Argumentaire de sécurité graphique pour l'assurance de sécurité des trains autonomes

Mohammed Chelouati, Boussif Abderraouf, Julie Beugin, El Miloudi El Koursi

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

Argumentaire de sécurité graphique pour l'assurance de sécurité des trains autonomes

Graphical safety argumentation for safety assurance of autonomous trains

CHELOUATI Mohammed
Institut de Recherche Technologiques Railenium
180 rue Joseph-Louis Lagrange, Valenciennes, F-559300, France
mohammed.chelouati@railenium.eu

BOUSSIF Abderraouf
Institut de Recherche Technologiques Railenium
180 rue Joseph-Louis Lagrange, Valenciennes, F-559300, France
abderraouf.boussif@railenium.eu

BEUGIN Julie
COSYS-ESTAS Université Gustave Eiffel,
20 rue Élisée Reclus, Villeneuve d'Ascq, F-59650, France.
julie.beugin@univ-eiffel.fr

EL KOURSI El-Miloudi
COSYS-ESTAS Université Gustave Eiffel,
20 rue Élisée Reclus, Villeneuve d'Ascq, F-59650, France
el-miloudi.el-koursi@univ-eiffel.fr

Résumé — L'introduction du concept d'autonomie dans le secteur ferroviaire pose de nombreux défis, notamment en termes de sécurité. En effet, la gestion des aspects sécuritaires liés à l'utilisation des systèmes d'Intelligence Artificielle (IA), et de manière générale, à l'utilisation des différents sous-systèmes d'un train autonome sont deux verrous scientifiques à traiter. Dans le premier cas, il n'existe pas dans les normes et règlements ferroviaires Européens actuels de moyens permettant d'appréhender la sécurité des systèmes d'apprentissage. Dans le deuxième cas, appliquer les méthodes et outils conventionnels d'assurance de sécurité pour élaborer l'argumentation de sécurité dans les Dossiers de Sécurité (DS) est défiant en raison de la complexité des systèmes autonomes. Ce papier se focalise sur le deuxième point en partant du constat que les formats textuels employés dans les DS freinent la mise en place d'une argumentation claire, précise et suffisante associée aux objectifs et preuves de sécurité. De nombreuses méthodes et outils graphiques ont été développés récemment pour présenter de manière plus formalisée les argumentaires de sécurité. La méthode « Goal Stucturing Notation » (GSN – Notation de structuration des objectifs) s'avère être la plus prometteuse pour répondre à cette problématique. Pour cette raison, après avoir expliqué les atouts de la GSN, nous proposons dans cette communication une approche d'assurance de sécurité pour le train autonome fondée sur cette méthode.

Mots-clefs — Sécurité ferroviaire, argumentation de sécurité, train autonome, dossier de sécurité, Goal Structuring Notation

Abstract **—** The introduction of autonomy in railways raises several challenges related to the safety assurance process and activities. Among these challenges: the qualification/certification of Artificial Intelligence (IA) based systems, and the management of Safety Cases arguments and evidence. The former one is related to the fact that European railway standards and regulations do not yet consider learning systems in the safety assurance process. The latter challenge is related to the complexity of argument and evidence management in safety cases that the autonomous train poses. This paper focus on the second challenge, particularly, issues related to the conventional textual practices through which argument and evidence were structured and communicated. Several graphical languages and methods were developed to deal with this problem, such as, Goal Structuring Notation (GSN). To address this issue, several graphical methodologies, such as Goal Structuring Notation (GSN), were created. In this work, we propose a safety assurance framework for the autonomous train with GSN-based safety case.

Keywords — Railway safety, safety argumentation, autonomous train, safety case, Goal Structuring Notation

I. INTRODUCTION

Le développement des trains autonomes est aujourd'hui en plein essor. Les acteurs ferroviaires y voient en effet plusieurs atouts découlant de l'optimisation de la conduite des véhicules : service de transport amélioré en termes de ponctualité, d'efficacité de circulation et de sécurité. S'ajoute à cela la réduction de la consommation d'énergie pour un train plus respectueux de l'environnement. En France, la Société Nationale des Chemin de Fer (SNCF) a lancé en 2016 un programme de recherches et développement appelé Tech4Rail pour établir les fondamentaux des systèmes ferroviaires du futur ainsi que le déploiement sûr des trains autonomes. Pour ce dernier objectif, trois projets de grande envergure ont démarré en partenariat avec l'Institut de Recherches

Technologiques Railenium[1] et d'autres partenaires industriels et académiques : *(i)* Train Fret Autonome (TFA), *(ii)* Train Autonome Service Voyageurs (TASV) et *(iii)* Train Téléconduit (TC-Rail). Les travaux présentés dans ce papier s'inscrivent dans le cadre du projet TASV.

D'un point de vue sécurité, l'enjeu principal pour le train autonome est de fonctionner tout en assurant un niveau de sécurité/risque acceptable dans l'ensemble des conditions opérationnelles. Pour cela, la démarche d'assurance de sécurité des trains autonomes doit s'appuyer sur un processus de démonstration de sécurité mis en œuvre tout le long du cycle de vie du système. En effet, les activités de démonstration de sécurité permettent de montrer la conformité aux exigences de sécurité des textes réglementaires (normes et directives européennes) ce qui permet alors d'obtenir une certification ou une autorisation de mise en service. La conformité aux normes ferroviaires est prouvée à l'aide d'arguments et de preuves de sécurité documentés et structurés dans un « Dossier de Sécurité » (DS) [1]. Récemment de nouvelles méthodes graphiques ont été développées pour structurer les éléments du DS, comme la méthode Goal Structuring Notation (GSN – Notation de structuration des objectifs) [2]. Ces méthodes représentent une alternative plus pertinente au format textuel de la documentation qui est aujourd'hui communément adopté. Les aspects graphique et visuel de ces méthodes permettent en fait d'améliorer la présentation et la compréhension des arguments et des preuves de sécurité [3]. Le développement actuel des trains autonomes constitue une réelle opportunité quant à l'usage de méthodes nouvelles et efficaces en termes de structuration de preuves de sécurité par rapport aux méthodes textuelles classiques. Dans cette communication, nous discuterons d'abord de l'utilisation de l'argumentaire de sécurité graphique (méthode GSN) pour la démonstration de sécurité dans le domaine ferroviaire. Nous proposerons ensuite un modèle d'argumentation de sécurité GSN pour l'assurance des objectifs de sécurité globaux (i.e., de haut niveau) pour le train autonome. Le modèle proposé a pour but de faciliter la gestion et la documentation des éléments liés à l'argumentation de sécurité dans un DS pour le train autonome et de fournir une meilleure visibilité et traçabilité de ces éléments pour les différents acteurs concernés.

La structure de ce papier est la suivante : dans la section 2, nous définissons ce qu'est un DS, son rôle, et son importance notamment dans le cadre de la sécurité ferroviaire. Dans la section 3, nous passons en revue quelques démarches existantes de construction de DS utilisant la GSN à la fois dans les domaines des véhicules autonomes et ferroviaire, ceci afin de montrer les atouts de cette méthode. En section 4, nous proposons une approche d'assurance de sécurité pour le train autonome fondée sur la GSN. Finalement, la dernière section conclue cette communication et apporte quelques perspectives.

II. DOSSIER DE SÉCURITÉ

Dans cette section, nous montrons en quoi le rôle des DS est important dans le processus de démonstration de sécurité des systèmes critiques, en particulier les systèmes contrôle-commande ferroviaires.

Au cours des dernières décennies, le concept de DS s'est largement étendu à plusieurs secteurs, comme au nucléaire, à l'aviation, à la défense ainsi qu'au secteur ferroviaire. Dans le secteur ferroviaire Européen, le DS est entré en vigueur par la British Standard, sous le nom de Règlements Ferroviaires (the Railway Regulations) en 1994 [4], [5]. Le concept de DS a été concrétisé plus tard dans la norme Européenne EN 50129 [6] en 2003. Selon la même norme (version 2018), un DS est *« une démonstration documentée que le produit (par exemple, un système, un sous-système ou un équipement) satisfait les exigences de sécurité spécifiées »*. Cette définition remonte à l'objectif initial de la norme EN 50129 visant l'acceptation des systèmes électroniques liés à la sécurité dans le domaine de la signalisation ferroviaire. Selon [7], le DS est *« un ensemble de preuves documentées qui fournissent un argument convaincant et valide selon lequel un système est suffisamment sûr pour une application donnée dans un environnement donné »*. Ces définitions soulignent les éléments clés qu'un DS doit fournir pour atteindre son objectif. Ces éléments clés se résument en trois aspects : *(i)* les *exigences* et les *objectifs* de sécurité, *(ii)* les *preuves* de sécurité et *(iii)* les *arguments* de sécurité. La norme EN 50129 est également associée à un guide pour l'établissement des DS et montre que ce processus commence par l'identification des objectifs de sécurité de haut niveau, puis se poursuit par l'emploi de méthodes et techniques permettant de justifier les activités tout au long du cycle de vie.

Les arguments de sécurité sont généralement utilisés pour décrire la relation entre les objectifs et les preuves de sécurité, et ont été historiquement présentés sous forme de textes narratifs. Malheureusement, la manière textuelle d'exprimer les arguments et les preuves de sécurité devienne de plus en plus complexe et génère des problèmes d'incompréhension, de clarté, et de désordre [1], [8]. Le premier problème se manifeste sur la qualité du texte utilisé pour exprimer un argument. En effet, les capacités de rédaction peuvent affecter considérablement la qualité des arguments malgré les bonnes pratiques d'ingénierie. Le deuxième problème est lié à la traçabilité des arguments ainsi que la relation entre les objectifs de sécurité de haut-niveau et les preuves associées de bas-niveau. S'ajoutant à cela le nombre de documents et de rapports qu'un DS contient habituellement, cela rend sa gestion problématique.

III. GOAL STRUCTURING NOTATION

Les problèmes liés à la représentation textuelle des arguments et des preuves a conduit à la création de nouvelles méthodes et outils graphiques permettant une gestion plus fluide de ces éléments. Parmi les outils graphiques existants, nous avons choisi de présenter la méthode Goal Structuring Notation (GSN). Le passage en revue de quelques démarches existantes de construction de DS utilisant la GSN dans les domaines des véhicules autonomes et ferroviaire permet de monter l'intérêt de cette approche.

A. Définition

La GSN est une technique structurée créée spécialement pour gérer la présentation des arguments d'une manière claire dans un DS. Les éléments clés d'une argumentation de sécurité (objectifs, stratégies, preuves/solutions et contextes)

[1] http://railenium.eu

sont exprimés à l'aide de la GSN [2], [3], [9]–[11]au travers des symboles présentés dans la Figure 1.

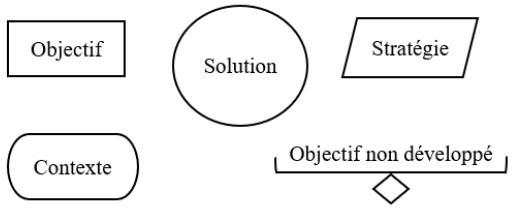

Fig. 1. Les symboles principaux de la GSN

Les symboles principaux de la GSN sont : (1) l'*objectif* d'assurance ou la *revendication*, (2) la *preuve* que l'objectif a été atteint, et (3) l'*argument* liant la preuve à l'objectif. La liaison de ces éléments GSN dans un réseau est appelée « structure d'objectifs ». Des symboles additionnels peuvent être utilisés sur des structures GSN, notamment des stratégies, hypothèses, justifications et contextes, etc. Selon le standard GSN [11], les structures d'objectifs GSN sont généralement implémentées d'une manière descendante (Top-Down) où les objectifs de haut-niveau sont décomposés en sous-objectifs jusqu'au niveau le plus bas. Toutefois, ces structures peuvent également être développées d'une manière ascendante (Bottom-Up). Le même standard fournit aussi d'autres extensions permettant un développement plus détaillé des arguments complexes de divers types d'assurance.

B. La GSN dans le domaine ferroviaire

La GSN est la méthode graphique la plus utilisée dans les domaines critiques de sécurité pour l'argumentation graphique de la démonstration de sécurité ; ceci grâce à ses avantages en termes de traçabilité, de clarté et d'explicabilité. En effet, la GSN est un langage générique qui permet de structurer les arguments dans n'importe quel domaine [12]. Dans ce cadre, nous présentons un succinct état de l'art impliquant l'argumentation de sécurité des DS construite à partir de la GSN dans les domaines ferroviaire et des véhicules autonomes.

Le projet INESS (Integrated European Signalling System)[2] est un des projets de recherche européens qui a adopté la méthode GSN pour structurer l'argumentation de sécurité des DS. Ce projet avait comme objectif de réduire le coût et le temps associés aux processus d'établissement des DS en évitant les redondances non nécessaires [13]. De plus, d'autres travaux ont proposé un module réutilisable fondé sur la GSN en conformité avec les normes de sécurité ferroviaires afin d'améliorer la traçabilité, et en l'occurrence, la qualité du DS [14]. Dans le but d'évaluer le niveau de confiance attribué aux arguments du DS, les auteurs [15], [16] ont développé une série de travaux pertinents s'appuyant sur la théorie Dempster-Shafer.

Le tableau 1 présente quelques travaux pertinents sur l'assurance de sécurité fondé sur la GSN dans le ferroviaire, en montrant quelques caractéristiques comme la conformité aux normes, le niveau traité par le travail ainsi que les applications associées.

C. La GSN pour les véhicules autonomes

Contrairement à l'utilisation « modeste » de la GSN dans le domaine ferroviaire, l'argumentation fondée sur la GSN est largement utilisée pour guider l'assurance de sécurité des systèmes autonomes, allant des voitures autonomes jusqu'aux drones autonomes. Des contributions précurseurs ont été présentés dans [17] où l'auteur a discuté la différence entre une approche traditionnelle (i.e., statique) et une approche nouvelle (i.e., dynamique) d'évaluation des risques d'un système autonome adoptant la GSN. Cette approche est aussi utilisée pour la traçabilité des exigences de sécurité qui est une activité clé permettant leur suivi tout au long du cycle de vie du système. Dans [18], l'approche proposée consiste à spécifier des exigences de haut-niveau pour ensuite les décomposer progressivement jusqu'à atteindre le niveau le plus bas d'exigences. Ce processus se révèle en fait être un moyen efficace pour argumenter l'exhaustivité et le respect des exigences. Une autre contribution dans [19] consiste à créer un motif GSN pour instancier le processus de d'assurance sécurité. Cette démarche est illustrée à l'aide du concept de «conscience de la situation » (*Situation Awareness*) dédié à l'analyse des activités opérationnelles [20]. Ce motif permet la réutilisation de la structure d'argumentation pour des systèmes similaires. Dans le contexte des voitures autonomes, les travaux proposés dans [22], [23] ont mené à une création d'un ensemble de motifs modulaires réutilisables de DS à l'aide de la GSN. Les auteurs de [24] ont présenté une structuration du contenu du DS en conformité avec la norme automobile ISO 26262. Dans [25], les auteurs ont proposé un processus de génération automatique des modules GSN en respectant le développement et l'évaluation de modèles (à l'aide du langage de modélisation SysML). Dans la même idée, les auteurs de [26] ont utilisé les motifs GSN afin de combler les gaps en phase d'exploitation liés à la gestion du fonctionnement auto-adaptatif d'un robot.

Le programme AAIP (*Assuring Autonomy International Program*)[3] a proposé un guide pratique pour le développement des systèmes autonomes sûrs de fonctionnement. Un motif de DS y est présenté pour illustrer le modèle proposé qui peut être atteint. Un guide sur l'assurance de sécurité liée à l'apprentissage automatique (*Machine Learning*) dans les systèmes autonomes appelé AMLAS (*Assurance of Machine Learning in Autonomous Systems*) est également fourni par l'AAIP [27]. Un ensemble de structures de motifs GSN a aussi été présenté pour pouvoir justifier et appuyer le développement et le déploiement sûr des composants dotés d'apprentissage automatique et intégrés aux systèmes autonomes.

[2] http://www.iness.eu/

[3] https://www.york.ac.uk/assuring-autonomy

D. Discussion

L'introduction de l'autonomie dans le domaine ferroviaire nécessite de revoir les méthodes de sécurité utilisées ainsi que les processus relatifs à constitution des DS. EN effet l'introduction du train autonome relève un problème majeur lié à sa conception et son intégration sûre dans le système ferroviaire global. Dans le règlement européen ferroviaire CSM-RA (*Common Safety Methods - Risk Assessment*, méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques) [28] indique le processus de démonstration de sécurité à suivre si un nouveau système représente un changement significatif dans le système ferroviaire global. Cette contribution considère que le train autonome représente un changement significatif par rapport aux trains conventionnels comme un système *entièrement nouveau* (concept de *changement significatif* dans la CSM-RA) et de mener le processus de démonstration de sécurité à partir d'une page blanche. La deuxième est de considérer que le train autonome n'entraine pas de *changement significatif* sur les trains conventionnels. Par conséquent, les activités de sécurité doivent se focaliser sur les écarts en termes de risques entre le système de conduite autonome (ADS) qui remplace le rôle du conducteur et les systèmes existants.

Dans nos travaux, nous supposons que le train autonome représente un changement significatif pour le train conventionnel. Cette hypothèse permet de se conformer au processus décrit dans le règlement européen CSM-RA. Dès lors, pour l'élaboration de l'argumentation de sécurité des sous-systèmes changeant significativement, en particulier l'ADS, la GSN permet une intégration efficace de cette argumentation dans le processus global de démonstration de sécurité. Ainsi l'approche proposée pour l'assurance de sécurité des trains autonomes à l'aide de la GSN est présentée dans la section suivante.

IV. Approche proposée

La démonstration de sécurité des trains autonomes nécessite un ensemble d'activités de sécurité menés sur trois niveaux hiérarchiques du système global (voir Figure 3) : *(i) au niveau du système global, (ii) au niveau des composants dotés d'IA* (ex, les modules de perception et de prise de décision) et *(iii) au niveau des logiciels d'IA* (ex, logiciel de détection d'obstacles). Ces activités de sécurité doivent être établis en parallèle avec le processus de développement du cycle de vie du système global.

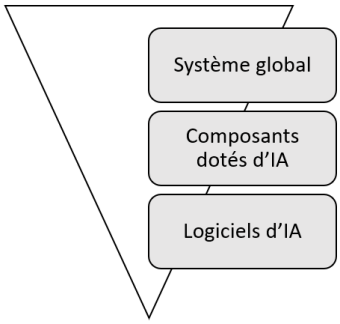

Fig. 2. Niveaux héararchique du système « train autonome ».

1) Niveau « système global » : l'objectif de sécurité à ce niveau est d'« *assurer que le train autonome est sûr de fonctionner pendant son exploitation dans son environnement spécifié* ». Cet objectif devra être atteint en assurant que l'ensemble des risques sont identifiés, évalués et contrôlés ou bien réduits à un niveau acceptable. À ce niveau, la norme européenne EN 50126 spécifie les activités et les processus de sécurité à établir ainsi que les preuves associées en commençant par la définition du système jusqu'à la spécification des exigences de sécurité.

2) Niveau « systèmes intégrant de l'IA » : à ce niveau, l'objectif de sécurité est d'« *assurer que les systèmes intégrant une composante logicielle d'apprentissage (i.e., algorithme d'IA) respectent les exigences de sécurité qui leur ont été alloués à partir des exigences de plus haut niveau* ». Les activités de sécurité à ce niveau consistent en : *(i)* la spécification de l'architecture du composant (matérielle et logicielle) et *(ii)* l'analyse dysfonctionnelle des dangers au niveau du composant.

Tableau 1 : quelques applications de la GSN dans le domaine ferroviaire

Références	[14]	[29]	[30]	[15]	[31]	[32]
Concepts théorique	-	✓	✓	-	-	-
Processus	✓	-	-	-	✓	✓
Produit	-	-	-	✓	✓	✓
Normes & directives	EN 50126	EN 50129	EN 50129 ISO 26262	EN 50128 EN 50129	-	EMC Directive (2014/30/EU)
Niveau système	✓	✓	✓	✓	✓	✓
Niveau sous-système	-	-	-	✓	-	✓
Applications	Modèle de traçabilité d'information	-	Outil MDSafeCer	Système de protection de glissière	Controlleur des portes	Equipement EMC (compatibilité électromagnétique)

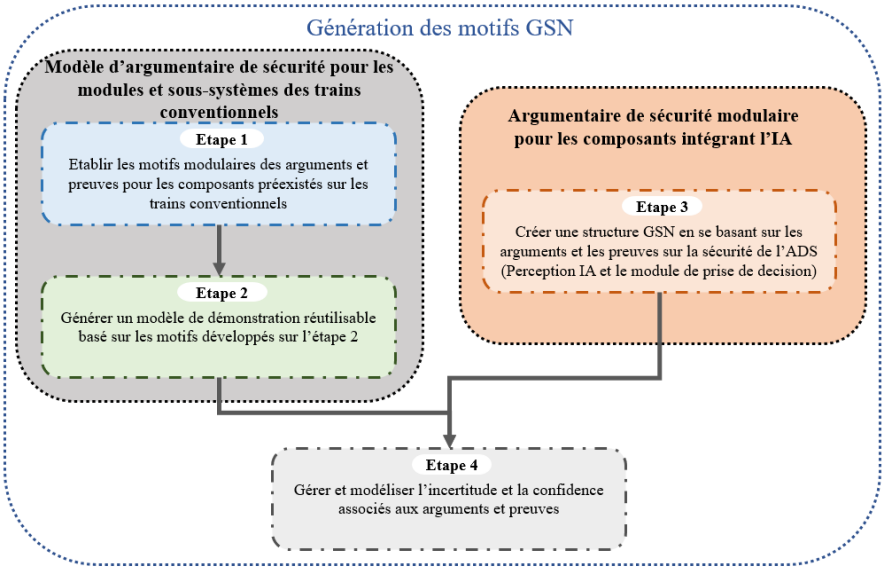

Fig. 3. les étapes essentielles d'établissement des motifs GSN d'argumentation de sécurité

Dans le cas des trains autonomes, « la sécurité de la fonction attendue » est un concept supplémentaire/complémentaire à prendre en compte durant l'analyse dysfonctionnelle. Il provient de la norme SOTIF connue dans le domaine automobile [29].

3) Niveau « algorithme d'apprentissage » : à ce niveau, un modèle ou algorithme d'apprentissage est à déployer sur le composant doté d'IA. L'objectif de sécurité est d'«*assurer que l'algorithme d'IA implémenté respecte les exigences de sécurité allouées à partir du niveau supérieur* ». Atteindre cet objectif est un défi déterminant d'autant plus que les normes du logiciels ferroviaires actuelles, les méthodes d'ingénierie et les règlements ne traitent pas encore cet aspect d'un point de vue sécurité logicielle.

Dans le but d'élaborer une démonstration de sécurité pour le train autonome, les motifs d'arguments basés sur la GSN doivent être établis en tenant compte de l'ensemble des activités de sécurité susmentionnées (en plus des activités de sécurité conventionnelles présentées dans la norme EN 50126).

L'approche proposée dans ce papier consiste à définir les étapes à suivre pour élaborer le processus de démonstration de sécurité à l'aide de la méthode GSN (durant la phase de conception), tout en s'appuyant sur l'évaluation des dangers identifiés durant la phase de développement. Les étapes que nous avons définies sont les suivantes :

Étape 1 : le train autonome inclus forcément un ensemble de modules préexistants sur les trains conventionnels qui seront en interaction avec le système autonome de conduite. Les motifs d'arguments et de preuves de ces modules doivent être repris (à partir de précédente démonstration de sécurité) et représentés en modèles GSN.

Étape 2 : l'objectif de cette étape consiste à créer un modèle global réutilisable de l'argumentation de sécurité dans du DS en se basant sur les motifs modulaires d'arguments et de preuves générés durant l'étape 1. Ce modèle doit contenir une structure GSN justifiant le niveau de sécurité global et démontrer clairement l'intégration sûre des composants existants sur les trains conventionnels.

Étape 3 : cette étape se concentre sur la création d'un module GSN pour présenter les arguments de sécurité relatifs au système ADS. Ce module doit être intégrable sur le modèle GSN globale élaborés à l'étape 3.

Étape 4 : finalement, cette étape détermine et évalue le niveau de confiance attribué aux arguments de sécurité présentés sur le DS. En effet cette étape a comme objectif la modélisation de l'incertitude.

La Figure 4 illustre un exemple de structure d'argumentation de sécurité à l'aide de la GSN. L'exemple montre la décomposition des objectifs de sécurité de haut niveau jusqu'aux preuves et recommandations des normes ferroviaires associées. L'exemple montre les avantages de la GSN en termes de traçabilité du processus de décomposition des objectifs en sous-objectifs, il permet également de visualiser les stratégies et les contextes dans lesquelles l'argumentation est structurée. L'*objectif* global **G1** dans la structure GSN est d'assurer que le train autonome est acceptablement sûr de fonctionnement. Cet *objectif* est traité dans trois *contextes* associés (**C1**, **C2** et **C3**). L'*objectif* global **G1** est appuyé également par une *stratégie* d'argumentation du déploiement du train autonome. Ensuite, l'*objectif* global est décomposé en plusieurs sous-objectifs (**G2**, **G3**, etc.). Parmi ces *sous-objectifs*, **G2** est relatif à l'assurance de sécurité de l'ADS, tout en tenant compte des *contextes* **C1** et **C2** liés aux pannes fonctionnelles et la liste des dangers identifiés pour l'ADS respectivement. Le *sous-objectif* **G2** est décomposé à son tour en *sous-objectifs* jusqu'au bas niveau des *preuves et recommandations* de sécurité qui montrent que les *objectifs* et les *sous-objectifs* sont atteints. Ces *preuves* sont présentées sur la structure par **Sn1** et **Sn2**.

L'approche d'assurance de sécurité proposée est basée sur l'hypothèse que les dangers et leurs mesures de mitigation associées sont identifiés durant la phase de développement du système. Néanmoins, le transfert de la responsabilité des conducteurs vers le système ADS doit être faite en assurant

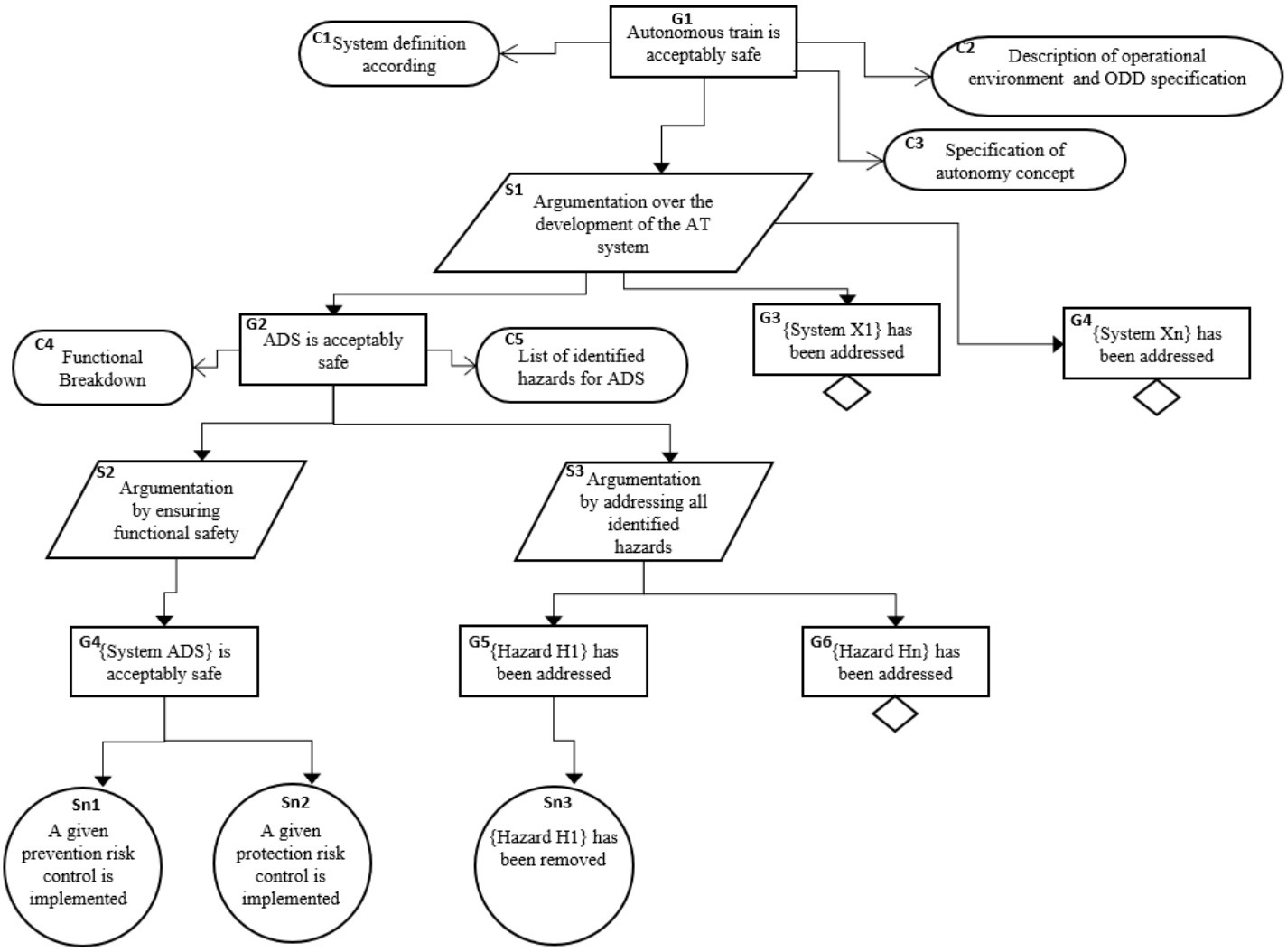

Fig. 4. Illustration simplifiée d'un structure globale GSN de l'argumentaire d'assurance de sécurité pour le train autonome

que le train autonome est capable d'analyser et d'évaluer dynamiquement les risques (i.e., durant l'exploitation et l'opération). Cette évaluation continue (et temps réel) pendant la phase d'exploitation est connue comme le concept de « *la conscience de la situation* » (*Situation Awareness*) [20], [21], [30]. Cette problématique de sécurité relative aux trains autonomes n'est pas le but de ce papier, cependant, elle reste un verrou scientifique majeur dans le processus de prise de décisions des systèmes autonomes.

V. CONCLUSION

Un des objectifs indispensables du train autonome est d'accomplir ses missions tout en assurant le maintien du niveau de sécurité global du système ferroviaire. En effet, l'intégration des trains autonomes dans le système ferroviaire global doit être appuyée par une démonstration de sécurité. Dans cette communication, nous avons discuté la pertinence de l'utilisation de l'argumentation graphique dans l'élaboration d'une démonstration de sécurité du train autonome. Dans un premier temps, nous avons présenté un aperçu global sur l'utilisation de la méthode GSN dans le domaine ferroviaire ainsi que pour les véhicules autonomes. Ensuite, nous avons proposé une approche d'assurance de sécurité pour les trains autonomes à l'aide de la GSN. L'approche proposée consiste à établir une structure globale GSN d'argumentation concernant l'assurance de sécurité du train autonome, en partant principalement de l'identification et de l'évaluation des dangers durant les phases de développement. Nos futurs travaux se focaliseront sur l'extension de l'approche afin de couvrir la partie dynamique de l'assurance de sécurité relative à la phase d'exploitation. En outre, nous considérons de développer un ensemble de motifs GSN d'arguments de sécurité permettant la réutilisation de la démonstration de sécurité pour les futurs systèmes autonomes ferroviaires. Cette librairie de motifs sera utilisée, initialement, pour présenter la démonstration de sécurité du train autonome dans le cadre du projet TASV (Train Autonome – Service Voyageur).

REMERCIMENTS

Ce travail est financé par le programme Français « Investissements d'Avenir » et fait partie du projet collaboratif Français TASV (Train Autonome Service Voyageurs), avec Railenium, SNCF, Alstom Crespin, Thales, Bosch, et Spirops.

RÉFÉRENCES :

[1] T. Kelly, « Safety cases », Handbook of Safety Principles, p. 361-385, 2017.

[2] T. Kelly et R. Weaver, « The goal structuring notation–a safety argument notation », Proc Dependable Syst Networks Workshop Assurance Cases, 2004.

[3] Q. Mahboob et E. Zio, Handbook of RAMS in Railway Systems : Theory and Practice, 1st Edition. New York, 2018.

[4] A. W. Evans, « Railway safety cases and railway risk assessment in Britain », in 4th International Conference on Competition & Ownership in Land Passenger Transport, 1995, p. 170-188.

[5] C. Edwards, « Railway Safety Cases », in Safety and Reliability of Software Based Systems, London, 1997, p. 317-322.

[6] « CENELEC - EN 50129 - Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling ».

[7] P. Bishop et R. Bloomfield, « A Methodology for Safety Case Development », Safety and Reliability, vol. 20, no 1, p. 34-42, mars 2000.

[8] R. Zocco, « Guide for Preparing Comprehensive and Complete Case for Safety for Complex Railway Products and Projects », in Handbook of RAMS in Railway Systems, CRC Press, 2018, p. 167-184.

[9] E. Althammer, E. Schoitsch, G. Sonneck, H. Eriksson, et J. Vinter, « Modular certification support — the DECOS concept of generic safety cases », in 6th IEEE International Conference on Industrial Informatics, 2018.

[10] T. S. Ankrum et A. H. Kromholz, « Structured assurance cases: three common standards », in 9th IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), 2005.

[11] The Assurance Case Working Group (ACWG), « GSN Community Standard (Version 2) », 2018, p. 82.

[12] R. Bloomfield et al., « Towards Identifying and closing Gaps in Assurance of autonomous Road vehicles -- a collection of Technical Notes Part 1, 2020 ».

[13] J. R. Müller, « The Formal Representation of the Safety Case Processes described in the EN 5012x norms », p. 46, 2009.

[14] K. Taguchi, S. Daisuke, H. Nishihara, et T. Takai, « Linking Traceability with GSN », in IEEE International Symposium on Software Reliability Engineering Workshops, 2014, p. 192-197.

[15] R. Wang, J. Guiochet, et G. Motet, « Confidence Assessment Framework for Safety Arguments », in Computer Safety, Reliability, and Security, Cham, 2017, p. 55-68.

[16] Y. Idmessaoud, D. Dubois, et J. Guiochet, « Belief Functions for Safety Arguments Confidence Estimation: A Comparative Study », 2020, p. 141-155.

[17] A. Wardziński, « Safety Assurance Strategies for Autonomous Vehicles », in Computer Safety, Reliability, and Security, Berlin, Heidelberg, 2008, p. 277-290.

[18] R. Alexander, T. Kelly, et N. Herbert, « Deriving Safety Requirements for Autonomous Systems », 2009.

[19] E. Heikkilä, R. Tuominen, R. Tiusanen, J. Montewka, et P. Kujala, Safety Qualification Process for an Autonomous Ship Prototype – a Goal-based Safety Case Approach. 2017.

[20] M. R. Endsley, « Toward a theory of situation awareness in dynamic systems », Human factors, vol. 37, no 1, 1995, p. 32-64.

[21] P. Feth, M. N. Akram, R. Schuster, et O. Wasenmüller, « Dynamic Risk Assessment for Vehicles of Higher Automation Levels by Deep Learning », in Computer Safety, Reliability, and Security, Cham, 2018, p. 535-547.

[22] S. Wagner, B. Schätz, S. Puchner, et P. Kock, « A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models », in IEEE 21st International Symposium on Software Reliability Engineering, 2010, p. 269-278.

[23] R. Palin, D. Ward, I. Habli, et R. Rivett, « ISO 26262 safety cases: Compliance and assurance », in 6th IET International Conference on System Safety, 2011, p. 1-6.

[24] Y. Luo, M. van den Brand, L. Engelen, et M. Klabbers, « A Modeling Approach to Support Safety Assurance in the Automotive Domain », in Progress in Systems Engineering, Cham, 2015, p. 339-345.

[25] I. Habli, I. Ibarra, J. Land, R. Rivett, et T. Kelly, « Model-Based Assurance for Justifying Automotive Functional Safety », 2010.

[26] B. H. C. Cheng, R. J. Clark, J. E. Fleck, M. A. Langford, et P. K. McKinley, « AC-ROS: assurance case driven adaptation for the robot operating system », in Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems, New York, NY, USA. 2020, p. 102-113.

[27] R. Hawkins, C. Paterson, C. Picardi, Y. Jia, R. Calinescu, et I. Habli, « Guidance on the Assurance of Machine Learning in Autonomous Systems (AMLAS) », 2021.

[28] H. OUFERROUKH, « Common Safety Methods », European Railways Agency (ERA), 2018.

[29] « ISO/PAS 21448:2019 », Road Vehicles - Safety Of The Intended Functionality (SOTIF), 2019.

[30] J. Reich, M. Wellstein, I. Sorokos, F. Oboril, et K.-U. Scholl, « Towards a Software Component to Perform Situation-Aware Dynamic Risk Assessment for Autonomous Vehicles », in Dependable Computing - EDCC 2021 Workshops, Cham, 2021, p. 3-11.

[31] C. Hirata, S. Nadjim-Tehrani, Combining GSN and STPA for Safety Arguments, in: International Conference on Computer Safety, Realiability, and Security, Springer, p.5-15, 2019.

[32] D. Pissoort, T. Bultinck, J. Boydens, J. Catrysse, «Use of the Goal Structuring Notation (GSN) as a generic Notation for an EMC Assurance Case», in: International Symposium on Electromagnetic Compatibility - EMC EUROPE, IEEE, Barcelona, p. 465-469, 2019.