Introduction à la sécurité et à l'analyse des risques technologiques et humains

Habib Hadj Mabrouk

Introduction à la sécurité et à l'analyse des risques technologiques et humains

Application à la certification des systèmes de transports ferroviaire

Habib Hadj-Mabrouk
Institut national de recherche sur les transports et leur sécurité. *mabrouk@inrets.fr*

RÉSUMÉ. *L'opérateur humain est un élément paradoxal : en situation de stress ou de fatigue, il peut être un élément de la perte de la fiabilité d'un système. Cependant, dans certaines situations critiques d'insécurité, il peut être un facteur de fiabilité, en rétablissant le bon fonctionnement du système, parfois par des actions non prévues par le règlement de sécurité de l'exploitation, mais, liées à sa connaissance, son expérience et son savoir-faire. Il faut donc optimiser la place de l'homme dans le système de transport en pleine connaissance de ses capacités mais aussi de ses limites. Inspiré des travaux de Reason, Rasmussen, Van Eslande et soutenue par quelques exemples d'application issus du domaine de la sécurité ferroviaire, l'approche proposée d'analyse et de modélisation de l'activité de l'homme dans l'analyse des scénarios d'accidents en vue améliorer le niveau de sécurité des systèmes de transports ferroviaires, fait intervenir trois niveaux complémentaires. Le premier niveau d'analyse contextuelle (avant l'accident) permet d'étudier les différents facteurs favorisant la production de l'erreur humaine à l'origine de l'accident. Ces facteurs sont relatifs à l'opérateur humain, à son environnement de travail, au système ainsi qu'aux diverses interactions de l'homme avec le système et l'environnement. Le deuxième niveau d'analyse cognitive (pendant l'accident) vise à identifier les erreurs humaines relatives au processus cognitif humain mis en jeu face à une situation d'insécurité donnée. Le troisième niveau d'analyse comportementale (après l'accident) s'attache à évaluer les conséquences d'une action erronée en termes de dommage sur l'homme, sur l'environnement et sur le système.*

MOTS-CLÉS : *Facteur humain, Retour d'expérience Scénario d'accident, Sécurité ferroviaire, Sureté de fonctionnement*

1. Introduction

Avec l'amélioration de la fiabilité technique, la tendance actuelle est d'attribuer les dysfonctionnements des systèmes, générateurs d'accidents, à une erreur de l'opérateur humain. L'opérateur est considéré comme point faible du système et limiteur de performance et de sécurité. Ainsi, l'erreur humaine constitue un facteur causal majeur de l'émergence des accidents dans plusieurs secteurs de sécurité dont celui des transports ferroviaires. La survenue de nouveaux accidents malgré la maîtrise du risque technologique est à la base de l'intérêt renouvelé à l'étude des facteurs humains dans l'analyse de la sécurité. Bien que, le Directeur de la sécurité, à la SNCF (Etienne M., 2002) confirme que la prise en compte compétente et lucide des questions de facteur humain est un thème essentiel pour la sécurité et les progrès des performances du service ferroviaire et son développement, la première journée consacrée aux Facteurs Humains dans la sécurité ferroviaire en France s'est déroulée le 19 septembre 2000 à Toulouse. D'autre part, les conséquences néfastes et le coût terrible des accidents dus au facteur humain, la survenue de nouvelles catastrophes malgré le progrès de la technologie, sont à la base de la mise en place d'un système de retour d'expérience (Rex) comme étant l'un des moyens essentiels de nature à promouvoir l'amélioration nécessaire de la sécurité. Néanmoins, le Rex dans les activités à risques reste encore largement limité à une dimension technique .Le recours à une démarche rigoureuse d'analyse du Rex centrée sur les facteurs humains et admise par tous les acteurs qui prennent part à l'élaboration du dossier de sécurité s'impose. L'objectif de la recherche est de rationaliser, d'harmoniser et d'homogénéiser le processus d'élaboration et d'exploitation du Rex et d'améliorer ainsi le niveau de sécurité des futurs systèmes de transports ferroviaires par la prise en compte des facteurs humains non seulement dès les phases de spécification et de conception du système, mais aussi dans le processus de retour d'expérience.

2. Sûreté de fonctionnement

La sûreté de fonctionnement d'un système (SdF) est définit comme la qualité du service délivré par un système, qualité telle que les utilisateurs de ce service puissent placer une confiance justifiée dans le système qui le délivre [BOU 06]. Son objectif est alors de connaitre et de maitriser les risques de dysfonctionnement des produits et systèmes complexes, notamment leur fiabilité en mettant en œuvre des méthodes prévisionnelles, expérimentales et opérationnelles appropriées [KRI et al 05]. Généralement, elle est caractérisée par quatre principales composantes : fiabilité (reliability), maintenabilité (maintenability), disponibilité (availability) ainsi que la sécurité (safety) et se nomme alors FDMS (RAMS). En outre, l'évolution technologique a contribué à l'apparition d'autres attributs à savoir : la qualité, le facteur humain et l'ergonomie. Selon la norme CEI 60050, la fiabilité est la caractéristique que le système accomplisse une mission donnée ou une fonction requise dans les conditions opérationnelles spécifiées [DES et al 03]. Associée au concept d'aptitude à la réparation, la maintenabilité est la caractéristique d'un système que ce dernier puisse être réparé dans l'intervalle de temps [t0, t1] sachant

qu'il peut être en panne à l'instant t0 [DES et al 03]. La composante disponibilité signifie que le système soit opérationnel à l'instant t1 du début de mission [DES et al 03]. Quand à la sécurité, elle demeure la composante capitale de tout système industriel à risque.

2.1. *Définition de la sécurité*

La norme européenne CENELEC 50129 définit la sécurité par « l'absence de tout niveau de risque inacceptable ». La probabilité d'occurrence d'un accident potentiel ainsi que la gravité des dommages engendrés par cet accident potentiel sont les deux composantes qui identifient la notion du risque. De ce fait, pour définir le niveau de probabilité d'un accident potentiel, la norme CENELEC EN 50126 propose un ensemble de catégories dont chacune est associée à une plage de fréquence. Vu la difficulté d'estimer ces fréquences, cette association quantitative/qualitative est favorable. De même, la norme CENELEC EN 50 126 définit le niveau de gravité en associant les quantifications avec les conséquences engendrées par l'accident potentiel. En effet, le niveau d'acceptabilité des risques est identifié et évalué en utilisant la matrice Occurrence/Gravité.

2.2. *Matrice Gravité/Occurrence*

a. Niveau de probabilité de l'accident potentiel

Les normes en matière de sécurité des transports tentent à définir l'ensemble des niveaux de probabilité d'occurrence sans prendre en compte le type d'analyse de sécurité dans lequel ces niveaux seront employés. Elles visent à proposer une échelle quantitative pour des probabilités dont la quantification est énormément complexe. Néanmoins, la norme EN 50126 propose des probabilités quantitatives, d'où la probabilité d'occurrence d'un événement peut être :

- ***Fréquent (A) :*** surviendra probablement souvent. Le risque de concrétisation du danger sera continuellement présent. **(P > 10-3)**
- ***Probable (B) :*** surviendra plusieurs fois. Le danger se concrétisera fréquemment. **(10-3 > P > 10-4)**
- ***Occasionnel (C) :*** surviendra probablement plusieurs fois au cours de la vie de système. Le danger se concrétisera plusieurs fois. **(10-4 > P > 10-5)**
- ***Rare (D) :*** surviendra probablement au cours de la vie du système. On peut raisonnablement s'attendre à la concrétisation de ce danger. **(10-5 > P > 10-7)**
- ***Improbable (E) :*** peu probable mais possible. On peut admettre que ce danger se concrétisera exceptionnellement. **(10-7 > P > 10-9)**
- ***Hautement improbable :*** Extrêmement improbable. On peut admettre que ce danger ne se concrétisera pas. **(10-9 > P)**

b. Niveau de gravité des dommages engendrés par l'accident potentiel

Les normes classifient les niveaux de gravité des dommages engendrés par l'accident potentiel sur trois niveaux : selon les dommages aux personnes, au système et à l'environnement. Considérant les conséquences sur les personnes, la norme EN 50126 propose quatre niveaux de gravité des dommages :

- ***Catastrophique :*** plusieurs blessés graves ou plusieurs morts
- ***Grave :*** un blessé grave ou un mort
- ***Signifiant :*** un blessé léger
- ***Insignifiant :*** ni blessé, ni mort

A noter que cette norme différencie les dommages dus à des accidents individuels de ceux qui résultent d'accidents collectifs.

c. Niveau de risque

Généralement, il existe une confusion entre le risque et le niveau de risque. En effet, le niveau de risque identifie la combinaison du niveau de probabilité d'occurrence de l'accident potentiel ainsi que le niveau de gravité des dommages engendrés par cet accident potentiel ; d'où plusieurs classifications apparaissent. La norme EN 50126 identifie 4 niveaux de risque :

- ***Risques intolérables :*** doivent être éliminés
- ***Risques non souhaitables :*** « ne peuvent être acceptés, avec l'accord du Responsable Sécurité, que si l'on ne peut pas réduire le risque »
- ***Risques tolérables :*** « acceptables, avec l'accord du Responsable Sécurité, et moyennant des précautions appropriées »
- ***Risques négligeables :*** « acceptables, avec l'accord du Responsable Sécurité »

A partir de ces définitions, les différentes normes recommandent la mise en place d'une matrice gravité/occurrence pour évaluer le risque ; d'où la matrice suivante identifiée par la même norme en vigueur :

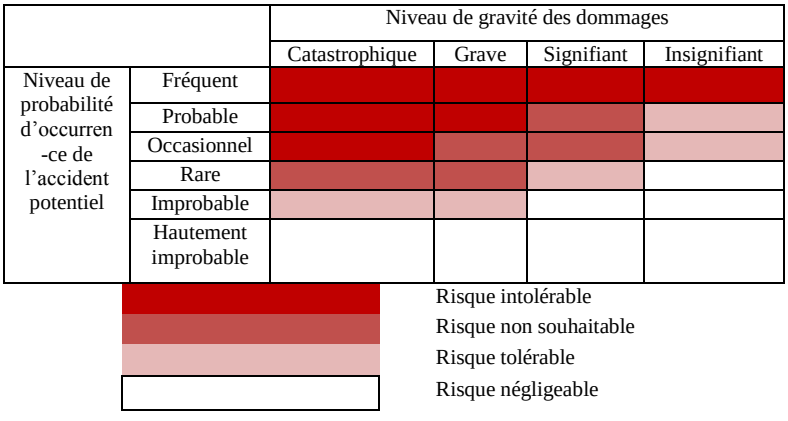

Figure 1. *Matrice gravité/occurrence*

Elaborer, administrer et évaluer la sécurité d'un système nécessite de faire appel à des principes, des techniques et des méthodes présentés ci-après.

2.3. *Principes de sécurité*

En Europe, on distingue trois grandes principes de sécurité. En Allemagne, on applique le principe MEM (Minimum Endogenous Mortality) qui prétend qu'on continue à améliorer le niveau de sécurité si seulement si le taux de mortalité dues aux faits technologiques (exogène à l'organisme) soit inférieur au taux de mortalité endogène (dans un lieu et un espace de temps déterminé). Au Royaume-Uni, le principe est plutôt d'ordre économique. En effet, le principe ALARP (As Low As Reasonably Practibale) y appliqué exige qu'un niveau de risque est acceptable si le cout dû à la réduction du risque est disproportionné en regard du gain d'amélioration. Apparu dans le décret 30 mars 2000, GAME (Globalement Au Moins Equivalant) est le principe retenu par le comité européen. Ce principe stipule que le niveau de sécurité d'un nouveau système doit être au moins équivalent à celui d'un système comparable déjà existant et réputé sûr.

2.4. *Techniques de sécurité*

Généralement, on parle de trois techniques de sécurité : intrinsèque, probabiliste et contrôlée. En effet, certains systèmes ne peuvent pas tolérer aucun niveau de défaillances. Afin de répondre à ce besoin, la sécurité intrinsèque vise à atteindre un niveau optimal de sécurité. Par contre, la sécurité probabiliste admet un niveau de risque acceptable et défini un seuil préétabli. De ce fait, elle démontre à priori que la probabilité d'occurrence d'un accident potentiel est inférieure à ce seuil. La troisième technique de sécurité est nommée contrôlée du fait que les défaillances sont détectées et leurs conséquences empêchées par des équipements spécifiques.

Dans le cadre d'un projet, après avoir retenu un principe de sécurité et une ou plusieurs techniques de sécurité, il convient maintenant à recourir à un ensemble de méthodes d'analyse de sécurité.

2.5. *Méthodes de sécurité*

Il existe une gamme très large de méthodes d'analyse qui peuvent être classées en trois niveaux : système ou automatisme, logiciel et matériel (figure 3). L'analyse de sécurité au niveau logiciel est généralement basée sur la méthode d'analyse des effets et des erreurs du logiciel (AEEL) ainsi que sur les lectures critiques de code. Généralement, l'analyse de sécurité matérielle porte notamment sur les cartes électroniques et les interfaces définies comme étant de sécurité. Cette analyse met en œuvre plusieurs méthodes: 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). Appliqué au niveau système, l'Analyse Préliminaire des Risques (APR) représente la méthode la plus répondu. Elle vise à identifier 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 mesures de protection et/ou de prévention.

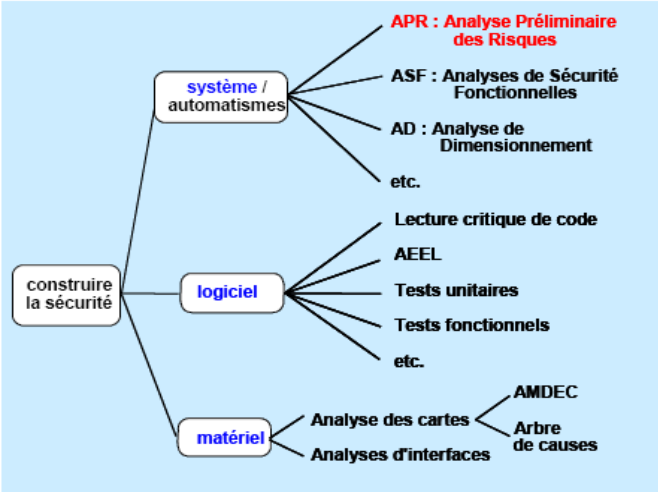

Figure 2. *Méthodes d'analyse de la sécurité [HAD 95, 97 et 98]*

3. Méthode d'Analyse Préliminaire des Risques

Théoriquement, l'Analyse Préliminaire des Risques est connue comme une démarche inductive [Lievens 76], [Villemeur 88] et [BNAE 86] (in HAD 98). Le raisonnement inductif va du plus particulier au plus général, ce qui conduit à une étude détaillée des effets d'une défaillance sur le système et son environnement. Dans le cadre de l'APR, il s'agit de rechercher principalement, par induction, l'ensemble des accidents potentiels à partir des dangers (ou éléments dangereux). Cependant, dans la pratique, on choisi une démarche plutôt déductive qui prend les accidents potentiels comme point de départ de l'APR. Cette divergence entre théorie et pratique existe non seulement au niveau de la démarche mais plus explicitement dans la représentation même d'une APR.

Nous proposons une méthode d'APR qui combine les deux approches inductive et déductive. A notre sens, une telle méthode renforce et perfectionne les démarches conventionnelles et garantie ainsi la qualité des analyses en termes de complétude et de cohérence. En effet, la méthode d'APR que nous retenons [HAD 97] s'articule autour de trois étapes complémentaires et itératives (figure 5).

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 5 schématise les différentes étapes impliquées dans le processus d'analyse de risque que nous retenons [HAD 97].

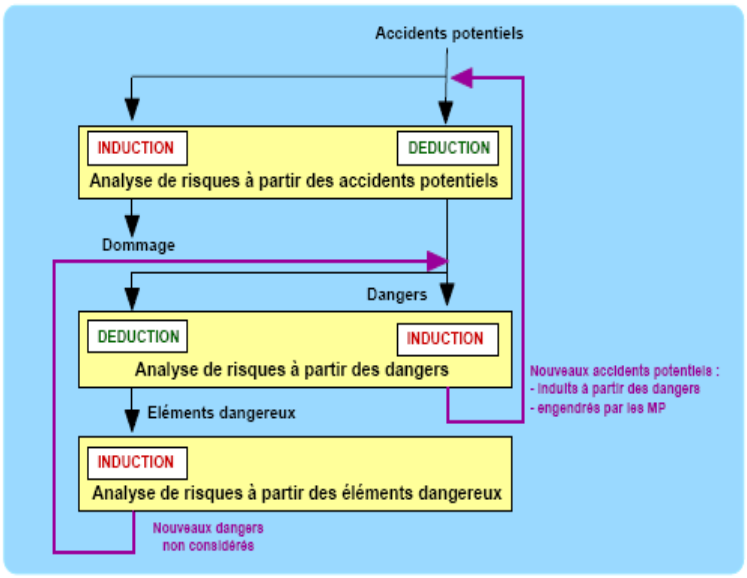

Figure 3. *Principe général de la méthode d'APR retenue [HAD 06b]*

3.1. *Importance de la méthode d'APR proposée dans le processus de construction de la sécurité*

Généralement, le processus de construction de la sécurité d'un système (figure 6) comporte plusieurs analyses complémentaires hiérarchisées [HAD 95 et 96] :

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) [HAD 06b].

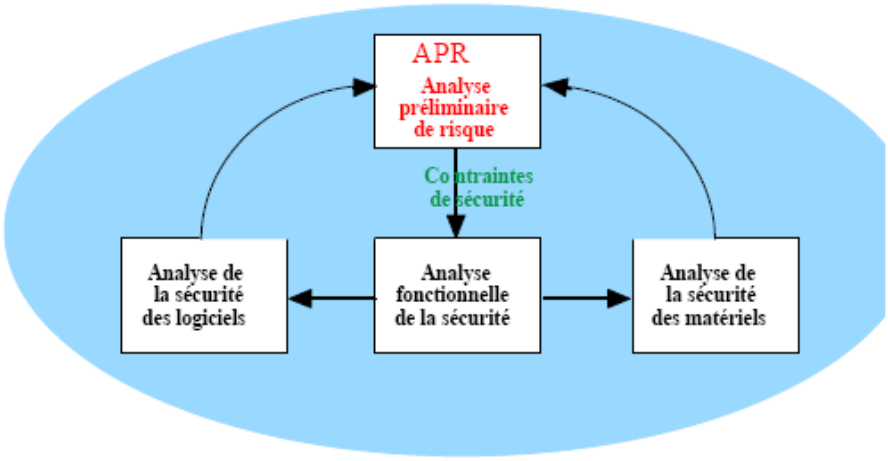

Figure 4. *Place de l'APR dans le processus de construction de la sécurité d'un système de transport [HAD 98]*

L'APR est généralement considérée comme « la première pièce du dossier de sécurité » [CHU 91] (in HAD 98) et représente ainsi la méthode fondamentale dans le processus de construction de la sécurité. En effet, c'est de la qualité et de l'exhaustivité de l'APR dépendent la qualité et la complétude des analyses postérieures (AFS, ASL, ASM).

3.2. *Intégration de la méthode d'APR proposée dans le cycle de développement d'un projet*

Classiquement, Le cycle de développement d'un système correspond à un diagramme en « V » qui comprend les phases de spécification et de conception dans la branche descendante, la phase de réalisation au coin et les phases d'intégration, de validation et d'homologation dans la branche ascendante. C'est en parallèle de ces

activités de développement que les différentes analyses de sécurité se réalisent (figure 4). En effet, à chacune de ces activités correspond une ou plusieurs méthodes d'analyses de sécurité.

L'APR est généralement élaborée pendant la première phase de spécification du système. Les résultats de cette analyse permettent non seulement 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) mais aussi de définir les exigences et critères de sécurité du système (de haut niveau) à prendre en compte lors des phases de conception et de réalisation des équipements matériels et logiciels. 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.

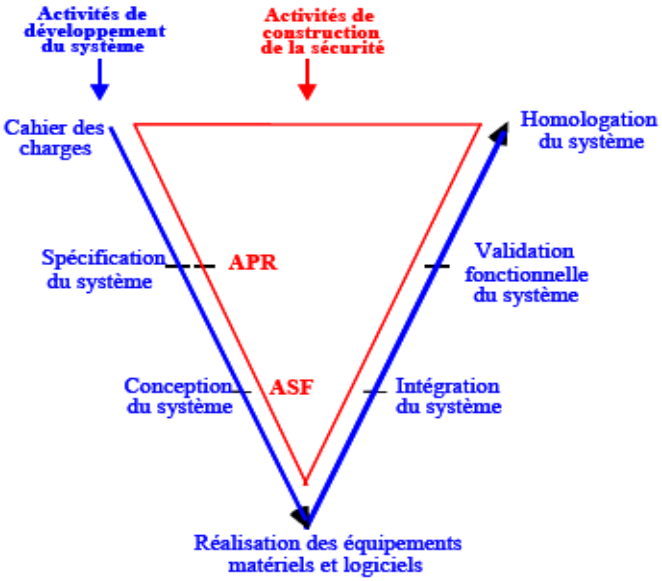

Figure 5. *Place de l'APR dans le cycle de développement d'un système [HAD 98]*

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 des experts du domaine et d'autre part du retour d'expérience (REX) [HAD 06b]. Afin de valider et démontrer le bien-fondé de la méthode d'APR proposée, nous avons fait recours au développement d'une maquette de faisabilité.

4. L'erreur humaine

4.1. *Définition*

La notion d'erreur humaine est un concept très large car elle a des dimensions multiples. Actuellement, il n'existe pas " un référentiel commun " pour définir l'erreur humaine. En effet, le terme erreur humaine couvre plusieurs significations selon l'angle sous lequel elle est vue. La diversité des points de vue est liée à la multiplicité des disciplines qui l'analysent (psychologie, ergonomie, ingénierie, sociologie, philosophie, juridique). En effet, le psychologue examine l'erreur humaine dans la perspective de l'activité qui dépend, en partie, des caractéristiques de la tâche (physiques, techniques, organisationnelles, sociologiques, etc). L'analyse sociologique de l'erreur tient compte non seulement de son coût économique sur le système technique où elle s'insère, mais également, de ses aspects psychologiques. De même, dans le domaine juridique, l'analyse de la responsabilité n'envisage pas l'erreur sous le seul angle de l'infraction, mais se base souvent sur les résultats de l'étude psychologique (rapports entre l'intention et l'erreur). Du point de vue de la philosophie analytique, l'erreur est définie comme étant une action intentionnelle d'un certain type qui a manqué son but (De Beaurepaire C. 1996). L'intention comporte deux éléments, une expression de l'état final à atteindre et une indication des moyens par lesquels il doit être atteint (Reason 1990). L'erreur ne peut être ainsi, définie sans se référer à l'intention humaine, car elle dépend du jugement de l'homme face à une situation spécifique (Rasmussen 1987). Pour l'ergonome, l'erreur humaine est le signe d'une inadéquation, d'un manque de compatibilité entre les caractéristiques techniques, organisationnelles, fonctionnelles... de la situation de travail, et les caractéristiques physiques, mentales, psychosociales...

L'opérateur humain. Leplat (1989) signale que l'erreur humaine est liée à la notion de la " tâche " ainsi qu'à la valeur accordée à cette tâche c'est-à-dire aux buts et aux conditions de l'action. L'erreur humaine en tant que dysfonctionnement du système homme-tâche, est un événement non souhaité, dont la récupération est possible à condition d'avoir été détectée, ou dont les conséquences néfastes doivent être minimisées (Neboit 1996). L'occurrence de l'erreur humaine est ainsi définie par le comportement global du système homme-tâche (Rasmussen 1987).

Dans le domaine du travail, Rasmussen (1983) définit l'erreur humaine comme étant la contrepartie négative de l'activité humaine, susceptible de conduire à une défaillance de l'opérateur (cité par Laprie 1995). La définition adoptée par Leplat (1985) est fondée sur l'analyse de l'activité au sein du travail ; l'erreur apparaît donc comme une caractéristique de l'activité ou comme conséquence de celle-ci. L'erreur constitue donc un révélateur, un indicateur ou un symptôme de l'activité. Elle se traduit par une action inadaptée sur le système, action qui ne réussira pas à rendre les résultats conformes au but. Une erreur humaine n'est pas réductible à l'incapacité ou l'incompétence à réaliser une tâche, mais peut provenir de l'impossibilité dans laquelle se trouve un opérateur d'exécuter correctement une tâche alors qu'il

possède la capacité de le faire. Cette impossibilité peut tout à fait provenir d'une définition incorrecte du travail à faire (De Terssac G. et Chabaud C. 1990).

4.2. *Modélisation et l'erreur humaine*

On distingue diverses taxonomies d'erreurs humaines :
- Le modèle de classification de Rasmussen et Jensen (1974) ;
- Le modèle de classification de Reason (1979) ;
- Le modèle de classification de Rasmussen (1980) ;
- Le modèle de classification de Norman (1981) ;
- Le modèle de classification de Rouse et Rouse (1983) ;
- Le modèle de classification de Swain et Gutmann (1983) ;
- Le modèle de classification de Leplat (1985) ;
- Le modèle de classification de Villemeur (1988) ;
- Le modèle de classification de Nicolet (1989) ;
- Le modèle de classification de Reason (1990) ;
- Le modèle de classification de Cellier (1990) ;
- Le modèle de classification de l'OACI - Organisation de l'Aviation Civile Internationale (1992) ;
- Le modèle de classification de Laprie (1995) ;
- Le modèle de classification de Van Eslande (1997).

Les divers modèles d'erreur humaine élaborées, selon le domaine ou la discipline, se répartissent généralement en deux grandes catégories. La première catégorie est d'ordre conceptuel théorique qui analyse le mode de fonctionnement cognitif de l'homme. Elle offre un modèle générique qui détermine les différentes étapes de raisonnement humain menant à l'action. L'objectif de cette catégorie est d'expliquer les différents mécanismes de production de l'erreur (Rasmussen, Reason, Norman, Rouse, Nicolet). La deuxième catégorie est d'ordre descriptif car elle classe les erreurs indépendamment du sujet. Elle est basée sur l'analyse de la tâche ainsi que sur les conséquences et les traces de l'erreur en termes de comportement ou d'action erronée. Spécifique du travail, elle a pour objectif de prédire et réduire l'erreur afin d'améliorer la fiabilité et la sûreté de fonctionnement des systèmes socio-techniques (Cellier, Leplat, Laprie, Villemeur). Ces différentes approches ont certes contribué à l'évolution des concepts de l'erreur humaine surtout sur le plan psycho-cognitif, mais leur intérêt et leur application pratique demeurent limités voire impossibles. En effet, malgré l'intérêt indéniable de ces modèles, leur mise en oeuvre dans le domaine de la sécurité des transports notamment ferroviaires n'est pas satisfaisante. Aucun modèle, à lui seul, ne permet d'assurer l'exhaustivité de l'analyse. En effet, ces modèles se complètent, mais aucun ne traite le problème dans son ensemble. Aucun modèle, sauf celui de Van Eslande, n'est soutenu par une application industrielle ou un cas réel d'accidents. D'où l'intérêt et l'objectif de ce travail qui s'attache à développer une nouvelle approche méthodologique qui vise l'intégration de l'erreur humaine dans le processus du retour d'expérience et notamment dès la phase de collecte des données.

5. Le retour d'expérience (REX)

Le Rex correspond à un examen approfondi des circonstances conduisant à la réalisation d'événements contraire à la sécurité. C'est une démarche qui vise à mettre en évidence les insuffisances, les dysfonctionnements et les incompatibilités du système de sécurité et à formuler des propositions susceptibles d'éviter de telles situations ou d'en réduire les conséquences (Joing et Keravel 1993). L'objectif est double, il s'agit non seulement de tirer des enseignements pour définir les mesures correctrices de sécurité efficaces à court terme, mais aussi de capitaliser et faire évoluer les connaissances des comportements humains et matériels à moyen terme (Joing 1991), (Dominati et al. 1996), (Ferrandez 1999) et (Wanner J-C 2000). En résumé, le retour d'expérience correspond à un processus dynamique de collecte, de stockage, d'analyse et d'exploitation des données relatives à des situations contraires à la sécurité (accident ou incident). Il consiste en une étude analytique causale des différents facteurs impliqués dans la genèse des incidents ou accidents. Le Rex permet une meilleure compréhension des mécanismes conduisant à des événements d'insécurité. Son but est de tirer profit des enseignements de l'expérience passée pour améliorer le niveau de sécurité en mettant en oeuvre les mesures préventives et correctives adéquates afin d'éviter la reproduction de tels scénarios porteurs de risque.

En termes de Facteur Humain, le Rex " Facteur Humain " concerne tous les événements qui ponctuent la présence de l'homme dans un système à l'intérieur d'un champ d'action. Il peut être considéré comme la capitalisation de données sur l'expérience humaine dans un système (Lamalle Y. 1994 et Malvache et al 1994).

Le Rex " Facteur Humain " repose sur la compréhension de situation de travail pour repérer des critères de sécurité et de fiabilité des systèmes. Son objectif est de tendre vers l'amélioration des performances et de la maîtrise de la fiabilité et de la sécurité des personnes et des systèmes. Le remède aux erreurs humaines revient à améliorer le couplage entre l'homme et les autres éléments du système (Lamalle Y. 1994).

6. Approche d'Intégration de l'erreur humaine dans le retour d'expérience

Afin de répondre aux exigences exprimées par la nouvelle réglementation nationale en matière de sécurité ferroviaire, les organismes nationaux, les gestionnaires d'infrastructure et les professionnels du secteur ferroviaire doivent désormais disposer d'une démarche méthodologique commune de retour d'expérience (Rex). Notre contribution porte sur l'élaboration d'une démarche rigoureuse du Rex centrée sur les facteurs humains. Cette démarche est présentée en deux parties. La première partie propose une approche globale du déroulement de Rex qui fait intervenir cinq grandes phases : collecte des données, analyse des données, stockage des données, exploitation des données et proposition de recommandations. L'accent sera mis sur l'importance des données relatives à l'opérateur humain dans le bon déroulement du Rex. La seconde partie présente une

approche d'analyse de l'erreur humaine centrée sur le déroulement d'un accident (en amont, pendant et en aval). L'objectif est d'extraire et d'identifier les principaux concepts relatifs à l'opérateur humain qu'il faut prendre en compte dès la phase de collecte des données.

La méthode que nous proposons est inspirée des travaux de Reason qui évoque trois niveaux de classification des erreurs humaines (comportemental, contextuel et conceptuel) correspondant à trois questions que l'on peut se poser sur les erreurs humaines (quoi ? où ? comment ?). Elle est également inspirée des travaux de Rasmussen relatifs au fonctionnement cognitif de l'homme et de Van Eslande relatifs aux scénarios types d'accidents. Centrée sur le déroulement d'un accident potentiel, cette méthode (figure 2) s'articule autour de trois niveaux complémentaires d'analyse de l'erreur humaine et reprend les trois niveaux suggérés par Reason : le niveau contextuel (en amont de l'accident), le niveau conceptuel cognitif (pendant l'accident), et le niveau comportemental (en aval de l'accident). Ainsi, à travers les deux premières étapes de l'approche proposée, on peut identifier les différentes erreurs humaines potentielles ainsi que leurs éventuelles interactions. C'est pour cette raison que l'approche proposée sera focalisée uniquement sur les deux premières phases d'analyse afin de déterminer les différents facteurs impliqués dans la production des erreurs humaines potentielles à l'origine de l'accident.

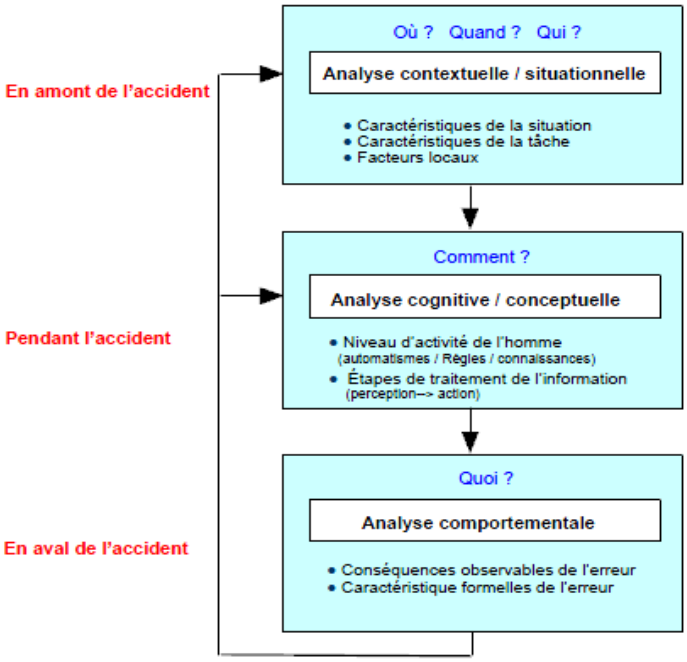

Figure 6. *Approche d'intégration des facteurs humains dans l'analyse des scénarios (Hadj-Mabrouk 2004)*

7. Conclusion

Cet article a présenté notre contribution à l'intégration du facteur humain dans le processus du retour d'expérience. Cette contribution est concrétisée par la proposition de deux approches méthodologiques, la première concerne le déroulement du Rex et la seconde porte sur l'analyse du comportement humain dans l'accident. L'approche globale du processus de Rex s'articule autour de cinq principales étapes : collecte des données, leur analyse et traitement, leur stockage et mémorisation, leur exploitation et utilisation et les recommandations qui en résultent. Cette approche a mis l'accent sur la place capitale de la collecte de données dans la mise en oeuvre et le bon déroulement du processus de Rex. La seconde partie de ce chapitre a été focalisée sur l'étude des données relatives à l'opérateur humain à travers la proposition d'une approche d'analyse de l'erreur humaine centrée sur le déroulement d'un accident. Cette approche fait intervenir trois niveaux d'analyse menés de manière conjointe et complémentaire : En amont de l'accident, (niveau contextuel), pendant l'accident (niveau cognitif conceptuel) et en aval de l'accident (niveau comportemental). L'intérêt et la faisabilité de cette approche sont soutenus par quelques exemples réels issus du domaine de la sécurité ferroviaire. Cette approche permet l'extraction et l'identification des principaux concepts relatifs notamment à l'opérateur humain, à prendre en compte dès la phase de collecte des données. Elle permet également de préciser, à chaque niveau d'analyse, une liste d'erreurs humaines potentielles qui contribuent à l'occurrence des accidents ferroviaires et qu'il faut prendre en considération dans le retour d'expérience pour améliorer le niveau de sécurité des nouveaux systèmes de transports. Néanmoins, cette démarche nécessite sa mise en oeuvre dans des conditions industrielles réelles, afin de valider et, le cas échéant, d'améliorer ce qui demeure une proposition.

8. Bibliographie

[BOU 06] BOULANGER J-L., « Expression et validation des propriétés de sécurité logique et physique pour les systèmes informatiques critiques ». Thèse de Doctorat de l'Université de Technologie Compiègne. 23 Mai 2006.

[BNA 86] Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE). « Guide des méthodes courants d'analyse de la sécurité d'un système missile ou spatial ». Recommendations RE. AERO 70111, Boulogue-Billancourt, 1986.

[CHO et HAD 96] CHOPARD-GUILLAUMOT G., HADJ-MABROUK H. « Définition des principaux concepts relatifs à la notion de sécurité dans les transports guidés ». Revue Générale des Chemins de Fer, Paris, n°2, pp23-36, Février 1996.

[CUI 04] Rémy CUISIGNIEZ. « La réglementation de sécurité à bord des navires marchands », chapitre 13. 2004

[DES et al 03] DESROCHES A., LEROY A., VALL2E F., « la gestion des risques : principes et pratiques ». Edition Hermes-science, 2003.

[HAD 92] HADJ-MABROUK H. Thèse de doctorat en Automatique Industrielle et Humaine. Université de Valenciennes. Titre : « Apprentissage automatique et acquisition des

connaissances : deux approches complémentaires pour les systèmes à base de connaissances. Application au système ACASYA d'aide à la certification des systèmes de transport automatisés ». Décembre 1992.

[HAD 95] HADJ-MABROUK H. « La maitrise des risques dans le domaine des automatismes des systèmes de transport guidés : Le problème de l'évaluation des analyses préliminaires des risques ». Revue Recherche-Transport-Sécurité, Numéro 49, décembre 1995, pp 101-112.

[HAD 96] HADJ-MABROUK H. « Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». Revue Routes et Transports, Montréal, vol. 26, n° 2, 1996.

[HAD 97] 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.

[HAD 98] 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.

[HAD 06a] HADJ-MABROUK H. « L'analyse préliminaire des risques – Application au domaine de la sécurité des transports ferroviaires » (tome pédagogique). Février 1997 (version mise à jour le 19 Décembre 2006).

[HAD 06b] 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-France, 10-12 Octobre 2006.

[KRI et al 05] KRISHNAKUMAR R., PREZELIN N., RAZAFINDRAKOTO H., « Les outils de sureté de fonctionnement », DESS Sécurité des transports, Université de Versailles Saint-Quentin en Yvelines. 2004-2005.

[NOR a] Norme CENELEC EN 50 126: Application ferroviaire – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).

[NOR b] Norme CENELEC EN 50 129 : Application ferroviaire – Systèmes de signalisation, de télécommunications et de traitement è Systèmes électroniques de sécurité pour la signalisation.

[RAP 03] Rapport du comité interministériel à l'aménagement et au développement du territoire du 18/12/03.

[RAP 05a] Rapport de la commission européenne sur la sécurité maritime

[RAP 05b] Rapport de la commission européenne sur les autoroutes de la mer. Article 12-bis des orientations RTE-T 2005.

[RAP 05c] Rapport de la Direction générale de la mer et des transports sur les autoroutes de la mer. 16 Juin 2005.

[RAP 06] Rapport de la commission européenne sur les appels à manifestation pour le lancement des projets des autoroutes de la mer

[RAP 07] projet transport Euro-Méditerranéen des autoroutes de la mer MEDA-MOS. Appel à projet octobre 2007.

[ROD 07] Jean-paul RODREGUE. « Straits, Passages and Chokepoints: A Maritime Geostrategy of Petroleum Distribution", in S.K. Multani (ed) Maritime Trade and Security, Hyderabad: ICFAI University Press, 2007. (Note: this is a reprint of an article published in 2004).

BOURDEAUX I. et GILBERT C. (1999) ; Procédures de retour d'expérience, d'apprentissage et de vigilance organisationnels : Approches croisées ; Programme risques collectifs et situations de crise, Grenoble, CNRS, septembre 1999

CARRON P. et KAPPES-GRANGE Y. (1993) ; Sécurité ferroviaire ; Revue RATP Entre les Lignes, n° 31, avril 1993

CELLIER J.M. (1990), L'erreur humaine dans le travail, Les facteurs humains de la fiabilité dans les systèmes complexes (Leplat J. et De TerssacG.), Ed Octarès, 1990

CIRCULAIRE OACI, 238-AN/143 (1992), Facteurs humains : ergonomie ; 3-9

DE TERSSAC G. et CHABAUD C. (1990), Référentiel opératif commun et fiabilité , Les facteurs humains de la fiabilité dans les systèmes complexes, Ed. Octarès 1990

DIRECTIVE 2004/49/CE concernant la sécurité des chemins de fer communautaires, 29avril 2004.

DOMINATI A., BONNEAU A. et LEWKOWITCH-ORLANDI A. (1996) 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 λμ n° 10, octobre 1996

FERRANDEZ F. (1999). L'apport des études détaillées d'accidents aux retours d'expérience en sécurité routière. Annales des Ponts et Chaussées n° 91, 1999, 36-42

GILBERT C. (2001) ; Retours d'expérience : le poids des contraintes, Annales des mines, avril 2001, 9-24

HADJ-MABROUK A. HADJ-MABROUK H. (2004) ; Approche d'intégration de l'erreur humaine dans le retour d'expérience, collections INRETS, synthèse n° 43, 104p, (à paraître)

HADJ-MABROUK H. (1996) Projet FACTHUS : prise en compte des facteurs humains dans le développement des projets industriels, Convention INRETS/DTT, rapport n° ESTAS/A-96-65, diffusion restreinte, 73 p, Arcueil, décembre 1996.

HADJ-MABROUK H. (1996), La nécessité de prendre en compte l'erreur humaine dans l'analyse de sécurité et le développement des systèmes de transports guidés.