Méthode systémique et organisationnelle d'Analyse Préliminaire des Risques basée sur une ontologie générique

Mohamed Habib Mazouni, Jean-François Aubry, El Miloudi El Koursi

3 S G S '0 8
WORKSHOP SURVEILLANCE, SÛRETÉ ET SÉCURITÉ DES GRANDS SYSTÈMES
UNIVERSITÉ DE TECHNOLOGIE DE TROYES 4 & 5 JUIN 2008

Méthode systémique et organisationnelle d'Analyse Préliminaire des Risques basée sur une ontologie générique

Mohamed Habib MAZOUNI[1,2] Jean-François AUBRY[1] El Miloudi EL KOURSI[2]

[1] - *Centre de Recherche en Automatique de Nancy (CRAN-ENSEM-INPL)*
[2] - *Institut National de Recherche sur les Transports et leur Sécurité (INRETS- ESTAS)*

Résumé – L'analyse Préliminaire des Risques (APR) a été développée au début des années 60 dans les domaines aéronautiques et militaires. C'est aujourd'hui la pierre angulaire du Système de Management de la Sécurité (SMS) dans de nombreuses industries.

Quasiment cinq décennies écoulées, mais la pratique d'APR accuse toujours une mauvaise compréhension. Une enquête[1] réalisée par l'INRS auprès de 220 experts de la sûreté de fonctionnement, révèle que 81% des experts disent utiliser l'APR, et seulement 9% d'entre eux considèrent qu'ils la maitrise. En effet, cette révélation surprenante est justifiée compte tenu les 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 toute sorte de divergence.

Dans une démarche de résolution des difficultés constatées, nous proposons la méthode Management Préliminaire des Risques (MPR) basée sur un processus accidentel 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) sur un point d'ancrage essentiel qu'est la gestion des processus techniques et organisationnels.

Notre objectif est triple, d'abord montrer les 10 difficultés majeures que nous avons constatées en matière de management des risques, ensuite présenter la méthode MPR que nous proposons pour résoudre ces difficultés dans le but d'exploiter efficacement l'échange de savoir-faire en matière de management des risques relatifs à différents systèmes voire issus de différents domaine, et enfin présenter de manière synthétique l'outil SIGAR (Système Informatique Générique d'Analyse de Risque) dédié à cette méthode.

Abstract – The Preliminary Hazard Analysis (PHA) was developed at the beginning of the sixties in the aeronautical and military fields. Since then, it has been used in many other industries and it becomes the cornerstone of the Safety Management System (SMS) building.

Almost five decades later, no generic model has been provided. An investigation carried out by the INRS among 220 RAMS experts, reveals that 81% of the experts practice the PHA, but only 9% of them consider their practice reasonably well. Indeed, this surprising revelation is justified regarding the many methodological, terminological, technical or organisational difficulties that we could identify. Consequently, the practice of the PHA remains problematic and completely beyond any harmonization optics.

In a step of resolution of the noticed difficulties, we propose the PRM (Preliminary Risk Management) method that would be based on a generic accidental process allowing to channel the mechanisms of capitalization and exploitation of knowledge relating to the accident scenarios (causality, entities, situations, events, etc). The PRM method is attached to the Safety Management System (SMS) via the management of the technical and organisational processes.

The purpose of this work is firstly to show the 10 difficulties in risk management that we have noticed, and secondly to deal with these difficulties through the proposal of the Preliminary Risk Management (PRM) method in order to enforce the pertinence of the hazard analysis regarding its predominant status in the SMS (Safety Management System). These proposals had been concretized through the development of an Interactive Decision-Making System (IDMS) in order to perform a complete assisted-analysis-process through an ergonomic GUI (Graphical User Interface).

[1] Les pratiques françaises en matière de sûreté de fonctionnement - Elie FADIER – INRS [4]

1. Introduction

La pratique d'Analyse Préliminaire de Risques est très diversement perçue [5]. Il faut d'abord remarquer que dans la majorité des cas, il s'agit d'Analyses Préliminaire de Dangers (APD), car on considère surtout la gravité des accidents, mais non pas les probabilités d'occurrence ; on devrait donc parler d'APD, que d'ailleurs les anglo-saxons dénomment « Preliminary Hazard Analysis (PHA) ».

Selon la norme CEI 300-3-9 [1], 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 plutôt que d'analyse des risques !

En effet, notre démarche MPR consiste à identifier les entités dangereuses d'un système étudié, puis à regarder pour chacune d'elles comment elles pourraient dégénérer en un incident ou un accident plus ou moins grave suite à une séquence d'événements causant une situation d'accident.

Pour identifier les entités et les situations d'accident 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.

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.

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

2. 10 préoccupations en matière de management des risques

2.1. Difficulté de définition du système et de son environnement

Il est évident que les spécialistes de la linguistique ont abordé le concept de système avec intérêt. Néanmoins, l'usage dans la pratique des définitions diverses et variées demeure une tâche fastidieuse.

Par conséquent, il est impératif de spécifier les deux parties structurelle et fonctionnelle du système et de spécifier clairement les différentes interrelations entre ces deux parties avec les différentes composantes de l'environnement.

2.2. Divergence des termes et des concepts

La linguistique 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.

En effet, nous avons pu constater que les différents acteurs industriels ont un sérieux problème dans l'usage des termes relevant du management des risques. Nous pouvons à titre d'exemple citer les difficultés syntaxique et sémantique suivantes :

- Association d'un même terme à plusieurs concepts, c-.à-.d le même terme renvoie souvent vers différents concepts,
- Association d'un même concept à plusieurs termes, c-.à-.d le même concept est parfois représenté par différents termes,
- Nuance des liens entre les différents concepts,
- Définition sommaire des termes sous forme de glossaires, souvent présentés par ordre alphabétique,
- Absence de rattachement au processus accidentel, c.-à-d. à quelle phase se situe un concept donné et quelle peut être sa contribution dans la réalisation de l'accident,
- Confusion entre les notions d'état et de transition,
- Usage excessif du descriptif littéraire, 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 dus à 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 Dangers) » et « APR (Analyse Préliminaire de Risques) » qui est le nom le plus répandu même s'il est le moins conforme aux normes, en l'occurrence ISO/CEI Guide 51 [9] et Guide 73 [10], précisant que dans une analyse de risques, on commence toujours par identifier les dangers et on fini par estimer les risques inhérents.

2.3. Divergence des Objectifs de Sécurité

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 d'acceptabilité et celles de tolérabilité.

Dans le monde industriel, on retrouve 3 approches principales autour desquelles s'est développé un certain nombre d'approches dérivées [3]. Ces approches sont le GAME français, l'ALARP britannique et le MEM allemand :

Principe GAME (Globalement Au Moins Equivalent) **:** 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.
Principe ALARP (As Low As Reasonably Practicable): Tout système possède une certaine probabilité de défaillance. Le principe ALARP consiste à évaluer le risque (gravité, fréquence) que représente cette occurrence, ceci, en intégrant le coût de la mise en œuvre des actions de réduction.

Principe MEM (Mortalité Endogène Minimale) **:** Il existe un «risque ambiant» que vit quotidiennement chaque individu, ce risque est calculé en fonction de l'espérance de vie. En effet, tout nouveau service mis à la disposition de l'usager ne doit pas faire augmenter notablement le risque ambiant.

2.4. Divergence des Indicateurs de Sécurité

Les niveaux de gravité et de probabilité d'occurrence sont généralement 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.

Cependant, les approches de classification par intervalle véhiculent une forte subjectivité, et plus particulièrement en ce qui concerne l'estimation des risques. 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.

2.5. Divergences d'ordre méthodologique

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, deux axes d'investigation des relations cause / effet sont explorables :

- L'approche causale inductive : c'est la démarche directe, on part d'une certaine connaissance sur les causes et on cherche à prédire les effets correspondants.
- L'approche causale déductive : c'est la démarche inverse, on part d'une certaine connaissance sur les conséquences et on essaye d'identifier les causes qui sont à l'origine.

2.6. Absence de suivi des risques

L'estimation à postériori des risques permet d'apporter une assurance quant à l'efficacité des mesures de réduction envisagées. Autrement dit, au fait que l'engagement d'une quelconque action tire le risque vers le bas, et que la sécurité obtenue n'est pas pire que ce qu'elle l'était avant cette mise en œuvre.

2.7. Enjeux organisationnels de la gouvernance des risques

La mise en œuvre des barrières de défense requises doit se baser sur des techniques scientifiques et organisationnelles de management du personnel. 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 dépit de la responsabilité technique, il existe une deuxième forme, en l'occurrence la responsabilité hiérarchique. Cette deuxième forme consiste en l'approbation ou le refus des actions de contrôle recommandées par l'équipe technique affectée au suivi du risque.

2.8. Enjeux d'interopérabilité : harmonisation des APRs système

L'une des préoccupations majeures en matière de management des risques est le fait de rendre les APRs interopérables, autrement dit, que des scénarios d'accident relatifs aux systèmes, soient rapprochés par des mécanismes de similarité et exploités par retour d'expérience (REX). Ceci, est une manière forte pour consolider la pratique du principe de sécurité GAME.

2.9. Enjeux d'intégrabilité : harmonisation des APRs sous-système

L'harmonisation a pour but de trouver une passerelle permettant de rendre intégrables les différentes APRs des sous-systèmes d'une même entité parent. Ces APRs sont généralement élaborées par des sous-traitants, dans le but de constituer l'APR du système global par l'intégrateur. Ceci permet, entre autres, d'identifier les effets domino entre sous-systèmes et aussi entre sous-systèmes et le système global. Autrement dit, déceler au niveau d'un 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.

2.10. Enjeux de traçabilité : prise en compte des effets domino

Un effet domino est le fait qu'un accident génère ou enclenche un autre. Ainsi, il convient 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 voisinage que nous appellerons dorénavant espace de danger.

3. Méthode MPR (Management Préliminaire des risques)

Notre démarche est basée sur un processus accidentel générique 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 de scénario d'accident [11] [12] [13].

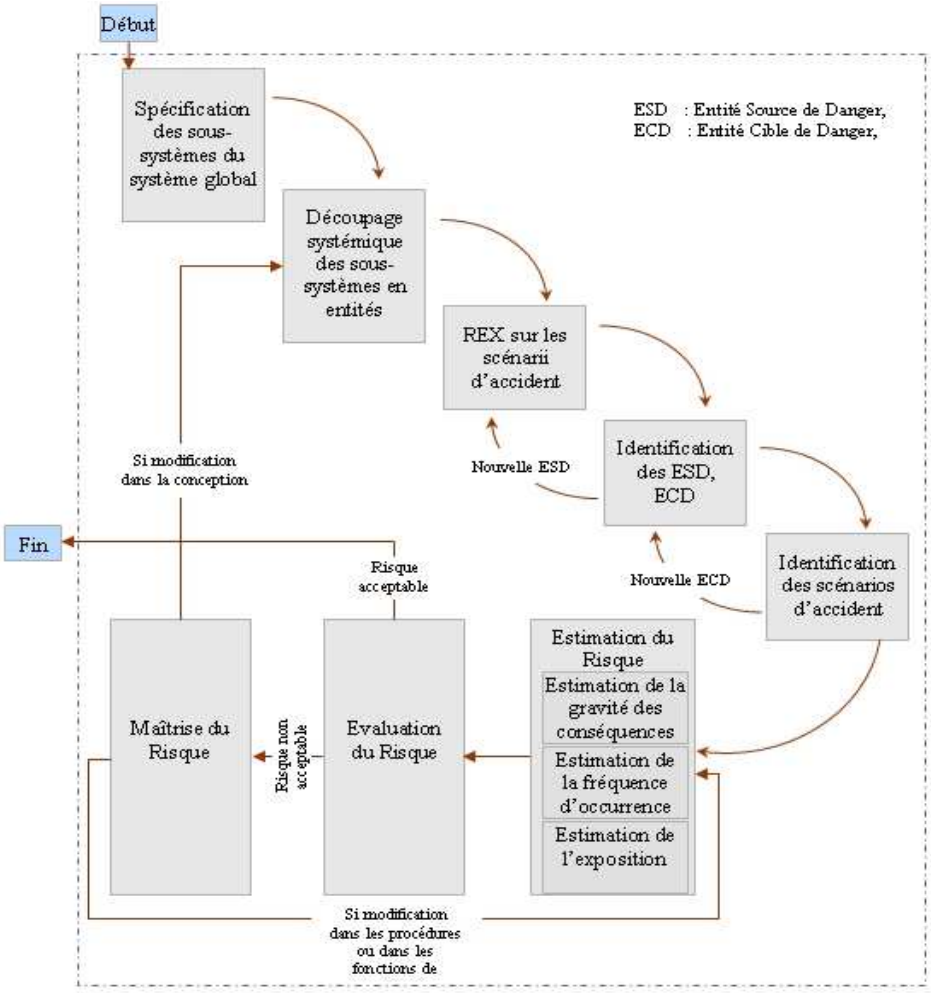

FIG. 1 : Démarche MPR (Management Préliminaire des Risques)

L'objectif principal de notre étude est de concevoir un Système Interactif d'Aide à la Décision en matière de management des risques. Par conséquent, il convient que notre formalisme ainsi que notre manière de présenter les données soient génériques et surtout adaptables aux différents types d'APR issues du monde industriel afin de pouvoir les capitaliser dans la base de données de notre outil [13].

1.1 Découpage systémique du système global en sous-systèmes

Saussure qui est l'un des grands de la linguistique définit le système comme une totalité organisée, faite d'éléments solidaires ne pouvant être définis que les uns par rapport aux autres en fonction de leur place dans cette totalité. Bertalanffy insiste lui aussi sur l'interaction de l'ensemble d'unités d'un système [6]. Cette interaction a un aspect dynamique et organisé en fonction d'un but.

Selon E. Morrin [14], un système est une unité globale organisée d'interrelations entre éléments, actions ou individus.

1.1.1 Système sociotechnique

1.1.1.1 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.

1.1.1.2 La main d'œuvre

C'est 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 de main d'œuvre 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

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.
- 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.
- 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).

1.1.2 Environnement

L. Goffin [7] 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 [7] :

- 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.
- 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.
- L'environnement « se délimite dans l'espace et le temps ». Il doit donc être localisé de façon précise, dans un cadre spatial et temporel.

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.

1.1.2.1 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).

1.1.2.2 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

1.1.2.3 Environnement naturel

L'environnement naturel peut englober les [8] :

- 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

1.2 Découpage ontologique des sous-systèmes en entités

Tout système global est chargé d'une mission qu'il doit accomplir à travers une promiscuité de coordination entre 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 parent ou avec des entités adjacentes du même niveau hiérarchique.

Nous avons adopté la notion d'entité définie par la norme CEI 50(191) [2] 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 ».

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 », la matière dangereuse transportée (ET1) et aussi la centrale nucléaire (ET2). Ces 2 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. Cette coordination passe à travers les SMS.

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 ontologie globale. Cette ontologie permettrait d'imaginer graphiquement la propagation du danger entre les différents niveaux hiérarchiques. Ainsi une situation d'accident relevant d'une entité donnée peut avoir un effet domino avec une autre entité de voisinage appartenant au même ascendant (entité parent), comme elle peut en avoir avec l'ascendant (entité parent) directement voire même avec un descendant (entité fille).

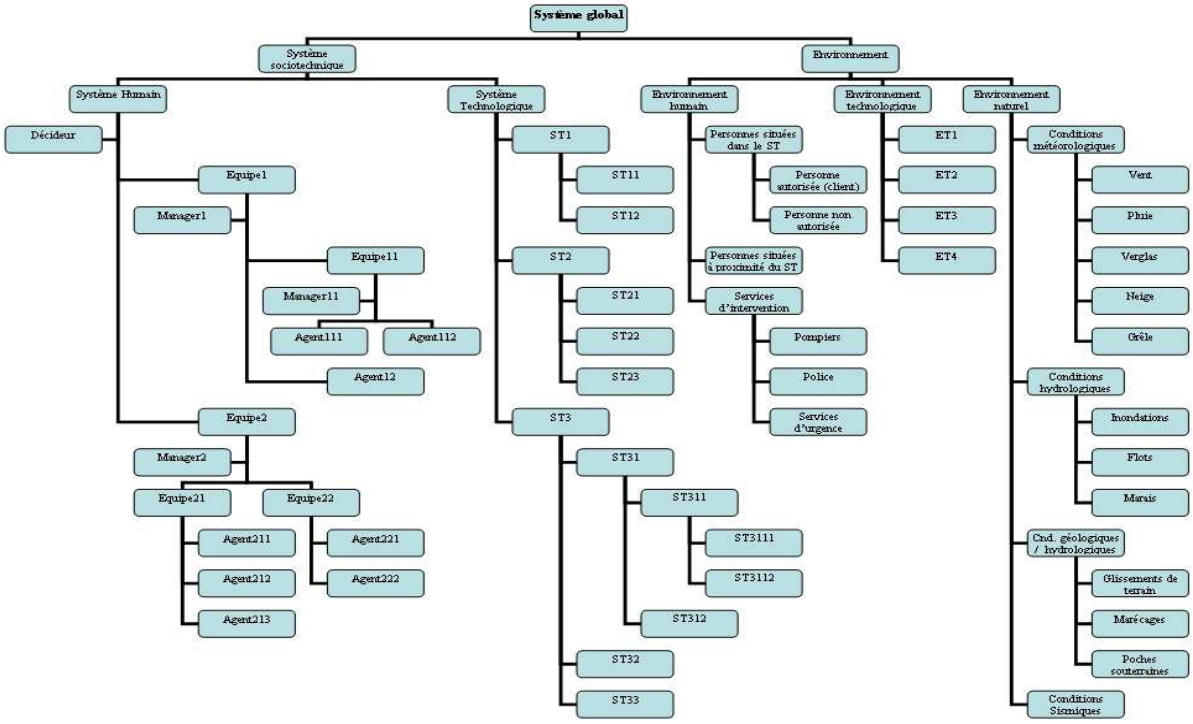

FIG. 2 : Ontologie du système global

1.3 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.

1.3.1 Analyse des scénarii d'accident

La phase d'identification des scénarios d'accident repose essentiellement sur un processus accidentel générique [11] [12]. 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).

Une ECD est une entité telle que les personnes, les biens ou les différentes composantes de l'environnement susceptibles, du fait de l'exposition au danger, de subir, en certaines circonstances, des dommages. Ces dommages sont causés par une entité porteuse ou génératrice de danger que nous dénommerons dorénavant ESD. Il peut s'agir d'un système naturel ou créé par l'homme, ou d'une disposition adoptée et comportant un ou plusieurs dangers.

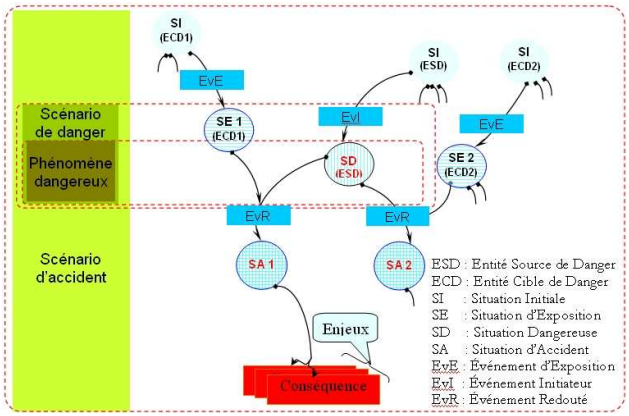

FIG. 3 : Scénario d'accident avec une source et deux cibles à travers le processus accidentel

Nous avons modélisé ce processus accidentel en tenant compte des règles suivantes [12] :

- L'accident est une réalisation qui se développe entre une source (ESD) et une ou plusieurs cibles (ECDs). Le risque est la mesure assignée à cette réalisation.
- Le scénario de danger est une partie du scénario d'accident (cf. FIG. 3) consacrée à l'analyse des dangers, ce qui permettra d'élaborer une cartographie des espaces de danger et 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.

1.3.1.1 Retour d'expérience sur les scénarii 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 scenarii d'accident

Situation d'Accident		Evénement 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

1.3.1.2 Phase I : identification déductive des associations d'entités ESD/ECD(s)

TAB. 2 : Identification des associations (ESD, ECDs)

1	2	3	4	5
Situation d'Accident	Evénement Redouté	Situation Dangereuse	Evénement Initiateur	ESD, ECD(s)

En partant des résultats du retour d'expérience sur les Situations d'Accident **(1)** et les Evénements Redoutés **(2)** associés, on essaye, cette fois ci, d'identifier à froid l'ensemble des Situations Dangereuses **(3)** préalables à l'apparition des EvR en question. Pour chaque SD, on identifie tout EvI **(4)** pouvant altérer la Situation Initiale d'une ESD, et enfin on élabore l'ensemble des associations (ESD, ECDs) **(5)** dont la promiscuité est accidentogène.

1.3.1.3 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 **(1)**, on décèle les EvI **(2)** significatifs ayant le potentiel de stimuler cette dernière qui devient alors génératrice de danger. De la même manière, on identifie les SD **(3)** qui en découlent de cette excitation de l'ESD, et pour chaque SD, on identifie les EvR **(4)** pouvant se produire. Enfin, pour chaque EvR, on identifie les Situation d'Accident potentielles **(5)** et on liste l'ensemble des ECDs **(6)** atteintes par la SA.

1.3.2 Evaluation des risques

TAB. 4 : Evaluation du risque

7	8	9	10	11
Evaluation				
Dommages	Gravité	Occurrence	Exposition	Risque

Cette partie consiste en l'évaluation des criticités des scénarios d'accident identifiés lors de la phase précédente. En effet, pour chaque scénario d'accident on fait une évaluation 'pire cas' (en anglais : *the worst case*) des conséquences pouvant être engendrés **(7)**, ensuite on estime la gravité correspondante **(8)** selon une grille systémique de gravité préalablement définie :

TAB. 5 : Grille systémique de gravité

Severity	Impact on the socio-technical System		Impact on the Environment			Other issues
	Human workforce	Technology	Human-Public	Technology	Natural Environment	
Minor (S1)	No wounded	Minor damage	No wounded	No effect	No effect	Technical
Important (S2)	Minor wounds	Important damage	Minor wounds	Minor damage	Significant threat	Commercial, Financial, Technical
Critical (S3)	Critical wounds, or one dead	Loss of the system	Critical wounds, or one dead	Important damage	Localized damage	**(Localized crisis)** Judicial, Commercial Financial, Technical

Catastro-phic (S4)	More than one dead		More than one dead	Loss of systems	Important damage	**(Important crisis)** Economic, Media effect, Judicial, Commercial, Financial, Technical,

Après avoir estimé la gravité, on estime la fréquence d'occurrence **(9)** de l'EvR donnant lieu à l'accident en question. Le tableau suivant est une adaptation de la métrique de fréquences de probabilité proposée par la norme NF EN 50126 [15] :

TAB. 6: fréquences d'occurrence adaptées de NF EN 50126

Qualitative label	Quantitative correspondence (/h)
Unlikely (O1)	Extremely incredible to occur during the life of the system (<= 10^{-9} occurrence per hour),
Rare (O2)	Incredible to occur but possible during the life of the system (> 10^{-9} occurrence per hour),
Occasional (O3)	Probable that it frequently occurs during the life of the system
Frequent (O4)	Probable that it frequently occurs during the life of the system

L'avant dernière étape de la phase d'évaluation du risque, est l'estimation du degré d'exposition au danger **(10)** des cibles ECDs concernées par le scénario d'accident en question :

- 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**

Une fois la gravité, la fréquence d'occurrence et le degré d'exposition sont estimées, il ne reste que calculer le risque correspondant **(11)** à partir d'un graphe de risque, dont voici un prototype :

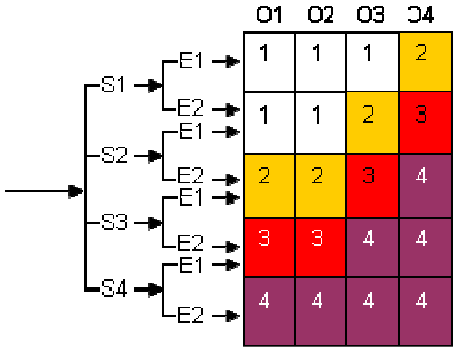

FIG. 4. Prototype d'un graphe de risque

En observant le graphe de risque proposé, on arrive à distinguer quatre zones à risque. En effet, chaque zone est caractérisée par des critères d'acceptabilité bien spécifiques :

TAB. 8 : Critères d'acceptabilité du risque

Zone de criticité	Acceptabilité des risques	
Négligeable	Acceptable	Risques acceptables sans accord de l'autorité de tutelle
Tolérable		Risques acceptables moyennant 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
Intolérable		Risques devant être éliminés

1.3.3 Maîtrise des risques

TAB. 9 : Maitrise et gouvernance des risques

12	13	14	15	16	17	18	19
Maitrise des risques					**Décision**		
Libellé	Type	Pilotage		Gains désirés	Libellé	Motifs	Responsable
		Equipe	Manager				

Cette partie concerne toutes les actions de réduction de risque (Protection, Prévention, Mitigation, Transfert). Idéalement, ces actions devront être codifiées par des libellés **(12)** permettant de les décrire clairement. Ces actions sont de natures différentes **(13)**, 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).

Le principe de défense en profondeur peut accompagner cette phase à travers les différentes situations et transitions du processus accidentel :

TAB. 10: Défense en profondeur via le processus accidentel

EvE	Situation Initiale	Situation d'Exposition	Internes ou externes aux ECDs	Réduire l'exposition et la vulnérabilité des ECD
EvI	Situation Initiale	Situation Dangereuse	Internes ou externes à l'ESD	Réduire la sensibilité des ESD et l'occurrence des EvI
EvR	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 la vocation pendant la situation dangereuse serait d'éviter l'apparition de l'événement redouté et enfin durant la situation d'accident, on se contente de minimiser les conséquences.

Les actions de maitrise des risques doivent être assignées à des équipes et des managers qualifiés à en assumer leur mise en œuvre. Néanmoins, la plupart des industriels rencontrent des difficultés d'ordre organisationnel en matière de maitrise 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

maitrise des risques. Ainsi, chaque mesure est affectée à une équipe **(14)** sous la responsabilité technique d'un personnel expérimenté **(15)**.

Cependant, avant l'approbation de ces actions par le ou les responsables hiérarchiques **(19)**, on doit, toutefois, estimée les gains désirés **(16)**, suite à l'application de ces mesures, par opposition du taux de réduction du risque (Gravité, Occurrence, Exposition,...) à la faisabilité et au coût de mise en œuvre.

Par conséquent, une action peut être accordée ou bien rejetée**(17)**. Cependant, l'approbation ou la désapprobation d'une quelconque action doit être explicitement motivée **(18)**.

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 ».

1.3.4 Présentation des résultats

Les résultats du MPR sont regroupés dans trois tableaux complémentaires : le descripteur de l'arborescence des situations d'accident (cf. TAB.1), le descripteur de l'analyse déductive (cf. TAB. 2), et enfin le troisième descripteur regroupant le reste des résultats de l'analyse et prend le format suivant (cf. TAB. 11) :

TAB. 11 : 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 Conclusion

Mis à part les difficultés linguistiques, nous avons recensé de nombreuses préoccupations majeures pour une meilleure pratique de management des risques.

Cependant, malgré les divergences constatées dans l'emploi des termes, concepts, approches, et autres, les pratiques de management des risques tournent essentiellement autours des quatre exercices suivants :

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

Néanmoins, en dépit de leur importance, plusieurs points importants ne sont que rarement mis en œuvre, 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 gravite, des enjeux capitaux tels que techniques, financiers, commerciaux, juridiques, médiatiques et économiques, etc.
- L'estimation de la fréquence 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 afin de rendre les résultats profitables par les analyses ultérieures.

Toutefois, le tableau suivant présente conjointement ces principaux enjeux de la pratique du management des risques dans le domaine industriel et les solutions que nous avons proposées et discuter dans ce papier afin d'y apporter des éléments réponses aux problématiques en question [11] [12] [13] :

TAB. 12 : Apports de la méthode MPR

Préoccupations		**Solutions**
Difficultés de spécification des limites et interfaces du système		Décomposition systémique du système global
Divergence des termes	Divergence des indicateurs de sécurité	Découpage ontologique des sous-systèmes en entités
Divergence des concepts		Modélisation d'un processus accidentel générique
Divergence des méthodes		**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 APRs***
Absence de responsabilisation		
Absence d'interopérabilité		
Absence d'intégrabilité		
Absence de traçabilité		
Absence de suivi des risques		
Absence de Complétude, cohérence, confidentialité, communication et portabilité des données		

Il est primordial de stimuler une réflexion plénière dans le but de définir une stratégie globale de convergence vers une réelle compréhension du management préliminaire des risques avant d'aspirer à appuyer les experts par des méthodes voire outils d'aide à la décision en matière d'élaboration et d'évaluation des études de sécurité relevant de différents systèmes cohabitant dans le même environnement.

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.

Justement, SIGAR 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 domaine : ferroviaire auquel il a été initialement développé, manufacturier, machine, professionnel, process, épidémiologie, et bien d'autres.

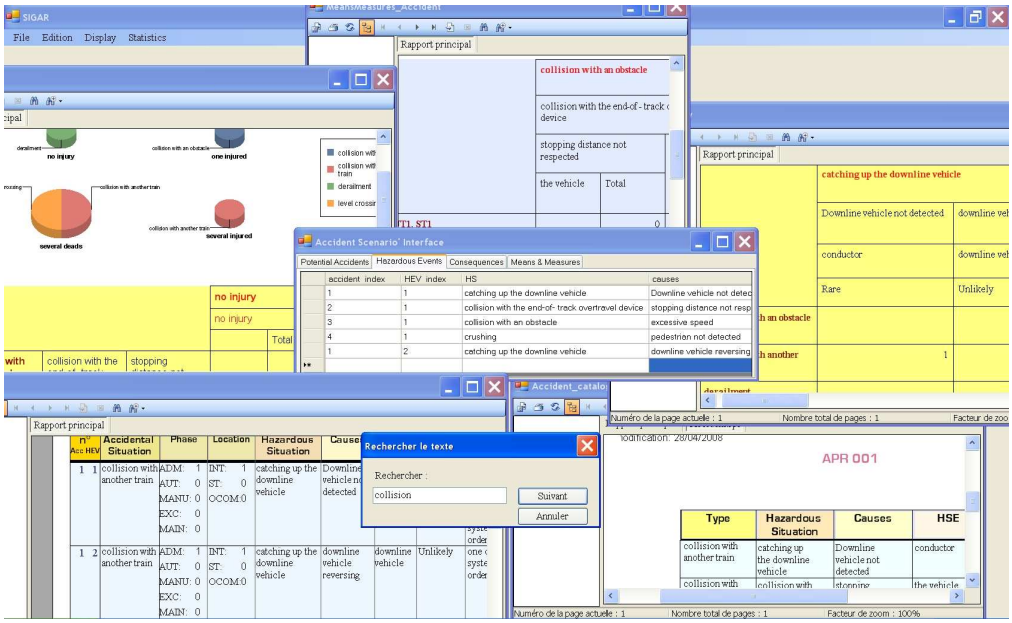

FIG. 5 : Aperçu sur l'interface graphique (GUI) de SIGAR

L'ergonomie de l'interface graphique permet, entre autres, de contraindre les experts de 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, 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 type « SQL Server Database Primary Data File » qui d'ailleurs ne peuvent être exploités qu'à travers l'outil, et d'éviter les textes électroniques ou les supports papiers ordinaires.

Références

[1] CEI 300-3-9 première édition, (1995). *Gestion de la sûreté de fonctionnement*.

[2] CEI 50(191) *International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service*, International Electrotechnical Commission, 1990.

[3] EL-KOURSI EM., MITRA S., BEARFIELD .G (2007). Harmonizing Safety Management Systems in the European Railway Sector - Safety Science Monitor, Issue 2, Vol 11, p 14.

[4] FADIER E. (2000). Les pratiques françaises en matière de sûreté de fonctionnement – Lambda Mu 12.

[5] Groupe de travail GTR 55, (2000). *Aspects sémantiques du risque.* Institut de Sûreté de Fonctionnement - Collège sécurité.

[6] GALLOU G, BOUCHON-MEUNIER B. Systémique : Théorie & Application. France : Lavoisier Edition, 1992.

[7] GOFFIN L. Environnement et évolution des mentalités, Thèse de doctorat, FUL, Arlon-Belgique, 1976.

[8] HMSO, (1995). *A guide to Risk Assessment and Risk Management for Environmental protection*.

[9] Guide ISO/CEI 51, (1999). *Aspects liés à la sécurité – principes directeurs pour les inclure dans les normes*.

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

[11] MAZOUNI MH, AUBRY JF. A PHA based on a systemic and generic ontology, in proc IEEE – ITS international conference SOLI'2007. Philadelphia- USA, 26-29 Août 2007. Paper No. 166.

[12] MAZOUNI MH. Modélisation générique des scénarios d'accident dans le but d'harmoniser les APRs. France : Actes INRETS, Avril 2007.

[13] MAZOUNI MH, BIED CHARRETON D, AUBRY JF. Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport, In: proc IEEE – SMC international conference SOSE'2007. San Antonio-Texas – USA, 18-21 Avril, 2007. Paper No. 98.

[14] MORRIN E. La Méthode, 1 : la nature de la nature ; 2 : la vie de la vie. France : Le Seuil Edition.

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