coût et une ouverture sur le principe dit « la sécurité passe avant tout », plus connu sous le nom « Safety first » qui consiste à accorder la plus haute priorité à la sécurité et ce, normalement avant les considérations économiques, opérationnelles, environnementales, sociales, ou autres.

L'efficacité de l'action se corrèle avec le coût et le délai de sa mise en œuvre. En effet, certains principes de sécurité, tel que ALARP (voir chapitre 3 §4.3), font un arbitrage entre les investissements en matière de sécurité et les gains potentiels à défaut de « shunter » la sécurité là où elle revient excessivement cher !

Toutefois, le décideur peut parfois faire un tri entre plusieurs actions que l'équipe technique lui propose. Il peut procéder de la manière suivante :

- Revoir des méthodes de réduction du risque suggérées par l'équipe technique.
- Comparer les différentes options (voir TAB. 11).
- Appliquer la méthode choisie pour contrôler les risques.
- Gérer les risques résiduels.

TAB. 11 Priorités des actions de maitrise des risques

Eléments du risque	Action idéale	Autres actions
Gravité	Supprimer les sources de danger	Réduire la dangerosité des sources de danger
Fréquence et/ou durée d'exposition	Supprimer l'exposition des cibles vulnérables	Réduire la fréquence et / ou la durée d'exposition
Probabilité d'occurrence	Supprimer les événements redoutés	Réduire la probabilité d'occurrence des événements redoutés

1.2.4 *Présentation des résultats*

Les résultats du MPR sont regroupés dans trois tableaux complémentaires : le descripteur de l'arborescence des situations d'accident (voir TAB.1, §1.2.1.1), le descripteur de l'analyse déductive (voir TAB. 2, §1.2.1.2), et enfin le troisième descripteur regroupant le reste des résultats de l'analyse qui prend le format suivant (voir TAB. 12) :

TAB. 12 : Présentation des résultats de la méthode MPR

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 désirés	Lib.	Motifs	Responsable
													Equipe	Manager				

2. Intégration de la méthode MPR au cycle de vie

La méthode 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 FIG. 1) 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 postériori 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 compliquée car elle consiste à 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.

.

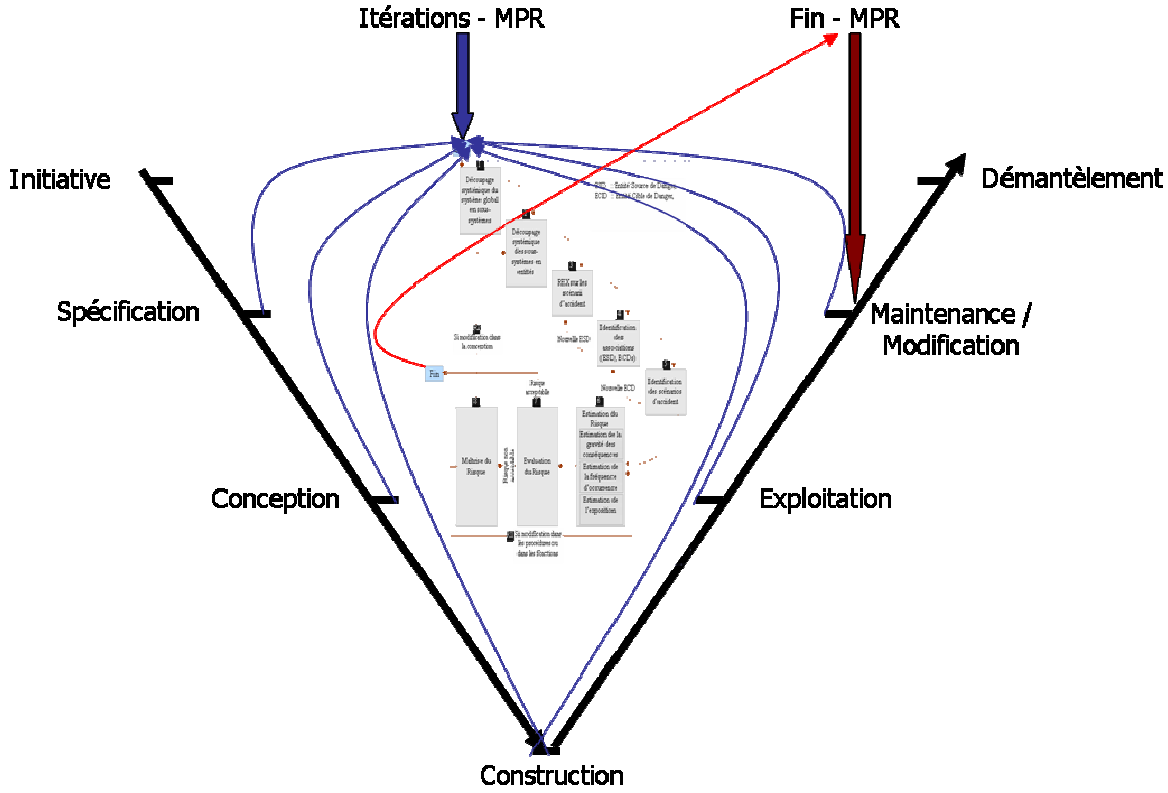


FIG. 6: Intégration de la méthode MPR au cycle de vie d'un système

La méthode peut idéalement accompagner le cycle de vie d'un system générique, autrement dit dès la phase de spécification jusqu'à la phase de démantèlement. Ceci consiste à répéter le processus MPR depuis la seconde phase (cf. FIG. 6) à chaque étape du cycle de vie (Initiative, spécification, conception, construction, exploitation, maintenance/modification, démantèlement).

3. Adéquation entre la méthode MPR et le SMS

3.1 Evolution de l'analyse technique vers le management organisationnel

Les approches d'analyse de risque ont fait l'objet de nombreuses évolutions. Au milieu des années 70 à l'approche technologique (la technologie comme source de problème) fut substituée une approche par l'erreur humaine (l'Homme comme source de problème). Cette transition a été justifiée par les résultats de l'enquête technique post-accident de la catastrophe aérienne survenue le 27 mars 1977 à l'aéroport de Tenerife – Espagne tuant 583 personnes, ainsi que par les rapports d'expertise de la catastrophe nucléaire vécue, deux ans plus tard,

quasiment jour pour jour, le 28 mars 1979 à Three Mile Island près de Harrisburg, Pennsylvanie – USA (accident classé niveau 5 sur l'échelle INES).

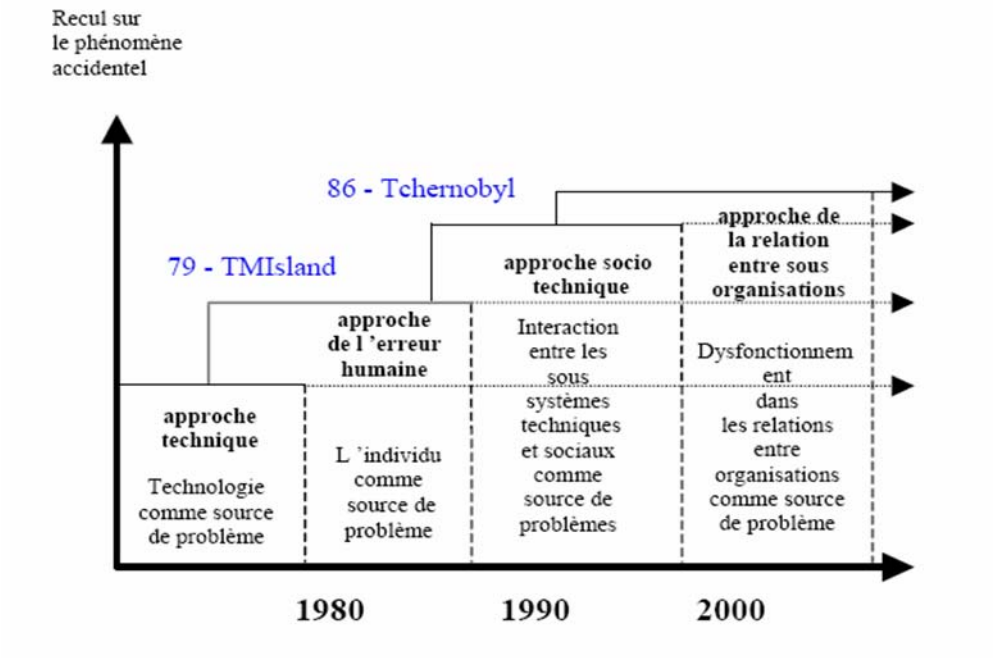


FIG. 7: Evolution de la recherche nucléaire (INERIS-DRA, 2003)

Néanmoins, l'approche humaine s'est avérée contestable à son tour. Par conséquent, à la fin des années 80, et principalement suite à la catastrophe nucléaire de Tchernobyl – Ukraine survenue le 26 avril 1986 (niveau 7 sur l'INES) portant atteinte à 9 millions d'adultes et plus de 2 millions d'enfants selon l'ONU (cf. Conférence OMS 1995) et causant plus de 560.000 morts par cancer, on a commencé à recentrer l'analyse sur les interactions entre les différentes composantes du système sociotechnique (Homme/ Système/ Environnement).

Encore quelques années plus tard, l'approche sociotechnique fut abandonnée progressivement au profit d'une approche organisationnelle et pluridisciplinaire considérant le dysfonctionnement dans les relations entre organisations comme source de problème. Autrement dit, c'est la prise en considération à travers un SMS global de toute sorte de défaillance technique, humaine ou organisationnelle.

Les SMS apportent essentiellement des améliorations considérables en matière de : planification de la sécurité, management des risques, échange d'information en matière de sécurité, mesure de la performance en matière de sécurité, et assurance du mangement de la sécurité. La qualité de ces améliorations dépend de la culture de la sécurité de l'organisme.

Dans le domaine ferroviaire la directive de sécurité (Directive 2004/49/EC, 29 avril 2004) dans son Annexe III, consacré d'ailleurs au SMS, stipule que : « Le système de gestion de la sécurité doit être documenté dans toutes ses parties et décrire notamment la répartition des responsabilités au sein de l'organisation du gestionnaire de l'infrastructure ou de l'entreprise ferroviaire. Il indique comment la direction assure le contrôle

aux différents niveaux de l'organisation, comment le personnel et ses représentants à tous les niveaux participent et comment l'amélioration constante du système de gestion de la sécurité est assurée ».

Dans le domaine des installations industrielles, on parle de « Système de gestion de la sécurité » regroupant l'ensemble des dispositions mises en œuvre (par l'exploitant) au niveau de l'établissement, relatives à l'organisation, aux fonctions, aux procédures et aux ressources de tout ordre ayant pour objet la prévention et le traitement des accidents majeurs » (INERIS-DRA ARAMIS, 2004).

3.2 Eléments de base d'un SMS centré-MPR

Le Système de Management de la Sécurité (SMS) est un processus technico-organisationnel de gestion des risques. Le SMS est un schéma complet d'activités d'analyse, d'évaluation et de maitrise des risques. En outre, il comprend aussi des stratégies de définition des responsabilités, de communication et de gestion des crises. Ces stratégies sont préalablement réfléchies sur les plans technique, humain et organisationnel.

Le SMS que nous proposons (cf. FIG. 9) est principalement centré sur la méthode MPR. Ce rapprochement SMS-MPR s'inscrit dans un processus d'amélioration de type PDCA (voir. FIG. 8).

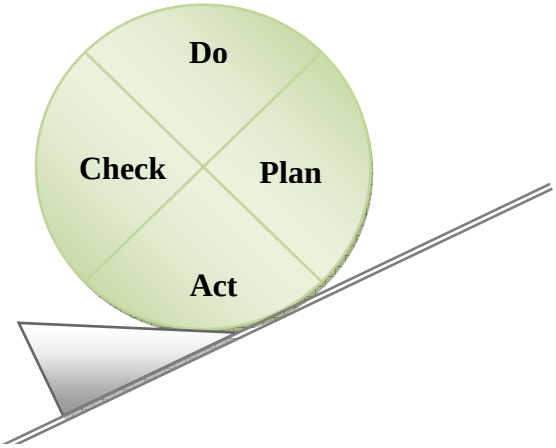


FIG. 8 : La roue de Deming d'amélioration continue (FD X 50-173, 1998)

- **P**lan (Planifier) : planifier et déterminer le degré de priorité des actions pour corriger les dysfonctionnements, maitriser les risques et déployer les objectifs Qualité.
- **D**o (Faire): mettre en œuvre et gérer des actions correctives et de progrès.
- **C**heck (Vérification) : vérifier l'efficacité du système qualité et évaluer les résultats obtenus par rapport à l'objectif qualité.
- **A**ct (Agir) : agir et exploiter les résultats à des fins de retour d'expérience et d'amélioration continue.

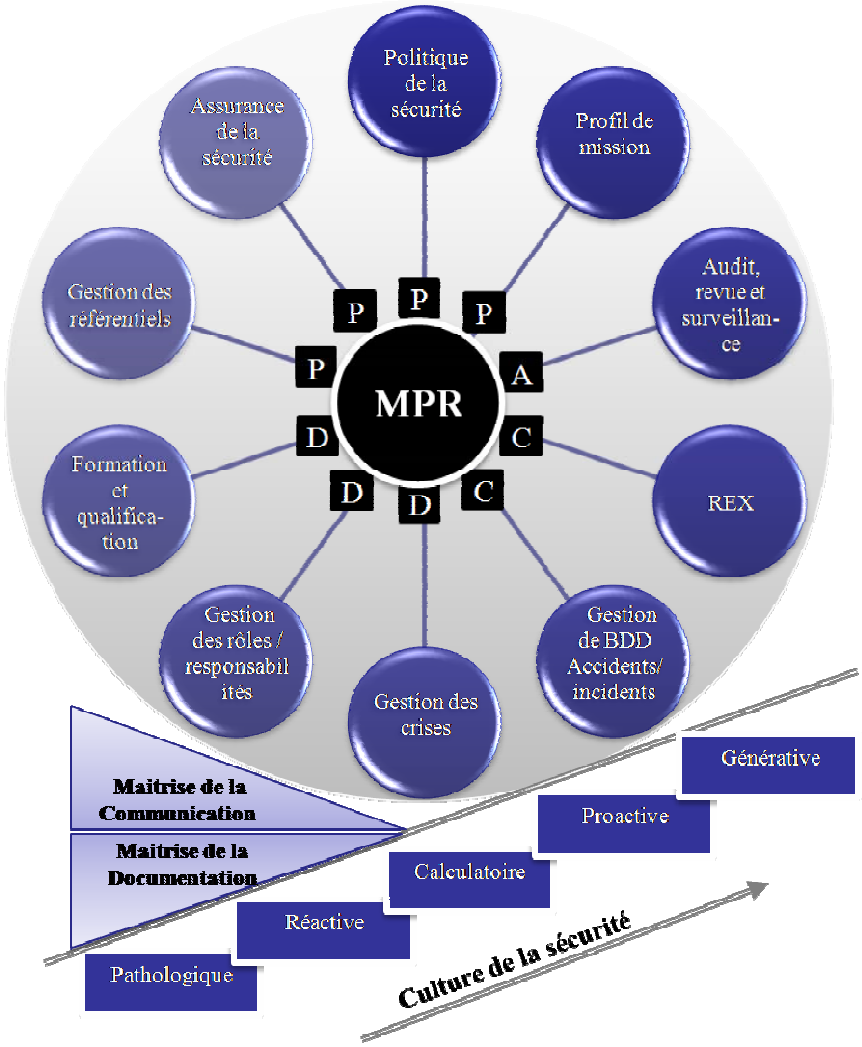


FIG. 9: Structure du SMS basé sur la méthode MPR

- **Profil de mission** : Les parties responsables doivent identifier la nature et les possibilités de leurs opérations. Elles doivent en particulier préciser les éléments qui sont sous leurs responsabilités.
- **Politique de la sécurité** : Chaque partie est tenue de démontrer ses capacités à maintenir la sécurité à un niveau acceptable.
- **Assurance de la sécurité :** Chaque partie responsable doit s'assurer de la bonne gestion de tous les risques ayant un lien avec le système global et qui ne sont pas sous son contrôle direct.
- **Gestion des référentiels :** Chaque partie responsable doit mettre en place des procédures d'identification des textes réglementaires, règles, normes et besoins techniques ayant un lien avec son activité.
- **Gestion des rôles et affectation des responsabilités**

1. **Gestion des crises :** Chaque partie responsable doit mettre en place un support de procédures génériques permettant de prévoir ce qu'il faut faire face à certaines situations de crise.

- **Gestion des Bases de Données accidents/incidents** : Chaque partie responsable doit mettre en place des mécanismes de capitalisation et d'investigation sur les accidents et incidents.

- **Retour d'Expérience (REX)** : Le retour d'expérience est le fait d'exploiter des connaissances historiques archivées afin de dégager un savoir-faire en matière de management de la sécurité.
- **Maitrise de la communication** : Toutes les parties responsables doivent s'assurer qu'ils sont au courant de la criticité des communications au sein du système global.
- **Formation et qualification** : Chaque partie responsable doit s'assurer de l'aptitude de ses employés à accomplir leurs tâches.
- **Audit, revue et surveillance** : Chaque partie responsable doit mettre en place des procédures régulières d'audit, et de revue du SMS.
- **Maitrise de la documentation** : Le SMS doit être documenté dans toutes ses parties en indiquer comment la direction assure le contrôle aux différents niveaux de l'organisation, et comment le personnel et sa hiérarchie contribuent à maintenir les plans QHSE[1] (Qualité, Santé, Sécurité, Environnement).

La culture de la sécurité peut être peu propice au maintien d'un niveau de sécurité optimal. Les 5 niveaux mentionnés dans la FIG. 9 sont souvent cités dans les travaux de recherche :

La culture de sécurité pathologique consiste à « friser » les limites de la réglementation sans chercher à améliorer la sécurité. La culture réactive traduit une pratique « nombriliste » qui consiste à réagir seulement après l'accident. La culture calculatoire est une culture d'infaillibilité caractérisée par un excès de confiance dans les mécanismes de sécurité mis en place. La culture dite proactive est une conception nettement plus intéressante qui consiste à réfléchir à tous les problèmes liés à la sécurité aussitôt qu'ils se présentent. Enfin la culture générative vient en premier lieu, car hormis la considération proactive des problèmes liés à la sécurité, cette dernière est considérée comme le centre d'intérêt. On favorise dans cette culture l'anticipation des problèmes en encourageant les idées innovantes et originales.

4. Conclusion

La méthode MPR que nous avons présentée dans ce chapitre est principalement basée sur le processus accidentel ontologique abordé dans le chapitre précédent.

La méthode 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 dysfonctionnement de l'organisation, 29% à la fiabilité des équipements, 11% imputable à un opérateur, 2% à l'environnement et 5% à d'autres causes.

[1] Quality – Health & Safety – Environment

La démarche systémique permet de situer l'ensemble des entités du système global que nous avons 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.

La démarche MPR est conforme aux définitions normatives du management des risques que nous avons abordées en détail dans le 2éme chapitre. Ainsi, nous retrouverons la phase d'identification des scénarios d'accident à travers les deux phases 4 et 5 (voir FIG. 1), la phase d'estimation des risques à travers la phase 6, la phase d'évaluation des risques à travers la phase 7, et la phase de maitrise des risques à travers la phase 8.

Il convient de rappeler que le processus MPR est itératif (itérations R1 et R2) (voir FIG. 1), ce qui assure plus de complétude et de cohérence et permet à la méthode de trouver des points d'ancrage dans le cycle de vie du système pour accompagner son développement de la spécification au démantèlement.

La démarche MPR est parfaitement compatible avec le Système de Management de la Sécurité (SMS) ainsi qu'avec le Système de Management de la Qualité (SMQ) et le Système de Management de l'Environnement (SME), ce qui permet d'établir un lien fort entre ces systèmes de management dans le but de réaliser un Système de Management Intégré (SMI) de type QHSE.

Enfin, la proposition d'un système interactif et ergonomique d'aide à la décision pour le management préliminaire des risques présente un intérêt incontestable. Justement, dans le cadre du prochain chapitre, nous allons présenter SIGAR (Système Informatique Générique d'Analyse de Risque) qui se présente comme un outil générique dédié à la méthode MPR. La généricité de l'outil est due principalement à la généricité de la méthode. Cela le rend applicable dans différents domaines : ferroviaire pour lequel il a été initialement développé, manufacturier, machine, santé et sécurité au travail, industrie de process, épidémiologie, et bien d'autres.

5. Travaux cités

AQS-GT OORS. (Mars 1996). *Management de la sécurité d'entrepreise, vocabulaire et concept.* Association Qualité-Sécurité (AQS) pour l'Observatoire de l'Opinion sur les Risques de la Sécurité.

CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement.* CEI.

CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service.* CEI.

Directive 2001/16/EC. (19 mars 2001). *Directive of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 2004/49/EC. (29 avril 2004). *Directive of the European Parliament and of the Council on safety on the Community's railways.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 96/48/EC. (23 juillet 1996). *Directive of the European Parliament and of the Council on the interoperability of the trans-European high-speed rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

EN 292/ISO 12100. (1995). *Sécurité des machines ; Notions fondamentales, principes généraux de conception.* ISO/CEN.

FD X 50-173. (1998). *Principes, acteurs et bonnes pratiques - Guide d'auto-évaluation.* AFNOR.

Gallou, G., & Bouchon-Meunier, B. (1992). *Systémique : Théorie & Application.* France: Lavoisier.

Goffin, L. (1976). *Environnement et évolution des mentalités.* Arlon, Belgium: Thèse de doctorat, FUL.

GT Aspects sémantiques du risque. (1997). *Vocabulaire lié au risque à travers une analyse bibliographique.* Institut de Protection et de Sûreté Nucléaire (IPSN) - Observatoire de l'Opinion sur les Risques et la Sécurité.

HMSO. (1995). *A guide to Risk Assessment and Risk Management for Environmental Protection.* England: Her Majesty's Stationery Office.

INERIS-DRA ARAMIS. (2004). *ARAMIS: Développement d'une méthode intégrée d'analyse des risques pour la prévention des accidents majeurs.* Ministère de l'Ecologie et du Développement Durable - INERIS.

INERIS-DRA. (2003). *Outils d'analyse des risques générés par une installation industrielle.* INERIS, Direction des Risques Accidentels.

Larousse. (2006). 38 dictionnaires et recueils de correspondances en CD ROM.

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, M.-H., Aubry, J.-F., & El koursi, 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, 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.

NF EN 60204. (Avril 1998). *Sécurité des machines.* Paris: AFNOR.

Reason, J., & Parker, D. (1993). *Managing the human factor in road safety.* Maatschappij: The Hague: Shell International Petroleum.

Whittingham, R. (2004). *The Blame Machine: Why Human Error Causes Accidents.* Oxford: Elsevier Butterworth-Heinemann.

TABLE DES MATIÈRES DU CHAPITRE 7 : OUTIL D'AIDE À LA DÉCISION EN MATIÈRE DE MANAGEMENT DES RISQUES

Chapitre 7

OUTIL D'AIDE À LA DÉCISION EN MATIÈRE DE MANAGEMENT DES RISQUES

Les bases de données, constituées de fiches, ont fait couler beaucoup d'encre avant l'apparition des outils informatiques et l'émergence des techniques de capitalisation, pérennisation et exploitation des données grâce à des SGBD (Systèmes de Gestion de Bases de Données).

Néanmoins, la manipulation des SGBD est une tâche nécessitant la maîtrise de l'outil informatique et la connaissance d'un langage de requête permettant à l'utilisateur de formaliser ses besoins.

En effet, nous allons présenter dans ce 7éme et dernier chapitre l'outil SIGAR (Système Informatique Générique d'Aide à l'Analyse de Risque) dédié à la méthode MPR étudiée dans le cadre du chapitre précédent.

SIGAR est un outil interactif d'aide et d'assistance au management des risques. Il est doté d'une interface graphique (GUI : Graphical User Interface) conçue de façon à permettre aux utilisateurs de naviguer à travers ses menus graphiques interactifs et d'exprimer en langage habituel leurs besoins en informations et données via la saisie de formulaires sans solliciter directement le SGBD via le langage de requête approprié. Les données introduites sont par la suite récupérées et puis composées sous la forme d'une requête informatique

avant d'être soumises au SGBD. Enfin, les résultats retournés sont aussitôt récupérés et affichés de façon graphique agréable et ergonomique.

1 Besoin d'aide à la décision

Un des problèmes-clefs de l'informatique est qu'elle ne peut progresser qu'en améliorant ses "schèmes" de base (les formalismes). En effet, ceux-ci montrent souvent leurs limites dès qu'il s'agit de formaliser la complexité des problèmes que posent la représentation des connaissances et leur manipulation par des utilisateurs non expérimentés.

Le génie informatique et plus spécifiquement l'intelligence artificielle s'attache à construire des modèles « computationnels » du traitement de l'information avec comme objectif de les faire exécuter par un automate. La programmation consiste en effet à assembler, à partir d'un formalisme de base, les différents objets calculables dont elle a besoin pour représenter une connaissance donnée.

Selon Dillenbourg (Dillenbourg & Martin-Michielot, 1995): « Bien que l'IA ait été originellement conçue pour reproduire l'intelligence humaine, de la perspective des didacticiels, la qualité des techniques de l'IA n'est pas leur degré de fidélité psychologique mais la mesure dans laquelle elles permettent de mettre en œuvre des interactions intéressantes ». Il ajoute aussi que l'apport des techniques d'IA peut être résumé en la capacité du système de résoudre des problèmes que l'apprenant est sensé résoudre et son aptitude à conduire des interactions de type « apprenant – expert » avec l'utilisateur.

En effet, il existe plusieurs domaines d'application des techniques de l'IA, comme l'aide à la décision, le traitement des langues naturelles, la planification, l'apprentissage automatique, etc.

Les outils d'aide à la décision ont pris aujourd'hui une place essentielle dans différents domaines sociotechniques. Depuis la naissance des bases de données (BD) au milieu des années 60, les besoins et les solutions n'ont cessé de frayer les chemins de l'exigence et de l'innovation.

Les outils d'aide à la décision permettent d'apporter des réponses pertinentes à des problématiques diverses mettant en œuvre plusieurs choix possibles. Parmi les systèmes d'aide à la décision on trouve les EIS (Executive Information System) et les SIAD (Système Informatisé d'Aide à la Décision). L'EIS est un outil permettant d'organiser, d'analyser et de mettre en forme des indicateurs afin de constituer des tableaux de bord. Ce type d'outil, facile à utiliser, ne permet de manipuler que des requêtes préalablement modélisées par le concepteur. A l'inverse un SIAD a pour but de permettre la modélisation de représentations multidimensionnelles diverses et variées mais nécessite un apprentissage plus lourd.

2 Base de données, Système d'Information et Base de Connaissances

Une donnée est un fait brut, c'est la mesure d'une caractéristique tel qu'un son, un texte structuré ou non, une image, une vidéo, etc. Perpen (Perpen, 2000) ajoute qu'une donnée est dit brute car aucune interprétation ne lui a été attribuée.

Contrairement à une donnée, une information répond à un besoin, autrement dit, elle a une signification (valeur) dans un contexte précis (pertinence). Selon la norme qualité ISO 9000 (ISO 9000, Décembre 2000), une information est un « renseignement, documentation sur quelqu'un ou quelque chose » constituant, selon Bück (Bück, 1999), un « Elément de la connaissance susceptible d'être transmis et conservé grâce à un support ou un code ». L'information est donc un processus grâce auquel une organisation s'informe sur elle-même et sur son environnement et réciproquement.

La connaissance est la faculté de connaître grâce au savoir, à la science ou à l'expérience (Larousse, 2006). Elle provient du fait d'associer un ensemble d'information à un contexte d'utilité, ce qui la rend inséparable du sujet contrairement à l'information qui revêt un caractère éphémère, volatile et d'obsolescence rapide (Bück, 1999).

Gouriveau (Gouriveau, 2003) a tenté de situer le triptyque donnée/information/connaissance au sein du processus décisionnel (voir FIG. 1) :

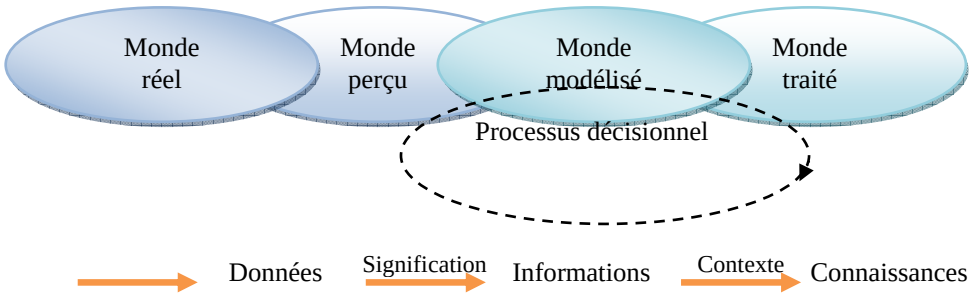


FIG. 1 : Données, informations, connaissances et processus décisionnel (Gouriveau, 2003)

Les connaissances peuvent être de natures diverses (Tourigny, 1998): certaines ou incomplètes, procédurales ou déclaratives, confidentielles ou non confidentielles, cohérentes ou contradictoires, quantitatives ou qualitatives, etc.

Les systèmes à base de connaissances ont plusieurs caractéristiques (Dankel & Gonzales, 1993):

- Ils utilisent les connaissances propres à un domaine pour résoudre des problèmes complexes.
- Ils font appel à un processus de résolution de nature heuristique plutôt qu'algorithmique.
- Ils présentent une séparation très nette entre les connaissances et les mécanismes de raisonnement utilisés tels que les moteurs d'inférence.
- Leur niveau d'expertise est au moins comparable aux meilleurs experts du domaine.

On peut assimiler une base de données à un réservoir commun partagé par des utilisateurs ayant des besoins différents en information. C'est un ensemble de données organisées de façon à servir plusieurs applications simultanément par une centralisation et une gestion qui donnent à l'utilisateur l'impression qu'elles se trouvent regroupées dans un seul endroit (Laudon & Laudon, 2001).

On peut aussi définir une base de données comme une entité dans laquelle il est possible de stocker des données de façon structurée et avec le moins de redondance possible. Ces données doivent pouvoir être utilisées par des programmes, et des utilisateurs différents.

Une base de données permet de mettre des données à la disposition d'utilisateurs pour une consultation, une saisie ou bien une mise à jour, tout en s'assurant des droits accordés à ces derniers. Cela est d'autant plus utile que les données informatiques sont de plus en plus nombreuses.

En effet, on parle généralement de Système d'Information (SI) pour désigner toute la structure regroupant les moyens mis en place pour pouvoir partager une masse importante de données. Un Système d'Information supporte les actions coordonnées visant à fournir, d'une manière proactive, la bonne information, au bon moment et à la bonne personne.

Cependant, il ne faut pas confondre base de données et base de connaissances. Une base de connaissance est une base de données stockant des questions, et éventuellement leurs réponses, au fur et à mesure qu'on les découvre. Un système à base de connaissance est une application capable d'effectuer dans un domaine des raisonnements logiques comparables à ceux que feraient des experts humains de ce domaine. Il s'appuie sur des bases de données de faits et de connaissances, ainsi que sur un moteur d'inférence, lui permettant de réaliser des inductions ou déductions logiques (chaînage avant et arrière). C'est avant tout un système d'aide à la décision (SIAD) qui sert à rassembler - de manière centralisée - l'expertise d'un domaine généralement formalisée de manière déclarative.

Un SGBD (Système de Gestion de Base de Données) est un ensemble de services essentiels dans un système d'information. Intuitivement, il permet à des utilisateurs concurrents de « *définir* » et de « *manipuler* » simultanément (insérer, modifier, supprimer et rechercher) les données contenues dans l'ensemble ou dans une partie autorisée des données.

Généralement, un SGBD offre des fonctionnalités indispensables qu'on peut résumer en 5 points:

1. Création des structure de données (table, classe d'objets) en précisant pour chaque champ le nom, le type, éventuellement si c'est une clé primaire et le cas échéant définir l'intégrité référentielle.
2. Saisie des données.
3. Exploitation de la base moyennant des fiches de consultation, fiches d'édition ou fiches de mise à jour.
4. Interrogation de la BD à l'aide d'un langage de requête tel que SQL (Structured Query Language). Une requête consiste à imposer des contraintes sur un ou plusieurs champs afin de connaître tous les enregistrements correspondants. Toutefois, même s'il est préférable de manipuler le langage SQL, il existe des outils tels que QBE (Query By Example) qui ne font appel à aucune connaissance particulière en langage de requêtes.
5. Affichage des résultats.

3 SIGAR : un outil d'aide au management préliminaire des risques

3.1 Objectifs et motivation

L'objectif principal de l'outil SIGAR est d'assister les évaluateurs dans la rédaction, la vérification et la mise à jour des dossiers de management des risques et entre autres les Analyses (Préliminaires) de Risque (Mazouni, Aubry, & El koursi, 2008).

Evidement, la proposition d'un système interactif et ergonomique d'aide à la décision pour l'évaluation de la sécurité des systèmes représente un intérêt incontestable. L'ergonomie de l'interface graphique (GUI) permet, entre autres, de contraindre les utilisateurs à utiliser un langage commun, d'éviter les copier/coller et reprises par habitude et de respecter les référentiels de sécurité.

Durant nos travaux de fin d'études d'ingénieur en informatique, nous avons développé un système d'aide graphique permettant de traduire les besoins exprimés par l'utilisateur en des requêtes écrites en un langage SQL. Ces requêtes sont ensuite communiquées par modules au moteur de requêtes, qui une fois qu'il les a exécutées retourne les résultats associés qui seront communiqués en un langage compréhensible à l'utilisateur (Mazouni & Hannachi, 1999). On peut donc s'inspirer de ces travaux pour définir une interface graphique adaptée aux besoins en matière de management des risques.

3.2 Choix technologiques

3.2.1 Visual Studio .NET 2005

Microsoft Visual Studio est une suite de logiciels de développement pour Windows conçu par Microsoft. Visual Studio est un ensemble complet d'outils de développement permettant de générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques et des applications mobiles (Horton, 2006). Visual C++ (Solter & Kleper, 2005), Visual Basic, Visual C# et Visual J# utilisent tous le même environnement de développement intégré (IDE, Integrated Development Environment), qui leur permet de partager des outils et facilite la création de solutions faisant appel à plusieurs langages. Par ailleurs, ces langages permettent de mieux tirer parti des fonctionnalités du Framework .NET, qui fournit un accès à des technologies clés simplifiant le développement d'applications.

Le noyau de Visual Studio .Net 2005 est basé sur la version 2 du Microsoft « Framework » (Sripriya & Kishore, 2002). Cette version apporte de nouveaux composants mais surtout de nouveaux « Namespaces », des nouvelles classes, de nouvelles fonctions, et une multitude de nouveautés ayant pour but de faciliter le développement.

Visual Studio intègre aussi une technologie de déploiement dite « ClickOnce » qui permet la mise à jour d'une application grâce à un simple lien hypertexte via un lien dans une page internet (intranet) ou même dans un mail, et le téléchargement de fichiers requis se fera alors systématiquement. Ainsi, l'administration d'un parc utilisant la même application est considérablement simplifiée.

3.2.2 Crystal Reports

Cristal Reports est un produit de « Business Objects » (acquise par SAP en Octobre 2007). C'est une application de « business intelligence » employée pour concevoir et générer des rapports à partir d'une quantité importante de données. Plusieurs autres applications, telles que Microsoft Visual Studio, empaquettent une version OEM de Cristal Reports comme outil d'usage universel de reportage.

Cristal Reports permet aux utilisateurs de faire une sélection de lignes et de colonnes spécifiques à partir d'une table de données compatibles (Microsoft SQL Server, Sybase, IBM DB2, Ingres, Microsoft Access, MySQL, Interbase et Oracle) (McAmis, 2004). Les utilisateurs peuvent alors positionner les données sur le rapport dans le format requis. Une fois que la disposition du rapport est complète elle est sauvegardée avec une extension .rpt. Un rapport peut être ré-exécuté en ré-ouvrant le dossier RPT et « en régénérant » les données. Si les données de base ont été mises à jour alors le rapport régénéré reflétera ces mises à jour. Le rapport peut être visionné sur l'écran, être imprimé préalablement sur le papier voire même exporté vers différents formats tels que MS Word (.doc, .tif) ou Excel, Acrobat Reader (.pdf), etc.

Les formats de rapport peuvent varier d'une colonne simple des valeurs aux dispositions comportant des graphes, des histogrammes, des tableaux synoptiques, des étiquettes et des sous rapports.

Cristal Reports peut aussi être lancé et contrôlé à partir d'un portail Internet. Business Objects a plusieurs produits de portails Internet : Business Objects Enterprise, Business Objects Crystal Decisions, Crystal Reports Server, etc.

Mis à part les bases de données, Crystal Reports supporte plusieurs autres sources de données, en l'occurrence : les tableurs (Microsoft Excel), Textes, les fichiers XML, les Groupwares (Lotus Notes, Microsoft Exchange et Novell GroupWise), et autres sources accessibles via le web service, ODBC, JDBC ou OLAP.

3.2.3 SQL Server 2005

SQL Server 2005 de son nom de code « Yukon » est un SGBDR (Système de Gestion de Bases de Données Relationnelles) de la plateforme Microsoft.

Pour les requêtes, SQL Server utilise T-SQL (Transact-SQL), il s'agit d'une implémentation de SQL qui prend en charge les procédures stockées et les déclencheurs (trigger).

Basé sur les points forts de son prédécesseur (SQL Server 2000), Yukon intègre beaucoup de nouvelles fonctionnalités à vocation productive :

- Créer et déployer des applications plus sûres, plus puissantes et plus fiables.
- Doter les développeurs d'un environnement de développement riche, souple et ergonomique.
- Partager des données entre diverses plates-formes, applications et systèmes.

- Faciliter les connexions locales et distantes aux bases de données.

SQL Server 2005 apporte aussi des changements significatifs concernant les points suivants:

- La montée en charge: Des améliorations comme le partitionnement, l'isolement des captures instantanées et la prise en charge des systèmes 64 bits, permettront de créer et de déployer les applications les plus exigeantes.
- Sécurité: Cryptage de base de données et choix de la sécurité maximale par défaut.
- Gestion: Une nouvelle suite d'outils de gestion de base de données et amélioration du Profiler SQL.
- Interopérabilité: Grâce à une prise en charge étendue des standards, des services Web et de Microsoft .NET Framework, SQL Server 2005 assure l'interopérabilité entre plates-formes, applications et systèmes.

D'un point de vue du développement, Yukon intègre également des nouveautés:

- Amélioration des outils: L'intégration avec l'outil de développement Visual Studio permettra un développement et un débogage plus efficaces des applications métier et décisionnelles.
- Intégration de la CLR (Common Language Runtime) dans le moteur de base de données: Les développeurs auront la possibilité de choisir parmi plusieurs langage (C++, C#, VB.NET, Transact-SQL, etc.) en vue de développer leurs applications de base de données.
- Support du XML.
- Support des Web Services: La prise en charge de standards ouverts, existants ou nouveaux, tels que HTTP (Hypertext Transfer Protocol), XML, SOAP (Simple Object Access Protocol).

3.3 Propriétés de SIGAR

L'architecture de SIGAR comprend les trois niveaux physique, conceptuel et opérationnel, conformément au standard ANSI/SPARC. Ceci permet d'avoir une indépendance entre les données et les traitements.

En effet, SIGAR est conçu conformément aux exigences suivantes :

- Indépendance physique : le niveau physique peut être modifié indépendamment du niveau conceptuel. Cela signifie que tous les aspects matériels de la base de données n'apparaissent pas pour l'utilisateur, il s'agit simplement d'une structure transparente de représentation des informations.
- Indépendance logique : le niveau conceptuel doit pouvoir être modifie sans remettre en cause le niveau physique, c'est-a-dire que l'administrateur de l'outil doit pouvoir faire évoluer la BD sans que cela ne gêne les utilisateurs.
- Manipulabilité : les personnes ne connaissant pas la base de données doivent être capables de décrire leur requête sans faire référence à des éléments techniques de la base de données.
- Rapidité des accès : l'outil doit pouvoir fournir des réponses rapides aux requêtes, cela implique des algorithmes optimisés de fouille de données.

- Administration centralisée : l'outil doit permettre de façon centralisée aux utilisateurs de pouvoir manipuler les données, insérer de nouveaux éléments, vérifier l'intégrité de l'ensemble de données, etc.
- Limitation de la redondance : l'outil doit pouvoir éviter dans la mesure du possible des informations redondantes, afin de préserver la cohérence et optimiser l'exploitation des ressources.
- Vérification de l'intégrité : les données doivent être cohérentes entre elles, de plus lorsque des éléments font référence à d'autres, ces derniers doivent être présents.
- Partageabilité des données : l'outil doit permettre l'accès simultané à la base de données par plusieurs utilisateurs.
- Sécurité des données : l'outil doit être doté de mécanismes permettant de gérer les droits d'accès aux données selon les profils d'utilisateur.

3.4 Définition des données

Avant toute étude concernant les applications et les systèmes de base de données, nous avons besoin d'une notation qui permet de comprendre la structure de données d'une application, soit le schéma de données.

Il existe dans une base de données deux types d'informations : les données et le schéma de données. Un schéma de données décrit la structure des données. En effet, un SGBD possède des contraintes sur les données et le schéma adopté.

L'intégrité référentielle est un ensemble de contraintes sur les clés étrangères utilisées dans la base de données. En effet, SQL Server permet de vérifier la validité de ces contraintes, autrement dit, à l'issue de l'attribution d'une valeur à un attribut défini comme clé étrangère, le SGBD doit s'assurer que l'enregistrement possédant la clé primaire correspondante fait partie de la table référencée. Ainsi, après la suppression d'un enregistrement contenant une clé primaire, le SGBD vérifie que cette dernière n'existe plus en tant que clé étrangère.

Mis à part les tables stockées, on peut exploiter des vues. Une vue est une table relationnelle définie en terme de langage de requête. Un autre usage des vues relationnelles est également possible, c'est de définir un sous-ensemble d'une table sur laquelle des utilisateurs particuliers ont l'autorisation de lire, d'écrire ou de faire des mises à jour.

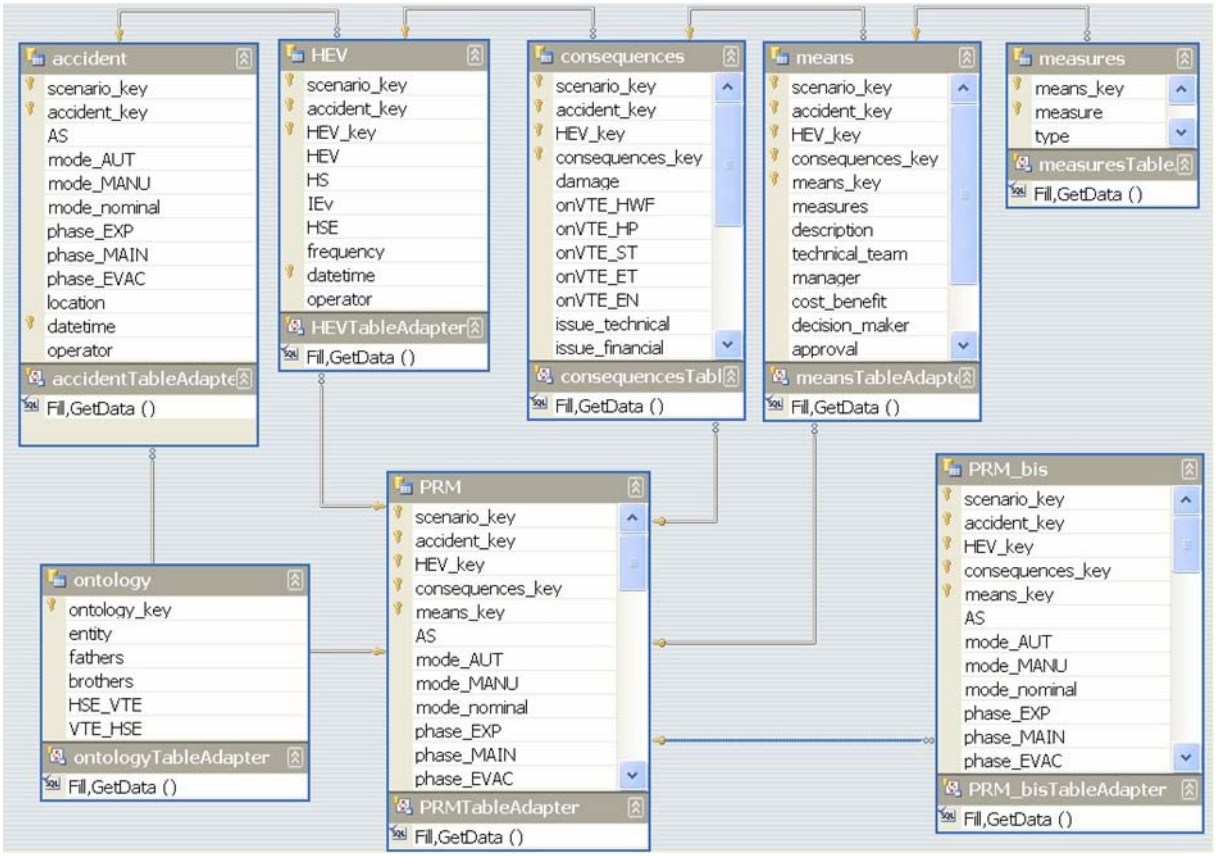


FIG. 2: Modèle de données de la base de données SIAD

L'outil SIGAR est organisé autours de la base de données SIAD. Le modèle de données de cette base de données est présenté dans la figure 2 (FIG. 2).

En réalité, SIAD est un entrepôt de données diversifiées et hétérogènes, mais à travers les fonctionnalités Visual Studio d'extraction, de transformation et de chargement de données, on peut travailler sur une partie restreinte des données, autrement dit, un cube de données (data cube) nommé SIADDataSet.

Le modèle de données adopté 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.

Le choix des types des attributs de chaque table est arrêté en vue de réduire au maximum les interventions de l'opérateur. Par exemple, les informations relatives à la date et au nom d'opérateur sont systématiquement capitalisées via la création et l'association des déclencheurs (triggers) aux tables.

La table « PRM_bis » est la table de travail sur laquelle l'opérateur effectue ses opérations d'édition. On peut dire qu'elle représente la version finale de l'étude. Tandis que la table « PRM » se présente comme l'entrepôt de données historiques et actualisées. Ainsi, on peut consulter le tracé historique d'un scénario donné, autrement dit, retrouver les différents changements dont il a fait l'objet, les dates et heures des interventions à la seconde prés, les opérateurs intervenants, etc.

Néanmoins, la table « PRM » est complètement transparente à travers l'interface graphique et ne peut être consultée voire modifiée qu'à travers l'administration de la base de données SIAD en utilisant les services SQL Server à l'image de SQL Server Management Studio (SMSS) ou la console de requête.

Les relations qui existent entre les différentes tables sont utilisées, entre autre, pour modifier ou supprimer, en cascade, des enregistrements liés.

Il convient de préciser qu'un scénario d'accident est une concaténation des informations liées aux caractéristiques de l'accident (type, mode de fonctionnement, phase, etc.), des informations relatives à l'espace de danger (situation de danger, événement initiateur, Entité Source de Danger, etc.), des informations liées à l'espace de vulnérabilité (les dommages, les Entités Cibles de Danger, la gravité, etc.). On peut ajouter à cette chaîne les moyens de maîtrise des risques (les mesures de réduction du risque, les coûts et les bénéfices, aspects organisationnels de la mise en œuvre des mesures envisagées).

Par conséquent, les tables « accident, HEV, conséquences et means » sont reliées à travers une cascade de clés étrangères. La clé primaire de la table accident est référencée dans la table HEV dont la clé est référencée dans la table conséquences dont la clé est référencée dans la table means.

3.5 Présentation de l'interface graphique utilisateur(GUI)

L'interface graphique de SIGAR (voir FIG. 3) contient plusieurs menus interactifs :

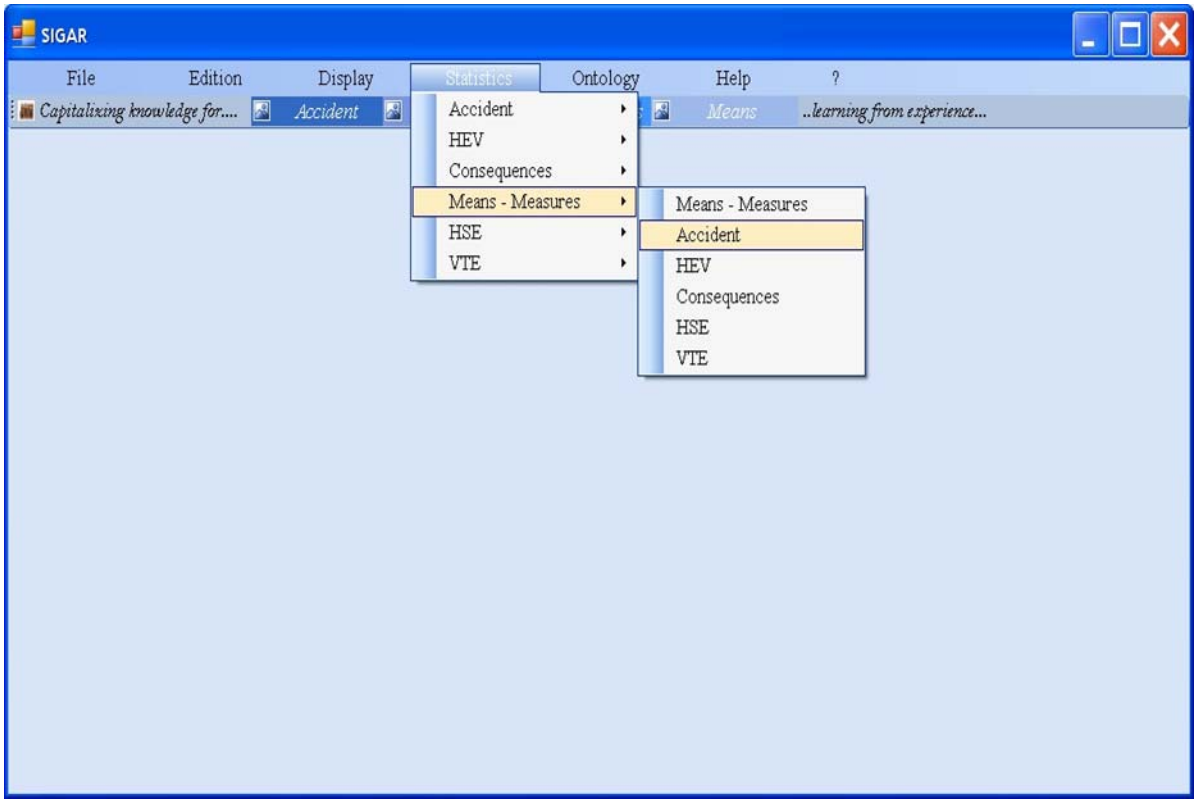


FIG. 3 : Interface graphique principale de SIGAR

- L'option « File » permet d'ouvrir ou de fermer un dossier de management des risques et aussi de quitter l'application.
- L'option « Edition » permet d'insérer, de supprimer ou de mettre à jour les données.
- L'option « Display » est relatif au « reporting ».
- L'option « Statistics » permet de réaliser des statistiques sur les scénarios d'accidents.
- L'option « Ontology » mène vers une interface de saisie des entités en fonction du découpage systémique du système global. Chaque entité est enrichie en fonction de ses associations de type (entité source de danger, entité cible de danger) décelées à partir des nouveaux scénarios.
- L'option « Help » contient une aide synthétique pouvant assister l'opérateur.
- Enfin, la ligne « Capitalising knowledge for learning from experience » sert à réaliser un retour d'expérience sur les composantes du scénario d'accident.

3.6 Manipulation des données

3.6.1 Opérations algébriques et SQL

Un langage de requête relationnel permet au moins la sélection, la projection et la jointure de données :

- La sélection produit un ensemble de lignes de la table
- La projection a pour résultat un sous-ensemble de colonnes de la table
- La jointure met en relation les enregistrements de différentes tables dont les attributs spécifiés possèdent des valeurs égales ou comparables

La manipulation de données fait appel au langage algébrique. Dans ce type de langage c'est l'utilisateur qui doit préparer sa séquence d'opérations pour qu'il puisse interroger la base (Dellobel & Adiba, 1985). L'expression d'un besoin se fait à l'aide d'opérations binaires et unaires dont les opérandes sont les relations de la base de données (voir FIG. 4).

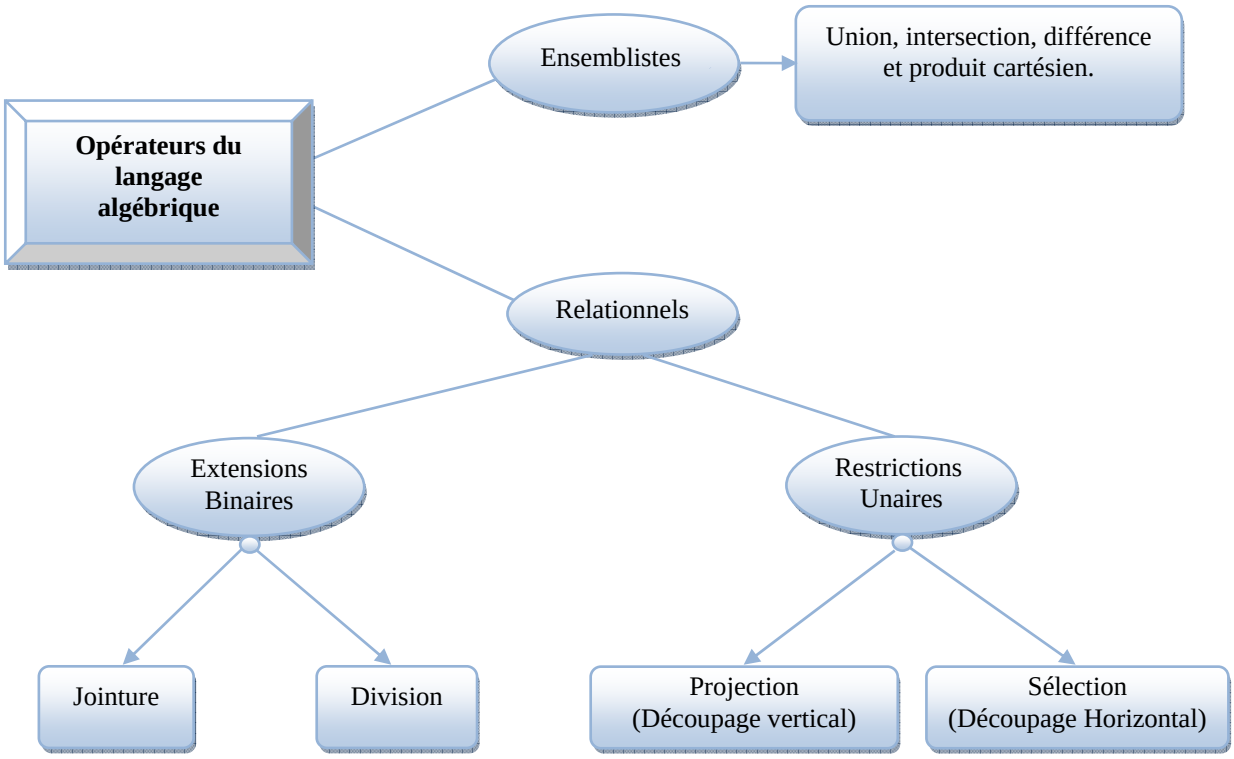


FIG. 4: Opérateurs du langage algébrique

3.6.1.1 Produit cartésien

Etant donné deux relations R(X) et S(Y) où les constituants X et Y sont disjoints, le produit cartésien de R par S, noté R x S est une relation définie par : R x S = R * S.

Dans le cas ou les relations R et S auraient les constituants non-disjoints, il est toujours possible de se ramener à l'hypothèse des constituants disjoints en renommant les doublures ou en conservant les domaines (Gardarin, 1998).

3.6.1.2 Union et intersection

Etant donné deux relations R(X) et S(X) où les constituants de R et S sont identiques et définis sur les mêmes domaines. L'union ($\cup$) et l'intersection ($\cap$) de R et S seront définie respectivement par : $R \cup S = R + S$ et $R \cap S = R * S$.

Dans le cas où les relations R et S n'ont pas la même liste de constituants, on dira qu'elles sont compatibles s'il existe une bijection entre les constituants de R et les constituants de S telle que les constituants en correspondance dans la bijection aient le même domaine (Gardarin, 1998).

3.6.1.3 Complément d'une relation

Le complément d'une relation R(X) notée $\neg$ R(X) sera défini par son prédicat : $||\neg R(X)|| = \neg||R(X)||$, où le symbole $\neg$ représente la négation logique. Le complément possède, par rapport à l'addition et au produit, les propriétés suivantes :

$\neg$ (R+S)(X$\cup$Y) = ($\neg$R * $\neg$ S)(X$\cup$Y).

$\neg$ (R*S)(X$\cup$Y) = ($\neg$R + $\neg$ S)(X$\cup$Y).

3.6.1.4 Différence

Etant donné deux relations R(X) et S(X) telles que les domaines associés aux constituants de la liste X de R soient identiques à ceux de la liste S.

On définira la différence de R moins S, notée R – S par son prédicat :

||(R – S)(X)|| = ||R(X)|| $\wedge$ $\neg$||S(X)||, ceci amène à : R – S = R * $\neg$S.

3.6.1.5 Projection

Soit R(X, Y) une relation où l'on a distingué le constituant X du constituant Y. La projection sur Y de cette relation au constituant Y noté R(X, Y) [Y] définie par son prédicat :

||R(X,Y)[Y]|| = $\exists$ a ||R(a,Y)||.

La projection R(X, Y)[Y] est une opération de découpage verticale de la relation R(X,Y) sur le constituant Y.

3.6.1.6 Division

La division d'une relation R(X, Y) par S(Y), notée R $\div$ S, est une relation définie sur le constituant X par le prédicat : ||R $\div$ S(X)|| = $\forall$ y $\in$S(Y) ||R(X,y)||.

3.6.1.7 Sélection

L'opération de sélection consiste à sélectionner dans une relation les n-uplets (lignes) qui satisferont à une propriété donnée. Pour exprimer cette propriété, on utilise une formule logique construite à partir des connectives de la logique.

Pour définir une expression de sélection, on partira de la notion de formule atomique dont la structure sera : (nom du constituant θ nom du constituant) ou bien (nom du constituant θ constante), où θ désigne un des opérateurs de comparaison. Une expression de sélection obéit aux règles de construction suivantes (Dellobel & Adiba, 1985)(Gardarin, 1998):

- Une formule atomique est une expression de sélection.
- Si E1 et E2 sont deux expressions de sélection, alors E1 $\vee$ E2, E1 $\wedge$ E2 et $\neg$E1 sont des expressions de sélection.
- Si E1 est une expression de sélection, (E1) est une expression de sélection.
- On désignera par « R : E » l'opération de sélection sur R suivant l'expression E. Ceci peut être défini par le prédicat : ||R : E(X)|| = || R(X)|| $\wedge$ E(X).

3.6.1.8 θ-jointure

Etant donné deux relations R(X1,X2,…….,Xn) et T(Y1,Y2,……..,Yk) tel que domaine(X1) = domaine(Y2) ; On définira la θ-jointure de R par T, noté R * (X1 θ Y1)T où θ représente un opérateur de comparaison comme étant une relation définie sur: (X1,X2,…….,Xn,Y1,Y2,……..,Yk) par le prédicat :

$$||(R * (X1\ \theta\ Y1)\ T)\ (X1,X2,\ldots\ldots,Xn,\ Y1,Y2,\ldots\ldots..,Yk)|| = ||R(X1,X2,\ldots\ldots,Xn)|| \wedge$$
$$||T(Y1,Y2,\ldots\ldots..,Yk\ )|| \wedge (\ X1\ \theta\ Y1).$$

Compte tenu de la définition de l'opérateur de produit cartésien et de la sélection, on peut remarquer que : R * (X1 θ Y1) T = (R x T) : X1 θ Y1. Cette équation exprime le fait que la θ-jointure peut être obtenue en effectuant d'abord un produit cartésien suivi d'une sélection (Gardarin, 1998)**.**

3.6.2 Opérations transactionnelles et SQL Server-Transact

SQL Server est un SGBD transactionnel capable de préparer des modifications sur les données d'une base et de les valider ou de les annuler d'un bloc. Ceci garantit l'intégrité des informations stockées dans la base.

Lors d'une transaction, les blocs de données contenant les lignes de données modifiées par cette transaction sont verrouillés. Les autres utilisateurs, en fonction du niveau d'isolation choisi, doivent attendre ou non la fin de la transaction pour pouvoir les modifier à nouveau.

Les verrouillages s'effectuent au niveau des lignes, pages, extensions, tables ou base de données. SQL Server ne verrouille que les ressources dont il a besoin (par défaut les enregistrements) et en fonction des besoins peut verrouiller à un niveau plus élevé (pages ou objet). Ceci évite aux utilisateurs d'attendre la fin d'une transaction pour mettre à jour des lignes de données qui n'ont pas été touchées par une modification et permet de diminuer la quantité de ressources consommées.

3.6.3 Edition (ajout, suppression, mise à jour)

Le menu « Edition » permet de visualiser le contenu des tables accident, HEV, consequences ou means et aussi de lancer l'interface d'édition des scénarios d'accident (voir FIG. 5).

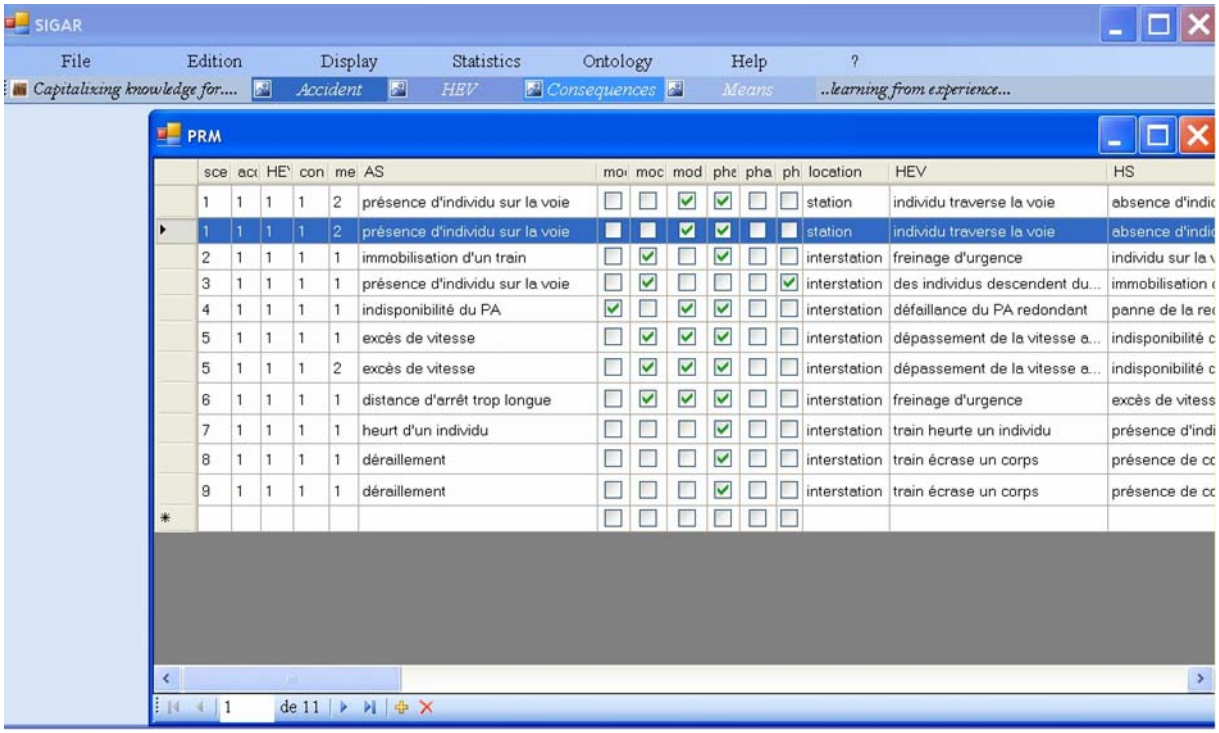


FIG. 5: Interface d'affichage et d'édition de la table PRM_bis

L'extraction des données s'effectue à travers des sélections sur les tables correspondantes. Les résultats affichés dans une forme tabulaire peuvent être triés en fonction d'une colonne donnée. Cependant, les opérations d'édition, de recherche ou d'accès rapide à une ligne s'effectuent à travers le « Binding Navigator ».

3.6.4 Affichage et impression

Le menu « Display » permet de générer automatiquement des rapports d'étude en se basant sur la richesse et la puissance de Cristal Reports en la matière. En effet, hormis la présentation ergonomique et les fonctions de base d'édition et d'impression d'un rapport, Cristal Reports offre des fonctionnalités très avancées de fouille de données.

Date et heure d'impression: jeudi 11 septembre 2008 12 h 24

MPR MHM-JFA-08

MAZOUNNocaladmin

AS	HEV	HS	IEv	HSE	VTE	ES	EEv	frequency	damage	severity	measures	descriptio
présence d'individu sur la voie	individu traverse la voie	absence d'indication sur les arrivées	panne de l'écran des arrivées	écran d'affichage des arrivées	personne autorisée (client)	précipitation pour rattraper le train	train aperçu à l'approche vers le quai opposé	O4	RAS	S1	Prévention	Installation des portes palières
présence d'individu sur la voie	individu traverse la voie	absence d'indication sur les arrivées	panne de l'écran des arrivées	écran d'affichage des arrivées	personne autorisée (client)	précipitation pour rattraper le train	train aperçu à l'approche vers le quai opposé	O4	RAS	S1	Prévention	Installation des portes palières
présence d'individu sur la voie	individu traverse la voie	absence d'indication sur les arrivées	panne de l'écran des arrivées	écran d'affichage des arrivées	personne autorisée (client)	précipitation pour rattraper le train	train aperçu à l'approche vers le quai opposé	O4	RAS	S1	Prévention	Installation des portes palières
...e	individu	absence	panne de	écran	personne	précipita	train	O4	RAS	S1	Protectio	Actionne

FIG. 6: Génération automatique d'un document d'APR

Les rapports sont directement extraits de la base de données et peuvent être sauvegardés sous le format original de Cristal Reports (.rpt), voire même exportés vers plusieurs formats tels qu'Acrobat Reader (.pdf), Microsoft Word (.rtf, .doc), Microsoft Excel (.xls), etc.

La figure 6 (FIG. 6) est une copie d'écran d'un document d'Analyse Préliminaire des Risques généré automatiquement à partir de SIGAR et exporté vers un format MS Word.

3.6.5 Statistiques et Traitement de données

Le menu « Statistics » regroupe plusieurs possibilités de traitement des corrélations entre les différentes composantes du scénario d'accident. Ainsi, on peut connaître, par exemple, l'impact d'un accident sur une Entité Cible de Danger donnée (voir FIG. 7) voire même observer la répartition des conséquences en fonction de l'Entité Source de Danger, etc.

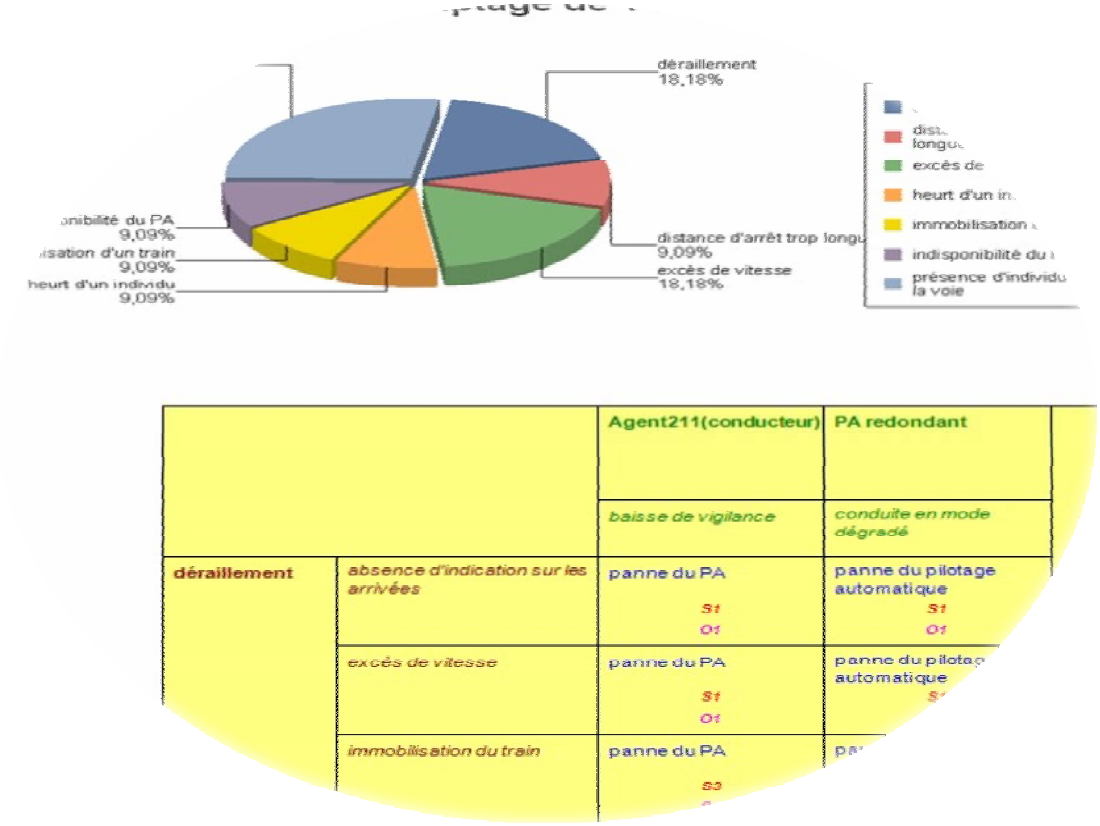


FIG. 7: Copie d'écran de statistiques générées automatiquement

3.7 Retour d'expérience

SIGAR propose quatre possibilités de retour d'expérience :

- REX sur les accidents (bouton accident) (voir FIG. 8).
- REX sur les espaces de danger (bouton HEV).
- REX sur les espaces de vulnérabilité (bouton Consequences).
- REX sur la maîtrise des risques (bouton Means).

Chaque bouton sert à capitaliser les données en cours de manipulation afin de servir au REX. Par exemple, en cas d'hésitation sur l'évaluation de la gravité d'un scénario d'accident, on peut actionner le bouton « consequences » qui affiche une table regroupant les conséquences de l'ensemble des études passées après avoir lancé l'ajout de la partie conséquence du scénario en question. Par conséquent, on peut trier les résultats en fonction des dommages, des cibles ou des indexes d'accident afin d'identifier les similarités permettant de fixer la gravité sollicitée.

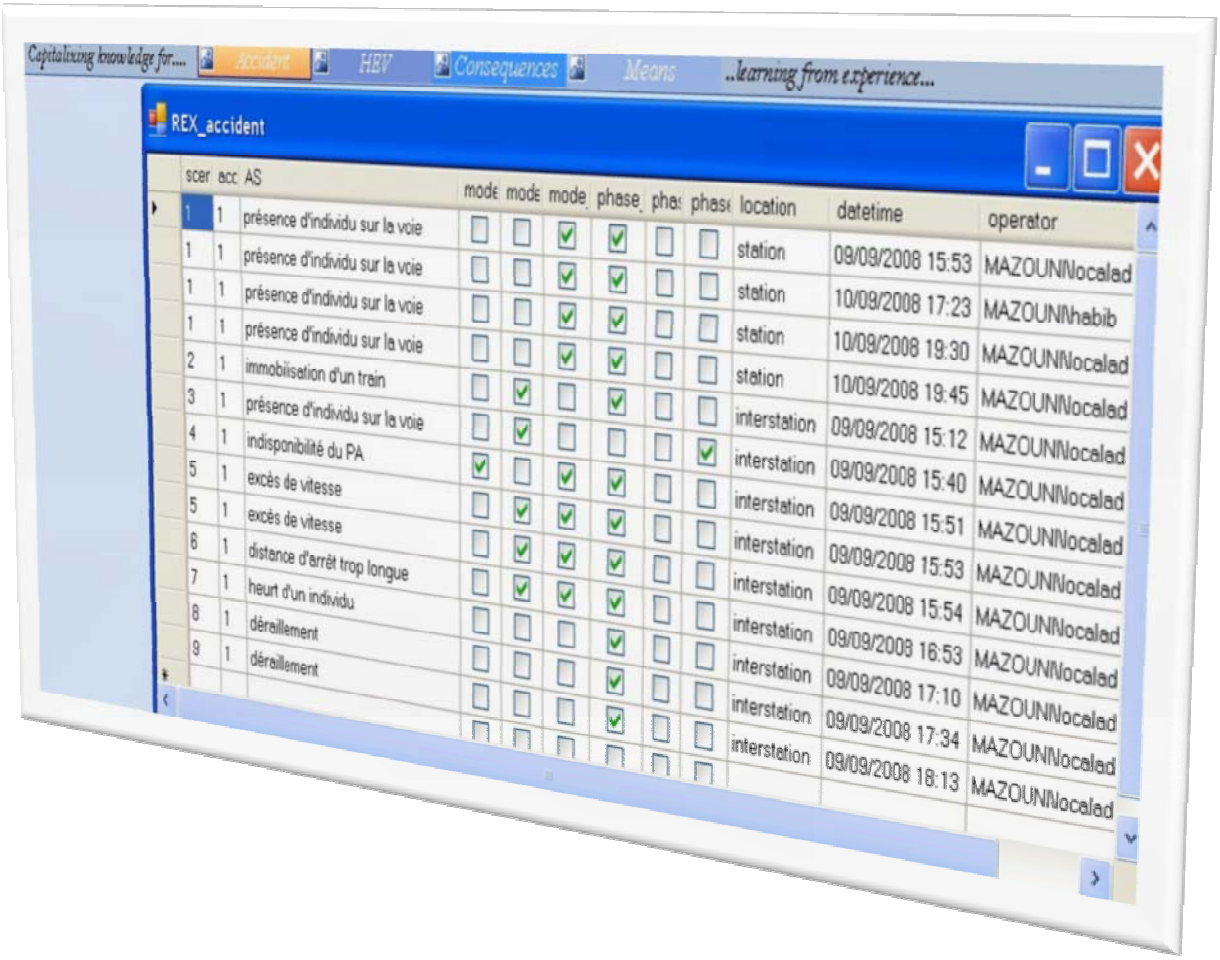


FIG. 8: Interface du REX sur les accidents

3.8 Fonctionnalités avancées

3.8.1 Gestion des droits d'accès

Les services exécutant chaque instance de SQL Server utilisent un compte de service. Ce dernier doit être choisi avec soin pour éviter d'éventuelles failles de sécurités sur le serveur. Celui-ci peut être : Service Système, Service Local, Service Réseau, compte utilisateur Windows local, compte utilisateur du domaine.

SQL Server s'appuie par défaut sur le système d'authentification de Windows. On peut donner des droits sur les différents éléments de SQL Server à un groupe ou à un utilisateur.

Lors de la connexion à la base de données, l'utilisateur est identifié grâce à son login Windows et accède aux ressources de la base de données auxquelles l'administrateur lui a donné droit par l'intermédiaire de son groupe Windows ou directement à son identifiant.

Les droits sur les bases de données sont donnés par l'intermédiaire de rôle de base de données, de groupes Windows ou directement à l'utilisateur. Il existe des rôles de bases de données système qui donnent des droits spécifiques sur la base de données et d'autres définis par l'administrateur qui donnent des droits sur les objets.

Il existe au niveau des bases de données des rôles applicatifs auxquels on peut affecter des droits et accessibles par mot de passe. Lorsqu'ils sont utilisés ils remplacent les droits de l'utilisateur courant par les droits affectés au rôle. Ils sont utilisés pour interdire l'accès aux utilisateurs à une base de données par d'autres moyens que l'application qui leur est fournie.

3.8.2 Historique des accès

Les transactions sont enregistrées dans le journal de transaction et les modifications des données sont intégrées à la base de données lors de points de contrôle (check point). Il est possible de forcer un point de contrôle grâce à l'instruction « CHECKPOINT ».

Le journal des transactions peut être conservé de trois manières différentes :

- Mode simple : toutes les modifications sont enregistrées dans le journal sauf pour les instructions de chargement en bloc telles que CREATE INDEX, SELECT INTO etc. Les transactions terminées sont supprimées du journal de transaction au prochain point de contrôle.
- Mode journalisé en bloc : Idem que le mode simple, sauf que les transactions terminées dont les données sont écrites sur le disque sont supprimées du journal de transaction à chaque sauvegarde de celui-ci.
- Mode complet : Idem que le mode journalisé, mais dans ce mode toutes les modifications sont enregistrées dans le journal.

Dans les 2 derniers modes, il est possible de sauvegarder la base de données et de la restaurer en précisant le temps ciblé à la seconde près ou bien en se référant à l'instant précédant une transaction donnée.

3.8.3 Busines Intelligence

«SQL Server Business Intelligence Development Studio» est l'outil de développement Microsoft Visual Studio 2005 adapté pour la création de projets « Analysis Services, Integration Services ou Reporting Services ». Tous ces projets se retrouvent dans le groupe « Projets Business Intelligence ».

« SQL Server Management Studio (SSMS) » est un outil qui permet de se connecter et d'administrer les différents moteurs SQL Server 2005. Il permet pour le moteur relationnel de développer des scripts Transact-SQL, avec la possibilité de regrouper l'ensemble de ceux-ci au sein d'une solution (comme sous Visual Studio).

« Notification Services » permet de requêter régulièrement la base de données et en fonction de ces requêtes de notifier des groupes abonnés à ces évènements.

« Analysis Services » permet de générer des cubes OLAP, données agrégées et multidimensionnelles. Il permet également d'implémenter des algorithmes de Data Mining.

« Reporting Services » est un moteur de génération d'états. Deux services web le composent, l'un permettant son administration, l'autre la génération, l'abonnement, le rendu des rapports. Les rendus se font sous Excel, PDF et HTML.

« Integration Services » est un outil d'ETL (Extracting, Transforming and Loading) très puissant qui se présente comme une plate-forme complète d'intégration de données. SSIS peut être utilisé pour réaliser des

opérations de maintenance de base de données ou de transfert de données à partir des textes Word ou des tableaux Excel classiques vers une base de données. En effet, SSIS est d'un grand intérêt dans le cas de notre étude, car l'ensemble des documents d'Analyse de risques à commencer par l'APR existent sous l'une de ces deux formats de MS office.

4 Conclusion

SIGAR se présente comme un outil générique applicable dans différents domaines : ferroviaire auquel il a été initialement dédié, manufacturier, machine, professionnel, process, épidémiologie, et bien d'autres.

Cette généricité est due au fait que la méthode MPR (voir chapitre 6) est basée conjointement sur une approche systémique et une modélisation ontologique des scénarios d'accident.

Rappelons que l'originalité de cette ontologie (voir Chapitre 5) provient du fait que chaque concept est abordé selon son aspect sémantique mais aussi en fonction de sa contribution dans la réalisation du scénario d'accident selon un processus accidentel générique.

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. En effet, étant donné que 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 BD SIAD et aussi l'intégration directe de nouvelles fonctionnalités dans SIGAR.

5 Travaux cités

Bück, J.-Y. (1999). *Le management des connaissances: mettre en oeuvre un projet de knowledge management.* Paris: Editions d'Organisation.

Dankel, A., & Gonzales, D. (1993). *The enginneering of knowledge-based systems, theory and practice.* New Jersey: Prentice Hall, Englewood Cliffs.

Dellobel, C., & Adiba, M. (1985). *Base de données et systèmes relationnels.* Dunod.

Dillenbourg, P., & Martin-Michielot, S. (1995). *Le rôle des techniques d'Intelligence artificielle dans les logiciels de formation.* CBT, Learntec.

Gardarin, G. (1998). *Bases de données: les systèmes et leurs langages.* Eyrolles.

Gouriveau, R. (2003). *Analyse des risques – Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision.* Thèse de Doctorat, Institut National Polytechnique de Toulouse.

Horton, I. (2006). *Beginning Visual C++ 2005.* USA: Wiley Publishing Inc. .

ISO 9000. (Décembre 2000). *Systèmes de Management de la Qualité - Principes essentiels et vocabulaire.* ISO.

Larousse. (2006). 38 dictionnaires et recueils de correspondances en CD ROM.

Laudon, K., & Laudon, J. (2001). *Les systèmes d'information de gestion : organisations et réseaux stratégiques.* Editions du Renouveau Pédagogique.

Mazouni, M.-H., & Hannachi, H. (1999). *Réalisation d'une interface graphique sous XWindow pour le SGBD Postgres. Mémoire d'ingénieur d'état en informatique, option Systèmes Informatiques* . Alger: Institut National d'Informatique.

Mazouni, M.-H., Aubry, J.-F., & El koursi, 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.

McAmis, D. (2004). *Professional Crystal Reports for Visual Studio .NET. Second edition.* Indianapolis - USA: Wiley Publishing, Inc.

Perpen, J.-L. (2000). *Définition et réalisation d'une application orientée objet pour la maîtrise du processus de coupe - Thése de Doctorat en mécanique.* Université Bordeaux I.

Solter, N., & Kleper, S. (2005). *Professional C++*. USA: Wiley Publishing, Inc.

Sripriya, & Kishore, S. (2002). *Microsoft Visual C++ .NET Professional Projects.* USA: Premier Press, Inc.

Tourigny, N. (1998). *Systèmes d'aide à l'étude de la sécurité routière - Vers des outils hybrides, ouverts et intelligents* .

CONCLUSION GÉNÉRALE

Nous avons commencé par clarifier les fondements de la sécurité, d'abord en la définissant par rapport au danger et au risque et ensuite en la confrontant aux autres composantes de la sûreté de fonctionnement. Par conséquent, nous avons passé en revue le concept de risque et ses corollaires tels que danger, phénomène dangereux, conséquence, dommage, gravité, fréquence d'occurrence, en les regroupant selon les liens sémantiques qui puissent exister entre eux. En outre, nous avons abordé les différentes facettes du risque, autrement dit, son concept, sa perception, sa prise, sa classification, son acceptabilité et ses différences avec d'autres concepts tels que gravité, probabilité d'occurrence, incertitude, etc.

En effet, après avoir cadré le concept de sécurité, nous avons abordé l'essentiel des activités relatives à la sécurité en commençant par le management des risques et son processus général qui contient justement, entre entres, l'analyse de risque.

Nous avons essayé de mieux situer la notion d'analyse de risque par rapport aux autres activités du management des risques. Nous avons d'abord clarifié le lien indissociable entre ces deux notions à travers de nombreuses définitions issues principalement des normes et parfois des travaux de groupes de recherche. Ensuite, nous avons présenté rapidement les principales méthodes d'analyse de risque avant d'y revenir en détail en Annexe 1.

Après avoir essayé de discerner les points forts et points faibles de ces méthodes d'analyse de risque, nous avons trouvé intéressant de pouvoir les comparer les unes aux autres, et proposer ensuite des critères de choix de la méthode la plus convenable à une étude donnée, et enfin nous avons proposé un certain nombre de critères d'évaluation de la qualité d'une analyse de risque.

Nous sommes revenus ensuite avec plus de détail à l'APR afin de comprendre pourquoi cette analyse pose le plus de problèmes au management des risques étant donné qu'elle demeure diversement perçue et qu'elle ne fait l'objet ni d'une norme ni d'un consensus entre spécialistes !

Nous avons essayé par la suite de déceler les problèmes pénalisant la pratique du management des risques et plus particulièrement l'APR. Nous avons regroupé les différents problèmes en 10 enjeux principaux tels que l'enjeu d'harmonisation, d'intégrabilité, d'interopérabilité, d'identification des effets domino, etc.

Ensuite, tout au long du reste de ce mémoire, nous avons tenté d'apporter des solutions méthodologiques, techniques et informatiques afin de résoudre les problèmes suscités. Ainsi l'ontologie proposée dans le cadre du cinquième chapitre peut être considérée comme une passerelle permettant d'harmoniser la terminologie et la sémantique de l'accident à travers le processus accidentel ontologique proposé.

Cette ontologie permet, entre autres, de modéliser le transfert de danger entre entités sources et cibles, et ce quelque soit leur niveau hiérarchique dans le système global. Elle permet aussi de poser un cadre propice à

l’identification des effets domino. Chose que nous avons illustrée à travers la modélisation d’une vingtaine de scénarios d’accident issus de différents domaines, dont 9 scénarios d’accident ferroviaires que nous avons liés par la suite dans un scénario complexe à effets domino.

Usuellement, l’APR ne se limite pas à la phase d’analyse des risques, mais elle fournit en sortie des mesures de maitrise des risques, ce qui fait d’elle une méthode de management des risques !

En effet, nous avons proposé la méthode « Management Préliminaire des Risques (MPR) » sous une forme itérative, ce qui assure plus de complétude et de cohérence et permet à la méthode de trouver des points d’ancrage dans le cycle de vie du système pour accompagner son développement de la phase de spécification à la phase de démantèlement.

La démarche MPR est parfaitement compatible avec le SMS ainsi qu’avec le SMQ et le SME, ce qui permet d’établir un lien fort entre ces systèmes de management dans le but de réaliser un Système de Management Intégré (SMI) de type QHSE.

Le développement de SIGAR a pour but de consolider la méthode MPR. La généricité de l’outil est due principalement à la généricité de la méthode. Cela le rend applicable dans différents domaines : ferroviaire pour lequel il a été initialement développé, manufacturier, machine, santé et sécurité au travail, industrie de process, épidémiologie, et bien d’autres.

En effet, la proposition d'un système interactif et ergonomique d’aide à la décision pour le management préliminaire des risques présente un intérêt incontestable.

L'ergonomie de l’interface graphique permet, entre autres, de contraindre les experts à respecter les référentiels de sécurité, d’utiliser un langage commun, et d’éviter les copier/coller et reprises par habitude.

Désormais, après avoir été guidé tout le long de la saisie de données, l’opérateur peut générer automatiquement des documents de management des risques, des statistiques ou des diagrammes. Il peut aussi faire des recherches avancées ou enregistrer ses documents dans la plupart des formats standards (word, excel, pdf, xml, etc.) et préserver une meilleure traçabilité via un échange rapide et efficace avec d’autres personnes concernées par son étude, à travers aussi les fichiers ‘releases’ comportant un listing des derniers changements, leur auteur, date, etc.

Enfin, dans sa course de survie vers la continuité et la pérennité, l’industriel emploie tous les moyens pour préserver son savoir faire et entre autres ses réservoirs de données, de tout accès non autorisé provenant de l’extérieur comme de l’intérieur de son organisation. Ces données se trouvent, en général, dans des fichiers textes ou sur des supports papiers ordinaires, et dans les deux cas sont vulnérables. Donc, afin de renforcer l’intégrité et la confidentialité des données, SIGAR permet de faire des échanges cryptés avec des fichiers de base de données qui ne peuvent être exploités qu’à travers l’outil, éventuellement moyennant des verrous et des codes d’accès.

PERSPECTIVES

Le but de la science ça n'est pas d'arriver à l'infini du savoir, mais c'est de mettre fin à l'infini de l'erreur. C'est bien dans cette thématique que nous inscrivons nos travaux de thèse. La recherche laisse naturellement entrevoir d'autres prolongements en rapport avec des développements scientifiques. Plusieurs pistes nous paraissent intéressantes :

- L'ontologie définie s'inscrit (par définition) dans un processus de codage minimal (voir les critères de Grüber d'évaluation d'une ontologie, chapitre 5 §1.5). Elle est donc générique mais ouverte à contenir de nouveaux concepts sans que cela ne modifie les fondements ontologiques sur lesquels elle était fondée. Il convient donc de bâtir des ontologies de domaine (voir la typologie des ontologies, chapitre 5 §1.3) à partir de cette ontologie principale.
- La définition des concepts à travers le processus accidentel ontologique, nous a permis de voir plus clair, avant de proposer la méthode originale « Management Préliminaire des Risques ». Cette dernière pourrait constituer une version préliminaire d'un projet de norme sur l'APR. Ce sujet a été évoqué auprès de la direction de valorisation de l'INRETS ainsi qu'auprès de Siemens Transportation Systems et d'un représentant de l'AFNOR.
- 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 dédié à une méthode d'analyse de risque telle que AMDEC, Arbre de Cause ou Arbre d'Evénement.
- La modélisation du processus accidentel ontologique est de type état/transition (spécification des états des entités, des événements, etc.). Ainsi, 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. Ceci garantira la traçabilité au sein du processus global de management des risques
- La modélisation des scénarios d'accident avec RdP mérite d'être retravaillée de façon plus outillée. Il existe une palette très riche d'outils de vérification, d'évaluation et de simulation du fonctionnement des RdP dont d'ailleurs certains sont orientés vers les besoins de la sûreté de fonctionnement. Ceci, permettra de rompre avec le clivage qui existe entre les approches d'analyse de risque qualitatives et quantitatives.
- L'outil SIGAR mériterait d'être repris par un éditeur de logiciel afin d'élaborer une version commercialisable. Il peut aussi être destiné à l'enseignement pédagogique de la méthode MPR.

Annexe A

PANORAMA DES MÉTHODES D'ANALYSE DE RISQUE

1. AMDE(C)

Référence : (CEI 60812, Janvier 2006) (CEI 300-3-9, 1995) (RE. Aéro 701 11 , Novembre 1986) (Lievens, 1976), (Villemeur, 1988), (Laurant, 2003)

Type : Inductive

Démarche : L'AMDEC repose sur les concepts de : défaillance (failure), mode de fonctionnement (functional mode), cause de défaillance (failure cause), effet d'un mode défaillance (failure mode effect) et de sa criticité (criticality).

SOURCE	*Défaillance*
CEI 50191	Cessation d'aptitude d'une entité à accomplir une fonction requise. Notes. 1. Après défaillance d'une entité, cette entité est en état de panne. 2. Une défaillance est un passage d'un état à un autre, par opposition à une panne, qui est un état. 3. La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une autre entité
RE. AERO 701 11	c'est pour un élément (composant, équipement, dispositif, etc.) la cessation de son aptitude à accomplir la fonction exigée de lui et/ou la possibilité de nuire au fonctionnement de l'ensemble auquel il appartient.

SOURCE	*Mode de défaillance*
CEI 50191	Sous-ensemble de l'ensemble complet des fonctions possibles d'une entité.

Le mode de défaillance constitue la façon par laquelle une défaillance est observée sur un élément du système.

SOURCE	*Cause de défaillance*

CEI 50191	Ensemble de circonstances associées à la conception, la fabrication ou l'emploi qui ont entraîné une défaillance.

La notion de causes de défaillance peut être vu comme l'ensemble des évènements qui conduisent aux modes de défaillances.

Effet d'un mode de défaillance :

Soit les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise.

Les modes de défaillance sont définis à partir des fonctions remplies par le système, ceci en se posant la question « qu'est ce qui se passe si »:

- La fonction ne se réalise pas à la sollicitation ? ou bien
- se réalise de façon intempestive ? ou bien
- est dégradée ? ou alors
- ne se réalise plus.

Pour chaque mode de défaillance, on identifie les causes possibles et ensuite les effets sur les fonctions supérieures du système et de ses interfaces.

Les criticités des modes de défaillance sont évalués en fonction de la gravité des conséquences et la fréquence d'occurrence des événements redoutés.

De manière très schématique, l'AMDEC se déroule suivant l'algorithme suivant :

Processus de déroulement d'une AMDEC :

Début_AMDEC

Pour tous les éléments (ou composant) du système faire

Debut_pour1

Pour tous les états de fonctionnement (normal, arrêt...) de cet élément faire

Debut_pour2

Pour tous les modes de défaillance faire

Debut_pour3

Identifier les **Causes** () ;

Identifier les **Conséquences** () ;

Evaluer la **Criticité** = (Probabilité, Gravité) ;

Tant que Criticité est non acceptable faire

Début_tq

Engager_des_actions_de_MdR (détecter le mode de défaillance, limiter les effets);

Re-évaluer la **Criticité** = (Probabilité, Gravité) ;

Fin_tq

Fin_pour3

Fin_pour2

Fin_pour1

Fin_AMDEC

TAB. 1 : Exemple d'un tableau de type AMDE [RE.Aéro 70111, 86]

Système: **Sous-système :** **Fonction :** **Elément :**							
Modes de défaillances	Causes possibles	Phases	Conséquences		Classification de la gravité de la conséquence	Actions correctives	Recommandations' application
			Sur le sous système	Sur le système			

TAB. 2 : Exemple d'un tableau de type AMDEC [RE.Aéro 70111, 86]

Système: **Sous-système :** **Fonction :** **Elément :**									
Modes de défaillances	Causes possibles	Phases	Conséquences		Classification de la gravité de la conséquence	Probabilité du mode de défaillance	Criticité	Actions correctives	Recommandations' application
			Sur le sous système	Sur le système					

La norme CEI 60812 présente une liste générique de modes de défaillance mais qui devrait être complétée selon les spécificités du système étudié :

TAB. 3 : Modes de défaillance génériques de la norme CEI 60812[CEI 60812, 06]

1	Défaillance structurelle (rupture)	**12**	Est en dessous de la limite inférieure tolérée	**23**	Fonctionnement après délai prévu (retard)
2	Blocage physique ou coincement	**13**	Fonctionnement intempestif	**24**	Entrée erronée (augmentation)
3	Vibrations	**14**	Fonctionnement intermittent	**25**	Entrée erronée (diminution)
4	Ne reste pas en position	**15**	Fonctionnement irrégulier	**26**	Sortie erronée (augmentation)
5	Ne s'ouvre pas	**16**	Indication erronée	**27**	Sortie erronée (diminution)
6	Ne se ferme pas	**17**	Ecoulement réduit	**28**	Perte de l'entrée
7	Défaillance en position ouverte	**18**	Mise en marche erronée	**29**	Perte de sortie
8	Défaillance en position fermée	**19**	Ne s'arrête pas	**30**	Court-circuit (électrique)
9	Fuite interne	**20**	Ne démarre pas	**31**	Circuit ouvert (électrique)

10	Fuite externe	**21**	Ne commute pas	**32**	Fuite (électrique)
11	Dépasse la limite supérieure tolérée	**22**	Fonctionnement prématuré	**33**	Autres conditions de défaillance exceptionnelles

Avantages: L'AMDEC est un outil incontournable d'analyse et d'évaluation de défaillances simples susceptibles de conduire à des défaillances globales au niveau système et aussi d'études de moyens adaptés permettant de limiter leurs effets et prévenir leurs occurrences.

Les résultats de l'AMDEC sont spécifiquement détaillés et notamment en ce qui concerne la propagation des défaillances et leurs conséquences.

L'AMDEC peut accompagner quasiment tout le cycle de vie du développement d'un système : conception, validation, test, etc.

Limites : La pertinence de l'AMDEC dépend de la possibilité de déterminer tous les modes de défaillance possibles d'un système. Ceci est extrêmement difficile s'agissant de sous-systèmes complexes présentant de possibilités de défaillances conjuguées ; le cas échéant l'analyse est complémentée par d'autres méthodes telles que les arbres de défaillances ou la méthode de combinaisons de pannes.

2. Hazard and Operability Study (HAZOP)

Références : (CEI 61882, Mai 2001), (CEI 60812, Janvier 2006) (CEI 300-3-9, 1995) (RE. Aéro 701 11 , Novembre 1986) (Lievens, 1976), (Villemeur, 1988), (Laurant, 2003)

Type : Inductive

Démarche : La norme CEI 61882 propose des exemples de mots-clés dont l'usage est particulièrement courant. Ces mots-clés sont repris dans le tableau ci-dessous :

TAB. 4 : Exemples de mots-clés pour l'HAZOP (CEI 61882)

Type de déviation	Mot-clé	Exemples d'interprétation
Négative	NE PAS FAIRE	Aucune partie de l'intention n'est accomplie
Modification quantitative	PLUS	Augmentation quantitative
	MOINS	Diminution quantitative
Modification qualitative	EN PLUS DE	Présence d'impuretés – exécution simultanée d'une autre opération/étape
	PARTIE DE	Une partie seulement de l'intention est réalisée
Substitution	INVERSE	S'applique à l'inversion de l'écoulement dans les canalisations ou à l'inversion des réactions chimiques
	AUTRE QUE	Un résultat différent de l'intention originale est obtenu

Temps	PLUS TOT	Un événement se produit avant l'heure prévue
	PLUS TARD	Un événement se produit après l'heure prévue
Ordre séquence	AVANT	Un événement se produit trop tôt dans une séquence
	APRES	Un événement se produit trop tard dans une séquence

La combinaison des paramètres observés avec les mots clé précédemment définis se fait de la manière suivante :

« Plus de » et « Pression » = « Pression trop haute »,

« Pas de » et « Niveau » = « Capacité vide ».

Dans le cas où une estimation de la criticité serait nécessaire, l'HAZOP est complétée par une analyse à priori de la criticité des risques sur les bases d'une technique quantitative simplifiée.

Le déroulement d'une étude HAZOP se fait suivant l'algorithme suivant :

Processus de déroulement d'une HAZOP :

Début_HAZOP
Pour tous les éléments (ou composant) du système faire
Debut_pour1
Pour tous les paramètres de fonctionnement de cet élément faire
Debut_pour2
Pour tous les mots clés faire
Debut_pour3
Générer une **dérive () ;** Evaluer les **Conséquences** () ;
Si cette dérive est crédible alors
Début_si
Identifier les **Causes** () ;
Evaluer la **Criticité** = (Probabilité, Gravité) ;
Tant que Criticité est non acceptable faire
Début_tq
Engager_des_actions_de_MdR (détecter cette dérive, limiter les effets);
Re-évaluer la **Criticité** = (Probabilité, Gravité) ;
Fin_tq
Fin_si
Fin_pour3
Fin_pour2
Fin_pour1
Fin_HAZOP

Le tableau suivant montre un exemple de descripteur type relatif à une étude HAZOP :

TAB. 5 : Descripteur de données d'une étude HAZOP (CEI 61882)

Date : **Ligne ou équipement :**								
N°	**Mot clé**	**Paramètre**	**causes**	**conséquences**	**détection**	**Sécurités existantes**	**Propositions d'amélioration**	**observations**

Avantages: HAZOP est une méthode très adaptée à l'étude de dangers dans le domaine des procédés tel que le domaine chimique.

Limites: HAZOP permet difficilement d'analyser les évènements résultant de la combinaison simultanée de plusieurs défaillances.

3. L'Analyse par Arbre de Défaillances, Arbre de causes ou Arbre de fautes

Références : (CEI 300-3-9, 1995), (RE. Aéro 701 11 , Novembre 1986), (Lievens, 1976), (Villemeur, 1988), (Laurant, 2003)

Type : Déductive.

Démarche : La méthode consiste en une représentation graphique des multiples causes d'un événement dangereux. Elle permet de visualiser les relations entre les défaillances d'équipement, les erreurs humaines et les facteurs environnementaux qui peuvent conduire à des accidents. On peut donc éventuellement y inclure des facteurs reliés aux aspects organisationnels.

L'algorithme suivant montre d'une manière systématique le déroulement d'une Analyse par Arbre de Défaillances :

Processus de déroulement d'une AAD :

Début_AAD

Considérer_un_Evénement_Final ;

Label_événement_intermediaire :

Identifier_les_**causes () ;** /*Identification exhaustive des causes immédiates*/

Définir_les_**événements**_en_question **() ;**

Lier_ces_**événements** () /* liaisons graphiques par portes logiques*/ ;

Pour chaque Evénement faire

Début_pour

Si cet Evénement est décomposable Alors /*n'est pas un événement de base*/

Début_si

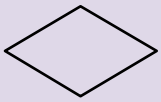
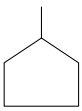
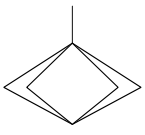
Goto Label_événement_intermediaire ;

Fin_si

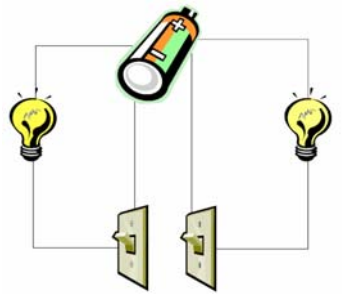
Fin_pour

Fin_AAD

Conception graphique :

Symbole	Signification
	**Événement de base** Événement initial ne nécessitant pas de développement. Il s'agit essentiellement d'une défaillance première d'une entité à la limite de l'analyse.
	**Événement non développé** Événement qui ne constitue pas un événement de base mais qui ne sera pas développé en raison d'un manque d'information ou d'autres considérations.
	**Événement intermédiaire** Représentation d'un événement qui est le résultat de la combinaison de d'autres événements.
	**Porte « ET »** Nécessite l'addition des événements *causes* pour engendrer l'événement *effet*.
	**Porte OU** Ne requiert qu'un seul des événements *causes* pour engendrer l'événement *effet*.
	**Transfert vers...** Indique que l'arbre se poursuit à la section indiquée par le numéro dans le triangle.
	**Transfert de...** Indique que cette portion de l'arbre est la suite détaillée de la section indiquée par le numéro dans le triangle.
	**Maison** Représente un événement qui correspond à une utilisation normale du système
	Représente un événement dont les causes ne sont pas encore développées, mais le seront ultérieurement

L'exemple suivant est relatif à un problème classique de commande de deux interrupteurs alimentés par une source d'alimentation commune :



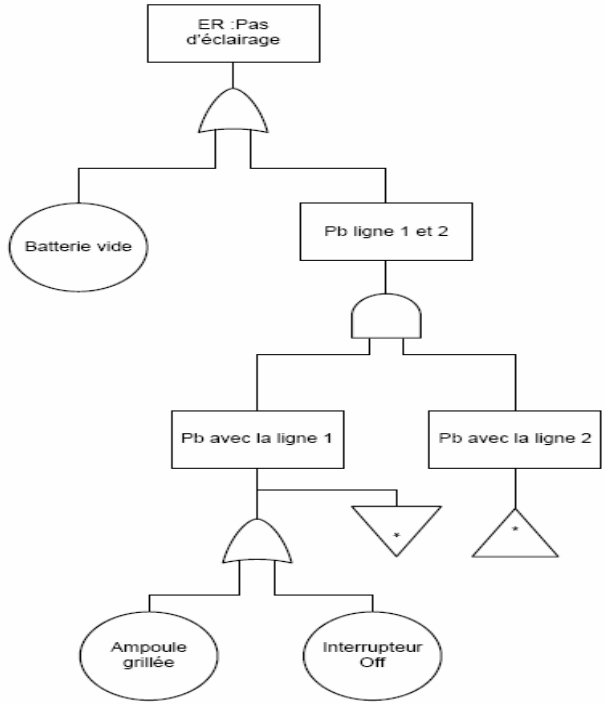


FIG. 1 : Exemple d'un arbre de défaillance

Voici quelques règles d'optimisation permettant de réduire les Arbres en faisant appliquer l'algèbre de Boole :

TAB. 6 : Règles d'optimisation des arbres de défaillances

Propriétés	**Produit (Porte logique And)**	**Somme (Porte logique Or)**
Commutativité	A . B= B . A	A + B= B + A
Idempotence	A . A = A	A +A = A
Absorption	A . (A + B) = A	A + A. B = A
Associativité	A . (B . C)= (A . B) . C	A + (B +C) = (A + B) + C
Distributivité	A . (B + C) = A. B + A . C	A + B .C = (A + B) . (A + C)

Avantages : L'analyse par arbre de défaillances est une étude prioritaire des défaillances relatives à des événements redoutés dont la gravité de production est plus significative. Elle permet de considérer des combinaisons d'évènements pouvant conduire à un événement redouté.

Un autre point fort essentiel est la lisibilité à travers la représentation graphique des combinaisons de causes aboutissant à des défaillances.

Limites : La méthode exige une parfaite connaissance des scénarios événementiels et donc du fonctionnement du système et de son interaction avec son environnement.

La lisibilité des arbres de défaillances peut s'avérer très compliquée quand il s'agit de systèmes complexes ou d'événement indésirable trop générique ou mal spécifié, à cet effet on utilise des outils informatiques de conception et de vérification.

Cette méthode est efficace pour analyser de petits systèmes, l'analyse d'un système complexe nécessiterait sa décomposition en plusieurs sous systèmes. Néanmoins, la dernière décennie à vu paraître plusieurs logiciels

offrant, entre autres, des fonctionnalités d'aides et d'assistance pour la conception graphique, la recherche systématique des coupes minimales et la propagation des probabilités.

4. Analyse par Arbre d'Evènements

Références : (CEI 60812, Janvier 2006) (CEI 300-3-9, 1995) (RE. Aéro 701 11 , Novembre 1986) (Lievens, 1976), (Villemeur, 1988), (Laurant, 2003)

Type : Inductive

Démarche : L'algorithme suivant montre une démarche systématique de l'analyse par Arbre d'Evénements:

Processus de déroulement d'une AAE :

Début_AAE

Considérer_un_Evénement_Initial ;

Classer_les_**Fonctions_de_sécurité**_à_affecter **() ; /* de Fonction 1 à fonction n */**

Pour i allant de 1 à n faire /* i entier*/

Début_pour

Supposer_Succès (fonction i) ; /* Fonctionnement de la Fonction de sécurité*/

Supposer_Echec (fonction i) ; /* défaillance de la Fonction de sécurité*/

Lier_les_deux_états () ; /*Liaisons graphiques Horizontales connectées aux sorties du niveau i-1. La branche supérieure désigne le succès avec une probabilité (P = exp(-λt)) égale à la fiabilité de la fonction i (λ étant son taux de défaillance), et la branche inférieure à l'échec avec la probabilité (1-P) */ ;

Fin_pour

Fin_AAE

Conception graphique : L'arbre d'événement suivant est une adaptation élaborée par M. RAUSAND dans son livre « System Reliability Theory » [Rausand, 04] d'un exemple proposé par la norme CEI 60300-3-9 [CEI 60300-3-9, 04].

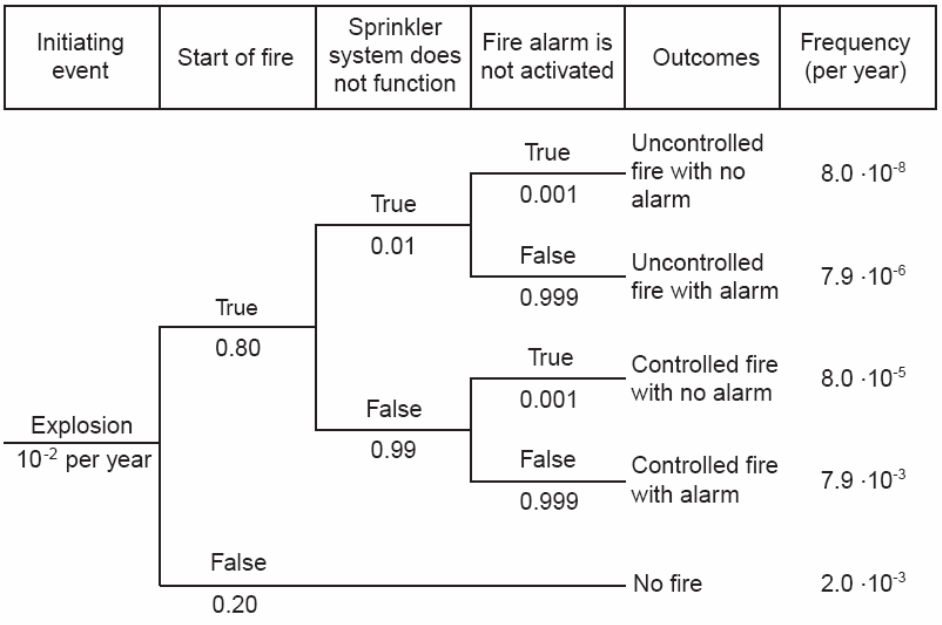


FIG. 2: Arbre d'événement d'un système anti-incendie [Rausand, 04]

Avantages : L'analyse par arbre d'évènements permet d'analyser l'évolution des événements initiateurs jusqu'à la réalisation d'événements redoutés. Elle peut être très efficace pour l'analyse des mécanismes de défense en profondeur (protection, prévention, mitigation).

Limites : La méthode peut s'avérer rapidement lourde à mettre en œuvre si les évènements initiateurs ne sont pas bien définis. Il convient donc de sélectionner les événements initiateurs pouvant effectivement conduire à des situations critiques.

5. Le nœud papillon

Références: (INERIS-DRA, 2003), (SAMRAIL Consortium, Septembre 2003),

Type : Inductive/déductive.

Objectifs: Le « Nœud Papillon » est une approche arborescente développée par SHELL permettant de considérer une approche probabiliste dans le management du risque.

Démarche: Le nœud papillon est un outil qui combine un arbre de défaillances et un arbre d'événements. L'INERIS a adapté une forme particulière combinant plusieurs types d'évènements :

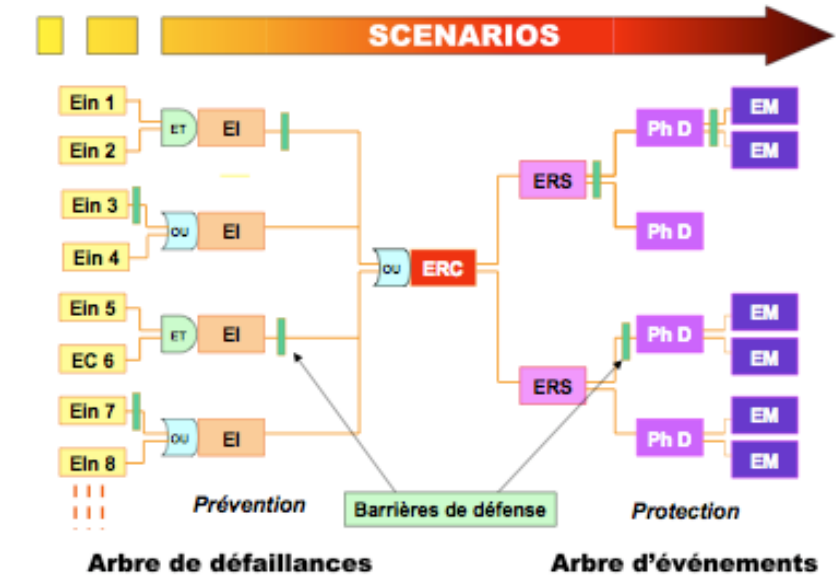


FIG. 3: Représentation de scénarios d'accident selon le modèle nœud papillon [INERIS, 2003]

TAB. 7 : Légende des évènements figurant sur le modèle du nœud papillon INERIS [INERIS, 03]

Désignation	Signification	Définition	Exemple
Ein	Evénement Indésirable	Dérive ou défaillance sortant du cadre des conditions d'exploitation usuelles définies	Le sur-remplissage ou un départ d'incendie à proximité d'un équipement dangereux
EC	Evénement Courant	Evénement admis survenant de façon récurrente dans la vie d'une installation	Les actions de test, de maintenance ou la fatigue d'équipements
EI	Evénement Initiateur	Cause directe d'une perte de confinement ou d'intégrité physique	La corrosion, l'érosion, les agressions mécaniques, une montée en pression
ERC	Evénement Redouté Central	Perte de confinement sur un équipement dangereux ou perte d'intégrité physique d'une substance dangereuse	Rupture, brèche, ruine ou décomposition d'une substance dangereuse dans le cas d'une perte d'intégrité physique
ERS	Evénement Redouté Secondaire	Conséquences directes de l'événement redouté central, l'événement redouté secondaire caractérise le terme source de l'accident	Formation d'une flaque ou d'un nuage toxique
PhD	Phénomène Dangereux	Phénomène physique pouvant engendrer des dommages majeurs	Incendie, explosion, dispersion d'un nuage toxique
EM	Effets Majeurs	Dommages occasionnés au niveau	Effets létaux ou irréversibles sur la

		des cibles (personnes, environnement ou biens) par les effets d'un phénomène dangereux	population
Barrières ou mesures de prévention		Barrières ou mesures visant à prévenir la perte de confinement ou d'intégrité physique	Peinture anticorrosion, coupure automatique des opérations de dépotage sur détection d'un niveau très haut…
Barrières ou mesures de protection		Barrières ou mesures visant à limiter les conséquences de la perte de confinement ou d'intégrité	Vannes de sectionnement automatiques asservies à une détection (gaz, pression, débit), moyens d'intervention…

Conception graphique :

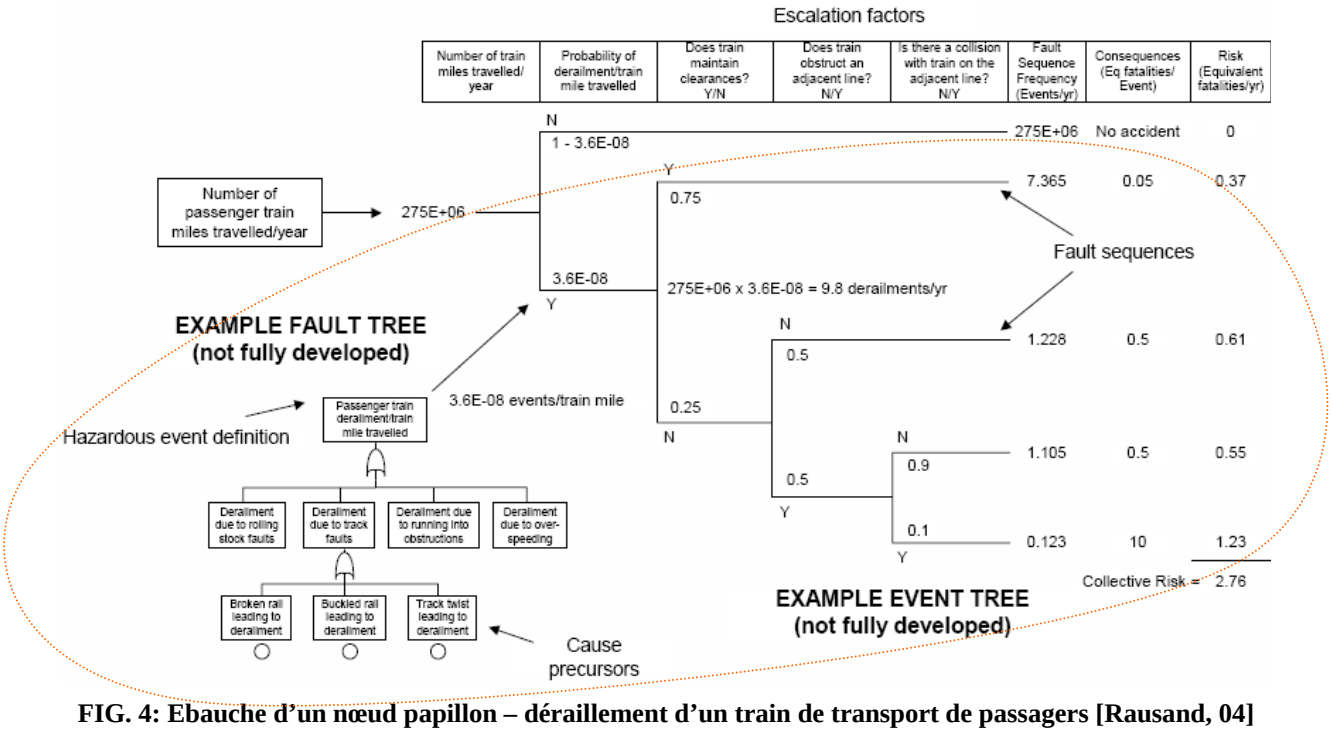


FIG. 4: Ebauche d'un nœud papillon – déraillement d'un train de transport de passagers [Rausand, 04]

Avantages: La représentation graphique offre une meilleure visualisation des scénarios d'accidents et met en valeur la mise en œuvre optimisée des mécanismes de défense en profondeur (barrières de défense).

Limites: La mise en œuvre de cette technique est très rigide et nécessite un temps énorme pour explorer d'une manière exhaustive tous les chemins menant des causes de défaillances vers les effets et leurs conséquences sur les cibles vulnérables. Il convient donc que son utilisation soit réservée aux événements principaux de scénarios jugés particulièrement critiques et nécessitant une démonstration de sécurité plus approfondie. Ce jugement peut être porté lors de la tenue de l'APR.

6. La méthode MOSAR

MOSAR contient deux modules hiérarchiques, un module macro « module 'A' » et un module micro « module 'B' » :

6.1 MOSAR – module A : Analyse Macroscopique

Le module 'A' (voir FIG. 5) a pour but d'identifier les dysfonctionnements techniques et opératoires provoquant un événement indésirable

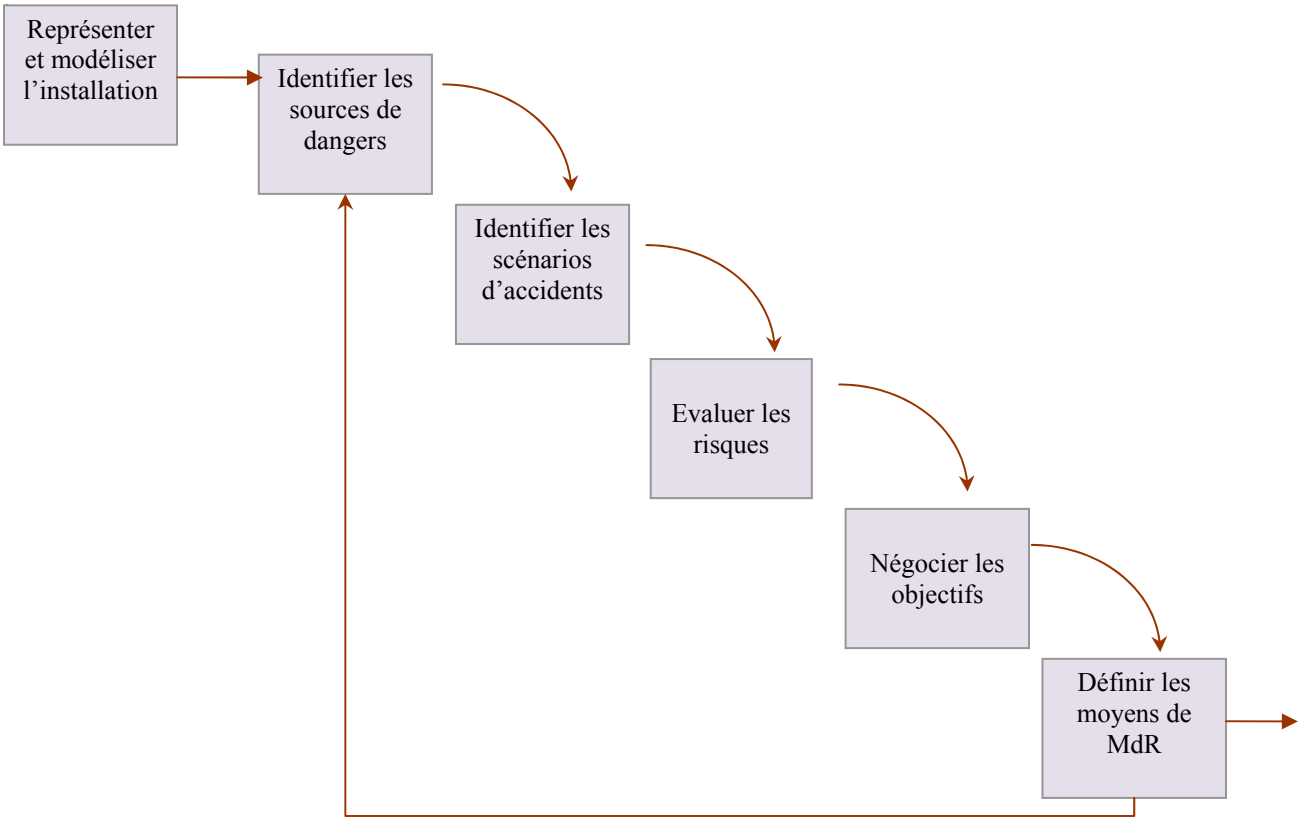


FIG. 5 : MOSAR – module A [Périlhon, 2001]

- **Modéliser l'installation:** préciser l'environnement du système et découper ce dernier en plusieurs sous systèmes en tenant compte des dimensions : technique, humaine et organisationnelle.
- **Identifier les sources de dangers:** identification des éléments dangereux susceptible d'être à l'origine d'un facteur de déclenchement du flux de danger.
- **Identifier les scénarios d'accidents:** identification des processus de dangers selon le processus de la MADS.
- **Evaluer les scénarios de risques:** estimation des fréquences d'occurrence et appréciation de risque.

- **Négocier les objectifs:** hiérarchiser les scénarii d'accidents et discussion de leur acceptabilité en fonction des objectifs de sécurité préalablement définis.
- **Définir les moyens de Maîtrise des Risques:** l'approche MADS du processus de dangers montre clairement le positionnement des barrières de prévention, de protection et de mitigation. L'objectif ici est de réduire l'occurrence des scénarios d'accidents identifiés.

6.2 MOSAR – module B : Analyse Microscopique

Le module B de la méthode MOSAR (voir FIG. 6) qui se présente d'ailleurs comme une suite logique au module A, permet d'effectuer une analyse détaillée des dysfonctionnements techniques et opératoires et aussi de l'impact qu'ils pourraient engendrer sur le système global.

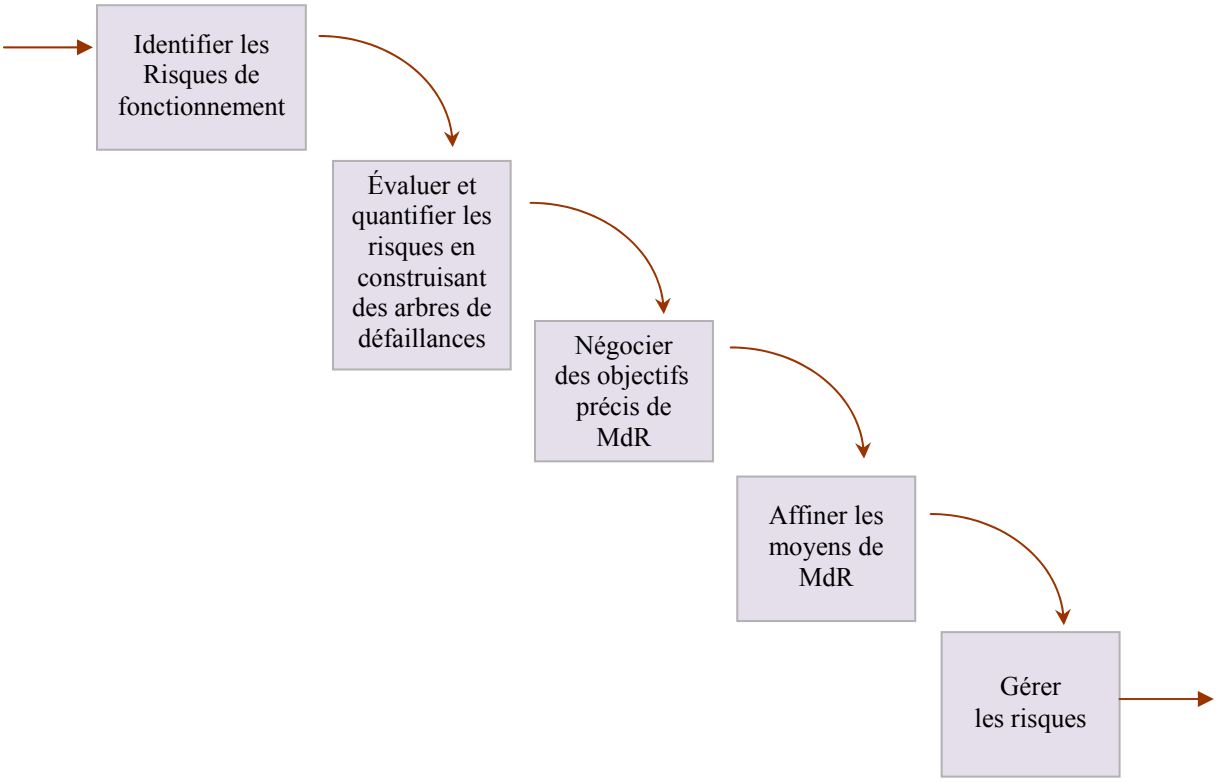


FIG. 6 : MOSAR – module B [Périlhon, 2001]

- **Identifier les risques de fonctionnement:** après avoir élaboré une liste de sources de dangers (deuxième étape du module A), cette étape s'intéresse aux détails de leurs dysfonctionnements techniques et opératoires.
- **Evaluer les risques en constituant des arbres de défaillances:** la puissance de modélisation par arbre de défaillances permet de rendre la méthode plus efficace et notamment par rapport à l'estimation des probabilités d'occurrence des événements, le calcul des coupes minimales et la mise en œuvre efficace des barrières de défense.
- **Négocier des objectifs précis de Maîtrise de Risques:** cette partie concerne l'allocation des exigences de sécurité dans le but de mettre en place des barrières de prévention ou de protection.

- **Affiner les moyens complémentaires de Maîtrise de Risques:** faire un arbitrage entre les enjeux financiers (relatifs aux coûts de mise en œuvre des barrières de défense) et les enjeux de sûreté de fonctionnement. Ceci renvoie à l'analyse coût/bénéfices.
- **Gérer les risques:** cette partie est relative à la documentation de l'analyse, la communication et le suivi des risques.

6.3 Fonctionnement global de la méthode MOSAR

Il existe différentes possibilités d'interconnecter les modules A et B (voir FIG. 7): soit en poursuivant intégralement le module B à l'issue du module A, soit partiellement à partir de l'étape 2, 3 ou 4.

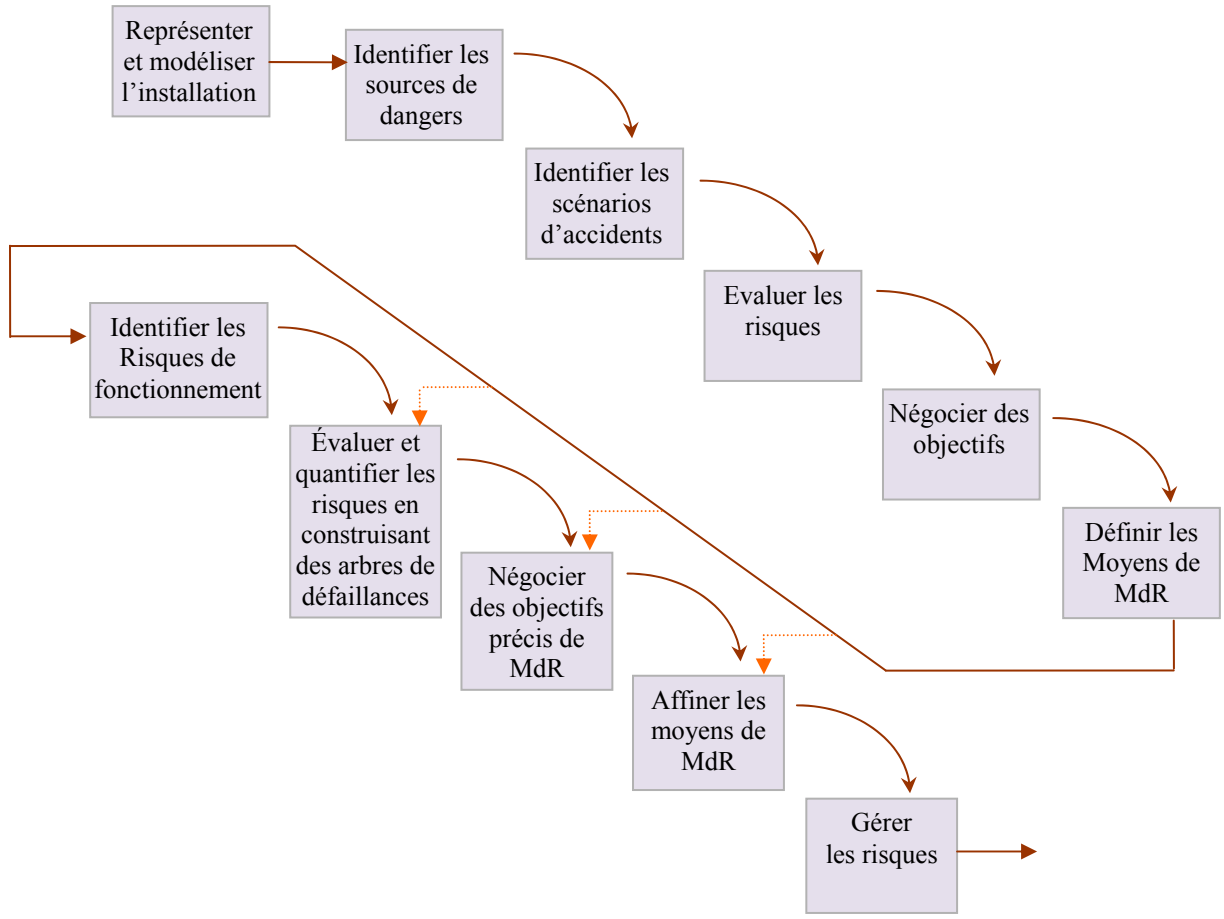


FIG. 7 : MOSAR [Périlhon, 2001]

Annexe B

ELÉMENTS DE BASE D'UN SMS CENTRÉ-MPR

Le Système de Management de la Sécurité (SMS) est un processus technico-organisationnel de gestion des risques. Le SMS est un schéma complet d'activités d'analyse, d'évaluation et de maitrise des risques. En outre, il comprend aussi des stratégies de définition des responsabilités, de communication et de gestion des crises. Ces stratégies sont préalablement réfléchies sur les plans technique, humain et organisationnel.

Le SMS que nous avons proposé dans le chapitre 6 (voir chapitre 6, FIG. 9) est principalement centré sur la méthode MPR. Ce rapprochement SMS-MPR s'inscrit dans un processus d'amélioration de type PDCA (voir chapitre 6, FIG. 8).

1. Profil de mission

Les parties responsables doivent identifier la nature et les possibilités de leurs opérations. Elles doivent en particulier préciser les éléments qui sont sous leurs responsabilités. Les responsables hiérarchiques doivent être au courant de leurs responsabilités en matière de management de la sécurité. En particulier, ils doivent clairement statuer sur leur assimilation des responsabilités individuelles ou communes avec d'autres parties.

2. Politique de la sécurité

Chaque partie est tenue de démontrer ses capacités à maintenir la sécurité à un niveau acceptable. Cet engagement doit être explicitement communiqué de la manière qui puisse mettre en lumière :

- Les actions de management de la sécurité,
- Les processus et les procédures mis en place,
- Les ressources allouées,
- Les aspects organisationnels y compris la concertation des partenaires industriels et autres sous-traitants.

3. Assurance de la sécurité

Chaque partie responsable doit s'assurer de la bonne gestion de tous les risques ayant un lien avec le système global et qui ne sont pas sous son contrôle direct. Le cas échéant, elle doit prévoir des canaux de communication et de surveillance de ces risques, tout en les intégrant dans son SMS, ce qui permet, entre autres, de s'assurer que les risques jugés résiduels par d'autres parties sont effectivement acceptables en interne.

4. Gestion des référentiels

Chaque partie responsable doit mettre en place des procédures d'identification des textes réglementaires, règles, normes et besoins techniques ayant un lien avec son activité. Elle doit mettre en place aussi, des procédures régulières d'audit, et de revue du SMS, et établir des procédures de préparation et de revue de son rapport annuel de sécurité qu'elle adressera ensuite aux autorités compétentes qui statueront sur la conformité de ses indicateurs en matière de sécurité et de qualité.

5. Gestion des rôles et affectation des responsabilités

Chaque partie responsable doit établir et maintenir clairement les périmètres qui sont sous sa responsabilité dans le processus de management de la sécurité. Les responsabilités d'interfaçage avec d'autres organisations doivent être proprement identifiées et intégrées au SMS.

Néanmoins, l'absence de critères équitables d'évaluation des degrés de responsabilité de chacun soulève un vrai problème dans la façon de répartir une responsabilité globale sur un groupe d'acteurs concernés et appartenant à différents niveaux hiérarchiques, voire à différentes organisations.

Toutefois, on peut dégager deux propriétés de base : les responsabilités lourdes et peu fréquentes se situant en haut de la hiérarchie et l'inverse, c-.à.-d au plus bas de la pyramides des responsabilités. Autrement dit, les acteurs du niveau opérationnel sont souvent les plus responsabilisés, ensuite à un moindre degré les

concepteurs et les experts de planification et enfin très rarement s'agissant des responsables définissant la politique et la structure de l'organisation.

6. Gestion des crises

La complexité des systèmes engendre des phénomènes intégrant, à la fois l'ordre imposé par la conception et l'organisation, mais aussi le naturel désordre résultant de tout dysfonctionnement ou toute erreur humaine. Ces phénomènes sont du point de vue de l'analyste, des précurseurs à l'occurrence de situations de crise.

Par conséquent, chaque partie responsable doit mettre en place un support de procédures génériques permettant de prévoir ce qu'il faut faire face à certaines situations de crise. Ces plans d'urgence doivent comprendre des actions de réduction du risque, de gestion des modes dégradées et de retour vers le mode nominal.

Dans le domaine des installations classées pour la protection de l'environnement (ICPE), il existe plusieurs types de plan de gestion de crise :

- **Plan d'Opération Interne** (**POI**) réalisé par l'industriel, il sert à évaluer la situation, envisager l'évolution probable du risque pour le public et pour l'environnement, lancer les actions pour revenir à une situation réputée sûre. Le POI prévoit également l'information immédiate des pouvoirs publics et, en particulier du préfet, de la Direction Générale de la Sureté Nucléaire et de la Radioprotection (DGSNR), et de la presse.
- **Plan Particulier d'Intervention (PPI)** réalisé par le préfet, il défini les dispositions à mettre en œuvre à l'extérieur de l'établissement. Il est lancé en cas d'accident présentant des conséquences radiologiques à l'extérieur du site. Le PPI est à disposition du public dans toutes les mairies des communes proches d'une centrale.
- **Plan de Prévention des Risques Technologiques (PPRT)** élaboré par le Préfet en concertation avec les collectivités territoriales, l'exploitant et le président du Comité Local d'Information et de Concertation (CLIC) : il sera utilisé pour la maîtrise de l'urbanisation autour des sites à risques.

7. Gestion des Bases de Données accidents/incidents

Dans un épitomé intitulé « Management de la sécurité d'entreprise, vocabulaire et concept », édité en Mars 1996 par l'Association Qualité-Sécurité (AQS) pour le groupe de travail de l'observatoire de l'opinion sur les risques et la sécurité, il est stipulé que l'analyse est à l'incident ce que la taille est au diamant.

En effet, les enquêtes techniques ne doivent pas se focaliser sur les scénarios caractérisés par des pertes importantes, vu leur rareté comparés aux incidents de moindre impact. Souvent, un événement négligeable peut s'avérer fort intéressant dans un concours de circonstances légèrement différent.

Par conséquent, chaque partie responsable doit mettre en place des mécanismes de capitalisation et d'investigation sur les accidents et incidents. Ces mécanismes permettent d'extraire, formaliser et archiver les scénarios de risque de façon à constituer une bibliothèque de cas types par recours aux techniques d'acquisition, modélisation et formalisation des connaissances. La base de données obtenue doit servir au Retour d'expérience. Il convient que les résultats du REX soient communiqués en interne ainsi qu'avec toutes les autres parties impliquées dans ou concernées par le projet en question.

8. Retour d'Expérience (REX)

Le retour d'expérience est le fait d'exploiter des connaissances historiques archivées afin de dégager un savoir-faire en matière de management des risques.

La mise en place d'un processus de REX implique plusieurs acteurs et beaucoup de facteurs. Il convient qu'une équipe soit chargée d' :

1. Extraire, formaliser et archiver les scénarios de risque de façon à constituer une bibliothèque de cas types par recours aux techniques d'acquisition, modélisation et formalisation des connaissances,
2. Exploiter les connaissances historiques archivées afin de dégager un savoir-faire en matière de management des risques.

Généralement, le processus de REX nécessite l'analyse et l'examen des phases suivantes : collecte de données, traitement de données, stockage de données, exploitation de données, et proposition de recommandations :

1. La première phase (collecte de données) consiste à recueillir le maximum de données, à s'intéresser à toutes les anomalies rencontrées et à faire appel à diverses ressources de recherche d'information. La collecte de données concerne les données relatives à l'opérateur humain, à son environnement interne ou externe, au système technique, à l'organisation du travail, aux procédures et aux éventuelles interactions entre ces composantes.
2. La deuxième phase (traitement de données) passe par une analyse des circonstances, des faits, des mécanismes et des causes des accidents potentiels. Elle permet de reconstituer la chronologie des faits, d'établir les scénarios à risque et d'évaluer les conséquences. Cette phase ne doit pas se limiter à l'analyse des causes primaires ou apparentes, mais à établir, par exemple, un arbre de causes permettant de mieux identifier les mécanismes générateurs d'accident.
3. La troisième phase (stockage de données) s'attache à mémoriser et archiver dans une base de données les données collectées et analysées. Lors de cette phase, une attention particulière est portée aux possibilités d'exploitation réelle de cette base de données.
4. La quatrième phase (exploitation de données) consiste à exploiter et interpréter les résultats issus des différentes requêtes d'interrogation de la base de données. L'objectif principal est d'extraire l'événement réellement prédictif, de prendre en considération les cas isolés et de prédire ou d'imaginer les futurs éléments qui vont être insérés dans la base de données comme étant de nouveaux scénarios d'accident ou d'incident.

5. La cinquième et dernière phase (proposition de recommandations) consiste à définir et identifier les mesures adéquates pour limiter la reproduction d'un scénario à risque. Il s'agit de mieux tirer profit des enseignements de l'expérience acquise pour améliorer la sécurité. Les recommandations visent la réduction du risque (probabilité/gravité) grâce à des mesures de prévention pour minimiser la fréquence d'occurrence d'un scénario d'accident et des mesures de protection en vue de réduire la gravité de ses conséquences. Ces recommandations se traduiront par des actions de maitrise agissant sur les facteurs humains, la technologie, l'environnement, l'organisation, la réglementation, les procédures, la documentation, etc.

La démarche de retour d'expérience que nous proposons se divise en 3 boucles hiérarchiques relatives à l'apprentissage rétroactif du premier, deuxième et troisième ordre. Plus le niveau d'ordre est supérieur, plus la criticité des décisions est importante. Une décision peut être une simple remise en fonction d'un dispositif, comme ça peut être la redéfinition pure et simple de la stratégie et des objectifs préliminaires d'une société.

1. L'apprentissage du premier ordre a pour objet d'assister et d'inspecter la correction des déviations dans l'exécution des cahiers de charges (missions),
2. Le second ordre repose sur une analyse complémentaire « à froid », qui sert à comprendre pourquoi les dysfonctionnements ont eu lieu. Cela consiste à déterminer, à la suite du traitement de certaines anomalies, quels sont les précurseurs les plus redoutés et ensuite leur affecter des priorités avant d'engager en conséquence une analyse avale plus approfondie,
3. Le troisième ordre quant à lui s'intéresse aux éléments structurels et fonctionnels ainsi qu'aux critères et objectifs globaux. Il s'agit d'adopter une vision plus approfondie et à long terme.

Nous pouvons constater que l'application de cette démarche en 5 phases au processus de REX en 3 boucles de rétroaction est une tâche nécessitant d'énormes efforts, une parfaite organisation, et plusieurs jours voire plusieurs semaines de préparation. Cependant, les moyens et les outils informatiques d'aide à la décision permettent de raccourcir considérablement les délais et apporter davantage une meilleure fiabilité en termes de résultats.

9. Maitrise de la communication

Le SMS doit être documenté dans toutes ses parties, à commencer par la répartition des responsabilités sur l'organigramme cible et l'élaboration de l'annuaire des compétences au sein d'une organisation. En outre, il indique comment la direction assure le contrôle aux différents niveaux de l'organisation, et comment le personnel et sa hiérarchie contribuent à maintenir les plans qualité.

La communication des informations doit être prédéfinie et documentée. Toutes les parties responsables doivent s'assurer qu'ils sont au courant de la criticité des communications au sein du système global. L'intégrité des informations communiquées en matière de sécurité doit être gérée en fonction de leur niveau de criticité. Ainsi, pour préserver un niveau d'intégrité requis, tous les documents critiques doivent être côtés par un numéro unique mis à jour au fur et à mesure.

Souvent, les acteurs du premier ordre approuvent des difficultés pour se familiariser avec les nouveaux plans élaborés par les concepteurs (acteurs du deuxième ordre). Ces derniers trouvent aussi des difficultés en cas de changement de politique ou d'objectifs globaux par les décideurs du troisième ordre.

Il est indispensable de sensibiliser et informer les employés de l'intérêt stratégique que doit occuper le REX, qui est souvent vue comme un moyen de recherche des responsables pour les sanctionner suite à une faute ou une erreur. En effet, la démarche doit être explicitée clairement au personnel. Les gestionnaires du REX doivent insister sur la préservation de l'anonymat des témoignages afin que l'employé soit rassuré que son témoignage ne constituera pas une charge contre lui.

Certes, le comportement humain présente un aspect difficile à comprendre. Cependant, il revient aux gestionnaires du SMS d'identifier les éléments du système global susceptibles d'être à l'origine d'une mauvaise interprétation pouvant induire un comportement inattendu. Les procédures édictées doivent être claires, simples, et se limiter à l'essentiel, sinon elles sont mal interprétées voire non respectées et se révéleront totalement inefficaces. En effet, si un employé est submergé par des instructions, il sera tenté de faire un tri entre celles qu'il juge justifiées et les autres, au risque de faire le mauvais choix, faute de disposer d'une vision systémique du système global.

10. Formation et qualification

Chaque partie responsable doit s'assurer de l'aptitude de ses employés à accomplir leurs tâches. Ainsi les compétences doivent être évaluées périodiquement et toute déficience doit être remédiée que ce soit par la formation ou par la réaffectation à d'autres missions ou postes convenables.

11. Audit, revue et surveillance

Chaque partie responsable doit mettre en place des procédures régulières d'audit, et de revue du SMS. Elle doit aussi établir des procédures de préparation et de revue de son rapport annuel de sécurité qu'elle adressera ensuite aux autorités compétentes qui statueront sur la conformité de ses indicateurs en matière de sécurité et de qualité.

En outre, les activités critiques doivent être surveillées de près. Il convient donc de :

- Désigner les activités devant être surveillées
- Identifié le type de surveillance : proactive ou périodique
- Définir des méthodes de surveillance des activités
- Evaluer l'efficacité des mesures de contrôle du risque sur les activités
- Evaluer l'efficacité du processus d'analyse de risques

12. Maitrise de la documentation

Le SMS doit être documenté dans toutes ses parties, à commencer par le profil de mission, la répartition des rôles et responsabilités sur l'organigramme cible et l'élaboration de l'annuaire des compétences au sein d'une organisation. En outre, des documents synthétiques doivent indiquer comment la direction assure le contrôle aux différents niveaux de l'organisation, et comment le personnel et sa hiérarchie contribuent à maintenir les plans QHSE[1] (Qualité, Santé, Sécurité, Environnement).

13. Vers un Système de Management Intégré (SMI) de type QHSE

Plusieurs travaux intéressants ont été menés dans différents domaines afin de définir un processus global de SMS. Edwards (Edwards, 2004) propose un schéma décliné directement du SMQ (Système de Management de la Qualité) proposé par la norme ISO 9001. Le consortium Européen SAMNET dont l'objectif était de trouver un consensus entre les acteurs ferroviaires Européens, a proposé une structure générique de SMS en s'inspirant des exigences de la réglementation communautaire et notamment la directive de sécurité [2004/49/CE, 2004].

Néanmoins, il se trouve que la dimension de management des risques ne constitue qu'une pièce parmi d'autres. Autrement dit, le management des risques et notamment la phase d'identification des scénarios d'accident n'a pas explicitement le rôle central.

Les séries ISO 14000 (environnement), ISO 9000 (qualité) et OHSAS 18000 (santé et sécurité – S&ST) forment un trio incontournable dans un SMI (Système de Management Intégré) de type QHSE (Quality – Health & Safety – Environment). En effet, comme elles sont établies sur le même modèle, elles permettent donc une intégration facile des trois systèmes : SMQ (Système de Management de la Qualité), SME (Système de Management de l'Environnement), SMS&ST (Systèmes de Management de la Santé et de la Sécurité au Travail).

L'ISO 9001 ne présente pas d'exigences concernant les produits. Les exigences relatives aux SMQ spécifiées dans cette norme sont génériques et s'appliquent à des organismes de tous secteurs industriels ou économiques, quelle que soit la catégorie de produit.

Quant à elle, la norme ISO 14001 fixe les exigences d'un SME qui met en œuvre et réalise le processus dynamique et cyclique « planifier, mettre en œuvre, contrôler et revoir ». Cette norme est destinée aux maîtres d'ouvrage qui souhaitent mettre en place un SME adapté aux opérations dont ils ont la maîtrise. Elle fournit également les critères et les exigences vérifiables qui peuvent servir à une certification du SME.

Cependant, L'OHSAS 18001 n'est pas une norme, c'est une spécification basée sur le volontariat dans le but de maîtriser les risques sur la santé et la sécurité au travail et d'améliorer les performances. C'est un

[1] Quality – Health & Safety – Environment

référentiel d'évaluation et de certification des SMS&ST, contenant des spécifications pouvant être utilisées par tout organisme quelle que soient sa taille et son implantation.

La compatibilité entre les normes ISO 14001 et ISO 9001 et le référentiel OHSAS 18001 est due à l'approche processus d'amélioration continue, sans établir d'exigences en matière de niveau des performances.

À la base, la plupart des modèles de systèmes de gestion, sinon tous, suivent le cycle d'amélioration continue proposé dans les normes qualité de la famille ISO 9001 et des normes de management de l'environnement ISO 14000. Le cycle d'amélioration est schématisé par la roue PDCA (PFVA en français) de Deming [FD X 50-174, 1998] [FD X 50-173, 1998].

14. Correspondance avec les exigences de la directive ferroviaire de sécurité

La directive de sécurité [2004/49/CE, 2004] dans son Annexe III, consacré au SMS, stipule que :
« Le système de gestion de la sécurité doit être documenté dans toutes ses parties et décrire notamment la répartition des responsabilités au sein de l'organisation du gestionnaire de l'infrastructure ou de l'entreprise ferroviaire. Il indique comment la direction assure le contrôle aux différents niveaux de l'organisation, comment le personnel et ses représentants à tous les niveaux participent et comment l'amélioration constante du système de gestion de la sécurité est assurée »

La structure du SMS proposé en annexe III de la directive de sécurité [2004/49/CE, 2004] est basée sur un retour d'expérience effectué sur plusieurs acteurs ferroviaires Européens. Elle couvre les thèmes suivants :

1. La politique de sécurité de l'organisation
2. les objectifs qualitatifs/quantitatifs de sécurité
3. Plans et procédures pour atteindre ces objectifs
4. Procédure pour répondre aux règles et normes techniques et opérationnelles
5. procédures d'évaluation des risques et méthodes de sélection des mesures de prévention et/ou de protection
6. programmes de formation et de qualification des personnels
7. Procédures de rédaction et prototypes de rapport de sécurité
8. Procédures de capitalisation et de retour d'expérience
9. Procédures de gestion de crises
10. Audit et revue du SMS

Le tableau suivant (voir TAB. 1) présente d'une manière synthétique comment le SMS basé sur la méthode MPR peut accéder aux exigences de la directive européenne de sécurité [2004/49/CE, 2004] :

TAB. 1 : Adéquation entre SMS-centré MPR et les éléments essentiels du SMS proposé par la directive de sécurité 2004/49

Éléments essentiels du système de gestion de la sécurité proposé par la directive de sécurité	Eléments du SMS centré-MPR

2004/49 – Annexe III			
1)	Une politique de sécurité approuvée par le directeur général de l'organisation et communiquée à l'ensemble du personnel ;	SMS	**Profil de mission**
			Politique de sécurité
2)	Des objectifs qualitatifs et quantitatifs de l'organisation en matière d'entretien et d'amélioration de la sécurité ainsi que des plans et des procédures destinés à atteindre ces objectifs ;	SMS	**Gestion des rôles et affectation des responsabilités**
3)	Des procédures pour satisfaire aux normes techniques et opérationnelles existantes, nouvelles et modifiées ou à d'autres prescriptions définies : dans les STI, ou dans les règles nationales visées à l'article 8 et à l'annexe II, ou dans d'autres règles pertinentes, ou dans les décisions de l'autorité, et des procédures pour assurer la conformité avec ces normes et autres prescriptions tout au long du cycle de vie des équipements et des activités;	SMS	**Politique de sécurité** **Gestion des référentiels**
4)	Des procédures et méthodes d'évaluation des risques et de mise en œuvre de mesures de maîtrise des risques chaque fois qu'un changement des conditions d'exploitation ou l'introduction de nouveau matériel comporte de nouveaux risques pour l'infrastructure ou l'exploitation ;	MPR	**R1 : rétroaction – si modification de la conception**
		SMS	**Assurance sécurité**
5)	Des programmes de formation du personnel et des systèmes permettant de veiller à ce que les compétences du personnel soient maintenues et que les tâches soient effectuées en conséquence ;	SMS	**Gestion des rôles et affectation des responsabilités**
			Formation et qualification
6)	Des dispositions garantissant une information suffisante au sein de l'organisation et, le cas échéant, entre les organisations opérant sur la même infrastructure ;	SMS	**Maitrise de la communication**
7)	Des procédures et formats pour la documentation des informations sur la sécurité et la détermination de la procédure de contrôle de la configuration des informations vitales en matière de sécurité ;	SMS	**Maitrise de la documentation**
8)	Des procédures garantissant que les accidents, les incidents survenus ou évités de justesse et les autres événements dangereux soient signalés, examinés et analysés, et que les mesures préventives nécessaires soient prises ;	SMS	**Gestion de la BDD accidents / incidents**
		MPR	**Phases (3, 4, 5, 6, 7, 8): Management des risques**
9)	Des plans d'action, d'alerte et d'information en cas d'urgence, adoptés en accord avec les autorités publiques compétentes ;	SMS	**Gestion des crises (POI, PPI, PPRT)** **Gestion des rôles et affectation des**

			responsabilités
		MPR	**Phase 7 : maitrise des risques –aspects organisationnels** **Phase 7 : maitrise des risques – Décision**
10)	Des dispositions prévoyant un audit interne régulier du système de gestion de la sécurité.	**SMS**	**Audit, revue et surveillance**

15. Correspondance avec le SMQ proposé dans la norme 9001 de la série ISO 9000

La démarche qui s'appuie sur un SMQ incite les organismes à analyser les exigences des clients, à définir les processus qui contribuent à la réalisation d'un produit acceptable pour le client et à en maintenir la maîtrise. Un système de management de la qualité peut fournir le cadre d'amélioration continue permettant d'accroître la probabilité de satisfaire client et autres parties intéressées. Il apporte, à l'organisme et à ses clients, la confiance en son aptitude à fournir des produits qui satisfont immanquablement aux exigences. Les exigences des clients peuvent être spécifiées contractuellement par le client qui, en définitive, détermine l'acceptabilité du produit. Les besoins et attentes des clients n'étant pas figés, et du fait de la pression de la concurrence et des avancées technologiques, les organismes sont amenés à améliorer leurs produits et processus de manière continue.

La structure du SMS- centré MPR possède de nombreux points communs avec le SMQ (voir TAB.2):

TAB. 2 : Adéquation entre le SMS-centré MPR et le SMQ de la norme ISO 9001

Éléments essentiels du SMQ –ISO 9001, ISO 9004			**Eléments du SMS centré-MPR**	
Plan	Responsabilité de la direction	Engagement de la direction Besoins et attentes des parties intéressées	SMS	**Profil de mission**
		Politique qualité	SMS	**Politique de sécurité**
		Planification	SMS	**Profil de mission**
		Responsabilité, autorité et communication		**Gestion des rôles et affectation des responsabilités**
			MPR	**Phases (1 & 2) : découpage systémique du système global**
		Revue de direction	SMS	**Assurance de la sécurité**
		Mise à disposition des ressources	SMS	**Gestion des rôles et affectation des responsabilités**
		Ressources humaines Infrastructures	SMS	**Formation et qualification**

Do	Management des ressources	Environnement de travail Informations Fournisseurs et partenariat Ressources naturelles Ressources financières		
Check	Réalisation du produit	Planification de la réalisation du produit Processus relatif aux parties intéressées Conception & développement	SMS	**BDD accidents/incidents** **Retour d'Expérience**
			MPR	**Phase (2 à 8) + R1 (modification de la conception) + R2 (ajout de fonctions ou de procédures)**
		Achats Production et préparation du service	SMS	**Gestion des crises**
		Maitrise des dispositifs de mesure et de surveillance	SMS	**Maitrise de la communication**
Act	Mesures, analyse et amélioration	Mesures et surveillance Maitrise des non-conformités Analyse de données Amélioration	SMS	**Audit, revue et surveillance**

16. Correspondance avec le SME proposé dans la norme 14001 de la série ISO 14000

Selon les termes de la norme internationale ISO 14001, le SME « est la composante du système de management global qui inclut la structure organisationnelle, les activités de planification, les responsabilités, les pratiques, les procédures, les procédés et les ressources pour élaborer, mettre en œuvre, réaliser, passer en revue et maintenir la politique environnementale ».

Dans la série ISO 14000, on retrouve le principe d'amélioration PDCA, néanmoins la terminologie diffère un petit peu car le cycle est dit PICR pour **P**lan (Planifier), **I**mplement (Implémenter), **C**heck (Vérifier), **R**eview (Revoir).

A l'égard du SMQ, le SMS centré MPR possède également une structure compatible avec le SME (voir TAB. 3):

TAB. 3 : Adéquation entre le SMS-centré MPR et le SME de la norme ISO14001

Éléments essentiels du SME –ISO 14001		**Eléments du SMS centré-MPR**	
Plan	Engagement de la direction	SMS	**Profil de mission**
	Politique environnemental	SMS	**Politique de sécurité**
	Aspects environnementaux Exigences légales et autres	SMS	**Gestion des référentiels**

	Objectifs et critères de performance internes Programme de management environnemental	SMS	**Profil de mission**
		MPR	**Phase (1 & 2) : découpage systémique du système global**
Implement	Structure et responsabilités	SMS	**Gestion des rôles et affectation des responsabilités**
		MPR	**Phase 2 : découpage systémique du sous-système Acteurs**
	Formation, sensibilisation et compétences	SMS	**Formation et qualification**
	Communication	SMS	**Maitrise de la communication**
	Documentation du SME Maîtrise de la documentation	SMS	**Maitrise de la documentation**
	Prévention des situations d'urgence et capacité à réagir	SMS	**Gestion des crises**
Check	Maîtrise opérationnelle	MPR	**BDD accidents/incidents** **Retour d'Expérience**
	Enregistrements	SMS	**Maitrise de la documentation**
	Surveillance et mesurage Non-conformité, action préventive/ action corrective Audit du SME		**Audit, revue, surveillance**
Review	Revue du SME		

17. Correspondance avec le SMS&ST proposé dans la norme 18001 de la série OHSAS 18000

A l'origine l'OHSAS a été élaborée en qualité d'outil pour auditer les entreprises clientes des organismes concepteurs et leur délivrer le cas échéant un certificat sans valeur internationale.

A ce titre, OHSAS 18001 est un référentiel (et non pas une norme internationale) qui résulte d'un travail commun d'un certain nombre d'organismes internationaux de normalisation et de certification. Il recense et capitalise toutes les spécifications propres à chaque organisme certificateur sur le thème du management de la santé et de la sécurité au travail.

Sa mise en œuvre est dépendante d'un contexte de santé et de sécurité au travail complexe, parfois précaire, évolutif comportant des risques de plus en plus grands.

L'OHSAS 18001 est très largement calquée sur l'ISO 14001 dans la structure logique et dans la terminologie. A ce titre, l'OHSAS paraît un outil adapté et complémentaire pour une entreprise souhaitant mettre en œuvre un système de management intégré (SMI).

Elle permet à un organisme d'établir, mettre en œuvre et entretenir et améliorer un SMS&ST, ensuite mettre en œuvre, entretenir et améliorer un tel système en s'assurant d'abord de sa conformité à la politique S&ST adoptée.

Les éléments du SMS-centré MPR sont compatibles avec les éléments essentiels du SMSS de la série OHSAS 18000 (voir TAB. 4):

TAB. 4 : Adéquation entre le SMS-centré MPR et le SMSS du référentiel OHSAS 18001

Éléments essentiels du SMSS – OHSAS 18001		**Eléments du SMS centré-MPR**	
Plan	Engagement de la direction	SMS	**Profil de mission**
	Politique OH&S (santé et sécurité)	SMS	**Politique de sécurité**
	Exigences légales et autres	SMS	**Gestion des référentiels**
	Objectifs et Programme(s)	SMS	**Profil de mission**
		MPR	**Phase (1 & 2) : découpage systémique du système global**
Implement	Ressources, rôles, responsabilité et autorité	SMS	**Gestion des rôles et affectation des responsabilités**
		MPR	**Phase 2 : découpage systémique du sous-système Acteurs**
	Compétences, formation et sensibilisation	SMS	**Formation et qualification**
	Communication, participation et consultation	SMS	**Maitrise de la communication**
	Documentation Maîtrise de la documentation	SMS	**Maitrise de la documentation**
	Maîtrise opérationnelle	MPR	**BDD accidents/incidents** **Retour d'Expérience**
	Prévention des situations d'urgence et capacité à réagir	SMS	**Gestion des crises**
Check	Investigation des incidents	MPR	**Phases (3, 4, 5, 6, 7, 8): Management des risques**
	Maitrise des enregistrements	SMS	**Maitrise de la documentation**
	Surveillance et mesurage de la performance Non-conformité, action préventive/ action corrective Audit du SMSS		**Audit, revue, surveillance**

Review	Revue du SMSS		

BIBLIOGRAPHIE

AQS-GT OORS. (Mars 1996). *Management de la sécurité d'entrepreise, vocabulaire et concept.* Association Qualité-Sécurité (AQS) pour l'Observatoire de l'Opinion sur les Risques de la Sécurité.

Argyris, C. (Septembre 1976). Single-Loop and Double-Loop Models in decision Making. *Administrative Science Quarterly* , Vol 21, pp 363-.

Aubry, J.-F. (2005). *Glossaire des termes relatifs aux Automates Programmables Industriels dédiés à la Sécurité.*

Aumas, M. (1996). *Plates-formes élévatrices mobiles de personnel.* Paris: INRS.

Barbet, J.-F. (Mars 1996). Maîtriser les risques. *Journal Préventique et Sécurité* .

Bellamy, L., & Van Der Schaff, J. (2000). *Major Hazard Management: Technical-Management Links and the AVRIM2 Method. Seveso 2000 – Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive Seveso II.* Athens: European Commission, Joint Research Centre, Major Accident Hazard Bureau.

Bergadaà, M., Chandon, J.-L., & Chebat, J.-C. (1984). Le temps comme intrant des attitudes á l'égard de la sécurité routière. *Revue d'Analyse Économique* , Vol 60, n°4, pp 495-513.

Bertalanffy, L. (Décembre 1972). The History and Status of General Systems Theory. *The Academy of Management Journal* , Vol. 15, No. 4, General Systems Theory, pp 407-426.

Bouchet, S. (2001). *Analyse des risques et prévention des accidents majeurs : Présentation des méthodes d'inspection TRAM, NIVRIM et AVRIM2.* INERIS, Direction des Risques Accidentels, Unité prévention.

Brandom, R. (1988). Inference, Expression and Induction. *Philosophical Studies Kluwer Academic Publishers* , Issue 54, pp 257-285.

Brenac, T., Nachtergaele, C., & Reiner, H. (2003). *Scénarios types d'accidents impliquant des piétons et éléments pour leur prévention, Rapport INRETS n°256.*

BSI 8800. (2004). *Occupational health and safety management system - Guide.* England: BSI.

BSI OHSAS 18001. (2005). *Occupational Health and Safety Management Systems – Specification.* England: BSI.

Bück, J.-Y. (1999). *Le management des connaissances: mettre en oeuvre un projet de knowledge management.* Paris: Editions d'Organisation.

CEI 1050. (Février 1991). *Transformateurs pour lampes tubulaires à décharge ayant une tension secondaire à vide supérieure à 1 000 V - (couramment appelés transformateurs-néon): Prescriptions générales et de sécurité.* CEI.

CEI 108. (1994). *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité.* CEI.

CEI 300-3-9. (1995). *Gestion de la sûreté de fonctionnement.* CEI.

CEI 50(191). (1990). *International Electro-technical Vocabulary, Chapter 191: Dependability and quality of service.* CEI.

CEI 60300. (Août 1996). *Gestion de la sûreté de fonctionnement.* CEI.

CEI 60812. (Janvier 2006). *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des Modes de défaillance et de leurs effets (AMDE).* CEI.

CEI 61069. (1996). *Mesure et commande dans les processus industriels - Appréciation des propriétés d'un système en vue de son évaluation - Parti 5: Evaluation de la sûreté de fonctionnement d'un système.* CEI.

CEI 61882. (Mai 2001). *Etudes de danger et d'exploitabilité (études HAZOP), Guide d'application.* CEI.

Center For Chemical Process Safety. (1993). *Guidelines for Auditing Process Safety Management Systems.* New York: American Institute of Chemical Engineers.

Chapman, C., & Ward, S. (2003). *Project Risk Management: Processes, Techniques and Insights. Second edition.* Southampton, UK: John Wiley & Sons Ltd.

Charlet, J., Zacklad, M., Kassel, G., & Bourigault, D. (2000). *Ingénierie des connaissances, évolutions récentes et nouveaux défis.* Eyrolles.

Chorafas, D. (2004). *Operational Risk Control with Basel II - Basic principles and capital requirements.* Elsevier Butterworth-Heinemann.

Christian, P. (2002). *L'Europe ferroviaire est-elle sur la bonne voie ?* les documents d'information de l'assemblée nationale, n° 388.

Circulaire DPPR/SEI2/CB-06-0388. (2006). *mise à disposition du guide d'élaboration et de lecture des études de dangers pour les établissements soumis à autorisation avec servitudes et des fiches d'application des textes récents.* DPPR.

Code de l'Environnement: Article L. 511-1. (17 janvier 2001). *Loi n° 2001-44 du 17 janvier 2001 art. 11.* Journal Officiel de la république française.

Cooper, D., Grey, S., Raymond, G., & Walker, P. (2005). *Project Risk Management Guidelines: Managing risk in large projects and complex procurements.* England: John Wiley & Sons, Ltd.

Cox, L.-A. (2008). What's wrong with risk matrices? *Journal of risk analysis* , Vol. 28, No. 2, pp 497-512.

Cox, S., & Tait, R. (1998). *Safety, Reliability and Risk Management: an integrated approach. Second edition.* Butterworth-Heinemann, Reed Educational and Professional Publishing Ltd.

Dankel, A., & Gonzales, D. (1993). *The enginneering of knowledge-based systems, theory and practice.* New Jersey: Prentice Hall, Englewood Cliffs.

Davies, J., Fensel, D., & Van Harmelen, F. (2003). *Towards the Semantic Web: Ontology-driven Knowledge Management.* England: John Wiley & Sons, LTD.

De Rosnay, J. (1977). *Le macroscope: vers une vision globale. Points Essais n°80.* Paris: Points.

De Saussure, F. (1913). *Cours de linguistique générale.* Payot.

Décret n° 2003-425. (9 mai 2003). *Décret n° 2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés* .

Dekker, S. W. (2005). *Human Factors in Transportation: Ten Questions About Human Error, A new view of human factors and system safety.* Lawrence Erlbaum Associates Publishers.

Dellobel, C., & Adiba, M. (1985). *Base de données et systèmes relationnels.* Dunod.

Desroches, A. (2005). L'Analyse Préliminaire des Risques. *Qualita'2005* . Bordeaux, France.

Desroches, A., Leroy, A., & Vallée, F. (2005). *La gestion des risques.* Lavoisier.

Dhillon, B. (2005). *Reliability, Quality, and Safety for Engineers.* Florida, USA: CRC Press LLC.

Dialo, G. (2006). *Une architecture à Base d'Ontologies pour la Gestion Unifiée des Données Structurées.* Grenoble: Thèse de doctorat, Université Joseph Fournier.

Dillenbourg, P., & Martin-Michielot, S. (1995). *Le rôle des techniques d'Intelligence artificielle dans les logiciels de formation.* CBT, Learntec.

Directive 1995/18/CE. (27 juin 1995). *Directive 1995/18/CE du Conseil du 19 juin 1995, concernant les licences des entreprises ferroviaires.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 2001/16/EC. (19 mars 2001). *Directive of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 2004/49/EC. (29 avril 2004). *Directive of the European Parliament and of the Council on safety on the Community's railways.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 96/48/EC. (23 juillet 1996). *Directive of the European Parliament and of the Council on the interoperability of the trans-European high-speed rail system.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Directive 96/82/EC (SEVESO II). (9 décembre 1996). *European directive on the control of major-accident hazards involving dangerous substances.* Brussels: Official Journal of the European Union, Commission of the European Communities.

Doucet., F., Gauthier, P., & Turcotte, J.-P. (2004). *Etude de cas : Application de la démarche d'analyse et de maîtrise du risque au projet McGro.* Université de Sherbrooke, université de quebec à trois rivières.

Durka, E., & Fae, J.-L. (2000). *Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels, Rapport final.* INERIS, Direction des Risques Accidentels.

Durka, E., & Fae, J.-L. (2000). *Sûreté fonctionelle des systèmes dédiés à la sécurité, Rapport final.* INERIS - Direction des Risques Accidentels.

Edwards, A.-J. (2004). *ISO 14001 Environmental Certification Step by Step.* Elsevier.

El-Koursi, E., Mitra, S., & Bearfield, G. (2007). Harmonizing Safety Management Systems in the European Railway Sector. *Safety Science Monitor* , Issue 2, Vol 11, 1-14.

El-Koursi, E.-M., Fletcher, S., Tordai, L., & Rodriguez, J. (2006, February). Safety and interoperability. *SAMNET synthesis report* .

EN 292/ISO 12100. (1995). *Sécurité des machines ; Notions fondamentales, principes généraux de conception.* ISO/CEN.

Faber, M., & Stewart, M. (2003). Risk assessment for civil engineering facilities: critical overview and discussion. *Reliability Engineering and System Safety* , Issue 80, pp 173–184.

Fadier, E. (2000). Les pratiques françaises en matière de sûreté de fonctionnement. *Congrès Lambda Mu 12* .

FD X 50-173. (1998). *Principes, acteurs et bonnes pratiques - Guide d'auto-évaluation.* AFNOR.

Flanagan, R., & Norman, G. (1993). *Risk Management and Construction.* Blackwell Science Ltd.

Gallou, G., & Bouchon-Meunier, B. (1992). *Systémique : Théorie & Application.* France: Lavoisier.

Gardarin, G. (1998). *Bases de données: les systèmes et leurs langages.* Eyrolles.

Goffin, L. (1976). *Environnement et évolution des mentalités.* Arlon, Belgium: Thèse de doctorat, FUL.

Gouriveau, R. (2003). *Analyse des risques – Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision.* Thèse de Doctorat, Institut National Polytechnique de Toulouse.

Green, P., & Rosemann, M. (2005). *Business systems analysis with ontologies.* Australia: Idea Group Publishing.

Greuning, H. V., & Bratanovic, S. (Avril 2003). *Analysing and managing banking risk - A framework for assessing corporate governance and finantial risk. Second edition.* Washington, D.C., USA: The world bank.

Grüber, T.-R. (1993). *A translation approach to portable ontologies. Knowledge Acquisition.*

Grüber, T.-R. (1992). *Ontolingua : A mechanism to support portable ontologies.* Standford University, Knowledge Systems Laboratory.

Grüber, T.-R. (1995). Towards principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies* .

Grüber, T.-R., & Thomas, R. (1993). *Towards principles for the Design of Ontologies Used for Knowledge sharing in formal Ontology in conceptual Analysis and Knowledge Representation.* Kluwer Academic Publishers.

GT 7 - CEI. *Enseignement - Terminologie.* CEI.

GT Aspects sémantiques du risque. (1997). *Vocabulaire lié au risque à travers une analyse bibliographique.* Institut de Protection et de Sûreté Nucléaire (IPSN) - Observatoire de l'Opinion sur les Risques et la Sécurité.

GT Méthodologie. (2003). *Principes généraux pour l'élaboration et la lecture des études de dangers.* INERIS.

GTR 55. (2000). *Les analyses préliminaires de risques appliquées aux transports terrestres guidés.* Institut de Sûreté de Fonctionnement - Collège sécurité.

Guarino, N. (1998). *Some ontological principles for designing upper level lexical resources.* IOS Press.

Hanquiez, A. (2003, Juillet). Evaluation des risques: les résultats dans un document unique. *Techniques de l'ingénieur* .

Hartolou, D., Bouchet, S., & Salvi, O. (2003). Mieux démontrer la maîtrise des risques industriels. *Revue Phoebus no. 27* .

Heurtel, A. (2003). *La gestion des risques techniques et des risques de management.* CNRS - IN2P3/LAL.

HMSO. (1995). *A guide to Risk Assessment and Risk Management for Environmental Protection.* England: Her Majesty's Stationery Office.

Horton, I. (2006). *Beginning Visual C++ 2005.* USA: Wiley Publishing Inc. .

HSE. (1992). *Generic terms and concepts in the assessment and regulation of industrial Risks.* UK: Health and Safety Executive.

HSE. (Février 1998). *Health and safety policies and risk assessment in agriculture.* UK: Health and Safety Executive.

HSE. (2001). *Proposed framework for addressing human factors in IEC 61508.* UK: Health and Safety Executive.

HSE. (2001). *Safety culture maturity model, Offshore technology report.* UK: Health and Safety Executive.

IAEA Safety glossary. (2007). *Teminology used in nuclear safety and radiation protection.* International Atomic Energy Agency.

ICAO. (1990). *Manual Concerning Safety Measures Relating to Military Activities Potentially Hazardous to Civil Aircraft Operations.* International Civil Aviation Organization.

ICAO. (2006). *Safety Management Manual (SMM).* International Civil Aviation Organization.

INERIS-DRA ARAMIS. (2004). *ARAMIS: Développement d'une méthode intégrée d'analyse des risques pour la prévention des accidents majeurs.* Ministère de l'Ecologie et du Développement Durable - INERIS.

INERIS-DRA. (2003). *Outils d'analyse des risques générés par une installation industrielle.* INERIS, Direction des Risques Accidentels.

INRS. (2004). *Evaluation des risques professionnels: Questions-réponses sur le document unique.* Institut National de Recherche et de Sécurité.

ISO 14001. (Novembre 2004). *Systèmes de management environnemental - exigences et lignes directrices pour son utilisation, 2 éme édition.* Paris: ISO.

ISO 14971. (2000). *Application de la gestion des risques aux dispositifs médicaux.* ISO.

ISO 21127. (Août 2002). *Information and documentation — A reference ontology for the interchange of cultural heritage information.* ISO.

ISO 9000. (Décembre 2000). *Systèmes de Management de la Qualité - Principes essentiels et vocabulaire.* ISO.

ISO/CEI 9126-1. (June 2001). *Software engineering - Product quality - Quality model.* ISO/CEI.

ISO/CEI Guide 2. (1986). *Termes généraux et leurs définitions concernant la normalisation et les activités connexes.* ISO.

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). *Management du risque – Vocabulaire – principes directeurs pour les inclure dans les normes.* ISO/CEI.

Joly, C., & Vallee, A. (2004). *Analyse des risques et prévention des accidents majeurs: Synthèse vis-à-vis de l'étude de danger.* INERIS-Direction des Risques Accidentels.

Kahneman, D., & Tversky, A. (Mars 1979). Prospect theory:An analysis of decision under risk. *Econometrica* , Vol 47, Issue 2, pp 263-292.

Kaufmann, A., Grouchko, D., & Cruon, R. (1975). *Modèles mathématiques pour l'étude de la fiabilité des systèmes.* Masson & Cie.

Kerven, G.-Y., & Rubise, P. (2001). *L'archipel du danger - Introduction aux cindyniques.* Paris: Eyrolles.

Kerzner, H. (2001). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling, seventh edition.* Ohio, USA: John Wiley & Sons, Inc.

Krishnan, S., & Singh, M. (2002). *Strategic Human Resource Management: Three-Stage Process And Influencing Organisational Factors.* Indian Institute of Management.

Laprie, J.-C. (2002). *Guide de la Sûreté de Fonctionnement.* Cepaduès .

Laprie, J.-C. (1994). *La modélisation des systèmes informatiques : concepts de base et terminologie - , rapport n° 94448.* Toulouse: LAAS.

Larousse. (2006). 38 dictionnaires et recueils de correspondances en CD ROM.

Larousse. (2006). Larousse Définitions.

Larousse. (2005). Larousse Expression.

Laudon, K., & Laudon, J. (2001). *Les systèmes d'information de gestion : organisations et réseaux stratégiques.* Editions du Renouveau Pédagogique.

Laurant, A. (2003). *Sécurité des procédés chimiques.* Lavoisier.

Le Moigne, J.-l. (1994). *Théorie du Système Général, théorie de la modélisation.* Paris: PUF.

Leveson, N. (Juin 2002). *A New Approach To System Safety Engineering.* Massachusetts, USA: Aeronautics and Astronautics Massachusetts Institute of Technology.

Lievens, C. (1976). *Sécurité des systèmes.* Cépaduès.

Macdonald, D. (2004). *Practical Machinery Safety.* Elsevier.

Manesh, K. (1996). *Ontology development for machine translation: Ideology and methodology. Memoranda in computer and cognitive science.* New Mexico State University, Computing Research Laboratory, Las Cruses, New Mexico.

Marsot, J. (1998). Nacelles élévatrices de personnel - Etude des schémas de commande. *Cahiers de notes documentaires - Hygiène et sécurité du travail - N°171, 2e trimestre 1998, INRS* .

Martin, W., Lippitt, J., & Webb, P. (2000). *Hazardous Waste Handbook for health and safety, 3rd edition.* Butterworth–Heinemann - Elsevier group.

Maslow, A. (1943). A Theory of Human Motivation. *Psychological Review* , Issue 50, pp 370-396.

Mazouni, M.-H. (2006, Avril). Concepts et terminologie de base pour l'Analyse Préliminaire des Risques dans le transport ferroviaire. *Communiquer, Naviguer, Surveiller-Innovations pour des transports plus sûrs, plus efficaces et plus attractifs* , Actes INRETS no. 109, pp 143-152.

Mazouni, M.-H. (2007, Avril). Modélisation générique des scénarios d'accident dans le but d'harmoniser les APRs. *Communiquer, naviguer,surveiller - Innovations pour des transports plus surs* , Actes INRETS n° 112, pp 17-27. Actes INRETS.

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, M.-H., & Hadj-Mabrouk, H. (2005, Avril). L'analyse des risques d'accidents dans les transports ferroviaires. Québec-Laval.

Mazouni, M.-H., & Hadj-Mabrouk, H. (2005, Décembre). Méthode et formalisme de base pour l'Analyse Préliminaire des Risques appliquée dans le transport ferroviaire. *6e Conférence internationale des sciences et des techniques de l'automatique (STA'2005)* . Sousse, Tunisie.

Mazouni, M.-H., & Hannachi, H. (1999). *Réalisation d'une interface graphique sous XWindow pour le SGBD Postgres. Mémoire d'ingénieur d'état en informatique, option Systèmes Informatiques* . Alger: Institut National d'Informatique.

Mazouni, M.-H., Aubry, J.-F., & El koursi, 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, 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.

McAmis, D. (2004). *Professional Crystal Reports for Visual Studio .NET. Second edition.* Indianapolis - USA: Wiley Publishing, Inc.

Mémorandum n°9. (1994). *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité.* CENELEC.

MIL-STD-1629A. (24 Novembre 1980). *Procedures for performing a failure Mode, Effects and Criticality Analysis.* Washington, D.C.: Department of Defense, USA.

MIL-STD-882C. (19 Janvier 1993). *System Safety Program Requirements.* Washington, D.C., USA: Department of Defense.

MIL-STD-882D. (10 February 2000). *Standard Practice For System Safety.* Washington, D.C., USA: Department of Defense.

Ministère de l'écologie et du développement durable . (29 septembre 2005). *Arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des ICPE* . Journal officiel de la république française.

Molak, V. (1997). *Fundamentals of Risk Analysis and Risk Management.* Ohio, USA: Lewis Publishers.

Mollah, A. (2005, Novembre). Application of Failure Mode and Effect Analysis (FMEA) for Process Risk Assessment. *Focus on Project Management* .

Monteau, M., & Favaro, M. (1990). *Bilan des méthodes d'analyse à priori des risques.* INRS.

Morin, E. (1977). *La Méthode, 1 : la nature de la nature ; 2 : la vie de la vie.* Le Seuil.

Mortureux, Y. (2002, Août). La Sûreté de fonctionnement: méthodes pour maîtriser les risques. *Techniques de l'ingénieur* .

NASA. (Mars 1999). *System Safety Handbook.* California, USA: Dryden Flight Research Center, NASA.

NEA - OECD. (2005). *Gestion des déchets radioactifs: Vers la réalisation d'un dossier de sûreté - Rapport de synthèse préparé au nom du WPDD par son Groupe d'étude sur l'analyse du dossier de sûreté de démantèlement. Rapport n° 6073.* Paris: Agence pour l'Energie Nucléaire - Organisation de Coopération et de Développement Économique.

NF EN 280. (2001). *Plates-formes élévatrices mobiles de personnel. Calculs, stabilité, construction. Sécurité, examen et essais.* Paris: AFNOR.

NF EN 280/A1. (2004). *Plates-formes élévatrices mobiles de personnel. Calculs de conception, Critère de stabilité, Construction.* Paris: AFNOR.

NF EN 50126. (Janvier 2000). *Applications ferroviaires : Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).* Paris: AFNOR.

NF EN 50128. (Juillet 2001). *Applications ferroviaires : Systèmes de signalisation, de télécommunication et de traitement, Logiciels pour systèmes de commande et de protection ferroviaire.* Paris: AFNOR.

NF EN 50129. (Mai 2003). *Applications ferroviaires : Systèmes de signalisation, de télécommunication et de traitement, Systèmes électroniques de sécurité pour la signalisation.* Paris: AFNOR.

NF EN 60204. (Avril 1998). *Sécurité des machines.* Paris: AFNOR.

NF EN 61508. (Décembre 1998). *Sécurité fonctionelle des systèmes électriques et électroniques programmables relatifs à la sécurité.* Paris: AFNOR.

NF EN 61511. (Mars 2005). *Sécurité fonctionnelle - systèmes instrumentés de sécurité pour le secteur des industries de transformation* . CENELEC.

NF EN ISO 9001. (Décembre 2000). *Systèmes de management de la qualité.* Paris: AFNOR.

Noy, N. F., & Hafner, C. (1997). *The State of the Art in Ontology Design.* The American Association for Artificial Intelligence.

OHSAS 18001. (2007). *Occupational Health and Safety Management Systems - Requirements.* OHSAS.

Perilhon, P. (1999). *Du risque à l'analyse des risques, développement d'une méthode MOSAR.*

Perilhon, P. (2000). Eléments méthodiques. *Phoebus no.12* .

Périlhon, P. (2003, Septembre). MOSAR : Présentation de la méthode. *Techniques de l'ingénieur* .

Perpen, J.-L. (2000). *Définition et réalisation d'une application orientée objet pour la maîtrise du processus de coupe - Thése de Doctorat en mécanique.* Université Bordeaux I.

Perrow, C. (1984). *Normal accident - living with High-Risk technologies.* Basic Books, Harper Torchbooks.

Peters, T. (1988). *Thriving on chaos.* London: MacMillan Ltd.

Petit Robert. (1984). *Dictionnaire.* Paris.

Pr NF ISO 31000. (Juin 2008). *management du risque: principe et lignes directrices de mise en oeuvre.* Paris: AFNOR.

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society.* Karlstad-Suède: Swedish Rescue Services Agency.

RE. Aéro 701 11 . (Novembre 1986). *Recommandations pour les études de l'industrie aérospatiale - Guide des méthodes courantes d'analyse de la sécurité d'un système missile ou spatial.* Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE).

Reason, J., & Parker, D. (1993). *Managing the human factor in road safety.* Maatschappij: The Hague: Shell International Petroleum.

Roche, C. (2005). Ontologie et Terminologie. *Larousse - Revue* , n° 157, pp 1-11.

Safety Regulation Group. (Janvier 2002). *An Introduction to Aircraft Maintenance Engineering Human Factors for JAR 66, Civil Aviation Authority (CCA).* UK: Documedia Solutions Ltd.

Sallak, M., Simon, C., & Aubry, J.-F. (2007). A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems* .

SAMRAIL Consortium. (Septembre 2003). *Analysis of existing approaches, D 2.1.1 report.* European Commission and SAMRAIL partners.

SAMRAIL Consortium. (Septembre 2004). *Common safety methods, D 2.3 report.* European Commission and SAMRAIL partners.

Saoulé, B. (2002). *Les risques en station de ski alpin : d'une explication monocausale à une perspective d'analyse systèmique.*

Secrétariat Général du Gouvernement. (2002, Janvier 8). *Arrêté d'application du décret n°2000-286 relatif à la sécurité du réseau ferré national*. Récupéré sur LégiFrance, Le service public de diffusion du droit: http://www.legifrance.gouv.fr

Secrétariat Général du Gouvernement. (2000, Mars 30). *Décret n°2000-286 relatif à la sécurité du réseau ferré national*. Récupéré sur LégiFrance, Le service public de la diffusion du droit: http://www.legifrance.gouv.fr/

Senge, P. (1990). *The Fifth Discipline: The Art & Practice of The Learning Organization.*

Solter, N., & Kleper, S. (2005). *Professional C++*. USA: Wiley Publishing, Inc.

Sowa, J. (1984). *Conceptual structures: Information processing in mind and machine - The system Programming series.* Wesley Publishing Inc.

Sowa, J. (2000). *Knowledge representation : logical, philosophical and computational foundations.* Paci_c Grove, CA, USA: Brooks/Cole Publishing.

Sripriya, & Kishore, S. (2002). *Microsoft Visual C++ .NET Professional Projects.* USA: Premier Press, Inc.

TECSSS. (Août 2002). *System Safety: A Science and Technology Primer.* The New England Chapter of the System Safety Society.

Tordai, L. (June 2005). *Common Safety Targets and Common Safety Indicators, Report D.1.2.3.*

Tourigny, N. (1998). *Systèmes d'aide à l'étude de la sécurité routière - Vers des outils hybrides, ouverts et intelligents* .

US Navy. (2003). *Naval Safety Supervisor.* USA: Naval Education and training Professional Development and Technology Center.

Van Elslande, P., Alberton, L., Nachtergaele, C., & Blanchet, G. (1997). *Scénarios types de production de l'erreur humaine dans l'accident de la route : problématique et analyse qualitative, Rapport INRETS n°218.* Paris: lavoisier.

Van Heijst, G., Schreiber, A., & Wielinga, B. (1997). Using explicit ontologies in kbs development. *International Journal of Human-Computer Studies* , 46(2/3), pp 183-292.

Van Heijst, G., Van Der Spek, R., & Kruizinga, E. (1996). Organizing corporate memories. *10th Banff knowlegde acquisition for knowledge based systems workshop - KAW'96* . Canada.

Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels.* Eyrolles.

Whittingham, R. (2004). *The Blame Machine: Why Human Error Causes Accidents.* Oxford: Elsevier Butterworth-Heinemann.

Wideman, R. (1992). *Project and Program Risk Management: A guide to Managing Project Risks and Opportunities.* Pennsylvania, USA: The Project Management Institute.