Analyse Des Risques Et De La Sécurité Du Transport Ferroviaire Autonome Pour Les Grandes Lignes : Contexte, Défis Et Solutions

Subeer Rangra, Mohamed Sallak, Walter Schön, Fabien Belmonte

RISK AND SAFETY ANALYSIS OF MAIN LINE AUTONOMOUS TRAIN OPERATION: CONTEXT, CHALLENGES AND SOLUTIONS

ANALYSE DES RISQUES ET DE LA SECURITE DU TRANSPORT FERROVIAIRE AUTONOME POUR LES GRANDES LIGNES : CONTEXTE, DEFIS ET SOLUTIONS

Subeer Rangra

IRT SystemX
8, avenue de la Vauve
91120 Palaiseau
subeer.rangra@irt-systemx.fr

Mohamed Sallak, Walter Schön

Sorbonne Université,
Université de Technologie de Compiègne
CNRS, UMR 7253, Heudiasyc
CS 60 203 Compiègne cedex
mohamed.sallak@utc.fr,
walter.schon@utc.fr

Fabien Belmonte

Alstom Transport
48 rue Albert Dhalenne
93484 Saint-Ouen cedex
fabien.belmonte@alstomgroup.com

Résumé

Ces dernières années, le transport autonome a connu des avancées technologiques significatives. Le transport ferroviaire urbain présente un avantage significatif dans l'exploitation d'un transport commercial entièrement automatisé. Le transport ferroviaire de grandes lignes vise également à bénéficier des avantages de l'automatisation. Ce travail est réalisé dans le cadre du projet TAS à l'IRT SystemX, avec les partenaires SNCF, Alstom Systra et l'Université de Technologie de Compiègne. Ce papier présente le contexte de l'automatisation du transport ferroviaire pour les grandes lignes. Les défis de la démonstration de la sécurité principalement pour les logiciels applicatifs sont discutés. En complément, une analyse de risque de certaines fonctions d'une automatisation complète (GoA 3/4) est effectuée. L'objectif de cette analyse est d'identifier les défis de la détermination des objectifs de sécurité d'un tel système autonome les développements ultérieurs et les démonstrations de la conformité.

Summary

Last few years have seen significant advances in the industrial application of autonomous road transport and has launched various actors in a technological race. Urban rail transport has a significant advantage in running fully automated commercial transport. Main line rail transport aims to also benefit from the advantages of automation. This work is done in the context of project TAS at IRT SystemX, with partners SNCF, Alstom Systra, and Université de Technologie de Compiègne. As part of the ongoing work this paper aims to present the context of automation for main line rail transport. The safety challenges in terms of the normative requirements, mainly for software-based solutions are discussed to identify developmental challenges. As a complement, risk analysis of some example functions for a full automation (GoA 3/4) is performed. The objective of this analysis is to identify the challenges associated with determining their safety targets, for subsequent development and demonstration to conformity.

1. Introduction

The recent surge towards autonomous driving in road vehicles has launched various actors in the transport domain in the so-called "relentless pace of automation"[1]. The railway domain, mainly urban transport has a significant advantage in running fully automated commercial transport since the early 1970s (Ruhlmann, 1964). Various technological, safety and operational challenges were identified and addressed in the development of such systems. These activities were far from straightforward, but were limited to a closed-world by controlling the environment and the operational context to a large extent (platform screen doors, zone of manual and automated operation, intrusion monitoring, etc.). The automation of main line rail transport in the open world environment renders most such solutions economically and technologically infeasible, and requires innovative solutions, in some cases such as the ones employed by autonomous road vehicles.

Furthermore, in main line rail travel the train driver is a central part of the transport system, and central part of its operational safety. In some cases explicitly recognized in national law (the French decree) train driver is explicitly identified to be *the* actor operating a train[2] (Le ministre de l'écologie du développement durable des transports et du logement, 2012). Making the regulatory context of a completely driverless train complicated. Moreover, these functions can sometimes be non-evident, for example detecting passengers trapped in between the platform screen doors, adapting to intrusions and climate related driving conditions, more such functions for metro operations are discussed for metro operations in (Karvonen et al., 2011). Thus, with such fundamental technological and functional changes, safety and risk analysis activities are faced with a challenge to identify and analyze the associated risk. Thus, on one hand main line autonomous rail transport has various opportunities (increased performance, cheaper freight service, optimization of

[1] Embracing the pace of automation: perspectives from other transport modes and countries https://www.rssb.co.uk/Pages/about-rssb/embracing-the-pace-of-automation.aspx

[2] « Driver: the person operating a train, whether operating the train directly or giving in-cab instructions to the person controlling the train controls. (Translation from French: « 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. »)

resources, etc.) in keeping up with such innovative solutions, and on the other it has to respect strict regulatory and normative frameworks and maintain the current level of safety of the system.

2. Context and objectives

The context of this paper is the work that is ongoing in the framework of the project TAS[3] (Transport terrestre Autonome en Sécurité dans son environnement / Safe Autonomous Land Transport) at IRT SystemX, with stakeholders and partners SNCF, Alstom Systra, and Université de Technologie de Compiègne. This project (with sister project TC Rail[4]) is part of a larger project *Train Autonome* of SNCF[5]. The main objective of this project, launched in April 2017 for a period of two years, is to design a system of perceiving the environment based on a combination of complementary sensors. It will be able to observe the environment and provide the information required to drive a train safely, to another system (excluded from the scope of the project), with for example, Automatic Train Operation-like (ATO) functionalities. The signaling context of this work is the French ` signaling (automatic block); trackside and track to train-based signaling systems (such as ETCS/ERTMS) are out of the scope of the project. For example, information provided by the system could be "there is a flashing red light on a signaling panel in front of the train" or "there is an object on the tracks". This work situates itself as one of the critical building blocks towards a GoA 3/4 level (IEC, 2009) of automation, with no/limited requirements from the railway trackside infrastructure.

The objectives of this paper are as follows:

- To present a preliminary discussion on the interpretation of GoAs for "autonomous train" in the context of main line operation.
- To discuss the challenges in terms of safety demonstration and compliance of such systems.
- To present a preliminary discussion to identify the safety targets of some core functions and ways forward in the context of Project TAS.

The next section of this paper discusses the notion of grades of automation and automation in metro transportation. The section 4 discusses some safety challenges in the context of main line rail transport vs. road transport, and further related to certification of software systems in this context. The section 5 presents some functions and risk analysis of those function to identify the safety requirements. The paper is concluded in section 6.

Table 1 *Grades of automation*

Grades and type of automation		Basic functions of train operation				
Grades of Automation	**Type of train operation**	**Ensuring safe movement of trains[6]**	**Driving (Control acceleration and braking)**	**Supervise track (prevent collision)**	**Supervision passenger Transfer**	**Operation in event of disruption**
GoA1	Non automated train operation (NTO)	Ensure safe speed : (ATP with Driver)	Driver	Driver	Driver	Driver
GoA2	Semi-automated train operation	Ensure safe speed (ATP)	Automatic (ATO)	Driver	Driver	Driver
GoA3	Driverless train operation (DTO)	Ensure safe speed (ATP)	Automatic	Automatic	Train Attendant	Train Attendant
GoA4	Unattended train operation (UTO)	Ensure safe speed (ATP)	Automatic	Automatic	Automatic	Automatic (Train Attendant)

3. Railway and automation

Automation in the context of rail transport is different from road transport. Their operational context and main functional requirements are different, hence require different definitions of automation.

i. Grade of automation (GoA) definitions and context

Four different grades of Automation have been defined for the context of railway. The norm "IEC 62267:2009 Railway applications - Automated Urban Guided Transport (AUGT) - Safety requirements" (IEC, 2009) defines these levels of automation in the context of urban guided transport, they are illustrated in Table 1.

GoA 0 refers to a manual operation with no automatic train protection. It refers to an on-sight train driving, where movements are fully under the control of the Train operator. Such as tramway and shunting movements in garages for the context of main line. GoA 1 and GoA 2 both require driver on the train with some functions accomplished by specific technical systems. In GoA 1 automatic train protection (ATP) system is installed, and will automatically apply the brakes if the train passes a closed signal or is travelling too fast. Most modern main line railway signaling systems implement varying (continuous or point-based control) degree of such an ATP system, preventing the unauthorized movement of a train irrespective of the

[3] Safe Autonomous Land Transport : http://www.irt-systemx.fr/project/tas/

[4] La Teleconduite sur Rail https://www.sncf.com/sncv1/fr/presse/article/teleconduite-sur-rail/191017

[5] Le Train Autonome : de quoi parle-t-on ? https://www.sncf.com/sncv1/fr/presse/article/train-autonome/160617 ; http://www.innovationrecherche.sncf.com/intelligence-artificielle-service-futur/ ;

[6] As per the norm ensure safe route (interlocking, etc) and ensure safe separation of trains (a signaling system) are all realized by a technical system for all these grades.

commands of the train driver[7]. ATP implements the idea of an independent safety system (more on discussion on this aspect in the section 3.). Some examples are: KVB (French: *contrôle de vitesse par balise*, English: Speed control by balise), ETCS (European train control system – the on-board and trackside systems implement an ATP system, among other functions), etc. GoA 2 implements in addition to this existing ATP, an automatic train operation (ATO) to control the movement of the train during regular operation. To note that in both these cases the driver is required on-board the train. GoA 3 and GoA 4 correspond to driverless and unattended train operation. In both these cases, as before ATP and ATO functions are still a part of the system, ensuring a safe movement and driving. GoA 3 retains an attendant on-board to operate doors, assist passengers and operate the train in event of disruption. In GoA 4, a train is fully automatic, as all the criteria listed above can be executed without a physical presence of a human on board. In the case of degraded modes the operation can be automated or assigned to a train attendant. Thus, the norm defines and categorizes the work of a train driver and technical systems in ensuring different classes of functions that are required to ensure safe operation. Depending on the context (tramway, metro, high-speed, conventional rail) of application the technical and economic feasibility, different applications use different grades of automation, the next section discusses them with a focus on the conventional rail application.

ii. Metro automation

Urban transport as discussed previously has a long history and industrial success; with such an industrial experience they have a relatively clearer idea of costs and key changes to achieve different grades of automation: GoA 1 (ATP) and GoA 2 (ATO) require mainly signaling, both on-board and trackside related modifications or replacements; GoA 3 and GoA 4 operations require considerations for (in addition to GoA1/2) communication and monitoring systems, as well as measures to supervise track and manage degraded modes. Further, the feasibility of these solutions depends on the specific characteristics of the system in question (Powell, Fraszczyk, Cheong, & Yeung, 2016). Some main advantages of GoA 4 feasibility in metro operations are the closed world advantages (lack of level crossings, presence of platform screen doors), ease of access in case of degraded operations (staff access and small interstation distances), limited and controlled zone of operations (no maintenance works near or on adjacent track during operation periods). Thus, full automation might not always be optimal choice depending on the possibility of track placement (underground, elevated, shared, etc.) and passenger demand, among other issues (Powell et al., 2016). Further, when modifying an existing system, there are various challenges that are present in the transition phase from existing semi-automated to full automation; the work in (Ghantous-Mouawad, Schön, Boulanger, & Churchill, 2006) discusses this for the case of metro traffic. They discuss on how the operational context is significantly different for the semi and fully automated trains – communication with operational center, timetable management, passenger exchange, etc. Hence, if normal traffic is to be maintained while carrying out the existing operations and there is need to manage, different kinds of traffic with specific operational procedures. Main line trains might not have such high traffic requirements, nevertheless managing semi-automated and full automated trains on the same track might require specific regulations. Thus, less improvements to trackside systems can keep disturbances to the existing operational context to a minimum.

iii. Adapting GoAs for the context of main line operations and its current state in the industry

It is to be noted that, although these grades of automation are well recognized in the railway industry, this standard is defined for “urban guided transport systems” (IEC, 2009). They do not apply to main line transport, as stated in the norm itself (IEC, 2009) : This standard does not apply to the following types of transport systems, unless specifically required by the Transport Authority : […] intercity and main line train services, generally operating in a rural environment on part of their routes.” Thus, there is a need to adapt these norms to main line transport, to manage the considerations of open world operating conditions and other operational differences. This further raises questions on its usage in describing the safety context of main line rail operations. A normative evolution might be required to define automation levels for mainline transport. Nevertheless the prudent step that we propose is to take the broad principles from the norm as-is, to illustrate the objectives of this paper. But as we discuss later, a separate analysis will be required to identify all the functions for main line.

The state of main line industrial application is currently limited to GoA1, there are very few if any implementations of GoA 2, and GoA 3/4 for main line service, or passenger service. The work in (Emery, 2017) illustrates the current state of GoA 2 applications for main line transport and the challenges towards GoA 3/4 in case of main line operations. A hybrid operational is where for a main line traverse a dense zone city section areas where there is a need to maximize the capacity of a particular section of the line. In such cases a train runs in dual automation modes: GoA 1 an ATP function (ETCS or class B[8]) in the suburbs and GoA 2 function of an ATO (a metro-like signaling system). Thameslink project in the UK uses ATO over ETCS (ATP) in the dense zone, only ETCS (ATP) in suburbs, Crossrail project implements CBTC in dense zone, standard ATP in suburbs, ongoing work for RER E, Eole in the Paris region also aims for GoA 2 operation in dense zones, and recent modernization of RER A by Alstom to GoA 2. Further, from standardization perspective ATO over ETCS for GoA 2 operations is said to be ready in the near futures for main line operations (Bienfait, Zoetardt, & Barnard, 2012). The work (Bienfait et al., 2012) lists some, main challenges in GoA 3/4: the first is the family of functions which are a result of the open world operational context: this includes the rather well known obstacle detection against potentially dangerous collisions; but a number of other observations – observation of the state of the train (self), other trains on the route (against irregularities), persons or animals alongside the tracks, on sight driving mode when a known danger is on the tracks. The on-sight mode is a degraded mode where special procedures apply, such as 30/40 km/h speed limit, also in case of problems of signaling-related known anomalies, this mode explicitly requires some “sight” capabilities. One solution can be remote driving, which is the objective of the TC Rail[9] project.

For the industrial and European actors, the context of ERTMS/ETCS-compatible automation make economic and technological sense. There have been various works in this context. In terms of incremental automations an ATO’s

[7] In nominal operating mode; in degraded cases by following specific procedures the driver can override these systems.
[8] Legacy train protection systems in European mainline rail transport as defined by the Control-Command and Signaling Technical specifications for interoperability regulation.
[9] La TéléConduite sur Rail : https://www.sncf.com/sncv1/fr/presse/article/teleconduite-sur-rail/191017

interface with ETCS is being developed and tested. The document (The ERTMS Users Group, 2016) describes the high level requirements for ATO over ETCS, they also make the following remarks, interesting from safety perspective:

- ATO is not safety critical; the existing systems such as ETCS are to manage the safety aspect;
- They identify the need to interface the ATO system with an "obstacle detection" system, and further precise that such a system is mandatory for GoA4.
- A “Supervise railway” function, which includes external obstacle detection/ railway supervision systems, platform/train interface, etc.

Thus, as a natural step GoA 2 can be implemented with more modern signaling systems such as ERTMS/ETCS, the specifications are in the process of standardization at EU level; however the requirements and concepts of GoA 3/4 still remain to be developed.

To conclude, the grades GoA 1/2 are achieved in current applications of main line (mixed) operations (GoA2) using existing ATP systems (ETCS, or existing class B systems) which are allocated the safety critical functions separately from functional aspects of driving a train. If the signaling system is composed of lateral signaling (ETCS Level 1, BAL (*block automatique lumineux*), etc.) for now a train driver is the only responsible actor. Thus, there does not exist yet even a GoA 2 solution for main line with lineside signaling. GoA 3/4 and existing industrialization require on one hand all that is expected in GoA1/2 in terms of signaling information. And other functionalities, which are yet to be developed fully, “sight” capabilities equivalent to a train driver on degraded operational context, obstacle detection, the surveillance of the railway environment (self-train and other trains) is a function which might require external and internal monitoring of a train and traffic. The next section discusses some challenges, in particular those related to safety concerning these functions.

4. Challenges of the safety demonstration and compliance processes in railway

As discussed before main line rail transport has no industrial implementation of (not at least in the EU) of complete GoA 3/4. Thus, there are very few works discussing the challenges related to safety demonstration of GoA 3/4-level for main line transport. One rather evident comparison in this context can be the normative and regulatory framework which plays an important role in defining the objectives and limit of the analysis. We present a short comparison with the automotive domain to put this in perspective. To expand on the challenges of certification process requirements, in particular, we discuss the case of software certification.

i. The normative and regulatory context in main line railway vs the automotive domain

Looking from a development perspective, automobile domain has seen the emergence of a large number of innovations and new technologies. In some cases main line rail transport can have a coherence between the requirements and operational contexts, and thus it might be prudent to consider exploring the application of some solutions successful in the automotive domain. In this line of reflection, it becomes important to reflect on the normative and regulatory context to compare the cross domain applicability of solutions (To note that we focus on the French and European regulations).

The work in (Baufreton et al., 2010) presents a cross domain discussion of normative and regulatory context. The high level of regulations are national regulations, which are high level texts stating safety objectives. These texts authorize another regulatory or assessment body to give certification and or qualification based on conformity to the specific standard (a norm). The automotive norm (ISO 26262) and railway norms (EN 50126, 50128, 50129) share a common ancestor, the IEC 61508. However, the chain of certification and commercial exploitation for railway systems passes through a Safety Authority (SA) and independent experts. These actors are a key aspect of railway safety. SA exist at national (EPSF, STRM-TG) and European (ERA) level. On the other hand for the automotive industry there is no such safety authority, nor national-level regulation to conform to. In this context, for railway the certification standards serve as 'codes of practice', and certification and qualification are given by the SA, on the demonstration of conformity to the specific standard, verified by independent experts (“notified body”). In addition, these requirements are getting more and more standardized, at least in Europe to aid in cross-border acceptance. Thus, the certification of railway systems, mainly if they deal with safety-related functions require conformity demonstrations and multiple levels of approvals before being commissioned.

The norms for railway being on multiple levels (EN 50126, generic for system level; EN 50126 for software and EN 50129 for hardware-based systems) are much more demanding and precise than the automotive norms. Such explicit requirements from process, systems (hardware and software) are lacking for the automotive domain. Although the automotive norm is currently going through an evolution, and questions on automation and functional safety are currently being discussed, interested reader can refer to (Griessnig & Schnellbach, 2017), (Bergenhem et al., 2015) (Palin, Ward, Habli, & Rivett, 2011). A detailed discussion of the norms is out of the scope of this paper. However, a particular case of software-based requirements is discussed in next subsection.

ii. Software safety demonstration in railway

The work in (Baufreton et al., 2010) also discusses this difference. In all the standards system-level feared events are assigned probability-based rareness based on their consequences (severity). For such systems, also refed to as technical systems (hardware and software) some probabilistic targets are assigned. To assess conformity to these targets, assessment for the hardware components can be done using probabilistic analysis since the norms take into account the probability of random hardware failures. Software on the other hand, is uniformly regarded as a deterministic artefact (Baufreton et al., 2010) whose functional failures, can only be caused by residual specification, design or implementation faults. Thus, in this case conformity is assessed based on the development in compliance with the domain specific standards. The probabilistic targets at system level are translated as different process requirements, for difference software functions. Thus, the certification objectives for technical systems are obtained through a mix of process-based and product-based development activities as recommended by the relevant norms. Thus, the safety assessment of software towards certification objectives is focused on software building process, heavily guided by the process described in the relevant norms.

This leads to an important conclusion that the safety assessment of software is focused on software safety building. Their assessment and measures towards certification objectives are mainly process-based and product-based development activities based on activities such as formal methods applications and other process or life-cycle requirements. Furthermore, for railway the regulatory context is relatively more exigent and thus a

close conformity needs to be maintained to the certification standard. Thus the next section goes into detail of the software norm EN 50128 for railways.

iii. Usage of AI in safety related functions

The open-world context of autonomous transport systems calls for some specific functionalities. Visual perception-based tasks which are performed currently by human actors. Such as visual-perception of signaling lights, obstacle recognition to detect people and other dangerous objects on tracks. Solutions to such specific problems are often based on artificial intelligence techniques. Since the context of TAS project is also detection of lineside signals, and obstacles on track: questions related their certification and safety demonstrations need to be posed. The question here becomes can a function (with its software part) based on AI be certified for accomplishing safety related functions? There are various point of views which can be taken to address this issue, this paper takes the existing norms in this case the software certification norm EN 50128.

The normative annex A of the norm (CENELEC, 2011), lists a number of techniques and different steps of the development cycle. With each technique a requirement, depending on its software safety integrity level (SIL), is associated. This requirement ranges from mandatory (M), Highly Recommended (HR), Recommended (R), Not Recommended (NR), and no recommendation (-). For, both extremes HR and NR, if the recommendations are not respected, the norm demands in the Software Quality Assurance Plan a "…rationale for using alternative techniques…" In this perimeter, the Table A.3 – Software Architecture, lists the technique "Artificial Intelligence – Fault Correction" as no recommendation for SIL0, and non-recommended (NR) for SIL1, SIL2, SIL3, and SIL4. The informative annex D, describes the aim of these techniques to "To be able to react to possible hazards in a very flexible way by introducing a mix (combination) of methods and process models and some kind of on-line safety and reliability analysis". Thus, the first roadblock is that the norms do not recommend the use of such techniques for safety related functions (SIL1 and up) for fault correction objectives (more precisely: fault prediction/correction, maintenance and supervisory actions), nor acknowledge their existence for other objectives.

Secondly, there are fundamental differences on how software-based functions are treated in the process-based software certification methods. Briefly speaking, they relate to the fact that the rules inferred by learning cannot be fully justified by human experts and therefore difficult to validate by conventional methods; even in the case of off-line learning, where the behavior of the resulting network is difficult to predict in some cases, although it remains deterministic. In case of incremental or on-line learning, the additional non-determinism of their behavior further complicates demonstration of its safety attributes. Despite of their successful applications in other applications they are less used for safety critical systems, in particular software-based safety critical systems which require much strict demonstrations of their validity. Fault tolerance mechanisms can be integrated into architecture of such functions (Rhazali, Lussier, Schön, & Geronimi, 2017), still development changes need to be addressed (Kurd, Kelly, & Austin, 2003).

A possible solution can be in a way in which railway systems manage safety (Baufreton et al., 2010). In railway systems safety is monitored and guaranteed by a specific system, often distinct from the system implementing the required function. On the other hand, automotive and aeronautics promote safe systems: the safety is "integrated" in the functional system (Baufreton et al., 2010). This reasoning follows from two criteria, the nature of system and cost. In the first case, it is difficult to lead the system to a safe state, this for example is difficult to do in the case of aeronautics. In the other case the automotive domain's focus on cost effectiveness also leads to more integrated safety systems rather than separate controls and systems. Rail systems make it easier to have fail-stop states to a certain limit, and being a public transportation system also allows a margin in terms of cost.

All these reasons culminate to the argument that it will be difficult to certify safety related functions based only on AI-related mechanisms for the existing safety context. However, the existing safety system in place can be kept to assure the safety related functions, and AI-based functions to increase performance.

5. Functions, operational context and safety targets for functions of a train driver

The objective of this section is to identify the possible safety requirements for some core GoA 3/4 functions. Functions of a train driver, from publicly available regulatory documents are used to illustrate the process. We follow the classical risk assessment steps of hazard identification, risk analysis and risk estimation. The main changes and challenges exist in all of these three steps. To resume, the first step is to identify the dangers: as discussed in previous sections identification of all the tasks of a human driver and the associated dangers is not evident, and will require an approach starting from a blank page; the safety requirements and even the performances of the tasks performed by a human driver can be difficult to define precisely. A technical system replacing a human driver will require justifying the safety targets and their derivations. This section aims to illustrate these challenges.

Focusing on a GoA 3/4 operational context, we take an example from a EPSF document (EPSF, 2016b) and another similar document (SNCF RÉSEAU, 2017) (translated from French). These both are reference documents which are French codes of practice documents for train drivers. The following Table 2 describes two functions, the relevant text in these documents and an equivalent function. These two functions are chosen so as to represent both the context of a GoA 3/4 (which includes a GoA 2 operation). The examples provided are to illustrate a possible solution to risk analysis of such operations and are not meant to be exhaustive.

Table 2 Functions of a system replacing a train driver for GoA 3/4 operation

Reference text	Source	ID	Function for GoA 3/4
Article 402 - Route Observation. During the journey, the driver must observe the track and the catenary as far as the driving of the train allows him to do so. He must be prepared to slow down or stop depending on the circumstances or the signals that could be given to him. The purpose of track observation is:	(EPSF, 2016b)	**F1**	**Observation of the track and catenary:** • **presence of *obstacles*** (for simplification only this objective is treated here)

• To recognize from as far away as possible the signals addressed to the train, the transition points of the speed limit, the stopping points, etc. • To monitor the general condition of the track and the catenary in order to detect a possible anomaly ; • To detect the possible presence of obstacles ; • To detect the presence of people in the tracks; • To detect and report malicious acts.			
Article 101. Observation and appearance of signals 101.1. Signal principles The signals shall in all circumstances give the agents concerned, in particular the drivers, the orders and information which they must comply with. The driver shall endeavor to recognize as far as possible the indications given by the signals and shall not lose interest in their observation until he has passed them. Every agent, whatever his function, must obey passively and immediately the signals concerning him.	(SNCF RÉSEAU, 2017)	**F2**	**Observation of the stopping signals (lineside signaling).** (to note that the relevant document also provides a relatively exhaustive list of the signals applicable on the French network (SNCF RÉSEAU, 2017))

i. Hazard identification, analysis and estimation.

The first step aims to identify the hazards associated with these two functions. A combination of top-down and bottom-up approaches is mandatory to ensure the completeness of the analysis. The two approaches are based on different categories of reasoning: top down is based on knowledge/experience and does not take into account design choices potential hazards; which is why a bottom-up (inductive) analysis based on the design spec shall also be performed). The top-down approach is also known as a Preliminary Hazard Analysis (PHA). The system here is the composed of the two functions as given in the Table 2, this is what we call in this case as the system under analysis or simply the system.

The logical relation of the elements of a PHA is made so as to be able to deduce the hazards in the perimeter of the system under analysis. It is given as follows:

ACCIDENTAL EVENTS AT RAILWAY SYSTEM LEVEL [are a propagation of] DANGEROUS SITUATIONS [which are caused by] HAZARD AT SYSTEM-LEVEL in the context of the system under analysis. The results of this top-down approach for the system under analysis is given in Table 3.

Table 3 PHA: a top-down approach to identify the hazards

ACCIDENTAL EVENTS AT RAILWAY SYSTEM LEVEL	DANGEROUS SITUATIONS	HAZARD AT SYSTEM-LEVEL
Collision of a train against an obstacle	Presence of an obstacle on the track	Failure of the observation function: Obstacle on the track not detected
Rear-end collision with a train	Spacing between trains not maintained, by not respecting stopping signals (lineside signals).	Failure of the observation functions: lateral signaling

The bottom-up functional approach on the same functions as a classical FMECA (Failure mode, effects and criticality analysis) is given in Table 4.

Table 4 The bottom-up functional approach to identify the hazards in the scope of the system

FUNCTION	FAILURE MODE	HAZARD AT SYSTEM-LEVEL	CONSEQUENCES AT THE RAILWAY SYSTEM LEVEL	POTENTIAL ACCIDENT AND CONSEQUENCES
F1. Observation of the track and catenary: presence of *obstacles*	Loss of **track and catenary** observation	Failure of the **Observation of the track and catenary** function: Obstacle on the track not detected	Collision with an obstacle on the track.	Multiple fatalities and damage to the environment
	Degraded output of the of **track and catenary** observation	Failure of the **Observation of the track and catenary** function: Obstacle on the track not detected or partially detected. Insufficient to make a decision.	Collision with an obstacle on the track.	Multiple fatalities and damage to the environment
	Presence of obstacle on the track observed, when there is none	Obstacle on the track detected when there is none.	Degraded service.	No safety-related damages, delay in service and degradation of brakes.
F2 Observation of the stopping signals.	Loss of **Observation of the stopping signals**.	Failure of the **Observation of a stopping signal.**	Rear-end collision with a train	Multiple fatalities and damage to the environment

	Degraded output of **Observation of the stopping signals.**	Incomplete **Observation of a stopping signal.** Insufficient to make a decision.	Rear-end collision with a train	Multiple fatalities and damage to the environment.
	Presence of a stopping signal observed when there is none	Stopping signal detected when there is none.	Degraded service.	No safety-related damages, delay in service and degradation of brakes.

The fusion of these two approaches that is the columns "Hazard at System-Level" from both the Table 3 and Table 4, gives a list of hazards in Table 5, also known as a hazard log. Only the hazards with catastrophic: Multiple fatalities and damage to the environment are considered from a safety point of view.

Table 5 Hazard log for the system under analysis

ID	Hazard at system-level with catastrophic consequence for the railway system
H1	Failure of the **Observation of the track and catenary** function: Obstacle on the track not detected
H2	Failure of the **Observation of the track and catenary** function: Obstacle on the track not detected or partially detected. Insufficient to make a decision.
H3	Failure of the **Observation of a stopping signal.**
H4	Incomplete **Observation of a stopping signal.** Insufficient to make a decision.

Once the hazards in the perimeter of the system are identified, the related risk needs to be estimated, in order to define the safety requirements for the concerned functions.

ii. Risk analysis and estimation

Each hazard is analyzed to estimate the risk associated with it. As prescribed by the section *8.3. Risk acceptance principles and risk evaluation*, of the part 2 of the norm EN 50126 (CENELEC, 2017), there are three possibilities of risk analysis and estimation:

1. Use of code of practice.
2. Use of a reference system.
3. Use of explicit risk estimation.

Since, there exist no applications of GoA 3/4 in main line transport, hence there is no existing Code of Practice or in a strict sense a reference technical system which performs obstacle detection function in the operational context of open track. For the detection of stopping signals, even though the main observation is performed by a train driver, safety related functions in some cases are managed by ATP functions.

F2 Observation of the stopping signals.

For the function *F2: observation of stopping signals* (lineside signals), a train driver is the only responsible actor, as recognized by the regulation (SNCF RÉSEAU, 2017). To note that F2 is limited to lineside static and dynamic signaling, there is also cabin-signaling which is not in the scope of this project. Thus, in this case Code of Practice or reference system can relate to a train driver. The question here becomes can a human actor be used as reference system for a technical system? And is a code of practice applicable to a human actor in this case, is also applicable to a technical system? Looking at the requirements to apply reference system-based analysis (CENELEC, 2017) the safety requirements and the corresponding hazards – are to be identified from the safety analysis of the reference system, a human driver in our case. In particular the hazards covered by the reference system (safety related functions) and related safety related performance. Given that signaling systems and lineside signals are in most case equipped with ATP systems which perform the safety function, while human plays a functional role. Thus, if the human driver is chosen as a reference system, and if the operational context is equipped with an ATP system, the human is not the only actor responsible for covering a hazard. It is apportioned between the human driver and the ATP. The ATP being a technical system, its safety performance is known. More advanced methods exist which allow precisely determining human performance (Rangra, Sallak, Schon, & Vanderhaegen, 2017), given a careful data collection and analysis process is followed. Since human safety performance-related data is difficult to obtain, and human performance heavily influenced by a given context, defining the human driver as a reference system is not an easy task.

Thus the first way is to use data from explicit evaluation of the human driver for the functions under analysis. A French infrastructure manager document (SNCF Réseau / Réseau ferré de France, 2008), which cites the absolute failure rate of a driver crossing a closed signal (FSA) as 2.4×10^{-5} per hour, without a KVB system in place (FSA when a signal is equipped with a working KVB system is 5.4×10^{-7}). It states that the data was obtained from empirical and expert sources. The context of operation analyzed in this report and function analyzed represent more closely the context of application of this work. Still, it covers only one aspect of a signal (a closed signal protecting a point). The main issue with such a data is that is dates back to 1990. Furthermore, although the process can be repeated to obtain a similar number it still does not address the issue of contextual factors.

Another, approach is to simply use the absolute value of human performance available in accident/incident data. The annual security report of EPSF for the French rail network (EPSF, 2016a) presents a section on the signals passed at danger (FSA: *franchissements de signaux d'arrêt*, in French). For the year 2016 it states 0.304 FSA per million train kilometers. Further, in a detailed analysis it states the number of such incidents in terms of their causal factors: 66 % are attributed to a train driver. This gives 0.2244 FSA per million train kilometers due to driver not respecting the stopping signal. To note that this is an absolute value, at a system-level. It represents a large operational context: activations of train protection systems, different signaling systems, garage and parking operations, etc. Thus it can be used as an upper limit for the safety target of a system replacing a human driver, and will need a translation from number of kilometers to hours, to calculate the safety target for *H3 and H4*.

A straightforward critique of values coming from accident/incident data is that it might be different between countries, thus requiring extra work if cross-border operation is required.

F1 Observation of the track and catenary function

As discussed before, GoA 3/4 application in main line transport does not exist, hence there is no code of practice or reference system that can be used. Hence, an explicit risk estimation is to be performed. The section 8.4 of the part 2 of the EN 50126 (CENELEC, 2017) describes the quantitative approach of explicit risk estimation. In this case for each hazard for the system under consideration a THR (Tolerable Hazard Rate) needs to be derived. For the system under consideration as a whole, the norm prescribes that the THR can be derived from accident reports by the railway duty holder. And the supplier is responsible for

apportioning the THR into the system or subsystem under consideration. Such an approach is illustrated here. The informative Annex B of the norm EN 50126 describes this process, starting with a disclaimer that "THR cannot be calculated from accident statistics unless rigorously collected statistics models are available." Given that such data is available, we illustrate an example below. The norm gives the formula as:

$$\lambda = \frac{N}{H \times U}$$

Where: N number of Hazardous failure per year, H total number of operational hours per year, U is the total number of units in operation per year of the system which concerns this particular hazard.

We use the publicly available database SNCF Open Data[10] to derive a THR for the hazard *collision with an obstacle*. This database lists railway incidents on the French national network. Apart from giving a generic list of incidents on the type of event (rear-end collision, collision with obstacle, etc.), it also defines if it was a remarkable security event (ESR, French for *événement de sécurité remarquable*). It is defined as a safety incident related to an event which endangered or was likely to endanger the lives of persons transported and in the vicinity of railway installations. We focus on the following ESRs, for hazards under analysis (H1 and H2):

- *Collision contre obstacle* (collision with an obstacle)
- *Présence d'obstacle sur voie* (presence of an obstacle on the track)
- *Collision contre obstacle et déraillement* (collision with an obstacle an derailment)
- *Obstacle sur voie* (obstacle on the track)

To note that, events which occur at level-crossings are out of scope of this work. Complete data is available for the year 2014, 2015, 2016 and 2017. The following data is obtained:

Year	Collision events	ESR's
2014	7	1
2015	26	3
2016	21	5
2017	16	4

We consider a normal probability distribution and use 95% confidence interval for the number of ESRs per year. Thus the mean ESR is 3.25, standard deviation 1.7, and standard error of mean for 95% confidence interval 0.85; giving an interval of $[1.8, 5.6]$ events per year. Using this data we calculated the upper and lower bounds on the rate of such ESRs per hour. For an average of 16 hours of operation (assumption) per day for a total of 15000 total trains (Source: SNCF Réseau website) in circulation on RFN. We get 87600000 total hours per year (H×U) of operation of all trains. And finally obtain the per hour rate of obstacle-collision related ESRs as belonging to the interval: $[1.8 \times 10^{-8}, 5.6 \times 10^{-8}]$. To note that, the standard error is of the same order as the mean. Such high standard error raises questions on the amount of the data available. Nevertheless, this gives an indication that the target assigned is of the order of 10^{-8} unless more precise data is available.

The norm further states that to assign this value as the THR there needs to be review of the accident statistics over a number of years. A small textual description is provided with the database, it can be used to identify the details on the type of obstacle, the operational context, etc. However all the textual descriptions are not uniform in terms of the details, and will need to be parsed manually to identify the relevance. The rigor, quality and quality of data will be need to be justified, the data collection process will also need to be scrutinized. Expert judgment will be needed to justify and argument for the use of such data and the THR identified. A similar discussion can be found in examples of the CSM-DT guide, in particular Page 103, the paragraph G3 and the footnote 19 (European Union Agency for Railways, 2017).

Another possibility to determine explicitly the safety targets is the use of CSM-DT (Common Safety Methods – Design Targets). The CSM-DT guide (European Union Agency for Railways, 2017) provides a detailed discussion and gives some examples. CSM-DT process is part of the Explicit Risk Estimation principle of the CSM process (Annex I, point 2.5.4. originally in Regulation No. 401/2013 (European Commission, 2013), amended in regulation No. 2015/1136 (European Commission, 2015) as article 2.5.5.). It allows fixing quantitative design targets in terms of quantitative requirements. The article 2.5.5. of (European Commission, 2015) states two conditions to apply as design targets (DT), as follows:

- "(a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.
- (b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable."

The first key first here is consequence, i.e. *critical* or *catastrophic*; and second "directly". Since there is no human on-board the repartition of this target relates directly to a technical system. Both of these terms are discussed below, as also defined in (European Commission, 2015).

In case of "*catastrophic"* accident category, "*highly improbable*" is defined as an occurrence of failure at a frequency less than or equal to 10^{-9} per operating hour; and in case of "*critical*" (affecting a small number of people, at least one fatality) "*improbable"* defined as less than or equal to 10^{-7} per operating hour. The table 6 of the guide summarizes the allocation of CSM-DT categories vs. number of affected persons (European Union Agency for Railways, 2017). Thus, a minima the obstacle detection system should be able to detect a person on the tracks, in that case 10^{-7} per operating hour can be used as a design target, and 10^{-9} for big obstacles and groups of people on tracks, with a possibility of collision at higher speeds. If it is not evident to determine the consequences, some examples in the guide (European Union Agency for Railways, 2017) present posing the following two alternative questions : "(a) Is the considered accident limited to a specific area of the train and thus exposes to risk only the passengers located in that area? Or (b) Is the considered accident affecting the whole train and thus exposes to risk all train passengers or are other trains or many third parties external to the railway premises exposed to risk (e.g. persons living in the vicinity of the track in case of derailment)?." The former leads to a *catastrophic* and the latter to a *critical* category. Depending on the complexity of the scenario these alternative questions can aid the reasoning.

Further, the term "*directly"* is defined in the amendment to the CSM regulation (Reg. 2015/1136 (European Commission, 2015), Annex I, point 2.5.8.(a)), as "…the failure of the function has the potential to lead to the type of accident referred to in point 2.5.5 without the need for additional failures to occur." The example of the CSM-DT's guide Annex 3, page 60, and paragraph G2 onwards discusses it further. They argue that, following the definition of directly the hazards and a failure of the function needs to

[10] SNCF Open Data : Incidents de sécurité https://ressources.data.sncf.com/explore/dataset/incidents-securite/information/?sort=date

occur at the same time to lead to an accident. That is : "…although a combination of events and failures is necessary to lead to the undesired consequence (an "AND" in the condition) in practice, it is still a single functional failure of the function…". The CSM-DT category, thus applies to directly and only the functional failure of a technical system under analysis.

Other point of views are also found, the *Modsafe project*[11]. The project (deliverable 4.2.) identifies the generic SIL requirements for different GoA application in urban guided transport systems. They classify the obstacle detection systems as safety related function, but state that a generic safety level cannot be identified for such functions. This discussion is extended in another deliverable (MODSafe Project, 2012), taking the Risk Graph Approach from the norm IEC 61508-2 (refer discussion in section 4.i.) to determine the safety requirements of functions with low demand modes. They classify an obstacle detection system as a "safety function operating in low demand mode". The low demand mode is applicable to functions which cover a safety related function but a failure of the said functions does not lead directly to a hazard, since the hazard is not continually present. They conclude an obstacle detection function falls under such a category. And in this case the safety requirements for such a function are to be determined based on three key parameters: the estimated appearance of the potentially unsafe event λ_I; (and the associated THR); the acceptable failure rate of the system λ_{SE};and the inspection/repair rate μ_{SE};The target (THR) for the system thus corresponds to:

$$\lambda_{SYS} = \lambda_I \frac{\lambda_{SE}}{\mu_{SE}}$$

Here, λ_{SYS} is the derived overall failure rate of the system, i.e. the quantitative safety requirement. Thus, following this approach this target needs to be adapted to derive the safety requirements, that is in this case the failure of an obstacle detection function (F1 or F2) and the presence of such an obstacle (one person, or consequences of a catastrophic accident for the train). Events like collision with huge obstacles at high speeds are relatively rare, and as seen previously it can be difficult to obtain sufficiently significant data. Also, as noted in the example of CSM-DT guide's previously, the authors still interpret such functions as a single functional failure of the function. And thus apply the derived safety target as-is.
More work will still be required in this case also. Defining the safety targets related to these hazards is only the first step, in the descending phase of the V-Cycle; but an important one nonetheless.

6. Conclusions

This paper presents a preliminary discussion on the safety challenges for the functions of observations of an autonomous train. More specifically the activities of safety in the context of TAS project. One of the main challenges is to identify the safety requirements and the associated targets towards GoA3/4 level of automation. The absence of such levels of automation in mainline railway presents technological as well as fundamental risk assessment and acceptance related challenges. This paper first establishes the positioning of mainline railway in a GoA-context. It also presents through a classical risk assessment process few ways to identify safety targets for two essential functions. The observation of lineside signaling, and obstacle detection. For both of these functions, we identify the risks using inductive and deductive reasoning. Multiple options for their risk analysis and estimation are presented as open discussion.

For the reception of signaling related information, the observation of lineside signaling is currently only managed by a human driver. New solutions are required in this case. The safety requirements in this case can be assigned to ATP systems which perform the safety function, while human plays a functional role. If the human performs a safety-related function. That is the overall target is apportioned between the human driver and the ATP, human performance related to those functions needs to be identified. Data from national safety reports can provide an indication of current-level of safety at the train system-level. Studies by railway operators evaluating train driver performances can also be used to obtain a human driver's safety related performance for risk analysis and assessment using a the reference system principle. This reasoning still poses the questions: can a human actor be used as reference system for a technical system? And is a code of practice applicable to a human also applicable to a technical system?

Main line rail transport has a handful of GoA 2/3/4 industrial implementation. The issue that has been highlighted also is that there does not exist a normative definition of GoA for main line transport. What exists is mixed traffic applications, and industrial applications in metro transport. So, the prudent step is to take the broad principles from the norm as is and then perform a separate analysis to identify functions for main line. But in the long term, a normative evolution will be required.

For obstacle detection functions the solutions for metro are in most cases not technically feasible for main line operations due to open world (environment and traffic) nature of their operations. We discussed a few possibilities to define the safety targets related to an obstacle detection function for main line transport. First, is the use of accident statistics to derive the relevant THR. The second is the use of quantitative safety targets from the common safety methods (CSM-DT) EU regulation – based on the consequences of a given hazards for the system. The challenges, such as the need of accident statistics to be rigorous, and CSM-DT targets for functional failures, of functions in low demand mode where the hazard is not continually present were also discussed.

This paper only dealt with descending steps of V cycle, the risk analysis and estimation steps. Next steps are the demonstration to conformity of the proposed solutions, to analyze the functions, the system designs, and put these functions in their operational contexts. Dealing with a large number of scenarios in an open work context might require more systematic model-based safety analysis approaches to simplify the safety analysis process. This will be addressed in the future work.

Acknowledgements

The authors would like to thank the funding agencies, project stakeholders and partners of the TAS project and IRT SystemX.

References

Baufreton, P., Blanquart, J. P., Boulanger, J. L., Delseny, H., Derrien, J. C., Gassino, J., … Ricque, B. (2010). Multi-domain comparison of safety standards. In *Proceedings of the 5th international conference on embedded real time software and systems (ERTS2)* (pp. 1–12). Toulouse, France.

Bergenhem, C., Johansson, R., Söderberg, A., Nilsson, J., Tryggvesson, J., Törngren, M., & Ursing, S. (2015). How to Reach Complete Safety Requirement Refinement for Autonomous Vehicles. *CARS* -

[11] MODSafe - Modular Urban Transport Safety and Security Analysis. http://www.modsafe.eu/

Critical Automotive Applications: Robustness & Safety. Retrieved from https://hal.archives-ouvertes.fr/hal-01190734

Bienfait, B., Zoetardt, P., & Barnard, B. (2012). Automatic Train Operation : the Mandatory Improvement for ETCS Applications. *Aspect 2012 Irse*, 1–10.

CENELEC. NF EN 50128 Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems (2011).

CENELEC. (2017). EN 50126-2:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety.

Emery, D. (2017). Towards Automatic Train Operation for long distance services: State-of-the art and challenges. In *17th Swiss Transport Research Conference. No. EPFL-CONF-230293*.

EPSF. (2016a). *RAPPORT ANNUEL SUR LA SÉCURITÉ DES CIRCULATIONS FERROVIAIRES 2016*. Retrieved from http://www.securite-ferroviaire.fr/les-donnees-chiffrees-de-la-securite/rapport-annuel-sur-la-securite

EPSF. (2016b). Recommandation RC A-B 2c n°1. Circulation des trains. Retrieved from http://www.securite-ferroviaire.fr/reglementations/circulation-des-trains-0

European Commission. (2013). Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009. Retrieved from http://data.europa.eu/eli/reg_impl/2013/402/oj

European Commission. (2015). Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment (Text with EEA relevance), *2015/1136/*(352), 6–10. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.185.01.0006.01.ENG

European Union Agency for Railways. (2017). Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013, *33*(0), 139. Retrieved from http://www.era.europa.eu/Document-Register/Pages/Guideline-supporting-the-implementation-of-(EU)-Regulation-20151136-on-harmonised-design-targets-(CSM-DT).aspx

Fairfield, N., & Urmson, C. (2011). Traffic light mapping and detection. *Proceedings - IEEE International Conference on Robotics and Automation*, 5421–5426. https://doi.org/10.1109/ICRA.2011.5980164

Ghantous-Mouawad, M., Schön, W., Boulanger, J.-L., & Churchill, G. (2006). Modelling and simulation of the traffic management in a migration phase: example of “Ligne 1” of the Parisian subway. In *Computers in Railways X* (Vol. 1, pp. 55–64). Southampton, UK: WIT Press. https://doi.org/10.2495/CR060061

Griessnig, G., & Schnellbach, A. (2017). Development of the 2nd Edition of the ISO 26262 (Vol. 748, pp. 535–546). https://doi.org/10.1007/978-3-319-64218-5_44

IEC. IEC 62267:2009 Railway applications - Automated urban guided transport (AUGT) - Safety requirements, 2009 Test § (2009). Retrieved from https://webstore.iec.ch/publication/6681

Karvonen, H., Aaltonen, I., Wahlström, M., Salo, L., Savioja, P., & Norros, L. (2011). Hidden roles of the train driver: A challenge for metro automation. *Interacting with Computers*, *23*(4), 289–298. https://doi.org/10.1016/j.intcom.2011.04.008

Kurd, Z., Kelly, T., & Austin, J. (2003). Safety criteria and safety lifecycle for artificial neural networks. *Proceedings of European Symposium on Intelligent Technologies, Hybrid Systems and Their Implementation on Smart Adaptive Systems*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.4490&rep=rep1&type=pdf

Le ministre de l’écologie du développement durable des transports et du logement. (2012). 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. Retrieved from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582663

MODSafe Project. (2012). *D4.2. Analysis of Common Safety Requirements Allocation for MODSafe continuous Safety Measures and Functions*. Retrieved from http://www.modsafe.eu/fileadmin/documents/deliverables/DEL_D4_3_UITP_WP4_120220_V_1.3.pdf

Palin, R., Ward, D., Habli, I., & Rivett, R. (2011). ISO 26262 safety cases: compliance and assurance. *6th IET International Conference on System Safety 2011*, B12–B12. https://doi.org/10.1049/cp.2011.0251

Powell, J. P., Fraszczyk, A., Cheong, C. N., & Yeung, H. K. (2016). Potential Benefits and Obstacles of Implementing Driverless Train Operation on the Tyne and Wear Metro: A Simulation Exercise. *Urban Rail Transit*, *2*(3–4), 114–127. https://doi.org/10.1007/s40864-016-0046-9

Rangra, S., Sallak, M., Schon, W., & Vanderhaegen, F. (2017). A Graphical Model Based on Performance Shaping Factors for Assessing Human Reliability. *IEEE Transactions on Reliability*, *66*(4), 1120–1143. https://doi.org/10.1109/TR.2017.2755543

Rhazali, K., Lussier, B., Schön, W., & Geronimi, S. (2017). Tolérance aux fautes pour détecter les comportements indésirables des réseaux de neurones. In *Qualita2 017*. Bourges, France.

Ruhlmann, H. (1964). Paper 4: Automatic Driving of Trains. *Proceedings of the Institution of Mechanical Engineers, Conference Proceedings*, *179*(1), 106–112. https://doi.org/10.1243/PIME_CONF_1964_179_017_02

SNCF RÉSEAU. Dispositions complémentaires à l’annexe VII de l’arrêté du 19 mars 2012 modifié - Signalisation au sol et signalisation à main (2017).

SNCF Réseau / Réseau ferré de France. (2008). *Bilan LOTI du contrôle de vitesse par balises (KVB)*. Retrieved from https://www.sncf-reseau.fr/sites/default/files/upload/_Import/pdf/bilan_loti_kvb-2.pdf

The ERTMS Users Group. (2016). *ATO OVER ETCS OPERATIONAL REQUIREMENTS*. Retrieved from http://www.era.europa.eu/Document-Register/Documents/ATO_Ops_Requirements_v1_7.pdf