Analyse des risques des systèmes de transport intelligents

Habib Hadj-Mabrouk

Workshop, Rabat 20 octobre 2009
Rôle des nouvelles technologies et des infrastructures dans la sûreté et la sécurité des systèmes de transport

Analyse des risques des systèmes de transport intelligents

Habib HADJ-MABROUK
Docteur en automatique industrielle et humaine
Habilité à Diriger des Recherches (HDR)
Chargé de recherche
INRETS Marne-la-Vallée. Bâtiment Nobel
23 rue Alfred Nobel – 77420 Champs-Sur-Marne – France
Mobile : + 33 612276612 – e-mail : mabrouk@inrets.fr

1. Introduction aux systèmes de transport intelligents (STI)

Les technologies de l'information et de la communication (TIC ou *NTIC* pour *« Nouvelles Technologies de l'Information et de la Communication »* ou IT pour *« Information Technology »*) ont un rôle primordial pour la promotion de la cohésion territoriale et l'amélioration de l'accessibilité. Ces technologies favorisent les interactions et les communications quotidiennes notamment en améliorant la gestion et le fonctionnement des transports de masse ainsi que le développement des systèmes de transports multimodaux. Les TIC regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, de l'internet et des télécommunications.

Les systèmes de transport intelligents (STI) (en anglais *Intelligent Transportation Systems (ITS)*) désignent les applications des nouvelles technologies de l'information et de la communication au domaine des transports. On les dit "Intelligents" parce que leur développement repose sur des fonctions généralement associées à l'intelligence : capacités sensorielles, mémoire, communication, traitement de l'information et comportement adaptatif. Il s'agit des systèmes dans lesquels sont appliquées des technologies de l'information et des communications pour soutenir le transport routier (notamment l'infrastructure, les véhicules et les usagers) et la gestion de la circulation et de la mobilité, ainsi que les interfaces avec d'autres modes de transport, notamment la mise en place d'une tarification interopérable multimodale. En effet, on trouve les STI dans plusieurs champs d'activité : dans l'optimisation de l'utilisation des infrastructures de transport, dans l'amélioration de la sécurité (notamment de la sécurité routière) et de la sûreté ainsi que dans le développement des services. Les STI interviennent dans un contexte mondial de congestion du trafic routier d'une part et de développement des nouvelles technologies de l'information d'autre part, en particulier dans les domaines de la simulation, du contrôle en temps-réel et des réseaux de télécommunication. On peut distinguer quatre grandes périodes dans le développement des STI :

- Années 1960-1970 : les prémisses
- Années 1980-1995 : investissement dans l'information routière embarquée
- Années 1995-2000 : interopérabilité, billettique et autoroute automatisée
- Années 2000-2005 : mobilité durable, multimodalité et sécurité routière.

2. Contribution et rôle des systèmes de transport intelligents (STI)

Les STI peuvent aider à une meilleure organisation de la multimodalité. Dans des zones où l'infrastructure urbaine se développe moins rapidement que la demande de mobilité, les systèmes STI apparaissent comme un ultime recours pour maintenir un fonctionnement régulier des réseaux. De récentes actions gouvernementales dans le domaine des STI sont davantage motivées par le besoin ressenti de sécurité du territoire. Bon nombre de STI se focalisent sur la surveillance des routes. Les STI peuvent aussi jouer un rôle important dans une évacuation de masse rapide des centres d'affaires urbains en cas d'évènements causant un nombre important de victimes comme des catastrophes naturelles ou d'autres menaces. Les technologies utilisées dans les systèmes de transport intelligents varient, allant de systèmes de gestion basiques comme les systèmes de gestion des carrefours à feux, les systèmes de gestion des conteneurs, les panneaux à messages variables, les radars automatiques ou la vidéo-surveillance aux applications plus avancées qui intègrent des données en temps-réel

avec retours d'informations de nombreuses sources, comme les informations météorologiques, les systèmes de dégivrage des ponts, les systèmes de navigation embarqués informant des temps de parcours en temps réel etc.
A ce jour, il existe plusieurs technologies implantées dans les STI comme la technologie de localisation, les communications sans fil, les technologies de calcul, les technologies de capteurs, les boucles électromagnétiques, les capteurs vidéo, etc. Les applications pour les transports intelligents sont multiples : le paiement électronique, la gestion d'urgence, en particulier en cas d'accident de la route, la gestion du trafic pour fluidifier les axes routiers et favoriser la circulation des transports publics, les transports publics des voyageurs pour optimiser l'exploitation du réseau, pour améliorer le confort des usagers et leur sécurité, les aides à la conduite pour les usagers de la route en vue d'améliorer la sécurité des personnes, de confort des usagers, de diminution des émissions de polluants, la gestion des flottes et du fret pour le transport de marchandises, le contrôle du respect de la réglementation comme les radars automatiques pour le contrôle de la vitesse et le contrôle automatisé du franchissement de feux rouges et en fin la gestion de données partagées pour connaître les caractéristiques des réseaux, les caractéristiques de la demande de trafic et des problèmes récurrents.

3. Facteurs affectant le développement des STI

Les STI sont des applications avancées qui, tout en ne représentant pas l'intelligence en tant que telle, visent à fournir des services innovants liés aux modes de transport et à la gestion de la circulation, et à permettre à différents utilisateurs d'être mieux informés et de faire un usage plus sûr, plus coordonné et plus "intelligent" des réseaux de transport. Dans la mise en place de nouveaux services plus performants (pour gérer au mieux une infrastructure ou un réseau de transports, améliorer le service à l'usager en anticipant les difficultés, en l'informant, garantir la sécurité, élargir l'offre…) les nouvelles solutions technologiques d'information et de communication jouent souvent un rôle essentiel. Mais, ces systèmes de transports intelligents, même s'ils facilitent les remontées, les traitements et les échanges d'information, ne sont pas les garants, en eux-mêmes, et peuvent soulever de nouvelles problématiques qui nécessitent une attention particulière :

- Comment valider, homologuer et certifier les équipements matériels et logiciels impliqués dans les STI ?
- Faut-il mettre en place un organisme ou service technique indépendant (organisme de certification) spécifique pour les applications STI ?
- Comment s'assurer que les équipements STI sont bien installés, bien entretenus et convenablement utilisés pour éviter les risques potentiels ?
- Comment garantir que les équipements STI exploités ne compromettent pas la santé et la sécurité des personnes et de l'environnement ?
- Les STI sont généralement réputés satisfaire à des spécifications techniques adoptées conformément à la réglementation en vigueur. Y a t-il des normes pertinentes consacrées aux STI ? Si oui, qu'elles sont les normes et réglementations nationale et européenne à mettre en œuvre pour évaluer et s'assurer de la conformité des équipements STI avant leurs mises en exploitation ?
- Comment s'assurer du bon fonctionnement des applications et/ou services STI sans prendre en compte et traiter les données à caractère personnel et confidentiel ? Les données et les enregistrements des STI doivent êtres protégés contre toute utilisation abusive, notamment les accès non autorisés, les modifications ou les pertes d'informations.
- Comment prendre en compte le problème d'interopérabilité des STI ?
- Comment développer des IHM ergonomiques qui favorisent une bonne coopération et communication Homme-Machine (STI) et Homme-Homme ?
- Comment concevoir et mettre en œuvre des systèmes de retour d'expérience (Rex) pour capitaliser et pérenniser l'expérience et le savoir faire des STI notamment en matière de sûreté et de sécurité ?
- Comment prendre en compte les facteurs humains liés à l'exploitation des STI ?
- **Comment s'assurer que l'exploitation des équipements matériels et logiciel STI n'induisent pas des risques ou dangers potentiels sur l'homme et/ou l'environnement ?**

Afin apporter un élément de réponse au dernier problème soulevé, relatif à la gestion et la maîtrise des risques dans les STI, on propose dans le cadre de ce Workshop une méthode d'Analyse Préliminaire des Risques (APR). Cette nouvelle approche méthodologique, qui est en cours de développement et de validation, s'inscrit dans le cadre du projet SAPRISTI initié à l'INRETS par HADJ-MABROUK depuis 1996.

4. Contribution de la méthode d'analyse préliminaire des risques aux STI

La sûreté est de façon générale un état de protection contre le danger ou les menaces. C'est une notion qui se focalise essentiellement sur la protection contre les dangers qui viennent de l'extérieur, à la différence de la sécurité qui, elle, est la condition de protection contre des défauts, des dommages, des erreurs, dangers, à caractère physique, financier, politique, émotionnel, psychologique, etc.
Beaucoup de systèmes d'information modernes, qui impliquent du logiciel et/ou du matériel, deviennent critiques sur le plan de la sûreté à cause des pertes de contrats ou des pertes financières, ou même de pertes en vies humaines qui pourraient résulter d'une mauvaise conception ou d'une défaillance et/ou d'une attaque malveillante.

La méthode d'Analyse Préliminaire des Risques (APR) peut être d'un apport bénéfique pour appréhender certains problèmes et améliorer ainsi le niveau de sécurité des STI.

4.1. Processus de construction de la sécurité d'un système de transport

Généralement, le processus de construction de la sécurité d'un système comporte plusieurs analyses complémentaires hiérarchisées [6], [7] et [8] : 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 œuvre 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. Le paragraphe suivant présente la principale méthode d'analyse de la sécurité des systèmes industriels : l'analyse préliminaire de risques.

4.2. L'analyse préliminaire des risques (APR)

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 [7]. 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. Lorsqu'on se limite à évaluer (généralement qualitativement) la gravité des dommages que pourraient causer les accidents potentiels, on parle d'analyse préliminaire des dangers, ou APD [10]. 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 (retour d'expérience). L'APR est un dossier qui reste généralement ouvert pendant toute l'étude et est constamment mis à jour. Du fait que cette analyse est réalisée très tôt dans le déroulement du programme, ses résultats peuvent être incomplets et imprécis. Une APR doit être donc complétée et mise à jour jusqu'à ce que la conception du système soit assez avancée (figure 1). Ceci permet de vérifier qu'à chaque accident potentiel de la liste correspond, dans la conception, une fonction, une précaution ou disposition pour contrôler, réduire ou éliminer sa probabilité d'occurrence [6].

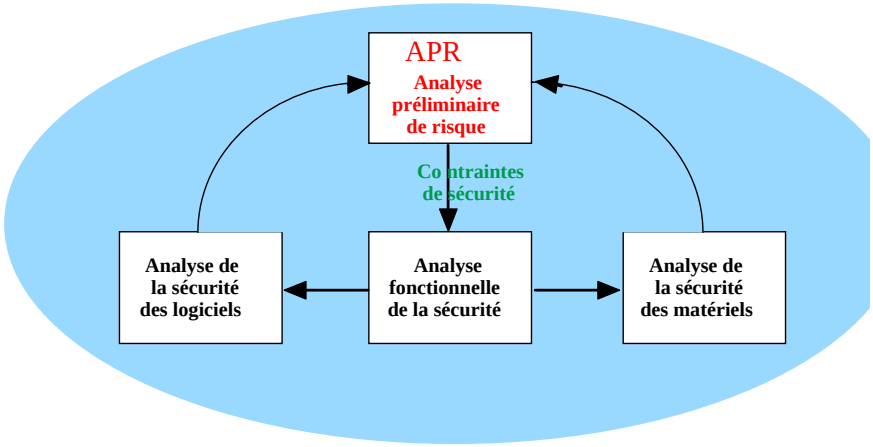

Figure1. Place de l'APR dans le processus de construction de la sécurité d'un système [6] et [8]

L'analyse préliminaire de risques est généralement classée en théorie parmi les démarches inductives [9] et [10]. Dans la démarche inductive, le raisonnement 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. Autrement dit, les méthodes inductives partent des événements élémentaires, soit pour rechercher directement les conséquences (ex : AMDE, AEEL), soit pour identifier les combinaisons d'événements qui peuvent avoir des conséquences critiques (ex : MCPR). Dans le cadre de l'APR, il s'agit de rechercher principalement, par induction, l'ensemble des accidents potentiels à partir de dangers (ou éléments dangereux). Cependant, dans la pratique et notamment dans le domaine de la sécurité des transports guidés, on utilise essentiellement une démarche déductive telle que la méthode de l'arbre de causes (MAC). Afin de renforcer la qualité des APR en termes de complétude et de cohérence, nous suggérons une méthode qui combine ces deux approches [7] et [8]. En effet, l'analyse de sécurité d'un système complexe nécessite de la part des experts du domaine la mise en œuvre d'un processus d'analyse itératif faisant intervenir à la fois des approches inductives et déductives. Il est généralement indispensable de recouper les résultats obtenus par une approche avec ceux obtenus au moyen d'une autre approche complémentaire.

4.3. Proposition d'une méthode originale d'APR

La méthode développée s'articule autour de trois étapes complémentaires et itératives [8]. 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.

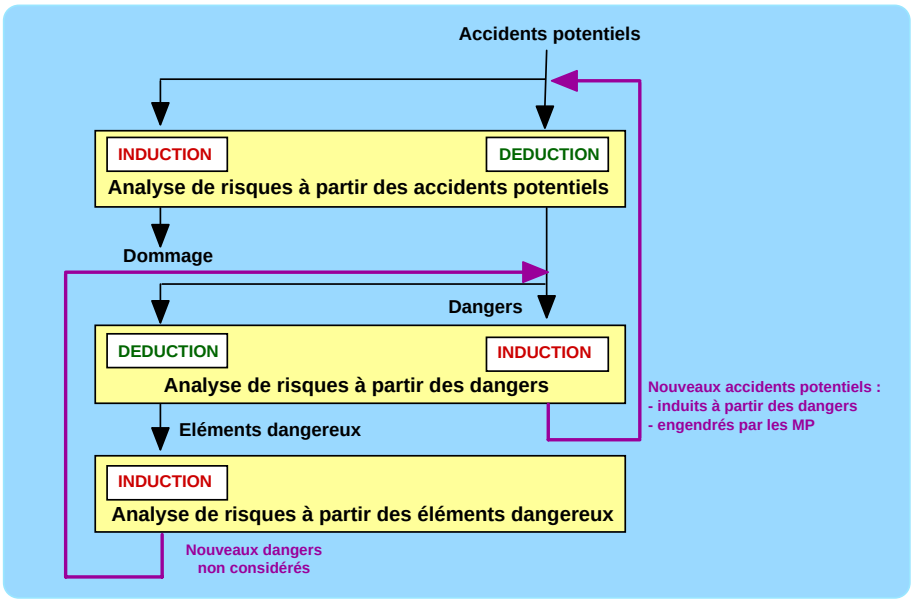

Figure 2. Principe général de la méthode d'APR proposée [7] et [8]

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 2 schématise les différentes étapes impliquées dans le processus d'analyse de risque que nous préconisons [8].

Conclusion

L'analyse préliminaire de risques est très différemment exercée et demeure mal définie. Plus particulièrement, le vocabulaire, la démarche d'élaboration et le format de représentation ne sont pas consolidés. Le recours à une démarche d'analyse rigoureuse et admise par tous les acteurs qui prennent part à l'élaboration d'un dossier de sécurité s'impose. Cette méthode qui repose sur un formalisme de représentation des connaissances d'APR, s'articule autour de trois étapes d'analyse complémentaires et itératives incluant conjointement des processus d'induction et de déduction. La principale originalité de cette nouvelle démarche réside essentiellement au niveau de la cohérence et de la complétude de l'analyse des risques. Cette méthode a pour vocation d'aider l'ensemble des acteurs qui participent à l'élaboration et à la validation d'un dossier de sécurité et contribue, à notre sens à l'amélioration de la sécurité des **systèmes de transport intelligents (STI)**. Une évaluation est nécessaire pour montrer la faisabilité et le bien fondé de cette nouvelle méthode d'APR dans les STI.

Références

[1] DJEBALI Karima. « Maquette de faisabilité d'un système à base de connaissances d'aide à l'analyse préliminaire de risques des systèmes de transport guidés ». Mémoire de stage de DEA Informatique : Systèmes Intelligents. INRETS, Arcueil, septembre 1999, 54 p. Sous la direction de H. HADJ-MABROUK

[2] 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, pp 23-36, Février 1996.

[3] Chopard-Guillaumot, Hadj-Mabrouk et Ganascia : « Contribution à une meilleure définition de l'analyse préliminaire de risques pour les systèmes de transport guidés ». *Journal Européen des Systèmes Automatisés (RAIRO-APII-JESA)*, Paris, vol. 30, n° 1, pp 121-143, Avril 1996.

[4] HADJ MABROUK H. « Examen du dossier Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport INRETS-ESTAS CR/A-94-64, Arcueil, 2/12/1994, 35p. *(diffusion restreinte).*

[5] HADJ-MABROUK H., BIED-CHARRETON D. « Avis de l'INRETS sur le document Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport ESTAS/A-95-15, Arcueil, 16 mars 1995, 38p. *(diffusion restreinte).*

[6] 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.

[7] 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.

[8]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.

[9] LIEVENS C. « Sécurité des systèmes ». Cépaduès Éditions, Toulouse, 1976.

[10] VILLEMEUR A. « Sûreté de fonctionnement des systèmes industriels ». Éditions Eyrolles, Paris, 1988.