Démonstration de la sécurité opérationnelle de la téléconduite des trains : contexte, méthodologie et défis

Abderraouf Boussif, Simon Collart-Dutilleul, François Baranowski, Julie Beugin, Walter Schön

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Démonstration de la sécurité opérationnelle de la téléconduite des trains : contexte, méthodologie et défis

Operational safety demonstration of train remote driving: context, methodology and challenges

Abderraouf Boussif
Institut de Recherche Technologique Railenium,
F-59300 Famars, France
abderraouf.boussif@railenium.eu

Simon Collart-Dutilleul[1,2]
[1]*COSYS-ESTAS, Univ Gustave Eiffel, IFSTTAR, Univ Lille*
F-59650 Villeneuve d'Ascq, France
[2]*Institut de Recherche Technologique Railenium,*
F-59300 Famars, France
simon.collart-dutilleul@univ-eiffel.fr

François Baranowski[1,2]
[1]*COSYS-ESTAS, Univ Gustave Eiffel, IFSTTAR, Univ Lille*
F-59650 Villeneuve d'Ascq, France
[2]*Institut de Recherche Technologique Railenium,*
F-59300 Famars, France
francois.baranowski@univ-eiffel.fr

Julie Beugin[1,2]
[1]*COSYS-ESTAS, Univ Gustave Eiffel, IFSTTAR, Univ Lille*
F-59650 Villeneuve d'Ascq, France
[2]*Institut de Recherche Technologique Railenium,*
F-59300 Famars, France
julie.beugin@univ-eiffel.fr

Walter Schön[1,2]
[1]*Alliance Sorbonne Université, Université de Technologie de Compiègne, CNRS, UMR 7253*
Heudiasyc, 60200 Compiègne, France
[2]*Institut de Recherche Technologique Railenium,*
F-59300 Famars, France
walter.schon@hds-utc.fr

***Résumé* —Dans cette communication, nous présentons le contexte général ainsi que la méthodologie mise en œuvre pour réaliser la démonstration de la sécurité opérationnelle de la téléconduite des trains fret. En complément, nous présentons une synthèse des résultats, soutenue par une discussion de la méthodologie.**

Mots-Clés —Train autonome, Téléconduite, Démonstration de sécurité, Analyse Préliminaire des Risques, Principe GAME.

***Abstract* — In this paper, we discuss the general context and the methodology established to perform the operational safety demonstration of freight train remote driving. In addition, we briefly present the obtained results supported by a critical discussion of the methodology.**

Keywords—Autonomous train, remote driving, safety demonstration, Preliminary hazard analysis, GAME principle

I. INTRODUCTION

La réglementation ferroviaire française et européenne exige, pour toute introduction de nouveau système ou modification/évolution d'un système existant (qu'il soit technologique, procédural ou organisationnel), une étude de sécurité démontrant et assurant que l'ensemble des risques associés sont maîtrisés. En effet, en France, l'Arrêté du 19 mars 2012 fixant les objectifs, les méthodes, les indicateurs de sécurité et la réglementation technique de sécurité et d'interopérabilité applicables sur le réseau ferré national [1] (article 5), stipule que « *toute évolution concernant un système ou sous-système compris dans le réseau ferré national exploité, telle que notamment l'intégration d'un nouveau sous-système, la mise en œuvre de technologies nouvelles ou la modification de l'organisation, des procédures, des équipements ou ensembles d'équipements compris dans l'infrastructure ferroviaire, des matériels roulants ou de l'exploitation, est réalisée de telle sorte que le niveau global de sécurité du réseau ferré national soit au moins équivalent à celui existant avant l'évolution considérée.* »

Aussi, le décret n°2017-440 du 30 mars 2017 [2] dans sa version en vigueur (article 3), quant à lui, stipule que « *Tout nouveau système de transport public guidé ou toute partie d'un système existant est conçu, réalisé et, le cas échéant, modifié de telle sorte que le niveau global de sécurité à l'égard des usagers, des personnels d'exploitation et des tiers soit au moins équivalent au niveau de sécurité existant, compte tenu de l'évolution des règles de l'art, ou à celui résultant de la mise en œuvre des systèmes ou sous-systèmes assurant des services ou fonctions comparables, compte tenu du retour d'expérience les concernant* ».

Les articles ci-avant mettent en évidence le concept GAME « *Globalement Au Moins Equivalent* » qui implique l'assurance de la non-régression du niveau de sécurité global entre un nouveau système (après modification/évolution) et un système existant [3]. Cette analyse de non-régression permet en effet de ne pas réitérer des démonstrations de sécurité lorsque celles-ci ont déjà pu être apportées pour le système de référence.

Dans le secteur des transports guidés urbains, les concepts de base d'une démonstration de sécurité GAME, sont présentés dans le *guide d'application* produit par le STRMTG[1] [4]. La démonstration GAME est en cohérence avec la démarche de mise en sécurité d'un système ferroviaire global ou d'un sous-système telle que définie dans la norme ferroviaire EN 50126 [5]. En effet, elle inclut (i) une phase d'appréciation du risque, permettant d'identifier et d'évaluer des nouveaux risques (engendrés par le nouveau système), et (ii) une phase de maîtrise des situations dangereuses, consistant à déterminer des exigences et mettre en œuvre des mesures de couvertures pour éliminer ou réduire ces risques à un niveau acceptable.

La démarche d'une démonstration GAME a été principalement utilisée pour la démonstration de sécurité des systèmes techniques. Aujourd'hui, elle est étendue vers des démonstrations d'évolutions organisationnelles, opérationnelles et/ou procédurales. À titre d'exemples, dans [6], des premiers résultats d'une investigation visant à caractériser les problématiques opérationnelles de la mise en œuvre du principe GAME dans le secteur ferroviaire sont présentés. Les trois dimensions (technologique, opérationnelle et organisationnelle) ont été considérées dans cette étude. Dans [3], une démonstration GAME relative à l'évolution de procédures d'exploitation ferroviaire est présentée. L'étude a démontré, avec illustration sur l'évolution des règles concernant la procédure « alerte radio », que le principe GAME reste aussi applicable dans le cadre d'une évolution procédurale ou organisationnelle, tout en présentant les adaptations nécessaires dans ce contexte.

Dans la lignée de ces travaux, nous présentons dans cet article une démarche d'analyse de la sécurité opérationnelle relative à la téléconduite des trains de marchandises. Cette étude s'intéresse essentiellement au transfert de la responsabilité de la conduite du conducteur vers le téléconducteur, ainsi que son impact sur le niveau de sécurité global de la conduite, sur l'accomplissement des tâches et activités relatives au conducteur, et sur les procédures et le comportement des autres agents impliqués dans la conduite.

Pour ce faire, nous avons établi une méthodologie d'évaluation de la non-régression de sécurité pour la téléconduite du train par rapport à un référentiel existant : *le référentiel conducteur de ligne* (RCL) [7]. L'objectif principal est, dans un premier temps, à travers une analyse d'écarts (en termes de situations dangereuses), l'identification de risques nouveaux engendrés par la téléconduite en elle-même sur le système ferroviaire et l'identification des risques dus à l'impossibilité éventuelle de celle-ci de pouvoir respecter totalement les prescriptions du RCL ; et dans un second temps, la maitrise de ces écarts et de ces nouveaux risques à travers la détermination des exigences de sécurité (contraintes de conception et opérationnelles) et des mesures de couverture des risques (nouvelles fonctions de sécurité) pour répondre aux objectifs de sécurité (i.e., le maintien du niveau de sécurité GAME à celui obtenu jusqu'à présent avec un conducteur qui suit les règles du RCL). Le travail est recensé et structuré dans un tableau inspiré de la méthode APR (Analyse Préliminaire des Risques).

II. CONTEXTE & OBJECTIFS

La conduite automatique des trains est déjà opérationnelle pour des applications métro pour différents niveaux d'automatisation, jusqu'à GoA4 (Grade of Automation 4) qui correspond à l'exploitation sans personnel à bord des trains. Par rapport aux systèmes urbains, la situation des autres systèmes ferroviaires (TGV, régional, fret) est plus complexe, de par un réseau ferré plus grand et interconnecté, une flotte diversifiée de matériel roulant ainsi qu'un système d'exploitation complexe, diversifié et dans un environnement complétement ouvert.

Dans ce contexte, l'objectif du programme Train Autonome la SNCF est de préparer le déploiement de la conduite autonome [8] et semi-autonome [9] des trains. Ainsi, en concertation avec le programme « Train Autonome »[2] de l'IRT RAILENIUM (et plusieurs partenaires publics, industriels, et académiques), trois grands projets ont été initiés dans ce sens, visant à développer, respectivement : (*i*) un train fret autonome, (*ii*) un train service voyageurs autonome, et (*iii*) un train téléconduit. Ce dernier serait le fruit du projet TC-Rail (*TéléConduite sur Rail*).

Le projet TC-RAIL (de Railenium, SNCF, Thales, ACTIA, CNES) [9] (Fig. 1) vise à développer un système de conduite en sécurité de locomotive depuis un site à distance, sans conducteur dans la cabine du train, avec un niveau de sécurité globalement au moins équivalent à celui obtenu en présence d'un conducteur en cabine. Il s'agit également de lever tous les obstacles techniques qui pourraient s'opposer à une telle exploitation. Cette conduite à distance s'appuie donc sur un lien de communication radio (terrestre et/ou satellitaire) entre le train et le site à distance ainsi que le développement d'une IHM (Interface Homme-Machine) de téléconduite. Le projet TC-RAIL cible principalement trois objectifs :

a) Eviter au conducteur de longs parcours inutiles entre son lieu de prise de service et l'endroit de la desserte fret;

b) Faciliter les manœuvres de trains depuis et vers les centres de maintenance ;

c) Par ailleurs c'est une brique essentielle pour le train autonome qui permettra de reprendre la main à distance sur un matériel roulant pour gérer certains modes dégradés.

Dans la présente communication, nous nous focalisons uniquement sur le premier objectif, visant à assurer les dessertes fret. Ainsi, le système considéré est *le Système de TéléConduite des trains fret* (abrégé dans le reste du papier par STC).

[1] http://www.strmtg.developpement-durable.gouv.fr/

[2] https://railenium.eu/fr/train-autonome/

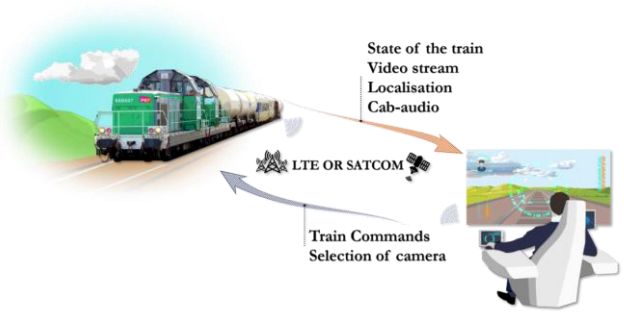

Fig. 1. Téléconduite des trains – Projet TC-RAIL [4]

A. *Le système de téléconduite des trains fret –STC*

Le système de téléconduite (STC) est un système technique permettant à un acteur, appelé « téléconducteur », d'agir sur un engin moteur (ou matériel roulant) et d'interagir avec un ensemble d'acteurs du système ferroviaire (techniques et humains) afin d'assurer une conduite de l'engin moteur à distance en toute sécurité. Ainsi, le téléconducteur et l'engin moteur sont les acteurs principaux s'interfaçant continuellement avec le STC. L'ensemble *engin moteur et STC* représente ce qu'on peut appeler « un train téléconduit ».

D'un point de vue architectural, le STC se compose de trois sous-systèmes :

1) **Sous-système bord :** il regroupe l'ensemble des capteurs et actionneurs embarqués sur l'engin moteur afin de permettre au STC de s'interfacer avec les composants usuels de l'engin moteur. Ainsi, le sous-système bord assure la perception de l'environnement entourant l'engin moteur et commande sa conduite ;
2) **Sous-système sol :** c'est une interface homme-machine (IHM), appelée aussi pupitre, permettant au téléconducteur d'observer l'environnement du train (à travers un ensemble de dispositifs vidéo, audio et autres) et de réaliser l'ensemble des tâches et activités de la téléconduite de l'engin moteur. Autrement dit, le sous-système sol joue le rôle d'une cabine de conduite à distance ;
3) **Sous-système de télécommunications** : un composant essentiel dans le STC, qui a pour rôle d'assurer l'échange des flux d'informations entre le sous-système sol et le sous-système bord, d'une manière continue, avec un niveau requis de qualité de service et de sécurité. Il est important de noter que le sous-système de télécommunications s'appuie sur un ensemble d'infrastructures de télécommunications externes au STC (i.e., l'infrastructure est vue comme une interface externe). Aussi, plusieurs technologies sont considérées (individuellement ou combinées) pour assurer les fonctions du sous-système, à savoir, les technologies 4G/LTE privées ou publics et les technologies Satcom.

Un aperçu global de l'architecture du système de téléconduite est présenté sur la Fig. 2.

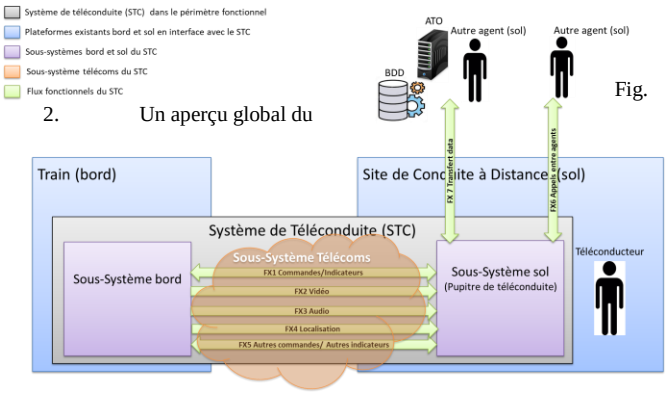

Fig. 2. Un aperçu global du système de téléconduite[3].

B. *Impact de la téléconduite sur le système ferroviaire*

La téléconduite des trains est une innovation majeure qui impacte les différentes couches techniques du système ferroviaire[4]. En effet, cet impact sera d'ordre technique, opérationnel et organisationnel. Dans cette section, nous présentons un ensemble (non-exhaustif) des éventuels impacts.

La téléconduite introduit un nouvel acteur appelé *téléconducteur*. Le conducteur[5] est, depuis toujours, un acteur principal dans la conduite du train et représente aussi une ultime barrière de sécurité face aux accidents potentiels. Ainsi, dans le cas de la téléconduite du train, le téléconducteur est censé (par hypothèse) *hériter* de la fonction du conducteur (et de l'ensemble de ses responsabilités). Aujourd'hui, il est difficile de donner une définition formelle au téléconducteur[6] : est-ce un conducteur conventionnel formé à la téléconduite ? Ou bien, un nouveau métier indépendant du métier du conducteur ? Toutefois, son indisponibilité physique au niveau de l'engin moteur implique son incapacité à réaliser un ensemble de tâches et activités incombant au conducteur ; par exemple, la mise en place des cales antidérive et des pétards, *etc*. Par conséquent, il est difficile d'imaginer que le téléconducteur assure à lui-seul l'ensemble des tâches/activités du conducteur. Ainsi, le rôle et la fonction du conducteur seront partagés par un ensemble d'acteurs (incluant le téléconducteur). Cette modification impacte effectivement l'organisation actuelle du système ferroviaire ainsi que les procédures de la conduite.

Dans la conduite conventionnelle des trains (i.e., avec conducteur à bord), le conducteur joue le rôle d'interface entre l'engin moteur (ou le train) et l'ensemble des acteurs humains (agent de circulation, agent de manœuvre, régulateur, *etc.*) et des acteurs techniques (autres engins moteur, gares, *etc.*). Le conducteur interagit avec les autres

[3] *Livrable de projet L2.2 – Cahier des charges fonctionnel.*

[4] *Système ferroviaire : l'ensemble constitué par les infrastructures ferroviaires de transport public ferroviaire de voyageurs ou de marchandises, les matériels roulants de toute catégorie et origine qui les utilisent, les personnels chargés de faire fonctionner et de maintenir ces équipements ou ces matériels et les procédures utilisées à cet effet (Arrêté du 19/03/2012).*

[5] *Conducteur : la personne assurant la conduite d'un train, qu'elle en assure les commandes directes ou qu'elle donne des directives en cabine à la personne maîtrisant les organes de commande (Arrêté du 19/03/2012).*

[6] *Dans le cadre du projet TC-Rail, la téléconduite reste assurée par des conducteurs conventionnels.*

opérateurs à travers divers moyens de communications (radio sol-train, signaux à main, signaux acoustiques, échanges de vive voix, *etc.*). Dans le cadre de la téléconduite (où le téléconducteur remplace le conducteur), cette interface « humaine » est par conséquent remplacée par un ensemble d'interfaces techniques (par exemple, des moyens de communication dématérialisés). Ainsi, la téléconduite aurait un impact réel sur les procédures et les gestes métiers assurant la communication entre le train et les divers agents participant à l'assurance d'une conduite en sécurité.

Aussi, contrairement à la conduite conventionnelle où chaque engin moteur a sa propre cabine de conduite intégrée, la téléconduite, quant à elle, implique une séparation entre l'engin moteur (avec le sous-système bord) et la cabine de conduite à distance (i.e., le sous-système sol). Ainsi, une même cabine de conduite à distance peut éventuellement être utilisée pour conduire différents engins moteurs. Deux cas de figures sont en effet envisageables :

(*i*) l'IHM associée à la cabine de conduite à distance a une architecture fixe (i.e., propre à un type d'engins moteurs), alors cette cabine de conduite à distance peut être utilisée pour conduire uniquement les engins moteur d'un même type ;

(*ii*) l'IHM associée à la cabine de conduite à distance a une architecture dynamique ou reconfigurable selon les types des engins moteurs, alors elle peut être utilisée pour conduire tout type d'engin moteur.

Il est clair que ces aspects caractérisant la téléconduite sont une évolution majeure dans le domaine ferroviaire et concernent l'ensemble des éléments du système ferroviaire, ce qui justifie effectivement une étude particulière concernant la sécurité opérationnelle de la téléconduite.

C. *Démonstration de la sécurité opérationnelle de la téléconduite*

Selon les nouveaux travaux de normalisation concernant la sécurité des systèmes autonomes et semi-autonomes (comme la téléconduite) [10,11], une démonstration de sécurité doit prendre en compte deux concepts de sécurité interdépendants : (*i*) la sécurité système, et (*ii*) la sécurité opérationnelle.

La sécurité système concerne la sécurité fonctionnelle, la sécurité technique et la cybersécurité du système et de ses composants. D'une manière générale, la démonstration de la sécurité système débute par une analyse préliminaire des risques (APR) à base d'une liste exhaustive d'accidents/événements redoutés[7], conjointement avec une analyse des risques (AdR) type EBIOS [12] pour la partie cybersécurité. Contrairement à la sécurité fonctionnelle qui se focalise sur le système et ses fonctions, la sécurité opérationnelle, quant à elle, a pour objectif l'assurance d'un fonctionnement sûr du système dans son environnement opérationnel. Ainsi, elle s'intéresse à l'ensemble des interactions du système avec d'autres acteurs techniques, humains et environnementaux. La démonstration de sécurité opérationnelle a comme objectif d'assurer que le système évoluera dans son contexte opérationnel (*Operational Design Domain - ODD*) [11] avec un niveau de sécurité acceptable. Autrement dit, elle permet de définir le domaine opérationnel sécuritaire pour le système.

Dans le cadre de cette communication, nous nous intéressons à la démonstration de la sécurité opérationnelle de la téléconduite. Ainsi, la finalité de ce travail consiste à déterminer le domaine opérationnel où un train téléconduit assure ses fonctions avec un niveau de sécurité GAME à celui d'un train avec un conducteur à bord. La méthodologie choisie consiste à démontrer la non-régression de la sécurité de la téléconduite par rapport à un référentiel réglementaire. En effet, partant du principe que les risques existants liés à la conduite d'un train sont couverts par la bonne application des tâches et des procédures du *Référentiel Conducteur de Ligne* (RCL), nous avons établi une méthodologie d'analyse préliminaire des risques opérationnels (APR) de la téléconduite du train par rapport au RCL. Cette démarche vise dans un premier temps, à travers une analyse d'écarts (en termes de situations dangereuses), à identifier les risques nouveaux engendrés par la téléconduite en elle-même sur le système ferroviaire, ainsi que les risques nouveaux dus à l'impossibilité éventuelle de celle-ci de pouvoir respecter totalement les prescriptions du RCL. Dans un second temps, elle vise à assurer la maitrise de ces nouveaux risques à travers la détermination des exigences de sécurité (contraintes de conception et opérationnelles) et des mesures de couverture des risques (nouvelles fonctions de sécurité) pour répondre aux objectifs de sécurité.

III. DÉMARCHE MÉTHODOLOGIQUE

La finalité de cette section est de présenter l'ensemble des étapes de la démarche méthodologique mise en œuvre pour l'analyse préliminaire des risques opérationnels de la téléconduite.

A. *Motivations*

Les activités de l'APR relatives à la conception d'un nouveau système ou à la modification/évolution d'un système existant commencent dès la phase de la définition des besoins et de la définition de l'architecture du système. En effet, l'APR exploite ces définitions, ainsi que les analyses fonctionnelles qui recensent les attentes et les écarts possibles à ces dernières. Elle permet d'anticiper les risques liés au système de téléconduite (en particulier, les éléments technologiques constituant le système et leurs interactions, tâches conducteur, impacts environnementaux, *etc.*), d'évaluer leurs criticités et de proposer des mesures de couverture pour les maîtriser et les réduire.

De manière générale, l'étude APR se réalise tôt par rapport aux phases de développement d'un projet. Ainsi, au démarrage des activités d'APR peu d'informations sont disponibles sur les détails de conception (analyse fonctionnelle, architecture du système, *etc.*) et, aussi sur les procédures d'exploitation et d'entretien. En l'absence de ces éléments d'entrée essentiels, l'APR peut, dans un premier temps, s'articuler sur l'ensemble des documents techniques, documents de procédures et référentiels préalablement définis (à travers l'analyse des écarts par rapport à ces référentiels). Cette dernière méthode se matérialise souvent à travers une exploitation des jugements d'experts [13].

Pour la présente étude, et partant du principe que les risques existants liés à la conduite d'un train sont couverts par la bonne application des tâches et des procédures décrites dans le référentiel conducteur de ligne (RCL), nous

[7] *Dans le domaine ferroviaire, la liste des événements redoutés est donnée dans l'Arrêté du 4 janvier 2016 relatif à la nomenclature de classification des événements de sécurité ferroviaire.*

avons mis en place une méthodologie basée sur le RCL pour la réalisation d'une APR de téléconduite. Le but de cette méthodologie est de déterminer les écarts (en termes de risques et situations dangereuses) de la téléconduite par rapport à la conduite *in situ* concernant la bonne exécution des prescriptions du référentiel. En fait, cette démarche méthodologique basée sur le RCL est motivée et justifiée par plusieurs facteurs :

- Tout d'abord, bien que l'exhaustivité soit une notion (théorique) difficile à confirmer en pratique, le RCL reste un document de référence couvrant l'ensemble des risques ferroviaires liés à la conduite du train et au métier de conducteur de ligne ;
- Par ailleurs, étant un document de référence depuis des dizaines d'années au sein de la SNCF, le RCL présente un niveau de maturité considérable à travers les mises à jour et les améliorations continues par des experts de la conduite et de sécurité de la SNCF. De plus, le RCL est un document prescriptif dont l'interprétation judicieuse et efficace se concrétise notamment par des gestes métiers connus et communiqués par les formateurs aux futurs conducteurs. Il existe donc une sorte de jurisprudence de bonne mise en œuvre du RCL s'appuyant sur les retours d'expériences capitalisés au sein des entités de formation ;
- Aussi, et en plus des processus assurant une conduite sécurisée, le RCL traite également des tâches procédurales et organisationnelles (gestion des documents, processus de communication verbale/écrite avec les autres agents). Ainsi, l'APR prendra en compte les écarts et les risques engendrés par la modification de ces tâches et éventuellement proposera des mesures de couverture et des modifications des procédures ;
- Enfin, à notre connaissance les procédures d'application du RCL n'ont jamais été identifiées ou pointées comme une cause d'accidents ou d'incidents ferroviaires.

Avant de présenter la méthodologie, nous donnons un bref aperçu du référentiel. Le RCL est un recueil des procédures que doit suivre un conducteur, tant pour la conduite d'un TER, TGV, ou d'un engin de chantier. Il décrit les tâches que doit exécuter l'opérateur ainsi que l'ordre de ses actions (*certaines procédures sont décrites sous forme de logigrammes*). Le but ultime du RCL est de faciliter l'acquisition de compétences des conducteurs afin d'assurer une conduite sécurisée. Ainsi, les conducteurs de ligne doivent appliquer l'ensemble des prescriptions du RCL pour répondre et régler toute situation métier. Le RCL (*version 2008*) est constitué de plus de 1000 pages et présente environ 700 articles et prescriptions regroupés en 6 chapitres indexés de A à F (voir TABLE I.).

TABLE I. STRUCTURE DU DOCUMENT RCL.

Chap.	*Titres*
A	Signalisation–Règles d'exploitation
B	Composition – Freinage – Vitesse limite des trains
C	Technique
D	Circulation et conduite des trains
E	Sécurité du personnel – Organisation – Communication
F	Anomalies – Incidents – Accidents

B. Présentation de la méthodologie

La méthodologie proposée pour la réalisation de l'APR basée sur le RCL se déroule en 3 étapes.

*a) **Étape 1** : Une pré-analyse du RCL*

Cette étape vise à étudier et analyser les articles du RCL afin d'identifier les tâches et procédures relatives à la sécurité ferroviaire. Étant donné que le projet TC-Rail est centré sur la téléconduite, nous portons une attention particulière aux activités et missions du conducteur durant sa vie de conduite (i.e., de sa prise de service jusqu'à la fin de service) dans notre analyse APR, en particulier les activités qui peuvent présenter un écart de la téléconduite par rapport à la conduite classique. D'une manière non exhaustive, ces diverses activités concernent :

- **L'interaction avec d'autres acteurs/agents** : en effet, parmi les activités qui présentent un écart téléconduite – conduite classique, sont les interactions du téléconducteur avec d'autres agents de vive voix/radio, par écrit ou par signalisation ;
- **L'interaction avec d'autres matériels :** *(autres trains, voies, gares, etc.)*
- **Les mouvements et déplacements du conducteur :** abandon de la cabine, descente sur la voie, etc.
- **La surveillance des environnements (interne et externe) :** cette activité englobe divers éléments de perception que le conducteur utilise afin d'assurer une conduite sécurisée de son engin. Ces éléments de perception sont :
    - **Perception visuelle (externe) :** signalisation, éléments statiques, état de l'infrastructure dont les caténaires, personnes, animaux et autres éléments mobiles, *etc.* ;
    - **Perception visuelle (interne) :** feu, fumée, intrusion en cabine, mouvements d'éléments statiques, etc. ;
    - **Perception auditive (interne et externe) :** voix et cris, instructions orales, sons spécifiques ferroviaires, *etc.* ;
    - **Perception olfactive :** détection de feux et autres odeurs particulières ;
    - **Perception kinesthésique et vestibulaire :** vitesse et accélération, vibrations et chocs, conditions climatiques (température, humidité), *etc.*

À la fin de cette première étape, nous avons une sélection d'articles relatifs à la sécurité opérationnelle de la conduite. La sélection a été organisée dans un tableau APR dont le canevas est donné en annexe de cet article. Ce dernier représente une donnée d'entrée qui alimente la 2ème étape.

*b) **Étape 2** : Entretiens directifs avec des experts de la conduite[8]*

[8] *Les experts de conduite sont des conducteurs expérimentés et des formateurs professionnels de la conduite chez SNCF. Ils connaissent bien la réalité des situations dans une cabine de conduite « réelle » et maitrisent les prescriptions du RCL. De plus,*

À partir du tableau APR produit durant la première étape, nous procédons à une évaluation initiale de la criticité des risques engendrés par les situations dangereuses/évènements redoutés identifiés (i.e., criticité acceptable ou non acceptable). Les éléments présentant une criticité non acceptable sont ultérieurement soumis à une analyse approfondie avec des experts de conduite SNCF. Le travail avec ces experts se déroule sous forme d'une série d'entretiens orientés par notre préanalyse afin de donner libre cours aux discussions et aux échanges.

Nous précisons que le but des entretiens avec les experts de conduite est d'affiner notre analyse relative aux éléments de l'APR présentant une criticité non acceptable. En particulier, ce qui concerne :

- La compréhension du contexte/motivation des prescriptions métiers du RCL ;
- L'identification des éventuels obstacles à la sécurité pour les éléments identifiés ;
- Les mesures et les pistes de couvertures des risques selon leurs visions et leurs expériences.

Le mode opératoire retenu pour mener ces entretiens est celui d'un questionnaire établi sous la forme d'une grille de réponses préremplie et à compléter au fur et à mesure des discussions[9]. Au terme de cette étape, nous retravaillons le tableau APR en intégrant les éléments pertinents, les clarifications, les recommandations et les suggestions des experts de la conduite.

Le tableau APR issu de cette 2ème étape est revu en validation finale (étape 3) avec des experts en sécurité ferroviaire (académiques et industriels).

Il est important de noter que les divers éléments de l'APR ayant des relations avec l'ergonomie et le facteur humain sont d'abord discutés avec le groupe de travail « facteur humain ». Cette démarche, de notre part, vise à produire une vision collective englobant toutes les dimensions (systémique, technique, facteur humain, organisationnelle et procédurale) permettant de consolider notre jugement (évaluation et appréciation) de la sécurité.

*c) **Étape 3 :** Jugement et validation par des experts de sécurité*

Cette dernière étape de la méthodologie a pour but une validation finale de l'APR ; en particulier, les éléments jugés antérieurement comme « à criticité non acceptable ». Cet objectif se réalise à travers la mise en place d'un groupe de travail, constitué de plusieurs experts en sécurité ferroviaire ainsi que des experts métiers qui se réunissent régulièrement, pour discuter, analyser, et évaluer les divers éléments de l'APR. Le principe est de préparer, pour chaque séance, une liste d'éléments de l'APR qui seront traités et validés durant la réunion. Ainsi, à l'issue de cette phase tous les éléments de l'APR seront validés et peuvent être exportés comme exigences de sécurité, contraintes et recommandations vers les autres lots du projet.

ils ne sont pas impliqués dans la définition fonctionnelle du système de téléconduite (i.e., indépendants).

[9] *En cas de difficultés liées par exemple, à l'analyse des facteurs humains, nous exportons un besoin vers le groupe de travail facteurs humains qui prend en compte la représentativité des sujets interrogés.*

Le tableau final de l'APR contient essentiellement 4 parties (voir TABLEAU 2, 3, 4 et 5 en annexe) :

1. **Analyse des articles du RCL :** cette partie présente les articles analysés du RCL et les éléments relatifs à la sécurité ;
2. **Identification et évaluation initiale des éléments de sécurité :** cette partie consiste à identifier les évènements redoutés engendrés par les éléments de sécurité à partir de l'écart « conduite en cabine - téléconduite » ;
3. **Formulation et évaluation des mesures de couvertures des risques :** cette partie consiste à fournir des exigences et des mesures de sécurité afin de couvrir les risques engendrés.
4. **Export des exigences et des contraintes :** cette partie assure un export de contraintes vers les autres lots/parties de conception du projet/système ;

IV. SYNTHESE DES RÉSULTATS ET DISCUSION

La finalité de cette section est de présenter une synthèse des résultats obtenus et de fournir quelques éléments de discussions concernant la méthodologie utilisée dans ce papier.

A. Synthèse des résultats

Les résultats de cette étude sont fournis dans un tableau APR, dont la structure est présentée en annexe. Les éléments de sécurité[10], analysés dans le tableau APR, peuvent être décomposés en quatre catégories :

Catégorie 1 : elle regroupe les éléments de sécurité dont l'écart par rapport à la conduite en cabine est jugé « *négligeable* ». Ainsi, le risque engendré par chaque écart est considéré comme « *acceptable* », sans application de mesures de couvertures supplémentaires. Des exemples de cette catégorie sont les interactions par radio sol-train entre les agents, la transmission et la réception des documents (dans un format dématérialisé) par le téléconducteur, la perception de la signalisation à travers des écrans et l'adaptation de la vitesse en conséquence, *etc*.

Catégorie 2 : elle regroupe les éléments de sécurité présentant un écart « *significatif* » par rapport à la conduite en cabine. Ainsi, le risque engendré par chaque écart est évalué et des mesures de couvertures sont proposées, en s'appuyant sur le système de référence existant et les directives et recommandations du RCL, afin d'assurer l'acceptabilité du risque final. Des exemples de cette catégorie sont la surveillance de l'environnement, la surveillance de la caténaire, la perception (à la demande du téléconducteur) des sons et des bruits à l'aide de capteurs dédiés, *etc*.

Catégorie 3 : elle regroupe les éléments de sécurité présentant un écart « *important* » par rapport à la conduite en cabine. Ainsi, le risque engendré par chaque écart et considéré « non acceptable » ; et la maîtrise de ce risque exige des modifications majeures au niveau du système de téléconduite ou un export de contraintes fortes vers les autres systèmes ou agents du système ferroviaire. Par conséquent,

[10] *Un élément de sécurité est une prescription d'un article du RCL relatif à la sécurité.*

ces éléments sont renvoyés à la direction du projet afin de juger la pertinence ou non de la téléconduite dans ces contextes opérationnels. Des exemples de cette catégorie sont la mise des cales et des pétards, les visites sommaires de l'extérieur au cours des arrêts, les déplacements du conducteur, la mise en place des attelages de secours par le conducteur, *etc*.

Catégorie 4 : elle regroupe les éléments de sécurité présentant un écart « *positif* » par rapport à la conduite en cabine. Autrement dit, la téléconduite assure un niveau de sécurité plus élevé que celui de la conduite en cabine pour l'ensemble de ces éléments de sécurité. Des exemples de cette catégorie sont : la sécurité du téléconducteur, l'utilisation des caméras de rétrovisions, les changements de directions (sans changement d'IHM), *etc*. Il est important de noter que cette dernière catégorie est essentielle dans une démarche GAME. En effet, les éléments de sécurité de cette catégorie sont utilisés dans la compensation des risques, afin d'assurer le concept de « globalité ».

Un exemple illustratif de la catégorie 2 est présenté dans l'annexe. Il concerne l'élément de sécurité suivant : « la *montée et la descente des agents dans la cabine de conduite (en l'absence d'un conducteur en cabine)* ».

B. Discussion sur la méthodolgie

Dans cette section, nous discutons la conformité de la méthodologie proposée avec la démarche GAME telle que recommandée dans le guide d'application produit par le STRMTG, ainsi que les éléments de base d'une analyse préliminaire des risques standard.

1) Exhaustivité de l'étude :

L'exhaustivité dans les analyses de sécurité consiste à identifier tous les risques, en termes d'évènements redoutés et de situations dangereuses, engendrés par le système à étudier. Il existe des référentiels et des standards qui fournissent des listes exhaustives des évènements redoutés à prendre en compte pour des systèmes bien définis (*comme la liste d'évènements de sécurité ferroviaire proposée dans l'arrêté du 04/01/2016 relatif à la nomenclature de classification des évènements de sécurité ferroviaire)* ; mais d'une manière générale, l'exhaustivité doit être assurée par le processus mis en œuvre pour l'identification des évènements redoutés. Dans le cas de notre étude, c'est le processus d'analyse d'écarts par rapport à tous les articles du RCL qui assure cette exhaustivité. Toutefois, cette exhaustivité reste conditionnée à l'hypothèse que « tous les risques opérationnels existants liés à la conduite d'un train sont couverts par la bonne application des tâches et des procédures du RCL ».

2) Le système de référence :

Le principe GAME consiste à démontrer l'équivalence, en termes de niveau de sécurité, entre un nouveau système et un système de référence assurant des services comparables. Ainsi, le choix du système de référence est une question primordiale dans l'assurance d'une étude GAME fructueuse. En effet, selon le guide d'application STRMTG [4], « *la question de la référence est essentielle dans le cadre de l'application du principe GAME dans la mesure où celle-ci fixe le niveau de sécurité à atteindre* ». Il est important de préciser que le système de référence peut être un système technique (par exemple, le système avant modification) comme il peut être aussi un référentiel réglementaire ou technique reconnu, pertinent et applicable (ex. norme).

Dans le cadre de notre étude, le système de référence est une combinaison entre le système existant (le système de conduite avec un conducteur en cabine) et un référentiel technique, qui est le RCL.

3) GAME – globalité et équivalence :

La notion de globalité dans le principe GAME consiste à considérer l'évaluation de la non-régression du niveau de sécurité au niveau système. Ainsi, elle introduit une certaine souplesse dans l'analyse à travers l'admission du concept de compensation en cas d'éventuelles insuffisances à l'égard d'un ou plusieurs risques. Toutefois, comme indiqué dans le guide d'application STRMTG [4], «*il n'est donc pas admis de compenser d'éventuelles insuffisances du système à l'égard d'un (ou plusieurs) risque(s) collectif(s) par des "gains" en matière de sécurité au niveau d'un (ou plusieurs) risque(s) individuel(s)* ». Ainsi, le principe de compensation n'est appliqué qu'entre des risques du même type et/ou du même niveau en termes de conséquences.

Il est clair que dans notre cas, la méthodologie proposée favorise plus la notion de *localité* que celle de *globalité*. En effet, notre travail consiste à évaluer l'écart en termes de sécurité par rapport à chaque article sélectionné du RCL (i.e., ligne par ligne au niveau du tableau APR). Ainsi, chaque situation de risque est maitrisée localement et indépendamment des autres situations (ce qui peut engendrer une sur-sécurisation au niveau du système global). Idéalement, il serait nécessaire de refaire une restructuration du tableau APR en deux catégories : (*i*) des évènements redoutés engendrant des accidents collectifs et (*ii*) des évènements redoutés engendrant des accidents individuels. Pour chaque catégorie, une évaluation des possibles compensations entre risques permet en effet d'assurer une évaluation « globale ».

4) Utilisation d'une matrice de criticité :

Afin d'évaluer le niveau de risque d'un système en cours d'examen, une matrice de criticité, combinant des niveaux de fréquence d'occurrence (d'un évènement redouté) et des niveaux de gravité (des accidents causés pour cette évènement redouté) est souvent utilisée. Dans le domaine ferroviaire, Il existe plusieurs matrices de criticité dont la principale reste la matrice recommencée dans la norme EN 50126-1[5]. Le choix d'une matrice de criticité, dans le cadre d'une étude sécuritaire, reste un sujet de discussion dans le secteur, et généralement dépend des besoins, des données présentes et de son utilité, comme détaillé dans [14]. Dans le cadre de notre étude, la matrice la plus adéquate avec notre méthodologie est celle du référentiel EPSF (SAM -F005[11]). Deux raisons motivent ce choix :

- *Les niveaux de gravité sont déterminés par une combinaison des conséquences humaines, matérielles et environnementales. En effet, dans le cas des accidents impliquant des trains autonomes et semi-autonomes (i.e., sans conducteurs et sans passagers), la gravité ne doit pas se limiter aux conséquences humaines ; à défaut, tout accident grave impliquant des trains autonomes (sans passagers) ne sera pas pris en compte.*
- *Le but d'une démarche de sécurité par analyse des écarts est d'éliminer les écarts existants (entre le système de référence et le système en examen), une évaluation binaire*

[11] *Référentiel EPSF : Performances de freinage du matériel roulant sur les lignes équipées de signalisation au sol (Version 2, 2017).*

de la criticité (acceptable ou non acceptable), telle que proposée par la matrice, est bien adaptée à notre étude ; contrairement à la matrice de la norme EN 50126, qui propose plusieurs catégories d'acceptation du risque : non tolérable, indésirable, tolérable et négligeable).

Il est important de noter que, dans notre étude, la matrice est utilisée pour évaluer les risques engendrés par les écarts, en termes de sécurité, entre la conduite en cabine et la téléconduite. Aussi, la gravité et la fréquence de chaque risque sont évaluées par jugement des experts.

5) Application de la méthode de sécurité commune (CSM-RA)

Afin d'assurer une harmonisation de la sécurité dans le secteur ferroviaire européen, l'agence ferroviaire européenne a défini une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques ferroviaires (CSM-RA). En effet, la CSM-RA identifie 3 principes d'acceptation du risque afin d'évaluer les risques, dont l'analyse a conclu qu'ils ne sont pas « acceptables ». Les 3 principes sont aussi adoptés par la norme EN 50126 [5].

Les trois principes d'acception du risque sont :

- ***L'utilisation du code de bonne pratique (CSM1) :*** *qui consiste à appliquer des référentiels (comme des normes, des règles nationales, etc.) pour maîtriser un ou plusieurs dangers spécifiques ;*
- ***La comparaison avec un système de référence (CSM2)*** *: qui consiste à comparer le système en cours d'examen avec un système similaire (i.e., les deux systèmes satisfont un ensemble d'exigences communes) afin d'apprécier les risques ;*
- ***L'estimation du risque explicite (CSM3) :*** *dans le cas où les dangers ne sont pas couverts par l'un des deux principes précédents, une estimation (quantitative ou qualitative) des risques découlant d'un danger dans un contexte opérationnel particulier peut être utilisée. Le but est effectivement d'estimer le risque et d'assurer qu'il est acceptable.*

Dans le cadre de notre étude, nous avons utilisé un système de référence, qu'il s'agit du système de conduite en cabine, tout en nous appuyant sur un référentiel (le RCL), jugé comme un code de bonne pratique. Ainsi, les principes d'acceptation du risque adoptés sont les CSM1 et CSM2. Toutefois, il était toujours possible de faire appel au CSM3 dans le cas des nouveaux risques engendrés par le système de téléconduite et non couverts par le RCL. D'ailleurs, la norme EN50126-2 [5] met aussi le principe GAME dans la liste des méthodes et moyens permettant de définir et d'exprimer le niveau de risque acceptable pour une utilisation du CSM3. Pour finir, il est important de préciser que le risque tolérable en ce qui concerne la sécurité d'un système ferroviaire dépend des critères d'acceptation du risque définis par le cadre légal ou par la société d'exploitation ferroviaire conformément aux règles établies par le cadre légal.

V. CONCLUSION

Cette communication présente une démarche d'analyse de sécurité opérationnelle de relative à la téléconduite des trains fret. La démarche est basée sur une démonstration GAME par rapport au système de conduite en cabine, tout en s'appuyant sur un référentiel de conduite (RCL). La méthodologie mise en œuvre consiste à analyser l'ensemble des articles du RCL afin de déterminer des éventuels écarts (en termes de sécurité) qui peuvent engendrer de nouveaux risques sur le système ferroviaire ; puis ensuite proposer des exigences de sécurité et mesures de couverture pour assurer les objectifs de sécurité.

Une qualité majeure de cette étude est son exhaustivité, puisque le RCL documente toutes les situations professionnelles auxquelles un conducteur de ligne est confronté et fournit un support pour interagir avec la connaissance métier des experts de la conduite. Cette étude nous amène à formuler, au niveau opérationnel, des exigences de sécurité nécessaires à la couverture des écarts constatés et aussi à déterminer et à raffiner le périmètre de l'exploitation de la téléconduite sur le réseau ferroviaire.

La difficulté principale rencontrée durant cette étude, était l'absence de données et des REXs sur les risques opérationnels et organisationnels. Ainsi, l'ensemble des évaluations des risques sont réalisées en se basant sur les avis des experts de la conduite et de la sécurité.

Notant que la méthodologie proposée se focalise actuellement sur le niveau opérationnel de la téléconduite ; une possible extension aux niveaux fonctionnel et technique fait partie des perspectives.

REMERCIEMENTS

Les auteurs tiennent à remercier les participants aux divers ateliers de sécurité dans le cadre du projet TC-Rail. Plus particulièrement, A. Ouedraogo, P. Chambon (SNCF), Marc Tressol (SNCF) et E. Lauriot (Thales).

REFERENCES

[1] Arrêté du 19 mars 2012 fixant les objectifs, les méthodes, les indicateurs de sécurité et la réglementation technique de sécurité et d'interopérabilité applicables sur le réseau ferré national. NOR: TRAT1208556A. (Version consolidée au 20 avril 2020).

[2] Décret n° 2017-440 du 30 mars 2017 relatif à la sécurité des transports publics guidés NOR: DEVT1609684D. (Version consolidée au 20 avril 2020).

[3] Parouty, R., Zhao, L., & Biechy, E. (2014). Démarche sécuritaire pour les organisations en exploitation ferroviaire. *Congrès Lambda Mu 19 de Maîtrise des Risques et Sûreté de Fonctionnement, Dijon, 21-23 Octobre 2014.*

[4] STRMTG, (2011). Système de transport public guidés urbains de personnes : Principe GAME - méthodologie de démonstration. *Guide d'applicaiton.*

[5] CENELEC. NF EN 50126-2: 2017 Railways applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: System approach to safety.

[6] Côte, T., Rigaud, E., & Garbolino, E. (2014). Diversité et complexité de la mise en œuvre du principe «globalement au moins aussi équivalent»(GAME). *Congrès Lambda Mu 19 de Maîtrise des Risques et Sûreté de Fonctionnement, Dijon, 21-23 Octobre 2014*.

[7] Référentiel Traction, Document d'application, *Référentiel Conducteur de Ligne version informatique*, chapitres 0 et A à F, Édition du 25-11-2008, SNCF, Tech Report.

[8] Trentesaux, D., *et al*., (2018). "The Autonomous Train," *13th Annual Conference on System of Systems Engineering (SoSE)*, Paris, pp. 514-520.

[9] Masson, É., Richard, P., Garcia-Guillen, S., Morral-Adell, G. (2019). "TC-Rail: Railways remote driving". *12th World Congress on Railway Research*.

[10] PAS 1881 (2020). Assuring the safety of automated vehicle trials and testing specifications. bsi strandards.

[11] UL 4600 (2019). Standard for safety for the evaluation of autonomous Products. Edge Case research.

[12] ANSSI, EBIOS. "EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité." (2016).

[13] Zwingelsein, G. (2014). "Evaluation de la criticité des équipements – Méthodes d'exploitation des jugements d'experts," *Techniques d'ingénieurs* –Réf. SE4004 V1.

[14] Castellani, O., Chrun, S., Cloarec, J. M., & Pourchier, J. M. (2014). Une matrice de risque: pour faire quoi?. *Congrès Lambda Mu 19 de Maîtrise des Risques et Sûreté de Fonctionnement, Dijon, 21-23 Octobre 2014*.

ANNEXE : STRUCTURE DE L'APR AVEC UN EXEMPLE ILLUSTRATIF

TABLE II. **PARTIE 1 – ANALYSE DES ARTICLES RCL.**

Analyse du Référentiel de Conduite de Lignes				
Sous-chapitre	**N° Article**	**N° Page**	**Contexte**	**Élément de Sécurité**
Conduite du train	ART A43.01	263	Lorsqu'**un agent de desserte prend place dans la cabine de conduite**, cet agent avise verbalement le conducteur que l'évolution circule sous le régime spécial de l'annexe 2 du Règlement S4A. Dans le cas contraire, cette information est donnée au conducteur par écrit par l'agent - circulation.	L'accès d'un agent dans la cabine de conduite du train : procédure et sécurité

TABLE III. **PARTIE 2** – IDENTIFICATION DES ÉLEMENTS DE SÉCURITÉ.

Identification des éléments de sécurité				**Évaluation de Risque Initial**		
N° APR	**Écart Téléconduite VS Conduite en cabine**	**Évènement Redouté**	**Accident**	**Gravité**	**Fréquence**	**Criticité**
APR_TC_31	*Absence de règles et moyens de communication entre l'agent de desserte en cabine de conduite et le téléconducteur*	*Accident de l'agent de desserte lors la montée et/ou la descente du train*	Accident de personnels	Critique	x	Inacceptable

TABLE IV. **PARTIE 3** – MÉSURES DE COUVERTURES DES RISQUES.

Évaluation du Risque Final							
ID_Ex1	Exigence téléconducteur	ID_Ex2	Exigence Systèmes de Téléconduite	Principe de couverture du risque (MSC)	Gravité	Fréquence	Criticité
REQ_TC_03	Des règles et moyens de communication entre les personnes accédant à la cabine (agent de manœuvre, etc.) et le téléconducteur doivent être définis	REQ_STC_07	Le STC doit détecter la présence d'une personne / agent montant ou descendant de la cabine de conduite	MSC 1	Critique	x	Acceptable

TABLE V. **PARTIE 4** – ALLOCATION ET EXPORT DES EXIGENCES.

Allocation et export des exigences et contraintes					
Procédurale	Formation	Système à Bord	Système à Distance (IHM)	Télécom	Cybersécurité
X		**Y**	**Y**		