APPORT DU RETOUR D'EXPERIENCE A L'ANALYSE DES RISQUES (CDROM)
Contribution of field data feedback to hazard analysis (CDROM)

Habib Hadj-Mabrouk
INRETS
2 av du Général Malleret-Joinville
94114 Arcueil Cedex, France

Feyrouz Hamdaoui
ISSAT Sousse
B.P.4. Bouhajla 3180 Kairouan- Tunisie

Résumé
L'analyse préliminaire des risques (APR) d'un projet nécessite en premier lieu le recueil d'une liste des accidents potentiels. A ce jour, le savoir faire des experts et le retour d'expérience (REX) sont la base essentielle d'acquisition de cette liste. Bien que primordiale dans le processus de construction de la sécurité, l'APR souffre encore de l'absence d'une méthodologie itérative qui intègre d'une manière explicite et systématique les résultats issus de REX. Cet article propose une méthodologie en « spirale » permettant d'exploiter systématiquement le REX en vue d'une part d'élaborer la méthode d'APR et d'autre part de prendre en considération les accidents potentiels dès la phase de spécification du projet.

Abstract
The preliminary hazard Analysis (PHA) of a project needs first of all the stacking of a potential accidents list. Up to now, experts' knowledge and field data feedback (FDF) are the essential base of the assembling of this list. Despite that it is fundamental on safety construction process; the PHA suffers from the absence of an iterative methodology which merges, on systematic way, the results descending from FDF. This article proposes a methodology allowing to exploit, systematically, FDF to develop PHA's method and to consider potential accidents since the specification phase of project.

1. Introduction

L'analyse préliminaire des risques (APR) permet d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin d'évaluer leur probabilité d'occurrence ainsi que la gravité des dommages qu'ils peuvent engendrer et enfin de proposer des solutions permettant de maîtriser les risques. Néanmoins, la pertinence de l'APR dépend de la complétude de la liste des accidents potentiels qui peut être identifiée principalement à partir du retour d'expérience (REX). Ce dernier est généralement défini comme étant un processus dynamique de collecte, de stockage, d'analyse et d'exploitation des données relatives à des situations contraires à la sécurité (accident/incident). L'objectif du REX est de tirer profit des enseignements de l'expérience vécue pour éviter la reproduction de scénarios porteurs de risque tout en mettant en œuvre des mesures préventives et correctives adéquates. Cependant, il n'existe pas encore une démarche rationnelle permettant d'exploiter de manière systématique les scénarios d'accidents fournis par le REX pour recenser la liste des accidents potentiels. Pour apporter un élément de réponse a ce problème, nous proposons une approche méthodologique « en spirale » permettant d'exploiter systématiquement les résultats issus du REX non seulement lors de l'élaboration de la méthode d'APR mais aussi dès la phase de spécification du système. L'objectif principal de l'étude vise la réduction du niveau de risque (Probabilité/Occurrence) et par conséquent contribuer à l'amélioration de la sécurité du système conformément à la nouvelle réglementation nationale et européenne en matière de sécurité ferroviaire.

2. Méthodologie proposée

2.1. Description générale de la méthodologie proposée

L'article 5 du décret n°2003-425 du 9 mai 2003 relatif *à la* sécurité des transports publics guidés exige que : « Tout nouveau système de transport public guidé, ou toute modification d'un système existant, est conçu et réalisé de telle sorte que le niveau global de sécurité à l'égard des usagers, des personnels d'exploitation et des tiers soit au moins équivalent au niveau de sécurité existant ou à celui des systèmes existants assurant des services comparables » (principe GAME). La notion d'équivalence introduite par le décret ne fait que traduire l'objectif de non régression du niveau de sécurité par rapport à celui d'un système existant et réputé sur. C'est à ce niveau que le REX apporte tout son intérêt. En effet, en se basant sur les résultats des enquêtes techniques, le processus REX a pour but de tirer profit de l'expérience vécue pour améliorer le niveau de sécurité tout en exigeant la prise en compte de certaines recommandations. De ce fait, il serait nécessaire voir primordial, de mettre en œuvre les mesures recommandées dès la phase de spécification d'un nouveau système (figure 1). Ainsi, notre méthodologie garantie la mise en œuvre explicite de la notion d'équivalence du principe GAME et par conséquent l'amélioration du niveau de sécurité. A ce jour, l'identification de la liste des accidents potentiels nécessaire pour élaborer l'APR, repose en grande partie sur l'expérience et le savoir faire des experts du domaine. Cette tache demeure cruciale pour tout concepteur de système. Or, la qualité, la pertinence et la complétude du dossier d'APR dépendent de l'exhaustivité des accidents potentiels. D'ailleurs, comme son nom l'indique, le dossier d'APR reste généralement ouvert tout au long du cycle de développement du projet et nécessite constamment des mises à jour. Pour apporter un élément de réponse à ce problème, nous proposons d'exploiter, d'une manière systématique, les scénarios d'accidents, fournis par le REX et notamment les listes des accidents potentiels (figure 1). Ainsi, cette approche contribue à l'amélioration de la qualité de l'APR. Les résultats de l'APR permettent de définir les exigences, les critères et contraintes de sécurité du système à prendre en compte lors des phases de conception et de réalisations des équipements matériels et logiciels (figure 1).

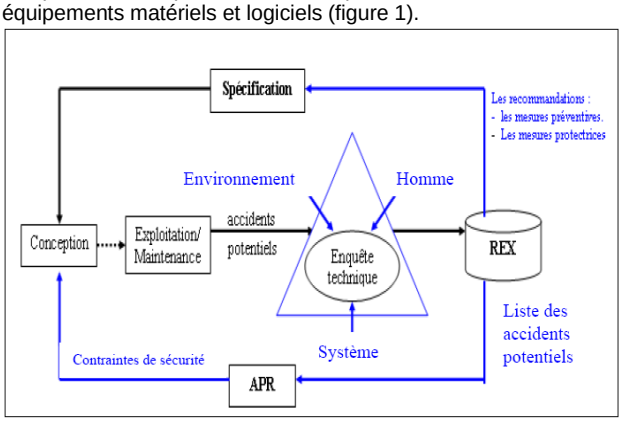

Figure 1. Description générale de la méthodologie proposée

La méthodologie que nous avons développée fait intervenir de manière conjointe et complémentaire deux méthodes : le REX [Hadj-Mabrouk H. & Hadj-Mabrouk A. 2004] et l'APR [Hadj-Mabrouk H. 2006a]. Les deux paragraphes suivants présentent successivement une description de la méthode de REX et de la méthode d'APR.

2.2. Retour d'expérience (REX)

2.2.1. Cadre réglementaire de REX

Un ensemble de récents textes législatifs et réglementaires nationaux ainsi que des directives européennes indiquent les principes, les objectifs et les modalités du processus du REX. Ces réglementations concernent surtout les enquêtes techniques après accidents et incidents ferroviaires (figure 2). Selon la

directive du 23/01/2002, une enquête est une procédure permettant de prévenir les accidents et les incidents et visent à collecter et analyser des informations, à tirer des conclusions, y compris la détermination des causes et, le cas échéant, à formuler des recommandations en matière de sécurité. Les directives européennes visent la création d'autorités de sécurité des Etats membres (dirigées par une agence ferroviaire européenne) ainsi qu'un organisme d'enquêtes permanent, spécialisé et indépendant, l'équivalent du BEA aérien (Bureau Enquêtes Accidents). Le but est de fonder un espace ferroviaire européen intégré afin d'harmoniser la structure réglementaire des Etats membres, d'élaborer des objectifs et des indicateurs de sécurité communs et de mettre en place un système de gestion de la sécurité, dont le processus du Rex, qui satisfait aux exigences communautaires et comporte des éléments communs [Hadj-Mabrouk H. 2006b].

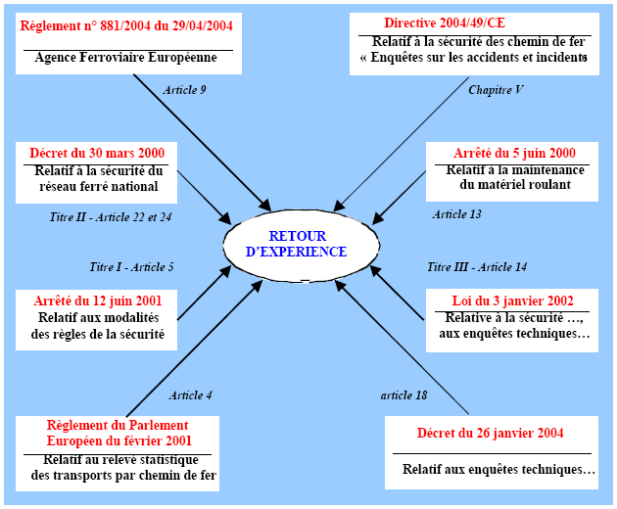

Figure 2. Cadre législatif et réglementaire du REX [Hadj-Mabrouk 2006b]

2.2.2. Définition de REX

Le concept « retour d'expérience » en matière de sécurité des transports est différemment défini selon les auteurs et les domaines. La partie commune à toutes les définitions réside dans l'intérêt de tirer des enseignements d'une expérience vécue pour éviter sa reproduction et augmenter ainsi le niveau de sécurité en mettant en oeuvre les mesures préventives et correctives adéquates. En effet, le REX correspond à un processus dynamique de collecte, de stockage, d'analyse et d'exploitation des données relatives à des situations contraire à la sécurité. Il consiste à une étude analytique causale des différents facteurs impliqués dans la genèse des incidents ou accidents [Hadj-Mabrouk H. & Hadj-Mabrouk A. 2004].

2.2.3. *Approche globale du processus de REX*

Inspirée des travaux de Joing (1991), de Stablier et Vittumi (1995) et de Dominati et al. (1996); l'approche globale du REX que nous avons proposé est fondée sur cinq grands principes : connaitre, comprendre, archiver, apprendre et recommander. Ces cinq principes complémentaires et itératifs correspondent respectivement aux cinq grandes phases : la collecte des données, leur analyse et traitement, leur stockage et mémorisation, leur exploitation et utilisation et les recommandations de sécurité qui en résultent (figure 3) [Hadj-Mabrouk H. & Hadj-Mabrouk A. 2004].

2.2.3.1. Collecte des données

Cette première phase qui répond au premier principe connaitre consiste à recueillir le maximum de données et à s'intéresser à toutes les anomalies rencontrées. La collecte concerne ainsi les données relatives essentiellement à l'opérateur humain, à son environnement interne et externe, au système technique.

2.2.3.2. Analyse des données

Cette phase qui répond au principe comprendre ne doit pas se limiter à l'analyse des causes premières apparentes mais à établir, par exemple, un arbre des causes des dysfonctionnements permettant de mieux cerner les mécanismes générateurs des événements affectant la sécurité.

2.2.3.3. Stockage des données

Cette phase répondant au principe archiver s'attache à mémoriser les données collectées et analysées dans une base de données grâce, souvent, à un système informatique.

2.2.3.4. Exploitation des données

Cette phase qui répond au principe apprendre du processus de REX consiste à utiliser et interpréter les résultats issus des différents traitements 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 scénarios d'accidents ou événements indésirables.

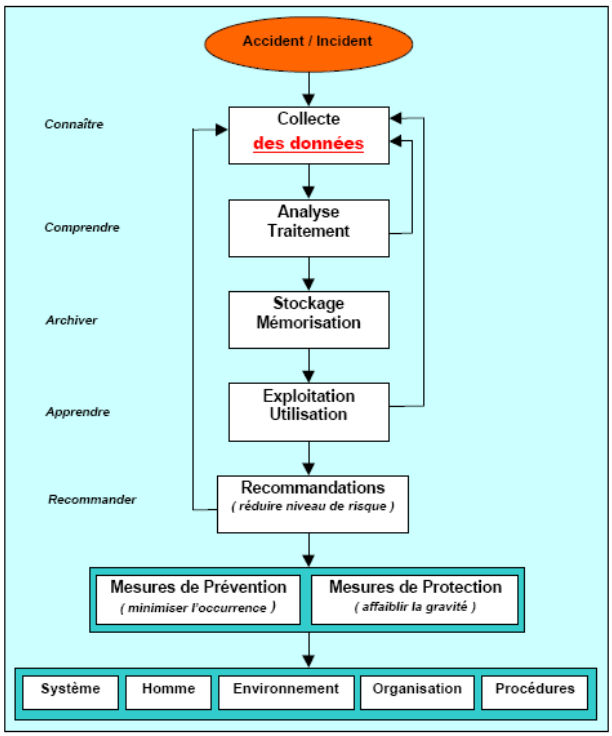

Figure 3. Articulation des différentes étapes de déroulement du REX [Hadj-Mabrouk H. & Hadj-Mabrouk A. 2004]

Après avoir présenter l'approche du REX retenue, le paragraphe suivant aborde la méthode d'APR adoptée [Hadj-Mabrouk H. 1998].

2.2.3.5. Recommandations

Elle répond au principe recommander qui consiste à définir et identifier les mesures adéquates pour limiter la reproduction d'un événement d'insécurité. Il s'agit de mieux tirer profit des enseignements de l'expérience acquise pour améliorer la sécurité.

2.3. Analyse préliminaire des risques (APR)

2.3.1. Cadre réglementaire de l'APR

Selon l'article 48 du chapitre III du titre V du décret n°2006-1279, le dossier préliminaire de sécurité (DPS) 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 toute la période d'exploitation du système ou du sous-système. L'arrêté d'application de 08/01/2002 du décret n°2000-286 précise que le DPS comporte notamment un document relatif à l'organisation du projet et s'appuie sur les résultats d'une APR. Cet arrêté précise aussi que 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 DPS. Il contient les conclusions des études de sécurité réalisées et les attestations de couverture des risques identifiées dans l'APR. Du fait que l'APR est réalisée très tôt dans le cycle de développement du système (dès la phase de spécification), ses résultats peuvent être incomplets ou imprécis. Ainsi le dossier de l'APR reste ouvert et est constamment mis à jour tout au long du développement du projet.

2.3.2. Processus de construction de la sécurité

Généralement, le processus de construction de la sécurité d'un système (figure 4) comporte plusieurs analyses complémentaires

hiérarchisées [Hadj-Mabrouk H. 1995], [Hadj-Mabrouk 1997] et [Hadj-Mabrouk H. 1998] : L'analyse préliminaire de risques, l'analyse fonctionnelle de la sécurité, et l'analyse de la sécurité du produit réalisé. L'analyse préliminaire de risques (APR) a pour but d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin de les évaluer et de proposer des solutions pour les supprimer, les réduire ou les contrôler. L'analyse fonctionnelle de la sécurité (AFS) a comme objectif de justifier que l'architecture de conception du système est sécuritaire vis-à-vis des accidents
potentiels identifiés par l'APR et par conséquent de s'assurer que toutes les dispositions de sécurité sont prises en compte pour couvrir les dangers ou les accidents potentiels. L'analyse de la sécurité du produit réalisé concerne l'analyse de la sécurité des logiciels (ASL) et l'analyse de la sécurité des matériels (ASM). L'ASL est généralement basée sur la méthode d'analyse des effets des erreurs du logiciel (AEEL) ainsi que sur les lectures critiques de code. L'ASM porte notamment sur les cartes électroniques et les interfaces définies comme étant de sécurité. Cette analyse met en oeuvre plusieurs types d'analyses : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC), Méthode des Combinaisons de Pannes Résumées (MCPR) et Méthode de l'Arbre des Causes (MAC).
Dans ce processus de construction de la sécurité, l'une des difficultés consiste à s'assurer de l'exhaustivité et de la cohérence des différentes analyses (APR, ASF, ASL, ASM) par la recherche des risques et scénarios contraires à la sécurité non pris en compte lors de l'élaboration du dossier de sécurité.[Hadj-Mabrouk H. 2006a]

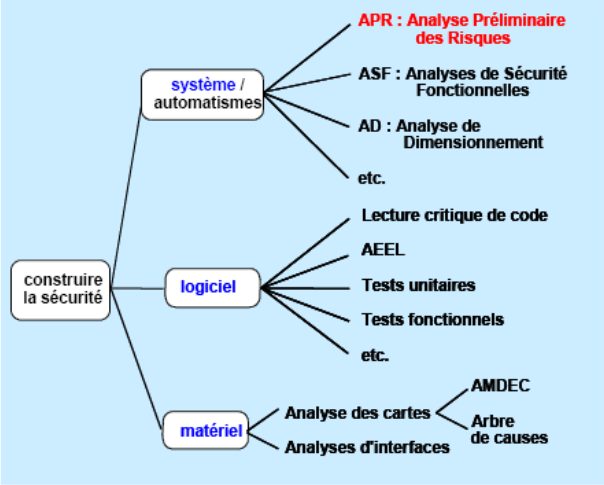

Figure 4. Processus de construction de la sécurité d'un système de transport ferroviaire [Hadj-Mabrouk H. 1995], [Hadj-Mabrouk H. 1997] et [Hadj-Mabrouk H. 1998]

2.3.3. Objectif et place de l'APR dans le cycle de développement d'un système

L'analyse préliminaire de risques (APR) permet d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin d'évaluer leur probabilité d'occurrence ainsi que la gravité des dommages qu'ils pourraient causer et enfin de proposer des solutions qui permettront de les réduire, les contrôler ou les supprimer [Hadj-Mabrouk H. 1995] et [Hadj-Mabrouk H. 1998]. Les résultats de cette analyse permettent de définir les exigences et critères de sécurité du système à prendre en compte lors des phases de conception et de réalisations des équipements matériels et logiciels et enfin d'établir les grandes lignes des analyses de sécurité situées en aval (analyse fonctionnelle de la sécurité, analyse de la sécurité des logiciels, analyse de la sécurité des matériels). En effet, la constitution d'une liste d'accidents potentiels permet de recenser les points du système qui peuvent être critiques pour la sécurité et qui méritent une attention particulière dans la conception, la réalisation, la validation et la maintenance du système.

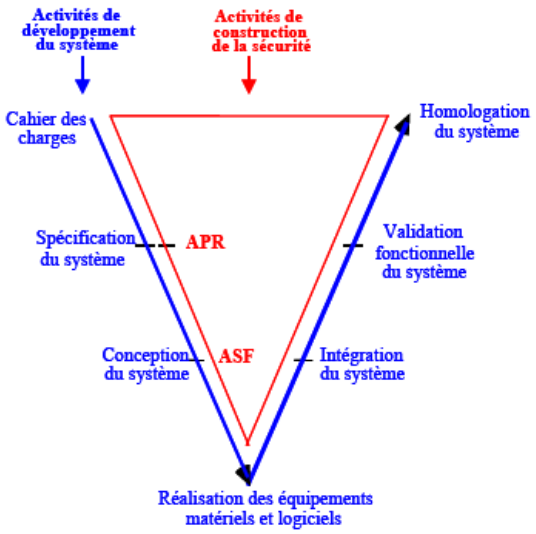

Figure 5. Place de l'APR dans le cycle de développement [Hadj-Mabrouk 2006a]

Une APR nécessite une bonne connaissance de la mission du système et de son environnement. Elle est indispensable pour les systèmes qui font appel à des technologies mal connues. Elle bénéficie d'une part de l'expérience et de l'imagination du constructeur et d'autre part du suivi en exploitation (REX) [Hadj-Mabrouk 2006a].

2.3.4. Méthode d'APR proposée

Notre méthode d'APR s'articule autour de trois étapes complémentaires et itératives. A partir des accidents potentiels, la première étape permet de déterminer par induction la liste des dommages que pourrait causer un accident et par déduction la liste des dangers qui peuvent se manifester dans le système.
La deuxième étape utilise les dangers précédents pour identifier par déduction la liste des éléments dangereux et, par induction, celle des accidents potentiels. Etablir à nouveau la liste des accidents potentiels à partir des dangers permet éventuellement d'engendrer de nouveaux accidents potentiels non considérés lors de la première étape. Dans ce cas, la première étape de l'analyse doit être reprise en vue d'enrichir la liste des dangers précédemment déduite. Il s'agit en fait d'une action de vérification qui permet d'accroître davantage la liste initiale des accidents potentiels.
La troisième étape de l'analyse consiste, à induire des dangers, à partir des éléments dangereux déduits lors de la deuxième étape. Le catalogue des dangers établi à l'issue de cette troisième analyse est confronté à celui qui est déduit lors de la première étape de l'analyse à partir des accidents potentiels. L'invention de nouveaux dangers impose de recommencer la deuxième étape d'analyse et éventuellement la première. Ce processus de contrôle itératif permet d'assurer la complétude et de tendre ainsi vers l'exhaustivité de l'analyse préliminaire de risques (APR). La figure 6 schématise les différentes étapes impliquées dans le processus d'analyse de risque que nous retenons [Hadj-Mabrouk 2006a].

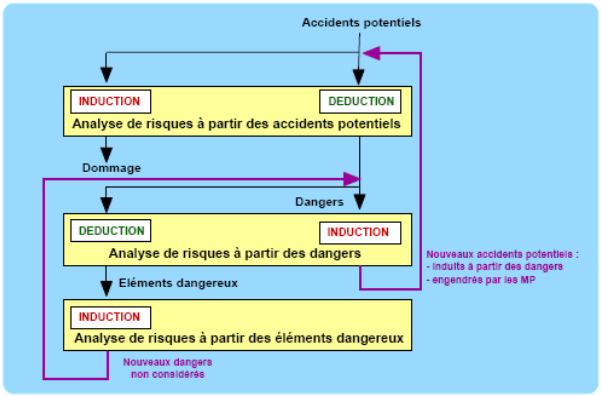

Figure 6. Principe général de la méthode d'APR proposée [Hadj-Mabrouk 2006a]

La description de ces deux méthodes : REX et APR, montre l'intérêt d'exploiter les résultats issus de REX non seulement dans l'APR mais aussi dès la phase de spécification du système. Le paragraphe suivant présente une description détaillée de la méthodologie proposée pour améliorer la sécurité du système.

2.4. Description détaillée de la méthodologie proposée

La méthodologie proposée, illustrée par la figure 7, se base sur un modèle en spirale formé par trois couches qui interagissent en vue de garantir la complétude et l'exhaustivité de l'APR.

2.4.1. Les couches du modèle en spirale

Le noyau du modèle proposé est le processus d'APR retenu qui s'articule autour de trois analyses complémentaires et itératives: à partir de l'analyse des accidents potentiels, on déduit une liste des dangers, l'analyse de ces dangers permet, à la fois, d'induire une nouvelle liste des accidents potentiels et de déduire les éléments dangereux, l'analyse des éléments dangereux contribue ainsi à l'induction d'une nouvelle liste des dangers.
Sur ce noyau, se superposent les cinq principes de REX : connaître le risque, le comprendre, l'archiver, l'apprendre et enfin proposer des recommandations; en formant ainsi la deuxième couche du modèle. Ces cinq principes du REX sont associés aux cinq phases de collecte des données relatives à un événement d'insécurité - analyse et traitement - stockage et mémorisation - exploitation - recommandations.
La troisième et dernière couche du modèle est composée des différentes étapes du cycle de développement d'un système : spécification, conception, réalisation, intégration, validation, certification, homologation, mise en service, exploitation et maintenance.

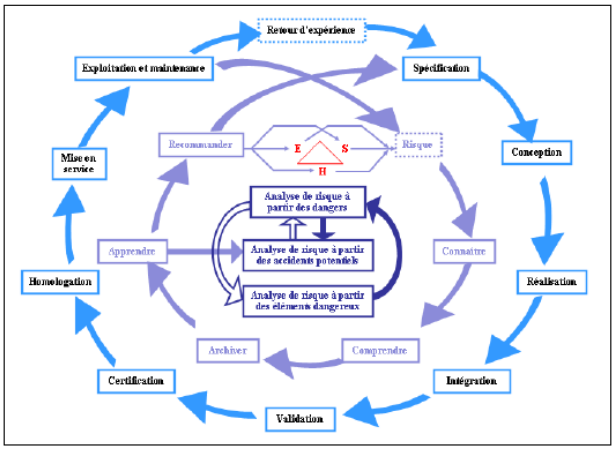

Figure 7. Modèle en Spirale d'intégration du REX dans l'APR

2.4.2. Articulations du modèle en spirale

La méthodologie constitue, en fait, un modèle compact et itératif garantissant ainsi l'interaction entre ces différentes couches d'une manière systématique.
En effet, conformément à la réglementation en vigueur, des enquêtes techniques de sécurité doivent être effectuées après les accidents/incidents graves survenus sur le système tout en prenant en compte les informations relatives aux erreurs humaines, technologiques et environnementales (figure 7). La première phase de collecte de données du REX correspond à rechercher et recueillir tous les éléments tant descriptifs qu'explicatifs ayant conduit à un événement d'insécurité. Ainsi, cette phase se base sur les résultats issus des différents rapports d'enquêtes (figure 7).
Après avoir analyser et stocker les données déjà collectées, la phase d'exploitation du processus de REX consiste à utiliser et interpréter ces données. L'objectif principal est d'extraire l'événement réellement prédictif, de prendre en considération les cas isolés et de prédire ou d'imaginer des futurs scénarios d'accidents ou évènements indésirables. A partir des résultats de cette phase, on peut explicitement extraire les listes des accidents potentiels et les utiliser directement comme entrées de l'APR (figure 7).
En effet, la phase ultime de la démarche de REX correspond à recommander des mesures de prévention (afin de minimiser l'occurrence des accidents potentiels) et des mesures de protections (en vue d'affaiblir la gravité des dommages engendrés). Ces recommandations ont pour but l'action sur les facteurs humains, les aspects techniques et l'environnement. Systématiquement, ces mesures sont prises en compte, dès la spécification, dans le cycle de développement de tout nouveau système afin de limiter la reproduction de tel évènement d'insécurité (figure 7).
A notre sens, l'originalité du modèle en spirale proposé réside dans le fait de considérer le REX comme étant le maillon fondamental qui enchaîne exploitation vers la phase de spécification (figure 7). Ainsi, la méthodologie proposée garantie la traçabilité de la gestion de risque en le suivant dès son apparition jusqu'à la mise en oeuvre concrète des mesures de protection et/ou de prévention.

3. Conclusion

L'objectif initial de notre recherche vise à améliorer la complétude de l'APR afin de disposer d'une liste exhaustive des accidents potentiels à prendre en considération lors de développement du projet.
Pour appréhender ce problème, nous avons proposés un modèle en trois couches incluant successivement les étapes de développement de l'APR, les phases du processus du REX ainsi que les étapes de développement d'un projet. L'ensemble de ces couches interagissent entre elles d'une manière explicite formant ainsi le modèle en spirale.
Nous avons démontrés comment exploiter de manière systématique et explicite les résultats issus de REX non seulement pour tendre vers l'exhaustivité de la liste des accidents potentiels (nécessaire pour disposer d'une méthode d'APR consistante), mais ainsi pour tirer des enseignements à prendre en considération dès la phase de spécification du projet.
Nous avons ainsi contribué à réduire le niveau de risque du système et par conséquent améliorer la sécurité du système. Malgré l'intérêt indéniable de ce modèle, des travaux de recherches sont en cours en vue de valider et démontrer le bien-fondé de l'approche proposé à travers un cas réel issu du domaine de transport ferroviaire.

4. Références

Bourdeaux I. et Gilbert C., « Procédures de retour d'expérience, d'apprentissage et de vigilance organisationnels : Approches croisées », Programme risques collectifs et situations de crise, Grenoble, CNRS, 09/1999.

Décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferroviaire national (RFN) et son arrêté d'application du 08 janvier 2002.

Décret n°2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés.

Décret n°2006-1279 du 19 octobre 2006 relatif à la sécurité des circulations ferroviaires et à l'interopérabilité du système ferroviaire.

Dominati A., Bonneau A. et Lewkowitch – Orlandi A., « Sacre : une base de données sur les incidents du parc nucléaire d'EDF au service du retour d'expérience facteur humain ». Colloque national de fiabilité et maintenabilité, n° 10, octobre 1996.

Hadj-Mabrouk H., « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés ». Revue RTS, numéro 49, pp 101-112, France, Décembre 1995.

Hadj-Mabrouk H., « Projet SAPRISTI : Proposition d'une méthode et d'une maquette d'aide à l'élaboration et à la capitalisation des analyses préliminaires de risques ». Rapport n° ESTAS/A-97-66, 17p, Arcueil, 19 novembre 1997.

Hadj-Mabrouk H., **«** Acquisition et évaluation des connaissances de sécurité des systèmes industriels. Application au domaine de la certification des systèmes de transport guidés **»**. Thèse d'Habilitation à Diriger des Recherches. Université de Technologie de Compiègne, février 1998.

Hadj-Mabrouk A. et Hadj-Mabrouk H., Approche d'intégration de l'erreur humaine dans le retour d'expérience. Application au domaine de la sécurité des transports ferroviaires, Synthèse INRETS n°43, février 2004, 104 p.

Hadj-Mabrouk H. « Méthode d'analyse préliminaire des risques dans les transports ferroviaires ». 15ème congrès de maîtrise des risques et de Sûreté de fonctionnement, Lille, 10-12 Octobre 2006.

Hadj-Mabrouk H. « Réglementation en matière de retour d'expérience dans les transports ferroviaires ». Workshop International: Logistique & Transport 2006 (LT' 2007) a technically IEEE/SMC co-sponsored workshop, 30 avril - 2 mai 2006, Hammamet – Tunisie.

Joing M., « le retour d'expérience à la SNCF », colloque la sécurité des transports collectifs, décembre 1991, Paris, 178-180.

LOI 2002-3 du 03 janvier 2002 relative à la sécurité …, aux enquêtes techniques après événement de mer, accident ou incident de transport terrestre ou aérien …

Sabier P. et Vittumi H., « Le retour d'expérience appliquée à la sécurité, la mise en oeuvre de la direction du transport à la SNCF », Revue Générale des chemins de fer, Juin 1995, 5-10.

Villemeur A., Sureté de fonctionnement des systèmes industriels, Collection de la direction des Etudes et de Recherches d'EDF, Paris, Editions Eyrolles, 1998.