Cas d'étude de mission ferroviaire télé-opérée

Sana Debbech, Simon Collart-Dutilleul, Philippe Bon

Cas d'étude de mission ferroviaire télé-opérée

Sana Debbech, Simon Collart-Dutilleul, Philippe Bon

Novembre 2018

Chapitre 1

Introduction

Lors de la conception d'un nouveau système, une analyse préliminaire des risques est requise. Une fois les risques bien identifiés, le but est de formaliser une défense à chaque défaillance vraisemblable. Imaginons par exemple, que dans le cadre d'un nouveau système, on souhaite piloter un train à partir d'un poste de conduite à distance en s'appuyant sur des moyens de télécommunications modernes et un dispositif technique de perception de l'environnement embarqué dans le train ; le nouveau système intégrant ces dispositifs particuliers de perception de l'environnement et de télé-opération nécessite une analyse de sécurité globale. Cette analyse de sécurité doit considérer l'aspect socio-technique du système et son environnement.

Dans cette étude, on va s'intéresser à un aspect particulier de la vie du conducteur de train : les opérations à effectuer lors d'une mission de conduite qui ne sont pas directement des actes de conduite. Dans cette catégorie d'opérations, on trouvera la protection d'obstacles se situant sur la voie et empêchant l'exploitation de l'infrastructure, ainsi que les opérations de sécurisation d'un train lorsqu'il est mis en échec lors du franchissement d'une rampe. En effet, selon le chargement, les conditions d'adhérence et la puissance de la motrice, une rampe peut ne pas être franchie. Dans cette situation, le conducteur peut s'appuyer sur sa vitesse initiale pour prendre son élan et franchir l'obstacle. Cependant des incidents de circulations peuvent entraîner un arrêt inopiné et dans ce cas particulier, on ne pourra plus s'appuyer sur l'inertie du train. Par conséquent, un démarrage en rampe doit être mis en œuvre si le contexte le permet. En cas d'échec, il est prescrit que le conducteur protège son train contre la dérive arrière en posant des cales. Cependant, dans le cas d'une télé-opération, le conducteur n'est pas présent dans le cabine et ne peut donc pas poser ces cales.

Ce rapport présente un travail académique **conceptuel**. Il vise à formaliser les étapes permettant une organisation de mission télé-opérée en intégrant le fait que les rampes doivent être franchies dans des conditions de sécurité raisonnables. Dans le cadre de l'évolution des infrastructures ferroviaires, on veut s'appuyer sur la valorisation des connaissances utilisée par un conducteur de lignes pour planifier sa mission. La proposition académique formalise la question suivante : « Comment le télé-opérateur pourrait valoriser la connaissance dont il dispose pour planifier sa mission en intégrant le nouveau contexte technologique ? ».

Chapitre 2

Cas d'étude de la préparation de la mission

2.1 Description du scénario

Dans cette étude, nous considérons deux scénarios spécifiant le déroulement de la préparation d'une mission télé-opérée en fonction des circonstances de la mission. Le *scénario nominal* consiste au déroulement de la mission dans les conditions classiques pour lesquelles le conducteur maîtrise parfaitement et de manière quasi-automatique les gestes du métier. Le *scénario nominal* est décrit comme suit :

1. Le conducteur d'un train de fret prend connaissance de la météo et du contexte général de sa mission. Pour cela, il contacte notamment le responsable de l'entrepôt où son train est garé.
2. Le conducteur prend connaissance de la constitution de son train à partir des documents qui lui sont fournis.
3. Le conducteur prend connaissance des capacités effectives de son train à l'aide d'essais de freins.
4. À l'issu de cette étape de prise de connaissance, le conducteur décide d'organiser la mission de manière classique.

À l'issu de l'étape 4, le conducteur peut constater qu'il existe un risque que son train ne soit pas capable de traverser une rampe présente sur son trajet. Le *scénario dégradé* défini ci-dessous se déroule en fonction du contexte de la mission et de l'intention de l'agent :

Il vérifie sur les documents dont il dispose si son matériel est équipé d'un dispositif de dépose de cales automatiques contre le refoulement en dérive et efficace pour la rampe considérée :

1. Si c'est le cas et s'il estime que le risque associé au non passage de la rampe est très faible (par exemple, cas d'une cuvette minimisant le risque de dérive arrière), il décide d'organiser normalement la mission.

2. Sinon (pas de dispositif de cales automatiques ou risque trop important malgré les cales), il reprend contact avec le site de la circulation et l'entrepôt pour demander :
   (a) Soit la mise à disposition d'une locomotive de remplacement pour être en mesure d'effectuer la mission.
   (b) Soit l'utilisation d'une deuxième locomotive de manière à être capable de passer la rampe dans des conditions acceptables. Remarquons que l'utilisation d'une locomotive complémentaire télé-opérée va probablement éviter la mise sous astreinte de conducteurs et va diminuer les délais d'acheminement de ces dernières.

Dans ce scénario, le danger consiste en la dérive d'un train en marche arrière, emporté par son poids après un arrêt au milieu d'une rampe sévère suite à un défaut d'adhérence et/ou de puissance lors du franchissement. Dans cette situation critique, le contexte de la mission est constitué de différents éléments liés à la fois au matériel roulant, à la connaissance de l'infrastructure et des règlements de circulation, aux conditions météo et à l'historique des missions effectuées par les trains précédents dans des conditions similaires. Le poids du train et sa constitution, ses propres capacités sachant qu'il peut y avoir des dispersions importantes entre les matériels notamment en fonction de l'usure, les conditions météo (rail mouillé, présence de givre, etc..), sont des paramètres critiques à identifier lors des phases de prise de connaissance.

2.2 Analyse & Interprétation

Le déroulement de ce scénario s'appuie notamment sur la prise de connaissance préalable du contexte globale de la mission. Dans cette étude, nous formalisons la modélisation conceptuelle d'une mission en considérant les caractéristiques de la connaissance du domaine. Dans cette conceptualisation, trois connaissances des domaines sont considérées, à savoir, l'analyse de sécurité, l'ingénierie des exigences dirigée par les buts (IEDB) [Van Lamsweerde 2001] et le concept du contexte dérivé du modèle de contrôle d'accès basé sur l'organisation (Or-BAC) [El Kalam et al. 2003]. Comme ce modèle de contrôle d'accès est initialement conçu pour assurer la sécurité-confidentialité des systèmes d'informations (SI), une ré-interprétation des concepts du point de vue sécurité-innocuité des systèmes critiques a été proposée dans [Debbech et al. 2018a]. Ensuite, une interprétation des concepts Or-BAC dans la sémantique du monde réel a été argumentée dans [Debbech et al. 2018b]. Afin d'assurer l'homogénéité sémantique entre les différentes connaissances des domaines, la modélisation conceptuelle doit être établie en se référant à une ontologie de haut niveau. Une ontologie de haut niveau est une représentation structurée et explicite de la réalité avec des concepts et des relations fondamentaux. Dans la littérature, les ontologies de niveau supérieur ou fondamentales sont largement utilisées dans le développement des ontologies du domaine ayant une interprétation dans la sémantique du monde réel. Cette pratique de l'ingénierie des connaissances permet d'approximer la conceptualisation à la représentation idéale du domaine en terme de consistance et de complétude. L'analyse des ontologies fondamentales existantes tel que BFO [Spear et al. 2016], DOLCE [Borgo & Masolo 2010] et UFO [Guizzardi 2005], nous permet d'affirmer que UFO propose un ensemble de concepts et de caractéristiques fondamentaux très utiles pour couvrir les aspects de cette étude. Ce choix a été justifié dans [Debbech et al. 2018b] en considérant à la fois les concepts clés de l'analyse de sécurité et de l'IEDB ainsi que la pertinence de la taxonomie fondamentale proposée par UFO. Par conséquent, la conceptualisation proposée et son développement sont respectivement fondés sur UFO et ses distinctions ontologiques du « pattern design ».

Afin de gérer l'aspect dynamique des systèmes critiques de sécurité tels que les systèmes ferroviaires, la notion du contexte est pertinente afin de capturer la connaissance liée à l'adaptation de l'organisation de la mission. En alignant les concepts introduits dans cette étude avec les concepts d'UFO, nous définissons le contexte comme une situation spécifique qui justifie la validité de la mesure de sécurité considérée pour éviter un risque. Autrement dit, la mesure de sécurité identifiée s'adapte au contexte perçu au moment de l'organisation de la mission. Cependant, le contexte global peut être décomposé en un ensemble de sous-contextes s'il est estimé critique en incluant plusieurs éléments à la fois. À l'issu de cette interprétation, nous proposons le modèle conceptuel illustré par la figure 2.1. Le langage de représentation du modèle conceptuel est OntoUML, qui est une extension du langage UML 2.0 pour assister la modélisation conceptuelle de haut niveau et l'ingénierie des ontologies de domaine [Guizzardi 2005]. Il intègre les importantes distinctions et caractéristiques proposées par UFO pour obtenir une représentation explicite et structurée des connaissances de domaines. La relation d'héritage en UML 2.0 est définie comme une relation de subsomption dans OntoUML. La relation de subsomption est une relation binaire entre un super-concept et un sous-concept. Plus de détails concernant les définitions des concepts d'UFO et l'alignement avec les concepts introduits peuvent être trouvés dans [Debbech et al. 2018b].

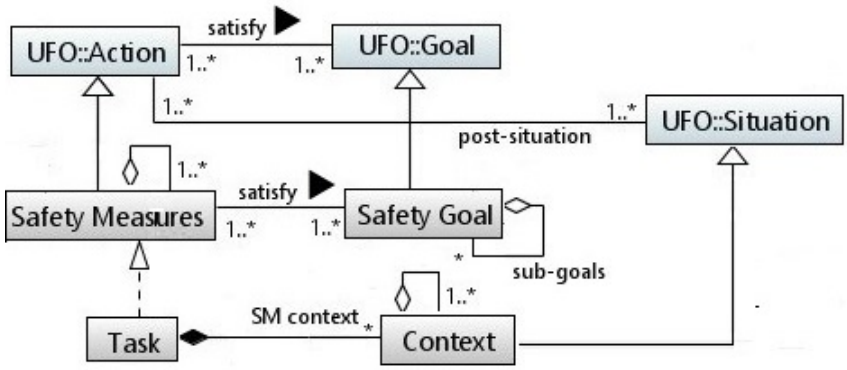

FIGURE 2.1 – Le fragment du modèle conceptuel représentant les relations entre les mesures de sécurité, le but et le contexte

L'ingénierie des exigences orientée-but (GORE) permet la gestion de complexité des pratiques de l'ingénierie des exigences (RE) guidée par les buts. Plusieurs approches de GORE existent dans la littérature notamment i* (i-Star), Techne, KAOS et GORO. Les trois premières approches se distinguent par leurs propres interprétations sémantiques des concepts et des relations entre eux. Tandis que, GORO est une ontologie de référence du domaine GORE, fondée sur UFO et basée sur l'intéropérabilité des approches existantes afin d'obtenir une représentation complète et consistante dans la sémantique du monde réel [Negri et al. 2017]. Comme l'un des principaux avantages des ontologies est la réutilisation, le fragment de GORO est réutilisé en se focalisant sur les relations entre le but, ses types fondamentaux proposés par UFO notamment *Intention*, *Belief* et *Proposition*, les exigences et les agents. Ce choix a été argumenté dans [Debbech et al. 2018b]. Dans ce rapport, nous présentons seulement les relations entre les mesures de sécurité, le but de sécurité, la mission (Task) et le contexte. La modélisation conceptuelle globale a été détaillée dans [Debbech et al. 2018c].

Le but représente l'exigence globale de plus haut niveau d'abstraction fournie par une organisation. Une organisation peut être une personne, un groupe de personnes ou une agrégation d'organisations. Le but de sécurité est un sous-type de but (UFO), et peut être décomposé en un ensemble de

sous-buts. Dans un niveau plus concret dans l'arbre des exigences, les buts sont raffinés en exigences. Ces exigences peuvent être attribuées à des agents comme indiqué dans la figure 2.2. De plus, une mesure de sécurité est proposée afin de satisfaire un but global de sécurité. De la même façon, une mesure de sécurité peut être décomposée en un ensemble de mesures de sécurité. La formalisation de ces relations ainsi que les axiomes définis afin de systématiser le processus intégral sont présentés dans [Debbech et al. 2018c]. La modélisation proposée dans ce rapport illustre un cas d'étude critique en s'appuyant sur les caractéristiques majeures de l'ingénierie des connaissances.

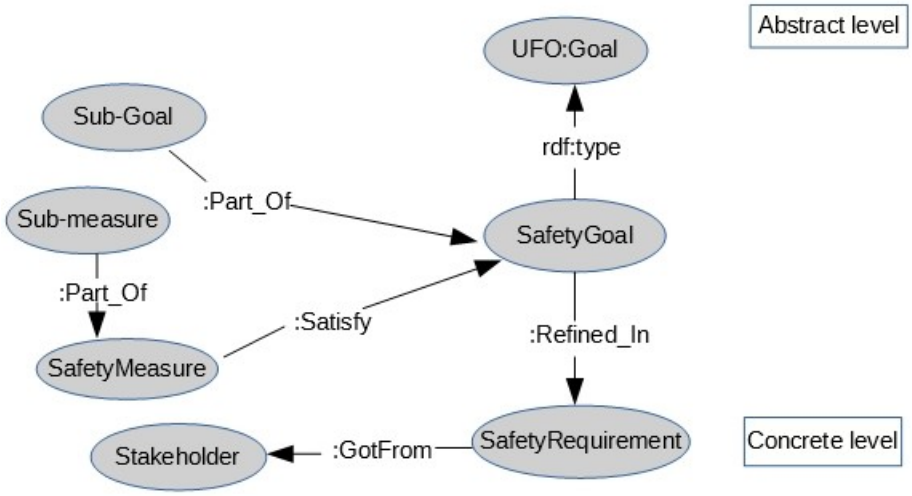

FIGURE 2.2 – La description du pattern du fragment de l'ontologie proposée

Afin de valider la flexibilité et l'expressivité de la taxonomie proposée, nous procédons à l'alignement des concepts avec les entités du scénario considéré. Les concepts et les relations sont représentés respectivement par les variables et les prédicats comme illustré par le tableau 2.1.

Relation	Type
hasPart(t,c)	Task × Context
realize(t,sm)	Task × Safety Measure
satisfy(sm,sg)	Safety Measure × Safety Goal

TABLE 2.1 – Les concepts et les relations du fragment proposé

Afin de valider sa capacité à représenter le scénario ci-dessus, nous avons décomposé les éléments du contexte et nous avons instancié le fragment du modèle conceptuel comme suit :

Soit c = $\{c_1, c_2, c_3, c_4, c_5, c_6\}$ l'ensemble de contextes décomposés dans le scénario, représentés par la relation *partOf*(c_i,c) | i ∈ [1,6] où :

— c_1 est la connaissance de la météo ;
— c_2 est la connaissance de la constitution du train ;
— c_3 est la connaissance des capacités effectives du train ;
— c_4 est la connaissance de la présence d'un dispositif de dépose de cales automatiques efficace pour la rampe considérée ;

— c_5 est la connaissance du risque associé au non passage de la rampe est faible en cas d'une cuvette ;
— c_6 est la prise de connaissance de l'historique des missions effectuées par les trains précédents dans les mêmes conditions.

Le processus d'organisation de la mission orienté-but est contraint par les axiomes exprimés en Logiques de description (LD) afin de mettre en avant les éléments critiques du contexte nécessaires pour l'analyse de sécurité. La relation de compostion est représentée par la relation *hasPart* qui associe un composé à un composant (Whole-Part). Cette relation est déclarée transitive, antisymétrique et irréflexive comme respectivement spécifié par les axiomes (2.1), (2.2) et (2.3). La relation *hasPart* est l'inverse de *partOf*.

$$hasPart \circ hasPart \sqsubseteq hasPart \tag{2.1}$$

$$\top \sqsubseteq \neg \exists hasPart.Self \tag{2.2}$$

$$\top \sqsubseteq \exists (hasPart \sqcap hasPart^{-}).\bot \tag{2.3}$$

Dans le scénario *nominal*, l'ensemble des contextes c_1, c_2, c_3 et c_6 représentent les circonstances classiques pour mener la mission t à terme. L'acquisition de ces données et leur intégration dans le processus de sécurité est nécessaire et suffisante pour organiser la mission de manière classique. Le contact du responsable de l'entrepôt (sm_1), la prise de connaissance des documents fournis (sm_2) et l'essai des freins (sm_3) constituent l'ensemble de mesures de sécurité qui sont respectivement adaptées aux contextes c_1 ou c_6, c_2 et c_3. L'ensemble des sous-mesures de sécurité considéré permet de satisfaire le but de sécurité global, à savoir le franchissement de la rampe en toute sécurité. La figure 2.3 représente l'illustration de l'annotation entre le modèle conceptuel et les instances du scénario nominal (les rectangles représentent les instances et les cercles représentent les concepts).

Le scénario *dégradé* est constitué des éléments critiques de sécurité liés à la fois au contexte et à l'image perçue dans le modèle cognitif de l'agent, basée sur des hypothèses (le concept Belief proposé par UFO). De ce fait, le conducteur vérifie sur les documents à sa disposition si son train est équipé d'un dispositif de cales automatiques efficace pour la rampe considérée (c_4). De plus, il prend en considération le contexte topologique, à savoir le cas d'une cuvette diminuant le risque de dérive arrière (c_5). À l'issu de la prise de connaissance de ces deux éléments du contexte, le conducteur décide d'organiser normalement sa mission. Pour cette partie de préparation de la mission, le processus d'annotation s'effectue de la même façon que le scénario nominal. Dans ce qui suit, nous nous intéressons à la situation d'absence des contextes c_4 ou c_5. Dans ce cas, le conducteur reprend contact avec le site de circulation et l'entrepôt. Ceci représente une mesure de sécurité globale (sm) qui peut être décomposée en deux sous-mesures de sécurité tel que :

— sm_4 : la mise à disposition d'une locomotive de remplacement ;
— sm_5 : l'utilisation d'une deuxième locomotive ;

Le « OU exclusif $\oplus$ » des deux sous-mesures de sécurité permet de satisfaire le but de sécurité sg, qui est le franchissement de la rampe dans des conditions acceptables. Néanmoins, la deuxième sous-mesure sm_5 est considérée meilleure vis-à-vis à la mise sous astreinte d'un autre conducteur et du délai d'acheminement des locomotives. La figure 2.4 représente l'annotation sémantique du scénario

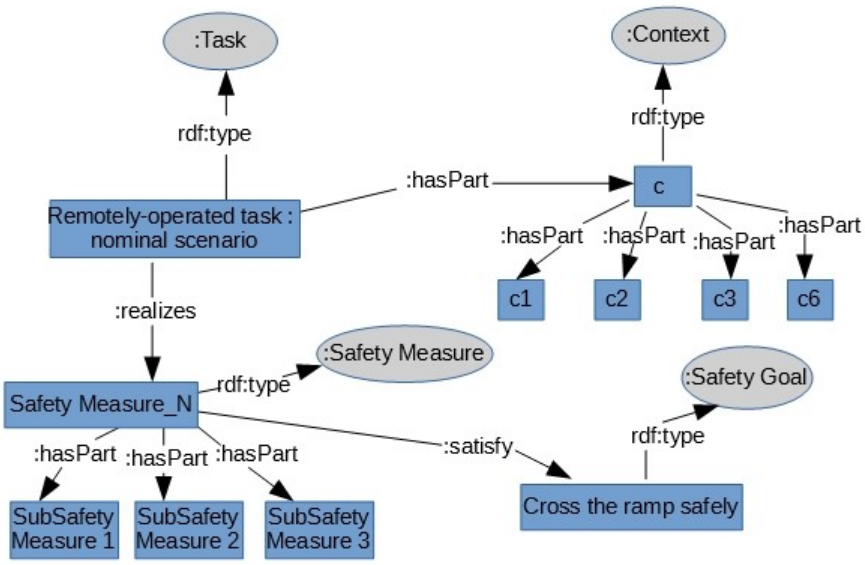

FIGURE 2.3 – La représentation graphique de l'annotation du scénario nominal

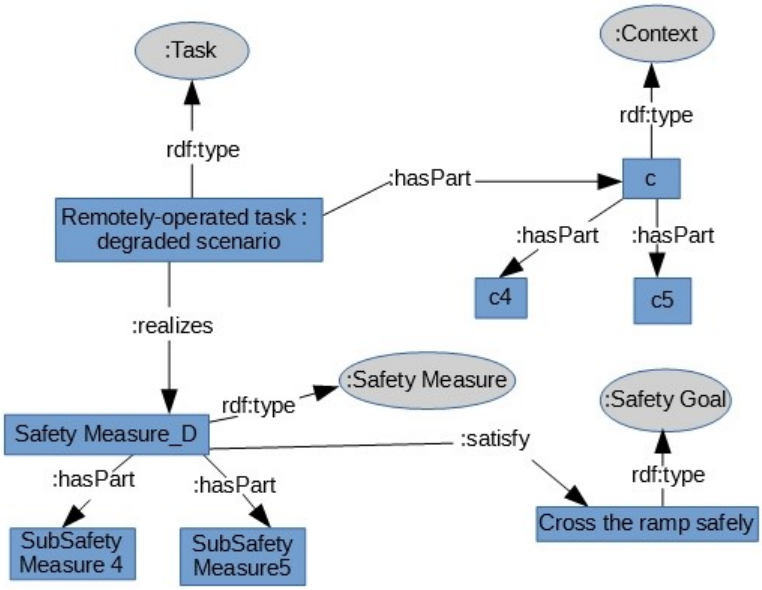

FIGURE 2.4 – La représentation graphique de l'annotation du scénario dégradé

dégradé et l'intégration de la prise de connaissance des éléments du contexte dans le processus de gestion des décisions de sécurité.

En définitive, la mission consiste en la réalisation d'une ou plusieurs mesures de sécurité dans un contexte spécifique afin de satisfaire un but. Ce processus de gestion de connaissances est défini

et contraint par un ensemble d'axiomes afin d'assister la prise de décision de l'agent impliqué dans la mission. Dans ce rapport, nous avon présenté une partie de la modélisation proposée qui met en exergue la pertinence de la taxonomie définie dans la sémantique du monde réel et sa capacité d'analyser des situations critiques. En effet, le modèle conceptuel met en relief le contexte et ses concepts environnants afin de systématiser le processus global de gestion des décisions de sécurité sur le plan conceptuel et opérationel. Suite à l'acquisition des connaissances liées au système et à l'environnement, la mission est organisée afin de satisfaire un but global de sécurité. Le modèle conceptuel proposé peut être instancié afin de représenter des situations du monde réel en s'appuyant sur la flexibilité de la sémantique introduite et le polymorphisme des concepts.

Chapitre 3

Conclusion

Pour une portion d'infrastructure donnée, une information de contexte pourrait avoir un sens critique en fonction de la nature de l'infrastructure. À l'heure où un dictionnaire général des données normalisées est à l'étude au niveau mondial pour l'infrastructure ferroviaire, l'union internationale de chemins de Fer (UIC) propose une ontologie des infrastructures ferroviaire[1]. Une extension de cette ontologie permettant d'intégrer des éléments de contexte liés à une étude de sécurité parait nécessaire. Afin de prendre en considération cet aspect, la taxonomie doit être proposée avec un haut niveau d'abstraction pour établir l'annotation sémantique.

Une représentation explicite avec un haut niveau d'abstraction des informations liées au contexte et son intégration dans le processus de l'organisation d'une mission télé-opérée est un atout majeur pour atteindre le niveau de sécurité requis. En effet, la perception préalable de ces données par l'agent au moment de l'organisation de la mission est nécessaire afin de gérer les décisions liées à la sécurité d'une manière plus restrictive. Le processus d'alignement des concepts fondamentales de UFO avec la taxonomie introduite permet d'avoir une clarification conceptuelle et une systématisation du processus de gestion des connaissances. La conceptualisation du processus orienté-but de gestion des décisions de sécurité permet d'avoir une vue partagée sans ambiguïté entre les connaisances de conception et de sécurité.

La taxonomie proposée dans la sémantique du monde réel, dont la définition des concepts est basée sur les modèles de référence et les standards, est nécessaire dans le domaine des systèmes critiques de sécurité tel que les systèmes ferroviaires. Grâce à ses caractéristiques fondamentales formalisées, l'ontologie proposée pourrait être ré-utilisée pour d'autres domaines critiques de sécurité. Dans ce rapport, notre proposition vise essentiellement la valorisation de la gestion des connaissances de l'agent pour planifier sa mission télé-opérée. D'un autre point de vue, l'ontologie a été développée en se basant sur une approche systématique commençant par l'élicitation des questions de compétence jusqu'à la phase de tests. En considérant d'autres perspectives telles l'ingénierie des exigences et l'analyse de sécurité, cette proposition sera étendue pour intégrer de nouveaux aspects notamment le processus de développement des mesures de sécurité, la gestion des décisions de sécurité guidée par les buts et la traçabilité des exigences.

1. Hlubuček, A. (2017). RAILTOPOMODEL AND RAILML 3 IN OVERALL CONTEXT. Acta Polytechnica CTU Proceedings, 11, 16-21.

Bibliographie

[Borgo & Masolo 2010] Borgo, S., & Masolo, C. (2010). Ontological foundations of DOLCE. In *Theory and applications of ontology : Computer applications*. pp. 279-295. Springer, Dordrecht.

[Debbech et al. 2018a] Debbech, S., Collart-Dutilleul, S., Bon, P. (2018). A Model-based system engineering approach to manage railway safety-related decisions. *International Journal on Transport Development and Integration*, 3(1), 30-43.

[Debbech et al. 2018b] Debbech, S., Collart-Dutilleul, S., Bon, P. (2018). Towards Semantic Interpretation of Goal-Oriented Safety Decisions based on Foundational Ontology. *Journal of Computers*, 14(4), 257-267.

[Debbech et al. 2018c] Debbech, S., Collart-Dutilleul, S., Bon, P. (2019). Conceptual Modelling of the Dynamic Goal-Oriented Safety Management for Safety Critical Systems. In proc. 14^{th} International Conference on Software Technologies ICSOFT, Prague.

[El Kalam et al. 2003] El Kalam, A. A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., & Trouessin, G. (2003). Or-BAC : un modèle de contrôle d'accès basé sur les organisations. *Cahiers francophones de la recherche en sécurité de l'information*, 1, 30-43.

[Guizzardi 2005] Guizzardi, G. (2005). Ontological Foundations for Structural Conceptual Model. PhD thesis, University of Twente, The Netherlands.

[Gruber 1993] Gruber, T. R. (1993). A translation approach to portable ontology specifications. Knowledge acquisition, 5(2), 199-220.

[Negri et al. 2017] Negri, P. P., Souza, V. E. S., de Castro Leal, A. L., de Almeida Falbo, R., & Guizzardi, G. (2017). Towards an Ontology of Goal-Oriented Requirements. In CIbSE pp. 469-482.

[Van Lamsweerde 2001] Van Lamsweerde, A. (2001). Goal-oriented requirements engineering : A guided tour. In Requirements Engineering Proceedings. 5^{th} IEEE International Symposium on Requirements Engineering (RE'01). pp.249-262.

[Spear et al. 2016] Spear, A. D., Ceusters, W., & Smith, B. (2016). Functions in basic formal ontology. *Applied Ontology*, 11(2), 103-128.