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

Evolution des méthodes d'évaluation des Risques dans le développement des Trains Autonomes

Evolution of Risk Evaluation Methods in the Development of Autonomous Trains

BARBAT Jérôme
SECTOR
Toulouse
jerome.barbat@sector-group.net

MACHKOUR Malake
SECTOR
Toulouse
malake.machkour@sector-group.net

BRACQUEMOND Annie
SAFER MOBILITY
Paris
a.bracquemond@safermobility.fr

Résumé — Dans le contexte actuel de réindustrialisation qui touche divers secteurs, l'industrie ferroviaire est en train de vivre une transformation majeure, l'automatisation des trains en particulier est en plein essor. Dans ce contexte, les exigences industrielles se renforcent et les innovations émergent, ce qui soulève la question de la Sûreté de Fonctionnement de manière essentielle.

Dans le cadre du développement d'un système de détection d'obstacle pour un projet de train autonome, SECTOR a utilisé une approche d'analogie en s'inspirant du secteur automobile qui a introduit une nouvelle norme pour les véhicules autonomes et leurs systèmes associés, à savoir l'ISO 21448 - Road Vehicles - Safety Of the Intended Functionality, également connue sous le nom de norme SOTIF [1]. Etant donné qu'en l'absence de conducteur humain l'application du critère de « Contrôlabilité du conducteur » n'est plus aussi pertinente pour les trains ou les systèmes de mobilité autonomes, il a été impératif de développer une méthode d'évaluation des risques adaptée à ce contexte spécifique.

Les travaux menés par SECTOR ont permis de proposer une méthode de spécification d'exigences de sécurité à destination d'une fonction automatisée, de caractériser la performance du facteur humain du conducteur (qui présente un haut niveau de variabilité en fonction des situations) et d'établir une cartographie des écarts entre la performance atteinte par le conducteur et les niveaux de sécurité requis par une fonction automatisée, considérant le risque dans l'absolu.

Mots-clefs — Sécurité, Train, Autonome, SOTIF, ISO 26262

Abstract — In the current context of reindustrialization affecting various sectors, the railway industry is undergoing a major transformation, train automation in particular is booming. In this context, industrial requirements are strengthening, and innovations are emerging, which raises the question of operational safety in an essential way.

As part of the development of an obstacle detection system for an autonomous train project, SECTOR used an analogy approach inspired by the automotive sector which introduced a new standard for autonomous vehicles and their associated systems , namely ISO 21448 - Road Vehicles - Safety Of the Intended Functionality, also known as the SOTIF standard [1], given that in the absence of a human driver the application of the "Controllability by the driver" criterion is no longer as relevant for trains or autonomous mobility systems, it was imperative to develop a risk assessment method adapted to this specific context.

The work carried out by SECTOR proposes a new method of specification of safety requirements for an automated function, to characterize the performance of the human factor of the train conductor (which presents a high level of variability depending on the situations) and to establish a map of the gaps between the performance achieved by the driver and the safety levels required by an automated function, considering the risk in absolute terms.

Keywords — Security, Train, Autonomous, SOTIF, ISO 26262

I. INTRODUCTION

Dans le contexte global d'un secteur des transports tendant de plus en plus vers l'autonomisation de la conduite, le secteur ferroviaire n'est pas en reste et est confronté à certaines problématiques inhérentes à cette transition technologique.

Dans le cadre d'un projet de train autonome, une Analyse Préliminaire de Risques (APR) a été menée et a permis de spécifier des niveaux de Safety Integrity Level (SIL) pour un certain nombre de fonctions réalisées actuellement par le conducteur mais qui seront automatisées dans le cadre du projet.

Cependant, contrairement à des tâches simples telles que le respect de la signalisation, la fiabilité de certaines fonctions réalisées aujourd'hui par l'homme telles que la détection d'obstacle sur la voie n'est pas constante dans le temps et dépend d'un certain nombre de facteurs de contexte ayant parfois un fort niveau d'aléa :

- Niveau de visibilité de la voie (dépendant de la luminosité, brouillard, environnement etc.) ;
- Nature, taille, distance, temps de révélation et dangerosité de l'obstacle ;
- Vitesse du train ;
- Niveau de vigilance du conducteur à la survenue de l'évènement et temps de réaction (dépend notamment de la phase de conduite et de ses tâches du moment) ;
- Etc.

Ainsi, il est largement pressenti que le niveau de fiabilité de l'homme associé à cette fonction est bien inférieur au taux de fiabilité humain associé à des tâches plus routinières. Cependant, la difficulté de quantification d'un taux de défaillance humain sur ce sujet précis résultant notamment de l'impact plus ou moins prononcé des différents facteurs aléatoires cités précédemment rend difficile la spécification d'un niveau de fiabilité global raisonnable à la fonction automatisée de détection d'obstacle.

L'objectif vise à établir quel serait le niveau de sécurité acceptable pour la fonction de détection d'obstacle en considérant le risque dans l'absolu et de le comparer avec la performance actuelle.

II. ANALOGIE AVEC LE SECTEUR AUTOMOBILE

Le secteur automobile défini une nouvelle norme applicable aux véhicules autonomes et leurs systèmes associés, l'ISO 21448 – Road Vehicles - Safety Of the Intended Functionality, ou norme SOTIF. En effet, l'application du critère de « Controllability by the Driver » n'étant plus possible pour un train ou un système de mobilité autonome, il devient donc nécessaire de trouver une nouvelle méthode d'évaluation des risques.

La chronologie des étapes proposées par SECTOR est représentée sur le schéma ci-dessous :

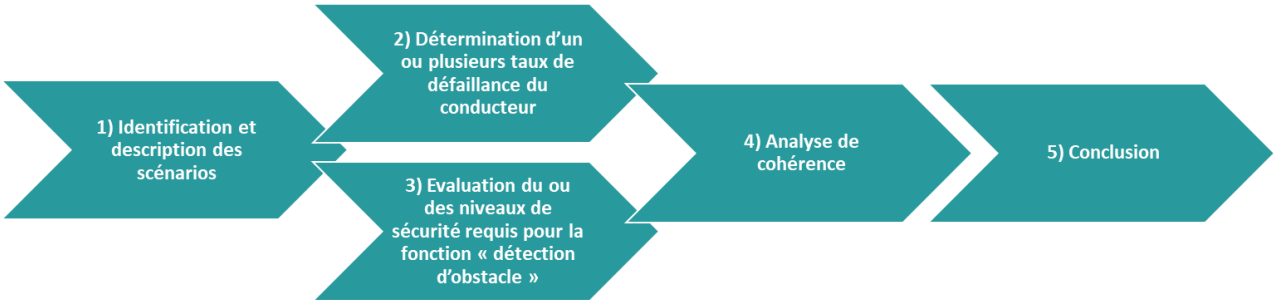

Fig. 1. Chronologie des étapes de la méthodologie proposée par SECTOR

A. Etape 1 : Identification et description des scénarios

L'objectif de cette première étape consiste à proposer une modélisation des scénarios identifiés dans une APR existante selon la taxonomie des scenarios définis par le SOTIF avec les « Conditions initiatrices (Triggering Conditions) » associés (environnementaux, humains, contextuels, techniques…) pouvant entrainer un comportement du train autonome potentiellement dangereux (cf. figure 2 de la norme ISO 21448 présentée ci-dessous). Cette modélisation permettra d'en déduire le niveau de risque de la fonction « détection d'obstacle » avec les actions de mise en sécurité qui en découlent.

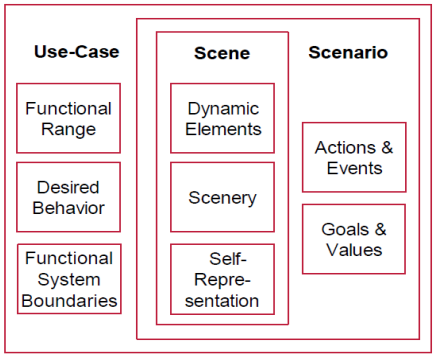

Fig. 2. Extrait de l'ISO 21448 – Taxonomy of use case, scene and scenario

Dans un premier temps, nous avons extrait à partir de l'Analyse Préliminaire des Risques réalisée, les situations de vie pouvant conduire à un événement de sécurité, associé à un dysfonctionnement de la fonction détection d'obstacle.

A partir de ces situations et de l'état de connaissance du groupe de travail réuni en ateliers pour cette étude, les scénarios ont été regroupés en séries, issus de la liste des dangers ferroviaires liés à la circulation des trains, à l'état de l'infrastructure ou à des éléments extérieurs, comme par exemple :

- Collision avec un piéton qui traverse les voies ;
- Collision d'un train avec un obstacle sur la voie, inerte (végétaux, engins, tracteurs..…), ou mobile (animaux, engins de travaux…) ;
- Collision avec un train (situation de nez-à-nez, rattrapage, prise en écharpe) ;
- Collision à la traversée de Passage à Niveau…

Les risques induits par les erreurs humaines des conducteurs, à des défaillances du système de signalisation, ou encore à une défaillance du matériel roulant sont considérés hors périmètre.

Dans chaque série, ont été identifié des scenarios structurés selon les paramètres suivants :

- Le descriptif du scenario ;
- Le cas d'usage dans lequel il se déroule, comme par exemple : en roulage basse vitesse pour s'arrêter en gare (décélération)…
- Le type d'infrastructure ferroviaire sur lequel le train roule, comme par exemple : en gare, en campagne, en tunnel…

Dans notre cas d'étude, nous allons nous attacher à décrire l'événement initiateur et la réaction du conducteur du train dans le cadre actuel des circulations et du système de sécurité ferroviaire, afin de pouvoir utiliser ensuite la méthode GAME (Globalement Au Moins Equivalent).

Les éléments suivants décrivent le scénario :

- L'événement initiateur qui peut entrainer un danger (ou trigger), avec les conditions environnementales et climatiques dans lequel se produit l'événement ;
- La scène en l'état actuel du système ferroviaire, avec la succession d'événements qui la décrivent, ou de réactions des éléments extérieurs ayant provoqué le danger.

Il était important d'intégrer dans cette analyse :

- Le comportement actuel d'un conducteur d'un train non autonome ;
- Et la scène attendue par le comportement souhaité (et spécifié) du train autonome.

Ceci dans le but de les comparer pour établir une correspondance entre l'étude relevant du SOTIF et l'étude relevant de l'évaluation quantitative du Facteur Humain (FH).

Dans un second temps, les situations fonctionnelles et logiques obtenues ont été étudiées pour déterminer les limitations du système et les événements déclencheurs potentiels qui pourraient déclencher un comportement potentiellement dangereux du système, en termes de SOTIF.

La norme ISO 21448 fournit un cadre d'argumentation général et des orientations sur les mesures visant à garantir la sécurité de la fonctionnalité prévue, qui est l'absence de risque déraisonnable dû à un danger causé par des insuffisances fonctionnelles, c'est-à-dire les insuffisances de la spécification de la fonctionnalité prévue au niveau du système de mobilité (en l'occurrence un véhicule), des insuffisances de spécification ou des insuffisances de performance dans la mise en œuvre des éléments.

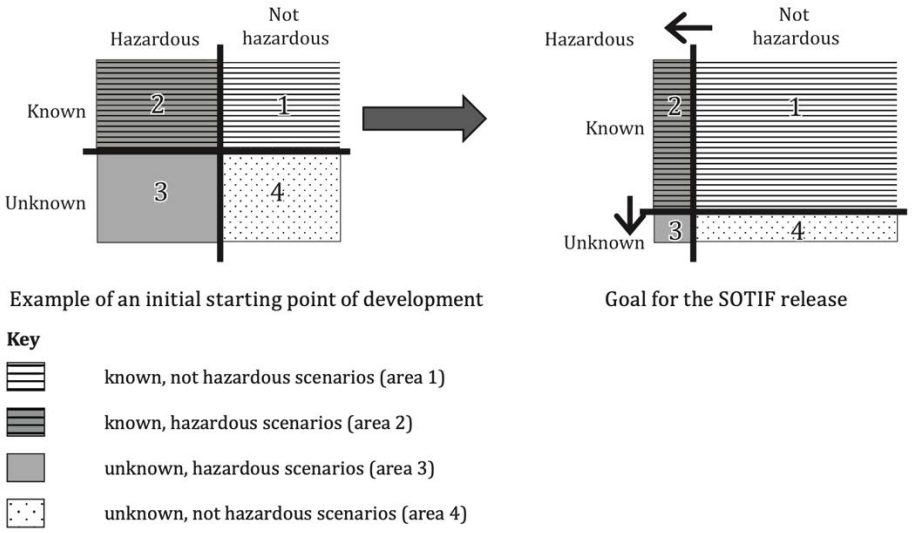

Fig. 3. Extrait de l'ISO 21448 : Alternative evolution of the scenario categories resulting from the ISO 21448 activities

L'évaluation des risques tient compte des limites de performance de la fonctionnalité prévue (ou spécifiée).

La méthode proposée décrit dans le cadre de ce même événement initiateur le comportement dangereux du train autonome dans le cas où le système de Détection d'Obstacle ne fonctionne pas/mal ou est en limite de performance. Nous obtenons ainsi la scène à risque :

- Avec le comportement dangereux du système de Détection d'Obstacle ;
- Induit soit par une défaillance soit par une limite de performance comme vue précédemment.

Comme le domaine de la sécurité ferroviaire ne dispose pas encore de démarche SOTIF, nous avons traité la fin de l'analyse par des méthodes classiques d'analyse de risque type APR ou HARA (Hazard Analysis and Risk Assessment), selon l'ISO 26262, en évaluant les événements redoutés en fonction d'un équivalent ASIL (Automotive SIL), afin de déterminer les niveaux de sécurité atteignables. En effet, une limite de performance peut provoquer le même effet ou dommage qu'une défaillance du même système.

B. Etape 2 : Détermination d'une ou plusieurs probabilités d'erreur humaine du conducteur pour la fonction « détection d'obstacle »

A partir de la cartographie de situations et scénarios identifiés en étape 1, l'objectif de cette étape n°2 est d'établir d'une ou plusieurs probabilités d'erreur humaine du conducteur vis-à-vis de la fonction « détection d'obstacle ».

Concernant ces méthodes d'évaluation de la fiabilité humaine, il est important de souligner que de nombreux modèles / méthodes existent présentant leurs spécificités et approches propres. Le premier objectif a été d'effectuer un benchmark de l'ensemble des méthodes existant dans l'état de l'art et de sélectionner celles qui seront les plus pertinentes dans le cadre de l'étude actuelle.

Les méthodes TESEO (Technica Empirica Stima Errori Operator) et HEART (Human Error Assessment and Reduction Technique) ont été sélectionnées pour leur pertinence dans le calcul de la fiabilité humaine pour ce projet.

1)La méthode HEART

Dans le cadre de cette méthode, les différentes phases suivantes ont été utilisées et suivies en adaptant la méthode HEART au projet pour déterminer la probabilité d'erreur humaine :

a) Phase 1 : Détemination de la tâche à considérer

La méthode HEART présente diverses tâches types avec des probabilités d'erreur humaine nominal, la première étape est de sélectionner parmi ces tâches celle qui reflète au mieux la tâche évaluée.

b) Phase 2 : Identifications des conditions conduisant aux erreurs

Il s'agit d'identifier les conditions applicables à notre cas de figure qui peuvent conduire à des erreurs humaines en utilisant une liste de 38 conditions conduisant aux erreurs EPCs (Error Producing Conditions) génériques de HEART. Pour ce faire, des entretiens ont été organisés avec des interlocuteurs du secteur ferroviaire dont un représentant des conducteurs, afin d'identifier les conditions applicables ainsi que leur poids estimé.

c) Phase 3 : Evaluation de la gravité des erreurs potentielles

Cette phase consiste à déterminer la pondération W_k estimée pour chaque EPC identifiée dans la phase 2 en utilisant une échelle de 0 à 1 qui reflète leur impact sur la tâche en question.

d) Phase 4 : Calcul de la probabilité d'échec de la tâche

Il s'agit d'utiliser les informations recueillies lors des phases précédentes pour calculer la probabilité d'échec de la tâche pour chaque scénario déterminé en utilisant une formule mathématique qui combine la probabilité d'erreur nominale et les pondérations des EPC.

$$P_{échec\_tâche} = P_{échec_{tâche_{nominale}} \times \prod_{k=1}^{N}[(EPC_k - 1) \times W_k + 1]} \quad (1)$$

Avec :

- $P_{échec_{tâche_{nominale}}}$: Probabilité d'échec de la tâche nominale, prédéfinie par la méthode HEART. On utilise la valeur associée à la tâche choisie dans la phase 1, qui reflète au mieux la tâche évaluée.
- EPC_k : Facteur prédéfini par la méthode HEART et associé à la $k^{ème}$ EPC identifiée dans la phase 2.
- W_k : Poids de la $k^{ème}$ condition identifiée dans la phase 3. Ce poids est choisi uniquement si la $k^{ème}$ condition conduit à l'erreur, et représente l'importance relative à cette condition en ajustant l'impact de chaque EPC_k en utilisant une échelle de 0 à 1.

2)Méthode TESEO

La méthode TESEO est une méthode de calcul de la probabilité d'erreur, elle utilise une approche basée sur cinq facteurs clés, K1, K2, K3, K4 et K5, pour estimer la probabilité d'erreur P(E). Ces facteurs incluent des éléments tels que la complexité du système, la fréquence d'utilisation, l'âge de l'équipement, les conditions environnementales et l'expérience de l'opérateur :

$$P(E) = K1 \times K2 \times K3 \times K4 \times K5 \quad (2)$$

Avec :

- K1 : type d'activité lié à la complexité de l'action ;
- K2 : facteur temporaire lié au temps disponible ;
- K3 : qualité de l'opérateur liée à la compétence de l'opérateur qui réalise la tâche ;
- K4 : facteur d'anxiété est un facteur émotionnel qui dépend de la gravité de la situation ;
- K5 : facteur ergonomique de l'environnement relatif aux conditions de travail.

Les valeurs pour chaque facteur sont déterminées à partir de tables prédéfinies empiriquement en fonction des caractéristiques supposées connues de la tâche et de l'opérateur humain.

3)Hypothèse générale

Il a été établi, de caractériser la défaillance de facteur humain comme suit dans le cadre de cette étude :

« *Absence de réaction dans un délai raisonnable de la part du conducteur suite à la présence d'un obstacle sur ou à proximité de la voie, dont la nature ou le comportement raisonnablement prévisible de celui-ci aurait nécessité une action du conducteur telle que : déclenchement d'un freinage d'urgence, actionnement du sifflet.* »

Ainsi, il est implicitement admis qu'une réaction du conducteur réalisée dans un délai raisonnable mais n'ayant pas permis d'éviter la collision n'est pas jugé comme faisant partie du domaine de l'erreur humaine. En effet, compte tenu des distances de freinage et des vitesses de circulation, il est admis qu'il est dans certains cas quasiment impossible d'éviter le danger.

Il est considéré qu'une réaction de déclenchement de freinage d'urgence demandée au conducteur en cas de présence d'un obstacle inopiné sur la voie en situation de nuit ou de conditions climatiques extrême (brouillard très dense) dans une phase de circulation autre qu'une marche à vue est jugée quasiment impossible à réaliser. Ainsi, le taux de défaillance de facteur humain considéré dans ce type de scénarios sera proche de 1.

C. Etape 3 : Evaluation du ou des niveaux de sécurité requis pour la fonction détection d'obstacle

Cette étape, réalisée indépendamment de l'étape n°2, a pour objectif d'évaluer les événements déclencheurs et des conditions prévisibles, identifiés dans les scénarios de l'étape 1, en tenant compte de la réponse du système à ces événements déclencheurs qui peut être considérée comme acceptable.

L'avantage d'une démarche de cotation où il n'y pas de distinction sur le type de cause initiale, SOTIF ou Défaillance, est de permettre une évaluation SIL. A cette étape, un nouveau chalenge se posait entre domaine ferroviaire et automobile : les cotations SIL et les cotations ASIL diffèrent beaucoup.

La démarche utilisée dans le secteur automobile, illustrée dans le schéma suivant, permet de comprendre l'influence de divers facteurs :

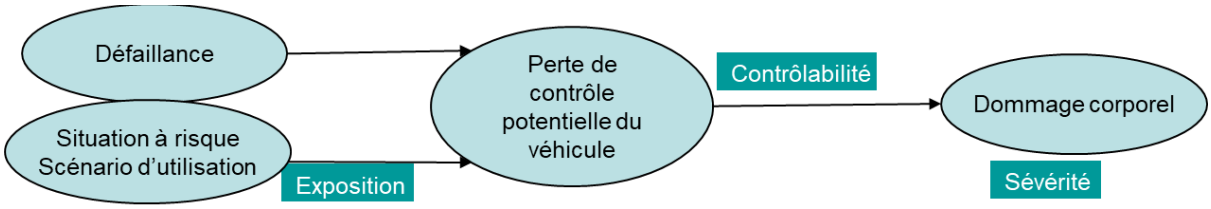

Fig. 4. Classification of hazardous events

Il s'agira de proposer des grilles de cotation des critères de « fréquence d'Exposition » au risque, de « Contrôlabilité » du risque, de « Sévérité » des dommages et enfin d'équivalents SIL.

Ces évaluations ont été effectuées par scénario de détection d'obstacle (établi à l'étape 1).

1)Exposition au risque

Dans la description de chaque scenario, les conditions d'apparition de la scène sont détaillées, en ne considérant **que les situations dimensionnantes et pouvant entrainer des dommages.**

Pour la cotation de l'Exposition, Il n'est pas trivial de comparer un véhicule automobile à un train. Nous avons donc proposé des équivalences qui correspondent à **l'expertise des conducteurs**. Nous obtenons cinq classes de l'exposition ferroviaire au risque que nous noterons EF0 à EF4, pouvant être considérées comme équivalentes aux classes E0 à E4 de l'ISO 26262.

A l'aide des experts du groupe de travail et du compte rendu d'une enquête statistique menée auprès d'un panel de conducteurs de train, nous avons attribué et fait valider chaque évaluation d'exposition (EF) au risque des scénarios définis.

2)Contrôlabilité

Dans l'ISO 26262, le troisième critère est la Contrôlabilité. Elle s'évalue de C0 (contrôlable en général) à C3 (difficilement contrôlable ou impossible).

La contrôlabilité est définie comme la capacité du conducteur ou des autres personnes à risque (par exemple, les piétons, les cyclistes, les passagers, les conducteurs d'autres véhicules) à éviter le dommage spécifié, en s'appuyant éventuellement sur des mesures externes.

Ainsi nous pouvons évaluer la Contrôlabilité qu'a le train autonome, en cas de défaillance ou de comportement dangereux en limite de performance de la fonction Détection d'Obstacle, pour éviter que le dommage ne se produise, en s'appuyant sur le système de signalisation, les communications entre train et surveillance déportée, émission de signal sonore automatique…

3)Sévérité

Après l'introduction des 2 critères E et C, l'évaluation du critère de Sévérité devait également faire l'objet d'une convergence entre normes du Ferroviaire et normes de l'Automobile.

Dans la norme ISO 26262, les 4 niveaux de gravité (Severity de 0 à 3) dépendent des dommages que le comportement dangereux du train autonome peut engendrer en termes de AIS (Abbreviated Injuries Scale) sur au moins une personne.

TABLE 1. CLASSES DE SEVERITE (SELON L'ISO 26262)

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Or le tableau de classification des niveaux de Gravité ferroviaires issus de l'EN 50126 les classe selon les principes suivants du plus faible au plus important :

TABLE 2. CRITERE GRAVITE SELON L'EN 50126

		Gravité (G)
		Conséquences pour les personnes ou l'environnement
Catastrophique	**IV**	Des morts et/ou plusieurs personnes gravement blessées et/ou des dommages majeurs pour l'environnement
Critique	**III**	Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement
Marginal	**II**	Blessures légères et/ou menace grave pour l'environnement
Insignifiant	**I**	Éventuellement une personne légèrement blessée

Ainsi, afin de nous affranchir de cette problématique, nous avons proposé l'hypothèse suivante en vue d'obtenir une passerelle conservative entre les 2 grilles : **Si la GRAVITE de type ferroviaire serait CRITIQUE (III, 1 mort) ou CATASTROPHIQUE (IV, plusieurs morts), nous appliquerons une SEVERITE de type automobile maximum à S3 (au moins 1 mort).**

4)Equivalence entre ASIL et SIL

La démarche utilisée dans le secteur automobile, illustrée dans le schéma suivant, permet de comprendre l'influence de divers facteurs pour établir un niveau d'ASIL (Automotive SIL) :

TABLE 3. TABLE DES ASIL

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

« QM ou Quality Management » se réfère au niveau de gestion de la qualité sans exigence particulière de sécurité, et les niveaux « A », « B », « C » et « D » indiquent différents niveaux de criticité en sécurité fonctionnelle dans l'industrie automobile, avec « A » représentant le niveau de sécurité fonctionnelle le plus bas et « D » le plus élevé.

Le tableau suivant donne des équivalences entre les différentes normes dérivées de l'IEC 61508 sur les niveaux SIL. Nous l'utiliserons pour faire convertir les ASIL et SIL ferroviaires.

TABLE 4. TABLE DE CONVERSION SIL/ASIL

Generic (IEC 61508)	**(SIL 0)**	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
Household (IEC 60730)	Class A	Class B		Class C	--
Automotive (ISO 26262)	QM	ASIL A	ASIL B / ASIL C	ASIL D	--
Medical (IEC 62304)	Class A	Class B		Class C	
Civil Aerospace (DO-178C)	Level E	Level D	Level C	Level B	Level A
Rail (EN 5012x)	(SIL 0)	SIL 1	SIL 2	SIL 3	SIL 4

Avec SIL 1 étant le moins critique et SIL 4 étant le plus critique en termes de sécurité fonctionnelle.

Cette étape a été réalisée par workshop de travail en brainstorming. Les 34 scenarios retenus ont ainsi été évalués en SIL ferroviaire, tout en appliquant notre méthode adaptée de détermination des ASIL aux scénarios d'un train autonome.

D. Etape 4 : Analyse de cohérence et proposition de pistes pour réduire le risque

1)Spécification de niveau de SIL par approche GAME conducteur

L'approche de spécification par la méthode Globalement Au Moins Equivalent (GAME) consisterait à spécifier des niveaux de sécurité fonctionnels (niveau de SIL - Safety Integrity Level au sens de l'EN 50126) au futur système autonome de détection d'obstacle en se basant sur le niveau de performance équivalent réalisé aujourd'hui par un conducteur humain, en prenant en compte la valeur la plus conservative parmi les 2 méthodes TESEO et HEART.

Cependant, l'approche de l'étape 2 évalue une probabilité d'erreur humaine « à la demande » (qui est l'équivalent du PFD selon la définition de la norme NF EN 61508), c'est-à-dire une probabilité d'erreur ponctuelle à chaque survenue d'une situation relative à un obstacle sur la voie.

Or le contexte ferroviaire couvert par la norme NF EN 50126-2 considère des valeurs de TFFR (Tolerable Functional Failure Rate) qui est l'équivalent du PFH selon la norme NF EN 61508 :

TABLE 5. EXTRAIT DE L'EN 50162 - TABLE 2 - SIL QUANTITATIVE AND QUALITATIVE MEASURES

TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	

Ainsi, par souci de cohérence avec la norme applicable du secteur ferroviaire, il convient d'effectuer une conversion des résultats quantitatifs obtenus à l'étape 2 vers le TFFR. Une première approximation proposée dans ce cadre de l'étude a été la suivante :

$$TFFR \cong P(E) \times F \quad (3)$$

Avec :

P(E) : La probabilité d'erreur humaine la plus conservatrice à la survenue d'une situation dangereuse ;

F : Fréquence d'occurrence de la situation par heure de roulage dans un cas d'usage.

Cette analyse menée conjointement avec un panel d'experts dont des conducteurs de train a permis de déterminer que dans la grande majorité des scénarios décrits dans l'étape 2, dans le cas de conditions environnementales complexes, il est impossible d'éviter l'obstacle. La performance du conducteur n'est donc pas évaluée en niveau de SIL (noté pour l'étude **SIL 0 ou QM**).

Pour les autres scénarios, il est intéressant de noter que la performance humaine est très élevée, avec un niveau de SIL équivalent élevé. Ces scénarios présentent les particularités suivantes : roulage en marche à vue ou de conducteur alerté de la présence d'un objet à proximité, rendant son niveau d'attention et donc sa performance maximale. De plus, il s'agit de scénarios à la survenue extrêmement rare ce qui se traduit par une conversion en une valeur très faible de TFFR.

Le même constat s'applique pour le scénario présentant une performance humaine intermédiaire, il présente les particularités suivantes : roulage en basse vitesse pour s'arrêter en gare, en décélération, avec une bonne visibilité et donc une situation favorable qui permet au conducteur d'avoir une excellente réactivité et de disposer du temps nécessaire pour freiner à temps.

Les autres scénarios présentent des niveaux de SIL équivalent inférieurs à SIL 1 ce qui n'est pas surprenant compte tenu des différents facteurs impactant la fiabilité de réaction du conducteur (temps de réaction, stress, conditions de visibilité…) mais également des facteurs venant pénaliser la conversion en TFFR, c'est-à-dire la fréquence de survenue de ces situations : plus la fréquence est élevée, plus la conversion en TFFR présentera un résultat élevé.

2)Etude comparative des deux approches

Les résultats obtenus mettent en évidence des écarts significatifs entre les niveaux SIL/ASIL issus de l'évaluation du facteur humain de l'étape 2 et ceux évalués à l'étape 3.

Ces écarts sont de 2 natures et doivent être interprétés selon les cas :

1) Le niveau de SIL atteint par l'étape 2 est supérieur au SIL requis de l'étape 3 : cette situation ne se présente que pour un seul scénario et peut être expliqué par le fait que, dans cette situation en particulier, les capacités humaines peuvent dépasser les exigences attendues de par l'aspect favorable des conditions permettant un haut niveau de fiabilité humaine dans une situation qui ne présente pas de risque particulièrement critique.

2) Le niveau de SIL atteint par l'étape 2 est inférieur au SIL requis de l'étape 3 : cette situation se présente pour une majorité de scénarios. Ces cas permettront de souligner l'apport d'une fonction automatisée de détection d'obstacle par rapport au conducteur seul, sous réserve que la fonction automatisée respecte les niveaux de SIL spécifiés par l'étape 3.

E. Etape 5 : Conclusion

L'étude permet d'apporter entre autres les 2 résultats suivants :

3) La proposition d'un cadre méthodologique ajusté au contexte ferroviaire train autonome, basé sur les normes ISO 21448 (SOTIF) et ISO 26262 qui sont utilisées dans le cadre de l'autonomisation de systèmes de conduite dans le secteur automobile ;

4) Un comparatif d'écart entre les performances actuelles et celles spécifiées avec ce cadre méthodologique qui vont pouvoir servir de base à la justification de l'apport de l'autonomisation de la fonction détection d'obstacle.

Cependant, il est important de souligner les limites potentielles de ces apports :

1) L'évaluation du facteur humain et sa conversion en équivalent TFFR se basent sur de nombreuses hypothèses présentant un fort niveau de variabilité et d'incertitudes ;

2) L'ajustement de la méthode au contexte ferroviaire, en particulier des grilles de cotation, est une proposition méthodologique qui peut être enrichie, compte tenu de l'absence de norme en la matière applicable directement au domaine ferroviaire.

Pour conclure, cette étude a permis d'établir une première cartographie des performances humaines du conducteur dans son rôle d'assurer la sécurité des usagers dans tous les cas de figure possibles liés à la présence d'un obstacle sur les voies, ce qui pourrait notamment permettre de spécifier des niveaux de sécurité fonctionnelles à un système autonome selon une logique GAME. La comparaison des résultats obtenus avec les méthodes d'évaluation des risques dans l'absolu issues des normes de sécurité fonctionnelles donne des perspectives intéressantes en vue de créer des spécifications de sécurité cohérentes et applicables pour l'ensemble des fonctions automatisables du transport par rail.

REMERCIEMENTS

Nous exprimons notre gratitude à tous les collaborateurs de SECTOR GROUP qui ont contribué à ce projet pour leur implication ayant permis de réaliser cet article. Nous souhaitons plus particulièrement remercier M. Jean-François BARBET, ex-président fondateur de SECTOR, pour sa supervision. Enfin, nous remercions l'ensemble des membres du comité de programme LM24 pour nous avoir offert la possibilité de présenter nos travaux.

REFERENCES

[1]. ISO/PAS 21448 : 2019 « Véhicules routiers - Sécurité de la fonction attendue »
[2]. Norme ISO 26262 : 2018 « Véhicules routiers - Sécurité fonctionnelle »
[3]. SECTOR : projet confidentiel de sécurisation de systèmes d'un futur train autonome