Méthode et Formalisme de base pour l'Analyse Préliminaire des Risques dans le Transport Ferroviaire

Mohamed Habib Mazouni, Habib Hadj Mabrouk

Méthode et Formalisme de base pour l'Analyse Préliminaire des Risques dans le Transport Ferroviaire

Mohamed Habib MAZOUNI

Habib Hadj-Mabrouk

INRETS
2, Avenue du Général Malleret-Joinville
F-94114 Arcueil Cedex FRANCE
Tel : (33) 1 47 40 72 13
Fax: (33) 1 45 47 56 06
mazouni@inrets.fr

Résumé :

Les approches des spécialistes vis-à-vis de l'analyse préliminaire des risques (APR) sont très diverses, les choix de représentations variés et les terminologies imprécises ou même parfois contradictoires. En effet, la terminologie et les concepts liés aux APR sont très fluctuants d'un système de transport à un autre ou d'un constructeur à un autre.

Les normes et les standards de gestion des risques se veulent génériques, de ce fait les constructeurs élaborent chacun son manuel de maîtrise des risques dans lequel sont documentées des méthodes adéquates, ceci avec un vocabulaire et un formalisme et un savoir-faire qui lui sont propres.

Ces divergences contextuelles furent et sont toujours l'objet de travaux de recherche afin de réaliser un objectif qui jusqu'à lors s'atteint doucement mais sûrement, c'est de converger vers une réelle standardisation d'un formalisme et d'un processus d'analyse et d'appuyer ensuite les experts par des outils d'aide à l'élaboration et l'évaluation des dossiers d'APR.

L'objet de cet article est de proposer un formalisme de représentation de connaissance nécessaire pour l'élaboration d'une approche d'analyse des risques. Le formalisme retenu et la méthode d'analyse proposée devraient amorcer le développement d'un système à base de connaissance d'aide à l'APR.

Mots Clés : *Analyse Préliminaire des Risques (APR), Accident Potentiel, Niveau de Risque, Transport, Formalisation, Induction, Déduction, Rétroaction.*

I. L'Analyse Préliminaire des Risques

Le Dossier de Sécurité (DS) d'un système de transport ferroviaire est une pièce exigée par la réglementation française [Cf. décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national et son arrêté d'application du 08 janvier 2002]. Il contient une démonstration de l'aptitude du système à être exploité et maintenu avec le niveau de sécurité requis, autrement dit, une attestation de la couverture des risques identifiés dans l'APR [MAZOUNI, 05].

Il convient donc que l'analyse préliminaire des risques (APR) identifie les accidents potentiels liés au système et à ses interfaces afin d'évaluer leurs probabilité d'occurrence et gravité des dommages et enfin de proposer les solutions permettant de maîtriser les risques.

La pratique de l'APR relève essentiellement du savoir-faire des experts. Ces derniers ont pour mission prévoir à travers cet exercice la totalité des événements indésirables, envisager les solutions adéquates qui seraient intégrées dans la conception du système inhérent. Le système et son dossier d'APR ont la même durée de vie [*Cf.* réglementation française, article 17 du décret n° 2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés]. En effet, la conception est revue à chaque fois que la correction d'une défaillance renvoi inévitablement à la modification de la l'architecture du système. Dans le cas échéant, le dossier d'APR est rouvert afin de réévaluer l'impact des changements qu'ont affecté le système sur la sécurité globale.

Les résultats de l'APR permettent de définir pour le système global les exigences et critères de sécurité à considérer lors des phases de conception et de réalisation des équipements matériels et logiciels et enfin d'établir les lignes directrices de l'Analyses de Sécurité Fonctionnelle « Fig. 1 ».

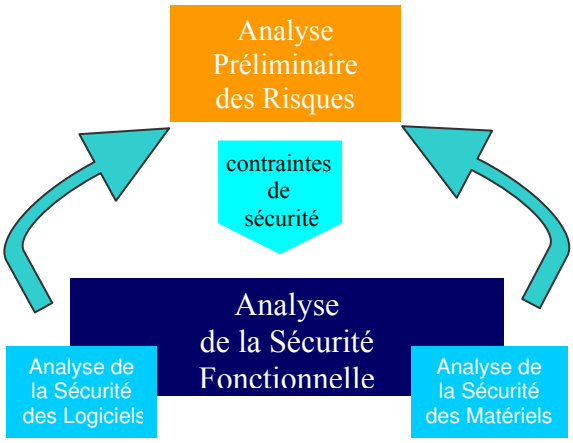

Fig. 1 Place de l'APR parmi les autres analyses [HADJ, 97]

II. Formalisme de base

Compte tenu la divergence dans l'emploi des termes et leur interprétation, il serait plus sage d'arrêter au préalable de toute étude un formalisme précis. La figure « Fig. 2 » propose un extrait du modèle syntaxique retenu :

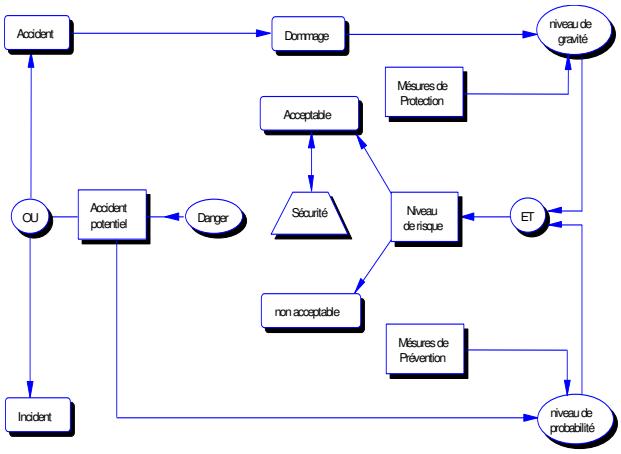

Fig. 2 Articulation de quelques concepts de base de la sécurité des systèmes de transport [HADJ, 95,03]

Les paragraphes suivants détaillent les concepts de base d'APR représentés dans la figure (Fig.2).

II.1 Accident Potentiel

Deux concepts de base sont facilement identifiables : l'« Accident potentiel » qui est une supposition prématurée et le « niveau de risque » qui est une qualification des conséquences abouties.

Le lien reliant le danger à l'accident potentiel (accident ou incident) schématise le passage par une situation dangereuse. Seule l'occurrence d'un événement dommageable attribue une identité accidentelle à l'Accident Potentiel, sinon l'Accident potentiel est simplement un Incident.

II.2 Dommage

La notion de dommage est relativement définie de la même façon dans la norme ISO 14971 (2000) et la norme générique CEI 300-3-9 (1995). La définition générique du ISO/CEI Guide 51 (1999) est utilisée dans le domaine médical où le dommage est défini comme : blessure physique ou une atteinte à la santé des personnes ou dégât causé aux biens ou à l'environnement.

II.3 Gravité

La nuisance des dommages provoqués par un Accident est évaluée par un niveau de gravité.
Pour les systèmes de transport, la notion de *gravité* est identique à de nombreux autres domaines technologiques. Voici un exemple :

- **Mineur :** peut éventuellement conduire à un ou plusieurs blessés légers et/ou à des dommages limités au niveau des trains ou des installations.
- **Significatif :** peut éventuellement conduire à un blessé grave et/ou des dégâts importants au(x) train(s) et/ou aux installations.
- **Critique :** peut éventuellement conduire à un mort et/ou plusieurs blessés graves.
- **Catastrophique :** peut éventuellement conduire à plusieurs morts et des blessés graves.

Notons que même si le choix des termes qualifiants les niveaux de gravité se fait sans règles de base, la correspondance qualitative quantitative résout les divergences possibles. Certains industriels ou exploitants tel que l'RATP préfèrent tout simplement numéroter les différents niveaux de gravité (niveau 0, niveau 1, niveau 2, niveau 3) afin d'éviter de mauvaises interprétations des termes qualificatifs en cas d'audit ou demande d'avis d'experts.

Dans le domaine de la médecine, la gravité concerne seulement l'impact sur l'humain [ISO 14971, 00] :

- **Catastrophique :** décès d'une ou plusieurs personnes
- **Majeur :** blessures ou maladies graves, infirmité permanente
- **Mineur :** blessures ou maladies mineures nécessitant un traitement médical
- **Minime :** légères blessures relevant des premiers soins (ne nécessitant pas un traitement médical)
- **Négligeable :** incident n'exigeant aucun traitement médical

Notons qu'il est toujours préférable de définir un nombre pair de métriques par soucis d'éviter la tendance naturelle de retenir la position médiane d'une classification impaire.

II.4 Probabilité d'Occurrence

L'accident ou l'incident se caractérise aussi par sa probabilité d'occurrence, autrement dit, la fréquence de sa survenue. Les probabilités sont regroupées dans des plages prédéfinies en appliquant une correspondance quantitative/ qualitative. Toutefois, le terme *probabilité* est généralement conservé. La norme ISO 14971 (2000) évoque le fait qu'«***une bonne description qualitative est préférable à une inexactitude quantitative***». Ceci provient en particulier de la difficulté d'estimer ces probabilités (retour d'expérience, techniques d'analyse ou de simulations, avis d'experts, etc.).

La liste suivante présente -à titre indicatif- un exemple de niveaux de probabilité d'occurrence utilisables pour une estimation qualitative :

- **Fréquente** (>1)
- **Probable** (1 *à* 10^{-2})
- **Occasionnelle** (10^{-2} *à* 10^{-4})
- **Improbable** (<10^{-4})

Dans cette classification, la qualification « *Fréquente* » indique une fréquence d'occurrence de l'accident potentiel plusieurs fois par an et « *Improbable* » correspond à une occurrence tous les 10000 ans.
Cette métrique donne une idée sur ce qu'est une fréquence d'occurrence. Dans les systèmes de transport, cette estimation dépend significativement du trafic (trajets ou nombre de kilomètres parcourus dans le ferroviaire et le routier, miles ou nombre de vols dans l'aérien….).

L'estimation des probabilités d'occurrence est l'une des tâches cruciales du processus d'APR [MAZOUNI, 2005]. Les travaux de recherche réalisés dans cette optique ont souvent mis en évidence cette phase sans pour autant proposer de solutions satisfaisantes. Dans les domaines de technologies de pointe tel que le nucléaire on a développé des méthodes pertinentes, mais qui ne sont ni génériques ni adaptables aux autres domaines, en l'occurrence le domaine des transports.

II.5 Niveau de Risque et Sécurité

Les niveaux de gravité ou de probabilité d'occurrence sont croisés dans une matrice de criticité. Cette matrice permet de spécifier les zones à risque où la sécurité est plus au moins menacée.

Le niveau de risque est la résultante du niveau de gravité et celui de probabilité d'occurrence. En s'inspirant de la classification graphique des niveaux d'alerte du plan Vigipirate français (4 niveaux d'alerte: écarlate, rouge, orange, jaune) mais en rajoutant un cinquième niveau "zone blanche" pour

représenter le risque négligeable, on a obtenu la représentation suivante :

	Catastroph -ique	Critique	Significatif	Mineur
Fréquente				
Probable				
Occasionnelle				
Improbable				

En observant cette matrice de criticité, on arrive à distinguer 5 zones à risque :

- *Zone écarlate* : niveau de risque très élevé.
- *Zone rouge* : niveau de risque élevé.
- *Zone orange* : niveau de risque important.
- *Zone jaune* : niveau de risque considérable.
- *Zone blanche*: niveau de risque négligeable.

II.6 Mesures de protection et de prévention

Des mesures de protection ou de prévention sont obligatoirement mises en œuvre afin de réduire le niveau de risque à un niveau acceptable.
Initialement, le risque appartient à l'une des 5 zones en question. La maîtrise du risque a pour vocation de faire déplacer cette appartenance vers la zone la plus claire possible, autrement dit, horizontalement à droite en réduisant la gravité des dommages encourus ou verticalement vers le bas en réduisant les possibilités d'occurrence d'accident.

III. Méthode d'Analyse des risques

Il est nécessaire d'identifier les phénomènes dangereux qui engendrent un risque dans le système ainsi que les formes qu'ils pourraient prendre. Il faut donc énoncer clairement les éléments dangereux constatés et principalement ceux qui sont à l'origine des accidents vécus auparavant selon les procédés du retour d'expérience [LégiFrance, 00,03].

Les données exploitées par l'APR sont de natures diverses : symboliques, descriptives, numériques, etc. Elles peuvent être inexactes, ambiguës, incomplètes et parfois contradictoires étant donné que l'APR s'effectue tôt à une phase prématurée du cycle de développement d'un système, plus précisément entre la phase de spécification et celle de conception. En effet, il convient que la phase de recueil de données soit faite en se basant sur un formalisme solide. Evidemment, ceci rend plus accessible les phases de capitalisation et d'exploitation.

Il convient de rappeler que l'APR a toujours été considérée comme une démarche inductive. Rares sont les travaux de recherche qui font allusion à une démarche purement déductive ou mixte inductive/déductive.

C'est très important de savoir qu'une démarche inductive/déductive n'est pas forcément rétroactive. La rétroaction est une particularité qui permet de filtrer des résultats cohérents parmi un ensemble initial d'éléments brutes, autrement dit, les nouveaux éléments (résultats) identifiés par les mécanismes d'inférence seraient à leur tour réintroduits et donc exploités (données). Cependant, une démarche inductive/déductive permet d'atteindre une bonne traçabilité et une meilleure complétude en matière de résultats

Complétude, traçabilité et cohérence des résultats ! Ne sont-elles pas des caractéristiques d'une analyse des risques convenable? Est-il donc possible de conjuguer le principe de rétroaction et les démarches dites inductive, déductive?

La figure suivante (Fig. 3) propose une régénération de la méthode originale d'APR proposée par Habib Hadj-Mabrouk [HADJ, 97].

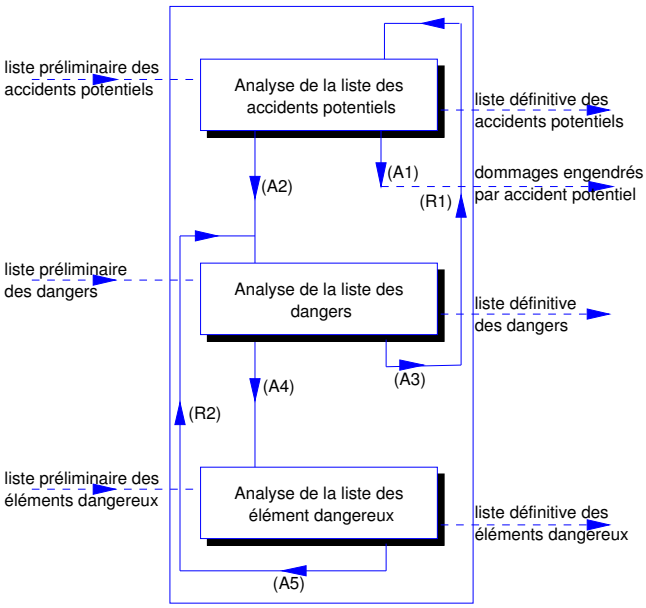

Fig. 3 Méthode inductive/ déductive rétroactive d'Analyse des Risques

Cette démarche inclut tout à la fois des phases de raisonnement déductives (A2, A4) et inductives (A1, A3, A5) ainsi que deux boucles de rétroaction (R1, R2) :

Les actions:

A1: phase inductive à partir des accidents potentiels pour identifier les éventuels dommages.
A2: phase déductive à partir des accidents potentiels pour identifiés les dangers.
A3: phase inductive à partir des dangers pour identifier les accidents potentiels.
A4: phase déductive à partir des dangers pour identifier les éléments dangereux correspondants.
A5: phase inductive à partir des éléments dangereux pour identifier les dangers qui peuvent surgir.

Les rétroactions:

R1: rétroaction en cas d'identification de nouveaux accidents potentiels à l'issue de la phase A3.
R2: rétroaction en cas d'identification de nouveaux dangers à l'issu de la phase A5.

Ordonnancement du processus d'analyse:

L'analyse de la liste des accidents potentiels exploite une liste préélaborée d'accidents potentiels pour en conclure les dommages possibles **(A1)**, on récupère en même temps à l'issue de cette phase une liste de dangers **(A2)**, cette dernière est ajoutée à une liste de dangers préliminaire, la liste obtenue est introduite pour une nouvelle phase qui retourne comme résultat la liste des accidents potentiels **(A3)** et aussi la liste des éléments dangereux correspondants **(A4)** qui seront examinés pour identifier les dangers inhérents **(A5)**.

Les nouveaux accidents potentiels et les nouveaux dangers identifiés respectivement lors des phases (**A3),** (**A5)** seraient examinés lors du prochain cycle de traitement (respectivement (**R1**) et (**R2**)).

En résumé, un cycle de traitement contient 3 phases d'analyse:

1. Analyse à partir des accidents potentiels,
2. Analyse à partir des dangers,
3. Analyse à partir des éléments dangereux.

L'introduction des rétroactions dans la démarche favorise la complétude de l'APR en permettant de dresser une nouvelle fois et de manière différente la liste des accidents potentiels et des dangers et de les enrichir au fur et à mesure.

L'arrêt de l'analyse est conditionné par l'atteinte d'un point fixe. Un point fixe renvoie à l'atteinte d'une configuration stationnaire, c'est-à-dire qu'à un cycle donné, aucun nouvel élément n'est identifié par les mécanismes d'induction ou déduction.

Soit $\boldsymbol{ANALYSE_1}$, $\boldsymbol{ANALYSE_2}$, $\boldsymbol{ANALYSE_3}$ les fonctions représentant les 3 phases d'analyse à partir des accidents potentiels, des dangers et des éléments dangereux. Soit $\boldsymbol{X_1}$, $\boldsymbol{X_2}$, $\boldsymbol{X_3}$: 3 variables représentant respectivement les sous ensemble d'accidents potentiels, de dangers et d'éléments dangereux :

Arrêt de l'analyse si et seulement si on obtient la configuration suivante :
$\boldsymbol{ANALYSE_1.A2(X_1) = X_2}$
$\boldsymbol{ANALYSE_2.A4\ (X_2) = X_3}$
$\boldsymbol{ANALYSE_2.A3(X_2) = X_1}$
$\boldsymbol{ANALYSE_3.A5(X_3) = X_2}$

L'exploitation de trois segments sources de données (liste des accidents potentiels, liste des dangers, liste des éléments dangereux) au même temps en lecture (données en entrée) et en écriture (résultats) fait appel à des techniques de l'informatique distribuée et notamment d'exclusion mutuelle. En outre, l'ordonnancement des différentes phases d'un cycle de traitement dépend de plusieurs facteurs telle que la qualité des données en entrée. Les 3 phases d'analyse sont ordonnées circulairement, on peut donc commencer par n'importe laquelle.

Conclusion

Dans ce papier nous avons présenté dans un premier temps une ébauche du formalisme de base qu'on a définit pour une Analyse Préliminaire des Risques appliquée dans le domaine des transport. Ensuite, nous avons exposé une méthode d'APR de type inductive/déductive rétroactive regroupant à la fois 3 actions inductives, 2 actions déductives et 2 rétroactions.

Nos travaux se poursuivent actuellement sur la conception et l'élaboration d'une base de connaissance d'APR et notamment l'exploitation de ces connaissances par un outil décisionnel d'aide à l'évaluation et l'élaboration de cette analyse.

Bibliographie

[CEI, 95] « Gestion de la sûreté de fonctionnement », CEI 300-3-9, première édition, 1995.

[CENELEC, 94] « Principes directeurs pour inclure dans les normes les aspects liés à la sécurité », CENELEC, Mémorandum n°9, Edition n°1, 1994.

[CENELEC, 05] « sécurité fonctionnelle - systèmes instrumentés de sécurité pour le secteur des industries de transformation », NF EN 61511, mars 2005.

[HADJ, 95] HADJ-MABROUK H., « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés», *RTS*, n°49, pp 101-112, France, Décembre 1995.

[HADJ, 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*, 1997.

[HADJ, 99] HADJ-MABROUK H., *Projet SAPRISTI : l'analyse préliminaire de risques des systèmes de transports guidés. Principaux travaux réalisés de 1994 à 1998.* , Rapport d'étape n° ESTAS/A-99-16, Arcueil, septembre 1999. *(diffusion restreinte).*

[HADJ, 03] HADJ-MABROUK H., *Concepts de base pour la sécurité des transports ferroviaires,* Rapport, Janvier 2003 *(Diffusion restreinte).*

[ISO 14971, 00] « Application de la gestion des risques aux dispositifs médicaux», ISO 14971, première édition , 2000.

[ISO/CEI, 99] « Aspects liés à la sécurité – principes directeurs pour les inclure dans les normes », Guide ISO/CEI 51, 1999.

[MAZOUNI, 05] MAZOUNI M-H., HADJ-MABROUK H., « L'analyse des risques d'accidents dans les transports ferroviaires » *40e Congrès annuel de l'AQTR (Association Québécoise du Transports et des Routes)*, Québec-Laval, Avril 2005.

[LégiFrance, 00] Décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national et son arrêté d'application du 08 janvier 2002

[LégiFrance, 03] Article 17 du décret n° 2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés

[VigiPirate, 78] VigiPirate : « Dispositif de sécurité français destiné à prévenir les menaces ou à réagir face aux actions terroristes »
Site Officiel du Ministère de l'intérieur :
http://www.interieur.gouv.fr