Quels axes pour la sûreté dans les transports terrestres collectifs?

El Miloudi El Koursi, Virginie Deniau, Sébastien Ambellouis, Mohamed Ghazel, Christophe Gransart, Saïd Hayat, Marc Heddebaut, Cyril Meurie, Mathieu Perin

▶ **To cite this version:**

El Miloudi El Koursi, Virginie Deniau, Sébastien Ambellouis, Mohamed Ghazel, Christophe Gransart, et al.. Quels axes pour la sûreté dans les transports terrestres collectifs?. Congrès Lambda Mu 21 " Maîtrise des risques et transformation numérique : opportunités et menaces ", Oct 2018, Reims, France. hal-02074285

HAL Id: hal-02074285
https://hal.science/hal-02074285

Submitted on 29 Mar 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Quels axes pour la sûreté dans les transports terrestres collectifs?

What are the security research priorities in land mass transportation?

El Miloudi EL KOURSI
Univ Lille Nord de France, IFSTTAR,
COSYS, ESTAS, F-59650
Villeneuve d'Ascq, France
El-miloudi.el-koursi@ifsttar.fr

Virginie DENIAU et al[a].
Univ Lille Nord de France, IFSTTAR
COSYS, LEOST, F-59650
Villeneuve d'Ascq, France
virginie.deniau@ifsttar.fr

Résumé
Dans le cadre de la cartographie des travaux de recherche menés en France et en Europe entre 2006 et 2016 dans le domaine de la sûreté dans les transports terrestres, nous présentons les besoins identifiés en matière de recherche et de développement dans les transports terrestres collectifs. Les thèmes prioritaires identifiés traitent des aspects liés à la detection, surveillance, sûreté par conception et cyber-sécurité. Ces thèmes seront presentés et discutés dans ce papier.

Mots clés : Sûreté, sécurité, transport

Summary
This paper presents the research priorities identified in land transportation sectors. These priorities were identified by analyzing French and European projects conducted in the period from 2006 to 2016. Four research priorities relates to detection, surveillance, security by design and cyber-security aspects will be presented and discussed in this paper.

a: Sébastien AMBELLOUIS, Mohamed GHAZEL, Christophe GRANSART, Saïd HAYAT, Marc HEDDEBAUT, Cyril MEURIE et Matthieu PERIN.

1 Introduction

La sûreté des systèmes de transports collectifs constitue un enjeu stratégique pour garantir une mobilité efficace et sûre des citoyens. Des mesures de sécurité et de sûreté ont été mises en œuvre pour améliorer l'attractivité des systèmes et continuer à répondre aux exigences fondamentales de disponibilité, d'accessibilité, de sécurité et d'ouverture des transports publics (Boudi et al., 2016). Pour répondre à ces enjeux, les nouvelles technologies et la révolution numérique sont mises au service pour faire face aux nouvelles menaces identifiées comme la cyberattaque. La sûreté couvre tout acte volontaire, qui va de la simple "incivilité" au terrorisme, et tous les degrés de la malveillance.

L'objectif de l'étude, présentée dans ce papier, est d'analyser en profondeur les projets de recherche pour obtenir un aperçu assez général des travaux de recherche menés en France et en Europe entre 2006 et 2016 dans le domaine de la sûreté dans les transports terrestres.

Cette collaboration entre l'IFSTTAR et la DGITM a permis de dresser une cartographie des projets de recherche dans le domaine de la sûreté des transports collectifs en l'organisant selon les dimensions clés : prévenir, détecter, dissuader, alerter, atténuer et retourner à une situation opérationnelle acceptable. L'analyse de l'ensemble de ces projets a permis de dégager des axes de recherche et de développement dans le domaine de la sûreté dans les transports (Ambellouis et al. 2017).

2 Démarche

En s'appuyant sur l'agenda stratégique (Brubiel *et al.,* 2016) élaboré dans le cadre du projet européen CARONTE « Creating an Agenda for Research On Transportation sEcurity », l'étude a été menée en deux phases:

- Phase 1 : Cartographies des projets de recherche
  - Identification et analyse de 108 projets PCRD, H2020 et autres relevant de la thématique sûreté dans les transports, dans la période 2006-2016.
  - Identification et analyse de 48 projets ANR relevant de la thématique sûreté dans les transports.
  - Identification des thèmes prioritaires.
- Phase 2 : Analyser en profondeur des thèmes de détection, surveillance, cyber-sécurité et sûreté par conception en se focalisant sur les solutions développées dans les projets sélectionnés. Des recherches plus approfondies ont été menées pour étudier la production des projets sélectionnés. Nous avons également pris contact avec les coordinateurs des projets et dans certains cas obtenus des entretiens pour compléter nos informations.

3 Analyse et synthèse

Cette analyse et synthèse s'articule autour des dimensions clés : prévenir, détecter, dissuader, alerter, atténuer et retourner à une situation opérationnelle acceptable. Les aspects résilience, gestion de crise, éthique, légal, sociétal et économique n'ont pas été pris en compte dans cette étude. Nous avons recensé un grand nombre de projets et avons effectué une fiche synthèse pour chacun de ces projets (tableau 1).
A la lecture de l'ensemble des fiches de synthèse, nous avons dégagé les principales thématiques suivantes :

- **La détection** d'attaques, d'incidents, d'objets ou de matières dangereuses tel que nucléaire, radiologique, biologique et chimique ou explosive (NRBC-E) et autres

- **La surveillance** de l'espace de transports terrestre, le suivi des personnes et des comportements
- **La sûreté par conception,** qui consiste à prendre en compte la résistance des moyens de transport à d'éventuelles attaques au moment de leur conception
- **La cybersécurité**, domaine dans lequel de nombreux projets ont été financés mais sans être nécessairement axés sur les transports

ACRONYME (FP6, FP7, H2020, ANR…)

Intitulé du projet :	
URL :	
Coordinateur :	Partenaires :
Date de début :	
Date de fin :	Budget:
Résumé :	
Aspects de la sûreté abordés: • cybersécurité * security by design * détection * surveillance * gestion de crise * interfaces * risque CRBN * ...	
• Solution développée: Un descriptif des travaux et de la solution • Type de la solution: - solution technologique / Niveau TRL R&T (TRL 1 - 4), étape de développement (TRL 5 – 7), disponible commercialement (TRL 8-9) - nouvelle réglementation - nouveaux standards - nouveaux process - nouvelle organisation ou entité - formation / tutoriel - dissémination de l'information, sensibilisation • Quelles sont les mises en œuvre concrètes, et par qui? • Les produits sont-ils opérationnels sur le terrain ou encore en laboratoire? • Chez quels opérateurs? • Pour quels cas d'usages?	
Limites de la solution: • Quelles suites ont-été données à ces actions de recherche? • Quels liens avec d'autres projets en cours de démarrage?	

Tableau 1 : Fiche type par projet.

3.1 Détection

Face aux évènements tragiques connus ces dernières années, l'amélioration de la prévention des risques et menaces dans les infrastructures critiques de transports tels que les aéroports, les gares, les véhicules ferroviaires ou routiers ou plus généralement, dans des files d'attentes, des manifestations sportives, des grands spectacles constitue un challenge considérable.
L'un des aspects de la sûreté qui est abordé dans de nombreux projets de recherche et développement depuis 2006 est celui de la détection, qu'elle soit vue sous l'angle des:

- colis potentiellement suspects, de vandalisme, d'individu ;
- risques de nature chimique, biologique, radiologique ou nucléaire ;
- attaques électromagnétiques ;
- cybersécurités.

Plusieurs projets, qui nous semblent majeurs, ont été montés durant la période 2006-2016 et ont traité de cette problématique. Il s'agit des projets comme REALEX (ANR); EGSISTES (ANR); IMAGINE (FP7); SMARTVISION(ANR); MOBILEPASS(FP7); DIRECT(H2020); REHSTRAIN (ANR); SEERS(FP7); SECRET(FP7); AEROCEPTOR; SCALA(FP7); CARONTE(FP7); SECUR-ED(FP7).
Avant de discuter du caractère technologique des solutions proposées dans les différents projets cités ci-dessus, il nous semble opportun d'introduire l'évaluation des risques dans le cadre de l'amélioration de la sûreté dans les systèmes de transports. Le projet – REALEX - a donc traité de l'évaluation de la vulnérabilité des installations industrielles présentant des risques de nature chimique, biologique, radiologique ou nucléaire, de la prévention et de la caractérisation de la situation pour le dimensionnement de la réponse face à l'apparition d'un évènement. Le projet - EGSISTES - quant à lui portait sur le développement de méthodes et de modèles physiques permettant d'analyser et d'évaluer le niveau de sécurité global d'un système de transport souterrain vis-à-vis des risques liés à la dispersion de gaz, la génération et la propagation des ondes de pression liées à une explosion.

Considérant la problématique de détection d'objets dissimulés, deux projets se sont récemment intéressés à ce sujet en se basant sur le développement d'un scanner à ondes millimétriques.

Dans le premier projet - IMAGINE -, un nouveau dispositif compact, aux performances élevés et aux coûts réduits, bien que devant être encore optimisé, a été développé pour être utilisable dans des enceintes autres que des hubs de transports majeurs. L'actualité récente sur les colis piégés au siège parisien du fonds monétaire internationals ainsi qu'au ministère allemand des finances renforce l'intérêt de disposer de systèmes de détection compact à coût réduit.
Le second projet - SMARTVISION - s'est davantage positionné sur l'inspection « on the move », automatique et sûre des passagers via le développement d'un système multi-capteurs composé de scanners millimétriques actifs et passifs. Il propose de limiter les longues files d'attentes fastidieuses pour les passagers et sources potentielles d'attaques ciblées. Dans un cadre proche portant sur la détection d'individu, le projet - MOBILEPASS – s'est concentré sur la recherche et le développement d'équipements mobiles autonomes et sans fils, technologiquement avancés, permettant aux autorités chargées du contrôle des frontières de vérifier de manière rapide et sûre les voyageurs légitimes. Ces deux projets ainsi que le test de la mise en place de la reconnaissance faciale en 2016 à l'aéroport de Roissy, puis en 2017 à l'aéroport d'Amsterdam - Schipol ainsi qu'à la gare du Nord de Paris, nous laisse à penser qu'au-delà du contrôle des passagers, la réduction des files d'attente générées par les procédures de contrôle devient une priorité.
Les infrastructures de transport y compris les espaces fermés comme les gares, les souterrains, les salles de spectacles, etc. peuvent aussi devenir des cibles potentielles pour des attaques par composés toxiques volatils à dispersion rapide. La détection par des techniques de mobilité ioniques ayant montré leur limite, le projet - DIRECT - a réalisé un instrument de détection de composés toxiques basé sur le couplage d'une source à pression atmosphérique avec un spectromètre de masse haute résolution utilisant la spectrométrie de masse à résonance cyclotronique ionique. Cependant ce dispositif élaboré à partir de 2009 ne semble pas avoir dépassé le

stade d'un projet de démonstration de faisabilité, à niveau de TRL bas.
Un autre projet nommé - REHSTRAIN - s'est intéressé à la mise en place d'un système considéré comme un « tube » doté d'une soufflerie d'air et de plateaux accrochant certains types de molécule permettant, in fine, de détecter des substances toxiques. Ainsi que lors de la section précédente, l'intérêt d'un tel système est d'éviter la congestion de passagers à un endroit donné, comme cela peut être le cas avec l'utilisation de portiques, et de permettre une détection « on the move » comme pour le projet cité plus haut. Il présente toutefois certaines limitations comme le paramétrage et la multiplication des plateaux, le masquage de substances, et enfin le coût de l'installation.
Le projet - SEERS - s'est intéressé au développement d'un capteur d'imagerie multi-spectrale dans une large bande du domaine infrarouge permettant en outre de détecter un déversement de liquide, de mesurer des températures et concentrations de gaz. Ce projet intègre une démonstration dans le cadre de la surveillance côtière et en tunnel.
Considérons maintenant le réseau ferroviaire européen qui se trouve être vulnérable aux attaques électromagnétiques. En effet, les systèmes de transport de masse automatisés comme le réseau ferroviaire européen, disposent de systèmes électroniques, informatiques et de télécommunication, sensibles aux interférences électromagnétiques qui peuvent être intentionnelles et générées avec des dispositifs relativement faciles à obtenir et à utiliser. Le projet - SECRET- a étudié cette problématique (Deniau, 2014). Dans sa dernière phase, il a proposé l'implémentation d'une architecture résiliente incluant les modules de détection et différents liens de communication afin de garantir le maintien de la communication pour la transmission d'informations critiques nécessaires à des fonctions de contrôle-commande, de communication ou de signalisation. A contrario, des générateurs électromagnétiques délivrant des signaux perturbateurs particuliers peuvent être réalisés tels des outils pour lutter contre le terrorisme.
C'est le cas du projet - AEROCEPTOR – qui a visé le développement d'un concept innovant de contrôle à distance et d'arrêt de véhicules (terrestre et maritime) au moyen de système aérien de type drone équipé d'armes électromagnétiques. L'avantage d'une telle solution réside dans sa capacité à intervenir rapidement et sous toutes conditions météorologiques, avec un niveau de sécurité élevé et un faible taux d'erreurs.
A un autre niveau d'échelle, les actes de malveillance ou d'attaques à perspective terroriste peuvent aussi être déclenchés par des pirates informatiques et donc vue sous l'angle de la cybersécurité. En effet les solutions de protection des infrastructures informatiques des entreprises ne semblent pas être directement utilisables par des systèmes industriels. Cela est notamment le cas pour les systèmes SCADA qui interviennent dans différents secteurs d'activités comme celui de la signalisation ferroviaire et donc qui se trouvent être une cible potentielle. Dans cet optique, le projet - SCALA - a, en outre, eu pour ambition de développer un prototype de protection et de détection d'intrusions sur un réseau industriel pour réduire et minimiser substantiellement le risque résiduel.
Au regard de l'émergence des actes de malveillance et de menaces terroristes, il nous semble important de regarder davantage deux projets phares et de grande ampleur récemment terminés, que sont les projets - CARONTE - et - SECUR-ED - consacrés tous deux à la sûreté des systèmes de transports terrestres. Le premier projet a eu pour ambition de définir un agenda de recherche qui identifie les sujets prioritaires et qui les classe selon trois thématiques. Le second projet terminé en 2004, était un projet de démonstration intégrant un ensemble interopérable de technologies et de processus couvrant tous les aspects de la sureté. Dans ce projet, quatre démonstrations principales et six démonstrations secondaires ont été présentées dans dix villes européennes et ont permis de valider les solutions proposées. Il en ressort un certain nombre de recommandations importantes sur différents aspects : organisation, gestion de l'information, surveillance et détection d'intrusion, réponses aux risques de nature chimique, biologique, radiologique ou nucléaire, télécommunications, cyber et résilience, etc, qui pourraient être mises en corrélation avec l'agenda proposé dans le projet - CARONTE -.

3.2 Surveillance

La fonction de surveillance constitue la réponse la plus commune pour améliorer la sécurité et la sûreté des systèmes de transport face à la menace. Cette fonction est mise en place depuis plus de 30 ans par les plus grands réseaux de transport collectifs routiers, ferrovaires et aériens. La surveillance n'est pas qu'une réponse technologique. Si un système de surveillance se compose d'un ensemble de capteurs (caméras, microphones) connectés à un système de supervision et d'acquisition (SCADA), ce système est défini et opéré de manière à garantir une interaction efficace avec un ensemble d'agents pouvant être postés devant des écrans de surveillance ou pouvant opérer sur le terrain. La menace terroriste n'a jamais été aussi élevée, et aujourd'hui la mise en place de systèmes de surveillance modernes adossés à un renforcement des troupes qui patrouillent sur le terrain constitue une première réponse efficace. Toutefois, la surveillance n'en reste pas moins un domaine de recherche important dont l'objectif est d'améliorer encore son efficacité, de lui apporter de nouvelles fonctionnalités et de garantir la sécurité du système.
Parvenir à développer un système de surveillance performant et en garantir sa sécurité, nécessite une connaissance précise de la vulnérabilité de chaque élément du système. Le projet – REALEX (ANR)- établit une évaluation des risques relatifs à l'attaque (malveillance ou terrorisme) contre des sites industriels sensibles. En cas de vol de matières dangereuses, le but est d'évaluer le risque d'une attaque ultérieure et ses conséquences.
Le consortium - COUNTERACT (FP7) - a montré que des différences de prise en compte et de gestion considérables existent entre états membres de l'Union Européenne et notamment entre les anciens et les nouveaux arrivants. Si la méthode d'évaluation est primordiale, COUNTERACT recommande surtout que les informations servant à l'évaluation de la menace soient reçues régulièrement et de manière structurée (notamment les données gouvernementales) par les grands et les petits opérateurs afin que ces derniers puissent définir une stratégie de sécurité de manière aussi efficace.
Depuis plus de 30 ans, les capteurs sont installés de manière presque systématique au sol sur les infrastructures avec pour principales fonctions de visualiser et d'enregistrer en temps-réel ce qui se passait sur un réseau. Les capteurs ont été installés, depuis une dizaine d'années, dans les véhicules de transportant des voyageurs (train, autobus etc.). Le nombre désormais très élevé de caméras qui composent le système, nécessite d'imaginer une intelligence numérique capable d'analyser tous ses flux de données et présenter une information pertinente à un agent susceptible d'ordonner et de mener une intervention. Les projets tels que SURTRAIN (ANR), DeGIV(ANR), Secur-ED (FP7) ou encore KIVAOU (FP7) proposent par exemple des solutions vidéo capables de détecter/suivre des individus se déplaçant sous un réseau de caméras et des méthodes de détection automatique de certains comportements. Le mode de surveillance privilégié est le mode vidéo : très peu de projets ont proposé d'y associer un mode audio (SURTRAIN (ANR)et DéGIV(ANR)).

Dans le domaine aérien et du contrôle des frontières, le projet MOBILPASS (FP7) a développé un nouvel appareil de prise d'empreintes et de capture faciale non intrusive afin de réduire la contrainte pour les passagers, de réduire le risque d'usurpation et de faciliter le travail des gardes-frontières et des agents de sécurité.
Des projets tels que Imagine et SEERS proposent de nouvelles technologies de capteurs capables de détecter des objets dissimulés sous les vêtements d'un individu, d'assurer le bon fonctionnement de la surveillance lorsque les conditions de visibilité varient (par exemple en présence de brouillard et de fumées) et de rester opérationnel dans le cadre d'un événement type NRBC (détection du déversement d'un liquide, mesure des concentrations de gaz et de températures etc.). Le risque NRBC bénéficie spécifiquement de nouveaux outils technologiques de lutte notamment grâce au projet REHSTRAIN (ANR) qui a développé une barrière soufflante permettant de détecter des molécules dangereuses.
Les projets précédents, exploitent des capteurs installés sur les infrastructures (gares, stations, aéroports) ou à l'intérieur des véhicules de transport de passagers. Les drones, qui se développent rapidement, offre des nouveaux moyens d'observer, de surveiller et d'interagir avec un ensemble de moyens humains déployé sur une infrastructure. Le projet – SURICATE (FP7) - propose quant à lui d'utiliser un drone instrumenté afin d'effectuer, d'une part, la surveillance et l'inspection des voies ferrées au profit de missions de maintenance mais aussi de lutte contre des actes de malveillance ou de vols de câbles, et d'autre part, la surveillance et l'inspection des lignes électriques HT ou THT (Haute Tension ou Très Haute Tension). Muni d'un système d'émission d'impulsions électromagnétiques, un tel drone peut contrôler à distance et arrêter (en sécurité) un véhicule non coopératif. Il s'agit d'une proposition du projet – AEROCEPTOR(FP7) - qui s'est concentré sur les véhicules terrestres et maritimes. Nous constatons toute l'utilité d'une telle solution dans le cas des dernières attaques terroristes ayant fait usage de voiture bélier.

Si un grand nombre de ces projets proposent une normalisation de leurs solutions (MOBILEPASS, Secur-ED), et si presque tous les projets comportent un volet éthique, les consortia les plus grands imaginent généralement des solutions globales intégrant notamment les questions d'organisation, de procédures et de formations. Ces systèmes globaux peuvent différer d'un opérateur à un autre voire d'une nation à une autre s'il s'agit de politique publique. Le projet – COUNTERACT - a montré qu'il est primordial d'identifier ce qui peut être pertinent dans ces systèmes et présent dans le grand volume de données disponibles. De même, lorsqu'elle cherche à se tenir au courant de l'évolution de la sécurité dans les secteurs du Transport de surface de passagers, du Transport de fret et du Transport aérien et de l'Énergie, la Commission européenne doit savoir ce que pensent les secteurs eux-mêmes des nouveaux développements en matière de sécurité et si de nouvelles mesures sont identifiées. Selon ce projet, la mise en place d'une cellule de travail permanente animée par l'UITP permettrait d'y parvenir.

3.3 Sûreté par conception

La sûreté est devenue une préoccupation majeure qui a nécessité la mise en place et l'intégration, par les opérateurs, des mesures de prévention, de protection et de mitigation pour continuer à répondre aux exigences fondamentales de mobilité, d'accessibilité, de sécurité et d'ouverture des systèmes de transports publics. Ces mesures ont été développées pour sécuriser les installations et les passagers et améliorer le sentiment de sécurité. Les systèmes actuels ou la conception des installations ont été guidées par des aspects de mobilité, d'exploitation, de sécurité et de coût. La prise en compte de la dimension sûreté a été intégrée tardivement dans la conception des installations fixes et mobiles suite aux récentes attaques. La prise en compte, assez tôt dans le cycle de développement des installations, de la dimension sureté par conception permet d'éviter des adaptations coûteuses à un stade ultérieur dans le domaine de construction et des TIC pour optimiser les stratégies de prévention et de résilience.
Plusieurs documents de politique européenne soulignent la nécessité d'améliorer le niveau de sûreté et de résilience sans mentionner explicitement la dimension «sûreté par conception» comme moyen d'y parvenir. Des initiatives européennes et nationales ont été prises pour améliorer les aspects sûreté dès la conception des systèmes de transports. Dans le cadre de la sûreté par conception, plusieurs projets ANR, FP7 et HORIZON 2020 ont été analyses. Parmi les projets examinés 6 ont proposé ou recommandé des aspects liés à la «sûreté par conception» des stations, infrastructures et véhicules:

- Le projet - SECURESTATION (FP7)- a visé à améliorer la résilience et la sécurité des stations et des terminaux face aux attaques terroristes par la mise en place des solutions technologiques et des méthodologies permettant de réduire l'impact du souffle, du feu crée par les explosifs et de la dispersion des agents toxiques sur les passagers, le personnel et l'infrastructure. Il a élaboré une feuille selon deux aspects : (1) Partage des bonnes pratiques relatives à l'évaluation des risques, au guide pour la conception, à l'usage des moyens technologiques et les solutions pour l'architecture des stations et terminaux. (2) Normalisation, harmonisation des procédures pour une meilleure résilience fonctionnelle et physique en traitant les scenarios d'attaques utilisant les explosifs, feu et matériaux dangereux (NRBC…).
- Le projet – SECUREMETRO (FP7) – a visé à améliorer la résilience des véhicules en étudiant et sélectionnant les matériaux qui permettent de renforcer l'intégrité de la structure contre l'utilisation des explosifs conventionnels (Bruyelle et al., 2014). Il a proposé des barrières pour contribuer à la sécurité des passagers et améliorer la tenue au feu/fumée et optimiser le retour à la situation normale d'exploitation après une attaque. Différentes solutions ont été apportées. Par exemple, les équipements situés en hauteur sont retenus par des câbles pour empêcher leurs chutes sur les passagers, des revêtements en plastique résistant empêchent la fragmentation des surfaces vitrées, des éléments de structure lourds sont remplacés par des matériaux plus légers absorbant l'énergie du choc. Les bénéfices apportés par des cloisons séparatrices intérieures en matériaux absorbants pour réduire l'impact de l'explosion ont également été étudiés.
- Le projet – CARONTE (FP7)- a défini un agenda de recherche sur les aspects sûreté dans les transports terrestres, sur la base de l'analyse de l'existant, de l'identification des besoins (risques, menaces / gaps) et des solutions/pistes potentielles. Une des thématiques identifiées prioritaires concerne la sûreté par conception.
- ELASTIC (FP7) a mis en place une stratégie globale pour la protection des infrastructures utilisant des capteurs intégrés à la structure pour aider à réagir aux agressions. Une série de recommandation couvrent les principaux risques (Vents violents, tremblements de terre, feux, impact d'avions, explosions, risques NRBC,

inondations), les évacuations et les réseaux de capteurs notamment intégrés à la structure.

- Le projet – COUNTRACT(FP6) – a visé à évaluer et à recommander des solutions réalisables et rentables pour l'amélioration de la sécurité dans quatre secteurs clés des infrastructures essentielles, les transports publics urbains, le transport ferroviaire, le transport aérien, le transport maritime, le transport de marchandises et l'énergie.
- Le projet – STRUCTURE (ANR) – a traité des effets des attaques électromagnétiques sur les infrastructures critiques (systèmes énergétiques, systèmes TIC, transports ...). Les «infrastructures critiques» (CI). Il analyse les risques d'une mise hors service volontaire ou de créations volontaires de défaillances au sein d'infrastructures critiques.

Trois aspects méritent une attention particulière:

- Recherche et développement d'outils de modélisation et de simulation pour évaluer l'impact des mesures de sûreté sur le flux de passager.
- Recherche sur l'intégration de mesures de prévention et de protection en station, sur l'infrastructure et dans les véhicules.
- Amélioration du sentiment de sécurité par un bon équilibre entre la surveillance / détection et le sentiment de sécurité.

3.4 Cybersécurité

La problématique de la cybersécurité, quasi inexistante au début 2000, est montée en puissance et a amené de nombreuses problématiques et projets au cours de ces dernières années. Cela est lié au fait que l'ensemble des personnes, terminaux et objets deviennent connectés et sont donc devenus autant de cibles potentielles pour des attaques ayant des buts différents : vols d'information, chantage en vue d'obtenir de l'argent (ransomware – San Francisco BART nov. 2016, 2000 machines de vente de tickets infectées, mai 2017 attaque mondiale), usurpation d'identité) … Cette dynamique de recherche s'est accentuée encore très récemment via des projets européens tels que Shift2Rail où une partie du programme de recherche est uniquement dédié à ce thème pour le domaine ferroviaire.

Le thème de la cybercriminalité constitue un enjeu désormais majeur pour nos sociétés, fortement soutenu tant au plan national qu'en Europe. Ce thème est présent notamment à Lille chaque année dans le cadre du désormais très couru Forum International de la Cybercriminalité (FIC). La commission européenne décrit les infrastructures critiques comme suit : « Les infrastructures critiques sont les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris les secteurs bancaires et financiers, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base ».

Comme on peut le constater, ces infrastructures critiques sont nombreuses et occupent une place importante dans notre quotidien, que ce soit directement, ou indirectement. À titre d'exemple, l'infrastructure de transport ferroviaire couvre de nombreux corridors prioritaires en Europe. L'infrastructure de transport routière constitue un autre exemple particulièrement important avec le développement attendu de la route automatisée ainsi que de la route de cinquième génération.

Plus dans l'actualité, Patrice Caine, président directeur général de THALÈS, expliquait en juin 2015 dans un entretien au journal "La Tribune" qu'une des forces opérationnelles et commerciales du groupe, est de marier la compétence métier, en l'occurrence les systèmes de signalisation ferroviaire dans l'activité transport, avec une autre, la cybersécurité et d'indiquer : « Nous discutons aussi bien avec les opérateurs de transport qui ont bien identifié que THALÈS est le seul acteur du monde de la signalisation ferroviaire grande ligne ou métro à avoir des capacités à traiter ce type de menaces qu'avec les grands équipementiers automobiles qui s'interrogent également. Demain, lorsque ces questions se traduiront en des exigences techniques dans les appels d'offre internationaux, nos concurrents auront bien du mal à y répondre. Et cela crédibilisera donc encore plus les systèmes THALÈS auprès de nos grands clients et donneurs d'ordres ».

La DGA-MI (Maîtrise de l'Information) concentre également actuellement des moyens et des compétences considérables afin d'assurer, pour ce qui la concerne, ses missions. De son côté, l'Agence Nationale de Sécurité des Services d'Information (ANSSI) accompagne les entreprises en fonction de leur profil par des actions de conseil, de politique industrielle et de réglementation afin de rendre disponibles des produits de sécurité et des services de confiance.

Cette analyse effectue un recensement ainsi qu'une analyse succincte des travaux menés essentiellement en France et en Europe. Elle propose également plusieurs pistes de recherche regroupées dans un thème commun que nous avons baptisé « RÉsilience des infrastructures critiques de Transport aux Risques liés à la cYbersécurité (RETRY) ».

Parmi les projets étudiés, nous avons relevé plusieurs tendances: préservation de la vie privée, amélioration de la cybersécurité des systèmes critiques, évaluation de nouvelles menaces et définition de solutions sur des systèmes de transports existants.

Toutefois, l'industrie ferroviaire, tant opérateurs que fournisseurs de matériels roulants et infrastructure, essaye de se structurer pour trouver une solution commune à cette problématique. Divers standards (IEC 62443, ISO-2700x, NIST-800, Ebios en France) sont évalués mais ne font pas l'unanimité. Il se dégage quand même une tendance vers le standard IEC 62443 pour la cyber sécurité des systèmes industriels. Cependant la mise en œuvre d'un standard demande beaucoup de temps et de volonté pour y arriver.

Le domaine automobile se base sur la norme ISO 26262 pour définir son architecture. Toutefois le concept d'aide à la conduite, de voiture connectée et, pour but final, de voiture autonome se base fortement sur une utilisation des technologies de géolocalisation via le GPS et dans un futur proche Galileo. Des expérimentations ont malheureusement montré qu'il est possible de tromper un récepteur GPS pour lui faire croire qu'il est à une autre position physique que celle où il est vraiment. De nouveaux types d'attaques permettront de détourner des véhicules autonomes pour les amener à des endroits non voulus pas les usagers, avec tous les problèmes qui seront liés (enlèvement, menaces physiques, vol de marchandises, …).

Les tendances qui ressortent sont le suivantes:

- Besoin de standards de cyber sécurité utilisables dans le domaine des transports
- Lien avec la standardisation des équipements certifiés.

4 Conclusion

Cette analyse plus détaillée a permis d'identifier les axes couverts par ces projets et à quel niveau d'avancement : les manques apparents en matière de recherche et

développement et le type de solutions ayant conduit à des implémentations réalisables et efficaces en milieu opérationnel. Les thèmes prioritaires identifiés traitent principalement des aspects liés à la detection, surveillance, sûreté par conception et cyber-sécurité. On relève que la tenue de ces projets contribue aux développements des compétences en matière de sureté chez les partenaires engagés, mais les exploitations concrètes par les industriels impliqués restent peu connues. Il est intéressant de noter que la simulation et la co-simulation doivent se structurer et que la place des sciences humaines, des questions d'acceptabilité, des approches cout-bénéfices et juridiques doit être renforcée.

5 Références

Sébastien AMBELLOUIS, Virginie DENIAU, El Miloudi EL KOURSI, Mohamed GHAZEL, Christophe GRANSART, Saïd HAYAT, Marc HEDDEBAUT, Cyril MEURIE et Matthieu PERIN Livrable 1: Etat de l'art des projets de recherche dans le champ de la sûreté des transports terrestres- Projets conduits ente 2006 et 2016. 23 Mai 2017.

BOUDI, Zakaryae, EL KOURSI, El Miloudi, GHAZEL, Mohamed, 2016, The New Challenges of Rail Security, Journal of Traffic and Logistics Engineering, JTLE, 5p, http://www.jtle.net/.

Joachim Burbiel, Sonja Grigoleit (Fraunhofer INT) and Mohamed Ghazel (IFSTTAR), projet CARONTE "Creating an Agenda for Research On Transportation sEcurity". Deliverable 6.2 - Public part: Research agenda for security issues in land transport. April 5th 2016.

Jean Luc, BRUYELLE, O'NEILL, Conor, EL KOURSI, El Miloudi, HAMELIN, Fabrice, SARTORI, Nicolo, KHOUDOUR, Louahdi, 2014, Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks, Safety Science, ELSEVIER, 62, pp 37-45, DOI : 10.1016/j.ssci.2013.07.022.

Virginie. Deniau, "Overview of the european project security of railways in Europe against electromagnetic attacks (SECRET)," IEEE Electromagnetic Compatibility Magazine, vol. 3, no. 4, pp. 80–85, 2014.

6 Remerciements

Ce travail de cartographie des projets de recherche dans le domaine de la sûreté des transports terrestres collectifs a été soutenu par la DGITM/DSUJ.