Ontologies pour la gestion de sécurité ferroviaire : intégration de l'analyse dysfonctionnelle dans la conception

Sana Debbech

N^o d'ordre : 385

Centrale Lille

THÈSE

présentée en vue d'obtenir le grade de

DOCTEUR

en

Spécialité : Automatique, Génie Informatique, Traitement du Signal et des Images

par

Sana DEBBECH

DOCTORAT DELIVRÉ PAR CENTRALE LILLE

Titre de la thèse :

Ontologies pour la gestion de sécurité ferroviaire : intégration de l'analyse dysfonctionnelle dans la conception

---

Soutenue le 14 Octobre 2019 devant le jury d'examen :

Président :	Walter SCHÖN, Professeur, *Université de Technologie de Compiègne*
Rapporteur :	Anne-Françoise CUTTING-DECELLE, Professeure, *Université de Genève*
Rapporteur :	Hélène WAESELYNCK, Directrice de recherche, *LAAS-CNRS, Toulouse*
Examinatrice :	Régine LALEAU, Professeure, *Université Paris-Est Créteil*
Examinateur :	Cédric DUMOULIN, Maître de conférence, *Université de Lille*
Invité	Airy MAGNIEN, Ingénieur, *UIC, Paris*
Directeur de thèse :	Simon COLLART-DUTILLEUL, Directeur de recherche, *IFSTTAR, Lille*
Encadrant :	Philippe BON, Chargé de recherche, *IFSTTAR, Lille*

Thèse préparée dans le Laboratoire d'Évaluation des Systèmes de Transports Automatisés et de leur Sécurité
IFSTTAR, COSYS/ESTAS, Villeneuve d'Ascq

École Doctorale SPI 072 (EC Lille)

Résumé

La sécurité-innocuité (Safety) est une propriété émergente des systèmes critiques de sécurité (SCS), notamment les systèmes ferroviaires. En effet, les interactions entre leurs composants peuvent conduire à des accidents impactant la vie des personnes, le système et l'environnement. Par conséquent, cet aspect dynamique complexifie le processus de développement de ces systèmes et nécessite un raisonnement judicieux permettant de diminuer les dangers associés. Dans le cadre de cette thèse, nous proposons une approche ontologique qui intègre les activités de sécurité dès les premières phases de la conception des SCS. Ce cadre ontologique structuré permet d'offrir une harmonisation sémantique entre les connaissances des domaines impliqués, tels que l'ingénierie de sécurité et l'Ingénierie des Exigences Dirigée par les Buts (IEDB). La logique métier intégrée dans cette approche est validée par des cas d'étude ferroviaires d'accidents réels et d'une mission télé-opérée.

Dans un premier temps, nous avons proposé une ontologie d'analyse dysfonctionnelle appelée *DAO* et fondée sur l'ontologie de haut niveau *UFO*. Elle capitalise les connaissances liées au domaine et fournit une clarification conceptuelle des relations entre les défaillances, leurs causes, leurs conséquences, le danger associé, etc. Les concepts d'analyse dysfonctionnelle sont interprétés dans la sémantique du monde réel, en s'appuyant sur les définitions proposées par les standards du domaine. En outre, DAO considère les aspects sociaux-techniques et environnementaux des SCS et intègre les différents types de fautes et de propriétés cognitives liés respectivement aux défaillances techniques et aux erreurs humaines. Le modèle conceptuel de DAO est exprimé en *OntoUML* et implémenté en utilisant le langage formel d'ontologie *OWL* afin de fournir un support d'interopérabilité sémantique et de raisonnement pour construire des mesures de sécurité.

Dans un deuxième temps, un pont sémantique est établi entre les mesures de sécurité, les buts de sécurité et les exigences de sécurité par le développement d'une ontologie de gestion de sécurité orientée-but, appelée *GOSMO*. La gestion des décisions de sécurité, qui s'adapte aux contextes dynamiques, est basée sur la réinterprétation du modèle de contrôle d'accès *Or-BAC* d'un point de vue sécurité-innocuité. L'adaptation de ce modèle au service de la sécurité ferroviaire répond aux contraintes organisationnelles et technologiques par analogie de l'attribut sécurité-confidentialité des systèmes d'information. À cet égard, GOSMO fournit une vue partagée entre les mesures de sécurité, les concepts de l'IEDB et les concepts d'Or-BAC. Le formalisme de la gestion des décisions de sécurité orientée-but permet de structurer les choix pour satisfaire les buts de sécurité. Afin d'assurer la cohérence globale des exigences, GOSMO permet de structurer la gestion des évolutions des exigences ainsi que leur traçabilité.

Mots clés : Sécurité ferroviaire, Analyse dysfonctionnelle, IEDB, Modélisation conceptuelle, Ontologie, Modèle *Or-BAC*, UFO, OntoUML, OWL.

Préambule

Cette thèse s'intègre dans le cadre de l'obtention du grade de Docteur de Centrale Lille en Automatique, Génie Informatique, Traitement du Signal et des Images au sein de l'École Doctorale Sciences Pour l'Ingénieur (SPI 072). Le fond scientifique de la thèse porte sur la proposition des ontologies pour la gestion de sécurité ferroviaire : intégration de l'analyse dysfonctionnelle dans la conception. La méthodologie ontologique proposée est illustrée par deux cas d'études d'accidents ferroviaires réels et un scénario de mission ferroviaire télé-opérée.

Les analyses d'accidents sont fournies dans des rapports du Bureau d'Enquêtes sur les Accidents de Transport Terrestre (BEA-TT) qui sont publics et accessibles sur leur site. Notre recherche est donc reproductible. Concernant le troisième cas d'étude, qui définit une mission ferroviaire télé-opérée, il est inspiré du mode opératoire des trains télécommandés. Ce cas d'étude est disponible sur l'archive HAL [Debbech *et al.*, 2018c].

Par ailleurs, la validation de la logique métier intégrée dans ces travaux de recherche ne repose pas sur des exemples simples élaborés sur mesure pour mettre en valeur les résultats obtenus. Il s'agit d'accidents réels et documentés par des experts indépendants. En définitive, il n' y a aucune contrainte de confidentialité dans ce mémoire ; L'auteur s'est attachée à utiliser les sources publiques et neutres comme données expérimentales.

Remerciements

Les travaux de thèse présentés dans ce manuscrit ont été réalisés à l'Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux (IFSTTAR), au sein du laboratoire Évaluation des Systèmes de Transport Automatisés (ESTAS) à Villeneuve d'Ascq.

Je tiens à exprimer mes remerciements les plus sincères à mon directeur de thèse *Simon Collart-Dutilleul* d'avoir dirigé ces travaux. Merci d'avoir cru en mes capacités et de m'avoir soutenu et encouragé pendant ces trois années pour mener à bien ce travail. Ses conseils judicieux et nos discussions enrichissantes m'ont bien guidé pour cerner à la fois le cadre industriel et scientifique.

J'adresse mes plus vifs remerciements à mon encadrant de thèse *Philippe Bon* d'avoir encadré ces travaux de thèse. Merci pour les mots d'encouragement et pour ton humour qui ont contribué à avoir une bonne ambiance de travail et de motivation. Ses conseils pertinents m'ont permis d'avancer et d'améliorer la mise en valeur de mes publications et mon manuscrit.

J'exprime également ma grande reconnaissance et remerciements à Madame *Anne-Françoise Cutting-Decelle*, Professeure de l'Université de Genève et Madame *Hélène Waeselynck*, Directrice de recherche du LAAS-CNRS, d'avoir accepté d'examiner ces travaux en qualité de rapporteurs. Je vous remercie pour le temps que vous avez accordé à la lecture de ce manuscrit et pour vos remarques pertinentes.

Mes sincères remerciements vont aussi à Monsieur *Walter Schön*, Professeur de l'université de Technologie de Compiègne, étant président de jury de cette thèse, à Madame *Régine Laleau*, Professeure de l'université de Paris Est-Créteil, et Monsieur *Cédric Dumoulin*, Maître de conférences de l'université de Lille, d'avoir accepté de faire partie du jury en qualité d'examinateurs, ainsi que Monsieur *Airy Magnien* de l'Union Internationale des Chemins de fer (UIC) à Paris pour sa présence en qualité d'invité.

Cette thèse a été précédée par une expérience professionnelle au sein de l'institut au laboratoire LEOST qui m'a permis de me familiariser avec le contexte ferroviaire et de m'initier dans la recherche. Je remercie *Marion Berbineau*, Directrice de recherche à l'IFSTTAR de Villeneuve d'Ascq qui m'a beaucoup aidé tant à l'échelle professionnelle que personnelle. Marion, merci pour ta gentillesse, ta générosité et tes conseils.

Je remercie aussi mes collègues et ami(e)s *Dalay*, *Ci*, *Mouna*, *Rahma*, *Kenza*, *Michel*, *Ouail*, *Amani*, *Matthieu* et *Mohamed* pour les moments de bonheur, les mots d'encouragement et nos fous rires qui ont rendu l'ambiance agréable au travail et en dehors de l'institut.

Je remercie chaleureusement tout le personnel de l'IFSTTAR-Villeneuve d'Ascq pour la bonne ambiance de travail, leur sympathie et leur gentillesse durant ces 4 ans et demi que j'ai vécu parmi eux entre les laboratoires LEOST ET ESTAS. C'était un grand plaisir de rencontrer des personnes magnifiques particulièrement *Sonia*, *Olivier*, *Nathalie*, *Corinne* et *Valérie* qui n'ont jamais hésité à m'aider et à m'encourager tout en étant souriants.

Cette thèse n'aurait pas pu aboutir à cet état sans le soutien et la présence de mon cher compagnon *Romain* qui a toujours été là pour m'encourager et me motiver dans les moments les plus difficiles. Merci d'avoir partagé avec moi les hauts et les bas et pour tout ce que tu as fait pour moi.

En ce jour tant attendu, nul mot ne peut exprimer ma joie et ma gratitude envers ma famille qui a toujours été fière de moi et qui n'a jamais cessé de me soutenir, de croire en moi et de me pousser pour aller plus loin tout au long de mon parcours. GRAND merci à mes parents *Hamda* et *Nebiha* pour leur amour et leur encouragements aux moments de stress. Je remercie mes frères *Habib* et *Ali* et ma belle soeur *Sana* pour leur soutien indéfectible. Je ne peux pas oublier ma petite nièce adorée *Majdoline* qui m'a comblé de joie et d'amour et qui m'a toujours encouragé à sa façon innocente.

En dernier, je remercie tous ceux qui ont contribué de près ou de loin à l'accomplissement de ces travaux de thèse dans de bonnes conditions.

Table des matières

Table des figures

Liste des tableaux

Glossaire

AdD Arbre des Défaillances. vii, 17, 19, 26, 29, 32, 36–40

ALARP As Low As Reasonably Praticable. xi, 45, 46

AMDE Analyse des Modes de Défaillances et de leurs Effets. 29, 31–33, 35, 36, 39, 90

AMDEC Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité. vii, xi, 17, 19, 26, 29–32, 36, 39

APR Analyse Préliminaire des Risques. vii, 17, 19, 26–29, 35, 36

DAO Dysfunctional Analysis Ontology. i, viii, xii, 8, 11, 12, 95, 96, 101, 108–110, 113–115, 119, 125, 126, 138, 148, 151, 159, 164, 179–181, 208

EAST-ADL Electronics Architecture and Software Technology-Architecture Description Language. 28

ERA European Union Agency for Railways. 45

FDMS Fiabilité, Disponibilité, Maintenabilité et Sécurité. xi, 20, 22, 23, 41–43

GAME Globalement Au Moins Equivalent. 45, 46

GORO Goal-Oriented Requirements Ontology. 9, 76, 146, 148, 180

GOSMO Goal-Oriented Safety Management Ontology. i, viii, ix, xii, xv, 9, 12, 141, 142, 151, 156, 157, 159, 162–164, 176, 177, 180, 181

HAZOP HAZard and OPerability. vii, xv, 17, 19, 26, 29, 33–36

IC Ingénierie des connaissances. 8, 11, 70–74, 99

IE Ingénierie des Exigences. vii, xv, 5–8, 11, 50, 51, 53–60, 62, 63, 66, 68, 86–88, 90, 96, 142–145, 157, 173

IEBM Ingénierie des Exigences Basée sur les Modèles. vii, 11, 53, 63, 64, 68

IEDB Ingénierie des Exigences Dirigée par les Buts. i, viii, 9, 11, 12, 66, 76, 87, 139, 141–144, 146, 148, 151, 152, 154, 155, 157, 158, 168, 173, 177, 179, 180, 208

IS Ingénierie Système. 54, 55, 57, 63

KAOS Keep All Objectives Satisfied. 66, 87, 145

LD Logiques Descriptives. 79

MEM Minimum Endogenous Mortality. 45, 46

MSC Méthodes de Sécurité Communes. 45

OCL Object Constraint Language. 28

Or-BAC Organization Based Access Control. i, viii, ix, 9, 12, 141, 142, 149–153, 155, 180, 181, 208

OWL Web Ontology Language. i, 9, 79, 90, 106, 119, 177, 179, 208

RAMS Reliability, Availability, Maintainability and Safety. 20

RPN Risk Priority Number. 31

SABiO Systematic Approach for Building Ontologies. xi, 8, 85, 98–101, 109, 138, 146, 151, 162, 179

SCS Systèmes Critiques de Sécurité. i, vii, viii, xi, 3–7, 9–12, 18, 19, 22, 26–29, 31, 32, 37, 49, 53–92, 95–139, 141–177, 179, 181, 208

SdF Sûreté de Fonctionnement. vii, 3, 10, 17–24, 111, 112, 179

SIL Safety Integrity Level. 48

THR Tolerable Hazard Rate. 48

UFO Unified Foundational Ontology. i, xii, 8, 76, 102–105, 111–113, 115, 117–119, 152

UML Unified Modeling Language. 28, 36, 55, 60, 65, 67, 68, 103

INTRODUCTION GÉNÉRALE

Contexte

On parle du système critique lorsque celui ci est susceptible de donner lieu à des conséquences inacceptables. Si ces conséquences sont liées à la sécurité, on parle de systèmes critiques de sécurité (SCS). Leur développement constitue un véritable défi dans divers domaines, notamment les domaines du transport, du nucléaire et de l'aérospatial. En effet, les facteurs clés de cette tâche résident dans la rigueur de l'analyse de sécurité ainsi que la cohérence de son intégration dès les premières phases de conception. La sécurité-innocuité, attribut de la Sûreté de Fonctionnement (SdF), représente une propriété primordiale des SCS car les interactions entre leurs composants peuvent conduire à des accidents impactant la vie des personnes, le système et l'environnement. En ingénierie de sécurité, le terme « système » se réfère généralement à la combinaison du système en construction ainsi que l'environnement dans lequel il opère. Ainsi, les préoccupations de l'environnement du système doivent être considérées dans l'analyse de sécurité. D'autre part, l'aspect socio-technique des SCS rend cette activité plus complexe car il nécessite un raisonnement judicieux permettant de diminuer les risques associés.

Par ailleurs, la sécurité est souvent considérée comme coûteuse, tant du point de vue économique que technique. En effet, elle entraîne généralement une complexité accrue du système, une performance opérationnelle réduite et un coût de développement supplémentaire. Cependant, la cause fondamentale de cette situation n'est due à aucune propriété intrinsèque de la sécurité elle-même. Elle relève, au contraire, des décisions majeures prises lors de la conception architecturale, des choix classiques d'ajout de redondances coûteuses, ou des marges de conception excessives pour garantir la sécurité. Dans l'optique d'une aide à la prise des décisions en matière de sécurité, une démarche plus pertinente consiste à intégrer les activités liées à la sécurité dans le cycle de vie du développement du système dès les toutes premières étapes. Cette pratique a été préconisée par les différentes normes de sécurité pour les domaines critiques. L'apport principal de cette thèse est de proposer une approche pour réaliser les activités liées à la sécurité au cours des premières étapes du développement des SCS.

Problématique

Lors de l'intégration des préoccupations de sécurité dès les premières phases de conception, les parties impliquées doivent composer avec des données critiques qui émanent des résultats qualitatifs et quantitatifs de l'analyse des risques. En effet, ces données impactent les décisions ou les contraintes de conception liées à la sécurité. Typiquement, les ingénieurs

sécurité commencent par l'identification des dangers et par le développement de contraintes sur la conception du système permettant d'atténuer ces dangers. Ensuite, l'activité de l'ingénierie de sécurité se poursuit en assurant l'intégration des contraintes de sécurité dans la conception des SCS. Toutefois, les accidents se produisent lorsqu'une contrainte de sécurité est violée par les composants des SCS. En effet, les contraintes de sécurité sont considérées comme des exigences de sécurité de haut niveau qui visent à éliminer ou à atténuer les dangers identifiés. Généralement, une contrainte de sécurité peut être exprimée sous forme de négation d'un danger identifié. Malheureusement, ce simple lien de négation entre le danger et les contraintes de sécurité ne fournit pas des indications suffisantes aux ingénieurs système pour la mise en œuvre de mécanismes d'atténuation.

D'autre part, s'assurer du maintien des contraintes de sécurité lors de la conception du système est une tâche difficile, notamment dans le cadre du développement des systèmes socio-techniques complexes, comme les SCS. Concernant les systèmes ferroviaires, le raisonnement en matière de sécurité repose sur trois parties principales, tel que, les installations techniques, les interventions humaines et les contraintes organisationnelles en relation avec l'environnement opérationnel. Dans un premier temps, les ingénieurs sécurité effectuent souvent leurs analyses sans liens avec les ingénieurs système, qui prennent des décisions critiques en matière de conception. Les résultats des analyses de sécurité sont souvent présentés comme des critiques de conception et encore plus souvent trop tard. Ces informations sont fréquemment ignorées ou rationalisées car la modification de la conception à une étape avancée du processus est coûteuse et chronophage. D'où l'intérêt de s'appuyer sur les informations communiquées par les ingénieurs sécurité pour établir un lien avec les exigences de sécurité du système à un stade précoce de la conception. La figure 1 met en avant la diversité disciplinaire des acteurs impliqués dans le développement des SCS. En outre, les différentes activités sont dépendantes et nécessitent un vocabulaire commun afin de mener à bien le processus de développement. Néanmoins, chaque partie a son propre vocabulaire et ses propres interprétations sémantiques liés à ses connaissances du domaine. Au vu de la différence des points de vues des ces parties, la partage des connaissances doit reposer sur une base sémantique homogène. En d'autres termes, l'efficacité de la communication relève de la qualité des informations complètes et non ambiguës qui servent de fondement au raisonnement entre les parties impliquées dans le développement des SCS.

Dans ce contexte multidisciplinaire du développement, les ingénieurs sécurité, les ingénieurs des exigences et les experts du domaine doivent communiquer et partager les connaissances afin d'éviter les conflits d'interprétation, et par conséquent, les erreurs de conception fondamentales. Par ailleurs, les besoins de la logique métier du domaine d'application doivent être définis et intégrés dans le processus de la prise de décisions de sécurité. L'hétérogénéité des sources de données utilisées ainsi que le vocabulaire associé peut engendrer des ambiguïtés sémantiques ayant un impact majeur sur la communication entre les équipes. Ce problème de communication des informations de sécurité aux

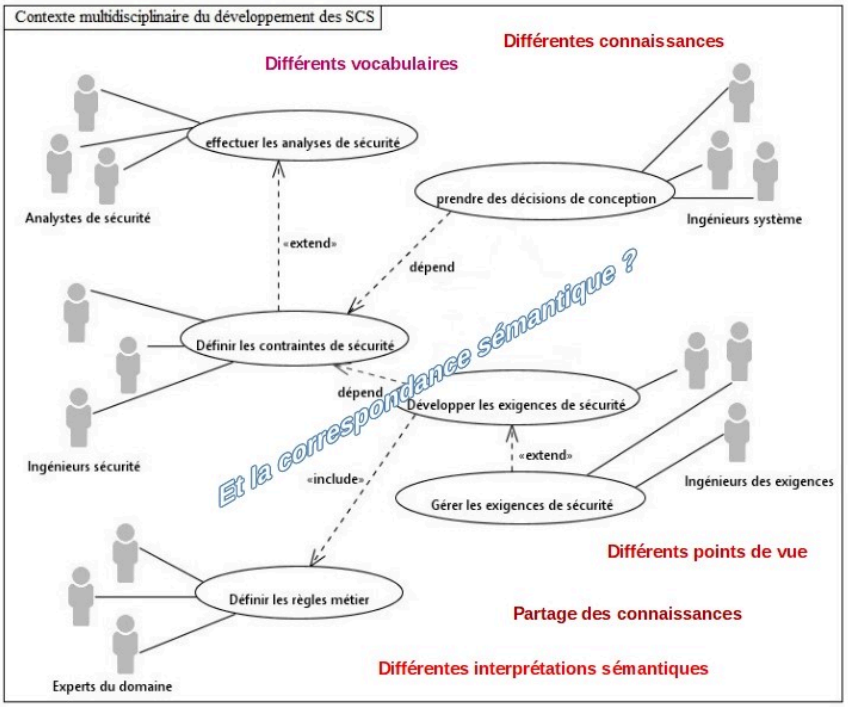

Figure 1 – Contexte multidisciplinaire du développement des SCS

ingénieurs des exigences est exacerbé lorsque l'effort d'ingénierie est réparti entre plusieurs organisations. Par conséquent, un alignement sémantique entre les différents points de vue est nécessaire afin de fournir un vocabulaire commun non ambigu et une interprétation unique des connaissances partagées. Il s'agit d'un enjeu majeur du processus collaboratif de développement qui contribue à l'aide à la prise des décisions de sécurité et de conception.

Motivations & Objectifs de recherche

Dans le cadre de cette thèse, nous nous intéressons à la problématique d'hétérogénéité sémantique dans le cadre du développement des SCS. D'une part, il est primordial de définir les contraintes scientifiques qui exigent un cadre structuré de partage de connaissances pour délivrer un système conforme à ses attendus en terme de sécurité. D'autre part, les contraintes industrielles liées au contexte d'application, à savoir le domaine ferroviaire, dans lequel cette thèse est menée, nécessitent une attention particulière lors de l'intégration des informations critiques de sécurité dans les premières activités de l'Ingénierie des Exigences (IE). Le domaine ferroviaire se distingue par diverses spécificités, à savoir la diversité de ses composants : des opérateurs humains, des dispositifs techniques ainsi que des procédures qui harmonisent le mode opératoire. Cet aspect socio-technique rend la tâche de gestion des décisions de sécurité plus difficile. Par conséquent, la cohérence de ces décisions avec les exigences de sécurité représente un défi lors des premières phases de conception.

Dans les pratiques actuelles du développement des SCS, l'analyse de sécurité est généralement basée sur le retour d'expérience (REX) du développement des systèmes antérieurs, l'application des méthodes d'analyse dysfonctionnelle et l'analyse des modèles dynamiques du comportement du système, comme les diagrammes de séquence, qui ne peuvent pas être obtenus dès les premières phases de conception. En outre, le développement des systèmes ferroviaires met en jeu plusieurs parties ayant des connaissances multidisciplinaires dont chacune s'appuie sur les normes et les référentiels liés aux domaines de compétence. En suivant le flux d'activités d'analyse de sécurité partant de l'identification des dangers et de l'analyse des causes et des conséquences jusqu'à la proposition des choix de sécurité qui mitigent ces dangers, les méthodes d'analyse dysfonctionnelle sont appliquées séparément de l'activité de l'IE.

Afin d'unifier la compréhension et l'interprétation des données, il est nécessaire d'établir une harmonisation sémantique entre les différents points de vue. L'analyse terminologique des concepts associés à l'analyse dysfonctionnelle tels que « défaillance », « causes », « conséquences », « danger », « accident » conduit à des ambiguïtés sémantiques. Bien que ces termes soient en corrélation avec l'intuition humaine, il reste nécessaire d'ajouter des contraintes sémantiques à la relation de causalité dans la sémantique du monde réel. Ces contraintes permettent de définir les types d'entités du monde réel pouvant être connectées par une relation de causalité. Par ailleurs, elles expliquent la manière dont les entités du monde réel coopèrent pour que la relation de causalité soit vraie. Ces considérations nous incitent à formuler l'objectif de recherche comme suit :

OR1 : *Comment faire face à l'ambiguïté sémantique des termes d'analyse dysfonctionnelle pour identifier des contraintes de sécurité pertinentes dans le cadre du développement des SCS ?*

Une compréhension harmonisée des causes et conséquences des dangers ainsi que des concepts liés à l'aspect socio-technique des SCS et leur environnement permet une meilleure conduite du développement des décisions de sécurité. Afin d'assurer la cohérence entre les décisions de sécurité et les exigences de sécurité, il convient de raisonner sur un modèle commun qui incorpore les connaissances des différents domaines. Ainsi, ce modèle partagé doit respecter différentes propriétés comme la modularité, l'abstraction, l'expressivité sémantique et l'interprétation par la machine. En effet, ces caractéristiques constituent des atouts pour la collaboration multidisciplinaire entre les acteurs où chacun contribue avec son expertise spécifique. De plus, la version interprétable par la machine fournit un support de raisonnement et d'aide à la prise de décisions de sécurité. Dans ce contexte, nous définissons un deuxième objectif de recherche :

OR2 : *Quel type de modélisation serait capable d'établir un pont sémantique entre l'analyse de sécurité et l'IE pour éviter les erreurs de conception qui conduisent à l'occurrence des dangers ?*

Une fois l'alignement établi entre les connaissances des deux domaines, la gestion des décisions de sécurité nécessite un cadre permettant de développer ces décisions et de les maintenir en cohérence avec les exigences de sécurité. Les besoins des SCS, tels que les systèmes ferroviaires, exigent une gestion dynamique des décisions qui s'adapte au contexte opérationnel et qui satisfait les buts de sécurité de haut niveau. Entre les décisions de sécurité, les exigences de sécurité et les buts de sécurité, une désambiguïsation terminologique et une interprétation sémantique des liens sont des besoins incontournables. Dans ce contexte, l'ensemble des concepteurs ont besoin d'un formalisme de gestion de sécurité qui permet de faire face au contexte dynamique et au contrôle organisationnel des SCS. Ceci nous amène à un nouvel objectif de recherche :

OR3 : *Quelle implémentation du modèle serait adaptée au contrôle et à la gestion de sécurité guidés par les buts de sécurité au sein de l'organisation pour les SCS ?*

L'adaptabilité des décisions de sécurité aux différents contextes entraîne des évolutions au niveau des exigences de sécurité et des relations avec les autres concepts de l'IE. Cet aspect émergent de la sécurité exige un cadre structuré qui réponde aux différents enjeux de la gestion des exigences, à savoir les relations de la hiérarchie et du raffinement, la satisfaisabilité des exigences et la cohérence du modèle de conception. Par conséquent, la gestion de l'évolution des exigences de sécurité qui émanent de ces décisions doit maintenir la traçabilité des exigences et la cohérence entre elles. Ce cadre structuré doit fournir une base de raisonnement et de vérification qui réponde aux enjeux définis auparavant. De ce fait, un dernier objectif apparaît à ce stade et nous le formulons comme suit :

OR4 : *Comment faire face à la complexité de la gestion des évolutions des exigences de sécurité pour maintenir la cohérence globale de l'architecture des SCS ?*

Après avoir introduit le contexte, la problématique et les motivations de la thèse, une série d'objectifs de recherche est élucidée pour cerner le périmètre de la thèse et orienter les propositions qui permettent de les satisfaire. En effet, ces objectifs de recherche seront affinés en questions de recherche, au fur et à mesure, après l'exploration des différentes pistes pour mener à bien les travaux. Les principales propositions de cette thèse, en réponse aux objectifs définis précédemment, sont introduites dans le paragraphe suivant.

Contributions

Après une analyse extensive de l'état de l'art et des méthodes d'analyse dysfonctionnelle, nous constatons que la mise en relief d'une vue interopérable des différentes notions liées à la sécurité mène à la proposition de décisions de sécurité satisfaisantes. Autrement-dit, une représentation structurée des différentes connaissances liées au développement

des SCS permet de fournir une interopérabilité sémantique qui améliore la conformité des décisions de sécurité proposées aux besoins prédéfinis. Par ailleurs, un cadre sémantique cohérent doit être établi entre les connaissances de l'analyse de sécurité, du développement des contraintes de sécurité et des exigences de sécurité afin de résoudre le problème de l'hétérogénéité sémantique qui émane de l'interdisciplinarité des parties impliquées.

Afin de faire face aux ambiguïtés sémantiques, il y a un besoin clair de conceptualiser les connaissances liées à l'analyse de sécurité des systèmes en prenant en compte les différents facteurs qui impactent la sécurité. On entend par « conceptualisation » une modélisation abstraite d'une réalité ou d'un domaine spécifique. Elle constitue une étape incontournable de l'Ingénierie des Connaissances (IC), thématique principale des contributions de cette thèse. La notion clé de cette discipline est l'**ontologie**, qui est une représentation structurée d'une conceptualisation partagée [Gruber, 1993]. Les ontologies présentent un véritable intérêt dans notre contexte de travail car elles comblent les lacunes de l'hétérogénéité sémantique et clarifient la terminologie utilisée. Par ailleurs, la considération des préconisations fournies par les normes des domaines concernés, tels que les normes ferroviaires et les référentiels des pratiques de développement des systèmes, est requise.

Afin de répondre à l'**OR1**, nous proposons une ontologie du domaine d'analyse dysfonctionnelle (DAO) permettant de lever les verrous scientifiques identifiés et de répondre aux contraintes industrielles du domaine d'application. Elle est développée en utilisant l'approche systématique SABiO [de Almeida Falbo, 2014] et elle contribue à la clarification conceptuelle en mettant à plat les concepts du domaine et leurs relations. La conceptualisation des connaissances d'analyse dysfonctionnelle ainsi que leurs interprétations sémantiques s'appuient sur l'acquisition des définitions fournies par les textes normatifs. En effet, leur interprétation dans la sémantique du monde réel améliore la qualité pragmatique du modèle car elle permet d'analyser la terminologie du domaine d'analyse dysfonctionnelle au regard d'une ontologie de haut niveau. Diverses ontologies fondamentales existent dans la littérature et les caractéristiques du domaine d'analyse dysfonctionnelle ainsi que le contexte d'application nous incitent à choisir l'ontologie Unified Foundational Ontology (UFO), comme une base fondamentale de DAO.

Le choix d'une ontologie de haut niveau pour le développement d'une ontologie de domaine est une bonne pratique préconisée par les référentiels d'Ingénierie Ontologique et les experts du métier, notamment pour résoudre les problèmes d'hétérogénéité sémantique entre plusieurs connaissances de domaines [Schulz, 2018], [Nardi *et al.*, 2013], [Guizzardi *et al.*, 2012], [Guarino, 1998]. Mis à part cet avantage qui augmente la qualité sémantique de la représentation des connaissances, l'utilisation d'une ontologie fondamentale permet d'harmoniser la compréhension et de fournir une vue partagée. En effet, l'alignement sémantique entre les domaines d'analyse de sécurité et l'IE est établi au regard d'UFO pour répondre à l'**OR2**. Le concept des mesures de sécurité, qui représente les contraintes

de sécurité de haut niveau issues de l'analyse dysfonctionnelle, est relié aux concepts de l'Ingénierie des Exigences Dirigée par les Buts (IEDB) tels que le but, l'agent, l'exigence et la tâche. Les concepts de l'IEDB sont acquis à partir du modèle de référence GORO [Negri *et al.*, 2017], qui est fondé sur UFO et fournit une vue interopérable des approches d'IEDB. Les liens structurés entre les concepts des domaines permet de fournir un contrôle de sécurité dirigé par les buts de sécurité et de valider leur satisfaction pour s'assurer de l'absence de conflits de conception dès les premières phases.

L'interprétation des contraintes de sécurité d'une perspective orientée-but permet d'assurer la cohérence avec les exigences de sécurité à un niveau plus concret dans la hiérarchie des exigences. Dans le contexte organisationnel des SCS, il est judicieux d'intégrer un formalisme de gestion des décisions de sécurité qui s'adaptent au contexte dynamique. En explorant la littérature, nous constatons l'existence d'un modèle de contrôle d'accès dans le contexte des Systèmes d'Information qui est en mesure de satisfaire les besoins de notre contexte métier. Il s'agit du modèle de contrôle d'accès appelé, Organization-Based Control Acces (Or-BAC) [Abou EL Kalam, 2003] qui gère les politiques de sécurité pour assurer la *sécurité-confidentialité*. L'idée principale est de réinterpréter les concepts du modèle Or-BAC pour adapter ses caractéristiques au profit de la gestion orientée-but des décisions de la sécurité ferroviaire. En effet, les concepts fournis par ce modèle sont intéressants pour répondre à l'**OR3** et aux besoins de la gestion des décisions de sécurité ferroviaire par analogie des deux domaines. La réinterprétation d'un point de vue *sécurité-innocuité* des concepts de ce modèle, tels que rôle, organisation, contexte, sujet, activité et permission est établie au regard de l'ontologie fondamentale UFO, des besoins du domaine ferroviaire et des concepts de l'IEDB. Principalement, la gestion des décisions de sécurité est structurée par l'attribution des rôles aux acteurs du système socio-technique, à savoir des dispositifs techniques et des acteurs humains par l'organisation. Ensuite les permissions sont accordées à ces rôles pour réaliser une activité qui satisfasse les buts de sécurité.

Ceci nous amène à la deuxième contribution de cette thèse, le développement de l'ontologie de gestion de sécurité orientée-but GOSMO. Il s'agit d'une ontologie à multi-vues qui permet de conceptualiser le partage des connaissances du modèle Or-BAC, de la gestion de sécurité et de l'IEDB. À l'instar du développement de DAO, GOSMO est fondée sur UFO afin d'aligner les deux ontologies et d'avoir un cadre structuré et cohérent. Par ailleurs, la validation des contraintes du métier est effectuée avec l'illustration des deux ontologies sur des cas d'étude ferroviaires représentant des scénarios d'accidents réels et d'une mission ferroviaire télé-opérée. Dans la phase d'implémentation des deux ontologies, le langage formel d'ontologie, Web Ontology Language (OWL), est choisi pour fournir une version opérationnelle et avoir un haut niveau d'expressivité sémantique. En effet, cette version implémentée en OWL représente une base de raisonnement grâce aux axiomes formulés permettant d'extraire des données, d'inférer de nouvelles connaissances et d'établir des annotations sémantiques des données réelles. Ce cadre sémantique structuré nous permet

de formaliser des axiomes permettant de poser des contraintes sur la gestion des exigences et leur traçabilité à l'issue du processus de gestions de sécurité. La traçabilité des exigences, leur satisfaisabilité et la cohérence entre elles sont des enjeux majeurs qui doivent être considérés à un stade précoce du développement des SCS. La série d'axiomes liés aux concepts de GOSMO, notamment l'exigence de sécurité, le but de sécurité et le contexte répond à l'**OR4** et traite les évolutions des exigences.

Afin d'établir le fil conducteur vers la présentation de nos contributions, nous décrivons la structure de ce mémoire en s'appuyant sur la figure 2 qui illustre la logique suivie.

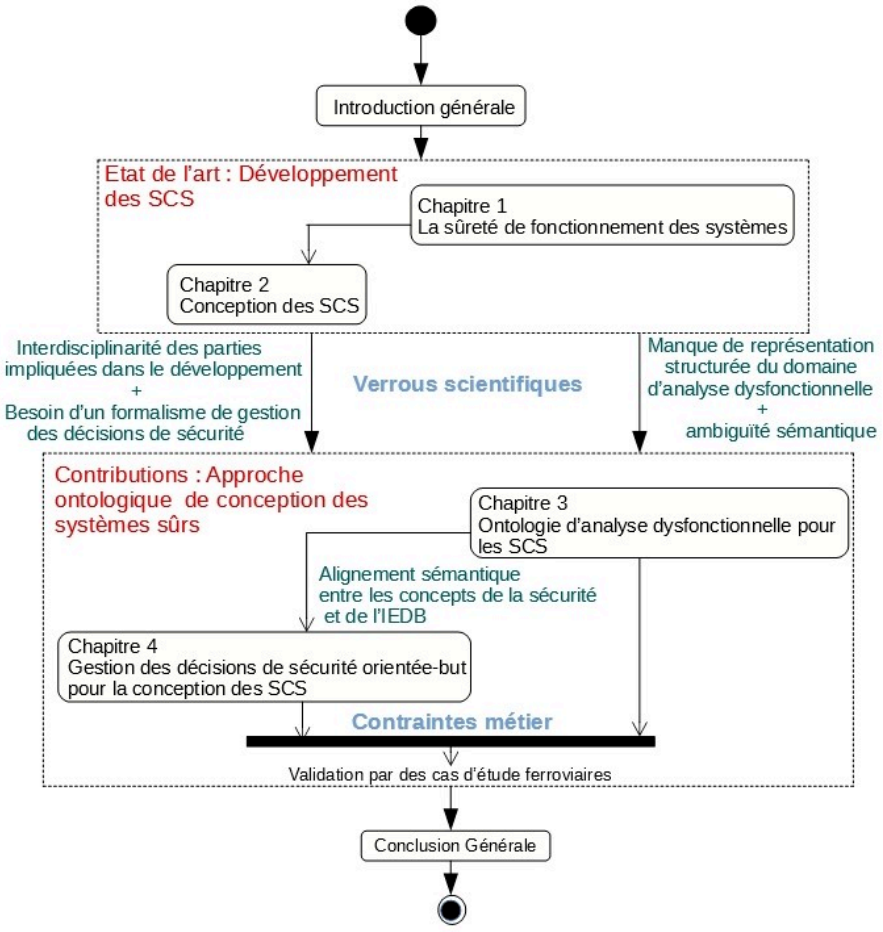

Figure 2 – Logique suivie pour structurer le mémoire

Structure du mémoire

Nous divisons ce manuscrit en deux parties : la première partie est consacrée à l'état de l'art concernant les différentes disciplines de la thèse, et la deuxième partie représente les contributions.

Le chapitre 1 représente la sûreté de fonctionnement (SdF) qui est un objectif central et critique du développement des SCS. Nous discutons les fondements de la SdF et nous

définissons ses différents attributs ainsi que l'objectif de leur analyse pour évaluer les performances des SCS. Ensuite, nous nous focalisons sur l'attribut « sécurité-innocuité » qui constitue le noyau structurant nos contributions. Afin de clarifier ses différents concepts et pour décrire le principe de l'analyse de sécurité, nous avons recours aux définitions fournies par les textes normatifs d'analyse de sécurité. Par ailleurs, nous introduisons les étapes de démonstration de sécurité et nous abordons les méthodes d'analyse dysfonctionnelle permettant de mener à bien l'analyse de sécurité. Ainsi, un état de l'art des méthodologies portant sur l'application de ces méthodes pour le développement des SCS ainsi que des outils proposés pour automatiser les processus sont discutés. Dans un deuxième temps, nous présentons les pratiques d'analyse de la sécurité ferroviaire qui représente le contexte d'application de cette thèse. Nous commençons par identifier les besoins du domaine ferroviaire et le cadre normatif du métier. Ensuite, nous déterminons les facteurs impactant l'analyse de sécurité pour les intégrer dans nos contributions. Nous finalisons ce chapitre en mettant l'accent sur le cadre réglementé de la gestion de la sécurité ferroviaire pour déduire les considérations permettant d'atteindre un niveau de sécurité acceptable dans le cadre du développement de SCS.

Le chapitre 2 présente la conception des SCS, cadre de cette thèse. Nous commençons par introduire la discipline de l'IE qui joue un rôle important dans l'obtention d'un système conforme à ses exigences. Nous nous intéressons à son intérêt pour la considération des préoccupations de sécurité dès les premières phases de conception. À l'issue de la définition des phases et des concepts de l'IE, nous mettons en exergue l'Ingénierie des Exigences Basée sur les Modèles (IEBM) qui représente divers avantages pour faire face aux conflits de compréhension et de réduction de la complexité du problème. Cette discipline nous amène à l'introduction de l'Ingénierie des Exigences Dirigée par les Buts (IEDB). Ensuite, nous passons à un niveau plus abstrait de modélisation, à savoir l'IC, pour présenter les ontologies, leur types et leur caractéristiques. Nous entamons la dernière partie de ce chapitre par l'ingénierie ontologique, son principe et ses objectifs pour tirer profit des bonnes pratiques. Nous abordons un état de l'art des principales contributions dans le développement des ontologies des domaines, tels que l'IE, le domaine ferroviaire et l'analyse de sécurité des SCS.

Le chapitre 3 décrit la première contribution de cette thèse qui se focalise sur le développement de l'ontologie d'analyse dysfonctionnelle DAO pour la conception des SCS. Nous commençons par définir les contraintes industrielles à prendre en compte lors de l'intégration de l'analyse dysfonctionnelle dans la conception des SCS. Ensuite, nous arguons le choix du cadre méthodologique qui répond aux verrous scientifiques et technologiques identifiés. À l'issue de ces choix, nous détaillons les phases du développement de DAO partant de l'identification des exigences attendues jusqu'à leur vérification. Afin de valider l'aspect métier, nous validons DAO avec deux cas d'étude ferroviaires tels

que le scénario d'accident de *Longueville* et celui de *Saint-Romain-En-Gier*. L'annotation sémantique de ces deux situations critiques et réelles justifie la validité de DAO, sa flexibilité et son intérêt à être intégrée dans la conception des systèmes ferroviaires pour éviter les accidents. Nous terminons ce chapitre par une discussion des caractéristiques de DAO et de ses différentes réutilisations pour d'autres cas d'études ferroviaires.

Le chapitre 4 présente l'approche ontologique de la gestion des décisions de sécurité orientée-but qui est proposée pour la conception des SCS. Nous discutons, tout d'abord, les différentes approches de l'IEDB pour justifier un choix méthodologique qui satisfasse nos objectifs de recherche. Ensuite, nous introduisons les motivations de la réinterprétation du modèle Or-BAC pour établir un formalisme de gestion de la sécurité ferroviaire par analogie avec la sécurité des systèmes d'information. Après l'identification d'un cadre méthodologique cohérent, nous détaillons les étapes du développement de GOSMO partant de l'identification de ses objectifs et la réinterprétation des concepts du modèle Or-BAC du point de vue sécurité jusqu'à l'évaluation de ses compétences. Ensuite, nous entamons la phase de validation de GOSMO par les deux scénarios d'accidents considérés auparavant ainsi qu'une mission ferroviaire télé-opérée inspirée des systèmes autonomes. Par ailleurs, nous discutons les contributions de GOSMO permettant de mettre en relief sa valeur ajoutée pour la gestion de sécurité des SCS. Enfin, nous introduisons les axiomes permettant d'assurer la gestion structurée des exigences et leur traçabilité afin d'assurer leur cohérence globale.

La dernière partie de ce manuscrit se consacre à la conclusion générale en récapitulant les caractéristiques majeures de nos contributions et en envisageant des perspectives scientifiques au service de l'innovation industrielle, notamment pour le développement des systèmes autonomes.

Publications et valorisation des travaux de thèse

Revues internationales

- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019). « Towards Semantic Interpretation of Goal-oriented Safety Decisions based on Foundational Ontology ». *Journal of Computers*, 14(4) :257-267.
- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019). « A Model-based System Engineering Approach to Manage Railway Safety-related Decisions ». *International Journal of Transport Development and Integration*, 3(1) :30-43.
- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2018). « An Ontological Approach to Support Dysfunctional Analysis for Railway Systems Design ». *Journal of Universal Computer Science (J.UCS)*, 30p. (Accepté sous réserve de modifications)

Conférences internationales

- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019). « Conceptual Modelling of the Dynamic Goal-Oriented Safety Management for Safety Critical Systems ». *In Proc. ICSOFT 2019-14th International Conference on Software Technologies - Volume 1*, 287-297, July, Prague, République Tchèque.
- de Almeida Pereira, D. I., Debbech, S., Perin, M., Bon, P. et Collart-Dutilleul, S. (2019). « Formal Specification of Environmental Aspects of a Railway Interlocking System Based on a Conceptual Model ». *In Proc. ER 2019-38th International Conference on Conceptual Modeling*, A. H. F. Laender et al. (Eds.) : LNCS 11788, pp. 338–351, November, Salavdor, Brésil.
- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2018). « Towards Semantic Interpretation of Goal-oriented Safety Decisions based on Foundational Ontology ». *11th International Conference on Computer Science and Information Technology*, December, Paris, France.
- Debbech, S., Bon, P. et Collart-Dutilleul, S. (2018). « Improving safety by integrating dysfunctional analysis into the design of railway systems ». *In Proc.16th International Conference on Railway Engineering Design & Operation : WIT Transactions on The Built Environment*, 181 :399-411, July, Lisbonne, Portugal.

Rapport de recherche

- Debbech, S., Collart-Dutilleul, S. et Bon, P. (2018). « Cas d'étude de mission ferroviaire télé-opérée ». Rapport de recherche, IFSTTAR - Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux. `https://hal.archives-ouvertes.fr/hal-02020997/`.

Première partie

ÉTAT DE L'ART

Chapitre 1

La sûreté de fonctionnement des systèmes

Sommaire

1.1 Introduction

L'analyse des aspects liés à la sûreté de fonctionnement (SdF) d'un système critique est considérée comme un objectif majeur sur le plan conceptuel et opérationnel [Villemeur, 1988, Mortureux, 2005]. Les systèmes critiques de sécurité (SCS) caractérisent principalement les domaines industriels tels que le domaine ferroviaire, aéronautique, automobile, nucléaire, etc. Dans le cadre de ces travaux de thèse, nous considérons l'aspect sécurité-innocuité (*Safety* en anglais) qui est crucial dans toute analyse de SdF menée tout au long du cycle de développement des systèmes ferroviaires. La sécurité prend en compte les situations critiques qui sont dues aux défaillances techniques et aux erreurs humaines ; mais en aucun cas les menaces d'attaques et d'intrusions liées à la cybersécurité et à la violation de la confidentialité du système. Au vu de la complexité et de l'utilisation répandue des SCS, ces systèmes se distinguent par le grand nombre de liaisons entre leurs composants, rendant les interactions difficilement prévisibles pour les concepteurs. Par conséquent, ils sont sujets aux erreurs et nécessitent la prise en compte des préoccupations de la SdF, en plus des aspects fonctionnels et non fonctionnels dans leur phase de conception. Les différents attributs de la SdF ainsi que les moyens à mettre en œuvre pour diminuer les risques font l'objet d'une démarche systématique et documentée tout au long du cycle de vie des SCS.

Dans ce chapitre, nous nous focalisons sur l'attribut « sécurité », un des indicateurs de la SdF, qui a pour objectif d'éviter l'apparition de situations critiques ou catastrophiques. L'analyse de la sécurité s'appuie principalement sur l'identification des dangers, les causes et les conséquences ainsi que l'analyse des modes de défaillances des composants du système. Elle est menée par un ensemble de méthodes et d'outils capables d'assister le processus de gestion de décisions de sécurité afin de mener le système à un état stable de fonctionnement requis et préserver la vie des personnes et l'environnement.

En effet, l'analyse des dysfonctionnements ou encore l'ensemble des risques encourus par ces systèmes constitue un préalable inéluctable à leur conception. Les méthodes d'analyse dysfonctionnelle, appelées aussi méthodes d'analyse de risques qualitatives, permettent le développement d'un système conforme à ses attendus en terme de sécurité. Ces méthodes constituent un support d'aide à la décision en termes d'identification des dangers, de leurs causes et leurs conséquences, et des relations de causalité entre les différents événements conduisant à l'événement indésirable. Elles permettent d'établir un raisonnement de sécurité pertinent pour le développement des SCS, à travers l'identification des contraintes de sécurité capables de réduire un risque spécifique et leur intégration dans la phase de conception. L'analyse dysfonctionnelle est généralement précédée par une analyse du système afin d'établir d'une façon exhaustive et systématique les relations fonctionnelles nominales du système et de son interaction avec l'environnement. Cette étape préalable à l'analyse dysfonctionnelle est fondamentale pour la compréhension et la description du

fonctionnement global du système.

Ce chapitre a pour objectif d'établir, tout d'abord, un aperçu sur le principe de la SdF et en particulier l'analyse de sécurité. Ensuite, nous abordons les méthodes d'analyse dysfonctionnelle les plus utilisées pour le développement des SCS. Ainsi, nous comparons les démarches d'analyse pour les différentes familles de méthodes distinguées et nous nous focalisons particulièrement sur l'analyse préliminaire des risques (APR), l'analyse des modes de défaillance, de leurs effets et leur criticité (AMDEC), la méthode HAZard and OPerability (HAZOP), ainsi que la méthode de l'arbre des défaillances (AdD), appelée aussi arbre de fautes ou de défauts. Parallèlement, nous évoquons un état de l'art sur les approches existantes pour l'utilisation de ces méthodes d'analyse dysfonctionnelle au cours du développement des SCS. Nous discutons par la suite des limites et des avantages de ces méthodes vis-à-vis de leur degré de pertinence dans le raisonnement de sécurité induit. Le raisonnement de sécurité qui en découle a pour objectif d'identifier les mesures de sécurité qui sont estimées capables de faire face à des situations dangereuses.

En second lieu, nous mettons l'accent sur les systèmes ferroviaires qui font l'objet de notre étude, et notamment sur les besoins du contexte métier qui impactent fortement les décisions liées à la sécurité guidées par des textes normatifs. Ensuite, nous mettons en exergue les pratiques de l'analyse de sécurité ferroviaire. Nous finissons par la mise en lumière de quelques verrous scientifiques qui sont apparus lors de l'intégration de l'analyse dysfonctionnelle dans le cycle de développement des SCS.

1.2 Les fondements de la sûreté de fonctionnement (SdF)

La complexité croissante des SCS, la réduction du coût de conception et d'exploitation ainsi que le maintien du fonctionnement désiré sur le plan opérationnel font de la SdF une activité omniprésente et structurante dans le cycle de développement. Elle est qualifiée comme un incontournable de l'évaluation de la performance des systèmes qui se décline suivant divers attributs comme le coût, le délai, la qualité et les aspects environnementaux et socio-techniques. Bien que les définitions des objectifs de la SdF soient diverses au niveau des termes utilisés dans les domaines d'application, le principe réside en la recherche incontestable d'un compromis entre l'état sûr, les contraintes économiques et la disponibilité du système. La SdF repose principalement sur des outils et des méthodologies systématiques permettant de prévoir, identifier, évaluer et maîtriser les risques, et sur la quantification des caractéristiques des composants du système afin d'évaluer leur conformité dans le temps aux exigences requises.

1.2.1 Concepts de la SdF

En combinant les définitions proposées par [Villemeur, 1988], [Laprie *et al.*, 1995], [Mortureux, 2005] et [Arlat *et al.*, 1996], nous pouvons définir la SdF comme la science

des défaillances qui se construit à travers les caractéristiques de performance du système, à savoir la fiabilité (*reliability*), la disponibilité (*availability*), la maintenabilité (*maintainabilty*) et la sécurité (*safety*). En effet, ces caractéristiques, formant l'acronyme FDMS (RAMS en anglais), permettent de placer et justifier le niveau de confiance accordé au service délivré dont la qualité doit être maintenue dans le temps. Afin de mieux appréhender la SdF, nous commençons par définir la terminologie des concepts utilisés pour mener une démarche structurée et systématique d'évaluation des performances du système. La figure 1.1 résume les notions liés à la SdF, à savoir les attributs, les entraves et les moyens d'analyse.

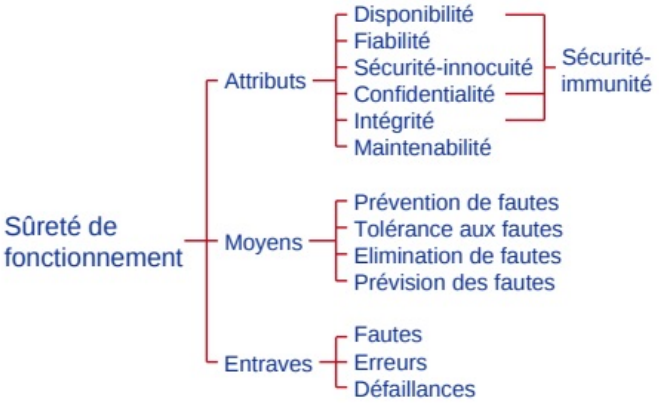

Figure 1.1 – Les lignes directives de la sûreté de fonctionnement [Laprie *et al.*, 1995]

Définition 1 . *(Entraves de la SdF). Conformément à la norme [IEC 61508, Norme Internationale, 2000], les entraves de la SdF constituent les événements qui peuvent affecter la SdF et sont définis comme suit :*

- *la défaillance est définie comme la cessation de l'aptitude d'une entité à accomplir une fonction requise. Autrement dit, la défaillance est observée lorsque le service délivré est différent du service exigé. Elle constitue la conséquence d'un comportement erroné d'un composant/du système.*
- *Ainsi une erreur est définie comme l'écart entre une condition mesurée et la condition théoriquement vraie. De point de vue système, elle est interprétée comme l'état d'un composant/du système susceptible de provoquer une défaillance. Une erreur est causée par une faute dont l'origine est due à un comportement humain ou à un phénomène physique erronés.*

L'ensemble récursif des {*faute*, *erreur*, *défaillance*} constitue les entraves pouvant affecter le fonctionnement du système et dégrader la SdF. Étant par ailleurs dénommée « la science des défaillances », la SdF se focalise sur l'anticipation, l'identification, l'évaluation, la classification et la maîtrise des défaillances.

Les indicateurs de la SdF permettent de définir les objectifs attendus du système et

d'évaluer la qualité de service délivré afin de cibler les améliorations critiques à envisager selon différents points de vue :

- La *fiabilité* représente l'aptitude d'une entité à accomplir une fonction requise dans des conditions spécifiques et pendant une durée donnée. Les conditions spécifiques sont principalement liées aux modes d'utilisation de l'entité impactant la fiabilité, les aspects environnementaux du système et la maintenance.

  La fiabilité peut être mesurée par la probabilité *F(t)* que celle ci accomplisse le service requis dans les conditions données pendant l'intervalle de temps $[0, t]$, sachant que l'entité n'est pas en panne à l'instant *t=0*. La métrique associée à cette probabilité représente la durée moyenne de fonctionnement d'une entité avant sa première panne ou Mean Time To Failure (MTTF) en anglais dont la définition formelle est donnée en 1.1. Ainsi, la durée moyenne entre deux pannes (Mean Time Between Failures (MTBF)) est déterminée pour exprimer la fiabilité globale des éléments réparables du système. La MTBF est mesurée par le rapport entre le temps de fonctionnement total et le nombre de défaillances.

$$MTTF = \int_0^\infty F(t)\mathrm{d}t \tag{1.1}$$

- La *disponibilité* désigne l'aptitude d'une entité à être dans un état permettant d'accomplir une fonction requise dans des conditions données à un instant t ou dans un intervalle de temps déterminé [Villemeur, 1988 ; IEC90]. Elle est caractérisée par la probabilité, à l'instant t, qu'une entité soit en état d'accomplir une fonction requise. Ensuite, la durée moyenne d'indisponibilité après la panne (Mean Down Time (MDT)) est mesurée afin d'identifier des actions d'amélioration de cet indicateur. La durée MDT est égale à la somme du temps de la détection de la panne (TDP), le temps de réparation (TR) et le temps de remise en service (TRS) suivant l'équation 1.2. Afin d'évaluer quantitativement la durée de réparation du système, une durée moyenne de fonctionnement après la réparation (Mean Up Time (MUT)) est calculée. Ainsi, la disponibilité moyenne D_{moy} s'exprime suivant l'équation 1.3.

$$MDT = TDP + TR + TRS \tag{1.2}$$

$$D_{moy} = \frac{MUT}{MDT + MUT} \tag{1.3}$$

- La *maintenabilité* est la capacité d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits [Villemeur, 1988], [IEC, IEC 50191, 1990]. Cet attribut de SdF est mesuré par la probabilité *M(t)* que la maintenance d'une entité s'achève à l'instant t, sachant que l'entité est en panne à l'instant *t=0*. La métrique qui évalue cette probabilité

représente la durée moyenne de réparation ou *Mean Time To Repair (MTTR)* qui est définie dans 1.4.

$$MTTR = \int_0^{\infty} [1 - M(t)] \mathrm{d}t \tag{1.4}$$

Ainsi, le taux de réparation μ est égale à l'inverse de MTTR. Dans le cas où MTTR = MDT, MTBF = MTTF + MTTR. Et si MTTR $\ll$ MTTF, MTBF $\approx$ MTTF (Figure 1.2).

- Selon [Laprie *et al.*, 1995], la *sécurité* est définie comme la sécurité-innocuité, par la capacité d'une entité à ne pas occasionner des événements catastrophiques pouvant affecter les personnes et l'environnement du système dans des conditions et une durée données. Cet attribut de SdF fait l'objet de plusieurs normes des domaines critiques notamment le domaine militaire [MIL-STD, 2002], le transport ferroviaire [CENELEC, NF EN 50126-1, 2017], [CENELEC, NF EN 50129, 2003] et l'électronique [IEC 61508, Norme Internationale, 2000]. De même que les autres attributs de la SdF, la sécurité est caractérisée par la probabilité que l'entité évite les événements catastrophiques ou critiques pendant une durée $[0, t]$. Les préoccupations de sécurité considèrent les dommages impactant le système socio-technique et son environnement. Ainsi, le processus de gestion des décisions liées à la sécurité repose sur un équilibre judicieux entre les contraintes d'efficacité opérationnelle, le coût et le délai.

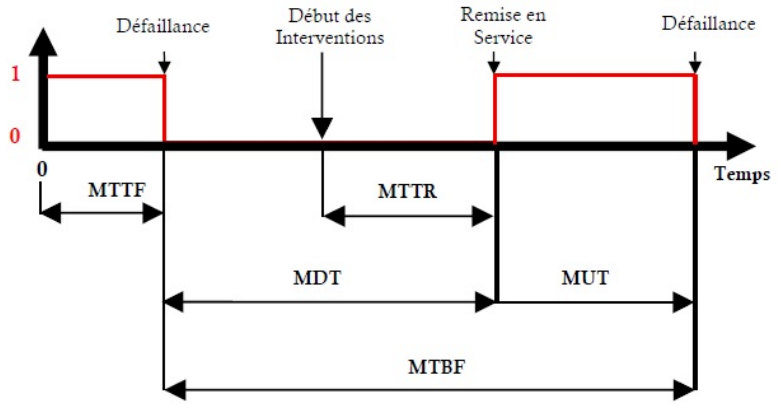

Figure 1.2 – Les indicateurs de temps moyens de FDMS

Dans le cadre de cette thèse, nous nous focalisons sur ce dernier indicateur de SdF afin de mettre en exergue la démarche rigoureuse d'intégration de l'analyse de sécurité dans les premières phases de conception des SCS, en particulier les systèmes ferroviaires. Dans ce mémoire, nous utilisons le terme « sécurité » pour faire référence à la « sécurité-innocuité ». Dès lors que la sécurité ou la disponibilité du système est mise en défaut, sa fiabilité est mise en cause. Ainsi, la maintenabilité intervient en cas de panne du système afin de le remettre dans ses conditions de fonctionnement initial. Enfin, la SdF est considérée comme l'ensemble de méthodes et des outils permettant de spécifier, concevoir, réaliser et

exploiter un système dont les défaillances restent tolérables par rapport aux seuils indiqués par les attributs FDMS.

1.2.2 La dualité sécurité-fiabilité

Les analyses liées à la fiabilité et la sécurité reposent souvent sur les mêmes valeurs de seuil et l'analogie des méthodes utilisées pour construire les démonstrations de sécurité ou de fiabilité est claire. Cette harmonisation des deux attributs de la SdF est illustrée par le regroupement des documents normatifs associés à ces activités sous un même référentiel méthodologique, comme la norme ferroviaire [CENELEC, NF EN 50126-1, 2017] dont l'intitulé est « spécification pour la démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité ». Cependant, les analyses de fiabilité et de sécurité se distinguent par leurs objectifs qui sont détaillés dans le tableau 1.1.

Sécurité	**Fiabilité**
S'applique principalement à un système et se focalise sur les problèmes d'interaction équipement-Homme	S'applique fréquemment à un équipement ou un dispositif technique spécifique
Prend en considération l'être humain comme un élément du système étudié	Ne prend pas en compte, à priori, les facteurs humains
Doit envisager toute combinaison événement-circonstance pouvant conduire à une situation dangereuse	Analyse le bon fonctionnement d'un équipement dans des conditions d'utilisation bien déterminées
Se focalise sur des événements dont le coût est d'un ordre d'ampleur visiblement supérieur à celui du coût normal d'une mission	Se focalise sur des événements dont le coût est du même ordre d'ampleur que celui du coût normal d'une mission
Repose sur de multiples combinaisons d'événements qui ne peuvent pas faire l'objet d'une étude statistique simple car elles sont peu probables	S'intéresse à des événements qui peuvent généralement être capturés par le retour d'expérience et l'étude statistique
Peut être améliorée par de multiples moyens, par exemple l'augmentation de la fiabilité des éléments critiques	Peut entrer parfois en conflit avec les objectifs de sécurité par la nécessité impérieuse des solutions techniques différentes
Utilisent le calcul probabiliste et les méthodes de la statistique	
Se développent par des démarches équivalentes : Détermination de spécifications, mettre en œuvre un véritable plan de qualité, retour d'expérience, recueil et traitements des données techniques...	
Le plan de fiabilité et le raisonnement de sécurité s'appliquent tout au long du cycle de vie du système ou de l'équipement depuis la conception jusqu'à l'exploitation	

Tableau 1.1 – Comparaison des objectifs de l'analyse de sécurité et de fiabilité

La démarche mise en œuvre pour l'analyse de sécurité du système s'appuie dans un premier temps sur la construction proactive de toutes les combinaisons de conditions critiques pouvant conduire à des situations dangereuses potentielles ; et dans un deuxième temps propose des mécanismes de protection afin de préserver les qualités socio-techniques du système et son environnement. Par ailleurs, la préoccupation majeure de l'analyse de fiabilité est l'identification et la maîtrise des défaillances techniques pouvant contribuer indirectement à l'analyse de sécurité du système. Les deux démarches reposent sur la spécification des domaines d'application, les acquis personnels ainsi que les recomman-

dations des référentiels de connaissances normatives. En effet, les objectifs de sécurité et de disponibilité ne peuvent être satisfaits qu'en répondant aux exigences de fiabilité et de maintenabilité tout en mettant en œuvre un contrôle continu des activités de maintenance, d'exploitation et de l'environnement du système. Ainsi, une mauvaise gestion des conflits entre les différentes exigences des attributs peut faire obstacle au développement d'un système sûr, ou en revanche entraîne le développement d'un système tellement sûr qu'il n'est jamais disponible. Afin d'éviter de favoriser les choix liés à un attribut de la SdF par rapport à un autre, chaque démonstration est menée indépendamment tout en respectant les textes normatifs et les objectifs globaux admis par les organisations qui définissent les politiques du domaine.

1.2.3 Le principe de l'analyse de sécurité

La sécurité est fondée sur l'identification et la couverture des phénomènes intrinsèques et extrinsèques liés aux défaillances des équipements et aux erreurs humaines. Cette analyse s'appuie essentiellement sur une stratégie de conception et développement afin de lutter contre les défaillances, réduire les incidences des erreurs humaines et minimiser les risques résiduels. Un ensemble de techniques d'analyse et de méthodologies est utilisé afin d'assurer la cohérence globale des solutions mises en application. La construction de la cohérence globale passe, à notre avis, par une phase d'harmonisation sémantique et cette harmonisation est une contribution majeure de cette thèse.

La norme MIL-STD-882 [MIL STD 882, 2002] introduit la sécurité d'un système comme « égale au degré de sécurité optimale compatible avec les contraintes d'efficacité opérationnelle, les coûts et les délais, et qui doit être obtenu par application systématique des principes de sécurité (conception et conduite) au cours des phases successives de la vie du système ». Cette définition semble être claire et facile à comprendre ; mais quand nous nous penchons davantage sur sa signification, elle révèle toute la complexité et la criticité de la tâche de l'évaluation du niveau de sécurité acceptable. Celle-ci résulte, d'ailleurs, d'un compromis entre les connaissances capitalisées à un instant donné et le contexte économique dans lequel opère le système. Ainsi, la détermination du niveau de sécurité requis revient à déterminer le niveau de risque acceptable qui est la pierre angulaire de tout raisonnement de gestion de décisions de sécurité liées aux risques envisagés [IEC 61508, Norme Internationale, 2000, CENELEC, NF EN 50126-1, 2017]. Ce processus permet de définir le niveau qualitatif et quantitatif des moyens et méthodes à mettre en œuvre durant le cycle de vie du système.

Avant même d'introduire les méthodes d'identification des risques et l'analyse des défaillances, nous commençons par appréhender la détermination du niveau d'acceptabilité de sécurité. Étape capitale du raisonnement de sécurité, elle consiste à établir des seuils tolérables ou non de probabilité d'un danger en fonction de la gravité de ses conséquences. Selon la norme ferroviaire [CENELEC, NF EN 50129, 2003], la sécurité est définie comme

l'absence des risques inacceptables.

Définition 2 . *(Risque et danger).*

Par ailleurs, la sécurité est liée aux notions de « risque » et « danger » qui sont généralement considérés comme interchangeables. Cela amène une certaine ambiguïté dans le vocabulaire de l'analyse de sécurité en général. Le danger est défini comme une propriété intrinsèque de toute source potentielle ou une situation physique pouvant causer des conséquences néfastes appelées dommages. Selon le référentiel [ISO 73 : 2009, 2009], un risque est un état ou un ensemble de conditions du système et/ou de son environnement qui entraînent inévitablement un accident. La notion du risque inclut deux facteurs principaux notamment la gravité des conséquences du danger et la fréquence de l'exposition au danger. Ainsi, le risque est défini comme la fréquence d'occurrence des accidents conduisant à des dommages (causés par un danger) et le degré de gravité de ces dommages [CENELEC, NF EN 50126-1, 2017]. Selon la même norme EN 50126, le danger est une condition pouvant conduire à un accident.

Nous introduisons maintenant la notion de niveau d'intégrité de sécurité du système (*Safety Integrity Level SIL*). Ces niveaux caractérisent l'aptitude du système à remplir les fonctions de sécurité requises et servent à caractériser la hauteur de l'effort consenti pour réduire le risque encouru [Summers, 1998], [IEC 61508, Norme Internationale, 2000]. Ils s'appliquent principalement aux systèmes critiques et spécifient le risque maximum tolérable par heure de fonctionnement. En effet, le principe de l'intégrité de sécurité repose sur la manière de contrôle des défaillances systématiques et des défaillances aléatoires relatives à une fonction de sécurité [Beugin *et al.*, 2016]. On entend, d'une part, par défaillance systématique toute défaillance non quantifiable liée de manière déterministe à des causes données dont l'origine est généralement dû à des erreurs humaines durant la phase d'exploitation. D'autre part, la défaillance aléatoire est relative aux défaillances matérielles mettant en cause la fiabilité des composants. Leur évaluation est menée à l'aide des calculs de probabilité connus des modes et des taux de défaillance.

Les SIL sont caractérisés par des indicateurs discrets et matérialisés par une échelle de quatre niveaux. Cette échelle varie entre le SIL4 désignant le niveau le plus haut d'intégrité de sécurité et est lié aux fonctions de sécurité les plus critiques et le SIL1 ayant le plus bas degré d'intégrité de sécurité. De ce fait, une correspondance entre les contraintes et obligations des organisations, les méthodes de conception et d'essais et les approches qualitatives non quantifiables est établie à chaque niveau de SIL. La notion de SIL a fait l'objet de plusieurs normes notamment pour les systèmes de défense [STAN 00-56, 1996] et pour les systèmes électroniques programmables [IEC 61508, Norme Internationale, 2000]. Cette dernière a été déclinée pour les systèmes ferroviaires [CENELEC, NF EN 50129, 2003]. La définition des niveaux de SIL par ces normes est représentée dans le tableau 1.2.

SIL	EN 50129 et IEC 61508	DEF STAND 00-56
4	$10^{-9}/\text{h} \leq < 10^{-8}/\text{h}$	Lointain $\approx 10^{-8}/\text{h}$
3	$10^{-8}/\text{h} \leq < 10^{-7}/\text{h}$	Occasionnel $\approx 10^{-7}/\text{h}$
2	$10^{-7}/\text{h} \leq < 10^{-6}/\text{h}$	Probable $\approx 10^{-6}/\text{h}$
1	$10^{-6}/\text{h} \leq < 10^{-5}/\text{h}$	Fréquent $\approx 10^{-5}/\text{h}$

Tableau 1.2 – Définition des niveaux de SIL par les normes

Le processus de démonstration de la sécurité est reconduit itérativement à chaque phase du cycle de vie. Il se construit par le biais de la justification et de la documentation de preuves de vérification ou de conformité. Au delà de l'application de simples parades technologiques, ce processus est articulé sur un ensemble de décisions afin de garantir la sécurité globale du système. Il convient donc de suivre une démarche systématique et documentée partant de la définition des objectifs requis, l'identification des risques, l'allocation des objectifs de sécurité aux fonctions du système jusqu'à la couverture du risque [Beugin *et al.*, 2016]. Dans la section suivante, nous nous focalisons sur les méthodes d'analyse dysfonctionnelle permettant de trouver et caractériser les combinaisons d'événements pouvant être à l'origine des accidents potentiels.

1.3 Méthodes de l'analyse dysfonctionnelle

L'analyse dysfonctionnelle représente une part importante dans le raisonnement de sécurité pour les SCS car elle constitue un ensemble de méthodes adéquates pour prévoir l'ensemble des défaillances pouvant survenir et identifier leurs causes et leurs conséquences. Bien que l'objectif de toute analyse dysfonctionnelle soit le même, il existe deux familles de méthodes qualitatives qui sont classifiées suivant le sens d'analyse souhaité en une démarche inductive ou déductive. La démarche inductive consiste à l'identification des conséquences d'une défaillance spécifique et inclut notamment l'APR, l'AMDEC et HAZOP. Quant à la démarche déductive, elle vise l'identification des causes d'une défaillance bien définie. La méthode déductive la plus connue et utilisée dans différents domaines est l'AdD.

1.3.1 Analyse Préliminaire des Risques (APR)

L'analyse préliminaire des risques consiste à identifier l'ensemble des événements redoutés ou des dangers et à étudier les situations dangereuses qui pourraient être en causes et en conséquences. Afin de mieux appréhender cette méthode, nous commençons par définir ce qu'est un risque. Bien que le domaine d'application de l'APR varie, l'interprétation du risque reste plus ou moins la même en se basant sur les différents standards de sécurité dans les domaines critiques.

L'APR repose essentiellement sur [Mortureux, 2005] :

— une liste des dangers qui peuvent se conjuguer avec des circonstances pour provoquer des situations dangereuses et par la suite des accidents ;

— la fréquence d'occurrence (O) des événements déclencheurs ou initiateurs d'une situation dangereuse ou un accident ;

— la cotation en gravité (G) des conséquences potentielles prévisibles des dangers.

Cette méthode a pour objectif de prévoir les risques potentiels présentés par un système et de déterminer les mesures permettant de réduire la probabilité d'occurrence des événements dangereux envisageables. L'APR présente essentiellement un intérêt au stade de la conception du système grâce à son analyse permettant de mettre rapidement en évidence les dangers susceptibles d'être rencontrés. Néanmoins, les constations induites par l'APR pourraient être mise à jour tout au long du cycle de développement du système en s'appuyant sur plusieurs facteurs notamment le retour d'expérience des experts du domaine concerné. En effet, la pratique de cette méthode relève particulièrement de l'imagination du constructeur et du savoir-faire des experts. Ces derniers ont pour mission de prévoir les événements indésirables et d'envisager les solutions adéquates, comme des mesures d'atténuation du risque, qui seraient intégrées dans la conception du système sous forme des contraintes de sécurité.

Après la phase d'identification, les mesures de prévention ou d'atténuation du risque tendent à diminuer la fréquence d'occurrence du danger ou à réduire ses conséquences. Ainsi, la notion d'occurrence est fondée sur une mesure ou une estimation et la notion de gravité réfère à la cotation de l'ampleur des conséquences d'un événement par rapport à une échelle de référence. Le produit occurrence-gravité représente une matrice bidimensionnelle qui permet d'attribuer un niveau de risque à un niveau d'acceptabilité (1.5). Le caractère à la fois objectif et subjectif de la qualification du risque permet d'établir leur classification, et par la suite définir les mesures à mettre en place afin d'atteindre le niveau d'acceptabilité requis. En effet, les seuils d'acceptation du risque sont déterminés avant de mener l'APR en s'appuyant sur les directives recommandées par les standards de sécurité du domaine concerné. Cette classification a pour objectif de cerner les critères de décision concernant les choix liés à la sécurité. Souvent cette analyse qualitative nécessite une étude quantitative afin de mieux articuler les contraintes de sécurité dès les premières phases du développement du système, tout en cherchant un compromis entre l'état sûr du système ainsi que ses restrictions de disponibilité ou de coût.

$$R = O \times G \tag{1.5}$$

Les SCS sont impliqués dans divers situations dangereuses qui peuvent engendrer des conséquences graves [Leveson, 2011]. Cette implication est expliquée par le fait que l'ana-

lyse préliminaire des risques inclut deux aspects principaux, à savoir le système cause un risque ou le système est exposé à un risque. Cette distinction doit être considérée durant l'APR menée pendant la conception des SCS, puisqu'elle peut servir comme un support heuristique de négociation pour établir un mécanisme d'atténuation des risques envisagés. Après une série de réunions de concertation, les dangers potentiels sont identifiés, suivis d'une liste d'actions de prévention ou de réduction de la gravité de leurs conséquences [Ericson *et al.*, 2015]. Cependant, l'identification détaillée des éléments dangereux liés aux risques envisagés est une tâche critique car elle nécessite une connaissance approfondie du comportement du système ; ce qui n'est pas forcément possible dans les premières phases de conception des SCS.

En analysant les approches existantes concernant l'APR pour la conception des SCS, nous constatons que la plupart des contributions ont mis l'accent sur la définition des approches systématiques capables d'assister le processus intellectuel d'identification et de classification des risques et définir les moyens de les atténuer ou de les contrôler. Une approche basée sur le langage EAST-ADL a été proposée pour établir l'APR des systèmes embarqués automobiles [Mader *et al.*, 2011]. Étant assistée par un cadre outillé, elle vise à identifier les propriétés indiquant la fiabilité de l'application de l'APR. Ces propriétés sont automatiquement vérifiées en s'appuyant sur un modèle d'analyse qui reflète les résultats de l'APR. Si les propriétés sont violées, l'approche prend en charge l'identification automatisée des solutions possibles et la correction automatique du modèle d'analyse. Dans [Stringfellow *et al.*, 2010], une approche d'analyse des risques des systèmes à logiciel prépondérant critiques de sécurité, appelée STPA (analyse de processus théoriques des systèmes), a été proposée pour une application dans les phases préliminaires du processus de développement. L'approche commence par l'identification des dangers potentiels et les besoins ou contraintes correspondants. Ensuite, les actions de contrôle inadéquates et leurs flux sont identifiés et un processus de gestion et de raffinement des contraintes visant à éliminer, réduire ou atténuer le risque est établi itérativement.

[Johannessen *et al.*, 2004] ont défini une technique appelée l'analyse des risques basée sur les actionneurs, qui peut être utilisée au début du développement et ne nécessite pas une description détaillée du système. L'approche est basée sur l'hypothèse que seuls les actionneurs du système peuvent affecter leur environnement et définit des classes de sévérité à chaque actionneur. Ainsi, le niveau de criticité déterminé permet de choisir les éléments de conception susceptibles de gérer les risques identifiés. D'autres travaux ont fait l'objet de l'utilisation des langages de modélisation notamment UML afin de proposer des méthodologies basées sur les modèles capables d'assister l'APR [Giese *et al.*, 2004, Sandberg *et al.*, 2010]. En combinaison avec l'outil proposé par [Lanusse *et al.*, 2009], l'approche permet la définition des propriétés en utilisant le langage de contraintes d'objets OCL ainsi que leur vérification automatique.

Pour résumer, le consensus obtenu montre que l'APR définit les grandes lignes directrices de l'analyse de sécurité du système nécessitant d'être prises en considération tout au long du cycle de développement du système. Toutefois, elle ne permet pas de caractériser en détail ni l'enchaînement des événements conduisant à un accident majeur, ni la précision terminologique des causes, des conséquences et de leur inter-dépendance. L'APR fournit un service utile mais limité aux hypothèses disponibles sur le système en amont de sa conception. Afin d'affiner les choix de sécurité dans le contexte des SCS, des méthodes faisant l'objet d'analyses plus détaillées comme l'AMDEC, HAZOP et AdD seront utilisées. Sur ce niveau préliminaire de conception d'un SCS, nous proposerons dans ce mémoire d'utiliser des mécanismes d'abstraction pour exprimer des propriétés de sécurité sur les concepts fondateurs du système à concevoir.

1.3.2 Analyse des Modes de Défaillances, de leurs Effets et leur Criticité (AMDEC)

L'AMDEC a été introduite pour la première fois dans le domaine militaire afin d'analyser et hiérarchiser les modes de défaillances et leur impact sur la sécurité des équipements [Lodgaard *et al.*, 2011]. On entend par le terme de défaillance toute inaptitude à délivrer le fonctionnement désiré ou prévu. L'utilisation de cette méthode a eu un succès important dans les domaines industriels notamment les domaines du transport et du nucléaire. L'AMDEC est une démarche inductive qui identifie les modes de défaillances intenses du système, leurs effets et leurs classes de criticité [Briones *et al.*, 2007]. La classification de criticité permet de hiérarchiser les modes de défaillances suivant leur ordre d'importance. La mise en œuvre de l'AMDEC est décrite dans la figure 1.3 conformément à la norme [NF EN 60812, 2006].

Cette analyse est planifiée après une analyse fonctionnelle détaillée afin de mieux étudier les problèmes à l'origine de l'échec de la fonction prévue. En effet, l'analyse fonctionnelle constitue un pré-requis essentiel à l'AMDEC afin de comprendre les interactions des composants et pouvoir effectuer, par la suite, l'analyse les modes de défaillances, leurs causes et leurs effets (AMDE). Après cette analyse qualitative faisant l'objet de l'AMDE, une analyse de criticité est menée afin de quantifier l'impact de la défaillance sur le fonctionnement et la sûreté globale du système. Selon la norme [NF EN 60812, 2006], la criticité d'une défaillance est définie comme la combinaison de la sévérité de son effet et de la fréquence de son apparition. Par ailleurs, la notion de criticité inclut un aspect subjectif (la sévérité de l'effet) et un autre objectif et mesurable (la fréquence) afin de prioriser les défaillances potentielles suivant leur criticité. Ce paramètre contribue à la prise de décisions, concernant les mesures de prévention ou d'atténuation des défaillances anticipées.

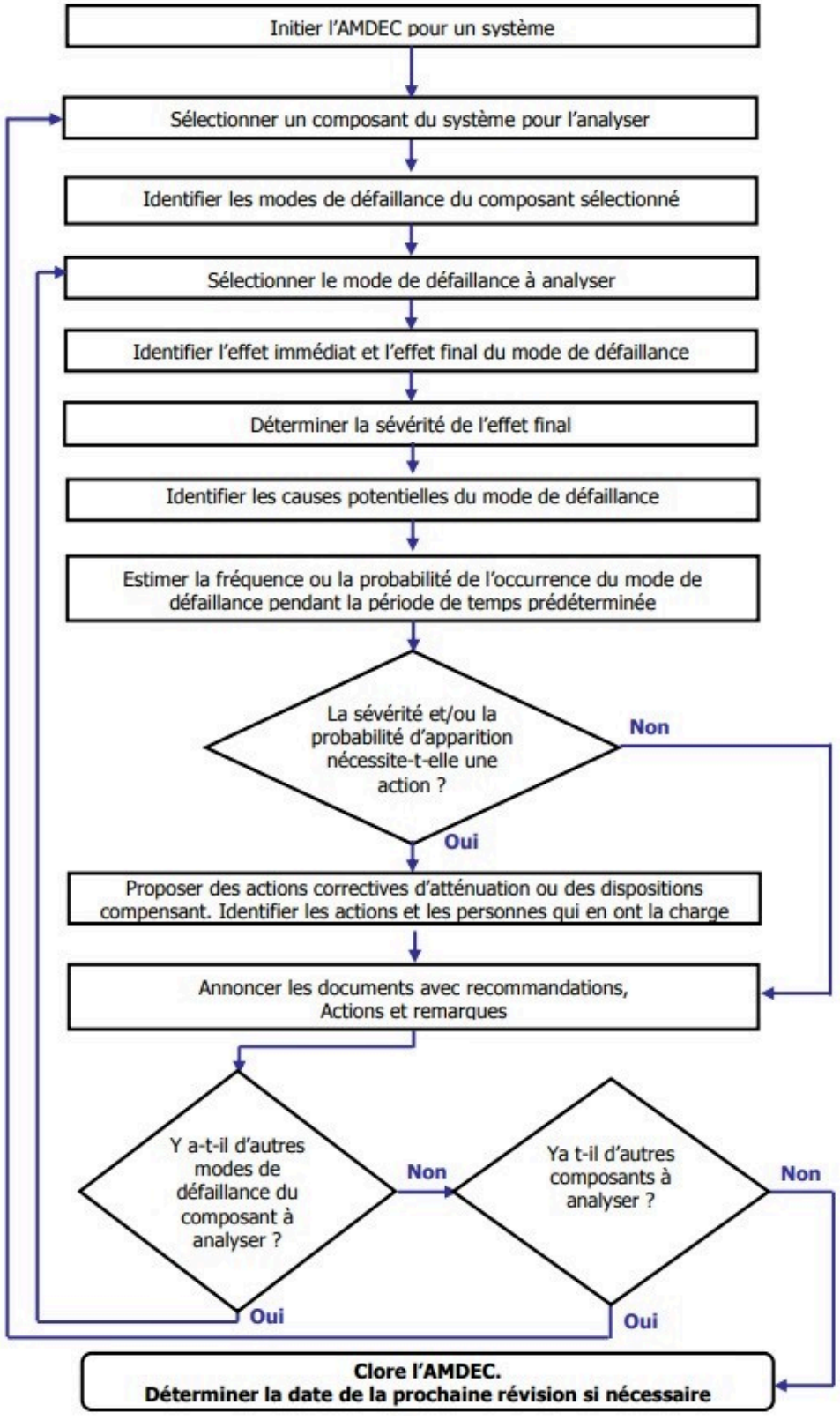

Figure 1.3 – Organigramme de l'AMDEC selon la norme NF EN 60812 [Laronde, 2011]

Après avoir défini les modes de défaillances des composants, une démarche quantitative peut avoir lieu afin d'évaluer les risques associés à chaque mode de défaillance. Cette évaluation consiste au calcul du rang de priorité du risque (*Risk Priority Number* (**RPN**)) en multipliant les taux de **sévérité** (S) de l'effet de la défaillance, de l'**occurrence** (O) de la défaillance, et de la **détection** (D) de la cause ou du mode défaillance avant son apparition. La valeur de RPN varie entre 1 (le meilleur) et 1000 (le pire).

L'avantage principal de cette analyse est son aptitude à prioriser les modes défaillances et définir des actions de mitigation pertinentes suivant la valeur de RPN. Par ailleurs, elle permet d'aboutir à un raisonnement adéquat notamment en cas d'égalité des taux de sévérité de deux ou plusieurs défaillances. Les valeurs de S, O et D varient entre 1 et 10 en utilisant les directives décrites dans le tableau 1.3.

Rang	**Sévérité de l'effet**	**Occurrence de la défaillance**	**Détection**
10	Dangereux	Presque certaine	Presque impossible
9	Potentiel	Très élevée	Négligeable
8	Extrême	Élevée	Très légère
7	Majeur	Moyennement élevée	Légère
6	Significatif	Moyenne	Faible
5	Modéré	Faible	Moyenne
4	Mineur	Légère	Moyennement élevée
3	Léger	Très légère	Élevée
2	Très léger	Négligeable	Très élevée
1	Non	Presque jamais	Presque jamais

Tableau 1.3 – Directives de cotation de la sévérité, l'occurrence et la détection

L'AMDEC a fait l'objet de plusieurs travaux académiques et industriels en termes de méthodologies et outils permettant d'améliorer la stratégie d'évaluation des risques dans le développement des SCS. Les approches proposées visent à lever plusieurs verrous scientifiques et technologiques liés aux résultats qualitatifs et quantitatifs. Afin de développer des systèmes de services robustes, des efforts ont été dédiés à la modification de l'AMDE pour traiter l'évaluation globale des défaillances de chaque fonction du système [Devadasan *et al.*, 2003] et l'intégration de l'AMDE dans la conception robuste comme proposé par [Mekki, 2006]. Cependant, divers défis restent à relever, notamment la modélisation de l'interaction entre l'impact interne de la défaillance du service et l'impact externe sur le système et la comptabilisation des RPN des défaillances de service dans une telle situation. Comme l'analyse des modes de défaillances s'appuie principalement sur une connaissance subjective des multi-attributs acquis des experts du domaine, des méthodologies portant sur la théorie des ensembles flous (*fuzzy sets theory*) ont été proposées afin de faire face au caractère ambigu de l'AMDE [Wang *et al.*, 2009]. En outre, les termes linguistiques

flous ont été utilisés dans la définition des trois facteurs du risque, à savoir l'occurrence, la sévérité et la détection [Dinmohammadi et Shafiee, 2013].

Dans le même contexte, diverses approches ont contribué à l'aide à la décision multi-attributs pour améliorer la qualité des résultats et mieux définir les actions de mitigation dans le développement des systèmes maritimes [Balmat *et al.*, 2009] et des yachts [Helvacioglu et Ozen, 2014]. Par ailleurs, l'utilisation de la théorie de l'incertitude [Liu, 2016] et les approches de raisonnement par évidence floue et les méthodologies fondées sur les règles de croyance [Liu *et al.*, 2013] ont été largement déployées dans la priorisation des modes de défaillances identifiés par l'AMDE. Ainsi, divers industriels ont opté pour l'automatisation de l'AMDE afin de diminuer la complexité de son exécution dans le développement des SCS [Montgomery *et al.*, 1996, Price *et al.*, 1995].

Étant une méthode d'analyse de la fiabilité du système, l'AMDEC possède divers caractéristiques, dont les principales sont décrites comme suit :

— Il s'agit d'une analyse exhaustive liée à une démarche systématique permettant d'identifier les différents modes de défaillance des composants et les conséquences sur le système et son environnement ;
— C'est une méthode analytique permettant d'étudier le système à partir de la liste des composants et leurs interactions. Les résultats obtenus sont améliorés et validés tout au long du cycle de développement ;
— C'est une méthode inductive dont les résultats sont obtenus à partir de l'identification des modes de défaillances des composants jusqu'à l'identification de leurs effets ;

Néanmoins, l'AMDEC a ses limites notamment au niveau de la qualité de ses résultats qui est fortement liée à la connaissance structurelle et fonctionnelle du système étudié. En effet, elle reflète l'état de connaissance du système à un stade donné de son cycle de développement. L'efficacité de l'AMDEC s'appuie sur des modèles dynamiques du système représentant le comportement des composants, ce qui n'est pas forcément acquis pendant les premières phases de conception. De plus, cette méthode ne peut pas être appliquée dans le cadre d'une démarche systématique utilisable pour plusieurs SCS en même temps. Autrement dit, elle est utilisée et adaptée aux besoins du domaine concerné afin de mieux quantifier les conséquences des défaillances. Par ailleurs, elle nécessite une connaissance approfondie du système afin de mieux anticiper les défaillances et leurs effets. Dans cette méthode, les phénomènes combinatoires et dynamiques ne peuvent pas être considérés et seule la relation binaire de cause-effet de la défaillance est prise en compte. Afin d'éviter les conflits dans le cadre de développement des SCS, d'autres méthodes complémentaires tel que l'arbre des défaillances AdD ou la méthode de combinaison des pannes sont mieux adaptées afin d'analyser la propagation ou la combinaison des défaillances [Villemeur, 1988].

1.3.3 La méthode Hazard and OPerability HAZOP

La méthode HAZOP a été développée par la société Imperial Chemical Industries (ICI) à la fin des années 1960. Son objectif initial vise l'identification des dangers liés au traitement des substances dangereuses et propose des mesures minimisant ou éliminant les sources potentielles de risque dans l'industrie chimique. Cette méthode a été étendue et adaptée à d'autres domaines industriels comme les entreprises pharmaceutiques, le domaine mécanique et électrique. L'analyse HAZOP est une analyse systématique qui considère deux propriétés du système, à savoir, la *sécurité* et l'*opérabilité* [Kletz, 2001]. Elle s'intéresse principalement à l'étude de l'impact des déviations potentielles des fonctions principales par rapport à leurs objectifs prévus de fonctionnement. Ces dérives imaginées pour chaque fonction sont systématiquement examinées afin de mettre en évidence leurs causes, leurs conséquences, les moyens de détection et les actions correctives. Comme la mise en œuvre de HAZOP nécessite une collaboration pluridisciplinaire, un ensemble de mots-clés, représentant les déviations, a été défini afin d'avoir un vocabulaire partagé non ambigu [IEC 61882, 2001]. Ces mots-clés ont pour objectif d'exprimer la déviation par rapport à l'état sûr et opérable et stimuler le processus de réflexion concernant les causes de la déviation, les fonctions de sécurité, les effets envisagés et les mesures adéquates. Le tableau 1.4 représente le dictionnaire de ces mots-clés utilisés dans la méthode HAZOP [Kotek et Tabas, 2012].

Mot-clé	Définition
Non	Négation totale de la fonction (activité) originale
Plus	Augmentation quantitative
Moins	Diminution quantitative
De même que	Augmentation qualitative (l'occurrence d'un autre cas)
Partie de	Diminution qualitative
Réversion	Fonction inverse
Autre que	Substitution totale
Tôt	Activité prématurée
Tard	Activité retardée
Avant	Lié à l'ordre ou l'enchaînement
Après	Lié à l'ordre ou l'enchaînement

Tableau 1.4 – Dictionnaire des mots-clés liés à l'analyse HAZOP

Comme pour l'AMDE, la démarche HAZOP est analytique et méthodique partant de l'identification de la déviation, des causes, des effets, des fonctions de sécurité concernées et des actions ou des barrières de sécurité afin de réduire l'occurrence de la déviation ou la sévérité de l'effet. Cependant, HAZOP est non exhaustive (contrairement à l'AMDE)

car elle ne traite pas toutes les déviations possibles pour chaque composant du système. La méthode HAZOP n'est pas une étude infaillible pour identifier chaque danger possible ou chaque problème de fonctionnement pouvant survenir sur le plan opérationnel. Les déviations examinées sont principalement celles qui conduisent aux dangers potentiels liés à la sécurité des personnes et de l'environnement [Crawley et Tyler, 2015]. En outre, la méthode HAZOP ne traite pas les événements résultant de la combinaison simultanée des déviations car le processus de génération des barrières de sécurité peut être complexe et insuffisant à l'égard du risque encouru.

Mis à part le traitement des déviations liées aux équipements du système, des approches « HAZOP humaine » (Human HAZOP) ont été développées afin de considérer les situations dangereuses dues aux erreurs humaines. Ces situations doivent être considérées comme un processus d'interactions humaines, notamment dans la phase de définition des mesures d'atténuation par l'amélioration de la qualité de la formation et des instructions. L'importance de cet aspect se reflète par la part importante des erreurs humaines dans le risque opérationnel, qui varie entre 50 % et 90 % [Baybutt, 2002]. Le principe de mise en œuvre de la méthode HAZOP humaine est semblable à l'analyse HAZOP traditionnelle, avec l'addition d'autres mots-clés qui sont interprétés d'un point de vue des facteurs humains, comme décrit dans le tableau 1.5. L'identification des déviations potentielles, liées aux erreurs humaines, représente une grande part dans l'identification des scénarios sensibles des accidents. En d'autres termes, les connaissances acquises lors de l'analyse structurée et systématique des situations dangereuses potentielles liées à la fiabilité du facteur humain est une grande aide pour la définition des actions correctives appropriées.

En effet, le processus d'identification des erreurs humaines doit être établi conformément à la distinction des erreurs des opérateurs humains, proposée par [Swain et Guttmann, 1983] :

- Les erreurs d'omission : Elles sont dues à l'oubli de la réalisation d'une tâche en totalité ou en une partie ;
- Les erreurs de commission qui sont plutôt dues à plusieurs situations : la réalisation incorrecte de la tâche, la réalisation d'une tâche qui n'aurait pas dû être réalisée, la réalisation d'une tâche en dehors de sa séquence (ordre chronologique) ou la réalisation d'une tâche tôt ou tard par rapport à ce qui est requis ;

La validité et la complétude de cette analyse sont évidemment liées à la compétence et l'expérience de l'équipe, la précision des informations utilisées et la qualité de la conception. Toutefois, la prise de décisions des mesures d'atténuation peut s'avérer complexe si l'affectation du mot-clé à un composant spécifique du système ou à une action réalisée est jugée difficile. Dans ce cas, le besoin de procéder à une analyse quantitative du risque correspondant émerge afin d'assister le processus de prise de décisions. En effet, l'évaluation qualitative du risque permet de proposer des recommandations et un plan de leur implémentation

Mot-clé	Définition
Non réalisée	Action non réalisée
Répétée	Action réalisée plusieurs fois
Moins	Action réalisée avec un effet inférieur
Plus	Action réalisée avec un effet supérieur
Plus tôt	Action réalisée plutôt
Plus tard	Action réalisée plus tard
Et aussi	Une autre action est aussi réalisée
Inversé	Une séquence d'actions est non respectée
Autre que	Une action différente est réalisée
Partie	Seulement une partie de l'action est réalisée

Tableau 1.5 – Dictionnaire des mots-clés liés à l'analyse HAZOP humaine

afin de réduire le risque identifié. Dans ce contexte, la combinaison de l'APR avec la méthode HAZOP se révèle nécessaire et efficace afin d'évaluer l'impact du risque lié à la dérive examinée et proposer des actions d'élimination ou de limitation du risque au niveau acceptable [Kotek et Tabas, 2012]. L'estimation du risque lié à la déviation est établie suite à la détermination de la sévérité des conséquences de la déviation et de la probabilité d'occurrence de la déviation. La détermination de ces paramètres s'appuie sur l'équation de l'évaluation du risque (1.5) ainsi que les valeurs des paramètres de la matrice bi-dimensionnelle d'analyse qualitative liée à APR (voir Section 1.3.1).

L'acceptabilité du risque doit être déterminée afin d'être capable de se décider par rapport aux scénarios sensibles et prioriser les actions de minimisation du risque. Suivant la classification du risque, les mesures préventives sont mises en place afin de réduire l'occurrence de la déviation et la sévérité de son effet. Néanmoins, certaines déviations pourraient nécessiter une analyse quantitative faisant l'objet d'une évaluation quantitative du risque si les mesures sont jugées insuffisantes. En effet, des améliorations sont proposées afin de pallier ces déviations avec des actions permettant d'atteindre le niveau de sécurité requis. Comme la méthode HAZOP est principalement qualitative, l'analyse quantitative doit être menée en dehors des réunions consacrées à l'analyse HAZOP afin de faire la part des deux aspects.

Divers travaux académiques et industriels ont été proposés afin d'enrichir la portée de la méthode HAZOP, notamment pour les systèmes électroniques programmables et les systèmes à énergie renouvelable [Dunjó *et al.*, 2010]. Ainsi, la forte ressemblance entre l'analyse HAZOP et l'AMDE a généré de nombreuses approches combinant les deux études afin de maximiser l'efficacité des résultats concernant l'identification des problèmes d'opérabilité et de fiabilité [Trammell *et al.*, 2004]. À titre d'exemple, la complémentarité

de ces deux méthodes a été justifiée et argumentée par l'identification des sources d'incertitude potentielles de la performance des systèmes passifs par l'AMDE et l'aide à la qualification des résultats obtenus par HAZOP [Burgazzi, 2004]. D'autre part, des méthodologies ont fait l'objet de l'intégration des facteurs humains dans HAZOP par un ensemble de mots-clés et des paramètres (personne, action) pour s'intéresser à la gestion des facteurs organisationnels pouvant contribuer au risque [Dunjó *et al.*, 2010, Baybutt, 2002]. Une méthodologie basée sur HAZOP-UML a été proposée afin de formaliser le développement des règles de sécurité et appliquée pour le développement des systèmes autonomes robotiques [Masson *et al.*, 2017].

Comme la méthode HAZOP est chronophage, des outils permettant d'anticiper les dangers et de proposer les mesures appropriées ont été implémentés dans un cadre interactif basé sur des règles [Heino *et al.*, 1988]. Dans [Galluzzo *et al.*, 1998], une méthodologie a été proposée pour l'automatisation de HAZOP qui inclut les causes et les conséquences des déviations et appliquée sur des systèmes continus. De nombreux outils ont été développés afin de faire face à plusieurs aspects de la méthode HAZOP partant de l'identification des déviations jusqu'au raisonnement quantitatif d'aide à la prise des décisions de sécurité en intégrant les modèles mathématiques [Vaidhyanathan et Venkatasubramanian, 1996] et la simulation dynamique [Eizenberg *et al.*, 2006].

À la lumière de ce qui précède, nous pouvons conclure que la méthode HAZOP possède des avantages dont le principal est son caractère systématique et analytique pour identifier les déviations potentielles, leurs causes et leurs effets ainsi que les mesures adéquates. De plus, il s'agit d'une étude pluridisciplinaire dont la qualité des résultats obtenus est fortement liée à l'expertise du groupe de travail, leur expérience et leur créativité. Ce critère est mis en avant par la précision et la complétude de représentation du processus HAZOP ainsi que son caractère rigoureux. Par ailleurs, elle considère les défaillances techniques et les erreurs humaines ainsi que leur implication dans les risques anticipés afin de faire face à la criticité de l'aspect organisationnel des systèmes socio-techniques. En effet, il s'agit d'un processus continu mettant l'accent sur la sécurité du système, des acteurs et de l'environnement ainsi que les aspects opérationnels liés à la fiabilité du système et de l'opérateur humain. Les mesures de sécurité mises en place doivent être capables de réduire ou éliminer le risque identifié.

Toutefois, les limites de la méthode consistent en son coût élevé en temps, son aspect complexe mais aussi son caractère non exhaustif. L'analyse HAZOP ne traite pas toutes les déviations susceptibles de survenir, mais seulement celles jugées les plus importantes. Par conséquent, nous remarquons une complémentarité de la méthode HAZOP avec l'APR et son aspect qualitatif et/ou quantitatif, ainsi qu'avec l'AMDEC. Le recours à des méthodes analysant judicieusement les séquences des événements qui pourraient causer des déviations, comme l'arbre des défaillances AdD, est considéré comme nécessaire afin

de combler l'insuffisance du caractère non combinatoire.

1.3.4 Méthode de l'Arbre des Défaillances (AdD)

La méthode de l'arbre des défaillances est une analyse déductive et descendante permettant de rechercher les combinaisons parallèles et séquentielles des événements dangereux élémentaires qui sont à l'origine d'un événement redouté, appelé l'événement sommet [Mortureux, 2005]. Elle est représentée sous la forme d'une arborescence graphique et composée des portes logiques de l'algèbre de Boole (ET, OU,..), qui déterminent l'enchaînement logique de toutes les défaillances intermédiaires possibles, pouvant conduire à une défaillance majeure du système.

L'AdD est utilisé tout au long du cycle de développement du système afin d'analyser minutieusement les combinaisons des événements de manière que chacun est causé par les événements des niveaux inférieurs. La décomposition des événements s'achève dès l'obtention des événements de base non décomposables et indépendants. La figure 1.4 représente un exemple simple de la construction de l'arbre des défaillances. Il s'agit d'un processus récursif et structuré partant de l'identification explicite et précise de l'événement sommet jusqu'à la description fine des causes qui sont liés par des connecteurs logiques. Cependant, les causes représentées dans l'arbre ne sont pas exhaustives ; elles constituent l'ensemble des causes immédiates, nécessaires et suffisantes à l'occurrence de l'événement sommet. En outre, cette démarche déductive permet d'anticiper et contrôler la performance du système en cours de développement, mais aussi de diagnostiquer les causes et les mesures correctives potentielles d'une défaillance observée d'un système existant.

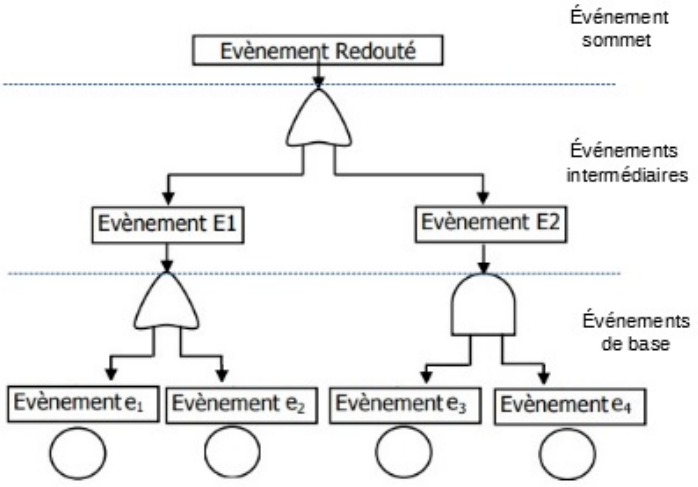

Figure 1.4 – Exemple simple d'un arbre des défaillances

Cette méthode est largement utilisée comme support outillé pour assister l'analyse de la sécurité et la fiabilité des SCS. En effet, l'analyse par AdD permet de visualiser les causes qui correspondent à l'événement sommet indésirable et qui peuvent être des défaillances

techniques ou des erreurs humaines [Stamatelatos *et al.*, 2002]. L'intégration des erreurs humaines dans l'enchaînement logique conduisant à la défaillance globale représente un aspect crucial dans l'analyse de sécurité des systèmes socio-techniques dont l'interaction sûre entre l'opérateur humain, les équipements techniques et l'environnement permet d'accomplir le service désiré.

Malgré le rôle important de l'arbre des défaillances dans le processus de prise des décisions de sécurité, la construction de l'arbre des défaillances reste une tâche compliquée et coûteuse en temps. De ce fait, la construction assistée par des outils a attiré une attention considérable dans le milieu académique et industriel et diverses méthodologies ont été proposées. Les approches ayant un intérêt marqué dans la construction automatisée de l'AdD sont essentiellement fondées sur :

- Des règles de détermination des portes logiques ainsi que leurs entrées [Haasl, 1965] ;
- Des algorithmes basés sur les diagrammes d'état [Rauzy, 2002] et l'utilisation des tables de décisions afin de modéliser, garder la traçabilité et combiner les défaillances des composants du système [Andrews et Henry, 1997] ;
- Un algorithme de construction automatique de l'AdD basé sur le diagramme de blocs du système [Wang *et al.*, 2002] ;

Les évaluations qualitatives et quantitatives peuvent être appliqués dans l'arbre des défaillances. Bien que l'AdD représente une évaluation qualitative des événements et les relations conduisant à l'événement sommet, une analyse quantitative additionnelle peut servir pour raffiner les informations critiques obtenus. En effet, l'évaluation qualitative transforme la combinaison logique de l'AdD en une forme logiquement équivalente et plus précise, appelée coupes minimales de l'événement sommet. Une coupe est une combinaison des événements de base pouvant causer l'événement sommet. Tandis qu'une coupe minimale est la plus petite combinaison déterminant le lien de causalité direct de l'événement de base vers l'événement sommet [Mortureux, 2005].

Les méthodes classiques de détermination des coupes minimales sont principalement les algorithmes fondés sur la manipulation booléenne [Walker et Papadopoulos, 2009] et les diagrammes de décisions binaires (Binary Decisions Diagrams) [Akers, 1978, Amari et Akers, 2004]. L'obtention des coupes minimales met l'accent sur les combinaisons des défaillances potentielles et oriente les modifications conceptuelles afin d'éliminer ou réduire les situations indésirables. Mis à part leur rôle essentiel dans l'analyse de la sécurité et la fiabilité du système, les coupes minimales obtenues permettent de valider l'arbre des défaillances en déterminant si la coupe minimale cause effectivement l'événement sommet. De plus, elles peuvent faire l'objet de l'analyse des dépendances liées aux défaillances de cause commune (DCC) [Xing, 2007]. Ainsi, les combinaisons des défaillances et des événements et leur propagation dans le système sont clairement visualisées à travers cette analyse qualitative. Par conséquent, l'élimination des redondances des événements au niveau des coupes est possible afin de converger vers des résultats qualitativement structurés

et précis.

Concernant l'analyse quantitative, elle dérive les données numériques significatives de l'arbre des défaillances, comme la probabilité de défaillance. Cette quantification sert à prioriser les événements de base contribuant à la défaillance principale, selon leur probabilité d'occurrence afin d'optimiser l'allocation des ressources. En effet, l'objectivité des mesures obtenues indique l'importance des composants contributeurs à l'occurrence de l'événement sommet au regard de la fiabilité du système. Les priorisations obtenues de la méthode de l'AdD constituent une base importante de priorisation des ressources et des coûts du système [Ruijters et Stoelinga, 2015]. Autrement dit, l'évaluation quantitative est fondée sur les résultats obtenus par l'analyse qualitative notamment les coupes minimales et ajoute des données numériques importantes à la prise des décisions. Les chemins critiques conduisant à la défaillance sont identifiés et classifiés afin de mener à bien la conception du système à travers la définition des contraintes de sécurité qui sont intégrées dans l'architecture du système.

Mis à part les contributions académiques, une panoplie d'outils a été proposée par les leaders industriels de l'analyse de sécurité et la fiabilité du système. Un programme d'AdD, appelé « FTA software »[1] a été développé afin de générer automatiquement des arbres des défaillances à partir de l'AMDE ou l'AMDEC. Il établit l'analyse qualitative en générant les coupes minimales et les fréquences de défaillances dans un intervalle de temps spécifique. L'outil appelé « OpenFTA »[2] possède les même fonctionnalités mais considère aussi l'analyse déterministe et les simulations Monte Carlo pour déterminer la fiabilité du système. Un autre outil a été développé afin d'analyser les AdD et les défaillances de cause commune, appelé « RiskSpectrum FTA »[3]. Il établit à la fois l'analyse qualitative et quantitative afin d'évaluer la fiabilité et la maintenabilité du système.

Dans le cadre de l'extension des arbres des défaillances, de nombreuses méthodologies ont été proposées afin combler les limites de l'AdD dues à son aspect statique. L'intégration de l'aspect temporel dans les AdD réside principalement dans les arbres des défaillances dynamiques [Boudali *et al.*, 2007]. Les autres extensions de l'AdD peuvent être résumées en plusieurs volets comme suit :

— L'utilisation de la théorie de l'incertitude et les nombres flous (fuzzy numbers) dans les cas où les probabilités des défaillances ou le comportement ne sont pas suffisamment connus [Ren et Kong, 2011] ;

— La gestion des systèmes où les événements de base sont dépendants de manière non-statistique, par exemple lorsqu'une défaillance d'un composant augmente le taux de défaillance d'un autre composant [Zang *et al.*, 2003] ;

— Des arbres de défaillance état/événement ont été introduits pour modéliser des

1. http ://aldservice.com/en/reliability-products/fta.html
2. http ://www.openfta.com/
3. http ://www.riskspectrum.com/en/risk

systèmes et des composants avec un état variable dans le temps et dans lequel cet état affecte les conséquences des défaillances de composants ou les taux de défaillance [Vaurio, 2002] ;

— Les arbres des défaillances réparables qui se focalisent sur la réparation et le recouvrement des composants défaillants suivant des politiques bien déterminées [Raiteri *et al.*, 2004] ;

— Le diagramme de cause-conséquence afin d'étendre l'AdD et de mieux décrire les effets séquentiels des chaînes d'accidents [Taylor, 1982] ;

En vertu de ce qui précède, nous pouvons conclure que la méthode d'AdD dispose de puissantes capacités, notamment avec l'analyse qualitative et quantitative qui présentent un aspect complémentaire dans l'analyse de la sécurité et la fiabilité des systèmes critiques. Cependant, nous constatons clairement les limites de cette méthode qui consistent en son caractère statique partant du principe que les événements de base doivent être indépendants, mais aussi du fait que l'aspect temporel des séquences d'événements conduisant à la défaillance n'est pas considéré. Par conséquent, la valeur ajoutée des contributions portant sur l'enrichissement de la portée de cette méthode ainsi que les outils proposés est indéniable afin de satisfaire les besoins des systèmes à multi-états (non binaire), à caractère dynamique et susceptibles à des variations temporelles.

1.4 Les pratiques de l'analyse de sécurité ferroviaire

Le processus de démonstration de sécurité pour les systèmes socio-techniques complexes, tel que les systèmes ferroviaires, est établi en co-activité avec leur cycle de développement. Mis à part leur aspect critique, ils se distinguent par des besoins correspondants aux exigences qualitatives et quantitatives du métier. Les besoins du domaine ferroviaire sont spécifiés dans des textes normatifs mettant en exergue la démarche systématique appliquée durant le cycle de vie du système. L'ensemble du processus méthodologique fournit les lignes directives permettant de mener à l'équilibre entre les préoccupations de sécurité et les contraintes économiques du développement. Par ailleurs, le management des décisions de sécurité considère les interactions de l'opérateur humain avec des dispositifs techniques et des organisations, fixant ainsi des objectifs de sécurité à satisfaire.

1.4.1 Les besoins du domaine ferroviaire et le cadre normatif

Le fonctionnement des systèmes ferroviaires repose sur trois parties principales, à savoir :

— les installations techniques,

— les interventions humaines,

— les contraintes imposées par les organisations ainsi que l'environnement opérationnel.

De ce fait, la stratégie de l'analyse de sécurité est liée à la détermination du couple (gravité, occurrence) des dommages affectant la vie humaine, l'infrastructure et l'environnement du système ainsi qu'à la réduction du risque associé. La démarche systémique de sécurité des systèmes ferroviaires est fondée sur l'identification des situations critiques à l'origine des défaillances intrinsèques du système et des erreurs humaines afin de faire face aux incohérences globales de leur interactions dans des circonstances données. En effet, le niveau de sécurité relève de la confiance qu'on peut avoir dans les équipements technologiques ainsi que dans la connaissance suffisante du comportement requis par l'intervenant humain. D'autre part, les moyens mis en œuvre pour lutter contre les défaillances et les erreurs humaines doivent êtres capables de maintenir un état stable du système sur le plan opérationnel. L'harmonisation des activités du développement et de sécurité des systèmes ferroviaires s'appuie souvent sur les normes pour justifier les critères des décisions.

Dans le cadre d'une approche générique, les exigences nécessaires et suffisantes pour réduire les risques ont été prescrites dans la norme [IEC 61508, Norme Internationale, 2000] appliquée pour les systèmes électriques-électroniques-programmables. Ensuite, cette dernière se décline en diverses normes pour des domaines spécifiques afin de prendre en compte les contraintes des secteurs comme le secteur nucléaire [NF, EN 61513, 2013], le secteur automobile [ISO, 26262-2, 2018] et le secteur ferroviaire [CENELEC, NF EN 50126-1, 2017], [CENELEC, NF EN 50128, 2011], [CENELEC, NF EN 50129, 2003] et [CENELEC, NF EN 50159, 2011]. La figure 1.5 représente les normes relatives aux systèmes ferroviaires ainsi que leurs contextes d'application.

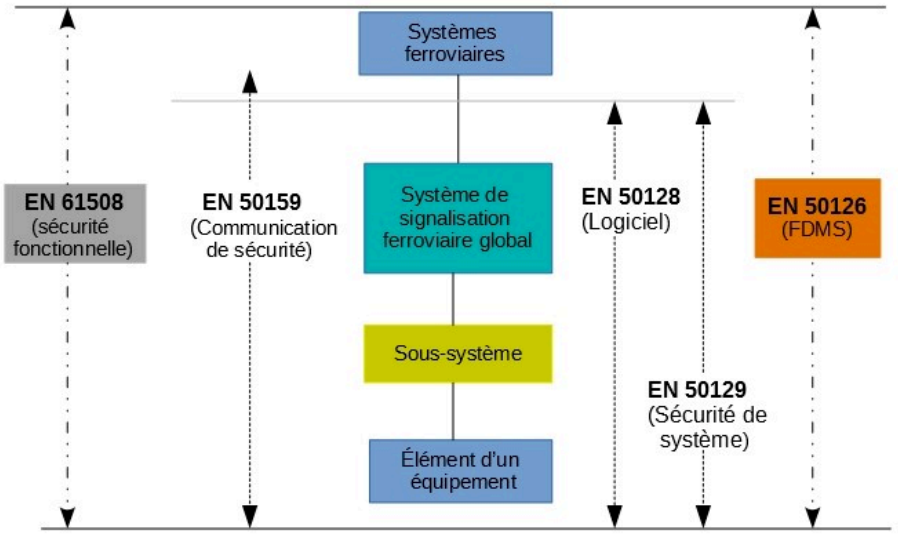

Figure 1.5 – Les normes liées au secteur ferroviaire

Les normes liées au domaine ferroviaire et regroupées sous le référentiel CENELEC sont décrites comme suit :

— La norme EN 50126 se focalise sur la spécification et la démonstration des attributs FDMS tout au long du cycle de vie du système ferroviaire. La norme EN 50126

définit les grandes lignes directives pour établir des mécanismes et des procédures capables d'identifier et contrôler les facteurs impactant les indicateurs FDMS. Elle structure le cycle de vie du système afin d'évaluer, gérer et contrôler les différents aspects du système incluant les paramètres FDMS afin de délivrer le service désiré respectant les contraintes du coût et de disponibilité.

— La norme EN 50128 porte sur la sûreté de fonctionnement des logiciels de commande et de protection ferroviaire pour les systèmes de signalisation, de télécommunication et de traitement. Elle recommande la mise en place d'une méthodologie rigoureuse du cycle de vie en V du logiciel avec ou sans besoins sécuritaires. Ainsi, cette norme introduit la notion d'un plan d'évaluation et de démonstration de la qualité de la solution logicielle mise en œuvre au regard des objectifs de sécurité attribués.

— La norme EN 50129 est applicable aux systèmes électroniques relatifs à la sécurité (y compris les sous-systèmes et les équipements) pour la signalisation ferroviaire tout au long de leur cycle de vie. Elle définit les niveaux de SIL et les exigences de sécurité pour les situations critiques identifiées par le processus d'analyse des risques défini dans la norme EN50126. Ainsi la construction du dossier de sécurité est menée afin d'inclure les conditions et les exigences de validation et démonstration des preuves de sécurité.

— La norme EN 50159 se focalise sur la communication des informations de sécurité entre les équipements de sécurité et le système de transmission. Elle spécifie les exigences de sécurité pour la communication impactant la mise en œuvre des équipements de sécurité connectés au système de transmission. Ces exigences correspondent à un contexte technologique particulier de la norme EN 50129.

1.4.2 Les facteurs d'influence de l'analyse de la sécurité

Selon la norme EN 50126, la sécurité du système ferroviaire dépend de trois éléments qui peuvent être distingués de la manière suivante :

— Les conditions du système liées à ses perturbations internes qui incluent les défaillances systémiques et aléatoires dans chaque phase de son cycle de vie.

— Les conditions d'exploitation relatives aux perturbations extrinsèques au système notamment les conditions environnementales, les erreurs humaines, les procédures et le changement du profil de la mission en phase d'exploitation.

— Les conditions de maintenance liées aux erreurs humaines et la gestion des décisions au niveau des procédures de maintenance.

L'identification des facteurs d'influence de la sécurité du système est une étape nécessaire pour le développement d'un système sûr afin de pouvoir évaluer leurs effets et maîtriser leurs causes. En effet, la norme EN 50126 recommande l'utilisation des diagrammes cause/effet afin de définir les facteurs qui s'opposent aux exigences de la FDMS spécifiées. La figure 1.6 représente un exemple de diagramme cause/effet extrait de la norme EN 50126 afin

d'illustrer le processus de recueil des informations liées à ces facteurs faisant l'objet de la première phase du cycle de vie du système dénommée *concept*. Cette dernière vise à définir le système ainsi que son contexte et ses limites afin d'accomplir le développement conforme aux exigences de FDMS.

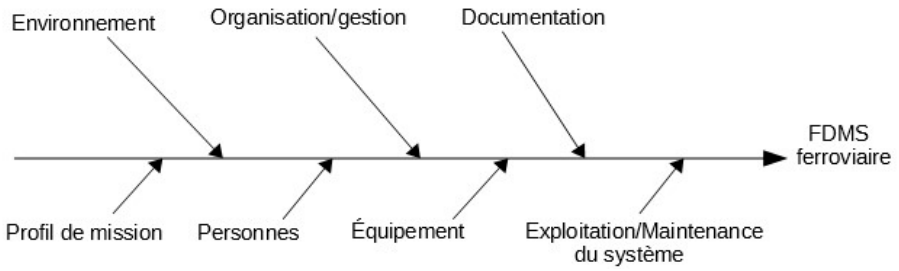

Figure 1.6 – Exemple d'un diagramme cause/effet extrait de la norme [CENELEC, NF EN 50126-1, 2017]

Les trois catégories des facteurs d'influence sont représentées dans le diagramme structuré proposé par la norme [CENELEC, NF EN 50126-1, 2017] dans la figure 1.7. Cette décomposition analytique des facteurs est liée aux trois aspects tels que les facteurs génériques, les facteurs relatifs au domaine d'application et les facteurs humains. Les facteurs génériques incluent les défaillances techniques des équipements et des composants du système, les conditions de l'environnement et les perturbations externes climatiques et électromagnétiques. Le deuxième aspect à prendre en compte dans les études de sécurité concerne l'architecture du système et son exploitation.

En effet, les facteurs liés à l'exploitation se focalisent sur les fonctions requises du système, le contexte opérationnel, la coexistence avec l'infrastructure déjà existante, les exigences liées à la durée de vie, le coût, la fréquence de service, ainsi que les effets des défaillances sur le fonctionnement du système. Enfin, les facteurs humains sont considérés comme un élément important et intrinsèque de l'analyse de sécurité des systèmes ferroviaires. Les opérateurs humains sont fortement impliqués dans la réalisation, l'exploitation et la maintenance du système. Sur le plan opérationnel, l'expertise des agents et la maîtrise des gestes du métier a une influence majeure sur la sécurité globale du système. Ainsi, l'adaptabilité du comportement des agents au terrain est nécessaire afin de faire face aux situations critiques. Quoi que les acteurs de l'environnement du système ne sont pas impliqués directement dans l'analyse de sécurité, ils peuvent dans certaines situations avoir un impact majeur. Lorsque l'erreur humaine est de type cognitif, des mesures de sécurité doivent être prises pour diminuer le risque lié à la perception et la mauvaise interprétation d'une situation opérationnelle. Dans cette thèse, nous traitons ces aspects et de leur intégration dès les premières phases de conception.

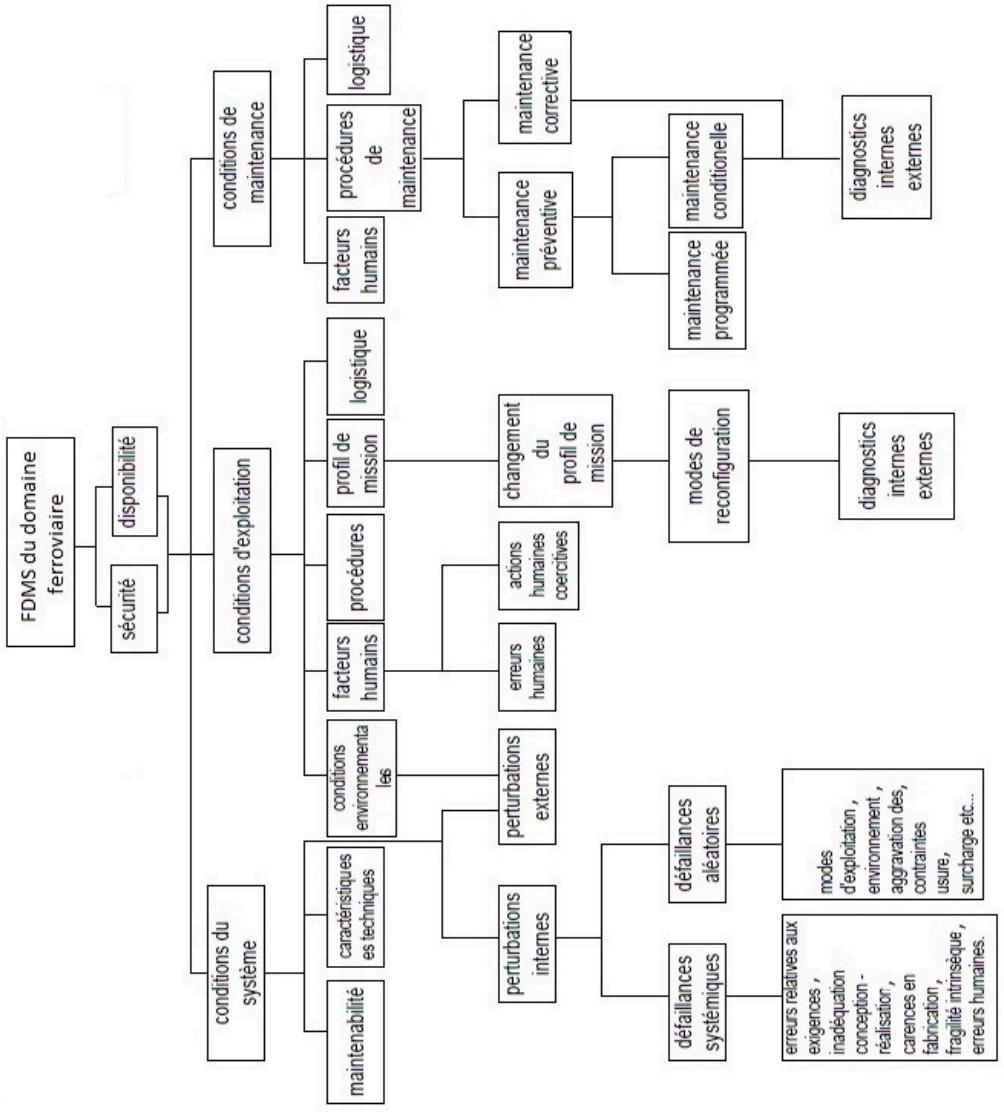

Figure 1.7 – La décomposition des facteurs d'influence de la sécurité ferroviaire [CENELEC, NF EN 50126-1, 2017]

1.4.3 D'un risque acceptable vers un objectif de sécurité

Le détermination des objectifs de sécurité et des seuils de performance des systèmes ferroviaires constitue un processus proactif et problématique. Dans un contexte d'interopérabilité et d'exploitation des infrastructures, divers changements opérationnels, techniques et organisationnels peuvent avoir un impact sur l'analyse de sécurité. À cet effet, l'agence ferroviaire européenne (ERA) a défini la directive 402/2013 [Règlement d'exécution, 402/2013/UE, 2013] des méthodes de sécurité communes (MSC) afin d'établir un cadre méthodologique harmonisé relatif à l'évaluation et l'appréciation des risques. Après la définition préliminaire du système, les MSC définissent le processus commun d'évaluation des niveaux de sécurité, d'accomplissement des objectifs de sécurité et de démonstration de conformité avec les exigences de sécurité. Ainsi, la MSC relative à l'évaluation et l'appréciation du risque établit un cadre réglementé pour maintenir le niveau de sécurité requis, la traçabilité des décisions, les justifications et les preuves résultantes du processus de gestion des risques.

La détermination des seuils d'acceptabilité se base sur des principes de sécurité afin de statuer sur le niveau d'acceptabilité du risque lié au système. Autrement dit, ces principes ont pour vocation de définir et maintenir les niveaux de sécurité que doivent au moins atteindre les différentes parties ou le système ; et proposer, le cas échéant, des améliorations pour satisfaire les objectifs globaux de sécurité. Dans la communauté ferroviaire européenne, trois grands principes de sécurité sont distingués et appliqués :

— Le principe GAME (Globalement Au Moins Equivalent) est appliqué en France. Il stipule que tout nouveau système ou toute modification d'un système en exploitation doit offrir un niveau global de sécurité au moins équivalent à celui des systèmes existants dits « de référence » qui sont réputés sûrs et offrant des services comparables dans les mêmes conditions opérationnelles et environnementales [Règlement d'exécution, 402/2013/UE, 2013]. Ce principe intègre la préoccupation de progrès dans la définition des objectifs quantifiés de sécurité.

— Le principe ALARP (As Low As Reasonably Praticable) est pratiqué au Royaume Uni. Il prétend que tout risque doit être réduit autant qu'il est raisonnablement admissible ou à un niveau aussi bas qu'il est matériellement raisonnable de le faire. Ce principe d'ordre économique conduit à la pondération du risque par le coût des surinvestissements permettant de se protéger.

— Le principe MEM (Minimum Endogenous Mortality) est appliqué en Allemagne. Il spécifie que tout risque dû à un nouveau système de transport ne doit pas significativement augmenter la valeur du risque de mortalité endogène auquel un usager est exposé. En d'autres termes, le niveau de sécurité continue à être amélioré jusqu'à établir le niveau de mortalité endogène minimale.

La considération des préoccupations sociales, individuelles et technologiques du risque varie selon le principe de sécurité appliqué. En effet, le principe MEM considère la préoccu-

pation individuelle lié au risque ambiant constaté par heure d'utilisation du système par l'usager. Par contre, la démarche ALARP considère la préoccupation collective qui met en balance le risque avec les investissements que la société peut admettre au regard des services attendus par le système. Elle correspond à un compromis économique entre l'effort fourni pour réduire le niveau de risque et le coût final de la solution mise en œuvre. Concernant le principe GAME, il prend en compte aussi bien le risque individuel que collectif dans son contexte d'application.

Tandis que les principes MEM et GAME reposent sur un seuil de risque tolérable à ne jamais franchir, le principe ALARP se caractérise par deux limites. En effet, la limite haute du risque caractérise le seuil à ne jamais franchir et la limite basse est celle en dessous de laquelle le risque est toléré. La zone entre les deux limites est dite la zone ALARP dans laquelle le risque est acceptable si la démonstration prouve que de tous les moyens raisonnables de le réduire ont été mis en œuvre. L'acceptation du risque relève principalement de l'équilibre entre les dépenses systématiques réalisées pour sa réduction et le coût induit par l'accident potentiel.

Afin de concevoir les systèmes ferroviaires et organiser leur fonctionnement, il est nécessaire de transformer les niveaux des risques acceptables en des objectifs de sécurité quantifiés. Cette démarche consiste à déterminer le seuil de probabilité d'un accident à travers ses conséquences ou encore le couple (occurrence, gravité). Ce seuil représente la limite au dessus de laquelle le risque n'est pas toléré. Dans la zone ALARP, le risque est réputé tolérable mais les conditions doivent être discutées. Comme le montre la figure 1.8, la notion de tolérabilité ne signifie pas que le risque est accepté mais qu'il est toléré face à deux situations :

— Soit face au bénéfice attendu de l'utilisation et de la fonctionnalité du système ;
— Soit parce que le coût des conséquences reste inférieur à l'effort à mettre en œuvre pour réduire le risque ;

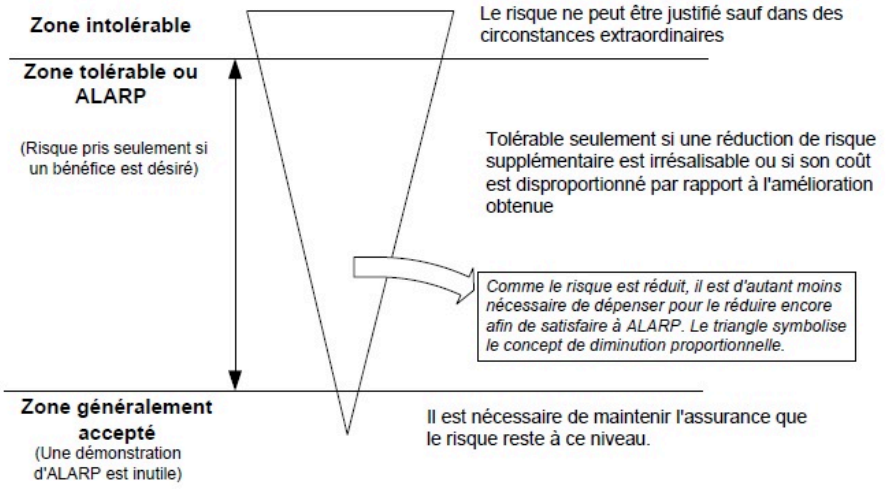

Figure 1.8 – La zone ALARP [IEC 61508, Norme Internationale, 2000]

Par ailleurs, la détermination des seuils maximaux des risques tolérables en fonction de leurs conséquences n'est pas une opération triviale. Ce processus repose sur des textes normatifs qui fournissent des critères pour guider les autorités nationales pour classifier les risques par catégories en fonction de la fréquence tolérable allouée et la gravité des conséquences. À ce niveau, le risque n'est pas considéré par l'événement à l'origine de l'accident mais plutôt par la gravité de la conséquence. La détermination des seuils tolérables constitue une démarche quantitative et qualitative. Elle est quantitative car elle fournit des valeurs définissant des critères limites des zones, et qualitative puisqu'elle caractérise l'effort qui doit être réalisé afin d'éviter l'occurrence d'une situation dangereuse aboutissant à une catégorie spécifique de conséquence.

La norme EN 50126 définit des critères qualitatifs des fréquences et de gravité des situations dangereuses. Cette norme classifie les niveaux de fréquence d'une situation dangereuse suivant la possibilité qu'un accident se produise. Cette classification est basée sur l'historique des incidents et accidents survenus dans l'exploitation. Ainsi, elle catégorise les niveaux de gravité suivant les dommages engendrés sur les personnes, le système et l'environnement afin d'estimer l'impact des scénarios d'accidents. Les tableaux 1.6 et 1.7 présentent respectivement les catégories de fréquence des situations dangereuses et de gravité des conséquences engendrées par ces situations.

Niveau	Description
Fréquente	Susceptible de se produire fréquemment. La situation dangereuse est continuellement présente.
Probable	Peut survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne souvent.
Occasionnelle	Susceptible de survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne à plusieurs reprises.
Rare	Susceptible de survenir à un moment donné du cycle de vie du système. On peut raisonnablement s'attendre à ce que la situation dangereuse se produise.
Improbable	Peu susceptible de se produire mais possible. On peut supposer que la situation dangereuse peut exceptionnellement se produire.
Invraisemblable	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas.

Tableau 1.6 – Échelle de fréquence des situations dangereuses [CENELEC, NF EN 50126-1, 2017]

Niveau de gravité	Conséquences pour les personnes ou l'environnement	Conséquences pour l'exploitation
Catastrophique	Des morts et/ou plusieurs blessés graves et/ou des dommages majeurs pour l'environnement	Perte de plusieurs systèmes importants
Critique	Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement	Perte d'un système important
Marginal	Blessures légères et/ou menace grave pour l'environnement	Dommages graves pour un (ou plusieurs) système(s)
Insignifiant	Éventuellement une personne légèrement blessée	Dommages mineurs pour un système

Tableau 1.7 – Les catégories de gravité des conséquences engendrées par les situations dangereuses [CENELEC, NF EN 50126-1, 2017]

Ces critères de classification de la fréquence d'occurrence et de la gravité permettent d'établir une matrice bidimensionnelle occurrence-gravité afin d'attribuer un niveau de risque à un niveau d'acceptabilité. Cette étape de classification du risque repose sur l'identification de la combinaison du niveau de fréquence d'occurrence ainsi que le niveau de gravité des dommages engendrés par l'accident. La figure 1.9 représente les 4 niveaux de risque définis par la norme EN 50126 comme suit :

- Risque inacceptable : il doit être éliminé,
- Risque indésirable : le risque n'est acceptable que lorsque sa réduction est impossible, dans ce cas l'accord des autorités organisatrices ou de l'exploitant est impératif,
- Risque acceptable : le risque est acceptable avec l'accord de l'exploitant et moyennant des précautions de contrôle appropriés,
- Risque négligeable : le risque est acceptable sans conditions.

Ainsi, le taux de danger tolérable (Tolerable Hazard Rate THR) est déterminé à travers les combinaisons des défaillances dangereuses et maîtrisées dans un scénario d'accident. Il s'agit d'un objectif de sécurité quantifié qui se rapporte à un mode de défaillance d'une fonction relative à la sécurité [Beugin *et al.*, 2016]. Ensuite le niveau d'intégrité de sécurité (SIL) est attribué à cette fonction sur la base des THR répartis et par la correspondance THR/SIL présenté dans le tableau 1.8 extrait de la norme [CENELEC, NF EN 50129, 2003].

Le processus d'allocation de SIL est itératif afin de vérifier que l'ensemble des objectifs de sécurité liés au THR et le niveau d'acceptabilité du risque est atteint. Ce processus permet de démontrer ensuite la conformité avec les exigences de sécurité et élaborer le

Fréquence d'une situation dangereuse	Niveau de gravité des conséquences d'une situation dangereuse			
	Insignifiant	Marginal	Critique	Catastrophique
Fréquente	Indésirable	Inacceptable	Inacceptable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Occasionnelle	Acceptable	Indésirable	Indésirable	Inacceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable

Figure 1.9 – La matrice Occurrence-Gravité définie par la norme [CENELEC, NF EN 50126-1, 2017]

THR (par heure et par fonction)	SIL
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Tableau 1.8 – Table de SIL de la norme [CENELEC, NF EN 50129, 2003]

document justifiant les choix et les décisions tout au long du processus de gestion des risques. Ainsi, les pratiques de l'analyse de sécurité ferroviaire sont guidées par les normes afin d'harmoniser le cadre méthodologique permettant d'unifier les choix pris à travers différentes perspectives du système.

1.5 Discussion

La sécurité doit être considérée au cours de développement des SCS car il s'agit d'une propriété « émergente » dans laquelle les situations dangereuses sont difficiles à anticiper. Cette notion d'émergence est devenue une notion classique du domaine des systèmes critiques. En effet, le contexte qui permet l'apparition de cette propriété et les interactions entre les composants et les acteurs sont difficiles à caractériser. Ils mènent à des comportements inattendus qui violent le but de sécurité global [Black et Koopman, 2009]. Ce processus a pour objectif de renforcer la sécurité en intervenant sur les interactions entre les composants du système à travers un ensemble de décisions. Ces choix de sécurité peuvent être intégrés dans l'architecture du système sous forme de contraintes de sécurité afin d'assurer un comportement sûr du système sur le plan opérationnel. D'un plus haut niveau, des restrictions de sécurité sont prises en compte lors de la démarche de raisonnement de sécurité par l'identification d'un ensemble de mesures de sécurité. Ces dernières peuvent

être des choix architecturaux, des dispositifs techniques ou des interventions humaines considérés afin d'amener le système à un état sûr.

La démarche de démonstration de sécurité ainsi que les critères des choix de sécurité sont justifiés à la fin du processus mené par l'application des méthodes de l'analyse dysfonctionnelle ainsi que les principes et les techniques de sécurité discutés dans ce chapitre. L'ensemble des choix de sécurité justifiés doit être capable d'atteindre un niveau de sécurité acceptable pour l'ensemble des opérations du système. D'autre part, la mise en œuvre des mesures de sécurité doit prendre en considération les contraintes validant ou déclenchant leur application ainsi que leur contexte d'application. L'ensemble de ces éléments permettent de définir les règles de sécurité pour prouver la satisfaction des objectifs de sécurité.

Par ailleurs, la qualité des décisions de sécurité relève de leur degré de conformité avec les exigences de sécurité. Les exigences de sécurité occupent une place importante dans le processus de gestion des risques et des décisions liées à la sécurité. Dans le cycle de vie d'un système, nous nous focalisons sur l'analyse de sécurité, composant de la sûreté de fonctionnement qui est une activité en amont de la phase de conception du système. La spécification des exigences fait l'objet de la première phase du développent du système afin de définir ses besoins et son contexte d'application. Ainsi, les différents acteurs impliqués dans le développement du système, notamment les ingénieurs de sécurité ont la responsabilité de respecter les exigences de sécurité spécifiées préalablement. Par conséquent, le lien entre le processus de gestion de sécurité et le domaine de l'ingénierie des exigences (IE) doit être établi d'une façon claire et non ambiguë comme le montre la figure 1.10. Dans ce contexte, nous nous posons plusieurs questions d'une manière non exhaustive : *Comment interpréter les liens sémantiques entre les différentes notions des domaines ? Quelle terminologie pourrait-être utilisée de façon à harmoniser le vocabulaire employé entre les différents acteurs de développement du système ? Quel type de modélisation sera adéquat pour fournir une vue partagée, permettant de répondre aux besoins des domaines ? Comment définir un processus de gestion des décisions de sécurité capable de faire face aux contraintes des aspects organisationnels, opérationnels et socio-techniques complexes ?*

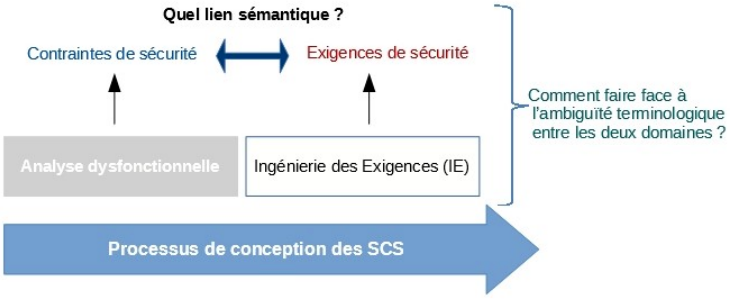

Figure 1.10 – Cohérence entre les contraintes de sécurité et les exigences de sécurité : Quel lien sémantique ?

Dans les travaux de cette thèse, nous essayons de répondre à ces questions de recherche afin d'éviter les conflits de communication entre les acteurs. En premier lieu, nous introduisons les grands concepts et les fondements de l'IE afin de définir les verrous scientifiques qui doivent être considérés dans nos travaux de recherche. Ensuite, nous dévoilons et discutons le type de modélisation et de représentation qui parait adéquat.

Chapitre 2

Conception des Systèmes Critiques de Sécurité (SCS)

Sommaire

2.1 Introduction

Le développement d'un Système Critique de Sécurité (SCS) repose sur un ensemble d'activités permettant sa mise en œuvre de manière structurée et systématique. Afin de faire face à la complexité croissante des systèmes, en particulier les SCS, une approche interdisciplinaire appelée *Ingénierie Système* (IS) a été développée pendant les années 1990. Elle vise principalement à définir, concevoir et vérifier un système tout en cherchant un compromis entre l'efficacité de la solution mise en œuvre et son aspect économique global. Cette démarche méthodologique est définie par l'Association Française d'Ingénierie Système (AFIS) [1] comme un processus coopératif s'appuyant sur les connaissances, les méthodes et les techniques issus du retour d'expérience et de la science. Elle est mise en œuvre pour apporter une solution à un besoin opérationnel défini tout en satisfaisant les contraintes de l'ensemble de ses parties prenantes. Cette démarche se représente souvent par le cycle en V qui englobe les étapes à suivre pour obtenir une solution performante au regard de ses services attendus mais également économique par rapport aux contraintes de performance. Les pratiques de cette démarche font l'objet de plusieurs documents normatifs afin de définir un cadre méthodologique capable de répondre aux besoins métier.

Partant de l'expression des besoins jusqu'à la maintenance, le développement d'un nouveau système fait appel à plusieurs acteurs pluridisciplinaires qui coopèrent entre eux afin de délivrer une solution conforme aux critères et aux contraintes définis en amont. Le point de vue systémique de l'IS s'intéresse à l'étude de la nature du système, l'étude de ses composants et l'étude de son comportement. Ainsi, une activité intégrante de l'IS, appelée *Ingénierie des Exigences* (IE) se focalise sur les éléments qui rendent ces études nécessaires. Dans ce chapitre, nous nous focalisons dans un premier temps sur les concepts de base de l'IE ainsi que son objectif majeur au cours du cycle de développement du système. Ensuite, nous présentons une partie de l'état de l'art abordant les méthodologies et approches dirigées par les modèles dans la discipline de l'IE. Nous nous intéressons particulièrement aux exigences de sécurité faisant l'objet de notre étude.

Afin de répondre à la problématique multi-acteurs engendrée par l'IS, nous considérons que la modélisation multi-vues est un enjeu majeur de communication entre les collaborateurs multidisciplinaires afin de maintenir la consistance entre les différentes vues des domaines impliqués. Par ailleurs, ceci nécessite la mise en œuvre d'un vocabulaire commun se traduisant par une sémantique et une syntaxe non ambiguës. De ce fait, nous mettons en lumière la conceptualisation des connaissances des domaines ou encore la modélisation conceptuelle dans la deuxième partie de ce chapitre. Dans ce contexte du développement des SCS, nous discutons de la capacité des ontologies à satisfaire à la fois nos objectifs de recherche et les besoins du domaine ferroviaire. Dans la dernière section, nous discutons la discipline d'ingénierie ontologique et présentons les contributions majeures dans les domaines de l'IE, du ferroviaire et de l'analyse de sécurité des systèmes critiques.

1. http ://www.afis.fr/pages/accueil.aspx

2.2 Ingénierie des Exigences (IE)

L'ingénierie des Exigences (IE) est une partie vitale du processus de l'Ingénierie Système (IS) et du génie logiciel ; elle permet de définir l'étendue du problème et de gérer les éléments correspondants. Comme l'indique le terme, l'IE inclut toutes les activités liées aux exigences, souvent définies par le développement et la gestion des exigences tout au long du cycle de vie du système. Bien que cette discipline soit définie de diverses manières, son objectif reste le même.

2.2.1 Positionnement de l'Ingénierie des Exigences

Avant d'appréhender mieux cette discipline et son objectif, nous commençons tout d'abord par définir *qu'est-ce qu'une exigence ?* Selon le standard [IEEE 1220, 2005], une exigence est un énoncé qui identifie un produit ou un processus, ou une caractéristique ou une contrainte opérationnelle, fonctionnelle ou de conception, qui est non-ambiguë, testable ou mesurable, et nécessaire à l'acceptabilité du produit ou du processus (par les parties prenantes ou les directives internes d'assurance qualité). Cette définition met en évidence plusieurs faces de l'exigence qui sont illustrées par la figure 2.1 et discutées comme suit :

- *Énoncé* : Un énoncé permet de définir la forme ou la structure d'une exigence. Lorsqu'il est sous forme textuelle, son interprétation peut être biaisée, néanmoins une exigence peut être énoncée sous forme de tableau comme le « Planguage » [Gilb, 2005], sous forme de diagramme comme les diagrammes UML [UML, OMG, 2003], ou encore en notations formelles comme la méthode B [Abrial, 1996]. Le plus important est d'obtenir un ensemble d'éléments traçables et gérables définis comme des exigences.
- *Produit ou processus* : une exigence peut définir des produits ou des processus pour les utiliser. Ainsi, des exigences liées à la qualité du produit et aux contraintes de son développement peuvent être stipulées.
- *Caractéristique ou contrainte opérationnelle, fonctionnelle ou de conception* : D'après cette définition, la classification des exigences se décline en exigences fonctionnelles et exigences de conception. Les exigences non-fonctionnelles n'ont pas été évoquées car leur signification n'est pas claire d'après la même norme. Les caractéristiques de conception sont définies en termes de performance, de sûreté de fonctionnement, d'opérabilité, etc. Ainsi, nous pouvons déduire la définition implicite des exigences non-fonctionnelles qui peuvent être des exigences de qualité ou de performance.
- *Non-ambiguë* : La non-ambiguïté représente le niveau de clarté avec lequel une exigence doit être exprimée pour être comprise de manière unique par toutes les parties.
- *Testable ou mesurable* : Les exigences peuvent être utilisées pour tester l'acceptabilité de la solution. Afin de parvenir à ce résultat, les exigences doivent être quantifiées.

- *Nécessaire pour l'acceptabilité du produit ou du processus* : Cet aspect met en lumière le rôle multi-dimensionnel des exigences. En effet, elles permettent de définir ce qui doit être conçu et développé, et aussi comment la solution doit être testée et acceptée. En d'autres termes, les exigences influent l'ensemble du processus du développement de la première à la dernière phase.
- *Par les parties prenantes ou les directives internes d'assurance qualité* : Les exigences proviennent de plusieurs sources, à savoir les clients, les utilisateurs, les experts du domaine, les organismes de réglementation, etc. Ainsi, la solution finale doit couvrir les points de vue divergents de toutes ces sources.

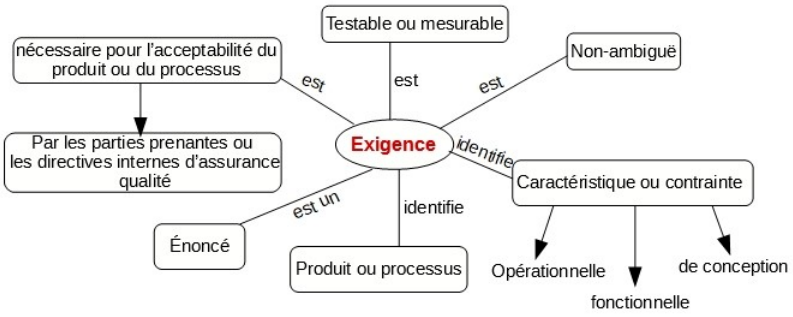

Figure 2.1 – Définition de l'exigence par la norme [IEEE 1220, 2005]

En génie logiciel, la définition d'une exigence est constituée des trois éléments suivants par la norme [IEEE 610.12, 1990] :

1. Une condition ou une capacité dont un utilisateur a besoin pour résoudre un problème ou atteindre un objectif (exigence du client).
2. Une condition ou une capacité que doit posséder un produit ou un composant de produit pour remplir un contrat, se conformer à une norme, une spécification ou tout autre document imposé formellement (exigence du système).
3. Une représentation documentée d'une condition ou d'une capacité comme définies ci-dessus dans **(1)** et **(2)**.

Après avoir introduit son concept central, nous nous focalisons sur l'IE qui est définie comme une approche systématique de spécification et de gestion des exigences qui a pour objectif de [Glinz, 2011] :

1. Prendre en connaissance les exigences principales, atteindre un consensus entre les parties prenantes par rapport à ces exigences, les documenter en s'appuyant sur des standards et les gérer systématiquement ;
2. Comprendre et documenter les besoins et les souhaits des parties prenantes ;
3. Spécifier et gérer les exigences afin de minimiser le risque de délivrer un système non conforme aux besoins et attentes des parties prenantes.

À partir de ces trois objectifs, nous pouvons déduire que l'IE est impliquée tout au long du cycle de vie du système partant de l'identification des besoins des parties prenantes, l'analyse des exigences pour en dériver d'autres, jusqu'à la documentation des exigences pour la spécification et leur validation à l'égard des besoins des parties prenantes. Par ailleurs, l'IE est ancrée dans le défi de réduction de la fréquence des problèmes de développement du système en mettant en œuvre en amont des méthodes permettant de garantir d'une manière systématique la prise en compte des exigences.

Dans le contexte de l'IS, l'AFIS admet explicitement que l'implication de l'IE ne peut pas être résumée à la première phase spécifiant ce que doit faire le système. En effet, il s'agit d'une combinaison des macro-activités « *développer* et *gérer* les exigences » qui visent à obtenir un référentiel des exigences validé par les parties prenantes et à le maintenir dans le temps. Ceci réside dans l'importance de produire une spécification des exigences complète, cohérente et précise pour maîtriser leurs changements au cours du temps.

Afin d'assurer leur développement et leur gestion efficace, la distinction doit être établie entre les domaines impliquant les parties prenantes pertinentes pour chaque niveau de développement des exigences. En effet, les phases de développement associées aux haut niveaux de description du système, à savoir l'énoncé des besoins et des exigences des parties prenantes doivent être ancrées dans le *domaine du problème*. Par ailleurs, les niveaux ultérieurs qui commencent des exigences du système jusqu'à l'architecture du système opèrent dans *le domaine de la solution*. La figure 2.2 représente le périmètre des besoins et des niveaux abstraits et concrets des exigences qui caractérisent respectivement les exigences du client et les exigences du système.

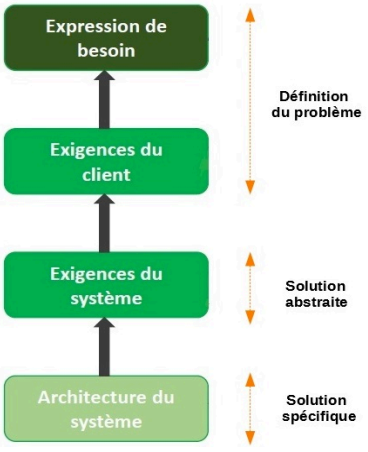

Figure 2.2 – Les niveaux d'abstraction des exigences

Après avoir présenté le positionnement de l'IE dans le développement des systèmes, nous détaillons les phases de ce processus ainsi que les concepts correspondants dans la section suivante.

2.2.2 Concepts de base de l'Ingénierie des Exigences

L'IE permet de définir une solution qui satisfait au mieux aux attentes et aux besoins des parties prenantes durant tout le cycle de vie du système. De ce fait, la transition entre les besoins et les exigences constitue un des enjeux majeurs du processus de l'IE. Cette étape impacte la conformité de la solution obtenue et peut conduire dans certains cas à des erreurs qui apparaissent tard dans un projet et sont coûteuses pour les corriger. On parle ici de l'« effet tunnel » qui peut être aggravé par un « effet de levier » stipulant qu'une erreur apparue dans une étape peut conduire à d'autres dans les étapes ultérieures [Sommerville, 2013]. Entre les besoins et les exigences, la perception du système ainsi que l'interprétation des problèmes peuvent entraîner des conflits de compréhension et de communication entre les différentes parties impliquées. En effet, un besoin définit la perception du système du point de vue utilisateur, tandis qu'une exigence est liée à la vision du système du point de vue concepteur ou développeur [Essame, 2002]. Par ailleurs, la perception de la solution désirée doit avoir une seule compréhension indépendamment de l'angle de vision du système. Ce consensus entre les partie prenantes est explicitement considéré dans la définition de l'exigence proposée par [Davis, 2013] : « *une exigence est une caractéristique observable de l'extérieur d'un système désiré* ». La figure 2.3 représente la transformation des besoins en exigences système techniquement satisfaisables et affinées en exigences techniques implémentables.

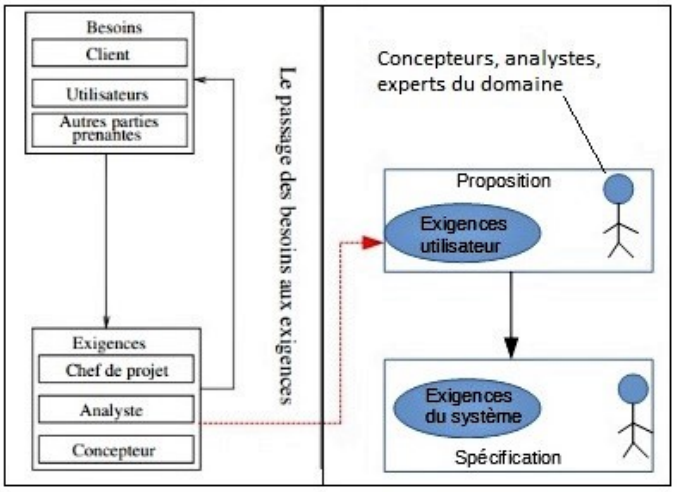

Figure 2.3 – La transition des besoins en exigences

La criticité de cette étape réside essentiellement dans la qualité de l'effort employé pour établir une spécification des exigences ; sachant que cette dernière doit satisfaire des critères requis pour la réussite de la mise en œuvre d'une solution. La satisfaction des besoins a pour objectif de répondre aux attentes des parties prenantes impliquées dans tout le cycle de vie de la solution délivrée. Les parties prenantes constituent tout individu, groupe de personnes, organisation ou toute entité ayant un intérêt direct ou indirect dans le

système. Ces parties peuvent être les agents participant à sa conception, son déploiement, sa maintenance et son retrait du service, mais aussi son utilisation et son exploitation avec ou sans impacts directs.

D'autre part, la satisfaction des contraintes opérationnelles et organisationnelles revêt une grande importance dans le cadre du développement des systèmes afin de maintenir leur performance. De toute évidence, la recherche d'un compromis entre les besoins des parties prenantes et les contraintes techniques relève de la mise en œuvre des paradigmes techniques et méthodologiques ainsi que du savoir-faire des experts du domaine. Après avoir présenté l'activité de l'IE et ses enjeux majeurs, nous entamons les phases de ce processus afin de mieux appréhender les étapes conduisant à la délivrance d'un système conforme aux besoins.

Le processus de l'IE est composé des phases successives d'**élicitation** (on trouve dans la littérature également le terme d'élucidation), de **modélisation**, d'**analyse**, de **spécification**, et de **validation** mises en parallèle avec la phase continue de **gestion** comme le montre la figure 2.4 [Nuseibeh et Easterbrook, 2000].

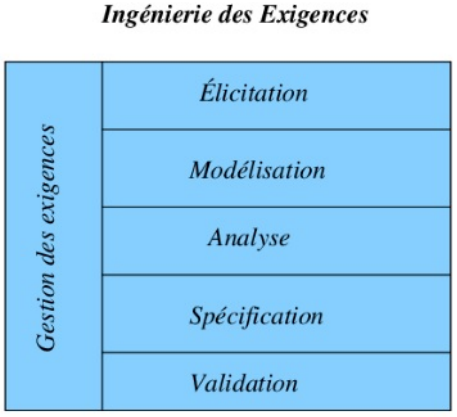

Figure 2.4 – Le processus de l'Ingénierie des Exigences [Nuseibeh et Easterbrook, 2000]

Le découpage de ce processus varie selon la perception du contexte par les différents auteurs ou selon la définition de ces activités dans les référentiels métier. [Kotonya et Sommerville, 1998], quant à eux ont fusionné la phase de modélisation et d'analyse en une seule phase d'analyse. Le référentiel CMMI (Capability Maturity Model Integration) [2] définit ces activités par les domaines de processus RD (Requirements Development) et REQM (Requirements Management) [Badreau et Boulanger, 2014]. Chacun de ces domaines de processus est décomposé en des objectifs à mettre en œuvre pour mener à bien le développement du système. D'autres référentiels comme l'IREB (International Requirements Engineering Board) [3] mettent en évidence 4 activités principales de l'IE, à savoir élucider, spécifier, valider et gérer les exigences [Badreau et Boulanger, 2014]. Les trois

2. http ://cmmis.free.fr/cmmi-dev/text/index.php
3. https ://www.ireb.org/en/landingpage/fr/

premières activités constituent les étapes qui mènent à la réalisation de la macro-activité « Développer les exigences » décrite dans la section 2.2.1. Ainsi, ce même référentiel inclut les phases d'analyse et de modélisation dans la spécification. Au delà de ces différentes visions, elles convergent vers un fond commun du processus de l'IE que nous illustrons par la figure 2.5.

Nous définissons les phases du processus de l'IE de la manière suivante :

— L'**élicitation**, également appelée élucidation, consiste en la collecte, la capture et la découverte des exigences à partir des différentes parties prenantes et d'autres sources légitimes afin d'affiner les exigences obtenues. Cette phase commence par une étape de préparation impliquant les différentes parties prenantes pour définir les restrictions ou les limites des domaines liés au système désiré. Cette étape est primordiale dans la phase d'élicitation car elle impacte les choix des parties prenantes et la catégorie des utilisateurs ainsi que l'identification des buts, des tâches, des cas d'utilisation et des scénarios. À l'issue de cette étape de préparation, la définition des besoins se poursuit pour déterminer le contour du domaine du système à développer et percevoir le domaine du problème. Cette perspective mettant en exergue les parties prenantes et le contexte du système permet d'acquérir les connaissances de base du domaine de l'organisation [Machado et Gomes, 2008]. Diverses méthodes et techniques sont utilisées dans cette étape comme le brainstorming, les interviews et la méthode de « Storytelling » [Machado et Gomes, 2006].

— La **modélisation** des exigences est définie comme la représentation graphique ou la description abstraite du problème réel afin de mieux comprendre et simuler les domaines du *problème* et de la *solution*. Elle vise principalement l'abstraction d'une réalité pour avoir une compréhension commune et une interprétation unique. La modélisation concerne les deux vues *statique* et *dynamique* du système et inclut différents niveaux/patrons de modélisation [Badreau et Boulanger, 2014]. Ainsi, elle porte sur la perspective *structurelle* du système liée aux données et à la structure des informations globales du système. Il s'agit de la modélisation primaire qui perçoit le système du point de vue utilisateur pour décrire une vue abstraite des modèles conceptuels des données comme le diagramme entité-association ou les diagrammes de classe UML. Lorsque la modélisation est utilisée pour comprendre la perspective *fonctionnelle* ou encore *comportementale*, on parle de la modélisation dynamique du système. Nous pouvons citer les diagrammes d'activités UML pour modéliser les exigences d'une perspective fonctionnelle et les diagrammes d'état pour modéliser le comportement du système. Nous discutons en détail cette phase dans la section 2.2.3.

— L'**analyse** constitue l'interprétation des exigences issues de la phase de modélisation afin d'obtenir une clarification des frontières du système et son interaction avec son environnement. Elle permet de supprimer les incohérences et résoudre les conflits

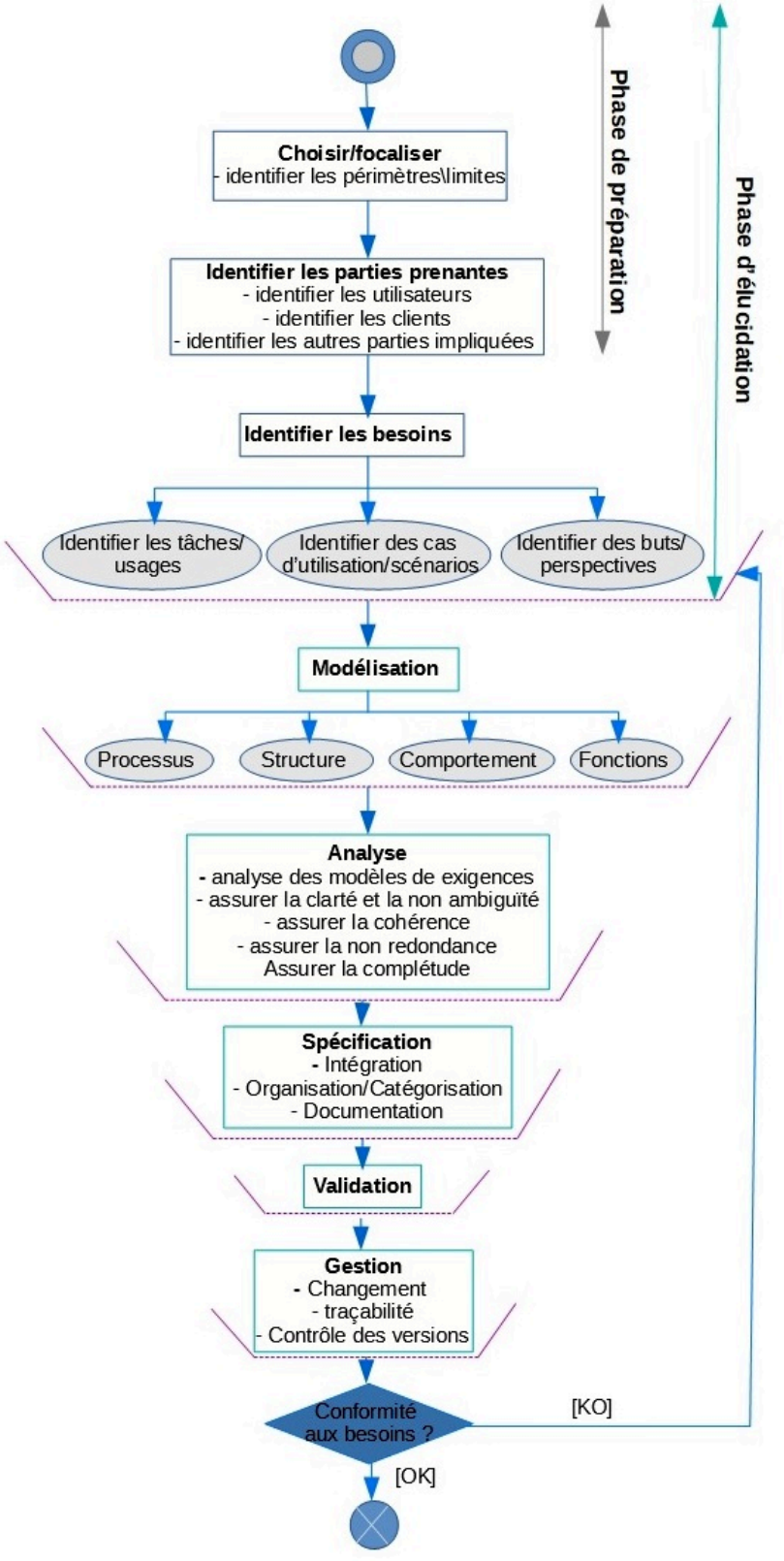

Figure 2.5 – Les phases détaillées de l'Ingénierie des Exigences

souvent par la négociation des meilleurs compromis afin d'obtenir un agrément partagé. Elle réduit et vérifie les exigences en éliminant les redondances et les incomplétudes pour définir le domaine du problème et les effets requis. Les techniques d'animation des exigences sont souvent utilisées dans la phase d'analyse [Liu et Wang, 2007].

— La **spécification** permet d'établir le document final des exigences constituant la base contractuelle entre les parties. Il est convenu d'utiliser des gabarits de rédaction et des glossaires pour générer un document permettant d'avoir une vision commune du système [Badreau et Boulanger, 2014]. Ainsi les exigences sont intégrées et classées suivant les types, les niveaux d'abstraction et les priorités. Autrement dit, l'intégration des exigences selon les différentes perspectives définit le comportement du système qui va produire les effets désirés dans le domaine du problème issus de la phase d'analyse.

— La **validation** se focalise sur la validation de la version finale du document des exigences pour s'assurer de la conformité de la spécification aux besoins et aux attentes des parties prenantes [ANSI, EIA-632, 1999]. En effet, l'objectif de cette phase vise à détecter les omissions et les déviations par rapport aux fonctionnalités attendues du système. Diverses techniques formelles sont utilisées notamment la méthode B et le model checking [Baier et Joost-Pieter, 2008] afin de certifier que les exigences satisfont les attentes des parties prenantes, et que leur qualité est conforme aux critères requis par les standards et les référentiels de bonnes pratiques du métier.

— La **gestion** permet de suivre l'évolution des exigences face aux différents changements technologiques, organisationnels et opérationnels. En effet, elle contribue à la traçabilité et au stockage des différentes versions des exigences. Par ailleurs, la gestion des exigences est une activité continue durant tout le cycle de vie afin de garder la trace des changements perçus et leur impact sur la cohérence globale initialement déterminée [Badreau et Boulanger, 2014]. La traçabilité est nécessaire à l'identification de l'impact des changements des exigences sur les autres éléments du système afin d'établir une preuve de validation des exigences vis-à-vis aux besoins du monde réel (domaine du problème). Elle sert principalement à capturer les justifications nécessaires pour la conception du système ainsi que les différents niveaux des exigences. En d'autres termes, il s'agit d'une phase intégrante du processus de l'IE qui permet d'évaluer l'impact de changements mais aussi de maintenir le référentiel établi entre les parties prenantes. Par conséquent, elle contribue à la réduction des risques des erreurs coûteuses ainsi que les coûts de maintenance.

Il est clair que l'IE joue un rôle fondamental dans le processus du développement des

systèmes, et en particulier les SCS car elle met en jeu l'aspect critique des exigences de sécurité. Le développement d'un système sûr relève de la rigueur de la démarche collaborative de l'IE, notamment la qualité des exigences spécifiées, leur perception, leur modélisation et les mécanismes appliqués pour maintenir la cohérence de ces exigences face aux divers changements. En effet, les exigences de sécurité, comme toutes les autres exigences, doivent être conformes aux attentes pour diminuer la fréquence des problèmes de développement en amont.

Dans le cadre de cette thèse, nous nous intéressons à la phase de modélisation et de gestion des exigences. Ces deux phases ont un impact majeur sur le succès de développement d'un système qui délivre le service désiré tout en respectant les contraintes et les restrictions imposées par les organisations. Dans la section suivante, nous discutons les paradigmes de l'IS utilisés pour mener à bien ces activités de l'IE.

2.2.3 Ingénierie des Exigences Basée sur les Modèles (IEBM)

D'un point de vue collaboratif du processus d'IE, les enjeux majeurs consistent à réduire la complexité du problème et améliorer la communication entre les équipes impliquées afin de cerner le problème et d'unifier sa compréhension. En effet, la décomposition et l'analyse du problème s'appuie sur des interactions multiples entre les acteurs multidisciplinaires afin d'avoir une communication efficace et une interprétation commune. De ce fait, la spécification des exigences du système doit correspondre au degré de compréhension des concepteurs, développeurs et des experts du domaine de ce qui est exigé et à leur capacité à délivrer la bonne ou, du moins, la solution satisfaisante. Par ailleurs, l'INCOSE (International Council on Systems Engineering) [4] admet l'importance de la compréhension, l'élucidation et l'analyse des exigences des parties prenantes (client) comme un facteur clé de succès, à travers son référentiel [SE Handbook Working INCOSE and others, 2011]. Ce dernier est adopté par l'AFIS comme un référentiel international qui est complété par son ouvrage de référence nommé « Découvrir et comprendre l'ingénierie système », représentant sa vision pédagogique. Il est donc essentiel d'organiser une révision des exigences du système avec toutes les parties prenantes et obtenir l'approbation, par celles-ci, du périmètre de la solution à proposer.

Le langage naturel est le medium principal de la communication sur les exigences entre les acteurs. Universel et flexible, ce langage ne nécessite ni une formation particulière ni un cadre outillé spécifique. Néanmoins, la communication basée sur le langage naturel est sujette à des multiples interprétations pouvant induire des écarts entre les besoins des parties prenantes et les exigences du système spécifiées. Par conséquent, la recherche d'un compromis sémantique entre le modèle mental des besoins construit par les parties prenantes, les connaissances du domaine, les exigences du système et les compétences fonctionnelles et techniques est une tâche critique qui repose sur une culture partagée

4. https ://www.incose.org/

ambiguë. Dans ces premières phases de développement, une compréhension inadéquate du domaine du problème et des mauvaises interprétations du domaine de la solution aboutit, de toute évidence, à la délivrance d'un système non conforme aux fonctions attendues.

Dans un objectif de comblement des lacunes de compréhension et de communication, le paradigme de l'ingénierie des exigences a été progressivement basculé du langage naturel vers un **modèle** [SE Handbook Working INCOSE and others, 2011], [Fockel et Holtmann, 2014], [Bijan *et al.*, 2013]. En effet, la discipline d'utilisation des modèle intégrés durant le cycle de vie du développement des systèmes-Ingénierie Système Basée sur les Modèles (ISBM)- se révèle prometteuse pour le paradigme de l'Ingénierie des Exigences Basée sur les Modèles (IEBM). À ce stade se pose la question suivante : « *Qu'est ce qu'un modèle ?* ». Nous pouvons le définir, en effet, comme une image ou une représentation abstraite de la réalité existante ou à concevoir afin de simplifier ses aspects pour un objectif donné [Rothenberg *et al.*, 1989]. Le modèle est caractérisé par trois notions importantes définies comme suit :

1. Représentation de la réalité : Chaque modèle représente certains aspects de la réalité perçue en des éléments graphiques. La création des modèles peut être descriptive ou prescriptive. Dans le cas de la construction descriptive du modèle, ce dernier est un support de documentation de la réalité existante. Dans un contexte prescriptif, le modèle sert comme prototype de la réalité fictive. Indépendamment de la perspective de la modélisation, les modèles peuvent être à la fois descriptifs pour les concepteurs et les développeurs et prescriptifs à l'égard du client qui imagine le système à développer. L'unicité du modèle partagé entre les acteurs est un atout majeur pour obtenir une solution satisfaisante.
2. Réduction de la complexité de la réalité : Il est important de décomposer et analyser finement le problème et la solution. En effet, la séparation du domaine du problème et de la solution est importante dans la modélisation. Dans le premier domaine, seulement les aspects pertinents pour l'univers de discours du système ou au regard des parties prenantes et du contexte sont modélisés. Dans le second domaine, les objets liés au système sont considérés dans la modélisation.
3. Propriété pragmatique : Un modèle est toujours établi pour un but donné et dans un contexte spécifique. L'objectif de modélisation varie selon la perspective de vision du système ainsi que le désir de l'acteur concerné. Idéalement, un modèle ne doit contenir que les éléments nécessaires et suffisants pour satisfaire l'objectif défini.

Dès lors, les exigences basées sur les modèles graphiques permettent d'améliorer la communication et d'assurer la compréhension commune et précise en échangeant les différents points de vue. Leur aspect graphique permet de mieux percevoir et mémoriser les informations visuelles par rapport aux textes, de cerner le périmètre de chaque acteur et de collaborer efficacement. Des langages spécifiques sont utilisés pour créer des modèles dont chacun est caractérisé par une *syntaxe* et une *sémantique* bien déterminées :

— Syntaxe : La syntaxe d'un langage de modélisation définit les éléments utilisés et spécifie leurs combinaisons valides.
— Sémantique : La sémantique définit le sens des éléments de modélisation et sert par la suite comme un fondement d'interprétation des modèles.

Les langages de modélisation sont classés en informel, semi-formel et formel, suivant le degré de formalisation. Ce degré dépend de la magnitude des définitions formelles ou encore du formalisme d'exactitude qui définit la syntaxe et la sémantique du langage. Ainsi, les modèles qui documentent les exigences du système sont appelés *les modèles des exigences*. Dans cette section, nous nous intéressons au langage de modélisation semi-formel UML permettant d'avoir une vue structurée et multi-perspectives des exigences du système [UML, OMG, 2003]. Ayant une syntaxe précise et standardisée, le langage UML et son extension SysML (System Modeling Language) sont largement utilisés dans la modélisation des exigences.

Il est convenu de faire la différence entre les modèles des exigences et les modèles de conception. Les modèles de conception documentent les solutions choisies durant le développent du système, tandis que les modèles des exigences représentent une vue « en boîte noire » des aspects spécifiques du problème. La propriété d'abstraction des modèles permet de satisfaire les différentes perspectives de documentation des exigences, du point de vue du domaine du problème ou celui de la solution. Par ailleurs, la combinaison des modèles et du langage naturel s'avère avantageuse pour la documentation afin de corréler les modèles des exigences avec des informations additionnelles. La figure 2.6 représente les différentes formes de documentation des exigences tirant profit de chaque phase de modélisation.

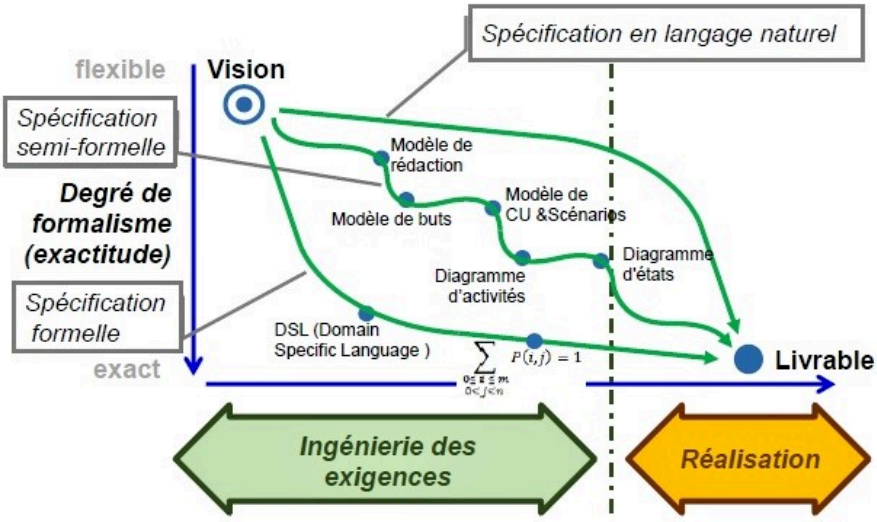

Figure 2.6 – Formes de documentation des exigences basée sur les modèles [Badreau et Boulanger, 2014]

Du point de vue documentation et communication des exigences, la modélisation permet de fournir un langage commun entre les acteurs impliqués dans le processus de l'IE ainsi qu'un support de raisonnement sur l'analyse du problème et sur la solution à concevoir. Ainsi, elle limite les ambiguïtés et les incompréhensions inhérentes au langage naturel grâce à l'abstraction, la syntaxe et la sémantique. De ce fait, différents types de modélisation sont mis en œuvre pour chaque niveau d'abstraction des exigences. La figure 2.7 récapitule la correspondance entre la modélisation et les différents niveaux des exigences.

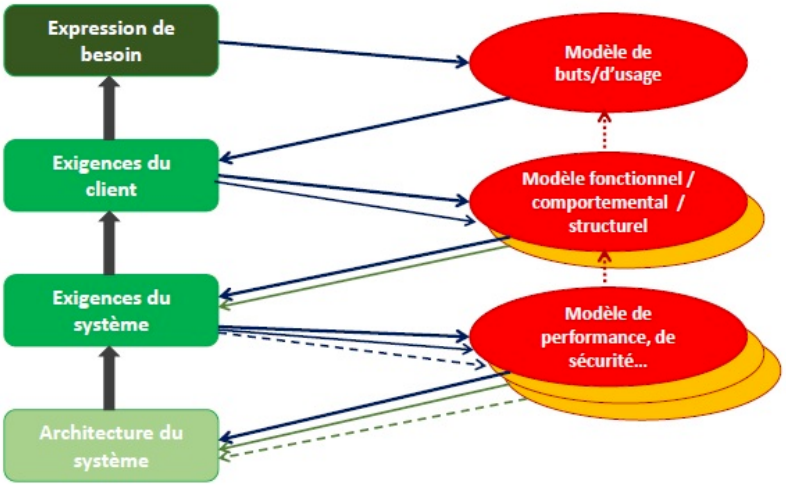

Figure 2.7 – Correspondance entre la modélisation et les différents niveaux des exigences

Dans une perspective de réduction de la complexité du problème et de la solution, les deux domaines sont considérés séparément dans la modélisation afin de se focaliser sur des aspects spécifiques du système impliquant les parties prenantes concernées. Dans le domaine du problème, les pratiques de l'analyse recommandent de commencer par la considération explicite des *buts* représentant les intentions des parties prenantes (utilisateurs) [Van Lamsweerde, 2001] et [Yu, 2011]. Ce principe découle du fait que les buts représentent les exigences de haut niveau et permettent d'affiner la vision du système du « pourquoi » vers le « comment ». Ayant un impact majeur sur la compréhension et la qualité des exigences, les méthodes ont évolué pour couvrir cet aspect dans le processus de l'IE et ont donné lieu à une activité prenant en considération l'aspect intentionnel de la solution à concevoir, à savoir l'Ingénierie des Exigences Dirigée par les Buts (IEDB). En effet, il ne s'agit pas d'une discipline séparée de l'IE mais d'une méthode prescriptive permettant de guider le développement des exigences et de faire face à la complexité de leur gestion d'une manière cohérente et structurée. La modélisation et la documentation des buts diffèrent suivant l'approche utilisée, à savoir l'approche KAOS (Keep All Objectives Satisfied) [Dardenne *et al.*, 1993, Van Lamsweerde, 2001], le framework i* [Yu, 2011], Techne [Borgida *et al.*, 2009], etc. Nous discutons ces approches dans le chapitre 4.

La figure 2.8 illustre la perspective de modélisation des exigences dans les domaines

du problème et de la solution. À l'issue de la phase de modélisation dirigée par les buts, la modélisation et la documentation des fonctionnalités de la solution à concevoir peuvent s'effectuer à l'aide des diagrammes de cas d'utilisation. Ces derniers permettent de modéliser les fonctions du système désiré d'un point de vue utilisateur ainsi que leurs inter-dépendances et les relations avec leur environnement. La spécification des cas d'utilisation est établie grâce à des gabarits de rédaction afin de documenter les scénarios qui en découlent. Ces modèles constituent des atouts majeurs d'analyse du problème et de compréhension des exigences du client ainsi que leur contexte grâce au principe d'abstraction du problème.

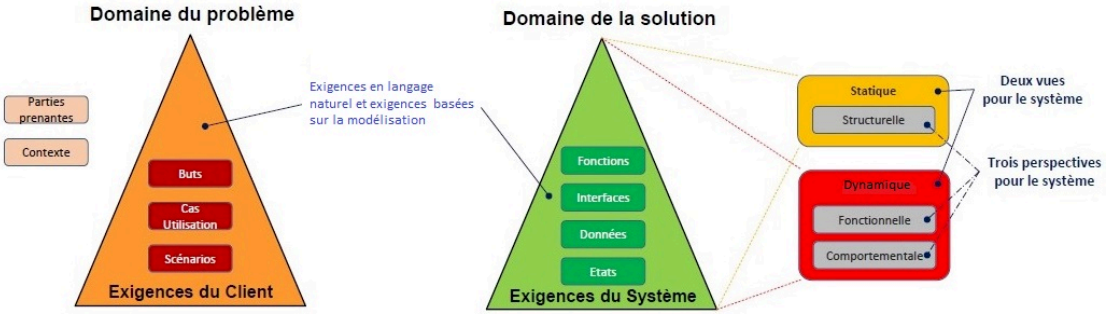

Figure 2.8 – Modélisation des exigences dans les domaines du problème et de la solution

Du principe de décomposition du problème vers la modularité de la solution, le domaine de la solution se focalise sur la modélisation séparée des vues du système statique et dynamique. Comme discuté dans la section 2.2.2, les patrons de modélisation (Modelling patterns) des exigences distinguent les trois perspectives du système en utilisant les langages de modélisation adaptés [Davis, 2013], [Pohl, 2010] :

— La perspective structurelle (données) : Dans cette perspective, la structure des données ainsi que les aspects à structure statique, tels que les fonctions d'usage et les relations de dépendance du système avec le contexte sont documentés en se basant sur les modèles comme les diagrammes d'entité-association [Chen, 2002] et les diagrammes de classe UML [UML, OMG, 2003].

— La perspective fonctionnelle : Cette perspective documente les informations du contexte qui sont manipulées par le système à développer ainsi que les données transmises par ce dernier au contexte. Les diagrammes d'activités UML sont les plus utilisés pour modéliser cette perspective des exigences.

— La perspective comportementale : Cette perspective s'intéresse à la documentation du comportement du système en s'appuyant sur ses états. Par exemple, la documentation de la réaction du système vis-à-vis d'un ensemble d'événements, la documentation des conditions qui déclenchent le changement d'état ou encore la documentation des effets du système sur son environnement font partie de cette perspective de modélisation des exigences. Afin de modéliser le comportement dynamique du système, les approches de modélisation basées sur la théorie des automates

sont généralement utilisées. Ainsi l'aspect réactif du comportement du système peut être modélisé par le biais des diagrammes d'état UML.

À la lumière de ce qui précède, nous admettons l'intérêt de la discipline d'IEBM pour la spécification des exigences mais aussi pour d'autres phases et aspects de l'IE dont nous récapitulons les avantages comme suit :

— Élucidation des exigences : La modélisation permet d'améliorer la complétude du référentiel structuré des exigences avec d'autres techniques.
— Analyse et vérification : La fabrication d'artefacts d'analyse et de conception ainsi que les capacités d'assurer la non-ambiguïté, la consistance et la complétude sont possibles grâce à la modélisation.
— Gestion des exigences : La modélisation garantit la structuration et la cohérence des exigences en gardant la traçabilité des exigences et leurs relations avec les autres éléments de conception. Ainsi, elle facilite la réutilisation des patrons de modélisation des exigences pour les nouveaux systèmes et la maintenance des exigences face aux divers changements.
— Communication entre les parties prenantes : l'abstraction, la formalité et la modélisation multi-vue offrent une base de raisonnement interprétable par la machine et améliorent la collaboration entre les parties prenantes.

Dans le cadre de cette thèse, nous nous intéressons aux avantages de la modélisation pour faire face aux évolutions des exigences, limiter les problèmes de compréhension et améliorer la communication entre les équipes impliquées dans la conception des (SCS). L'aspect critique de sécurité intégré dès les premières phases de conception implique le partage multidisciplinaire et la collaboration des différentes équipes notamment, les analystes de sécurité, les ingénieurs de sécurité, les ingénieurs des exigences, les concepteurs et les experts du domaine d'application du système.

Ainsi, le niveau d'abstraction joue un rôle fondamental dans l'intérêt de la modélisation pour partager différentes connaissances des domaines. En effet, le degré d'exactitude utilisé, dans un stade initial de conception, pour modéliser les exigences et les éléments associés ne peut toujours pas lever l'ambiguïté de la sémantique et de la syntaxe. Le degré d'exactitude élevé peut, parfois, poser une hétérogénéité sémantique de telle façon qu'une notion peut avoir plusieurs interprétations ; cela peut engendrer des conflits de communication. Autrement dit, les éléments des modèles pertinents pour une partie prenante ne le sont pas obligatoirement pour d'autres qui ont une vision différente du système ou s'intéressant à d'autres aspects. Par exemple, la spécification des exigences de sécurité implique à la fois la mise en œuvre des connaissances de l'ingénierie de sécurité et de l'ingénierie des exigences. De ce fait, tous les éléments de l'analyse de sécurité du système doivent être modélisés séparément avec un haut niveau d'abstraction. Par conséquent, l'efficacité de la communication relève de la propriété pragmatique du modèle partagé afin de mener à bien le développement du système.

Si les exigences jouent un rôle central dans le développement des SCS, leur cohérence doit être maintenue durant leur cycle de vie. En effet, la traçabilité des exigences permet de comprendre la transformation des exigences de haut niveau vers des exigences du système et de garder la trace des relations entre les différents niveaux du développement du système. Le choix des mécanismes mis en œuvre pour assister la traçabilité des exigences impacte les choix de conception ainsi que toutes les phases de développement du système. Dans un contexte des SCS, la tâche devient complexe face aux changements organisationnels, techniques et opérationnels. Généralement, les standards recommandent l'utilisation du cycle en V dans le développement des SCS afin de gérer et garder la trace des évolutions des exigences. L'analyse d'impact des changements perçus permet de cerner les choix de conception, établir un compromis de coût/bénéfices des changements et suivre l'avancement du développement tout en évitant les conflits dans des phases ultérieures. La figure 2.9 représente le rôle de la traçabilité dans le cycle du développement des systèmes.

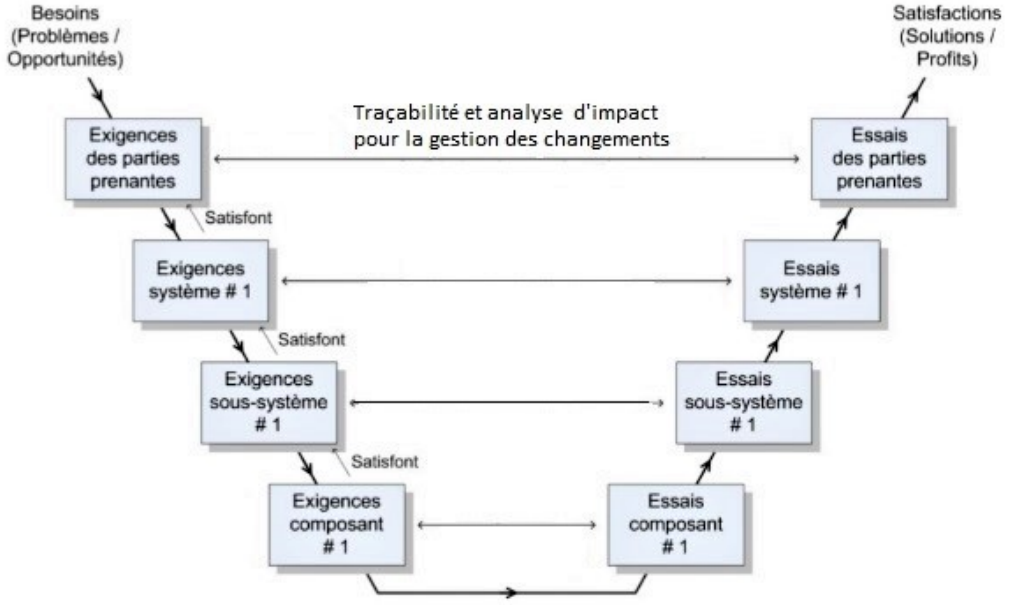

Figure 2.9 – Le rôle de la traçabilité des exigences dans la gestion des changements

L'intégration des exigences de sécurité dans le modèle de conception nécessite le maintien d'une structuration et d'une cohérence durant leur cycle de vie. Leur aspect émergent et leur adaptation dynamique au contexte opérationnel constitue un enjeu majeur de la phase de gestion. Par ailleurs, la gestion des changements des exigences nécessite un cadre structuré permettant d'assurer la cohérence globale du système et de son environnement. Afin de répondre à la problématique de nos travaux de recherches, nous estimons que la représentation structurée des connaissances des domaines est capable d'abstraire les vues, de lever les ambiguïtés de compréhensions et de fournir une base de raisonnement et de cohérence globale des exigences. Nous entamons dans la section suivante la notion de **conceptualisation**, nous introduisons ses fondements et justifions son intérêt dans notre

étude.

2.3 De « la modélisation » vers « la conceptualisation »

La conceptualisation d'un problème constitue une activité cruciale dans le développement d'un système. Elle est définie comme une vue abstraite et structurée d'une partie de la réalité, contenant les objets et les entités, jugés nécessaires pour satisfaire un objectif spécifique, ainsi que les relations entre eux [Gruber, 1993]. En effet, la collaboration de plusieurs acteurs ayant différentes connaissances des domaines vise à réaliser un objectif commun, à savoir obtenir un système performant et satisfaisant les besoins. Les parties prenantes construisent souvent un *modèle mental* de la solution, sur laquelle ils se fixent, même si elle n'est pas adéquate, appropriée, ou proche de l'optimale. L'alignement de ce modèle mental avec les exigences du système spécifiées et leur intégration dans l'architecture du système nécessite la définition d'*un pont sémantique* permettant de l'établir et le maintenir durant le cycle de vie.

La conceptualisation permet de partager un modèle commun mais multi-vues qui se focalise sur un objectif unique mais dont chaque vue traite un aspect particulier de la conception des SCS. La représentation des connaissances s'appuie sur les *ontologies* et s'articule dans la discipline de l'*Ingénierie des Connaissances* (IC) que nous abordons dans la section suivante.

2.3.1 Ingénierie des Connaissances & Ontologies

Dans le cadre du développement des SCS, une variété de connaissances tacites, explicites, structurées et non structurées est mise en œuvre pour analyser le problème et répondre aux besoins. Les connaissances diversifiées et multi-domaines nécessitent un cadre structuré permettant leur acquisition, leur partage et leur réutilisation. Ces activités constituent la discipline de l'Ingénierie des Connaissances (IC) qui permet de modéliser le problème d'une manière formelle afin d'obtenir la solution satisfaisante [Charlet, 2003]. En effet, l'IC est une approche systématique qui vise à recueillir et structurer un raisonnement afin de guider la manière d'aboutir à la solution. Domaine actif de l'intelligence artificielle, le cadre théorique de l'IC consiste à concevoir un système dont le fonctionnement permet d'opérationnaliser des connaissances portant sur la résolution d'un problème donné [Charlet, 2004]. Autrement dit, elle repose sur trois objectifs majeurs tels que la modélisation du problème, la méthode de résolution dans un contexte spécifique et l'opérationalisation du modèle obtenu. Le raisonnement suivi dans le choix des ontologies pour résoudre la problématique de cette thèse est illustré par la figure 2.10.

Comme toute ingénierie, l'IC s'appuie sur le paradigme Processus-Méthodes-Outils. Le processus de l'IC porte sur la transformation des connaissances psychologiques ou empiriques des experts afin de les implémenter dans un système expert. Cette transformation

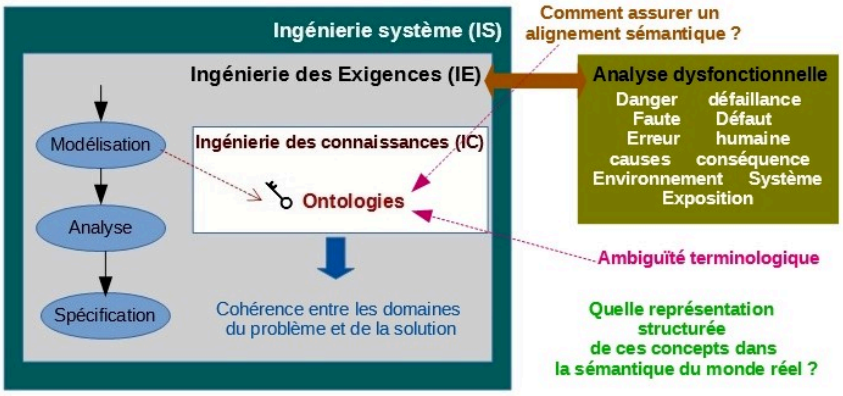

Figure 2.10 – Raisonnement pour le choix des ontologies

est menée en trois étapes principales : *le recueil, la modélisation et la représentation des connaissances*. Carrefour multidisciplinaire de réflexions, l'IC met en exergue les méthodes empruntées par diverses disciplines, à savoir :

— la psychologie cognitive pour élaborer les techniques d'élucidation ;
— la linguistique pour formuler des connaissances ;
— l'informatique pour opérationnaliser les modèles formels ;
— l'ergonomie pour interpréter le comportement du système opérationnel ;
— la sociologie pour gérer le système dans son environnent organisationnel.

Avant d'appréhender les trois étapes de l'IC, nous avons évoqué son mot clé *connaissances* sans le définir. Nous définissons une **connaissance** par une information, une donné ou un savoir individuel ou collectif exploité dans un contexte donné. Par ailleurs, elle repose sur trois caractéristiques : dépendance avec un environnement technique, interprétation humaine et outil informatique pour la mémoriser [Charlet, 2004].

La figure 2.11 récapitule les phases du processus de l'IC que nous décrivons comme suit :

- **Le recueil ou l'élucidation des connaissances** constitue une étape cruciale de familiarisation avec le domaine d'expertise ou de l'activité pour cerner le contexte et identifier les sources des connaissances.
- **La modélisation des connaissances** représente un véritable enjeu de l'IC permettant de modéliser et structurer de manière qualitative les connaissances. Elle permet de construire des modèles adaptés à la nature des connaissances pour pouvoir ensuite les représenter dans des formalismes adéquats.
- **La représentation des connaissances** est élaborée de manière à ce que la mémorisation, l'extraction, l'inférence et le raisonnement soient possibles sans impact sur les caractéristiques requises des connaissances. Ces caractéristiques sont la complétude, la consistance, l'accessibilité, la réutilisation, etc.

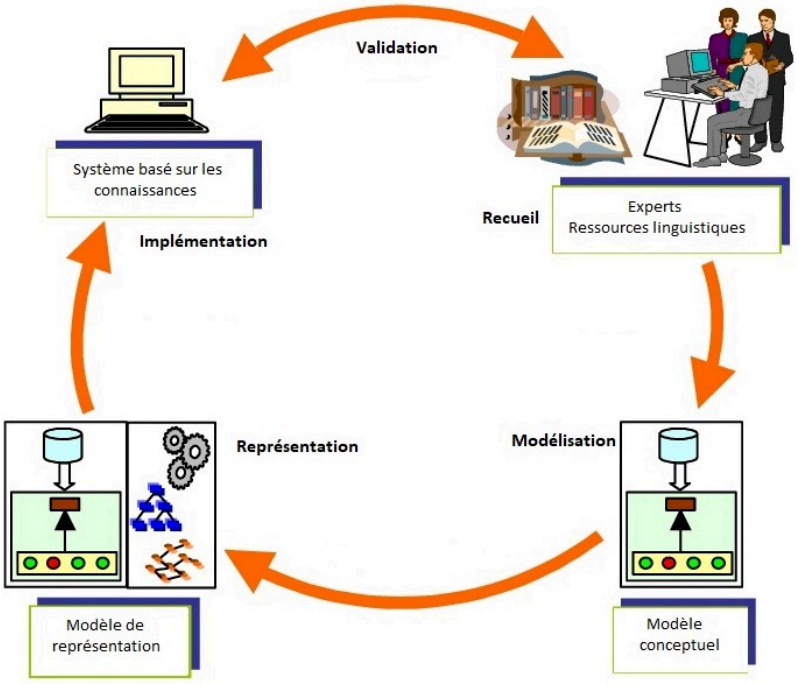

Figure 2.11 – Le processus de l'Ingénierie des Connaissances

Dans la phase de recueil des connaissances, les sources constituent les perspectives relatives au contexte du problème à résoudre, notamment des documentations techniques, des ouvrages de référence, des manuels propres au domaine concerné, ou bien encore la transcription d'interviews menées avec des spécialistes. Diverses techniques de recueil sont utilisées selon la nature des sources et du domaine d'application. Il s'agit d'une étape nécessaire pour savoir quelles connaissances doivent être mises à plat pour capturer un domaine dans un corpus. Le corpus comporte l'expression des notions sous forme des unités linguistiques dont la modélisation est jugée nécessaire. Une première vue du problème exige la sélection des unités linguistiques, appelées *concepts*, les plus pertinents pour représenter un problème. Autrement dit, on définit des concepts par des libellés linguistiques qui sont acquis, classés et organisés afin d'établir une base stable de primitives nécessaires à la modélisation des connaissances.

Dans la phase de modélisation, trois types de connaissances font l'objet de modèles distincts selon trois niveaux : les **connaissances du domaine**, les tâches et les méthodes. Les connaissances du domaine sont les connaissances relatives au domaine d'application et nécessaires à l'exécution des méthodes de raisonnement. Les tâches sont définis par les buts à atteindre par le système en utilisant des méthodes de raisonnement et en s'appuyant sur les connaissances du domaine. Il est convenu de différencier le niveau de modélisation des connaissances du domaine et de leur implémentation comme argué dans [Newell *et al.*, 1982]. De ce fait, une distinction consensuelle est établie en IC entre le *niveau de connaissances* (knowledge level) et le *niveau symbolique* (symbol level). Le premier niveau se

concentre sur le comportement du système et sur les types de connaissances impliquées dans la génération de tels comportements, indépendamment de son implémentation formelle. Ce niveau permet de modéliser le système comme un agent rationnel qui doit atteindre des buts (« le Quoi »), effectue des actions (« le Comment ») et dispose de connaissances et des lois de conduite (« le Pourquoi »). Le deuxième niveau s'intéresse aux techniques de calcul et structures de représentation (par exemple, règles, cadres) qui fourniront la base du système mis en place. Ce type de modélisation distingue le modèle de domaine qui représente le « Quoi », du modèle de raisonnement qui représente le « Pourquoi et Comment ».

La fusion de ce modèles forme la spécification du comportement de l'artefact à construire, appelé le *modèle conceptuel*. Les modèles conceptuels sont des descriptions abstraites des objets et opérations d'un système, formulées de manière à ce qu'elles capturent les intuitions que les humains ont de ce comportement. Le langage dans lequel les modèles conceptuels sont exprimés n'est pas le langage formel de techniques de calcul, mais le langage qui relie les phénomènes du monde réel au cadre cognitif de l'observateur. En ce sens, le modèle conceptuel est subjectif et relatif au vocabulaire et au cadre cognitifs de l'observateur humain. Ainsi, il doit être compréhensible et interprétable par un spécialiste du domaine. Un modèle opérationnel, défini au niveau des programmes, traduit en termes algorithmiques les connaissances formalisées du modèle conceptuel. Ce dernier est à la fois la spécification et le support de raisonnement du système opérationnel.

Définition 3 *(Modèle conceptuel). Le modèle conceptuel se caractérise par trois éléments principaux tels que les concepts, les relations et les fonctions. Les concepts réfèrent à la fois aux notions concrètes (objets, personnes) et abstraites (intention, événement, etc). Ce sont des blocs de construction mentaux utilisés par les êtres humains pour réfléchir sur un problème donné. L'ensemble des concepts impliqués dans la résolution du problème forme ce qu'on appelle l'univers du discours. Ainsi, la connectivité du concept permet son intégration dans un réseau formant des interconnections avec d'autres concepts. Ces interconnections représentent les relations entre les concepts dans un univers du discours. D'autre part, une fonction est un cas spécifique de relations où la valeur du dernier concept est unique pour les concepts précédents. Par exemple, le concept femme est unique pour le concept personne quand ils sont liés par la relation mère*Biologique_de*.*

Le modèle conceptuel est intéressant dans le contexte de développement des systèmes car il fournit un cadre sémantique partagé entre les différentes équipes impliquées. Il assure une communication efficace entre les acteurs et permet d'élaborer une représentation formelle des connaissances exploitable dans diverses perspectives comme la réutilisation, le raisonnement, l'aide à la décision, etc. Une parade méthodologique définie en IC, notamment CommonKADS (Knowledge Acquisition and Documentation Structuring) [De Hoog *et al.*, 1993], KOD (Knowledge On Demand) [Vogel, 1988] et MASK (Method for Analysing

and Structuring Knowledge) [Aries *et al.*, 2008], offre des guides et des lignes directives permettant de construire le modèle conceptuel. Ces lignes directives consistent principalement à définir le langage de modélisation, le vocabulaire et la démarche de modélisation.

Les langages de représentation des connaissances sont classées en deux familles : les *frames* et les *réseaux sémantiques* [Kayser, 1997]. Les frames représentent la description de la connaissance conceptuelle où les concepts sont exprimés sous forme de classes hiérarchisées. Proche d'une représentation orientée objet en informatique, les concepts sont des classes ayant des attributs/valeurs ainsi que des instances. Néanmoins, la différence essentielle entre les deux est que la représentation des connaissances exploite des descriptions déclaratives explicites, tandis que le paradigme orienté-objet est intrinsèquement procédural. D'autre part, les réseaux sémantiques sont des structures de description de connaissances sous forme de patterns ou motifs composés de nœuds (concepts) et des relations hiérarchiques entre eux (propriétés) [Sowa, 2014]. Ces relations expriment des liens sémantiques comme *est-un*, *partie-de*, *type-de*, etc. Les réseaux sémantiques peuvent être transformé en des notations formelles utilisant la logique propositionnelle. Un terme qui devient de plus en plus populaire dans les débats sur la représentation des connaissances est l'**ontologie**. Notion prometteuse dans divers domaines, l'ontologie représente le noyau de nos travaux. L'ontologie fait l'objet des sections qui suivent afin de définir ses caractéristiques et expliquer son intérêt pour répondre à notre problématique de recherche.

L'ontologie est une notion issue de la philosophie grecque et composée de deux mots : *ontos* [être] et *logos* [mot]. Ainsi, elle illustre la science de l'être ou de l'existence. De l'intelligence artificielle au web sémantique, l'ontologie représente une pierre angulaire de représentation des connaissances du domaine. Depuis la dernière décennie, elle est communément utilisée dans le domaine de l'informatique et a fait l'objet de normalisation [NF, ISO 21127, 2014]. Une première définition largement citée au sein de la communauté de l'IC et devenue une référence consensuelle est celle de [Gruber, 1993] :

≪ *Une ontologie est la spécification explicite d'une conceptualisation* ≫.

Dans cette définition, une spécification explicite est considérée comme une description formelle et une conceptualisation représente la manière de décrire un domaine avec un ensemble de concepts et de relations entre eux. En s'appuyant sur cette définition de Gruber, Borst a défini une ontologie comme suit [Borst, 1997] :

≪ *Une ontologie est une spécification formelle d'une conceptualisation partagée* ≫.

Ensuite, ces deux définitions ont été fusionnées et expliquées comme suit [Studer *et al.*, 1998] :

≪ *Une ontologie est une spécification formelle, explicite d'une conceptualisation partagée. La conceptualisation représente un modèle abstrait d'un phénomène en définissant ses concepts pertinents. Explicite signifie que le type des concepts utilisés ainsi que les contraintes de leur utilisation doivent être explicitement définis. Formelle veut dire que l'ontologie doit être compréhensible par la machine et l'être humain. Partagée reflète la*

notion que l'ontologie capture des connaissances consensuelles, qui ne sont pas restreint à un individu, mais accepté par un groupe ≫.

En vertu de ces définitions, nous pouvons considérer l'ontologie comme un réseau sémantique partagé et composé d'un ensemble structuré de concepts du domaine et de relations entre eux. Dans la section suivante, nous proposons une définition plus formelle de l'ontologie.

2.3.2 Fondements des ontologies

Nous proposons la définition 4 [Debbech *et al.*, 2018a] de l'ontologie comme une représentation structurée et partagée d'un domaine de connaissances constituée d'un ensemble de concepts, de relations, d'axiomes et d'une sémantique afin de les interpréter dans un univers du discours :

Définition 4 *(Ontologie). Supposons que O est une ontologie considérée comme un 5-tuple : O = {U, C, R, A, S} tel que :*

-U est l'univers du discours ;

-C est l'ensemble de concepts du domaine ;

-R est l'ensemble des relations binaires entre les concepts qui peuvent être taxinomiques ou sémantiques ;

-A est l'ensemble des axiomes pour restreindre les valeurs des concepts et des relations ;

-S est la sémantique utilisée pour interpréter les concepts et les relations entre eux.

L'univers ou le domaine du discours représente le domaine défini pour capturer ses connaissances à l'aide d'un ensemble de concepts. Les relations taxinomiques sont les relations de subsomption qui définissent une hiérarchie de concepts par abstraction des caractères communs afin d'aboutir à une organisation taxinomique. Les relations sémantiques sont les relations associatives, d'inclusion, d'alignement et des propriétés. Le premier argument de la relation est appelé ≪ *domaine* ≫ et le deuxième argument est appelé ≪ *co-domaine* ≫ donnant son échelle de valeurs. Par ailleurs, un ensemble d'axiomes formels sert à modéliser des contraintes sur l'ensemble des concepts et des relations. Ils permettent de déduire de nouvelles connaissances ou extraire des connaissances existantes par des règles d'inférence. L'intérêt majeur des axiomes réside dans leur capacité à vérifier la consistance de l'ontologie ainsi que les connaissances mémorisées. Enfin, la sémantique définit le vocabulaire spécifique utilisé pour établir une corrélation entre la représentation définie et le monde réel. La sémantique et la représentation des connaissances par les concepts et les relations établissent une *terminologie* permettant l'interprétation commune et la communication efficace entre les acteurs.

La classification des ontologies est établie en fonction du contexte de son utilisation et de l'objectif de sa mise en œuvre. Dans la section suivante, nous abordons les différents types des ontologies.

2.3.3 Différents types des ontologies

La typologie des ontologies varie selon leur usage et peuvent être divisées en quatre types : *les ontologies génériques*, *les ontologies du domaine*, les ontologies spécifiques à une tâche et les ontologies d'application [Guarino, 1998] :

- Ontologies génériques (Upper/top level ontologies) : elles gardent la notion philosophique originale d'≪ ontologie ≫. Ces ontologies visent à fournir des conceptualisations de notions de très haut niveau et indépendantes des domaines, telles que le temps, l'espace, les événements et les processus. Certains groupes ont publié des collections intégrées d'ontologies fondamentales. SUMO (Suggested Upper Merged Ontology) [5], DOLCE (Descriptive Ontology for Linguistic and Cognitive Engineering) [Gangemi *et al.*, 2002], BFO (Basic Formal Ontology) [Arp *et al.*, 2015], GFO (General Formal Ontology) [Herre, 2010] et UFO (Unified Foudational Ontology) [Guizzardi, 2005] en sont des exemples significatifs. Ainsi, elles permettent de concevoir des ontologies du domaine en fournissant des *patterns design* et des caractéristiques fondamentales à réutiliser. Nous discutons, en détail, de ces ontologies dans le chapitre 3 afin d'argumenter nos choix méthodologiques.
- Ontologies du domaine : elles spécifient une description d'un domaine particulier à l'aide d'un vocabulaire générique. Leur concepts sont considérés comme des spécialisations des concepts des ontologies génériques. Une ontologie du domaine représente une spécification sémantiquement riche d'un domaine sous forme d'une hiérarchie de concepts et d'une terminologie précise. Diverses ontologies de domaines ont été définies comme GORO (Goal-Oriented Requirements Ontology) dans le domaine de l'IEDB (GORE) [Negri *et al.*, 2017] et OntoPneumo pour le domaine de la pneumologie [Charlet *et al.*, 2009], etc. Les ontologies de domaine varient considérablement en termes de niveaux de formalisation. Des communautés de nombreux domaines ont publié des ensembles de concepts partagés sous forme de vocabulaires et de thésaurus. De tels schémas conceptuels ont généralement une structure sémantique relativement faible, indiquant de nombreuses relations hiérarchiques, qui correspondent le plus souvent à des relations de subsomption. Cela a provoqué une distinction dans la littérature entre les ontologies faibles et fortes. Le modèle SKOS [6], qui fait partie de l'effort du Web sémantique W3C, vise à permettre aux propriétaires de thésaurus de publier leurs schémas de concepts de manière interopérable, de sorte que le partage de ces concepts sur le Web devienne plus facile.
- Ontologies spécifiques à une tâche : elles spécialisent les ontologies du domaine en créant des patterns pour accomplir des tâches spécifiques. En général, les conceptualisations des connaissances du domaine nécessaires pour les algorithmes de raisonnement prennent la forme d'ontologies spécifiques à une tâche. Une ontologie

5. http ://ontology.teknowledge.com/
6. http ://www.w3.org/2004/02/skos/

spécifique à tâche spécifie des entités qui relèvent de la résolution d'un problème et fournit les définitions des concepts et relations utilisés pour spécifier un processus de raisonnement lors de la réalisation d'une tâche particulière.

- Ontologies d'application : elles fournissent des concepts et des termes liés à une application spécifique, tels que des informations sur les vues et la configuration. Elles décrivent le processus de raisonnement d'une façon indépendante d'un domaine et d'une implémentation donnée. Ainsi, elles permettent aux experts du domaine d'utiliser le même langage que celui de l'application.

La figure 2.12 représente la typologie des ontologies dont l'intérêt diffère d'un contexte d'application à un autre.

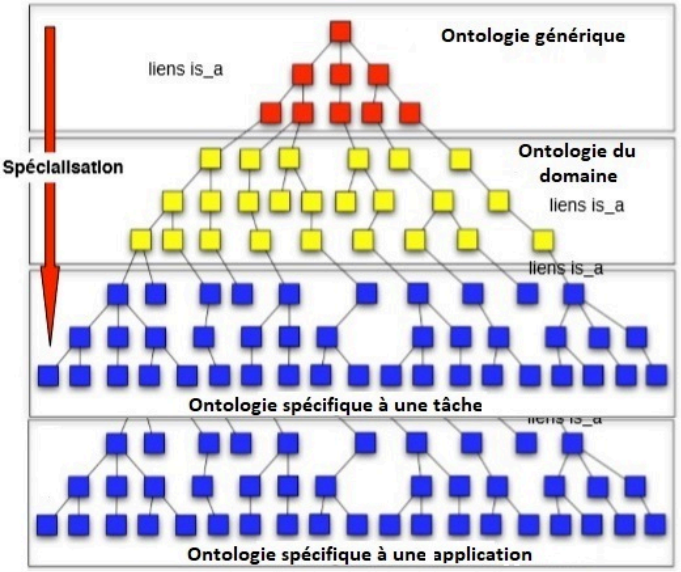

Figure 2.12 – Les types des ontologies

2.3.4 Caractéristiques des ontologies

Selon [Davis *et al.*, 1993], une représentation des connaissances a cinq rôles, que nous pouvons résumer brièvement comme suit :

1. Un substitut des éléments du monde réel ;
2. Un ensemble d'engagements ontologiques ;
3. Une théorie des constructions représentatives ainsi que des déductions qu'elle sanctionne/ recommande ;
4. Un support pour un calcul efficace ;
5. Un support pour l'interprétation humaine.

Pour satisfaire ces rôles, les ontologies sont modélisées en utilisant différentes techniques de modélisation de connaissances et implémentées dans divers langages. Les langages de

représentation des connaissances se caractérisent par des règles prédéfinies et des notions permettant d'offrir un certain niveau d'expressivité sémantique. Ces langages varient selon leur expressivité et peuvent être placés dans un spectre d'ontologie. Ce spectre part de ceux qui fournissent quelques hypothèses et supposent une sémantique fixe ou implicite en langage naturel (informel) jusqu'à ceux qui sont très expressifs et fournissent une sémantique formelle, des théorèmes et des preuves de propriétés comme la complétude et l'inférence valide (et donc une haute interopérabilité). Ce spectre d'ontologies est illustré par la figure 2.13. Toutefois, les ontologies exprimées en langage informel ne sont pas considérées par tous comme des ontologies car elles ne sont pas compréhensibles par la machine [Gruber, 1995].

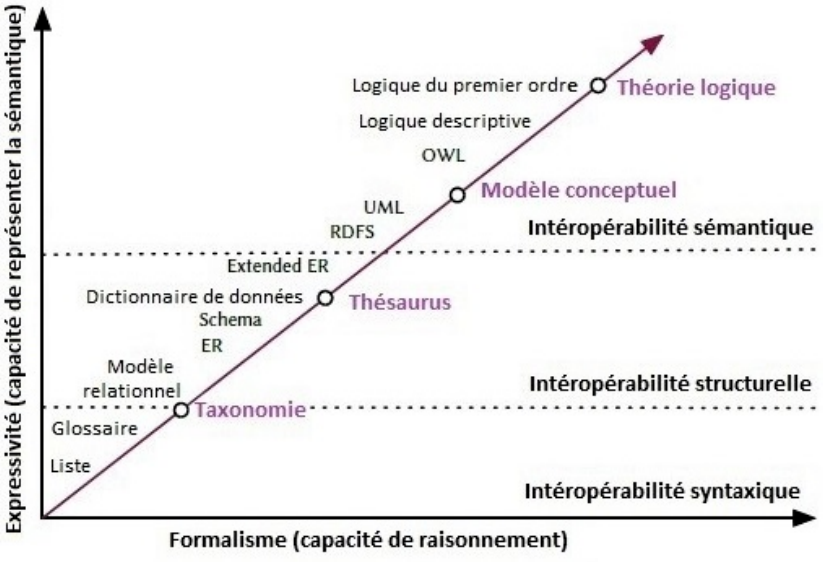

Figure 2.13 – Spectre d'ontologie

Les catalogues de données informelles fournissent simplement aux concepteurs des systèmes des manières symboliques convenues de représenter des concepts et échanger les informations à l'aide d'un vocabulaire connu et contrôlé. Les glossaires donnent, en outre, des définitions des termes en langage naturel facilitant la désambiguïsation, mais aucune sémantique de données lisible par la machine n'est capturée. Les thésaurus s'étendent sur cette interopérabilité syntaxique de base en encodant des relations de base, telles que des synonymes (équivalence) et des associations entre les concepts. Les taxinomies (arbres) fournissent plus d'expressivité en permettant aux hiérarchies « *types_de* » d'être représentées d'une façon plus claire et interprétable par la machine. Parmi les exemples des taxinomies d'usage courant, nous pouvons citer WordNet [Miller, 1995] qui fournit une sémantique pour l'analyse lexicale des mots, et SNOMED CT (Systematized Nomenclature of Medicine Clinical Terms) [7] qui est utilisée pour les soins de santé électroniques et la prescription.

7. http ://snomed.org/

Pour représenter des ontologies formelles, une manière de décrire formellement le monde réel utilisant une sémantique formelle bien spécifiée est nécessaire. Les notations qui permettent d'atteindre ce degré de flexibilité sont appelées les *langages d'ontologies*. Plusieurs langages d'ontologies sont présents dans la littérature comme le format d'échange de connaissances KIF (Knowledge Interchange Format) [Genesereth *et al.*, 1992], EXPRESS [ISO 10303-11, 2004], [Schenck et Wilson, 1994] et OWL (Web Ontology Language) [Group *et al.*, 2009]. OWL est le langage le plus répandu et bénéficie d'une adoption publique à grande échelle et d'un soutien en outillage. Il s'agit d'un langage désigné pour créer des ontologies formelles interprétables par les machines. OWL s'appuie sur la sémantique de logiques de description ou logiques descriptives LD (Descriptive Logics DL). Les LD introduisent une distinction entre les *classes* et les *individus* (concepts et instanciations de concepts) et permettent d'exprimer des relations entre les concepts. Les caractéristiques de ces relations peuvent également être exprimées de manière lisible par la machine, permettant de déduire des informations basées sur les rôles (relations) reliant les concepts. Ainsi, les LD définissent des restrictions en utilisant des constructions logiques, qui sont majoritairement empruntés à la logique de premier ordre (FOL), telles que la négation, la conjonction et la restriction. Les ontologies formalisées en LD peuvent fournir un bon compromis entre le pouvoir expressif et la complexité de calcul.

OWL a été principalement conçu pour fournir un moyen de décrire formellement des ontologies pour le web sémantique. Divers sous-ensembles ou profiles de OWL sont fournis dans la spécification de OWL2. Ces sous-ensembles sont codés de la même manière que OWL2 DL, mais modifient l'expressivité de l'ontologie pour proposer différents compromis en matière d'efficacité de calcul :

- **OWL Full** n'impose aucune restriction à la syntaxe OWL, mais peut créer des modèles pour lesquels le raisonnement est intraitable. OWL Full est souvent utilisé comme langage de notation ou en association avec des raisonneurs non complets qui sont plus rapides mais ne calculent pas nécessairement 100% des déductions.
- **OWL DL** est le sous-ensemble le plus expressif d'OWL2 et fournit un raisonnement robuste et complet [8] à l'aide d'un logiciel approprié. Le raisonnement à travers les grandes ontologies OWL DL peut être intraitable, et en conséquence les raisonneurs DL sont rarement utilisés dans les applications avec de gros volumes de données.
- **OWL EL** est conçu pour les applications avec de grandes ontologies mais un petit ensemble d'instances de données, et garantit de bonnes performances dans cet environnement [Dentler *et al.*, 2011]. OWL EL garantit qu'un ensemble particulier de caractéristiques de raisonnement peut être déduit en un temps inférieur au temps polynomial en terme du nombre d'assertions dans l'ontologie.

8. La validité du raisonnement implique que tous les axiomes déduits sont corrects. La complétude mesure la proportion de toutes les inférences possibles qui sont inférées. Les raisonneurs qui produisent des résultats complets et valides tels que Pellet, RACER et FaCT++ sont appelés robustes et complets

- **Les ontologies OWL Query Language (QL)** permettent un raisonnement efficace sur un grand nombre d'individus, tant que la taille de l'ontologie (et l'expressivité) est faible. Les requêtes sur les ontologies OWL QL peuvent être ré-écrites en SQL, fournissant des bases de données relationnelles à utiliser pour stocker des données.
- Le langage de règles OWL (RL) est un sous-ensemble légèrement restreint de OWL DL qui garantit de meilleures performances dans la plupart des situations. Le raisonnement en langage de règles (RL) peut être implémenté à l'aide de règles de raisonnement, et peut fournir d'excellentes performances si un raisonnement robuste mais incomplet est acceptable.

La figure 2.14 illustre l'expressivité des sous ensembles OWL en les comparant avec d'autres langages d'ontologies. L'expressivité est une caractéristique des ontologies exprimées en langage formel. Elle permet l'interopérabilité sémantique facilitant la communication entre les acteurs et les systèmes pour interpréter les connaissances et leur signification indépendamment sans ambiguïté.

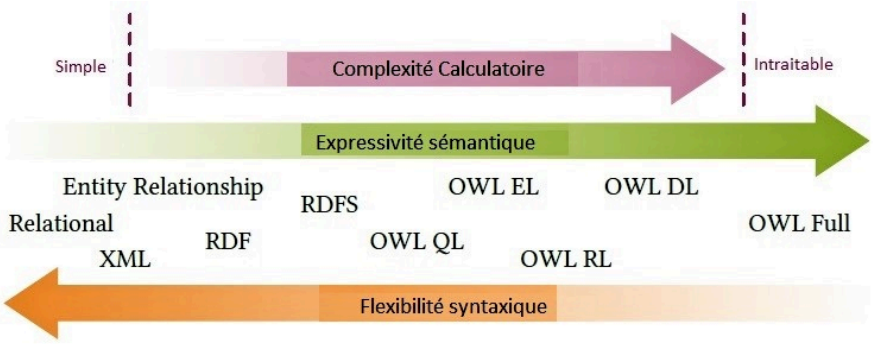

Figure 2.14 – Caractéristiques d'expressivité des profiles OWL

Les ontologies peuvent être considérées comme des vocabulaires contrôlés exprimés dans un langage formel de représentation d'ontologie et capturent la sémantique du domaine du discours d'une manière interprétable par la machine. Elles visent à abstraire la représentation des connaissances indépendamment d'une application particulière en vue d'encourager leur réutilisation. Les vocabulaires contrôlés constituent des ensembles de termes définis sans ambiguïté. Chaque terme peut être interprété correctement par des systèmes ayant des connaissances préalables des définitions du vocabulaire. Elles peuvent inclure des informations détaillées décrivant la signification et la sémantique de chaque terme et s'appuient sur une logique codée dans une application pour contextualiser et interpréter l'information.

Ainsi, la signification des données peut être déduite à partir d'axiomes présents dans l'ontologie. Ces axiomes expriment l'interaction des concepts du vocabulaire, afin qu'ils puissent être utilisés par une machine pour déduire de nouvelles connaissances. En codant

l'information et le sens de manière formelle, les faits qui sont inclus dans les ontologies et les modèles de données sémantiques peuvent être exploités par des ordinateurs pour établir de nouvelles connaissances, de la même manière que les humains raisonnent sur l'information. Ce processus est appelé *inférence logique*, et peut également être utilisé pour faciliter l'intégration des données entre les systèmes et ainsi aligner les modèles. En outre, il est possible de déduire de nouveaux faits en mettant en œuvre une logique sur le domaine du discours. La mesure dans laquelle cette inférence peut être réalisée dépend de l'expressivité de l'ontologie, et donc du langue choisi pour sa représentation. Des représentations plus expressives offrent un plus grand potentiel d'inférence en terme d'efficacité calculatoire [Brachman et Levesque, 2004].

Le raisonnement dans OWL DL peut fournir les fonctionnalités suivantes :

— **Subsomption** : vérifier les classes dont un concept est nécessairement un membre (principalement par héritage),
— **Satisfaisabilité** : une classe qui n'a pas nécessairement de membres (par le biais d'une définition contradictoire) est insatisfaisable,
— **Vérification de la cohérence** : vérifier si une ontologie est en conflit avec elle-même dans une définition spécifique. Par exemple, si les classes « Humain » et « Chat » sont disjointes, et « Fred » est membre des deux, l'ontologie est incohérente,
— **Équivalence** : vérifier si deux concepts sont équivalents,
— **Implication** : création de nouvelles assertions suivant la logique fournie par l'ontologie.

Dans certaines circonstances, le raisonnement conforme aux fonctionnalités des raisonneurs OWL DL peut être indésirable. Ces raisonneurs calculent souvent des inférences utilisant une méthode de « démonstration de théorème », qui calcule toutes les implications permises et ensuite déduit les non valides [Brachman et Levesque, 2004]. Ces circonstances incluent :

- Les applications où l'inférence complète n'est pas requise, et l'efficacité de calcul est préférable par rapport à l'implication ;
- Le raisonnement où les axiomes au-delà de l'expressivité de OWL DL sont nécessaires, comme dans l'alignement des ontologies ou lors de l'affirmation des connaissances spécifiques à un domaine ;

Dans le cadre de cette thèse, les caractéristiques des ontologies qui nous intéressent sont principalement l'*abstraction*, l'*expressivité sémantique* et la *modularité*. Dans un contexte multidisciplinaire, l'abstraction représente un facteur clé de communication efficace des connaissances entre les acteurs. D'autre part, l'expressivité sémantique établit une clarification du domaine du discours ainsi qu'un partage sémantiquement uniforme entre les parties impliquées dans le développement des SCS, et interprétable par la machine. Par ailleurs, les capacités prometteuses de OWL DL en expressivité sémantique fait de ce lan-

gage un bon candidat de représentation d'ontologie pour répondre aux problématiques de cette thèse. Nous discutons en détail la syntaxe des symboles DL et les termes OWL correspondants dans le chapitre 3. Ainsi, la modularité est une propriété d'ontologies permettant de diviser l'ontologie en des modules spécifiques à des tâches ou à des sous-domaines. Dans notre contexte, la modularité permet d'obtenir une modélisation à multi-vues des connaissances des domaines concernées, à savoir l'analyse de sécurité et l'ingénierie des exigences. En effet, quand les ontologies deviennent grandes, elles deviennent également plus difficiles à gérer et à être réutilisées [Gruber, 1995].

La modularisation ontologique est la pratique de la division du modèle de l'ontologie en un certain nombre de morceaux plus petits, ou modules. Nous résumons certaines motivations principales et avantages de la conception d'ontologies modulaires [Stuckenschmidt *et al.*, 2009] :

— **Compréhensibilité et documentation** : En séparant les modules de l'ontologie par tâche ou sous-domaine, les utilisateurs peuvent examiner et comprendre chaque module facilement plutôt que de devoir analyser une représentation monolithique de l'ensemble du problème. Chaque module peut être annoté et documenté indépendamment, en fournissant des provenances et des contextes plus granulaires.
— **Facilité de réutilisation** : La modularisation permet de réutiliser plus facilement les connaissances par d'autres parties. En suivant le principe d' « engagement ontologique minimal » , les utilisateurs de modèles de domaine ne peuvent s'engager que dans une partie spécifique de la conceptualisation, assister l'efficacité calculatoire ou réaffirmer des parties d'un domaine dans d'autres façons.
— **Scalabilité** : La performance et l'effort calculatoire du raisonnement de l'ontologie sont souvent affectés par le nombre d'axiomes qu'un raisonneur doit prendre en compte lorsqu'il fait les déductions. En effet, la qualité du comportement de nombreux raisonneurs dépend de la taille de la base de connaissances traitée. Plutôt que de raisonner sur toute une base de connaissances, la modularisation offre la possibilité de raisonner uniquement sur ces aspects requis pour une application particulière et contribue ainsi à la performance.
— **Maintenance et validation** : Comme en génie logiciel, la maintenance de petits modules est, de toute évidence, plus simple que celle d'un seul modèle monolithique. Plusieurs modules d'ontologie peuvent être élaborés simultanément par diverses personnes, qui peuvent tirer profit des pratiques du génie logiciel telles que le test unitaire et le contrôle de source. Une validation supplémentaire est également plus facile, car les modules peuvent être testés par rapport aux exigences connues pour un cas d'utilisation particulier.

De l'ingénierie des connaissances au web sémantique, un grand nombre d'ontologies a été développé en utilisant différentes méthodes et techniques dans divers domaines. L'ensemble d'activités concernant le processus de développement des ontologies,

les métho- dologies et les outils fait l'objet d'une discipline appelée *Ingénierie Ontologique*. Nous abordons cette discipline dans la section suivante afin d'appréhender les étapes et les méthodologies permettant de passer d'une expression linguistique des connaissances à une ontologie opérationnelle. Ensuite, nous exposons les contributions majeures en développement des ontologies des domaines cernant le contexte de ces travaux de thèse, à savoir l'ingénierie des exigences, le domaine ferroviaire et l'analyse de sécurité des systèmes critiques.

2.4 Ingénierie Ontologique

L'ingénierie ontologique ou l'ingénierie des ontologies a pour vocation de combler le fossé entre l'ingénierie des connaissances et le génie logiciel. Mettant en œuvre les pratiques du génie logiciel au profit de l'ingénierie des connaissances, l'ingénierie ontologique fournit les lignes directives de la construction des ontologies dans un domaine ou une application spécifique. Ces lignes directives constituent la logique de conceptualisation du domaine du discours, les contraintes sémantiques de ces concepts ainsi que les méthodes et les technologies permettant la capitalisation des connaissances. En intelligence artificielle, cette évolution est caractérisée par la mise en place d'un guide intelligent capable d'assister l'ingénierie des connaissances conventionnelles. Ainsi, l'ingénierie des connaissances représente la recherche d'heuristiques spécifiques au domaine pour résoudre un problème ; tandis que l'ingénierie ontologique est la recherche des concepts abstraits, réutilisables, partageables et maintenables pour construire un modèle de connaissances capable d'aider les parties à résoudre des problèmes.

2.4.1 Principe et objectifs

Les méthodes d'ingénierie des ontologies formelles aident à guider les concepteurs de l'ontologie à créer des modèles conformes aux besoins, en particulier aux premières étapes d'un projet. S'appuyant sur des techniques de génie logiciel, beaucoup de ces méthodes ont été proposées ; la plupart décrivent le développement d'une ontologie en plusieurs étapes distinctes. Ces dernières sont résumées par [Iqbal *et al.*, 2013] et expliquées comme suit :

- **Spécification** : Identification du but et de la portée d'une ontologie, définition des motivations, des exigences et des limites du système afin de cerner les objectifs auxquels l'ontologie doit répondre ;
- **Conceptualisation** : Conception de l'ontologie, en spécifiant les concepts, les relations et la formulation des fragments de connaissances exactes à représenter. Cette étape est souvent entrepris en langage naturel ou en utilisant des diagrammes.
- **Formalisation** : L'encodage d'un modèle conceptuel en langage formel expressif tel que la logique du premier ordre ou UML couplé avec OCL [Duarte *et al.*, 2003]. Cette étape spécifie généralement les axiomes et les contraintes à poser sur les

concepts et les relations (voir section 2.3.1).

— **Implémentation** : La création d'une ontologie finale en s'appuyant sur le modèle formel. L'engagement envers une technologie n'est nécessaire qu'à ce stade.

Les auteurs [Pinto et Martins, 2004] recommandent la mise en œuvre de trois tâches durant le processus de développement de l'ontologie :

— **Maintenance** : Maintenir l'ontologie à jour pour assurer la pertinence durant la conception, l'implémentation et l'utilisation,

— **Acquisition de connaissances** : L'utilisation des techniques automatiques/bibliographiques ou des experts du domaine pour assembler une représentation précise du domaine en ontologie comme discuté dans la section 2.3.1,

— **Évaluation et documentation**. L'évaluation continue de l'ontologie par rapport aux critères initialement définis et la documentation en langage naturel pour aider la réutilisabilité.

La nécessité de valider et d'évaluer les ontologies a été reconnue dans la littérature [Gangemi *et al.*, 2006] et [Pinto et Martins, 2004]. La validation est importante et a fait l'objet de différentes approches suggérées dans plusieurs méthodes d'ingénierie ontologique. Considérant que la validation de la conception de modèles de données traditionnels, en génie logiciel, peut souvent être établie en vérifiant directement un modèle par rapport à un ensemble d'exigences fonctionnelles (et quantifiées) formulées par une application, cette approche n'est pas adaptée aux ontologies. En effet, les modèles du domaine sont délibérément dissociés des exigences d'une application particulière. Des méthodes d'évaluation qualitatives tel que OntoMetric [Lozano-Tello et Gómez-Pérez, 2004] recommande de demander à des experts du domaine d'examiner et de noter des modèles subjectivement suivant un ensemble de métriques. Cette approche peut produire des indications de couverture, de qualité et d'exactitude de l'ontologie, mais a plusieurs inconvénients. Tout d'abord, il est difficile de choisir le bon groupe d'utilisateurs, si des experts de domaine sont utilisés, la logique de modèle et la sémantique peuvent être mal comprises, et si des experts en modélisation sont utilisés, les concepts de domaine peuvent être mal compris. Deuxièmement, les critères de notation sont nécessairement très subjectifs : OntoMetric exige que les utilisateurs évaluent divers facteurs allant de « très faible » à « Très élevé », mais ne peut fournir aucun point de référence pour établir la signification de ces évaluations.

Afin d'améliorer la qualité d'évaluation d'une ontologie, l'utilisation des approches formelles ou automatisées de validation d'ontologies permet d'avoir des résultats plus objectifs. Ces métriques incluent principalement cinq critères à prendre en compte [Gruber, 1993] :

1. **Clarté** : La définition d'un concept doit être être formulé explicitement, de manière aussi « objective » que possible (indépendamment du contexte). Une définition doit de plus être « complète », c'est à dire, définie par des conditions à la fois nécessaires

et suffisantes et ensuite documentée en langage naturel.

2. **Cohérence** : Rien qui ne puisse être inféré de l'ontologie ne doit entrer en contradiction avec les définitions des concepts y compris celles qui sont exprimées en langage naturel. Autrement dit, les inférences faites à travers une ontologie doivent être cohérentes avec leurs définitions.
3. **Extensibilité** : Les extensions qui pourront être ajoutées à l'ontologie doivent être anticipées. Il doit être possible d'ajouter de nouveaux concepts sans avoir à toucher aux fondations de l'ontologie.
4. **Déformation d'encodage minimale** : Une déformation d'encodage a lieu lorsque la spécification influe la conceptualisation. Un concept donné peut être plus simple à définir d'une certaine façon pour un langage d'ontologie donné, bien que cette définition ne corresponde pas exactement au sens initial. Ces déformations doivent être évitées autant que possible.
5. **Engagement ontologique minimal** : Une notion importante en ingénierie ontologique est l'engagement ontologique. Chaque instruction d'une ontologie engage son utilisateur sur une vue particulière du domaine. Les ontologies doivent contenir le moins possible de concepts pour soutenir les activités de partage des connaissances. Contrairement aux bases de connaissances, on n'attend pas d'une ontologie qu'elle soit en mesure de fournir systématiquement une réponse à une question arbitraire sur le domaine. Une ontologie est la conceptualisation des connaissances consensuelles du domaine ; elle ne définit que les termes nécessaires pour partager la connaissance liée à ce domaine. De ce fait, le but d'une ontologie est de définir un vocabulaire pour décrire un domaine, si possible de manière complète.

Les méthodes les plus utilisées en ingénierie ontologique [Cardoso, 2007], [Simperl et Luczak-Rösch, 2014], [Simperl *et al.*, 2009] peuvent être classées en quatre groupes, en fonction de leurs caractéristiques et de leur objectif :

— Les premières méthodes d'ingénierie ontologique « monolithiques » supposent un processus de conception unique, non itératif et mettant l'accent sur le choix du langage de modélisation et de la formalisation des connaissances. Nous pouvons citer dans cette catégorie la méthode proposée par [Uschold, 1995] appelée ENTERPRISE et la méthode utilisée dans la création de l'ontologie Toronto Virtual Enterprise (TOVE) [Gruninger et Fox, 1994].

— Les méthodes d'ingénierie ontologiques itératives mettent moins l'accent sur la spécification formelle initiale d'un modèle, et préconisent les tests, le raffinement et la réutilisation des ontologies, tels que METHONTOLOGY qui est largement utilisée [Fernández-López *et al.*, 1997], On-To-Knowledge [Sure *et al.*, 2004].

— Les méthodes « Web post-sémantique » telles que la méthode NeON [Suárez-Figueroa *et al.*, 2012], l'ingénierie distribuée des ontologies (DILIGENT) [Pinto *et al.*, 2004] et l'approche systématique SABiO (Systematic Approach for Building

Ontologies) [de Almeida Falbo, 2014] mettent l'accent sur la collaboration et la flexibilité, et fournissent des approches de création d'ontologies plus pragmatiques que les méthodes antérieures.

— Les méthodes d'apprentissage ontologique axées sur l'utilisation automatisée ou des outils semi-automatisés pour reconfigurer les connaissances, tels que ROD (Rapid Ontology Development) [Zhou *et al.*, 2002].

Avec l'émergence du Web sémantique, un large éventail d'outils a été développé pour éditer et créer des modèles OWL. Bien que les ontologies puissent être entièrement décrites manuellement à l'aide de la notation DL et la syntaxe abstraite OWL, le progrès du web sémantique et le désir de permettre aux non-mathématiciens de créer des ontologies a conduit à la création de plusieurs outils d'édition des ontologies. Ces outils sont généralement utilisés pour créer la partie terminologique du modèle, la connaissance du domaine, tandis que d'autres outils sur mesure sont utilisés pour importer ou acquérir des connaissances selon l'application. L'un des outils les plus répandus est *Protégé*[9] que nous utilisons dans le cadre de cette thèse. Il s'agit d'un outil d'édition d'ontologies graphiques open source créé par une équipe du Centre de recherche biomédicale de Stanford. La version actuelle de Protégé [Noy *et al.*, 2001], [Musen *et al.*, 2015] s'appuie sur les travaux réalisés depuis 1987 sur les outils de représentation des connaissances biomédicales. Protégé permet la manipulation des ontologies OWL, et fournit des outils pour la création de classes/individus, l'édition des axiomes, le raisonnement DL et la visualisation de base. Il est largement utilisé, selon les dernières enquêtes suggérant qu'il est l'éditeur graphique le plus populaire disponible chez les auteurs d'ontologies [Khondoker et Mueller, 2010].

2.4.2 Ontologies de l'Ingénierie des Exigences

Les ontologies ont été largement utilisées dans les activités d'IE afin de faire face à leur complexité notamment l'élucidation des exigences [Zhi, 2000], la spécification des exigences [Avdeenko et Pustovalova, 2015], l'analyse des exigences [Siegemund *et al.*, 2011] et la gestion des changements des exigences [Baxter *et al.*, 2008]. La modélisation ontologique des connaissances du domaine et la modélisation des exigences dans l'activité de l'IE montre une forte corrélation en terme du processus [Dobson et Sawyer, 2006]. Plusieurs efforts ont été consacrés à l'adoption des technologies du Web sémantique et des techniques dirigées par les connaissances en IE. Dans [Kossmann *et al.*, 2009], le méta-modèle OntoRem est proposé afin d'assurer la cohérence et la complétude des exigences à l'égard des concepts génériques de l'IE. Une approche OSCL (Open Service for Life cycle Collaboration) est développée dans [Alvarez-Rodríguez *et al.*, 2014] et vise à assurer la gestion des exigences basée sur les standards du web sémantique.

Dans une autre perspective, l'IE est étendue et guidée par l'identification et la formulation des buts. Les buts deviennent un concept de base des activités de l'IE et permettent

9. http ://protégé.stanford.edu

de couvrir des aspects d'interopérabilité lorsque l'alignement avec d'autres concepts du domaine est effectué (voir section 2.2.3). Une ontologie de référence des exigences dirigée par les buts est proposée afin de clarifier la conceptualisation de ce domaine tout en assurant l'interopérabilité entre les différentes approches d'IEDB [Negri *et al.*, 2017]. Dans [Lee et Gandhi, 2005], un framework actif d'IE basé sur une ontologie est proposé en réutilisant les concepts de l'IEDB. Il permet l'élucidation et la spécification des exigences mais il ne tient pas compte de la vérification des exigences et de leur traçabilité. D'autre part, le modèle des buts KAOS/SysML a été enrichi par une représentation des connaissances du domaine en s'appuyant principalement sur la satisfaction des buts [Tueno *et al.*, 2017]. Dans [Yu, 2011], un cadre outillé est proposé pour assister le raisonnement des objectifs globaux et leur raffinement. Le tableau 2.1 récapitule les principaux concepts utilisés dans les études ayant un objectif de recherche similaire au nôtre, les sources d'acquisition de connaissances ainsi que la méthode d'ingénierie ontologique (IO) choisie.

Dans le cadre de cette thèse, nous tirons profit des ontologies pour faire face à la modélisation et la gestion des exigences de sécurité. Afin de fournir une vue partagée entre les domaines considérés, nous nous intéressons à la réutilisation de quelques concepts de l'ontologie de référence [Negri *et al.*, 2017]. La logique suivie dans ce choix est illustrée par la figure 2.15 et justifiée en détail dans le chapitre 4.

2.4.3 Ontologies du domaine ferroviaire

Dans le domaine ferroviaire, les ontologies sont généralement utilisées pour l'analyse des données afin de représenter l'intégration des données ferroviaires et la traçabilité des informations de sécurité. À l'issu du projet InteGrail [10], une ontologie du domaine ferroviaire RDO (Railway Domain Ontology) a été développée. Cette ontologie a essentiellement été utilisée dans les systèmes de surveillance afin de faciliter la communication et l'intégration de données pour la détection d'événements dangereux dans les systèmes ferroviaires. Le logiciel AMaas (Asset Monitoring as a Service) est un exemple pratique d'utilisation de l'ontologie RDO dans un système de surveillance [Tutcher, 2014]. RDO décrit la manière d'ajouter des connaissances aux structures de données prédéfinies pour l'échange d'informations entre les systèmes et elle représente les connaissances du domaine pour l'analyse des risques, l'inférence ontologique (par exemple, catégorisation des entités) et l'extension du système en ajoutant des informations. D'autres se focalisent sur l'analyse des risques basée sur le big data pour fournir une aide à la gestion des décisions liée à la sécurité pour les systèmes ferroviaires britanniques [Van Gulijk *et al.*, 2015] et [Lewis, 2015].

D'autre part, la collaboration entre le groupe de travail ERIM (European Rail Infrastructure MasterPlan) de l'union internationale des chemins de fer (UIC) et la communauté RailML [11], fournit un cadre complet permettant la communication entre les applications

10. http ://www.integrail.eu/
11. http ://www.railml.org

Ontologies de l'IE	Concepts utilisés	Source d'acquisition	Méthode d'IO
[Siegemund *et al.*, 2011]	Artifact, TestCase, Influencer, Softmetric, RequiremntArtifact, Problem, story, Requirement, Challenge, Risk, Obstacle	Méta-modèle d'IEDB	Pas de méthode
[Baxter *et al.*, 2008]	Customer voice, technical voice, system objective, function structure, application cost, dimensions, controls	Réutilisation du processus de conception + modèle basé sur l'ontologie pour la conception du produit	Pas de méthode
[Negri *et al.*, 2017]	Goal, Requirement, Assumption, Specification, Stakeholder, Task, Complex task, Atomic task	Intéropérabilité terminoloique entre les approches d'IEDB et fondé sur l'ontologie de haut niveau UFO	SABiO
[Tueno *et al.*, 2017]	Concept, domain model, domain cardinality, relation, attribute, individual, etc	SysML/KAOS	Pas de méthode
[Yu, 2011]	Actor, resource, task, role, position, agent, softgoal	i*	Pas de méthode

Tableau 2.1 – Étude comparative des concepts manipulés dans les ontologies de l'IE

ferroviaires hétérogènes, appelé RailTopoModel [UIC RailTopoModel, 2016]. Il s'agit d'un modèle logique pour normaliser la représentation de la topologie du réseau ferroviaire européen et les relations entre ses éléments afin de comprendre comment le réseau est connecté et comment les éléments dépendent les uns des autres. Développé dans l'objectif de permettre aux données du réseau d'être partagées entre les gestionnaires d'infrastructure, RailTopoModel définit un format d'échange de données ferroviaires, à partir de plusieurs modèles de données existants.

Ensuite, le développement des ontologies dans le domaine ferroviaire s'est concentré sur la formalisation des documents de la spécification des exigences du système ERTMS (European Rail Traffic Management System) [Hoinaru *et al.*, 2013]. Par ailleurs, une ontologie

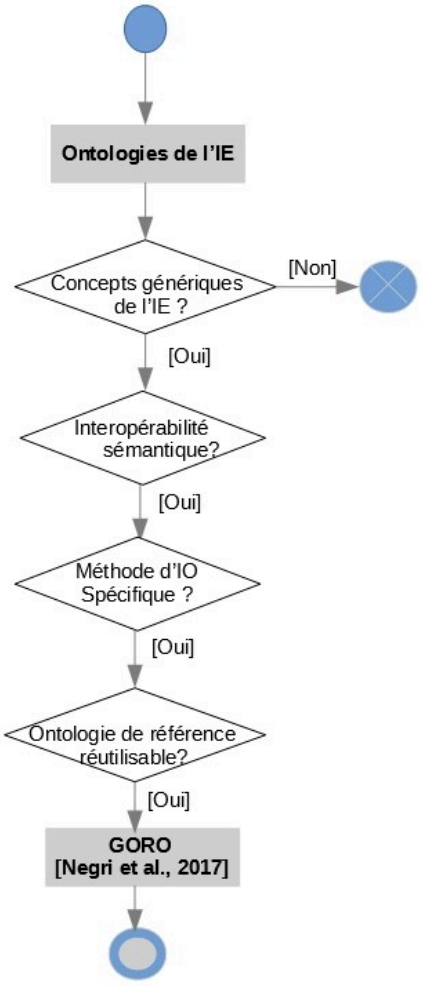

Figure 2.15 – Raisonnement pour la réutilisation des concepts de l'ontologie GORO

de trois niveaux de qualité de service (QoS) à été développée pour ERTMS/ETCS afin de représenter et inférer les connaissances temporelles et non-temporelles [Sango *et al.*, 2015]. Ainsi, des approches ontologiques ont été proposées pour le raisonnement par cas (Case-Based Reasoning) d'analyse des accidents ferroviaires [Maalel *et al.*, 2012], et pour fournir un raisonnement actif à l'intérieur du middleware des backbones du train [Verstichel *et al.*, 2007].

Le tableau 2.2 récapitule les principaux concepts utilisés dans les ontologies proposées dans le domaine ferroviaire. L'objectif principal de ces ontologies est la modélisation des données liées à l'infrastructure ferroviaire, au matériel roulant ainsi qu'aux différentes procédures. Différemment de leur objectif, nos travaux de recherche visent à proposer une ontologie capable de gérer la sécurité ferroviaire dès les premières phases de conception. L'intérêt principal de notre étude est l'alignement sémantique entre une ontologie qui capture les concepts liés à la sécurité ferroviaire et une autre qui se focalise sur les concepts d'IE. Par conséquent, nous ne réutilisons pas les concepts des ontologies proposées ; mais nous proposons de nouveaux concepts qui représentent les connaissances pertinentes des

domaines d'intérêt.

2.4.4 Ontologies de l'analyse de sécurité des systèmes critiques

Les ontologies ont été largement utilisées dans l'analyse de sécurité (safety) des systèmes critiques et leur conception. Dans [Rehman et Kifor, 2016], une ontologie a été proposée pour représenter et gérer les connaissances de l'AMDE dans le secteur automobile. Ensuite, elle définit des actions d'atténuation du risque anticipé et permet l'extraction d'informations de sécurité à l'aide de sa version opérationnelle en OWL. D'autre part, une conceptualisation des connaissances du danger (Hazard Ontology) [Zhou *et al.*, 2017] a été proposée afin d'identifier le danger dès les premières phases de conception des SCS et élucider les exigences de sécurité permettant de le diminuer. Dans [Zhou *et al.*, 2015], une approche d'élucidation des exigences de sécurité a été proposée en s'appuyant sur la représentation des connaissances de l'environnement, comme un ensemble d'hypothèses, et sur des règles de raisonnement. Dans [Provenzano *et al.*, 2017], les auteurs ont proposé une approche ontologique pour élucider les exigences de sécurité basée sur la conceptualisation des connaissance du danger. L'approche heuristique proposée décrit l'analyse des composants de danger selon leurs propriétés, rôles et relations entre eux. Ensuite, l'élucidation des exigences de sécurité est effectuée en extrayant ces connaissances et en gérant les relations entre les composants.

2.5 Synthèse

L'IE joue un rôle fondamental dans la conception des SCS notamment dans l'élucidation des exigences de sécurité et leur modélisation pour fournir une vue partagée entre les différents acteurs impliqués. La communication entre les concepteurs, les analystes de sécurité et les experts du domaine constitue un véritable enjeu de la compréhension du problème et de la mise en œuvre de la solution. Ainsi, la mise à disposition d'un vocabulaire commun permet de résoudre les conflits d'ambiguïté et d'interpréter d'une façon harmonisée les différentes vues du système. D'autre part, la gestion des changements des exigences nécessite un cadre formel de raisonnement capable de fournir une aide à la décision des choix liés à la sécurité.

Notion prometteuse, l'ontologie permet de structurer les connaissances de ces domaines afin de fournir un cadre sémantique partagé entre les parties prenantes. Partant de l'analyse de sécurité jusqu'à la gestion des exigences de sécurité, il est nécessaire de mettre en avant une approche systématique de conception des systèmes critiques sûrs. Ainsi, la combinaison de l'analyse de sécurité proactive avec la logique métier du domaine ferroviaire dans une approche ontologique permet une meilleure conduite des activités de développement et de gestion des exigences par la suite.

Afin de répondre à notre problématique de thèse, nous nous posons plusieurs questions

Ontologies du domaine ferroviaire	Concepts utilisés	Sources d'acquisition	Méthodes d'IO
[Tutcher, 2014]	RollingStock, Infrastructure, Timetable, TrackSection, TrainProtection Capability, ERTMS capability, CharacteristicChange	Experts du domaine et littérature	NeON
[Van Gulijk *et al.*, 2015]	Alarm, DecisionSupport, MobileEntity, FeedsForDynamicData, BDRA, etc	Experts du domaine	Pas de méthode
[UIC RailTopoModel, 2016]	Network resource, NetElement, CompositionNetElement, SpotLocatoion, LinearLocation, etc	Modèles de données existants	Pas de méthode
[Hoinaru *et al.*, 2013]	Driver, ERTMS, Procedure, ERTMS network layer, ETCS, Application level, etc	Documents normatifs : ERTMS/ETCS System Requirement Specification, Glossaire ERTMS	méthode basée sur le corpus
[Sango *et al.*, 2015]	ERTMS, ETCS, TrackSide, OnBoard, QoS, Parameters,Temporal, Integrity, Interval, etc	ERTMS/ETCS System Requirement Specification	Pas de méthode

Tableau 2.2 – Étude comparative des concepts manipulés dans les ontologies du domaine ferroviaire

afin de trouver le fil conducteur à notre approche : Quels sont les concepts principaux de l'analyse de sécurité à prendre en compte et comment les organiser ? Selon quels critères les choix méthodologiques et technologiques sont établis afin de répondre aux contraintes académiques et industrielles ? Comment aligner les concepts de l'analyse de sécurité avec les besoins des domaines critiques, en particulier le domaine ferroviaire ? Dans quelle mesure les facteurs organisationnelles, technologiques et humains sont intégrés dans cette approche ? La réponse à ces questions et la présentation de nos contributions fait l'objet du chapitre suivant.

Deuxième partie

CONTRIBUTIONS : VERS UNE APPROCHE ONTOLOGIQUE DE CONCEPTION DES SYSTÈMES SÛRS

Chapitre 3

Ontologie d'Analyse Dysfonctionnelle pour les SCS

Sommaire

3.1 Introduction

L'analyse dysfonctionnelle est une tâche essentielle et exigeante des premières étapes du développement des systèmes critiques de sécurité (SCS). Actuellement, l'intégration de l'analyse dysfonctionnelle au plus tôt de la phase de conception ne se pratique pas couramment et manque de support théorique pour son intégration. En effet, les méthodes d'analyse dysfonctionnelle s'appuient principalement sur trois facteurs, à savoir les modèles dynamiques de comportement du système, l'expertise des analystes de sécurité et le retour d'expérience (REX) obtenu lors du développement des systèmes antérieurs. Néanmoins, les modèles dynamiques du comportement du système tel que les diagrammes de séquence et les automates finis ne peuvent être obtenus dans les premières phases de conception, et sont sujets aux changements durant le cycle de vie des systèmes. Ainsi, il y a un besoin émergent de spécifier une conceptualisation des connaissances du domaine afin de garantir une intégration efficace durant le cycle de vie des SCS. Cette représentation structurée permet d'établir un cadre sémantique partagé entre les différentes parties, unifie la terminologie utilisée et capitalise les connaissances afin d'être réutilisées pour d'autres systèmes.

Ce chapitre a pour objectif de présenter nos contributions par rapport à la conceptualisation explicite des connaissances de l'analyse dysfonctionnelle pour la conception des SCS. Nous commençons par définir le cadre industriel du domaine d'application afin de cerner le choix des concepts pertinents à considérer. Ensuite, nous justifions les choix du cadre méthodologique de cette thèse en tenant compte des contraintes techniques et du métier. Une fois les choix argumentés, nous entamons le processus de développement de l'*ontologie d'analyse dysfonctionnelle (DAO)*, une ontologie du domaine ayant pour vocation de clarifier le « jargon » du métier en s'appuyant sur les normes et les référentiels du domaine. Ainsi, une validation par des cas d'études ferroviaires réels est détaillée afin d'illustrer les capacités de DAO à décrire d'une manière structurée les situations critiques. Enfin, nous discutons la valeur ajoutée de cette ontologie dans le domaine d'analyse dysfonctionnelle et nous argumentons le besoin de son alignement avec les connaissances de l'IE pour mener la conception des SCS d'une manière harmonisée.

3.2 Cadre Industriel

Avant de procéder à la définition des concepts du domaine, il faut commencer par définir le cadre applicatif et méthodologique. En effet, les choix sont fixés par rapport aux contraintes extraites de l'analyse du domaine et des capacités techniques. Dans les domaines critiques, les contraintes organisationnelles et environnementales ainsi que l'aspect socio-technique ont un impact majeur sur le comportement sûr des SCS. Dans cette section, nous discutons les contraintes liées au domaine ferroviaire afin d'identifier les lignes directives de la conceptualisation d'analyse dysfonctionnelle.

3.2.1 Systèmes socio-techniques

Les systèmes ferroviaires sont des systèmes socio-techniques complexes mettant en jeu l'interaction des opérateurs humains et des dispositifs techniques. Cet aspect a été étudié dans [Debbech *et al.*, 2018b] afin de justifier le besoin d'intégrer les différents facteurs d'analyse dysfonctionnelle dès les premières phases de conception des systèmes ferroviaires. Ainsi, l'ensemble des situations dangereuses sont le fruit d'articulations des erreurs humaines, des défaillances techniques et des facteurs organisationnels et environnementaux. De ce fait, la mise à plat des concepts relatifs à ces facteurs permet de développer une vision proactive de l'analyse dysfonctionnelle. Dans le chapitre 1, nous avons discuté les facteurs impactant l'analyse de sécurité ferroviaire et nous sommes parvenus à un consensus : l'hétérogénéité des causes de dangers impose la prise en compte simultanée de différents éléments dans l'analyse dysfonctionnelle. En effet, l'abstraction des concepts indispensables à cette analyse s'avère nécessaire. Cette abstraction a pour objectif de faciliter le raisonnement de sécurité, et par la suite, l'élucidation des exigences de sécurité. D'autre part, la flexibilité sémantique constitue un facteur clé de communication efficace entre les analystes de sécurité et les experts du domaine. Cet aspect consiste à rechercher un compromis terminologique entre les facteurs discutés ci-dessus et la sémantique du monde réel. Nous discutons ce point de vue dans la section suivante.

3.2.2 Ambiguïté terminologique

Les activités d'analyse dysfonctionnelle sont guidées par des textes normatifs définissant les bonnes pratiques à adopter afin de mener à bien le processus. Ces documents normatifs contiennent des définitions et des recommandations permettant d'orienter les décisions en utilisant le jargon métier, et parfois des termes ambigus qui sont sujets à diverses interprétations. Prenons par exemple la définition du terme « danger » dans la norme ferroviaire [CENELEC, NF EN 50129, 2003] : « Le danger est une condition qui peut causer un accident ». Nous remarquons que cette définition représente des ambiguïtés au niveau des termes condition, accident et la relation de causalité entre eux. Comment les interpréter d'une manière unique en s'appuyant sur un vocabulaire commun ? Qu'elle est la nature du terme « condition » dans la sémantique du monde réel et comment tracer le chemin des défaillances vers le danger ? Quels sont les éléments contributeurs à l'occurrence du danger ? Une série de questions s'impose à ce niveau pour solliciter la définition d'un vocabulaire commun qui servira de base de communication durant le cycle de vie des SCS. Partant de cette perspective, l'ontologie proposée contribue à l'alignement des points de vue des parties prenantes grâce à une représentation structurée et une interopérabilité sémantique. Les motivations du contexte industriel sont donc identifiées et la finalité globale de l'ontologie est introduite. Dans la section suivante, nous justifions les choix méthodologiques permettant de répondre à ces contraintes principales.

3.3 Cadre méthodologique

Pour notre cadre méthodologique, nous nous reposons sur trois facteurs qui nous semblent indispensables et qui impactent la qualité du développement des ontolgies, à savoir la méthodologie d'ingénierie ontologique, l'ontologie de haut niveau à réutiliser et le langage d'ontologie. En effet, le choix de ces éléments dépend principalement des contraintes du contexte d'application déjà définies et des exigences attendues de l'ontologie. Nous avons discuté, dans le chapitre 2 (section 2.3.1), les caractéristiques de chaque facteur et nous agrégeons, maintenant, nos choix au sein d'une méthodologie.

3.3.1 Choix de l'approche d'ingénierie ontologique

Dans la section 2.4 du chapitre 2, nous avons présenté et comparé les méthodologies de développement des ontologies au regard de divers critères validés par la communauté d'ingénierie ontologique. En effet, le choix d'une méthodologie dépend essentiellement du type d'ontologie à développer, à savoir une ontologie du domaine, une ontologie spécifique à une tâche ou à une application ; mais aussi des degrés d'interopérabilité sémantique et de modularité désirés de l'ontologie.

L'objectif de notre contribution est de développer une ontologie du domaine permettant de fournir une clarification conceptuelle des connaissances de l'analyse dysfonctionnelle. Nous estimons qu'un processus pragmatique de développement des ontologies est adapté à notre contexte car il met en valeur la flexibilité de la conceptualisation et la collaboration entre différentes parties pour aboutir à une ontologie du domaine qui répond aux exigences prévues. Ainsi, l'aspect collaboratif du développement des SCS exige un vocabulaire commun interprétable dans la sémantique du monde réel. De ce fait, un développement dirigé par une analyse ontologique et une réutilisation des modèles de référence existants permet de résoudre cet enjeu fondamental d'harmonisation sémantique. Par conséquent, une méthode qui incorpore les bonnes pratiques d'ingénierie ontologique et qui considère les avantages de l'analyse ontologique durant le processus de développement de l'ontologie est intéressante.

À l'issue de la contextualisation et l'élucidation de nos critères de choix, nous avons entamé une recherche extensive des méthodologies d'ingénierie ontologique dans la littérature. Nous récapitulons l'étude comparative des méthodes d'ingénierie ontologique dans le tableau 3.1.

Suite à cette étude comparative, nous avons choisi **SABiO** [de Almeida Falbo, 2014]. *Pourquoi SABiO ?* Il s'agit d'une approche systématique de développement des ontologies qui hérite des bonnes pratiques du génie logiciel et de l'ingénierie ontologique. En effet, le processus de développement proposé par SABiO intègre des méthodes et des techniques appropriées à la création des ontologies de qualité. Comme le montre la figure 3.1, SABiO inclut cinq phases principales : (i) *identification de la finalité et définition des*

Méthodes d'IO	Processus de conception	Réutilisation des ontologies	Collaboration
TOVE	Pas d'étape de modélisation conceptuelle	Non : formalisation des connaissances à partir du corpus	Non
ENTERPRISE	Processus unique et non itératif	Non	Non
METHONTOLOGY	Processus itératif basé sur l'IC et le Génie Logiciel	Oui	oui
NeON	Processus basé sur les scénarios et un processus de suppor, pas de techniques d'évaluation	Oui	Oui
SABiO	Processus incrémental et itératif basé sur les phases du cycle de vie du système, Techniques d'évaluation + processus de support +	Oui : analyse ontologique	Oui
ROD	Processus ascendant et un un processus descendant	Non	Non

Tableau 3.1 – Étude comparative des méthodes d'Ingénierie Ontologique (IO)

exigences de l'ontologie ; (ii) *capture et formalisation de l'ontologie* ; (iii) *conception* ; (iv) *implémentation* ; et (v) *test*. Bien que ces phases soient similaires à celles d'un cycle de vie du système, il n'y a pas de modèle de cycle de vie spécifique prescrit par SABiO.

Afin de vérifier et valider la formalisation de l'ontologie au regard de ses exigences dès les premières phases, SABiO recommande un développement incrémental et itératif. Par ailleurs, SABiO se focalise sur le développement des ontologies de référence du domaine et distingue celles-ci des ontologies opérationnelles. On entend par une ontologie de référence du domaine toute ontologie développée dans l'objectif de fournir une description *optimale* du domaine. Autrement dit, une ontologie de référence est une spécification indépendante de la solution ayant pour vocation d'établir une description claire et précise des concepts du domaine. Cette spécification représente le *modèle conceptuel* qui a été défini dans le

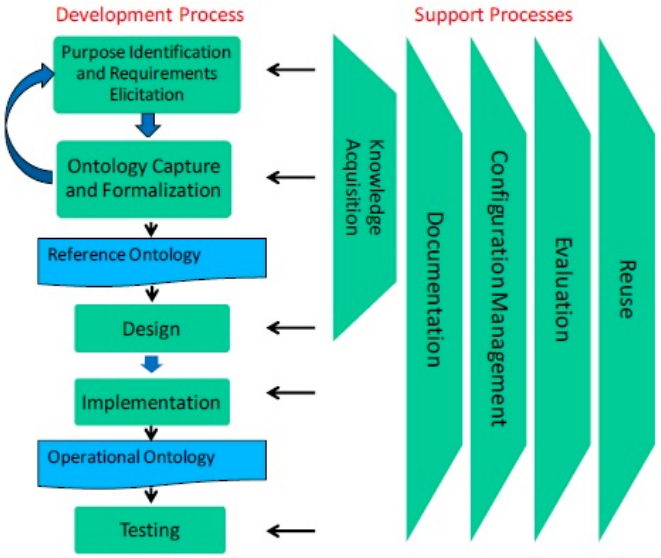

Figure 3.1 – Le processus SABiO [de Almeida Falbo, 2014]

chapitre précédant (Définition 3). En effet, ce modèle de référence fournit une *conceptualisation commune* qui joue un rôle important dans la communication efficace entre les parties et la résolution du problème. Cet aspect est pertinent pour notre contexte de travaux car il permet de combler les lacunes de l'ambiguïté terminologique discutée auparavant.

D'autre part, la version opérationnelle peut être implémentée afin de garantir les propriétés d'efficacité calculatoire telles que l'inférence de nouvelles connaissances, l'extraction de données, la scalabilité et la facilité de réutilisation de l'ontologie. L'ontologie opérationnelle exprimée dans un langage interprétable par la machine permet d'évaluer la cohérence de l'ontologie ainsi que la violation des contraintes du domaine. Dans la phase de conception de l'ontologie, le modèle conceptuel est transformé dans un langage formel afin de garantir l'expressivité sémantique.

Un autre avantage dans l'utilisation de SABiO est sa prise en compte de l'analyse ontologique dans la conceptualisation du domaine. L'analyse ontologique a pour objectif de fournir une base solide pour la modélisation de concepts, si on suppose que ces derniers visent à représenter la réalité. En d'autres termes, elle consiste en l'analyse des concepts et des relations d'une ontologie du domaine à la lumière d'une *ontologie de haut niveau*. Cette pratique a de nombreux avantages pour le développement d'une ontologie du domaine :

— La définition rigoureuse des modèles, en terme de sémantique du monde réel ;
— L'identification des problèmes de définition, d'interprétation ou d'utilisation des concepts ;
— Des recommandations pour améliorer les modèles de formalité ;
— L'héritage du pattern design de l'ontologie de haut niveau et des règles de modélisation correspondantes ;

Le choix de la méthodologie SABiO ayant été fixé, nous procédons au développement de

l'ontologie d'analyse dysfonctionnelle suivant les phases et les caractéristiques présentées. Avant d'entamer ce processus et dans l'objectif de fournir une représentation adéquate des connaissances de l'analyse dysfonctionnelle, nous commençons par choisir l'ontologie de haut niveau à utiliser dans le développement de DAO. Au delà du fait que cette pratique est préconisée par SABiO, elle nous permet d'avoir une approximation de la représentation idéale du domaine et de fournir une interprétation de ces connaissances dans la sémantique du monde réel. Le choix de l'ontologie de haut niveau dépend essentiellement du domaine d'intérêt, des types et des propriétés de ses concepts, ainsi que du niveau d'abstraction attendu. Nous discutons et justifions le choix de l'ontologie de haut niveau dans la section suivante.

3.3.2 Choix de l'ontologie de haut niveau

Dans cette étude, nous avons choisi de recourir à une ontologie de haut niveau afin de lever certains verrous scientifiques identifiés. Ce choix méthodologique est justifié par le raisonnement permettant de répondre aux différents besoins illustrés par la figure 3.2.

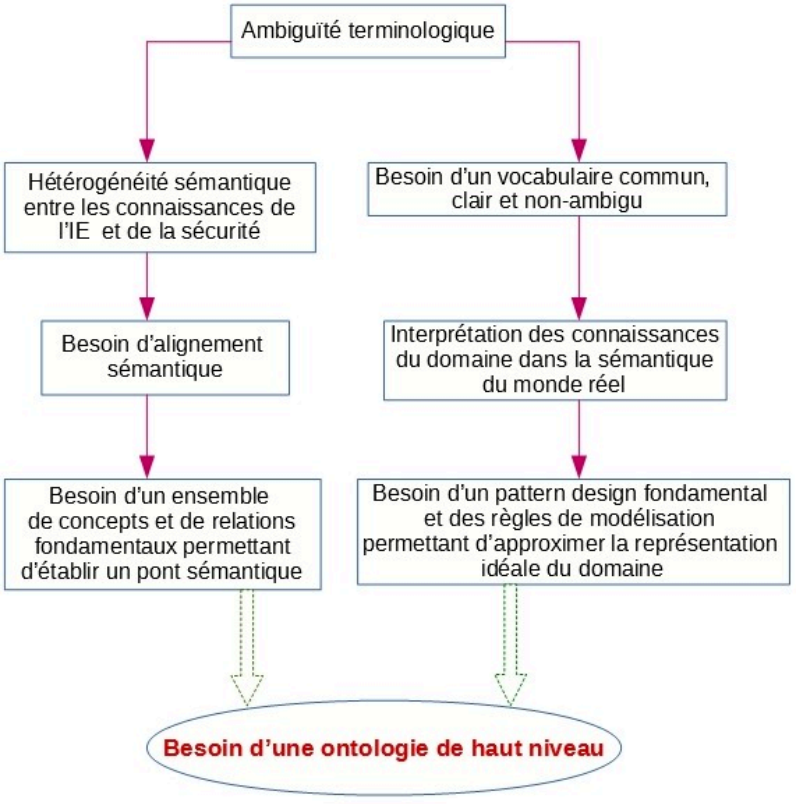

Figure 3.2 – Le raisonnement suivi pour recourir à une ontologie de haut niveau

Les ontologies de haut niveau ou fondamentales fournissent un ensemble de concepts fondamentaux et de relations dans le but d'obtenir un modèle de référence d'un domaine. Avant de choisir une ontologie fondamentale, nous commençons par fixer les critères de

choix. En effet, la pertinence d'une ontologie de haut niveau réside dans la capacité d'obtenir l'*alignement* efficace entre ses concepts et les concepts du domaine d'intérêt. Cet alignement consiste à établir une interprétation dans la sémantique du monde réel entre les concepts fondamentaux et les concepts du domaine. Ensuite, il y a un besoin de trouver un ensemble fondamental de concepts et de relations pertinent permettant de former le squelette de l'ontologie du domaine à développer. Le choix de cet ensemble s'appuie sur les distinctions ontologiques fournies par l'ontologie de haut niveau. D'autre part, les distinctions et les caractéristiques fondamentales de l'ontologie de haut niveau constituent un des facteurs clé de notre choix.

Dans le contexte de notre étude, nous nous intéressons aux entités fondamentales ayant des propriétés capables de représenter les concepts de l'analyse dysfonctionnelle, à savoir une situation dangereuse, un événement dangereux, un danger, une défaillance, etc. De ce fait, des catégories fondamentales d'entités persistantes dans le temps et rigides en termes d'identité sont intéressantes pour instancier les concepts d'analyse dysfonctionnelle. Ainsi, une comparaison entre les ontologies fondamentales suivant ces critères aboutit à choisir une ontologie de haut niveau, appelée **UFO** (**Unified Foundational Ontology**) [Guizzardi, 2005], [Guizzardi *et al.*, 2015]. *Pourquoi UFO ?* Nous répondons à cette question dans ce qui suit.

En la comparant à d'autres ontologies de niveau supérieur telles que GFO [Herre, 2010] et BFO [Arp *et al.*, 2015], on remarque que UFO propose une ensemble complet de concepts couvrant les aspects importants de l'analyse dysfonctionnelle. En effet, les propriétés temporelles et spatiales considérés par GFO et BFO ne sont pas appropriées à notre contexte d'application. Le domaine d'intérêt d'analyse dysfonctionnelle nécessite une description dynamique basée sur des concepts à caractère événementiel et, par conséquent, les distinctions d'entités de BFO et GFO en deux catégories ne conviennent pas à notre étude. D'autre part, nous avons choisi UFO parce qu'elle a été construite dans l'objectif principal de développer les fondements de la modélisation conceptuelle. Par conséquent, UFO aborde de nombreux aspects essentiels de la modélisation conceptuelle, qui n'ont pas reçu une attention suffisamment détaillée dans d'autres ontologies fondamentales. Nous pouvons citer par exemple les notions de relations matérielles et de propriétés relationnelles que DOLCE, qui s'est focalisée uniquement sur les propriétés intrinsèques (qualités), n'a pas traité. De plus, UFO a été utilisée avec succès dans un certain nombre d'analyses sémantiques comme discuté dans [Guizzardi *et al.*, 2015].

L'avantage d'utiliser UFO réside dans l'observation d'entités sous un angle uniforme dans le monde réel. La sémantique du monde réel vise à établir des relations entre les concepts d'analyse dysfonctionnelle et les concepts fondamentaux tels que objet, événement, situation, disposition, dans le développement d'une ontologie de domaine [El Ghosh *et al.*, 2017]. Par conséquent, ces concepts fondamentaux fournissent l'externalisation de la sémantique du monde réel des concepts d'ontologie, le choix d'un pattern

pour représenter des connaissances du domaine et sa justification solide et consensuelle de haut niveau. Dans la phase de conceptualisation, les concepts et relations pertinents doivent être identifiés et organisés. Pour mener à bien cette phase, un modèle graphique est un instrument clé pour assister la communication, la négociation et l'établissement d'un consensus avec les experts du domaine. Pour construire des ontologies de domaine de référence, des langages d'un haut niveau d'expressivité doivent être utilisés pour créer des ontologies fortement axiomatisées qui se rapprochent le plus possible de l'ontologie idéale du domaine. Ainsi, ces langages mettent l'accent sur l'adéquation de la représentation, car les spécifications résultantes sont destinées à être utilisées par des humains.

L'autre avantage d'utiliser l'ontologie fondamentale UFO, dans cette étude, consiste à fournir une interprétation et une modélisation multi-vues avec un vocabulaire commun. Ceci est possible grâce au langage de haut niveau d'expressivité défini pour la modélisation conceptuelle, appelé *OntoUML* [1]. Il s'agit d'une extension UML proposée par Guizzardi afin de réinterpréter le méta-modèle UML 2.0 pour la modélisation conceptuelle et l'ingénierie des ontologies du domaine [Guizzardi, 2005], [Guizzardi *et al.*, 2015]. Les diagrammes OntoUML ressemblent de loin aux diagrammes de classes UML et incorporent les importantes distinctions fondamentales établies par UFO. Cet aspect est approprié à notre problématique car le modèle conceptuel expressif sert comme base de communication et de compréhension non-ambiguë du domaine.

L'ensemble de concepts et des relations, étant approprié à être réutilisé dans le développement de l'ontologie d'analyse dysfonctionnelle, est illustré par la figure 3.3.

Remarque 3.1 *Dans ce mémoire de thèse, les concepts et les relations sont inscrits respectivement en caractères gras et italiques. Ce choix de style est appliqué dans la description des concepts et relations fondamentaux et du domaine afin d'améliorer la lisibilité. Ainsi, tous les concepts et les relations sont exprimés en anglais afin de garder le sens exact et précis des distinctions fondamentales.*

Dans ce diagramme OntoUML, les concepts sont représentés dans des rectangles ; les relations associatives sont labellisées par $\ll \blacktriangleright \gg$ pour indiquer le sens de lecture ; la cardinalité est mentionnée à chaque extrémité d'une relation associative et les relations de subsomption sont représentées par $\ll \triangle \gg$ pour lier un sous-concept à son super-concept. Ces notations sont utilisées, dans ce manuscrit, pour conceptualiser les connaissances du domaine. Lorsque l'on illustre par des exemples ferroviaires, les concepts et leurs instances sont utilisés indistinctement dans cette section. Cette illustration ferroviaire des concepts fondamentaux permet de justifier la validité de notre choix d'ontologie mais aussi de simplifier la définition des concepts abstraits UFO.

La figure 3.3 représente le fragment UFO en OntoUML mettant en avant la distinction établie par UFO dans la taxinomie des **Individuals** entre les **Events** et les **Endu-**

1. https ://ontouml.org/

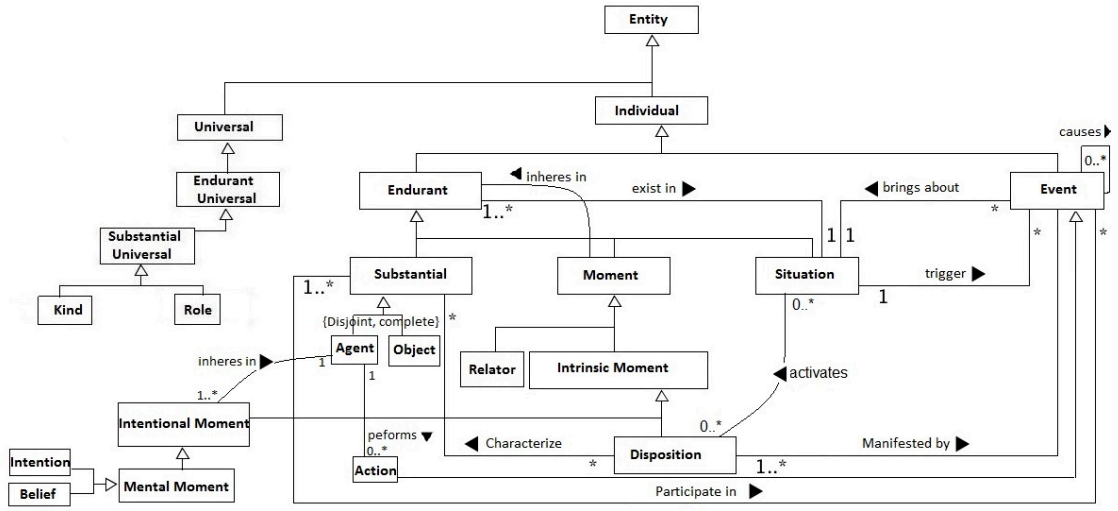

Figure 3.3 – Fragment UFO des **Events** et **Endurants**

rants. Un événement, instance d'**Event**, est une entité qui s'étend dans le temps tout en acquérant ses parties temporelles constitutives. En d'autres termes, les parties d'événement ne peuvent pas exister simultanément et un événement dépend « existentiellement » de ses parties. Par exemple, les éléments constitutifs de l'événement « collision entre deux trains » sont « collision dans une zone occupée » et « trains heurtés », qui existent dans un ordre chronologique. Au contraire, un endurant, instance d'**Endurant**, est une entité dotée d'une identité unique en la conservant dans le temps.

Un **Endurant** incorpore (*subsumes* en anglais) divers sous-concepts tels que **Substantial**, **Situation**, **Moment** et **Disposition**, qui sont intéressants pour notre contexte de travail. Un substantial, instance de **Substantial**, est un endurant existentiellement indépendant des autres endurants. Par exemple, un train est un substantial dont l'existence est indépendante de tout autre endurant. Une situation, instance de **Situation**, est établie par un ou plusieurs endurants. Dans ce contexte, une situation est considérée comme un état des choses ou une combinaison de circonstances à un moment donné. La relation entre la **Situation** et ses composants **Endurants** est nommée *existe in*.

Ainsi, un moment, instance de **Moment**, dépend de l'existence de plusieurs autres endurants tel que l'occupation de la zone qui dépend de la présence du train (situation) et du circuit de voie[2] (objet). Cette illustration justifie la relation *inheres in*[3] entre un **Moment** et un **Endurant**.

D'autre part, une disposition, une instance de **Disposition** est un type spécial du **Moment** et dépend existentiellement d'un seul endurant. Par exemple, la vitesse du train est une disposition qui ne dépend que du train. Une **Disposition** se manifeste dans certaines **Situations** par l'occurrence d'un **Event**. D'où la relation *activates* entre les concepts **Si-**

2. Un circuit de voie est un dispositif technique qui détecte l'occupation de la zone.
3. Il s'agit d'une relation d'appartenance intrinsèque entre les endurants.

tuation et **Disposition**. La relation *characterize* entre la **Disposition** et l'**Endurant** correspondant est définie afin de caractériser un endurant par des propriétés.

Les relations causales fondamentales définies par UFO entre les concepts **Situation** et **Event** sont nommées *triggers* et *brings about*. En langage naturel, ces relations ont un sens commun sauf qu'elles sont distinguées dans la modélisation conceptuelle de UFO pour désigner les relations causales, dans le sens direct et inverse, entre une **Situation** et un **Event**. En outre, un **Event** se produit par la manifestation de différentes **Dispositions** qui existent dans (*exist in*) une **Situation**. À titre d'illustration, l'événement ≪ le train entre dans une zone en franchissant un signal fermé ≫ est la manifestation des dispositions ≪ le mouvement du train ≫ et ≪ la permission de franchir la fin d'autorisation de mouvement (EOA) [4] ≫ délivrée par l'agent de trafic.

Ensuite, un **Event** peut changer l'état des choses d'une **Situation** à une autre par la relation *brings about*. Par exemple, l'événement ≪ le train franchit EOA ≫ change la réalité de la situation ≪ le train se déplace à une vitesse spécifique ≫ en la situation ≪ le train se déplace à la vitesse cible à l'EOA ≫. En effet, il y a un lien technique entre la vitesse cible et la nécessité de s'arrêter avant l'EOA.

En comparant UFO avec d'autres ontologies fondamentales, une des différences majeures et intéressantes consiste à définir deux concepts pour distinguer le type de **Substantial**. Dans la présente étude, seuls les concepts **Agent** et **Object** sont pertinents pour couvrir l'aspect socio-technique des systèmes ferroviaires. Un **Object** est défini comme une entité **Substantial** ≪ non-agentive ≫. Un **Agent** en tant que **Substantial** est une entité concrète ou un individu qui est capable de réaliser des **Actions** et porte des propriétés intentionnelles (**Mental Moments**) tels que les **Belief**, **Intention** et **Desire**. Dans notre contexte, nous nous intéressons particulièrement aux concepts **Belief** et **Intention** pour représenter les propriétés intentionnelles des agents. Une **Intention** représente l'engagement interne de l'**Agent** d'agir en vue d'un but par un plan permettant de l'atteindre [Negri *et al.*, 2017]. D'autre part, une croyance (**Belief**) est basée sur les hypothèses des parties prenantes et représente une **Situation** dont l'agent croit être vraie.

Dans cette section, nous avons présenté les critères de choix de l'ontologie de haut niveau à utiliser dans le développement de l'ontologie de l'analyse dysfonctionnelle. Ensuite, nous avons argumenté le choix de l'ontologie UFO et nous avons défini ses concepts et ses relations fondamentaux qui sont intéressants pour cette étude. Ainsi, le fragment UFO pouvant être réutilisé est défini pour pouvoir exploiter ses concepts pour la conceptualisation du domaine d'analyse dysfonctionnelle. Ensuite, le passage de la phase de conceptualisation à la phase de conception de l'ontologie nécessite la transformation du modèle conceptuel obtenu dans un langage formel interprétable par la machine. Dans le chapitre précédent (section 2.3.4), nous avons discuté les langages d'ontologies et leur classification suivant le

4. L'autorisation de mouvement (MA) est un distance qui se termine par un ≪ End Of Authority ≫ (EOA). L'EOA est un signal pour arrêter le train.

niveau d'expressivité. Pour répondre à nos besoins d'expressivité sémantique, nous avons retenu le langage formel OWL. Nous adoptons ce langage pour formaliser l'ontologie du domaine proposée et nous présentons sa syntaxe et ses symboles dans la section suivante.

3.3.3 Langage d'ontologie

OWL DL permet de construire des ontologies avec un haut niveau d'expressivité et c'est l'un des motifs de son choix comme langage d'ontologie pour les modèles décrits dans cette thèse. En effet, le profile OWL DL a une sémantique basé sur la logique de description *SROIQ (D)*. OWL fournit un moyen très expressif pour définir des ontologies formelles et maintenir la facilité de traitement. Ainsi, il est toujours possible pour un raisonneur automatisé à faire des déductions solides et complètes sur une ontologie exprimée de cette manière. OWL permet le raisonnement basé sur les hypothèses du monde ouvert (*Open World Assumptions (OWA)*). Lors de l'utilisation de l'OWA, seules les affirmations faites dans une base de connaissance particulière sont connues pour être vraies. En fait, l'absence d'une déclaration n'implique pas qu'elle soit fausse mais qu'elle est juste inconnue. Cela rend l'OWA approprié pour la modélisation sémantique et la découverte de connaissances, où seulement des représentations partielles d'une vision du monde sont créées. La capacité de raisonner sur des informations incomplètes est parfois une caractéristique désirée. Cependant, dans certaines situations, l'hypothèse du monde fermé (*Closed World Assumption (CWA)*) adoptée par les applications de base de données peut être plus appropriée car elle permet de valider les données et de poser des contraintes sur les informations.

L'absence de la sémantique du monde fermé dans OWL crée des difficultés pour mettre en œuvre certaines caractéristiques pratiques telles que la validation des données et la vérification des contraintes. Pour cette raison, il existe plusieurs façons d'entreprendre le raisonnement en monde fermé (*closed world reasoning*) dans OWL. En effet, la déclaration explicite des axiomes dans la sémantique du monde fermé permet aux raisonneurs de comprendre à la fois la sémantique du monde ouvert et fermé. D'autre part, il est possible d'interpréter la sémantique OWL à travers les hypothèses du monde fermé et de les traduire dans des requêtes SPARQL (Sparql Protocol and RDF Query Language) [Kaminski et Kostylev, 2016]. SPARQL est un langage pour exécuter des requêtes complexes sur des graphes RDF (Ressource Description Framework) [Cyganiak *et al.*, 2014]. SPARQL permet d'effectuer les opérations de recherche et de mise à jour de données RDF, ainsi que les recherches des données en utilisant des modèles exprimés dans un format RDF. En effet, les ontologies exprimées en OWL DL sont transformables en des graphes RDF ; Un graphe RDF est construit sur l'idée d'un triple, qui code une relation entre un sujet et un objet à travers une propriété, ou un prédicat, sous la forme $< sujet >< prédicat >< objet >$.

Dans le cadre de cette thèse, nous utilisons le fragment logique $DLP_{\exists}$ [Carral *et al.*, 2013] pour encoder le pattern de l'ontologie d'analyse dysfonctionnelle proposée. Ce fragment permet d'avoir un raisonnement traitable pour combler les manques d'OWA évoqués

ci-dessus et pour avoir une implémentation efficace de l'ontologie proposée. Ainsi, nous utilisons la notation des logiques de description (DL) pour spécifier les axiomes permettant de contraindre la taxonomie proposée et renforcer le comportement de la version implémentée de l'ontologie. Afin d'améliorer la compréhensibilité et la lisibilité de la description de notre contribution, nous illustrons la syntaxe et les symboles de la notation DL et la correspondance en termes OWL dans le tableau 3.2.

Symbole DL	**Terme OWL**	**Exemple/Description**
	owl :Class	rdf :type of ressources définies comme des Classes
	owl :Individual	rdf :type of ressources définies comme des Individuals
$\top$	owl :Thing	La classe à laquelle tous les individuals appartiennent
$\bot$	owl :Nothing	La classe à laquelle aucun individual appartient (ensemble vide)
$\sqcap$	owl :intersectionOf	Lion $\sqsubseteq$ Animal $\sqcap$ Carnivore
$\sqcup$	owl :unionOf	Humain $\sqsubseteq$ Adulte $\sqcup$ Enfant
$\exists$R.C	owl :someValuesFrom	Existentiel « has some » restriction : Human $\sqsubseteq \exists$hasPart.Visage
$\forall$R.C	owl :allValuesFrom	Universel « only has » restriction : Train $\sqsubseteq \forall$ roule.Rails
$\leq$ n U	owl :minCardinality	Minimum cardinality restriction : Voiture $\sqsubseteq \leq 4$ hasPart.Roues
$\geq$ n U	owl :maxCardinality	Max cardinality restriction : Train $\sqsubseteq \geq 1$ hasPart.Wagon
	owl :TransitiveProperty	« Lucas frère de Benjamin, Benjamin frère de Romain » infère « Lucas frère de Romain »

Tableau 3.2 – Constructeurs OWL et les symboles DL correspondants

À titre d'illustration, nous prenons l'exemple suivant : Un train a au moins une voiture et peut être de type voyageurs ou marchandises. Cette affirmation est représentée en notation $DLP_{\exists}$ comme suit :

$$\text{Train} \sqsubseteq \geq 1 \mathit{hasVoiture}.\top \sqcap (\forall \text{hasType.Voyageurs}) \sqcup (\forall \text{hasType.Marchandises})$$

Dans cet exemple, les concepts `Train` et `Thing` ($\top$) sont des concepts atomiques, de même que les deux types `voyageurs` et `marchandises`. *hasVoiture* et *hasType* sont des prédicats binaires ou des relations atomiques. Comme le montre tableau 3.2, le concept `Thing` ($\top$) correspond au concept auquel tous les individus appartiennent. L'élément `R.C`

représente une restriction de valeurs de l'ensemble des concepts liés à la classe `C` à travers la relation `R`. Ainsi, la valeur de cardinalité d'une relation est bornée par une valeur `n` minimale ($\geq$) ou maximale ($\leq$). La figure 3.4 définit d'autres constructeurs du fragment logique $DLP_{\exists}$ adopté dans la formalisation de l'ontologie proposée. Dans la base de connaissances $DLP_{\exists}$, les axiomes sont classés en des déclarations *ABox* A, *TBox* B et *RBox* R[5]. Un TBox [RBox] est un ensemble fini d'inclusions de concept général (GCI) [axiomes d'inclusion de rôle (RIA)] décrits dans le tableau 1. Un *ABox* est un ensemble fini d'assertions de concepts et de rôles. En outre, $DLP_{\exists}$ oblige le constructeur de restriction cardinale au plus un ($\leq$ 1`R`.`C`) à apparaître uniquement dans le côté droit de GCI.

Nom	Syntaxe	Sémantique
Concept Assertion	$C(a)$	$a^{\tau} \in C^{\tau}$
Role Assertion	$R(a,b)$	$\langle a,b\rangle \in R^{\tau}$
GCI	$C \sqsubseteq D$	$C^{\tau} \subseteq D^{\tau}$
Existencial Restriction	$\exists R.C$	$\{\delta \mid there\ is\ \epsilon\ with\ \langle\delta,\epsilon\rangle \in R^{\tau}\ and\ \epsilon \in C^{\tau}\}$
$\leq$ 1 Card. Restriction	$\leq 1R.C$	$\{\delta \mid \#\{\langle\delta,\epsilon\rangle\} \in R^{\tau} \mid \epsilon \in C^{\tau}\} \leq 1$
Concept Conjunction	$C \sqcap D$	$C^{\tau} \cap D^{\tau}$
Top concept	$\top$	Δ^{τ}
Bottom concept	$\bot$	$\emptyset$
RIA	$R \sqsubseteq S$	$R^{\tau} \subseteq S^{\tau}$
Role Inverse	R^{-}	$\{\langle\delta,\epsilon\rangle \mid \langle\epsilon,\delta\rangle \in V^{\tau}\}$
Role Chain (RIA)	$R_1 \circ \cdots \circ R_n$	$R_1^{\tau} \circ \cdots \circ R_n^{\tau}$
Role Conjunction	$R \sqcap S$	$R^{\tau} \cap S^{\tau}$

Figure 3.4 – Les constructeurs de $DLP_{\exists}$. C et $D \in$ `C`, R et S sont des rôles [Carral *et al.*, 2013]

Après avoir défini les choix méthodologiques et les contraintes métier, nous présentons, dans la section suivante, notre contribution par rapport au développement d'une nouvelle ontologie du domaine d'analyse dysfonctionnelle, appelée **DAO** (**Dysfunctional Analysis Ontology**). Une partie des concepts introduits dans DAO ont été inspirés d'une ontologie existante dans la littérature pour clarifier la terminologie des fautes, défauts et erreurs pour les logiciels [Duarte *et al.*, 2018]. Cette ontologie se focalise sur les anomalies logicielles qui peuvent impacter la sécurité-confidentialité. Néanmoins, le présent mémoire étudie essentiellement la sécurité-innocuité pour clarifier les concepts de l'analyse dysfonctionnelle appliqués aux SCS. Les besoins en termes de la structure des concepts, leur interprétation ainsi que le contexte d'application sont donc très différents.

Dans DAO, l'interprétation des concepts dans la sémantique du monde réel repose sur leur adaptation du point de vue sécurité-innocuité pour répondre aux besoins des SCS. Différemment de l'ontologie proposée par [Duarte *et al.*, 2018], nous intégrons les aspects humains et techniques liés à l'environnement du système qui peuvent contribuer

5. Respectivement des boxes d'assertions, terminologique et de rôles

à l'exposition au danger. D'autre part, nous proposons des concepts liés aux propriétés intentionnelles des erreurs humaines qui s'appuient sur une interprétation du modèle de l'erreur humaine de James Reason [Larouzée *et al.*, 2014]. En effet, l'aspect malicieux lié aux intrusions et aux cyberattaques n'est pas pertinent pour la sécurité-innocuité des systèmes ferroviaires. Afin d'avoir une représentation complète des connaissances du domaine, nous considérons les notions de « **danger** » et « **mesures de sécurité** » qui sont structurantes pour l'analyse dysfonctionnelle.

3.4 L'Ontologie d'Analyse Dysfonctionnelle proposée (DAO)

Dans la section 3.2, nous avons identifié des verrous scientifiques et technologiques que nous allons lever. Afin d'établir une méthodologie de développement guidée par ces verrous, nous formulons une première question de recherche (QR1) à laquelle nous répondons dans ce chapitre :

QR1 : *Comment fournir une représentation structurée de l'analyse dysfonctionnelle dans la sémantique du monde réel pour combler les lacunes d'ambiguïté terminologique et d'hétérogénéité sémantique ?*

La réponse à cette question est amenée par les différentes étapes de la méthodologie SABiO que nous détaillons dans ce qui suit. La figure 3.5 illustre l'utilisation de SABiO dans le développement de DAO.

3.4.1 Identification des objectifs et des exigences de DAO

Dans le contexte de collaboration multidisciplinaire du développement des SCS, les techniques traditionnelles d'analyse de sécurité sont toujours basées sur une connaissance approfondie des comportements du système, ce qui n'est pas facile à acquérir dès les premières phases de conception. Les méthodes d'analyse dysfonctionnelle sont appliquées afin d'identifier les dangers, définir comment les composants impliqués contribuent à l'occurrence des situations dangereuses et dériver les mesures de sécurité qui mitigent les dangers. Ensuite, ces mesures de sécurité sont prises en compte par les concepteurs du système afin de satisfaire des buts de sécurité globaux. Par conséquent, le développement des SCS s'appuie sur le partage des connaissances entre les experts du domaine, les ingénieurs sécurité et les concepteurs.

Actuellement, il manque une clarification conceptuelle et une taxinomie complète qui fournissent une formalisation bien établie de la notion de **défaillance** et des concepts liés dans la terminologie des SCS. Les éléments d'analyse dysfonctionnelle tels qu'une défaillance, ses causes et ses effets sont généralement formulés de manière informelle par ce qu'ils présentent et comment ils sont présentés. Dans ces travaux, nous considérons deux aspects de l'analyse dysfonctionnelle : un composant du système est exposé à un danger et

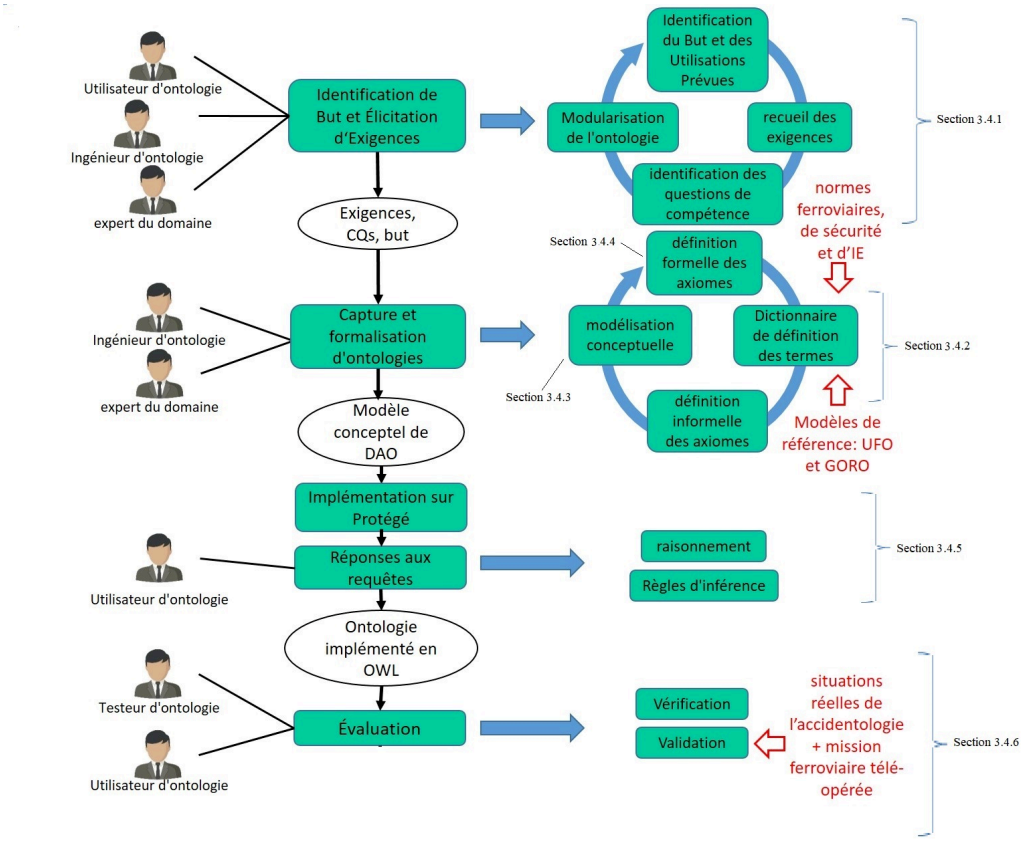

Figure 3.5 – Illustration de l'utilisation de SABiO pour le développement de DAO

un composant du système provoque un danger, qui déclenche des accidents. D'autre part, la relation de causalité à travers les défaillances en cascade doit être prise en compte dans le processus d'analyse dysfonctionnelle.

Dans la première phase de l'approche SABiO, un ensemble de *questions de compétence* (QC), qui sont des questions auxquelles l'ontologie doit pouvoir répondre [de Almeida Falbo, 2014], sont déterminées pour définir l'étendue de l'ontologie. En d'autres termes, ces QC définissent les exigences fonctionnelles de l'ontologie afin d'orienter le processus de développement dès les premières phases et sont utilisées dans la phase d'évaluation pour vérifier la conformité de l'ontologie proposée à ses exigences prévues. Ensuite, la vérification et la validation de DAO sont effectuées à l'aide des techniques de validation et de vérification définies par SABiO.

L'ontologie DAO proposée pour la conception des SCS vise à fournir une analyse ontologique des termes d'analyse dysfonctionnelle tels que la défaillance, ses causes, ses effets et les mesures de sécurité. La systématisation d'analyse dysfonctionnelle proposée est indépendante des méthodes d'analyse de la sécurité requises pour la conception des SCS. Elle fournit, en effet, une vue interopérable de ces méthodes, puisque la conceptualisation et la formalisation de DAO prennent en compte plusieurs aspects tels que les défaillances des composants du système, les défaillances dues aux facteurs environnementaux (objets)

et aux erreurs humaines du système et de son environnement.

Étant une ontologie de domaine, DAO est fondée sur l'ontologie de haut niveau UFO afin de faire face à l'hétérogénéité sémantique et aux conflits entre les parties. Dans ce contexte, la QR1 capturant la question de recherche globale est raffinée en des QC à l'égard de la modélisation conceptuelle dirigée par UFO. Autrement-dit, la réponse aux exigences de DAO doit être effectuée en s'appuyant sur les concepts et les relations d'UFO. Ces QCs sont élucidées comme suit :

- **QC1** : Qu'est-ce qu'une défaillance ?
- **QC2** : Comment une défaillance peut-elle se produire ?
- **QC3** : Quelles sont les situations résultantes d'une défaillance ?
- **QC4** : Qu'est-ce qu'une mesure de sécurité ?
- **QC5** : Quel est le type de comportements humain et physique en relation avec la défaillance ?

3.4.2 Acquisition des connaissances de l'analyse dysfonctionnelle

Avant de conceptualiser les connaissances d'analyse dysfonctionnelle, nous procédons au recueil des connaissances à partir des experts des domaines, des textes normatifs et des modèles de référence. Cette étape d'acquisition des connaissances a pour objectif d'identifier les concepts du domaine pertinents à la conceptualisation commune d'analyse dysfonctionnelle. En effet, l'harmonisation conceptuelle de la défaillance et de ses concepts environnants est basée sur une extraction des définitions établies par les normes internationales et sur les connaissances du domaine ferroviaire, qui est notre domaine d'application. Dans cette section, nous justifions la pertinence des concepts utilisés dans DAO par rapport aux besoins et leur sources d'acquisition. Par ailleurs, les définitions évoquées dans le chapitre 1 sont rappelées ici afin de créer le lien logique entre les connaissances qui émanent de différentes normes. La représentation structurée de ces connaissances dans modèle met en lumière la cohérence entre les normes utilisées.

Faisant partie des entraves de la sûreté de fonctionnement SdF (présentées dans le chapitre 1, Définition 1), la **défaillance** est définie par la norme [IEC 61508, Norme Internationale, 2000] comme la cessation de l'aptitude d'une entité à accomplir une fonction requise. Ainsi, elle représente la conséquence d'une **erreur** observée au niveau du comportement du système. Selon la même norme, cette erreur est interprétée comme un état du système représentant un écart entre une condition mesurée et la condition théoriquement vraie. Cet écart est dû à une **faute** dont l'origine est due à un comportement humain ou à un phénomène physique erronés. De ce fait, nous pouvons déduire la relation de causalité implicite entre les entraves de la SdF ainsi que leur relation avec le **comportement humain** et le **phénomène physique** erronés. Néanmoins, la terminologie utilisée dans ces définitions n'est pas précise et ne met pas en avant une interprétation claire et commune de ces concepts pertinents à l'analyse dysfonctionnelle.

Mise à part le type d'entités et de relations, les entraves de la SdF et les concepts en liaison directe et indirecte doivent être représentés explicitement et interprétés dans la sémantique du monde réel. Autrement-dit, une clarification conceptuelle permettant de définir la nature terminologique de ces concepts est nécessaire afin de lever les ambiguïtés. Ces concepts sont considérés dans la modélisation conceptuelle de l'analyse dysfonctionnelle proposée afin de faire un compromis entre les définitions établies par les standards du domaine et la définition des concepts fondamentaux de UFO. Ce compromis s'appuie principalement sur un alignement bien établi des concepts du domaine et les concepts de l'ontologie de haut niveau UFO.

D'autre part, le **danger** constitue un concept fondamental de l'analyse dysfonctionnelle. Dans la norme [CENELEC, NF EN 50126-1, 2017] le danger est défini comme une condition pouvant conduire à un accident (Définition 2). Ainsi, la fréquence de l'**exposition** au danger et la gravité des conséquences du danger sont deux concepts clé de la notion de risque. Par conséquent, les concepts de danger et de l'exposition sont requis dans la représentation des connaissances d'analyse dysfonctionnelle. En fait, le danger représente une propriété intrinsèque de toute source potentielle pouvant causer des dommages sur le **système**, les **acteurs humains** et **l'environnement**. L'exposition représente, en effet, une caractéristique de toute entité exposée à un danger représentant la nature et la manière de l'exposition. En effet, le système peut être à la fois en exposition au danger et une source de danger. Par contre, nous jugeons que le concept du risque n'est pas nécessaire pour la compréhension du domaine d'analyse dysfonctionnelle car il est déduit à partir des propriétés du danger (occurrence et gravité des conséquences). Nous rappelons que l'objectif principal d'une ontologie du domaine est de capturer les connaissances clé du domaine.

En outre, la **mesure de sécurité** est généralement définie comme une exigence de sécurité qui permet de réduire le risque et atténuer le danger [Zhou *et al.*, 2017]. Cette définition implique deux connaissances des domaines différents ainsi que l'équivalence des mesures de sécurité et des exigences de sécurité qui pose des ambiguïtés dans la conception des SCS. Par ailleurs, il convient de fournir une harmonisation sémantique permettant d'éviter les conflits de conception. Dans ce chapitre, nous considérons l'interprétation des mesures de sécurité de la perspective de l'analyse dysfonctionnelle. Cependant, les relations entre ce concept et les concepts du domaine d'ingénierie des exigences sont définis dans le chapitre 4. Dans l'objectif de garder la traçabilité de ce concept tout au long du cycle de développement des SCS, il est plus judicieux d'établir un alignement entre les connaissances des deux domaines pour avoir une vue partagée. De ce fait, nous commençons par établir une analyse ontologique de ce concept du point de vue sécurité afin de faciliter la tâche d'alignement par la suite.

Comme discuté dans la section 3.2.1, l'aspect socio-technique des systèmes ferroviaires et leur environnement exige une prise en compte des différents concepts ayant un impact sur

leur comportement. Toutefois, la relation entre les concepts recueillis ci-dessus et cet aspect n'est pas mise en avant explicitement par les documents normatifs du domaine ferroviaire ni les les standards de sécurité des SCS. Par conséquent, une clarification conceptuelle est nécessaire pour représenter les entités importantes du domaine d'analyse dysfonctionnelle et assurer une compréhension efficace.

3.4.3 Conceptualisation de l'analyse dysfonctionnelle

Dans le contexte de la prise de décision collaborative, la modélisation conceptuelle est une activité préliminaire pour fournir une représentation compréhensible des connaissances du domaine basée sur des hypothèses du monde réel. Dans cette section, nous présentons une nouvelle conceptualisation commune des éléments principaux de l'analyse dysfonctionnelle acquis auparavant. Ainsi, le modèle conceptuel de DAO permet de systématiser son intégration précoce dans le processus de conception des SCS. La figure 3.6 représente le modèle conceptuel de l'ontologie DAO en utilisant le langage de modélisation conceptuelle proposé par UFO, OntoUML. L'interprétation des concepts dans la sémantique du monde réel vise à établir des relations entre le domaine d'analyse dysfonctionnelle et les distinctions fondamentales de UFO. Les nouveaux concepts définis dans le cadre de cette étude sont cadrés en rouge afin de les distinguer des concepts existants.

Le modèle conceptuel de DAO est fondé sur UFO afin d'améliorer la clarification conceptuelle du raisonnement de sécurité ainsi que la gestion des décisions de sécurité. Cette description ontologique des connaissances de l'analyse dysfonctionnelle répond à la **QR1**. À l'issue de la phase d'acquisition, la capture des connaissances est basée sur les connaissances du domaine ferroviaire et celles recueillies à partir des experts du domaine.

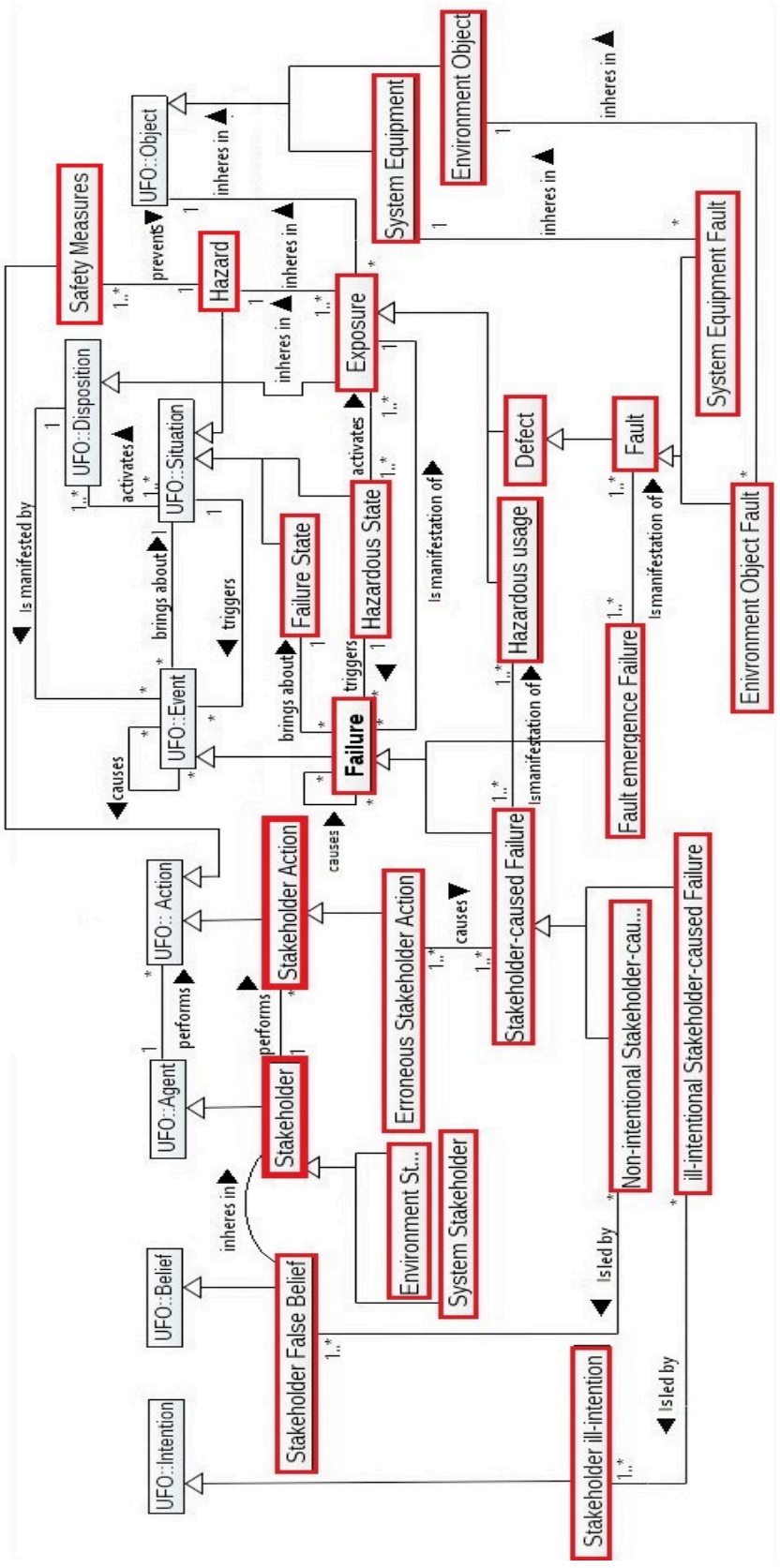

Figure 3.6 – Modèle conceptuel de l'ontologie d'analyse dysfonctionnelle DAO

Les considérations prises lors de la phase de l'acquisition permettent d'avoir une ontologie claire et réutilisable pour d'autres domaines critiques mais aussi une taxonomie de DAO flexible et non ambiguë. La modélisation conceptuelle est établie d'une façon itérative et incrémentale afin d'obtenir une vue syntaxique, structurée et sémantique de l'analyse dysfonctionnelle, répondant aux QC élucidées au préalable. Dans la description du modèle conceptuel, nous utilisons le style énoncé dans la Remarque 3.1 pour améliorer la lisibilité et mettre en lumière le processus d'alignement des concepts d'analyse dysfonctionnelle avec les concepts d'UFO. La construction du modèle conceptuel est basée sur le principe de modularisation afin de gérer la complexité du domaine d'analyse dysfonctionnelle. Ainsi, la combinaison des différents modules de DAO permet de fournir une ontologie du domaine qui satisfait aux contraintes scientifiques et aux contraintes métier identifiées dans une phase préliminaire.

Concept central de DAO, la défaillance (**Failure**) constitue le noyau de l'analyse dysfonctionnelle et son apparition conduit à de nombreux problèmes durant tout le cycle de vie des SCS, à savoir sa conception, son exploitation et sa maintenance. Selon les normes [IEEE 610.12, 1990], [IEEE 1012, 2016] et la littérature [Johnson, 2003], une défaillance *est un*[6] événement (**Event**, concept d'UFO).

Les concepts fondamentaux fournis par UFO permettent de mieux comprendre comment se produit une défaillance en tant qu'événement au cours de la phase opérationnelle des SCS. Dans un contexte système, une défaillance est considérée comme un événement dans lequel un système ou un composant est incapable d'effectuer sa fonction requise comme attendu. En d'autres termes, chaque événement qui est en conflit avec les objectifs des parties prenantes et qui viole l'ensemble des conditions d'appartenance à l'état de sécurité est considérée comme une défaillance. En outre, en tant que caractéristique du concept **Event**, une défaillance peut entraîner (*causes*) d'autres défaillances dans une chaîne d'événements comme une défaillance en cascade. Par exemple, la défaillance du système de signalisation ferroviaire peut causer le défaillance du circuit de voie et de tous les sous-systèmes associés. Dans une perspective UFO, un **Event** est lié à deux **Situations** différentes par deux relations de causalité de haut niveau (voir Section 3.3.2). Afin de clarifier la terminologie des causes/conséquences d'une défaillance, nous nous appuyons sur cette distinction fondamentale proposée par UFO :

1. La situation qui existe avant l'occurrence de la défaillance est représentée comme un état dangereux (**Hazardous State**) qui déclenche (*triggers*) la défaillance.
2. La situation engendrée par l'occurrence de la défaillance lorsqu'elle provoque (*brings about*) un état de défaillance (**Failure State**).

6. La relation *est un* représente la subsomption (*is_a*) des concepts afin d'établir une hiérarchie.

En effet, la première situation (**Hazardous State**) indique l'état d'être exposé à un risque qui active (*activates*) la **Disposition** (**Exposure**) qui se manifeste par (*is manifested by*) la défaillance (**Failure**). Ainsi, nous introduisons le concept d'exposition (**Exposure**) comme un *sous-type de* **Disposition** (un type spécial de **Moment**). Il représente le moment d'exposition (**Exposure Moment**) qui appartient intrinsèquement (*inheres in*) aux objets (le concept **Object** de UFO) et est activé par l'état dangereux (**Hazardous State**). La relation *inheres in* est introduite aussi entre les concepts **Exposure** et **Hazard**. Nous justifions cette interprétation par le fait que l'exposition au danger est inhérente au danger (**Hazard**) et l'existence du risque dépend des deux facteurs à la fois. La mise en avant des ces concepts ainsi que la relation de haut niveau proposée par UFO entre eux contribue au processus d'analyse qualitatif des risques. D'autre part, l'aspect quantitatif de cette analyse peut être intégré sous forme de propriétés et types de données lorsqu'une version interprétable par la machine est implémentée.

À partir de cette analyse préliminaire des risques, un ensemble de mesures de sécurité **Safety Measures** est introduit pour prévenir le danger ; d'où la relation *prevents* entre les deux concepts **Safety Measures** et **Hazard**. Par ailleurs, il convient d'interpréter ces mesures de sécurité d'un point de vue sécurité et conception des SCS.

Définition 5 . *(Mesures de sécurité) Nous définissons les mesures de sécurité comme des* ***Actions*** *mises en œuvre pour éviter un danger perçu. Dans une terminologie de conception des SCS, ces actions peuvent être un choix architectural, un dispositif technique ou une intervention humaine. Par conséquent, nous avons ajouté la relation de composition du concept* ***Safety Measures*** *en sous-mesures de sécurité.*

Systèmes socio-techniques par essence, les systèmes ferroviaires et la gestion de leur sécurité impliquent des opérateurs humains, des défaillances techniques, des interactions dysfonctionnelles entre les composants du système, ou même des perturbations externes d'environnement. Afin de répondre à ces contraintes du métier ferroviaire, nous considérons les deux types de défaillances dues à des erreurs humaines et techniques, dans les deux perspectives système et environnement.

La défaillance (**Failure**) englobe (*subsumes*) deux sous-types différents :

1. la défaillance causée par les humains (**Stakeholder-caused failure**) : elle représente toute défaillance provoquée par des erreurs humaines dont l'origine est une ou plusieurs actions erronées.
2. la défaillance due à des fautes (**Fault emergence failure**) : ce concept contient toutes les défaillances causées par des erreurs techniques dues à des fautes de composants techniques.

Cette interprétation sémantique satisfait à la fois les définitions établies par les normes (Définition 1) et les contraintes industrielles imposées par la logique métier. En effet, le premier type (**Stakeholder-caused failure**) est *causée par* une action erronée d'un

acteur humain (**Erroneous Stakeholder Action**). *Sous-type* d'**Agent**, l'acteur (**Stakeholer**) peut être (*subsumes*) un acteur du système (**System Stakeholder**) ou un acteur d'environnement (**Environment Stakeholder**). Cette distinction est considérée afin de représenter certaines situations critiques pouvant se produire en tenant compte des connaissance de l'accidentologie et du retour d'expérience des systèmes antérieurs. D'autre part, les textes normatifs [CENELEC, NF EN 50126-1, 2017] préconisent la considération de l'aspect environnemental du système comme un facteur qui impacte la sécurité globale.

Dans l'analyse de la fiabilité humaine, les erreurs humaines sont souvent classifiées sous différents aspects, à savoir comportemental, contextuel et conceptuel [Larouzée *et al.*, 2014]. Dans le cadre de cette étude, nous nous intéressons à l'aspect conceptuel qui met en exergue les mécanismes *cognitifs* à l'origine de la production de l'erreur. Nous jugeons, en effet, qu'il est judicieux d'avoir une vue claire sur l'origine de l'erreur afin de pouvoir agir efficacement en terme de raisonnement de sécurité. À partir du moment où la cause principale des erreurs humaines est dévoilée, les choix liés à la sécurité sont plus motivés et structurés.

Afin de clarifier cet aspect, [Reason, 1987] a proposé une modélisation des erreurs en distinguant celles qui précédent la détection du problème et celles qui la suivent. Dès lors, une distinction fondamentale se dessine entre les erreurs d'exécution d'une action et les erreurs de planification de cette action. Cette notion de planification révèle d'un niveau de contrôle élevé lié à *l'intentionnalité* de l'action. À l'issue de cette interprétation, nous introduisons les concepts **ill-intentional Stakeholder-caused failure** et **Non-intentional Stakeholder-caused failure**, deux sous-types de **Stakeholder-caused failure**.

Le premier type (**ill-intentional Stakeholder-caused failure**) concerne les erreurs de planification de l'action qui n'atteignent pas le but désiré. En effet, cette erreur est menée par (*is led by*) une intention non appropriée (**Stakeholder ill-intention**) car elle ne se déroule pas en accord au *plan* associé à l'intention ou le plan est inadéquat pour atteindre le but. Cette correspondance entre les concepts introduits et les connaissances du domaine issues de la littérature [Larouzée *et al.*, 2014] nous amène aux caractéristiques fondamentales incorporées dans UFO. Cette ontologie de haut niveau considère une relation fondamentale, nommée est menée par (*is led by*), entre le concept **Action** et les concepts **Intention** et **Belief** définis dans la section 3.3.2. Nous rappelons qu'une **Intention** représente l'engagement interne de l'**Agent** d'agir en vue d'un but par un plan permettant de l'atteindre [Negri *et al.*, 2017]. Par ailleurs, cette erreur (**ill-intentional Stakeholder-caused failure**) n'est pas due à une intention malveillante mais plutôt à certains facteurs comme le manque des connaissances métier, la non-maîtrise des gestes et des règles professionnelles, et la violation des procédures imposées, qui affectent la qualité de planification de l'action. Nous citons par exemple le cas d'un conducteur qui n'utilise pas le système de freinage d'urgence le nécessitant, et cela en opposition à l'application des procédures prescrites.

Dans la même vision cognitive de l'erreur humaine, le second type non intentionnel (**Non-intentional Stakeholder-caused failure**) se focalise sur les dysfonctionnements lors de l'exécution des actions. Elle est menée par (*is led by*) par une fausse croyance ou une croyance erronée qu'une situation existe dans l'environnement de l'agent. Selon UFO, une croyance (**Belief**) est basée sur des *hypothèses* qui sont des situations dans l'environnement que l'agent croit être vraies. En fait, l'agent se fait un schéma mental qui ne correspond pas à la réalité et surtout au cadre contextuel de son activité. Si ces hypothèses sont fausses, elles conduisent à des situations qui ne satisfont pas le but désiré. Généralement, ces croyances erronées sont dues à des erreurs de mémoire, d'attention, de conditions physiques et adviennent pour les activités au niveau de contrôle bas basé sur les automatismes ainsi que les tâches routinières. Prenons l'exemple d'un conducteur qui franchit un signal fermé à cause du dysfonctionnement des freins alors qu'il ne s'en rend pas compte ou parce qu'il réagit en retard ; et celui qui n'effectue pas les tests des freins avant le démarrage de son train par oubli.

Afin d'établir le lien sémantique entre cet aspect cognitif de l'origine de production de l'erreur humaine et le danger, nous introduisons le concept (**Hazardous usage**). Un usage dangereux (**Hazardous usage**) est *un sous-type* d'exposition (**Exposure**). Il décrit le **Moment** dans lequel un acteur (**Stakeholder**) effectue une manipulation dangereuse et il *est manifesté par* une défaillance due à une erreur humaine (**Stakeholder-caused failure**). Cette liaison entre la notion de moment mental (**Mental Moment**) [7] et la **Disposition** [8] (**Intrinsic Moment**) satisfait les distinctions de UFO interprétées et adaptées à notre contexte d'étude. D'un point de vue technique du système, le concept défaut (**Defect**) est un sous-type d'**Exposure** inhérente aux (*inheres in*) (**Objects**). Quand il *est manifesté par* une **Fault emergence failure**, le défaut *est une* faute (**Fault**).

En effet, le concept **Fault** *subsumes* deux types : des fautes des objets du système (**System Equipment Fault**) et celles de son environnement (**Environment Object Fault**). En tant que **Disposition**, ces types de fautes sont inhérentes aux (*inheres in*) équipements système (**System Equipment**) et aux objets d'environnement (**Environment Object**). Sous-concepts du concept fondamental **Object**, ces derniers sont distingués afin de mettre en valeur les caractéristiques des composants du système et de leur environnement qui contribuent à l'occurrence du danger.

À la lumière de cette conceptualisation, nous avons tiré profit des concepts abstraits proposés par UFO afin de fournir une base solide d'analyse dysfonctionnelle dans la sémantique du monde réel. En effet, le modèle conceptuel obtenu représente une vue sémantique non ambiguë permettant de satisfaire les qualités syntaxiques et pragmatiques requises dans le cadre développement des SCS. La clarification conceptuelle d'une défaillance, ses causes, ses conséquences, l'origine de production de l'erreur humaine et

7. inclue les concepts **Intention** et **Belief**
8. subsumes le concept **Exposure**

la nature des fautes et l'analyse ontologique de leurs relations à l'égard de UFO permet de fournir une taxonomie commune du domaine. En s'appuyant sur les considérations normatives, les distinctions fondamentales de UFO et les contraintes métier, le modèle conceptuel de DAO est proposé afin de faire face aux conflits de conception des SCS dès les premières phases et d'harmoniser la base de connaissances partagée entre les acteurs multi-disciplinaires. Afin d'améliorer la compréhensibilité de DAO et sa flexibilité pour d'autres domaine critiques, la taxonomie de l'ontologie proposée est détaillé dans [Debbech *et al.*, 2018a]. Cette capture de connaissances est établie à l'égard de l'ontologie de haut niveau UFO afin d'approximer une représentation idéale du domaine qui donne lieu à une ontologie de référence. Pour disposer d'une version opérationnelle de DAO et augmenter sa réutilisation, les spécifications conceptuelles doivent être transformées en un langage formel interprétable par la machine. Ceci fait l'objet de la section suivante.

3.4.4 Formalisation de DAO

Le modèle conceptuel est formellement encodé en utilisant le langage formel d'ontologie OWL défini dans la section 3.3.3. Dans cette section, nous spécifions les axiomes en utilisant le fragment logique $DLP_{\exists}$ introduit auparavant. Ainsi, nous commençons par présenter les axiomes spécifiés pour contraindre la taxinomie proposée. Ensuite, nous justifions l'interprétation à l'égard du modèle conceptuel.

Selon [Guizzardi *et al.*, 2013], les relations de causalité $\mathbf{R}$ [9] définies par UFO et réutilisées dans le modèle conceptuel de DAO, sont déclarées comme des relations d'ordre partiel strict. Par conséquent, $\mathbf{R}$ est irréflexive (ou antiréflexive), asymétrique et transitive, et ces propriétés sont décrites comme suit :

- $\mathbf{R}$ est irréflexive : $\top \sqsubseteq \neg\exists\mathbf{R}.Self$;
- $\mathbf{R}$ est asymétrique : $\exists(\mathbf{R} \sqcap \mathbf{R}^{-}).\top \sqsubseteq \bot$;
- $\mathbf{R}$ est transitive : $\mathbf{R} \circ \mathbf{R} \sqsubseteq \mathbf{R}$;

Axiomes de DAO : Les axiomes liés aux différents modules [10] de l'ontologie DAO sont spécifiés comme suit :

$$Failure \sqsubseteq Event \sqcap \exists bringsAbout.FailureSate \sqcap \forall causes.Failure \sqcap \forall isManifestationOf.Exposure \tag{3.1}$$

$$FailureState \sqsubseteq Situation \sqcap \forall bringsAbout^{-}.Failure \tag{3.2}$$

$$HazardousState \sqsubseteq Situation \sqcap \forall triggers.Failure \sqcap \forall activates.Exposure \tag{3.3}$$

$$\top \sqsubseteq \leq 1 bringsAbout.\top \tag{3.4}$$

9. $\mathbf{R}$ représente les relations *causes*, *triggers* et *brings about*

10. les modules de DAO sont divisés par aspect socio-technique et par perspective système et environnement.

$$\top \sqsubseteq \leq 1 triggers^{-}.\top \tag{3.5}$$

$$causes \circ bringsAbout \sqsubseteq bringsAbout \tag{3.6}$$

$$causes \circ triggers^{-} \sqsubseteq triggers^{-} \tag{3.7}$$

$$triggers^{-} \sqsubseteq isTriggeredbBy \tag{3.8}$$

$$StakeholderCausedFailure \sqsubseteq Failure \sqcap \forall isManifestationOf.HazardousUsage \sqcap \forall causes^{-}.ErroneousStakeholderAction \tag{3.9}$$

$$FaultEmergenceFailure \sqsubseteq Failure \sqcap \forall isManifestationOf.Fault \sqcap \neg \forall causes^{-}.ErroneousStakeholderAction \tag{3.10}$$

$$Exposure \sqsubseteq Disposition \sqcap \exists inheresIn.Object \sqcap \exists inheresIn.Hazard \tag{3.11}$$

$$SystemEquipment \sqcap EnvironmentObject \sqsubseteq Object \tag{3.12}$$

$$HazardousUsage \sqcap Defect \sqsubseteq Exposure \tag{3.13}$$

$$Fault \sqsubseteq Defect \sqcap \forall isManifestedBy.FaultEmergenceFailure \tag{3.14}$$

$$EnvironmentObjectFault \sqsubseteq Fault \sqcap \forall inheresIn.EnvironmentObject \tag{3.15}$$

$$SystemEquipmentFault \sqsubseteq Fault \sqcap \forall inheresIn.SystemEquipment \tag{3.16}$$

$$SystemStakeholder \sqcap EnvironmentStakeholder \sqsubseteq Stakeholder \tag{3.17}$$

$$Stakeholder \sqsubseteq Agent \sqcap \forall performs.StakeholderAction \tag{3.18}$$

$$ErroneousStakeholderAction \sqsubseteq StakeholderAction \sqcap \forall causes.StakeholderCausedFailure \tag{3.19}$$

$$NonIntentionalStakeholderCausedFailure \sqsubseteq StakeholderCausedFailure \sqcap \forall isLedBy.StakeholderFalseBelief \tag{3.20}$$

$$IllIntentionalStakeholderCausedFailure \sqsubseteq StakeholderCausedFailure \sqcap \forall isLedBy.StakeholderIllIntention \tag{3.21}$$

$$SafetyMeasures \sqsubseteq Action \sqcap \forall hasPart.SubSafetyMeasures \sqcap \exists prevents.Hazard \tag{3.22}$$

$$hasPart \circ hasPart \sqsubseteq hasPart \tag{3.23}$$

$$\top \sqsubseteq \neg \exists hasPart.Self \tag{3.24}$$

$$\top \sqsubseteq \exists (hasPart \sqcap hasPart^{-}).\bot \tag{3.25}$$

Interprétation des axiomes

En tant qu'événement (**Event**), une défaillance (**Failure**) est liée à deux **Situations** différentes comme imposé par les Axiomes (3.1), (3.2) et (3.3). La relation de subsomption

est représentée par le constructeur GCI (*Genral Concept Inculsion*) du fragment $DLP_{\exists}$ ayant la syntaxe d'inclusion ($\sqsubseteq$) entre les concepts (voir figure 3.4). Ainsi, une défaillance transforme l'état d'une réalité en une autre. La situation préalable consiste en **HazardousState** qui active (*activates*) l'existence de la **Disposition** (**Exposure**) qui est manifesté par (*isManifestedBy*) [11] la défaillance. Néanmoins, cette dernière ne se produit pas si la **Disposition Exposure** n'est pas activée.

Dans la post-situation, **Failure** *isTriggered By* **HazardousState** et une transformation de la réalité se produit (*bringsAbout*[12]) en situation **FailureState** dans laquelle le système ne peut pas exécuter ses fonctions prévues. Les Axiomes (3.4) et (3.5) renforcent la fonctionnalité de ces propriétés et respectivement automatisent :

1. une défaillance entraîne (*bringsAbout*) au plus `un` état de défaillance **FailureState**,
2. elle est provoquée par (*isTriggeredBy*) au plus `un` état dangereux **HazardousState**.

La propriété *causes* est déclarée transitive et asymétrique. De ce fait, l'assertion de rôle *bringsAbout*($\mathtt{f}_1$,`fs`) est impliquée si *causes*($\mathtt{f}_1$,$\mathtt{f}_2$) et *bringsAbout*($\mathtt{f}_{2s}$,`fs`) sont le cas pour tout individu $\mathtt{f}_2$. Cette chaîne de rôle est automatiquement générée suite à l'Axiome (3.6). De même, l'assertion de rôle *triggers*$^-$($\mathtt{f}_1$, `hs`) est impliquée si *causes*($\mathtt{f}_1$,$\mathtt{f}_2$) et *triggers*$^-$($\mathtt{f}_2$,`hs`) sont le cas pour tout individu $\mathtt{f}_2$ comme appliqué par l'Axiome (3.7). La fonctionnalité des propriétés *bringsAbout* et *triggers*$^-$ prévient la création d'instances incorrectes de la propriété *causes*. Les restrictions déclarées par les axiomes (3.4) à (3.7) sont définies afin de récupérer et d'interroger sur toutes les défaillances existantes causées par une défaillance (**Failure**) donnée qui *isTriggeredBy* (respectivement *bringsAbout*) un **HazardousState** donné (respectivement un **FailureState**). La propriété *isTriggeredBy* est définie comme l'inverse de *triggers* par l'Axiome (3.8).

Le concept **Failure** *subsumes* deux sous-types différents : **StakeholderCausedFailure** et **FaultEmergenceFailure**. Le premier *est une* défaillance qui *est causé par* (l'inverse de *causes*) **ErroneousStakeholderAction** comme déclaré par l'Axiome (3.9). Le deuxième *est une* défaillance qui est la manifestation de (*isManifestionOf*) **Fault** et *n'est pas causé par* les **ErroneousStakeholderAction**, comme défini par l'Axiome (3.10).

Une exposition (**Exposure**) *est une* **Disposition** qui dépend de manière existentielle (*inheresIn*) aux équipements système (**SystemEquipment**) et aux objets d'environnement (**EnvironmentObject**) appliqués par l'Axiome (3.11). **SystemEquipment** et **EnvironmentObject** sont des **Object** comme indiqué par l'Axiome (3.11). Le concept **Exposure** *subsumes* deux sous-concepts **Defect** et **HazardousUsage** à partir des Axiomes (3.12) et (3.13).

À partir des Axiomes (3.11) et (3.13), un **Defect** *est un sous-type d'***Exposure** qui est inhérente à (*inheresIn*) **Object**. Quand il est manifesté par (*isManifestedBy*) (l'inverse de

11. cette propriété est déclarée comme l'inverse de *isManifestationOf*
12. son inverse est *bringsAbout*$^-$

isManifestationOf) une **FaultEmergenceFailure**, une **Fault** *est un* **Defect**. En imposant la transitivité de la relation de subsomption, une **Fault** *est une* **Disposition** qui est manifestée par (*isManifestedBy*) **Failure** .

En s'appuyant sur les Axiomes (3.14) à (3.16), une **Fault** *subsumes* deux types distincts : **SystemEquipmentFault** et **EnvironmentObjectFault**. En tant que **Disposition**, **Fault** est une propriété de **Object** qui est activée par (*isActivatedBy*) (l'inverse de *activates*) une situation particulière (**HazardousState**).

Par ailleurs, **HazardousUsage** *est un sous-type d'***Exposure** qui dépend existentiellement (*inheresIn*) de **Object** à partir des Axiomes (3.11) et (3.13). Il désigne le cas dans lequel il est manifesté par (*isManifestedBy*) **StakeholderCausedFailure**, comme appliqué par l'Axiome (3.9). En s'appuyant sur les hypothèses de monde fermé (CWA) du domaine d'application, un **Stakeholder** *subsumes* deux sous-types : **SystemStakeholder** et **EnvironmentStakeholder** comme indiqué par l'Axiome (4.17). Un **Stakeholder** effectue une action erronée (**ErroneousStakeholderAction**) qui *cause* **StakeholderCausedFailure**, tel qu'appliqué par les Axiomes (3.18) et (3.19).

D'autre part, **StakeholderCausedFailure** *subsumes* deux sous-types : **NonIntentionalStakeholderCausedFailure** et **IllIntentionalStakeholderCausedFailure**. La première est menée par (*isLedBy*) **StakeholderFalseBelief** comme appliqué par l'Axiome (3.20). La deuxième est menée par (*isLedBy*) **StakeholderIllIntention** comme déclaré par l'Axiome (3.21).

Ensuite, l'exposition (**Exposure**) est inhérente à (*inheresIn*) un danger (**Hazard**), qui est une **Situation** comme déclaré par l'Axiome (3.11). Afin de contribuer à l'aide à la décision en matière de sécurité et garder la traces de ces informations, les mesures de sécurité (**SafetyMeasures**) sont des **Actions** prises en compte pour prévenir (*prevents*) un danger (**Hazard**) comme indiqué par l'Axiome (3.22). Elles sont *composées* de sous-mesures de sécurité (**SubSafetyMeasures**) comme indiqué dans la Définition 5. La relation de composition est définie par la propriété *hasPart* (part/whole). Cette relation fondamentale est transitive (3.23), irréflexive (3.24) et anti-symétrique (3.25). Ces déclarations permettent de contraindre la création des instances ainsi que l'extraction des données et la création de nouvelles classes par les règles d'inférence.

3.4.5 Implémentation de DAO

Le pattern de DAO est implémenté à l'aide de Protégé 5.2.0 [13], qui est l'un des outils open-source les plus populaires pour le développement d'ontologies grâce à ses capacités en termes de création, modification et interrogation d'ontologies. Les résultats de l'implémentation de DAO en termes de la hiérarchie des classes, les ≪ object properties ≫ sont respectivement représentés par les figure 3.7, 3.8. Toutes les classes sont

13. http ://protégé.stanford.edu

déclarées disjointes, mais ces restrictions ne sont pas spécifiées dans cette section afin d'améliorer la lisibilité. La disjonction n'est pas seulement une bonne pratique dans la formalisation OWL, mais aussi une condition nécessaire pour que le pattern de DAO soit exprimé en $DLP_{\exists}$.

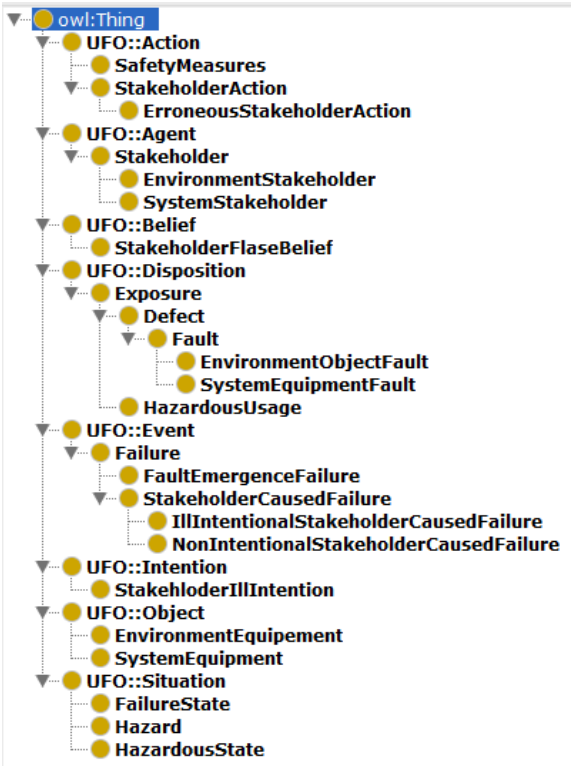

Figure 3.7 – Hiérarchie des classes de DAO sur Protégé

Figure 3.8 – Les propriétés de type ObjectProperty de DAO sur Protégé

Toutes les cardinalités et les restrictions du domaine/co-domaine, comme indiqué dans le modèle conceptuel, sont appliquées dans l'implémentation OWL. Les restrictions du domaine/co-domaine doivent être prises en compte explicitement afin de combler les lacunes de certains scénarios réels. Les Axiomes (3.26) et (3.27) sont inclus à titre d'exemple

afin de montrer comment appliquer ces restrictions, où **HazardousUsage** est le *co-domaine* et **StakeholderCausedFailure** est le *domaine*. Les Axiomes d'application du domaine/co-domaine pour les autres classes et propriétés sont spécifiés de la même manière. Le résultat de cet exemple de restrictions sur Protégé est illustré par la figure 3.9.

$$\exists isManifestationOf.HazardousUsage \sqsubseteq StakeholderCausedFailure \tag{3.26}$$

$$\exists isManifestationOf^{-}.StakeholderCausedFailure \sqsubseteq HazardousUsage \tag{3.27}$$

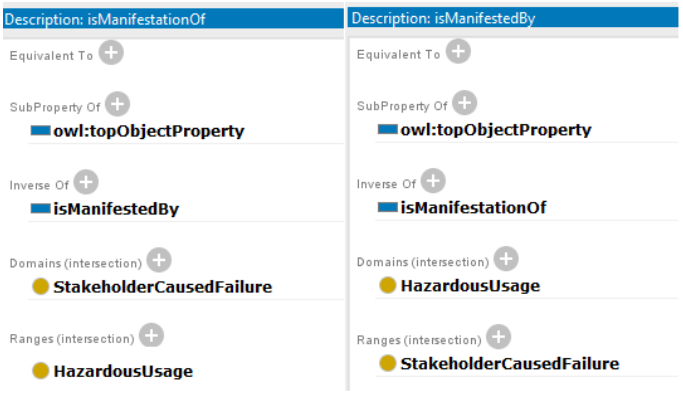

Figure 3.9 – Restrictions du domaine/co-domaine sur Protégé

Un exemple d'instances (« individuals » représentées par des losanges violets) pour la classe **FaultEmergence Failure** est illustré par la figure 3.10. L'instance SwitchSystem-Failure est un type de **FaultEmergence Failure** et est liée aux autres instances par les propriétés représentés par des rectangles bleus. Les instances sont déclarés différentes afin de s'affranchir du problème de l'absence d'hypothèse du nom unique .

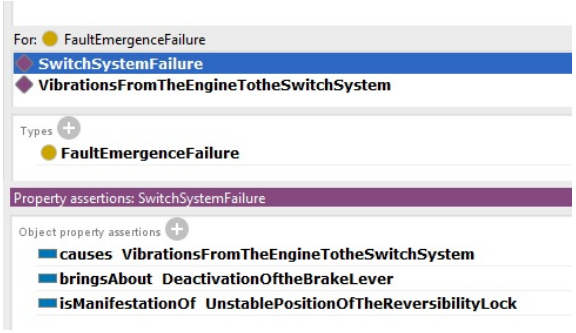

Figure 3.10 – Exemple d'instances de la classe FaultEmergenceFailure sur Protégé

Un exemple d'axiomes de DAO pour contraindre les classes et les propriétés est illustré par la figure 3.11 grâce à la définition logique fournis par les constructeurs OWL équivalents aux constructeurs DL.

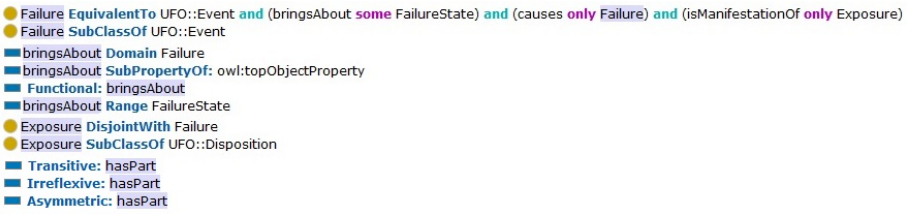

Figure 3.11 – Exemple d'axiomes logiques issus de DAO sur Protégé

3.4.6 Évaluation de DAO

Le processus d'évaluation de l'ontologie DAO est effectuée à l'aide des méthodes de vérification et de validation proposées par SABiO et guidées par les QC définies en phase préliminaire du développement. Ce processus permet une vérification et validation dynamique du comportement de DAO en termes de sa **compétence** vis-à-vis de ses exigences attendues (QC) et de sa **flexibilité** à l'égard d'un ensemble de scénarios de test. Pour la vérification, la table de gestion des concepts et relations est établie afin de vérifier la capacité de l'ontologie à répondre aux questions de compétence (QC). Ensuite, l'aspect validation sera assuré par l'instanciation de l'ontologie DAO dans la section 3.5 afin d'illustrer des situations réelles de scénarios d'accidents ferroviaires. Le tableau 3.3 illustre les résultats de la vérification de DAO à l'égard de ses QC.

QC	Concepts et Relations
QC1	A **Failure** is a *subtype of* **Event**. It *brings about* a **Failure State** and a **Hazardous State** *triggers* a **Failure**. As an **Event**, a **Failure** *causes* an other **Failure** (cascading failure).
QC2	A **Hazardous State**, as a *subtype of* **Situation**, *triggers* a **Failure** and *activates* an **Exposure**, which is a *subtype of* a **Disposition**. This **Exposure** *inheres in* a **Hazard** and is manifested by a **Failure**. This **Exposure** *subsumes* a **Hazardous Usage** and a **Defect**.
QC3	A **Failure State** is *a subtype of* **Situation** and is *brought by* a **Failure**.
QC4	A **Safety Measure** is a *subtype of* **Action**. It *is composed into* sub-safety measures and it *prevents* **Hazard**.
QC5	A **Stakeholder-caused failure**, as a *subtype of* **Failure**, is a *manifestation of* a **Hazardous Usage** and is *caused by* an **Erroneous Stakeholder Action**. This failure *is classified into* **Non-intentional** and **ill-Intentional** that are respectively *lead by* **Stakeholder False Beliefs** and **Stakeholder ill-intentions**. A **Fault emergence Failure**, as a *subtype of* **Failure**, is a *manifestation of* a **Fault**. As a *subtype of* **Defect**, a **Fault** can be a **System Equipment Fault** and an **Environment Object Fault**.

Tableau 3.3 – Table de vérification de DAO : QC et leurs réponses par DAO

Ce tableau peut servir comme un outil de gestion de l'ontologie ou comme support de traçabilité afin de faire face aux extensions apportées à l'ontologie et satisfaire les besoins d'autres domaines. Par ailleurs, l'ontologie proposée fournit un ensemble complet de concepts et de relations non ambigus qui répondent à l'objectif de l'ontologie DAO. En outre, l'expressivité et la clarté sont considérées comme des critères pertinents dans l'étape de vérification. Ils montrent comment l'ontologie communique objectivement le sens de sa taxinomie et comment celle-ci est exprimée avec des langages très expressifs dans chaque phase de son processus de développement. DAO est fondée sur l'ontologie de haut niveau UFO afin de fournir une sémantique du monde réel ; et représentée en utilisant le langage bien fondé OntoUML, ce qui augmente ses qualités syntaxique et sémantique. La formalisation OWL augmente sa qualité pragmatique, sa formalisation et sa ré-utilisabilité pour d'autres domaines critiques comme le domaine avionique. Ainsi, l'implémentation OWL permet de répondre aux requêtes d'extraction des données et de vérification de la cohérence. Enfin, les résultats de la vérification montrent que l'ontologie proposée remplit toutes les QC soulevées et couvre tous les aspects prévus du domaine d'analyse dysfonctionnelle. Afin de garder le même vocabulaire et faciliter le partage des connaissances, nous présentons les réponses aux QC en anglais. Comme le montre la figure 3.12, le raisonneur Pellet a été utilisé pour vérifier la cohérence (≪ consistance ≫) et créer la hiérarchie inférée de l'ontologie.

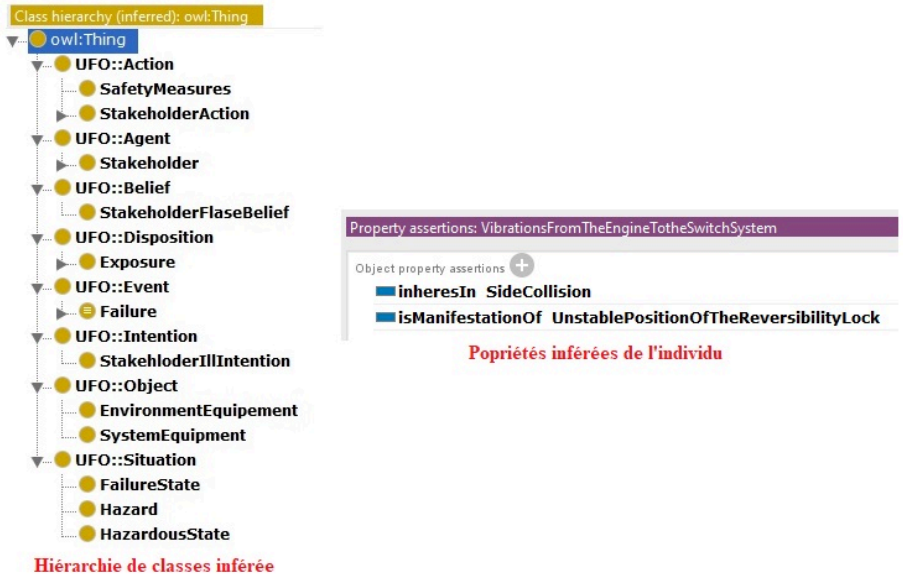

Figure 3.12 – Hiérarchie des classes de DAO inférée sur Protégé

3.5 Validation de DAO par des cas d'étude ferroviaires

Une ontologie de domaine doit valider son critère d'adaptabilité pour représenter plusieurs situations réelles, annoter différents types de données et faciliter le processus de prise

de décisions dans une tâche spécifique. Pour la validation de l'ontologie et afin d'illustrer leur analyse dysfonctionnelle par DAO, nous nous référons à deux scénarios d'accidents ferroviaires, celui de Longueville [14] et celui de Saint-Romain-En-Gier [15].

3.5.1 Scénario d'accident ferroviaire de Longueville

L'accident ferroviaire survenu à Longueville (France) le 16 février 2005, consistait en une prise en écharpe (collision latérale) entre deux trains de voyageurs lorsque le train 117710 en provenance de Provins (Seine-Marne) a percuté longitudinalement le train 117578 dans la gare de Longueville (Seine-et-Marne). En effet, le train 117578 en direction de Paris est parti à l'heure prévue et cisaillait les voies A et 1 avant d'emprunter la voie 2 côté Paris. Ce dernier s'est arrêté, après un signal d'alarme tiré par un voyageur, et se trouve avec sa voiture pilote sur la traversée jonction double (TJD) n°155/156. Comme le montre la figure 3.13, cette TJD donne accès d'un côté à la voie unique de Provins et aux voies 1 et 2 côté Paris, de l'autre aux voies A et B. La partie du quai desservant les voies A et 1 se situe au niveau de cette TJD.

Le train 117710 en provenance de Provins à l'heure prévue ne pouvant pas arriver à la gare de Longueville (suite à l'arrêt de l'autre train), devait donc s'arrêter au signal carré 163 maintenu en position de fermeture. Néanmoins, ce train a franchi le signal fermé suite à une absence de freinage et a pris en écharpe le train arrêté 117578. La collision latérale s'est effectuée à une vitesse de l'ordre de 20km/h au niveau de l'extrémité arrière de la voiture de tête du train tamponné 117578.

Selon le rapport du BEA-TT [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005], il n'y avait pas de pertes humaines mais plutôt des dommages matériels subis. Les dégâts principaux sont résumés comme suit :

— la voiture de tête de la rame tamponnée a été éventrée sur environ 5 mètres,
— la locomotive de la rame tamponneuse a eu quelques dommages dans son châssis,
— la voie a été déformée au niveau de la TJD 155/156 et le quai a été heurté et déplacé latéralement provoquant l'engagement du gabarit de la voie 1.

Les deux trains sont constitués de rames réversibles où une cabine de conduite est disposée à chaque extrémité. Le principe de réversibilité est détaillé dans la section 3.5.3.3 du rapport [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005]. L'absence du freinage au niveau du train 117710 est due à une protection mécanique insuffisante de la poignée de la serrure de réversibilité. La serrure de réversibilité dénommée Interrupteur général ZG est un organe permettant de configurer la locomotive au plan du freinage en situation de « menante » du train, ou en situation de menée (si la conduite du train s'effectue depuis la cabine de réversibilité de la voiture pilote). La locomotive est aussi en situation de « menée » lorsqu'elle entre dans la composition d'une unité multiple

14. http ://www.bea-tt.developpement-durable.gouv.fr/resume-du-rapport-final-a51.html
15. http ://www.bea-tt.developpement-durable.gouv.fr/resume-du-rapport-final-a2.html

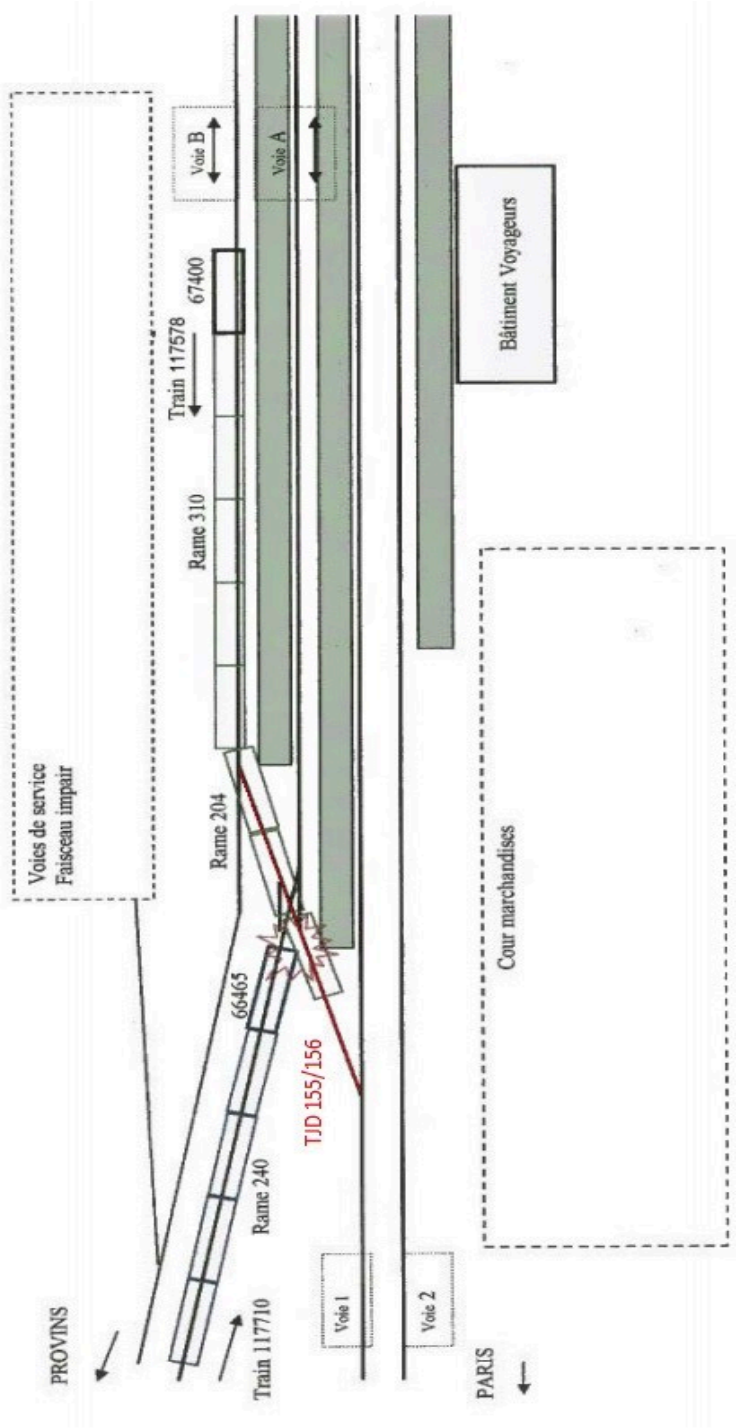

Figure 3.13 – Plan de voie de l'accident de Longueville [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005]

avec une autre locomotive du même type pour tirer un train lourd. Dans ce scénario, cet interrupteur général est un organe mécanique [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005].

Le système mécanique de réversibilité de la locomotive, qui active la commande du

frein, n'a pas été bloqué en position locomotive « menante » et s'est trouvé dans un état instable entre les positions « menante » et « menée ». Les vibrations subies par l'engin moteur transmises au système de réversibilité ont provoqué la déconnexion de la commande du frein. Par conséquent, la commande normale du frein de la cabine de la locomotive est désormais inefficace. La relation entre la position de la serrure de réversibilité et l'engin moteur est expliquée dans l'annexe A.

Toutefois, le conducteur n'a pas mis en œuvre les moyens de freinage d'urgence à sa disposition ; même quand il s'est rendu compte qu'il était en dérive. Le conducteur de ce train 117710 s'est servi du frein à main de la locomotive qui agissait sur un seul essieu au lieu de quatre. Cette manœuvre est, en conséquence, insuffisante pour arrêter le train immédiatement avant les aiguilles d'entrée de la gare de Longueville où se trouve immobilisé le train 117578. Dans ce scénario, il clair que ce conducteur ne maîtrisait pas les gestes du métier en situation d'urgence ; ce qui a été confirmé par l'enquête menée par le BEA-TT.

À partir des éléments présentés dans ce scénario, l'accident est dû à deux facteurs principaux :

— la défaillance du système de réversibilité due à une faute de la serrure de réversibilité non verrouillée à la position opérationnelle « menante ». Les vibrations de l'engin transmises au système de réversibilité ont provoqué l'inhibition de la commande de frein.

— La réalisation d'actions erronées par le conducteur du train 117710 :

1. deux actions lors de son départ de Provins qui consiste à la non réalisation de l'essai réglementaire de frein [16] et à la vérification statique de la VACMA [17] alors qu'un essai en marche aurait été nécessaire.

2. des gestes inappropriés lors de la constatation de l'état de dérive du train. Dans le cas présent, plusieurs manipulations de secours auraient permis de provoquer l'arrêt du train avant le point protégé, qu'elles soient mises en œuvre séparément ou simultanément comme l'ouverture du robinet d'urgence, utilisation du frein direct de la locomotive, etc. En effet, le conducteur s'est aperçu qu'il était en dérive lors de son arrêt commercial manqué à Sainte-Colombe et n'a utilisé que le frein à main pour arrêter son train. Il a omis les gestes du métier préconisés par le référentiel « conducteur de ligne » applicable. Une deuxième omission a eu lieu quand il a aperçu le train 117578 en arrêt à l'entrée de la gare de

16. Le référentiel de conduite TT 0 513 indique que lors d'un changement de poste de conduite, le conducteur doit effectuer un essai de serrage et de desserrage pour s'assurer que la commande du frein est effective pour piloter la pression CG.

17. VACMA : « veille automatique avec contrôle du maintien d'appui » : système de sécurité à bord de l'engin moteur surveillant l'état d'activité normale du conducteur. Sur le réseau ferré national, si le non maintien par le conducteur des appuis VACMA excède 5 secondes, un signal sonore retentit, suivi quelques secondes après d'un déclenchement du freinage d'urgence si aucun appui n'est repris.

Longueville.

3. Avant d'arriver à la gare de Longueville, le conducteur du même train 117710 a franchi un signal d'avertissement fermé et a acquitté le franchissement. Il a tenté d'arrêter son train en serrant le frein à main seul, sauf qu'il a agit sur un seul essieu de la locomotive. Ensuite, il a franchi le tableau indicateur de vitesse 30 et du carré 163 fermé en acquittant ces deux signaux. Dans ce cas, le non acquittement aurait déclenché le serrage d'urgence avant d'arriver à l'obstacle. En effet, ≪ *l'acquittement d'un signal carré ne se fait que lors du franchissement sur ordre de l'agent circulation de ce signal carré ; le franchissement d'un signal carré est un acte grave, l'acquittement au franchissement de ce signal sans ordre de l'agent de circulation, est aberrant* ≫ [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005].

— la situation ≪ attentiste ≫ de l'agent du train 117710 d'un avertissement de sifflet de détresse de la part du conducteur. En effet, cet agent a déclaré qu'il n'imaginait pas la situation critique du conducteur et il n'a pas pu déclencher un signal d'alarme arrêtant le train, en cette absence d'instruction. D'autre part, la rame n'a pas été équipée d'une interphonie pour établir la communication avec le conducteur. Ainsi, il n'a pas été en mesure de décider de lui-même d'arrêter le train en tirant le signal d'alarme, surtout que cette disposition ne fait pas partie de la réglementation de la société exploitante de la ligne Longueville-Provins.

Après la description du scénario et la contextualisation de ces circonstances, nous procédons à l'instanciation de l'ontologie DAO à la lumière des facteurs principaux de l'accident. L'accident de Longueville est la combinaison de plusieurs événements qui se sont enchaînés pour engendrer la prise en écharpe. Afin d'assurer la clarté de l'instanciation, nous avons choisi deux facteurs de l'accident pour valider la capacité de DAO à représenter la combinaison des différentes situations à la fois. Les figures 3.14 et 3.15 montrent respectivement les graphes RDF des deux principaux facteurs liés à l'occurrence du scénario d'accident en utilisant le patron DAO. Ces notations graphiques, sont générées sous forme de graphes, sont utilisées pour visualiser l'instanciation de l'ontologie proposée et l'intégration de différents types d'ensembles de données avec le modèle de conception de DAO. Les rectangles représentent les individus (instances) et les cercles représentent les classes de DAO.

Le premier facteur est la défaillance du système de réversibilité qui est un sous-type de (*rdf :type*) **Fault emergence Failure**. Elle est une manifestation (*isManifestationOf*) d'une faute de l'équipement du système (**System Equipment Fault**). Cette dernière se matérialise par la position instable de la serrure de réversibilité qui permet de commuter les locomotives et d'activer la commande de frein qui est inhérente (*inheres in*) au danger de prise en écharpe. En effet, le non verrouillage de la position opérationnelle de la serrure qui n'était pas bloquée dans la position menante de la locomotive représente l'état dangereux

(**Hazardous State**). Par conséquent, les vibrations de l'engin transmises au système de réversibilité, qui est une défaillance en cascade (par la relation *causes*), inhibe la commande de frein (**Failure State**). Ce graphe RDF est illustré par la figure 3.14.

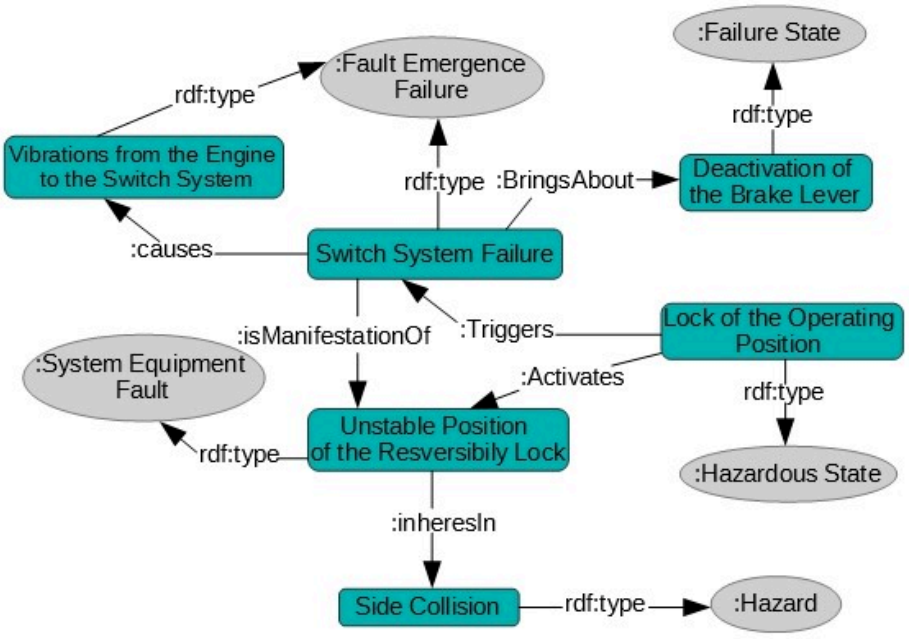

Figure 3.14 – Graphe RDF d'une défaillance technique liée à l'occurrence de l'accident de Longueville

La deuxième erreur humaine qui contribue d'une façon majeure dans la survenue de l'accident est la non application des gestes du métier réglementés par les référentiels applicables. Le manquement principal du mode opératoire mis en œuvre par le conducteur est la non maîtrise des réactions appropriées aux situations d'urgence. En effet, le conducteur n'a pas déclenché l'arrêt d'urgence et n'a pas utilisé le frein direct de locomotive. Il s'est concentré sur le frein à main pour faire un arrêt effectif du train, mais le frein n'a agi que sur un seul essieu. Nous avons choisi de nous focaliser sur cette erreur car elle a été commise deux fois : une première fois quand il a détecté la dérive et a manqué l'arrêt de Sainte-Colombe et une autre fois quand il a franchi le signal d'entrée fermé de la gare de Longueville.

D'après le compte rendu final de la chaîne des événements élaboré par le BEA-TT (Section 4.1.3 du rapport), la première erreur correspond au concept **Non-intentional Stakeholder Caused Failure** qui est menée par (*is Led By*) **Stakeholder False Belief**, les deux introduits par DAO. En effet, il s'agit d'une erreur du schéma mental lors de l'exécution de l'action comme constaté à partir de ses déclarations extraites du même rapport : « *sa représentation mentale a pu être la suivante : « je n'ai pas réalisé d'essai formel du frein avant le départ- en l'occurrence, pas d'essai de serrage, je n'ai plus de frein = je n'ai plus d'air » d'où la réaction de ne s'occuper que du frein à main* ». Le **False**

Belief est basé sur des hypothèses qu'il a crues être vraies, alors que ce n'est pas le cas. Ce concept correspond aussi à la situation « attentiste » de l'agent du train qui avait de fausses hypothèses concernant la situation du conducteur et l'arrêt du train. De ce fait, l'interprétation de l'aspect cognitif de l'activité humaine aurait empêché l'occurrence de cet accident en prenant des mesures préventives au niveau de la formation au métier de conducteur ou le contrôle des procédures de sécurité.

La deuxième erreur, que nous avons choisi de modéliser dans la figure 3.15, est l'erreur de perception liée à un plan inadéquat à l'accomplissement de l'objectif prévu qui est l'arrêt du train dans ce scénario. Cette erreur correspond au concept DAO **ill-intentional Stakeholder Caused Failure** qui est menée par (*is Led By*) **Stakeholder ill-intention**. Elle représente l'incapacité du conducteur à arrêter le train et *est causée par* l'utilisation du frein à main seul au lieu de l'arrêt d'urgence (**Errouneous Stakeholder Action**). Par conséquent, le frein à main agissait sur un seul essieu (au lieu de quatre), ce qui rendait impossible le non franchissement du signal fermé et l'arrêt du train avant l'aiguillage où le train 117578 était immobilisé. L'enchaînement de ces événements a donné lieu à la prise en écharpe entre les deux trains.

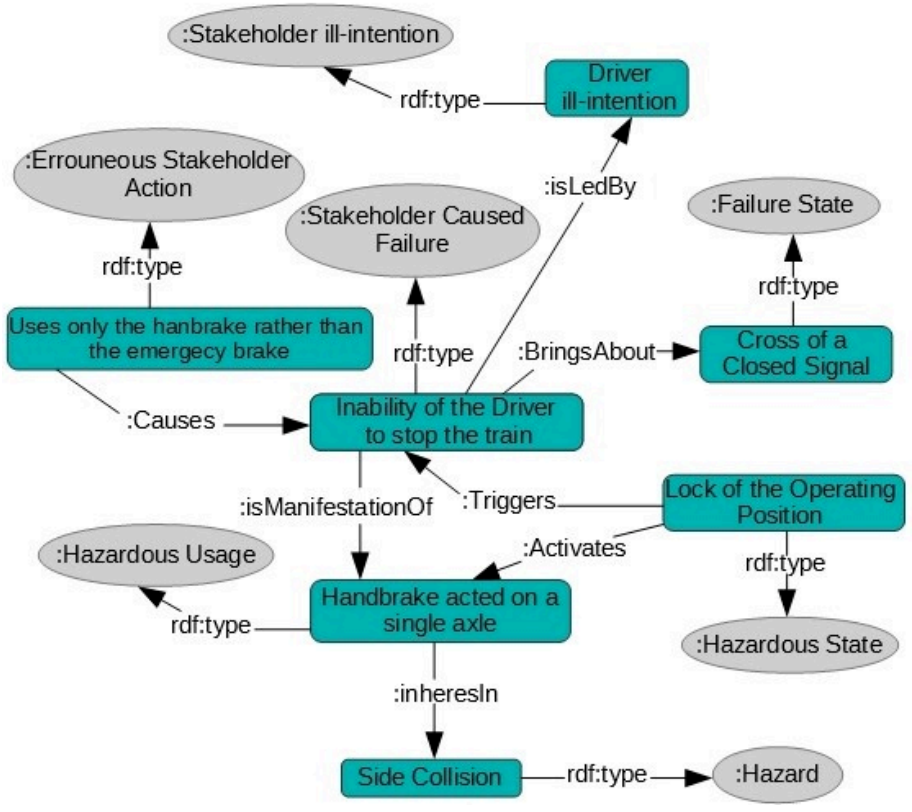

Figure 3.15 – Graphe RDF d'une erreur humaine du conducteur liée à l'occurrence de l'accident de Longueville

Ce scénario d'accident est considéré afin de valider l'adaptabilité de l'ontologie proposée et justifier la flexibilité de la taxonomie associée ainsi que sa capacité de représenter des situations critiques. Ensuite, l'ensemble complet des concepts proposés et les relations cohérentes entre elles montrent que le modèle conceptuel de DAO peut couvrir et analyser la coexistence des facteurs techniques et humains à l'origine de l'accident. En effet, nous pensons que la mise en œuvre de l'ontologie DAO dès les premières phases de conception des systèmes ferroviaires constitue un formalisme efficace pour faire face aux dangers potentiels. L'aspect technique en combinaison avec le facteur humain et la modélisation conceptuelle de l'origine de la défaillance et l'erreur humaine contribue à la gestion de décisions de sécurité au sein de l'organisation. Cet aspect sera traité dans le chapitre 4 pour assurer la continuité du processus de conception en parallèle avec la gestion de la sécurité des SCS.

Afin de justifier la validité de l'ontologie DAO pour au moins deux situations différentes, nous considérons le scénario d'accident de Sait-Romain-En-Gier, décrit et illustré dans la section suivante.

3.5.2 Scénario d'accident ferroviaire de Saint-Romain-En-Gier

Le scénario d'accident de Saint-Romain-En-Gier est une collision frontale (nez à nez) qui a eu lieu le 5 avril 2004 entre un train à grande vitesse (TGV) vide et un train de travaux (TTX) sur la ligne entre Lyon et Saint-Étienne [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004]. Cette collision survenue au km 532.730 sur la voie 2 vers Saint-Étienne où une rame TGV-Duplex (Train n° 740010) a heurté un TTX. Les dommages de cet accident représentent un bilan humain de deux conducteurs du TGV et du TTX blessés ainsi que des dégâts matériels importants au niveau des engins moteurs de la rame TGV ayant le châssis faussé et les anneaux d'intercirculation déformés, et du locotracteur placé en tête du TTX ayant des déformations.

Les circonstances de cet accident correspondent à la combinaison de diverses situations qui se sont déroulées comme suit :

— La présence des TTX pour des travaux sur l'infrastructure dans la zone Rive de Gier/Givors sur les voies 1 et 2 comme le montre la figure 3.16. Les travaux ont été programmés pour la nuit du 4 au 5 avril où deux TTX (un train de terre et un train de longs rails soudés) ont été engagés sur la voie 1, et les deux autres TTX (un train de ballast et une bourreuse) sur la voie 2. Lors de la mise en œuvre du chantier sur la voie 2, la panne d'engin moteur d'un TTX a provoqué un retard au niveau du planning horaire prévu. Par conséquent, les voies 1 et 2 ont été interceptées par des demandes d'interception de voie (DIV) jusqu'au matin du 5 avril. La DIV est définie comme « une procédure permettant au service chargé de la maintenance de l'infrastructure d'effectuer des travaux sur une portion de ligne ou de voie, dépendant de deux agents de circulation, avec la garantie qu'il n'y aura pas

de circulation commerciale pendant une période de temps déterminée » [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004].

— À sa prise de service le 5 avril au matin, l'agent de circulation de Givors-ville restitue la DIV déposée de la voie 1. Contrairement à la DIV déposée sur la voie 2, elle s'étend de Rive de Gier à Givors le jour de l'accident, à la place de couvrir habituellement Rives de Gier à Trèves Bruel. L'agent de circulation n'a pas été informé de ce changement et avait la représentation mentale que la voie est exploitée normalement de Givors à Trèves Burel, et que la zone interceptée par les travaux se situe au delà.

— Le PC (Poste de commandement) de Lyon annonce une première circulation commerciale se dirigeant de Lyon vers Saint-Étienne. L'agent de circulation établit l'itinéraire permettant d'engager ce TGV par son itinéraire normal voie 2 vers Rive de Gier, puis Saint-Étienne.

— Ayant fini les travaux organisés, le TTX ballast quitte les lieux en se dirigeant vers Givors. À l'approche de la gare de Trèves-Burel, le TTX s'apprête à quitter le premier pas de l'installation permanente de contre sens (IPCS) [18] pour s'engager sur le deuxième pas comme indiqué dans la figure 3.16. Ainsi, il rencontre le signal carré fermé et il l'a franchi alors qu'il n'a pas été autorisé à le faire. Le conducteur du TTX poursuit son trajet à contre sens voie 2 jusqu'à franchir un autre signal éteint qui n'est pas mentionné franchissable dans le bulletin à sa disposition pour gérer sa circulation jusqu'à sa sortie de la zone interceptée. Ce signal était éteint car l'agent de circulation permettait le passage d'un train commercial dans le sens opposée au sien. En arrivant à proximité d'un passage à niveau, les barrières ont été baissées et le conducteur du TTX pensait que c'est lui qui a déclenché l'annonce alors qu'en réalité c'est le TGV progressant dans le sens normal de la voie 2 qui l'avait déclenché. Quelques mètres après le passage à niveaux, le train de travaux entre en collision frontale à une vitesse d'environ 20km/h avec le TGV arrivant en face.

À la différence de l'accident de Longueville, le présent scénario d'accident est dû à la combinaison des facteurs humains et organisationnels. Nous pouvons constater que chacun des acteurs a contribué à l'occurrence de la collision nez à nez. Tout d'abord, le site n'a pas été protégé par l'agent de sécurité afin d'empêcher la circulation des trains dans cette zone. Ensuite, l'agent de circulation du matin qui a établi l'itinéraire du TGV en forçant le dispositif d'attention [19]. Il n'a pas remarqué les incohérences de la présence du dispositif

18. Les IPCS sont des installations se substituent aux procédures spéciales et empêchent les situations interdites telles que deux circulations ferroviaires de sens contraire sur la même voie. Le pas d'IPCS est une section de ligne équipée d'IPCS dont chacune des deux voies est exploitable dans les deux sens ; il est normalement encadré par des aiguilles de communication reliant les deux voies et permettant aux trains de changer de voie.

19. Dans les postes d'aiguillages, ce dispositif se place sur les organes de commande d'itinéraire de façon

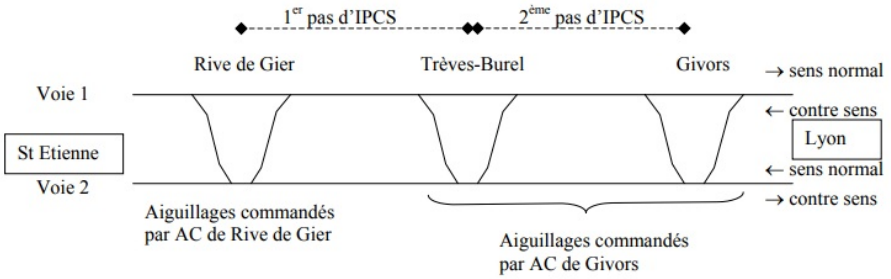

Figure 3.16 – Représentation de l'infrastructure de la ligne Lyon/Saint-Etienne [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004]

d'attention pour le pas d'IPCS Trèves-Burel/Givors, qui est en principe contradictoire avec l'absence de mention d'une DIV couvrant ce pas d'IPCS sur l'état de circulation et sur le carnet de dépêches. Cette contradiction apparente aurait dû conduire l'agent circulation à en rechercher la raison, et à se reporter aux DIV en cours et à la consigne d'exploitation temporaire. Mais cette contradiction apparente n'est pas prise en charge par l'agent circulation, qui voit peut-être dans les DA en place un simple oubli de retrait par son collègue de nuit. Par ailleurs, la remise du service entre les deux agents de circulation en pleine nuit et lors d'intempéries n'est probablement pas le contexte le plus favorable à la transmission d'information critiques.

D'autre part, le conducteur du TTX franchi deux fois un signal éteint et il ne s'est pas rendu compte qu'il était à contre sens de circulation. L'agent d'accompagnement du TTX n'avait pas non plus une vision claire du fonctionnement d'IPCS ainsi que du sens de circulation et n'a pas remarqué que les signaux franchis sont non autorisés. Selon le rapport [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004], il n'avait pas pris connaissance des installations au-delà de Trèves-Burel, situées en dehors des limites de son établissement ; il ne raisonnait pas en fonction de l'existence de deux pas d'IPCS mais semblait penser qu'il n'y en avait qu'un seul de Rive de Gier à Givors. Par conséquent, le « sens secours » mentionné sur son aide mémoire et qu'il avait demandé à l'agent circulation de Rive de Gier suffisait pour lui.

Le conducteur du TTX pensait être protégé par la DIV et il s'agit d'une erreur du schéma mental. Le franchissement d'un signal fermé correspond, en effet, au concept **Non-intentional Stakeholder Caused Failure** qui est menée par (*is Led By*) **Stakeholder False Belief**. Nous avons choisi de modéliser cette erreur car elle a fait l'objet de plusieurs modifications des référentiels pour la gestion de la circulation des trains de travaux et le sens de circulation. La figure 3.17 représente le graphe RDF de ce facteur contribuant à l'occurrence de cet accident. En effet, la relation de causalité des événements/situations ainsi que l'activation de l'exposition au danger (**Hazardous Usage**) qui représente le mouvement du TGV dans le sens normal de la voie n'ont pas pu empêcher la survenue de

à rappeler que leur utilisation ne doit se faire que sous certaines conditions bien particulières.

la collision frontale.

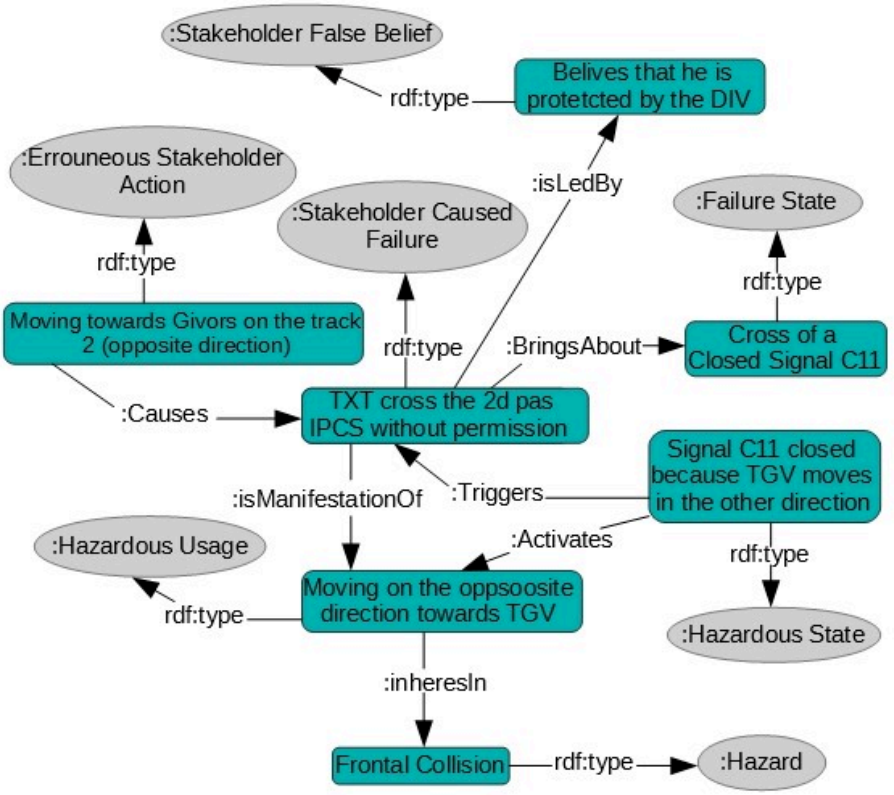

Figure 3.17 – Graphe RDF de l'erreur de conducteur du TXT par DAO

Les facteurs organisationnels consistent en la gestion inefficace de la circulation des trains de travaux et du sens inverse, l'absence de la mise en application des règles de délimitations du chantier, ainsi que l'absence de la mise à disposition aux agents d'accompagnement des documents de signalisation de la section de ligne dans laquelle ils opèrent. Ces facteurs ont sollicité l'attention des organisations pour renforcer les conditions d'élaboration et de contrôle et établir des documents de référence pour la gestion des travaux entre les établissements. Ceci permet d'assurer l'interopérabilité des infrastructures ainsi que la prise de connaissance de tous les éléments nécessaires pour accomplir la mission dans les bonnes conditions. Cet aspect organisationnel sera traité dans le chapitre 4.

L'accident de Saint-Romain-En-Gier a été considéré afin de valider l'importance de la modélisation conceptuelle cognitive du facteur humain dans l'analyse dysfonctionnelle des SCS. En effet, les concepts et les relations de DAO justifient leur flexibilité pour représenter diverses situations sans modifications nécessaires. Ceci augmente la validité de l'ontologie proposée et assure sa réutilisation pour d'autres situations critiques et son extension pour d'autres SCS.

Afin de tester la recherche des données avec des requêtes SPARQL sur les graphes RDF

fournis, la figure 3.18 illustre un simple exemple de requête SPARQL testée sur DAO ainsi que les résultats obtenus.

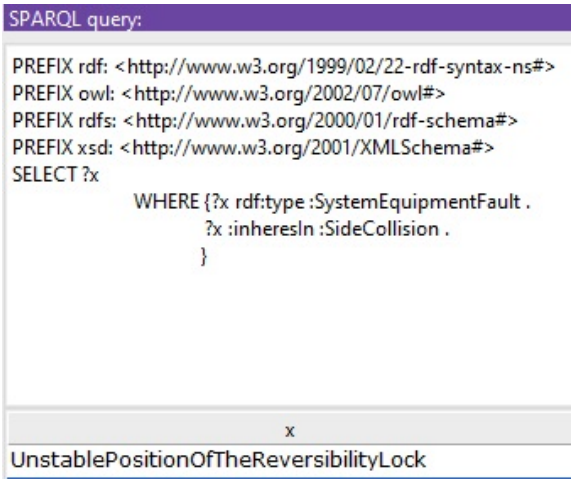

Figure 3.18 – Exemple d'une requête SPARQL et son résultat pour la recherche d'un individu

3.6 Discussion

DAO fournit une conceptualisation du type de défaillance, de ses causes, ses effets et du danger associé. Cette analyse conceptuelle est basée sur l'utilisation des concepts fondamentaux UFO et des relations entre eux ainsi que les définitions proposées par les standards des domaines. Ensuite, l'ontologie proposée clarifie l'utilisation ambiguë du terme « défaillance » et de ses concepts associés dans la terminologie des SCS. En outre, trois aspects d'analyse dysfonctionnelle sont pris en compte dans la conceptualisation des connaissances :

1. Les défaillances des composants des équipements du système et d'environnement et leur cascade par la relation de causalité,
2. Les erreurs humaines causées par les acteurs du système et de l'environnement et le type du moment mental définissant l'origine des erreurs humaines,
3. La situation qui cause la défaillance et celle qui est en conséquence de cette défaillance.

Par ailleurs, la conceptualisation est basée sur l'interopérabilité des méthodes d'analyse dysfonctionnelle existantes. La vue interopérable fournie par DAO permet d'avoir une ontologie extensible et réutilisable puisque sa formalisation dépasse le cadre typique de concepts et de relations simples. L'interprétation sémantique du monde réel et la conceptualisation dirigée par UFO permet l'intégration des connaissances en fonction des besoins spécifiques du domaine d'application. De plus, DAO peut être utilisée pour annoter et récupérer des données en fonction de la granularité requise du domaine d'application.

Dans la phase de son évaluation, DAO satisfait ses exigences attendues et assure l'analyse ontologique et la clarification conceptuelle de situations critiques du monde réel, grâce à ses qualités de flexibilité, d'adaptabilité et d'expressivité. Ainsi, DAO établit un vocabulaire commun pour le partage des connaissances afin d'améliorer la communication et d'éviter l'hétérogénéité sémantique entre les acteurs de domaines. La version opérationnelle de DAO et sa formalisation OWL sont fournies puisque nous croyons aux bonnes capacités de ce langage d'ontologie formel en termes de clarté et de raisonnement pour contribuer à l'aide à la prise de décisions de sécurité. En tenant compte de ces différents critères, DAO est considérée comme une ontologie de domaine de référence fondée sur UFO. Néanmoins, une évaluation suivant d'autres métriques et en utilisant des outils puissant est envisagée dans les perspectives à court terme.

L'objectif de cette ontologie est la systématisation de l'intégration de l'analyse dysfonctionnelle pour la conception des SCS. Pour concrétiser cet objectif, nous avons instancié et validé DAO avec un scénario d'une mission télé-opérée, décrit dans [Debbech *et al.*, 2018c] et illustré dans [Debbech *et al.*, 2018a]. En effet, cette validation à l'égard des systèmes à concevoir justifie l'intérêt de l'aspect technique et la vue du système et d'environnement de cette ontologie pour le développement des systèmes sécuritaires mais aussi pour l'aide à la prise de décisions. D'autre part, le module de DAO lié à l'aspect environnemental a été réutilisé pour clarifier conceptuellement les entités d'environnement considérées lors de la spécification formelle en B du système d'enclenchement ferroviaire. Cette contribution est valorisée dans le cadre du projet LCHIP, et a fait l'objet d'une publication [de Almeida Pereira *et al.*, 2019]. Dans le cadre du même projet, cette étude sera étendue pour utiliser le module de l'aspect technique de DAO afin d'intégrer l'analyse dysfonctionnelle dans la spécification du système d'enclenchement et vérifier ses propriétés de sécurité.

3.7 Conclusion

Dans ce chapitre, nous avons présenté la première contribution de cette thèse qui consiste en une ontologie de domaine d'analyse dysfonctionnelle (DAO). Cette ontologie est proposée afin de fournir une spécification formelle de la conceptualisation d'analyse dysfonctionnelle pour la conception des SCS. Fondée sur l'ontologie de haut niveau UFO, DAO établit un vocabulaire clair et non ambigu permettant d'avoir une conceptualisation partagée entre les différents acteurs impliqués dans la conception.

En premier lieu, nous avons commencé par définir les contraintes du domaine d'application ainsi que les choix méthodologiques permettant de répondre aux verrous scientifiques et technologiques identifiés. La construction de DAO est basée sur l'approche systématique SABiO pour le développement des ontologies du domaine de référence. Ainsi, nous avons détaillé les différentes phases de sa construction partant de l'élicitation de ses exigences sous forme de QC jusqu'à la vérification et la validation de DAO. Le processus d'évaluation

valide les critères de l'ontologie en termes de compétence du domaine, d'expressivité et de flexibilité. En effet, la réponse à ses QC est vérifiée et les graphes RDF de différents cas d'étude réels du domaine ferroviaire par le patron de conception de DAO sont établis.

Cette étape préliminaire de conception des SCS permet de définir les fondements de l'analyse dysfonctionnelle pour proposer des mesures de sécurité atténuant les risques perçus. Néanmoins, des conflits de communication et d'interprétation des données peuvent avoir lieu entre les ingénieurs de sécurité et les ingénieurs des exigences. Ceci peut conduire à des problèmes critiques de conception des SCS notamment en termes de violation de l'aspect de sécurité. Afin d'assurer la cohérence sémantique entre les mesures de sécurité induites de l'analyse dysfonctionnelle et les exigences de sécurité à spécifier, une conceptualisation multi-vues est nécessaire. Par ailleurs, l'alignement des connaissances des deux domaines est un besoin émergent pour fournir un modèle structuré et cohérent de contrôle et de gestion de sécurité pour la conception des SCS. D'autre part, le processus de gestion de décisions de sécurité doit être établi en s'appuyant sur un modèle commun pour un partage de connaissances sans ambiguïté et une interopérabilité sémantique entre les parties impliquées. La conceptualisation de ce processus doit prendre en compte à la fois l'aspect dynamique des décisions de sécurité, l'aspect organisationnel des SCS et le lien sémantique avec les exigences de sécurité de haut niveau, sous forme de **buts**, pour spécifier les exigences de sécurité. Dans le chapitre suivant, nous introduisons un formalisme permettant de faire face aux aspects organisationnel et dynamique des SCS, nous traitons la perspective de l'ingénierie des exigences dirigée par les buts (IEDB) et nous définissons son lien sémantique avec DAO afin de répondre aux besoins métier et aux objectifs de recherche.

Chapitre 4

Gestion de Décisions de Sécurité Orientée-But pour la conception des SCS

Sommaire

4.1 Introduction

Dans le chapitre précédent, nous avons proposé une ontologie d'analyse dysfonctionnelle permettant de conceptualiser les connaissances liées aux défaillances, leur causes et les dangers perçus. En s'appuyant sur les dangers identifiés et leurs causes associées, des mesures de sécurité peuvent être développées et deviennent par conséquent comme des exigences de sécurité de haut niveau qui visent à éliminer ou à atténuer les dangers identifiés. Généralement, une contrainte de sécurité peut être proposée sous forme de négation d'un danger identifié afin d'amener une opération à un niveau de sécurité acceptable. Cependant, ce type de liaison directe du danger vers les mesures de sécurité fournit peu de conseils aux ingénieurs pour la mise en œuvre des mécanismes d'atténuation.

Afin d'éviter les erreurs de conception, ces mesures de sécurité doivent être intégrées en tant que structure de contrôle pour le renforcement effectif de la sécurité du système. Par conséquent, les connaissances en matière de sécurité doivent être prises en compte dans le modèle de conception, en particulier dans les pratiques de l'IE. De ce fait, les mesures de sécurité ne sont pas limitées à prescrire ce qu'il ne faut pas faire mais donnent aussi une indication sur la manière de les satisfaire. Autrement dit, l'analyse de sécurité doit être liée d'une manière cohérente et structurée à la phase d'élucidation des exigences de sécurité. La liaison directe des deux activités permet d'assurer l'incorporation des barrières de sécurité appropriées dans l'architecture du système. Par conséquent, les erreurs d'interprétation des données critiques de sécurité sont anticipées afin de garantir la délivrance d'un système sûr.

Dans ce chapitre, nous proposons un cadre sémantique permettant de combiner les connaissances des deux domaines et d'établir une vue partagée. La figure 4.1 représente le raisonnement suivi pour l'élaboration de cette contribution. L'objectif principal de cette contribution est de faire face à l'hétérogénéité sémantique et de fournir une conceptualisation du processus de gestion des décisions de sécurité basée sur l'alignement des connaissances. Ainsi, nous procédons à la détermination des liens sémantiques entre les paramètres de sortie de l'ontologie précédemment introduite (DAO), à savoir les mesures de sécurité, et les concepts principaux de l'IE. Afin de fournir une vue hiérarchique partant des mesures de sécurité jusqu'aux exigences de sécurité, les pratiques de l'**IEDB** sont pertinentes dans ce contexte d'étude afin de garantir la cohérence et la satisfaisablité à plusieurs niveaux.

Ensuite, un processus de développement des mesures de sécurité appropriées est proposé afin de répondre aux contraintes organisationnelles des SCS et à l'aspect dynamique des décisions de sécurité. Ce faisant, nous introduisons un formalisme de gestion de sécurité pour les SCS fondé sur la réinterprétation de point de vue *sécurité-innocuité* du modèle de contrôle d'accès **Or-BAC**(**Organization-Based Access Control**) [Abou EL Kalam, 2003] qui est initialement introduit pour assurer la *sécurité-confidentialité* des systèmes d'information. Une fois le background introduit, nous présentons l'*ontologie de gestion de sécurité orientée-but*, appelée **GOSMO**, qui permet de répondre aux deux questions de

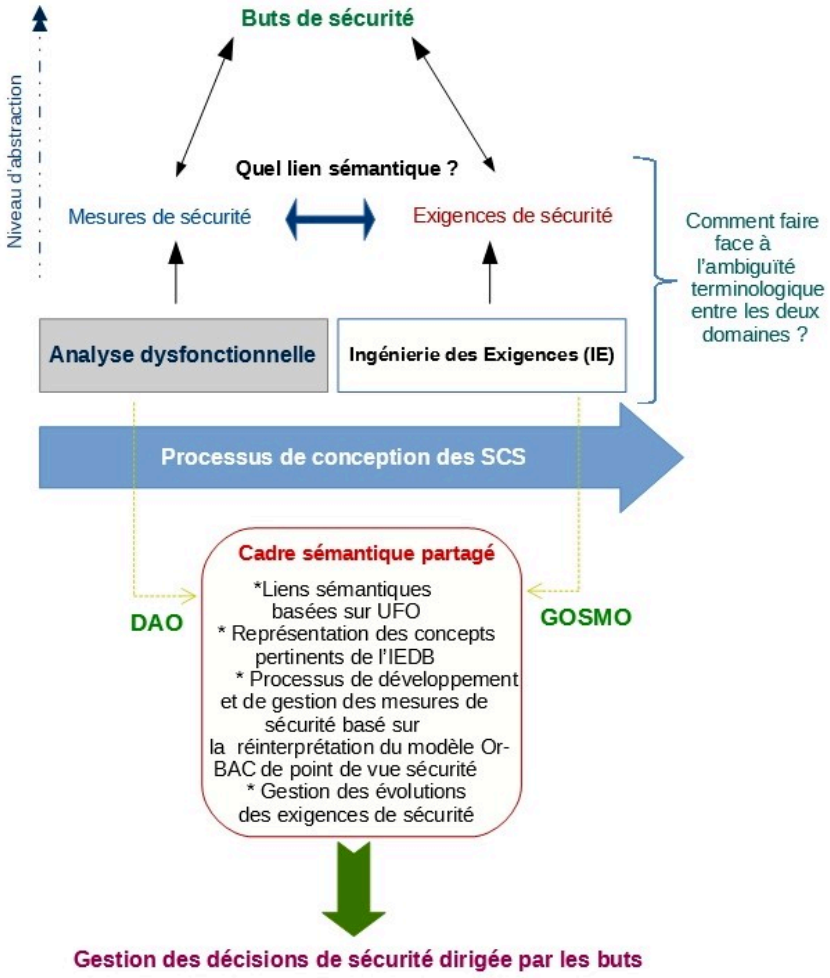

Figure 4.1 – Raisonnement suivi pour l'élaboration de cette partie

recherche suivantes :

- **QR2** : Comment interpréter et conceptualiser les mesures de sécurité et les lier aux concepts de l'IEDB dans la sémantique du monde réel ?
- **QR3** : Quelle interprétation sémantique et représentation structurée des concepts Or-BAC seraient en mesure de fournir un modèle de contrôle de sécurité ferroviaire et de traiter l'aspect organisationnel des SCS ?

Une évaluation par des cas d'études ferroviaires est effectuée, par la suite, afin de valider le contexte métier. Enfin, nous abordons une notion fondamentale de l'IE, la **gestion** des exigences et leur **traçabilité** afin d'assurer la cohérence entre elles de manière structurée et répondre à la question de recherche suivante :

- **QR4** : Comment faire face à l'évolution des exigences de sécurité issues des décisions de sécurité et maintenir la cohérence avec les différents éléments de conception ?

4.2 Ingénierie des Exigences Dirigée par les Buts (IEDB)

Dans le chapitre 2 (Section 2.2.3), nous avons évoqué l'intérêt de l'IEDB pour la réduction de la complexité du problème et le développement cohérent et structuré des exigences du système. Le concept central de cette activité est le **But** (Goal) qui représente l'intention d'une partie prenante (Stakeholder) ou une situation désirée qu'elle veut atteindre [Glinz, 2011]. À partir des buts élucidés, un modèle de buts est établi afin d'affiner la vision du système et modéliser les fonctions globales désirées. Ce modèle de buts est défini comme une structure ordonnée des sous-buts (sub-goals). En effet, ils peuvent exprimer des propriétés fonctionnelles associées aux services à fournir ou des propriétés non fonctionnelles associées à la qualité de service comme la sécurité, la fiabilité, etc. Par ailleurs, ils sont exprimés sous forme d'énoncés déclaratifs et peuvent être formulés à différents niveaux d'abstraction partant des buts stratégiques de haut niveau, par exemple *la collision des trains doit être évitée*, jusqu'aux buts de niveau inférieur tactiques, comme *le franchissement d'un signal fermé doit être autorisé par l'agent de circulation.*

Les buts apportent de nombreux avantages à la pratique de l'IE, qui sont récapitulés comme suit [Van Lamsweerde, 2001] :

- Les buts fournissent un critère précis pour une complétude suffisante de la spécification des exigences ;
- Ils assurent la pertinence d'une exigence si sa spécification est utilisée dans la preuve d'au moins un but ;
- Ils gardent les liens de traçabilité d'une exigence par raffinement et justifier son existence ;
- Leur raffinement fournit un mécanisme naturel pour structurer les documents d'exigences complexes et améliorer la lisibilité ;
- Ils détectent les conflits entre les exigences et les résoudre ;
- Ils séparent les informations stables de celles qui évoluent par hiérarchie ;
- Ils guident l'élucidation des exigences ;

Afin de fournir une base de raisonnement sur la cohérence, la complétude et la gestion des évolutions des exigences, les buts sont modélisés par diverses caractéristiques intrinsèques comme leur types, leur attributs et les liens avec les éléments du modèle des exigences. Ces modèles dépendent de l'approche d'IEDB utilisée dont chacune a incorporé les avantages définis ci-dessus pour améliorer les pratiques de l'IE. Nous comparons et discutons les caractéristiques de ces approches dans la section suivante.

4.2.1 Étude comparative des approches d'IEDB

Un éventail d'approches d'IEDB existe dans la littérature et se distingue par la manière de modéliser les relations des buts avec les autres éléments. Le Framework i^* [Yu, 2011] est un langage de modélisation approprié à la compréhension d'un problème dès les premières

phases de modélisation du système. Il propose divers modèles à différents niveaux d'abstraction pour décrire les dépendances entre les acteurs ainsi que leur propriétés intentionnelles. Dans un haut niveau d'abstraction, le modèle de dépendance stratégique (Strategic Dependency model) décrit les relations de dépendance entre les acteurs dans un contexte organisationnel : un acteur dépend d'un autre pour accomplir une intention. Un élément intentionnel peut être un but (*Goal*), une tâche (*Task*), une ressource (*Resource*) ou un but léger (*SoftGoal*). Dans un niveau inférieur, le modèle de justification stratégique (Strategic Rationale model) décrit et affine les éléments intentionnels dans la limite de chaque acteur, en explorant les raisons qui les sous-tendent. L'approche i^* se focalise sur les premières phases de l'IE, en identifiant les parties prenantes et en apportant leur buts stratégiques dans les modèles. Son apport principal est de fournir des outils pour modéliser les aspects sociaux guidés par les intentions des acteurs dans l'IE. Par ailleurs, *Tropos* [Bresciani *et al.*, 2004], une variante de i^*, inclut le concept de la décomposition du but pour réduire le niveau d'abstraction vers une spécification des exigences. Une nouvelle version de i^*, appelée *iStar*, inclut le raffinement des buts, qui peut être utilisé pour dériver les exigences du système à partir des buts de haut niveau [Dalpiaz *et al.*, 2016].

KAOS [Dardenne *et al.*, 1993] est une approche systématique permettant de définir et structurer les exigences. Elle se distingue par des modèles conceptuels ainsi qu'une sémantique spécifique pour capturer les relations de raffinement des buts ainsi que les relations avec les autres éléments, à savoir un *Agent*, *Opération*, *Exigence*, *Propriété du domaine*, etc. Dans KAOS, un but est une déclaration prescriptive d'intention que le système doit satisfaire. Le modèle de but vise à décrire les buts à atteindre par le système, les buts de haut niveau qui sont liés à la portée du système et aux intentions des parties prenantes (plus stratégiques), et les buts de bas niveau (plus technique). Les objectifs de niveau supérieur peuvent être décomposés/raffinés consécutivement, par différents types *AND/OR* ou *milestone* (ordonné), en niveaux inférieurs plus opérationnels pour exprimer comment ils peuvent être atteints. Les raffinements AND, OR et milestone décomposent un but respectivement à un ensemble de conjonction, de disjonction et de séquencement de sous-buts. Le premier raffinement signifie que la satisfaction de tous les sous-buts est suffisant pour satisfaire le but parent ; tandis que le deuxième signifie que la satisfaction d'un sous-but est suffisante pour la satisfaction du but principal [Van Lamsweerde, 2001]. Ainsi, diverses relations ont également été définies pour relier les buts aux agents sous forme de liens de *responsabilité*. La notion de « Responsabilité » signifie que l'agent s'engage à limiter son comportement en effectuant les opérations qui lui sont assignées uniquement dans des conditions restreintes, à savoir celles prescrites par les conditions préalables, les post-conditions et le conditions de déclenchement (trigger).

Techne [Borgida *et al.*, 2009] est un langage de modélisation des exigences fondé sur l'ontologie Core pour l'IE (CORE) [Jureta *et al.*, 2009]. CORE est basée sur l'ontologie de haut niveau DOLCE, introduite précédemment, qui vise à capturer les catégories on-

tologiques du langage naturel sous-jacent et du sens humain. Techne distingue différents états mentaux des parties prenantes à représenter dans le modèle des buts. Les désirs des agents sont des exigences que le système doit satisfaire et sont capturés à travers des instances du concept **but** quand ils décrivent une condition fonctionnelle vérifiable. Dans le cas contraire, ils sont capturés à travers d'autres concepts comme *SoftGoal*. Les croyances (*Beliefs*) impliquent des hypothèses du domaine définies comme des situations concernant le futur système et/ou son environnement. Les *intentions* indiquent des engagements à agir pour la satisfaction des exigences et sont capturées via le concept tâche (*Task*).

Le tableau 4.1 récapitule l'étude comparative de ces approches suivant des critères qui répondent à nos objectifs de recherche. Après cette description comparative, nous pouvons constater que les différents langages visent à représenter essentiellement les mêmes concepts, à savoir les buts et les notions associées. Cependant, étant donné qu'ils ont été construits de manière indépendante, nous ne pouvons pas ignorer que leurs constructions sous-jacentes pourraient ne pas partager la même sémantique. En outre, ces constructions sont principalement décrites avec des méta-modèles, qui sont des structures puissantes pour définir la syntaxe abstraite d'un langage, mais pas pour en clarifier la sémantique. En effet, ils utilisent différentes sémantiques pour interpréter les concepts de l'IEDB et les relations entre eux. Ainsi, il est clair que l'utilisation d'un langage par rapport à un autre peut poser des ambiguïtés au niveau de la compréhension et conduire à des conflits et des erreurs de conception.

Notre objectif principal est de proposer un cadre sémantique harmonisé permettant de combiner les connaissances des domaines dans une vue partagée. Par conséquent, une sémantique formelle des concepts ainsi qu'une vue interopérable entre les différentes approches est nécessaire pour répondre à la **QR2**. C'est pourquoi nous avons opté pour un modèle conceptuel de référence du domaine d'IEDB, appelé **GORO** (**Goal-Oriented Requirements Ontology**) [Negri *et al.*, 2017], qui intègre les distinctions ontologiques pour clarifier la sémantique formelle des concepts de l'IEDB, tout en assurant l'interopérabilité entre les approches définies ci-dessus. Le raisonnement suivi dans ce choix est illustré par la figure 2.15. Nous introduisons cette ontologie du domaine de référence dans la section suivante.

4.2.2 Choix méthodologique retenu

GORO est une ontologie de domaine de référence fondée sur l'ontologie fondamentale UFO. Elle établit une clarification conceptuelle de la notion de but et les concepts associés. Elle a été développée en s'appuyant sur l'approche systématique SABiO et en tirant profit des analyses ontologiques proposées par UFO, des modèles conceptuels des différentes approches d'IEDB pour fournir une harmonisation sémantique de haut niveau. Ces caractéristiques sont intéressantes pour notre contexte d'étude car la réutilisation de ce modèle de référence favorise l'alignement des connaissances d'analyse de sécurité et des

Approches d'IEDB	Concepts & relations utilisés	Expressivité sémantique	Propriétés de modélisation
i^*	Actor, Goal, Task, Resource, AND-Refinement, OR-Refinement, Refinement	-	Deux niveaux d'abstraction : Modèle de dépendance stratégique et modèle de justification stratégique (intentionnel)
KAOS	Goal, Operation, Expectation, Requirement, Domain Property, AND-Refinement, OR-Refinement, Operationalization	+	4 modèles : Modèle des buts, Modèles des responsabilités, Modèle des opérations, Modèle Objet
Techne	Goal, Task, Domain Assumption, Inference, Preference, SoftGoal, Conflict	++	Langage de modélisation fondé sur CORE/DOLCE, Distinction ambiguë entre le but et l'exigence, Ne considère pas le concept Agent
GORO	Stakeholder, Requirement, Task, Assumption, decomposes, alternative, intends to operationalize	++++	Ontologie de domaine d'IEDB, fondée sur UFO, considère une sémantique formelle, fournit une vue interopérable entre les approches précédentes : considère les concepts pertinents de l'IEDB

Tableau 4.1 – Étude comparative des approches d'IEDB

concepts de l'IEDB. D'autre part, GORO s'intéresse aux notions du moment mental de l'agent, définies dans le chapitre précédent, pour établir les relations entre le concept but et les propriétés intentionnelles proposées par UFO. Selon GORO, il existe une distinction du type du **But** en tant que contenu propositionnel de (*propositional content of*) deux moments mentaux : l'intention (**Intention**) ou le désir (**Desire**) de l'agent. D'autre part, le **But** peut être un *sous-type* d'une **Proposition** quand il est basé sur les hypothèses de l'agent.

Afin de répondre aux besoins de la gestion dynamique de la sécurité dirigée par les buts, nous réutilisons le fragment de GORO représenté par la figure 4.2 qui se focalise sur les relations entre le concept **But** et le concept **Moment Mental**. La relation est établie entre les concepts **Belief** et **Assumption** pour représenter cette propriété intentionnelle par rapport aux hypothèses qui décrivent une situation dans l'environnement que l'agent estime être vraie. Ainsi, les hypothèses (**Asumptions**) représentent le contenu propositionnel des croyances (**Belief**) et n'expriment pas le but d'un agent, mais une conviction qu'une certaine situation existe dans son environnement. Ce fragment permet de fournir le lien sémantique entre l'ontologie DAO qui incorpore ces propriétés intentionnelles et les concepts de l'IEDB dès les premières phases de conception des SCS.

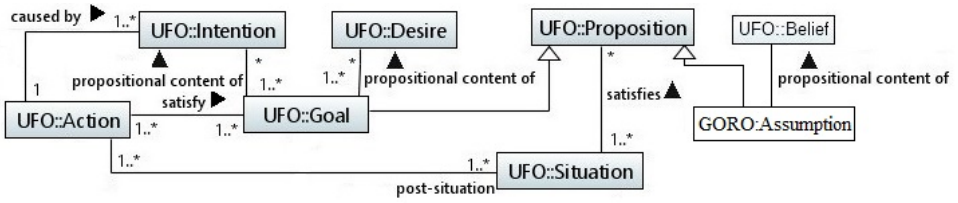

Figure 4.2 – Le fragment GORO se focalisant sur les concepts **Goal** et **Mental Moment** [Negri *et al.*, 2017]

D'autre part, la liaison entre les mesures de sécurité et les exigences de sécurité doit être guidée par les buts de sécurité et opérationnalisée par le biais d'un **Plan** qui définit la manière de satisfaire ce but de sécurité. Le concept **Task**, introduit par GORO, est intéressant pour illustrer cette interprétation et cerner les liens sémantiques entres les différents concepts. Ce concept est défini comme une instance du concept **Action Universal**, proposé par UFO, et signifie qu'une ou plusieurs exécutions de cette tâche produit une post-situation qui satisfait le but global. Nous détaillons la conceptualisation de cette notion ainsi que les relations entre le but, l'exigence de sécurité, la mesure de sécurité, l'agent, etc dans la section 4.4.

Dans le contexte des SCS, en particulier les systèmes ferroviaires, la gestion des décisions de sécurité nécessite un cadre dynamique permettant de satisfaire les contraintes organisationnelles. D'une part, les mesures de sécurité induites par l'analyse dysfonctionnelle doivent être exprimées d'une perspective orientée buts de sécurité afin d'assurer la satisfaisabilité globale. D'autre part, les mesures de sécurité doivent être mises en œuvre

au regard d'un plan qui satisfait ce but de sécurité global, dont l'exécution n'entre pas en conflit avec d'autres buts de sécurité. Afin de définir des décisions sur-mesure qui s'adaptent au contexte d'application et qui restent sous le contrôle d'une organisation, il est nécessaire d'intégrer un formalisme de gestion de sécurité qui incorpore à la fois l'aspect organisationnel et dynamique. Dans l'optique de répondre à ces besoins métier, nous introduisons une représentation structurée du processus de développement des mesures de sécurité basée sur la réinterprétation, du point de vue sécurité, du modèle Or-BAC [Abou EL Kalam, 2003]. Nous présentons ce formalisme et nous justifions ce choix dans la section suivante.

4.3 Formalisme de gestion de sécurité basé sur Or-BAC

Dans cette section, nous commençons par les motivations qui nous ont conduit au choix du modèle Or-BAC pour répondre aux enjeux scientifiques et technologiques. Ensuite, nous présentons les concepts principaux de ce modèle afin de les adapter d'une manière structurée à notre contexte.

4.3.1 Motivations

Dans le contexte des systèmes critiques de sécurité (SCS), la sécurité est considérée comme un problème de contrôle émergent. En effet, la gestion de la sécurité doit être assurée par une organisation de contrôle intégrée dans un système socio-technique adaptatif. Le but de cette organisation de contrôle est d'imposer les mesures de sécurité sur le comportement du système dès les premières étapes de conception. En outre, la garantie de la sécurité doit toujours être maintenue et le système doit préserver la sécurité de son comportement face aux divers changements. Par conséquent, il est nécessaire de définir les mesures de sécurité appropriées en fonction du contexte dans lequel opère le système pour tenir compte de toutes les évolutions. De ce point de vue, les SCS souffrent d'un manque de modèles de développement de mesures de sécurité dérivées de l'analyse dysfonctionnelle pour assurer le contrôle au sein de l'organisation.

Le modèle de contrôle d'accès Or-BAC intègre l'aspect organisationnel et structure les politiques d'accès aux systèmes d'information. Il a été initialement conçu dans l'optique d'assurer la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Ce modèle représente également des notions intéressantes comme le contexte, la hiérarchie des organisations, des rôles accordés aux utilisateurs et des permissions accordées aux rôles pour réaliser une activité au sein de l'organisation. Ainsi, il représente un intérêt pour répondre à notre problématique. Cependant, les deux systèmes mis en jeu, tels que les systèmes d'information et les systèmes ferroviaires représentent des différences en termes de :

— Besoins du domaine,

— Propriétés à garantir, à savoir la sécurité-innocuité et la sécurité-confidentialité,
— Contextes d'application,
— Buts à satisfaire,
— Actions à réaliser,
— Contraintes associées,

Afin de fournir une interprétation sémantique, une conceptualisation et une formalisation de ces notions pour la gestion des décisions de la sécurité ferroviaire, nous commençons par identifier les concepts principaux du modèle Or-BAC.

4.3.2 Le modèle Or-BAC pour les Systèmes d'Information

Le modèle Or-BAC est fondé sur une architecture à deux niveaux : un niveau *abstrait* et niveau *concret*. La figure 4.3 illustre la structure des concepts associés à ces deux niveaux ainsi que les relations entre eux. Le niveau abstrait contient les concepts **Rôle**, **Activité**, **Vue** et le niveau concret inclut les entités **Sujet**, **Action** et **Objet**. Le concept central du modèle Or-BAC est l'**Organisation** qui est définie comme un groupe d'individus qui jouent des rôles et gère un ensemble de politiques de sécurité. Ainsi, la hiérarchie des organisations est considérée dans Or-BAC et chaque sous-organisation possède ses propres politiques de sécurité.

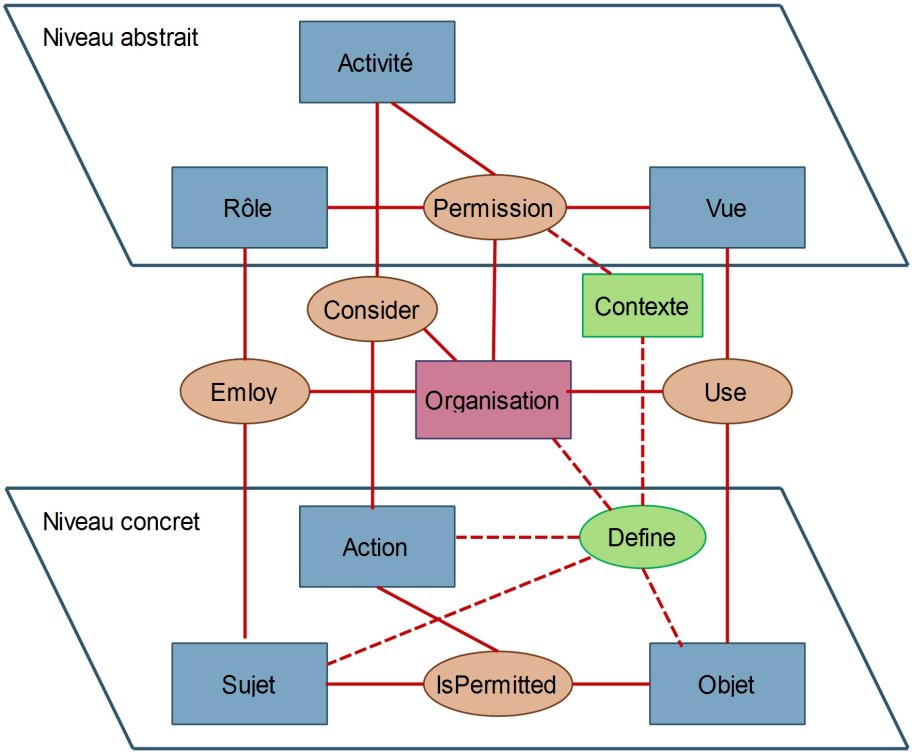

Figure 4.3 – Le modèle Or-BAC : les entités et les relations sont respectivement représentées par des rectangles et des ovales [Cuppens et Miège, 2004]

Le concept rôle a été initialement introduit dans le modèle RBAC (Role-Based Access

Control) [Ferraiolo et Kuhn, 1992] pour représenter une fonction dans une organisation. Un rôle est attribué à un sujet par le biais d'une relation *Employ(Organisation, Sujet, Rôle)* pour remplir une fonction dans une organisation. Ainsi, la relation *Consider(Organisation, Action, Activité)* est introduite pour définir une activité comme une abstraction d'un ensemble d'actions ayant le même objectif dans une organisation. Par ailleurs, une vue est une abstraction d'un ensemble d'objets qui partagent une propriété commune dans une organisation comme défini par *Use(Organisation, Objet, Vue)*.

Dans le modèles Or-BAC, des *permissions* sont accordées par l'organisation aux rôles pour réaliser des activités sur les vues. Ces permissions peuvent être des permissions, des interdictions, des obligations ou des recommandations pour gérer les politiques de sécurité. En effet, elles sont accordées dans un **Contexte** spécifique défini comme toute information qui caractérise la situation d'une entité ou qui spécifie les circonstances concrètes de cette attribution. Cette notion de contexte est intéressante pour les systèmes ferroviaires car elle prend en considération l'aspect dynamique de la gestion des décisions de sécurité. La modélisation du contexte dans Or-BAC se décline en plusieurs types, à savoir le contexte spatio-temporel, le contexte déclaré par l'utilisateur, le contexte prérequis et le contexte provisionnel [Cuppens et Miege, 2003].

Après le recueil des concepts principaux du modèle Or-BAC, nous introduisons dans la section suivante l'ontologie GOSMO qui intègre la réinterprétation des concepts Or-BAC dans la sémantique du monde réel pour la sécurité ferroviaire ainsi que leurs liens sémantiques avec les concepts de l'IEDB.

4.4 L'Ontologie de Gestion de Sécurité Orientée-But (GOSMO)

Le développement de GOSMO est basé sur l'approche systématique SABiO adopté pour le développement de DAO afin d'assurer la cohérence entre les deux ontologies proposées. Afin de récapituler le processus de développement de cette ontologie, nous identifions explicitement ses motivations et ses objectifs. La formulation des questions de compétence (QC) est nécessaire afin de définir la portée de l'ontologie et faciliter sa compréhension, sa réutilisation et son évaluation. Ensuite, nous présentons le modèle conceptuel qui émane du recueil des connaissances des domaines et leur l'interprétation sémantique. Par ailleurs, nous formalisons la conceptualisation en spécifiant des axiomes permettant de déduire des règles d'inférence et de raisonnement. Enfin, nous évaluons GOSMO par la vérification de sa compétence et la validation à l'égard des cas d'étude ferroviaire.

4.4.1 Identification des objectifs de GOSMO

Les QC énumérées ci-dessous représentent un haut niveau de granularité des QR2 et QR3 initialement définies et sont utilisées pour affiner la portée de GOSMO et pour guider

son processus d'évaluation :

- **QC1** : Qu'est ce qu'une mesure de sécurité et comment la relier aux concepts de l'IEDB ?
- **QC2** : Comment opérationnaliser ces mesures de sécurité ?
- **QC3** : Comment aligner sémantiquement le concept rôle proposé par Or-BAC avec le concept de rôle de UFO ?
- **QC4** : Comment conceptualiser le contexte lié aux permissions Or-BAC à l'égard de UFO ?
- **QC5** : Quelle implémentation, guidée par UFO, du concept d'organisation est capable de faire face à l'aspect organisationnel des SCS ?
- **QC6** : Quelle est la réinterprétation de l'attribution des rôles proposé par Or-BAC qui conviendrait pour les SCS ?
- **QC7** : Comment gérer les décisions en matière de sécurité-innocuité dans la conception SCS en s'appuyant sur la réinterprétation de la relation de permission de Or-BAC ?

4.4.2 Réinterprétation des concepts d'Or-BAC pour la sécurité ferroviaire

L'analogie entre la sécurité ferroviaire et la sécurité-confidentialité des systèmes d'information a été abordé auparavant par [Yangui, 2016] pour la modélisation, la vérification et la validation des règles d'exploitation ferroviaires. Ces règles visent à fournir une structuration des autorisations de déplacement des trains sur les lignes ferroviaires nationales équipées du système de gestion du trafic ferroviaire (ERTMS) [Schön, 2014]. Dans leur travaux, une approche basée sur le couplage UML/B a été proposée en adaptant les modèles RBAC et Or-BAC au profit de la sécurité ferroviaire [Ben Ayed *et al.*, 2014], [Ben-Ayed *et al.*, 2015].

Différemment de leur objectif de recherche, nous proposons de réinterpréter les concepts du modèle Or-BAC pour structurer le processus de développement des mesures de sécurité au regard des buts de sécurité. En effet, l'alignement entre les mesures de sécurité, les concepts d'Or-BAC et les concepts de l'IEDB s'avère nécessaire pour fournir une représentation structurée et partagée de ce processus. Afin de faire face à l'hétérogénéité sémantique entre ces connaissances, nous procédons à un alignement guidé par l'ontologie fondamentale UFO. En effet, la réinterprétation sémantique basée sur UFO établit un vocabulaire commun entre les différents domaines et la formalisation de cette conceptualisation fournit une base de raisonnement sur les décisions de sécurité.

Cette réinterprétation prend en considération les contraintes métier liées au domaine ferroviaire et les liens sémantiques des concepts d'Or-BAC avec les **buts de sécurité**, les **exigences de sécurité**, le **plan** mis en œuvre pour satisfaire ce but et les **agents** impliqués. Dans un stade précoce de conception des SCS, l'implication des agents inclut deux

aspects : les agents représentant les **parties prenantes** qui définissent le but à satisfaire, et les **acteurs** du système qui peuvent agir et procéder pour satisfaire ce but. En effet, les SCS tels que les systèmes ferroviaires peuvent impliquer un dispositif technique, une intervention humaine ou un système organisationnel, comme une solution à implémenter pour satisfaire un but de sécurité. En d'autres termes, le type d'acteurs des systèmes ferroviaires ne peut pas être défini à l'avance pour attribuer des rôles et des permissions comme c'est le cas pour les systèmes d'information. Dans le contexte ferroviaire, un acteur du système peut être une combinaison d'opérateurs humains et des dispositifs techniques coopérant entre eux pour atteindre un but de sécurité. En conséquence, la notion d'attribution de rôles au sein d'une organisation est plus délicate car cette dernière représente une agrégation complexe de différents acteurs.

Ainsi, nous essayons de satisfaire cette contrainte métier en fournissant une conceptualisation dans la sémantique du monde réel des entités *sujet* et *rôle*, introduites dans le modèle Or-BAC, au regard des concepts fondamentaux d'UFO et le modèle de référence GORO. Selon GORO, « un **Agent** devient un **Stakeholder** lorsque le **But** devient une **Exigence** » est une situation spécifique qui est considérée par une solution mise en œuvre ou un **Plan** associé. De ce point de vue, nous considérons cette situation spécifique comme l'attribution d'un rôle à l'agent par l'organisation. Dans cette situation, l'**Agent** devient un acteur du système qui est déclaré comme une instance du concept **Kind** proposé par UFO. En effet, le concept **Kind** introduit par le fragment UFO (Figure 3.3 du chapitre précédent) est un sous-type de **Substantial Universal**. Il représente toute entité rigide avec une identité unique permanente. Ce concept fondamental est lié au concept **Role** proposé par UFO qui représente un **Substantial Universal** non rigide ayant une identité qui change suivant les circonstances. Ainsi, le concept **Role** instancie **Kind** dans certaines situations et en se basant sur des contraintes spécifiques. En affinant cette interprétation, nous constatons que chaque **Kind** joue un **Role** pour exécuter une **Activité**. Cette activité représente un ensemble d'actions à effectuer pour satisfaire un but de sécurité et opérationnaliser une exigence de sécurité. Cette entité met en exergue le concept de tâche (**Task**) dans GORO, qui définit un plan d'actions pour satisfaire un **But**.

À l'issue de cette interprétation sémantique à l'égard de UFO et GORO, nous adaptons les concepts sujet, rôle et activité proposés par Or-BAC pour la gestion orientée-but de la sécurité ferroviaire :

Définition 6 . *(**Sujet**, **Rôle** et **Activité**) Un sujet est une instance de **Kind** qui joue un **StakeholderRole** représentant une instance de **Role**. Ce **StakeholderRole** est attribué par l'**Organisation** pour exécuter une activité (**Task**). Du point de vue GORO, cette activité (**Task**) est un sous-type d'**Action Universal** et son exécution conduit à une **post-situation** qui satisfait un but (**Goal**).*

Cette clarification conceptuelle des concepts sujet et rôle a été abordée et illustrée au

fur et à mesure par des exemples ferroviaires pour valider l'aspect métier dans [Debbech *et al.*, 2019c]. Une fois l'analogie entre les systèmes ferroviaires et les systèmes d'information déterminée, nous définissons l'interprétation sémantique des autres concepts tels que **Contexte**, et **Organisation** et **Action** ainsi que les relations d'*attribution de permission* et d'*attribution de rôle*.

Une **Organisation** est considérée comme un *sous-type* du concept **Agent**. Elle est une agrégation de **Stakeholder** qui représente une *instance de* **Kind**. Afin d'intégrer la hiérarchie des organisations, une organisation est composée de plusieurs sous-organisations. Le caractère dynamique d'attribution de rôles au sein de l'organisation doit être limité par certaines contraintes permettant l'alignement entre les concepts d'UFO et d'Or-BAC. À cet égard, nous déduisons que **StakeholderRole** est attribué au **Stakeholder** pour exécuter une tâche (**Task**) dans un contexte spécifique. Cette attribution est valide *uniquement* dans la même organisation et dans le même contexte. Dans l'optique d'interpréter cette contrainte dans la sémantique du monde réel, nous introduisons le concept **Assignment**, un *sous-type* du concept **Relator** défini par UFO. Le concept fondamental **Relator** est pertinent pour la validité de cette contrainte car il représente un *sous-type* du **Moment** et son existence dépend de plusieurs entités à la fois.

Similairement, la relation d'attribution de **Permission** à des **Stakeholder Role** pour exécuter une activité (**Task**) représente un *sous-type* de **Relator**. Ainsi, un **Contexte** est lié au concept **Task** par un lien de composition afin de mettre en lumière leur dépendance explicite. Le **Contexte** est introduit comme un sous-type de **Situation** (concept UFO) qui valide les circonstances de la **Permission** pour cette **Task**. Par ailleurs, le concept **Task** représente une vue abstraite d'un ensemble d'actions qui sont des **Mesures de Sécurité**.

L'interprétation sémantique des concepts d'Or-BAC du point de vue sécurité ferroviaire et orienté-but est établie en se basant sur les concepts de haut niveau d'UFO ainsi que les contraintes métier. Afin de fournir une vue claire et structurée de l'ensemble des concepts, nous présentons le modèle conceptuel global de la gestion de la sécurité orientée-but dans la section suivante.

4.4.3 Conceptualisation de la Gestion de Sécurité Orientée-But

Les connaissances des domaines, introduites auparavant, sont capturées dans le modèle conceptuel fondé sur UFO et représenté par la Figure 4.4. Le modèle conceptuel, exprimé en OntoUML, illustre la conceptualisation des relations entre les mesures de sécurité, les concepts de l'IEDB et d'Or-BAC. Il représente un ensemble de **nouveaux** concepts représentés d'une manière structurée afin de satisfaire les objectifs de recherche. Les concepts représentés en gris sont développés dans cette étude et les concepts en bleu sont les concepts de haut niveau. Cette étape de modélisation conceptuelle des connaissances partagées est détaillée et illustrée dans [Debbech *et al.*, 2019b]. Dans les domaines cri-

tiques, les **Mesures de Sécurité** sont définies comme les règles de sécurité imposées par l'organisation. Ce concept représente le noyau central de l'ontologie GOSMO car il établit un pont sémantique entre l'analyse dysfonctionnelle, les concepts de l'IEDB et d'Or-BAC. En effet, une **Mesure de Sécurité** est un *sous-type* d'**Action**, qui est lui-même un *sous-type* d'**Event**. Par transitivité, une **Mesure de Sécurité** change l'état de la réalité de la situation de danger (**Hazard**) vers une **post-situation**. Cette **post-situation** satisfait une **Proposition** qui est un super-concept du **But**. Par conséquent, nous introduisons la relation *satisfy* entre les concepts **Mesure de Sécurité** et **But de Sécurité**. Comme stipulé dans la définition 5, une **Mesure de Sécurité** *est composée de* plusieurs sous-mesures. De manière analogue, nous considérons la *composition* du **But de Sécurité** en sous-buts. La composition du but est une relation formelle (Whole-part) qui représente un **But** comme une disjonction de sous-buts. Ainsi, un But est atteint en satisfaisant au moins un sous-but. Ensuite, nous partons de l'hypothèse qu'une sous-mesure de sécurité peut être une partie de deux mesures de sécurité et peut contribuer à satisfaire deux sous-buts. L'ensemble de ces contraintes est spécifié par les axiomes dans la section 4.4.4.

Pour clarifier la sémantique de composition utilisée pour les mesures de sécurité, nous présentons un exemple ferroviaire illustratif sur une zone de freinage critique. Le but de sécurité est de respecter la signalisation dans un contexte de freinage en cas d'une forte descente. Les moyens de freinage et les procédures usuelles pourraient nous amener à un franchissement de signal. En effet, la distance de freinage est non classique : le conducteur va être surpris. Pour compenser ces difficultés, nous pouvons considérer la liste d'actions suivante : introduire une limitation de vitesse bien déterminée, introduire une procédure spécifique basée sur la connaissance de la ligne, renforcer le freinage du matériel roulant, contraindre le tonnage du convoi fret : interdire les liquides pour éviter les ≪ effets de balourd ≫. Partons du fait qu'une action (mesure) peut se définir comme un ensemble d'actions, toute action qui permet de garantir le respect de la signalisation dans ce contexte particulier est une sous-mesure. Par ailleurs, une action est une orchestration des différentes actions qui permet de satisfaire le but de sécurité. Au point actuel de la conception, nous ne pouvons pas savoir si la formation du conducteur pour anticiper le freinage est réaliste. En outre, il n'existe peut-être pas de solution d'ordre technologique pour résoudre le problème au niveau du matériel roulant. Enfin, est-il économiquement et fonctionnellement acceptable de limiter le tonnage ou interdire les liquides sur cette voie ?

C'est une question à laquelle nous ne pouvons généralement répondre qu'au stade de la conception. En définitive, nous avons juste caractérisé le besoin. Contrairement à la composition en UML qui vise à décrire un système, la relation *Whole-part* décrit des liens entre des concepts sans contraindre le système de manière directe.

Afin d'établir le lien sémantique entre un **But de Sécurité** et une **Exigence de Sécurité**, nous nous référons aux définitions fournies par les standards [IEEE 610.12, 1990] et [ISO/IEC/IEEE, 29148, 2011]. Nous considérons une **Exigence de Sécurité** comme un

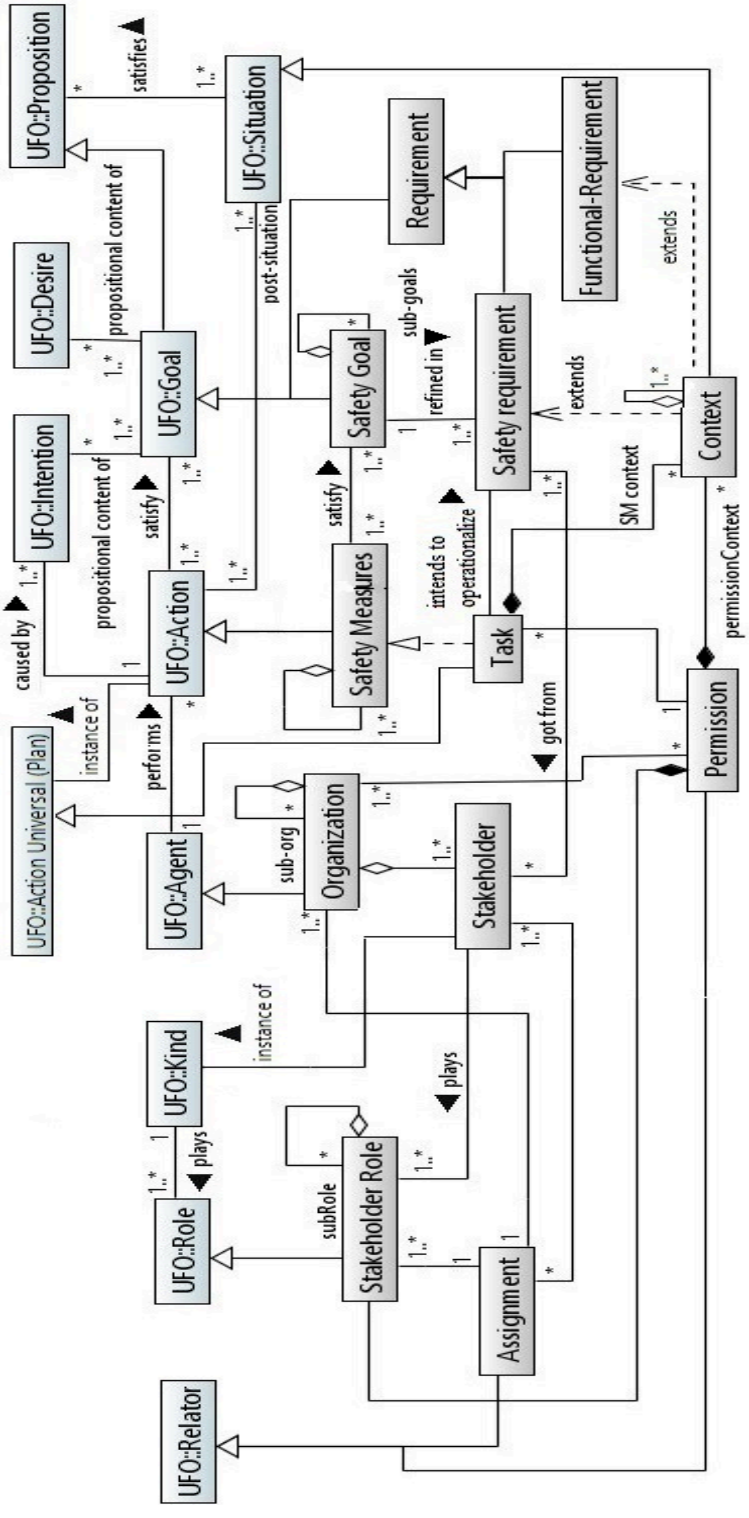

Figure 4.4 – Modèle conceptuel de l'ontologie de gestion de sécurité orientée-but GOSMO

raffinement du **But de Sécurité** pour satisfaire une spécification. Une spécification peut être un artefact, un document officiel de déclarations à satisfaire ou le jugement d'un agent pour satisfaire une situation spécifique. Ce raffinement permet de séparer l'exigence de haut

niveau d'abstraction (But) de son implémentation comme recommandé par les référentiels du domaine de l'IE. D'autre part, il établit une hiérarchie des exigences qui facilite le processus de leur vérification, leur gestion et leur traçabilité. Afin de déterminer et cerner la validité d'une exigence de sécurité ou une exigence fonctionnelle, nous définissons le concept du **Contexte** comme une situation spécifique composée d'un ensemble de sous-contextes. Cette interprétation est illustrée par la relation *extends* entre les deux concepts. Elle considère que la validité ou l'exécution d'une exigence est potentiellement liée à un contexte. Elle met en lumière la relation standardisée *extends* introduite par UML. Cette relation est définie pour établir une cohérence entre les exigences de sécurité et les mesures de sécurité qui appartiennent au même but de sécurité.

Le concept de tâche (**Task**) est considéré comme une vision abstraite d'une ou plusieurs **Mesures de Sécurité**. Elle permet de réaliser les mesures de sécurité par le biais de la relation *realizes*. En effet, une tâche est composée d'un **Contexte** caractérisant les circonstances ou la situation spécifique dans laquelle la **Permission** est accordée par l'**organisation** à un **Stakeholder Role** afin d'accomplir cette tâche (**Task**). D'autre part, la hiérarchie de **Stakeholder Role** est définie par l'agrégation de sous-rôles afin de factoriser les **Permissions** associées. Par conséquent, ce formalisme assure l'héritage des permissions du **Stakeholder Role** aux sous-rôles.

À la suite de cette modélisation conceptuelle fondée sur UFO, une taxonomie non ambiguë de la gestion des décisions de sécurité est introduite en s'appuyant sur Or-BAC et les concepts de l'IEDB afin de fournir une vue partagée entre les connaissances des domaines. Dans la section suivante, nous fournissons une caractérisation formelle de GOSMO en OWL pour garantir l'expressivité sémantique et fournir une version interprétable par la machine et réutilisable par d'autres domaines critiques.

4.4.4 Formalisation OWL de GOSMO

Dans la phase de formalisation de GOSMO en OWL, nous spécifions comme suit les axiomes en utilisant le fragment logique $\text{DLP}_{\exists}$ afin de définir les contraintes sur la taxinomie proposée :

$$\begin{aligned} &\mathit{SafetyMeasures} \sqsubseteq \mathit{Action} \sqcap \forall \mathit{hasPart}.\mathit{SubSafetyMeasures} \\ &\sqcap \exists \mathit{prevents}.\mathit{Hazard} \sqcap \forall \mathit{satisfy}.\mathit{SafetyGoal} \sqcap \exists \mathit{realises}^{-}.\mathit{Task} \end{aligned} \tag{4.1}$$

$$\mathit{satisfy} \circ \mathit{satisfy} \sqsubseteq \mathit{satisfy} \tag{4.2}$$

$$\top \sqsubseteq \neg \exists \mathit{satisfy}.\mathit{Self} \tag{4.3}$$

$$\top \sqsubseteq \exists (\mathit{satisfy} \sqcap \mathit{satisfy}^{-}).\bot \tag{4.4}$$

$$\mathit{satisfy}^{-} \sqsubseteq \mathit{isSatisfiedBy} \tag{4.5}$$

$$\top \sqsubseteq \geq 1(\mathit{partof} \circ \mathit{satisfy}).\top \tag{4.6}$$

$$\top \sqsubseteq \geq 1(partof \circ isSatisfiedBy).\top \tag{4.7}$$

$$SubSafetyMeasures \sqsubseteq \leq 2partOf.SafetyMeasures \tag{4.8}$$

$$SafetyGoal \sqsubseteq Goal \sqcap \forall hasPart.SubSafetyGoals \sqcap \forall isSatisfiedBy.SafetyMeasures \sqcap \forall isRefinedIn.SafetyRequirement \tag{4.9}$$

$$SafetyRequirement \sqsubseteq Requirement \sqcap \exists refinmentOf.SafetyGoal \sqcap \forall gotFrom.Stakeholder \sqcap \forall extends^{-}.Context \sqcap \exists intendsToOperationalize^{-}.Task \tag{4.10}$$

$$Task \sqsubseteq ActionUniversal \sqcap \exists realizes.SafetyMeasures \sqcap \forall intendsToOperationalize.SafetyRequirement \sqcap \forall hasPart.Context \sqcap \exists memberOf.Permission \tag{4.11}$$

$$Permission \sqsubseteq Relator \sqcap \forall hasMember.Task \sqcap \forall hasMember.Organization \sqcap \forall hasPart.Context \sqcap \forall hasPart.StakeholderRole \tag{4.12}$$

$$Task \sqsubseteq \leq 1memberOf.Permission \tag{4.13}$$

$$Context \sqsubseteq Situation \sqcap \forall extends.FunctionalRequirement \sqcap \forall extends.SafetyRequirement \sqcap \forall hasPart.subContext \sqcap \exists partOf.Permission \sqcap \forall partOf.Task \tag{4.14}$$

$$Stakeholder \sqsubseteq (Agent \sqcap \forall partOf.Organization \sqcap \forall gotFrom^{-}.SafetyRequirement) \sqcup (Kind \sqcap \forall plays.StakeholderRole \sqcap \forall partOf.Organization \sqcap \forall membertOf.Assignment) \tag{4.15}$$

$$StakeholderRole \sqsubseteq Role \sqcap \forall hasPart.SubRoles \sqcap \forall plays^{-}.Stakeholder \sqcap \exists memberOf.Assignment \sqcap \exists partOf.Permission \tag{4.16}$$

$$Assignment \sqsubseteq Relator \sqcap \forall hasMember.StakeholderRole \sqcap \exists hasMember.StakeholderRole \sqcap \forall hasMember.Organization \tag{4.17}$$

$$Organization \sqsubseteq Agent \sqcap \forall hasPart.SubOrganization \sqcap \forall hasPart.Stakeholder \sqcap \forall memberOf.Permission \sqcap \forall memberOf.Assignment \tag{4.18}$$

L'Axiome (4.1) spécifie les relations entre **SafetyMeasures** et les concepts **Hazard** et d'IEDB. La propriété *satisfy* introduite entre **SafetyMeasures** et **SafetyGoal** est une relation d'*ordre partiel stricte*. Par conséquent, elle est transitive, antiréflexive et asymétrique comme respectivement déclaré par les Axiomes (4.2), (4.3) et (4.4). L'inverse de la propriété *satisfy* est déclaré par l'Axiome (4.5). Afin de spécifier les hypothèses de composition des **SafetyMeasures** et **SafetyGoal** ainsi que la propriété *satisfy* entre eux, nous introduisons les Axiomes (4.6), (4.7) et (4.8). L'Axiome (4.6) permet de créer, extraire et raisonner par rapport aux **SubSafetyMeasures** qui sont des parties de la même **SafetyMeasure** et qui satisfont le même **SafetyGoal**. La restriction de la cardinalité permet à une **SubSafetyMeasure** de satisfaire au moins un **SafetyGoal**. D'autre part, l'Axiome (4.7) permet

de générer des instances correctes de tous les **SubSafetyGoals** qui sont des parties du même **SafetyGoal** et qui est satisfait par au moins une **SubSafetyMeasure**. L'Axiome (4.8) est spécifié pour formaliser l'hypothèse introduite : une **SubSafetyMeasure** peut être une partie d'*au plus deux* **SafetyMeasures**.

L'Axiome (4.9) spécifie les relations entre **SafetyGoal**, **SafetyMeasures** et **SafetyRequirement** comme interprétées et conceptualisées. Ensuite, l'Axiome (4.10) définit la formalisation de **SafetyRequirement** et les concepts associés. L'Axiome (4.11) spécifie les relations de **Task** avec les concepts **SafetyMeasures**, **SafetyRequirement**, **Context** et **Permission**. La propriété *memberOf* représente la relation d'inclusion qui associe un membre à son groupe. Elle diffère de la relation *partOf* en sa sémantique car cette dernière relie une entité complexe à ses entités composants. Comme la relation *partOf*, la relation *memberOf* est transitive, antisymétrique et irréflexive. L'Axiome (4.12) spécifie les relations du concept **Permission** afin d'imposer les conditions nécessaires pour accorder une **Permission** au **Task**. Grâce aux caractéristiques de propriétés *memberOf* et *hasPart*, une **Task** ne peut être réalisée qu'avec une **Permission** associé comme imposé par l'Axiome (4.13). Les relations liées au **Context** sont spécifiées par l'Axiome (4.14) en formalisant la conceptualisation introduite auparavant.

La classification du type du **Stakeholder** considérée dans cette étude est spécifiée par l'Axiome (4.15). La première partie de la disjonction représente l'**Agent** qui contribue à la proposition des exigences de sécurité comme une source légitime au sein de l'organisation. La deuxième partie représente le **Stakeholder** en tant que **Kind** qui *joue* un **StakeholderRole** attribué par l'**Organization**. L'interprétation proposée pour **StakeholderRole** est définie par l'Axiome (4.16) pour formaliser sa hiérarchie ainsi que ses relations avec les autres concepts. L'attribution du **StakeholderRole** au **Stakeholder** est effectuée par le biais du concept **Assignment** comme imposé par l'Axiome (4.17). Enfin, l'Axiome (4.18) spécifie les relations du concept **Organizaion**.

4.4.5 Implémentation de GOSMO

Similairement à l'implémentation de DAO, le pattern de GOSMO est implémenté en OWL à l'aide Protégé. Les restrictions liées à la disjonction des classes ainsi qu'aux caractéristiques des propriétés (transitivité, fonctionnalité, réflexivité, etc) sont prises en compte. Par ailleurs, les cardinalités et les restrictions du domaine/co-domaine sont appliquées dans l'implémentation OWL. L'implémention de GOSMO en termes de la hiérarchie de ses concepts et ses propriétés est illustrée par les figures 4.5 et 4.6. Les restrictions de cardinalité et du domaine/co-domaine (≪ domain ≫ et ≪ range ≫) sont implémentées pour les classes et les propriétés.

La figure 4.7 représente un exemple de restrictions du domaine/co-domaine pour la propriété *refinedIn*.

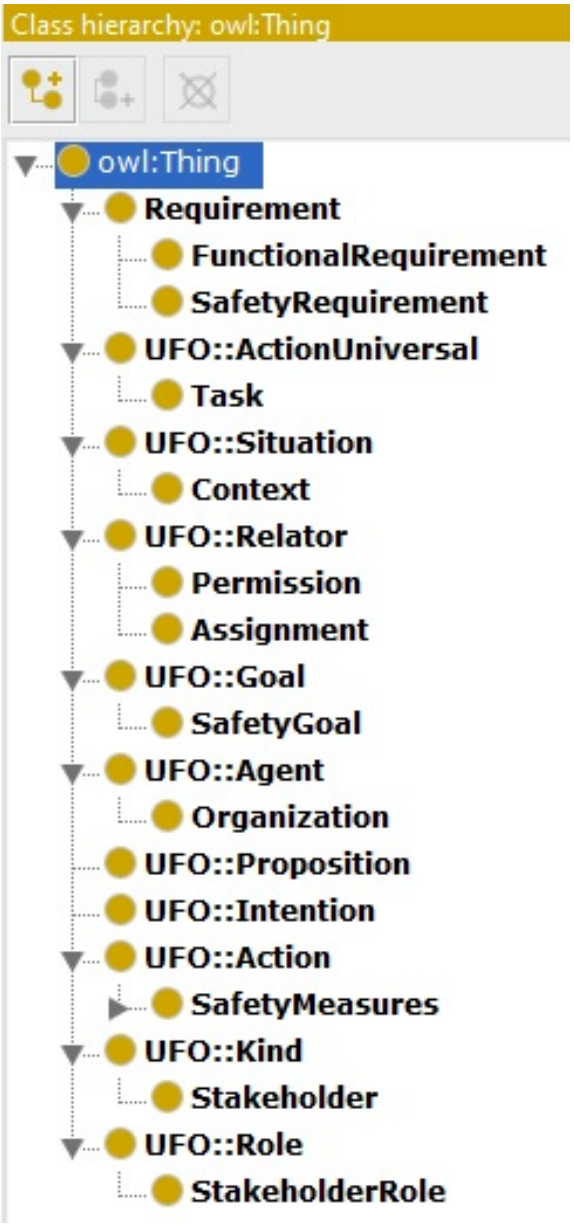

Figure 4.5 – Hiérarchie des classes de GOSMO sur Protégé

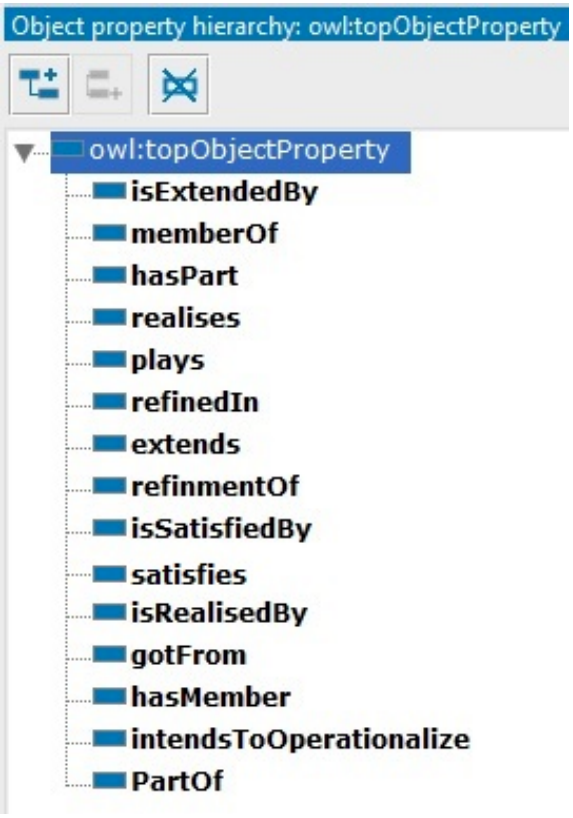

Figure 4.6 – Propriétés de type ObjectProperty de GOSMO sur Protégé

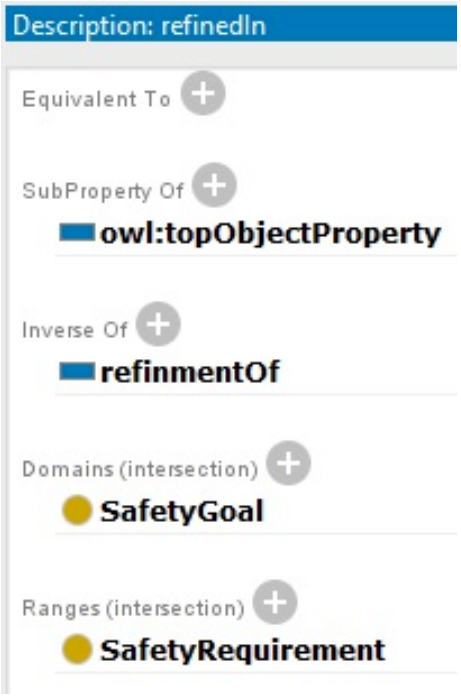

Figure 4.7 – Restrictions du domaine/co-domaine des classes de GOSMO sur Protégé

Un exemple d'axiomes de GOSMO pour contraindre les classes et les propriétés est illustré par la figure 4.8 grâce à la définition logique fournis par les constructeurs OWL équivalents aux constructeurs DL.

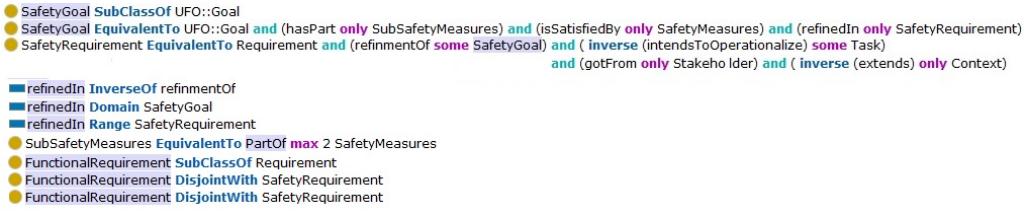

Figure 4.8 – Exemple d'axiomes logiques issus de GOSMO sur Protégé

Par ailleurs, GOSMO a été instanciée afin de concrétiser l'ontologie et de pouvoir tirer profit de ses caractéristiques tels que le raisonnement et l'interrogation par des requêtes SPARQL. La figure 4.9 illustre un exemple d'individus pour la classe **Safety-Measures**. Les instances sont déclarées différentes (Different individuals). Les propriétés liées à l'instance « UseofEmergenceyBrakes » sont représentés dans la partie « Property assertions » en bas.

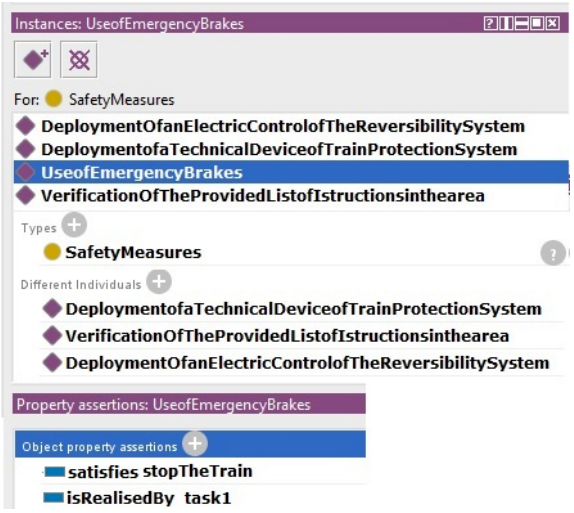

Figure 4.9 – Exemple d'instances de la classe SafetyMeasures et leur propriétés implémentés sur Protégé

Après avoir obtenu une version opérationnelle de GOSMO, nous passons à la vérification des compétences attendues en appliquant les techniques de vérification proposées par SA-BiO.

4.4.6 Évaluation de GOSMO

Le tableau 5.1 représente les résultats de la vérification de GOSMO à l'égard des QC prédéfinies. Les résultats obtenus indiquent que GOSMO répond à toutes les QC. GOSMO satisfait ses exigences attendues et fournit une conceptualisation partagée entre

les différents domaines tout en assurant l'harmonisation sémantique. La spécification des exigences de GOSMO est formulée dans le même vocabulaire en langage naturel afin de fournir un support de documentation et de communication efficace.

QC	Concepts et Relations
CQ1	A **SafetyMeasure** is a *subtypeOf* **Action**. It *hasPart* **SubSafetyMeasures**. It *satisfies* a **SafetyGoal** that *hasPart* **SubSafetygoals**. A **SafetyGoal** is *refinedIn* **SafetyRequirement** *gotFrom* a **Stakeholder**. When the **Task** is performed, a **post-Situation** occurs and *satisfies* a **Proposition** (**Goal**).
QC2	A **Task** is accomplished by a **Permission** assigned to **StakeholderRole** by an **Organization** according to a specific **Context**.
QC3	A **StakeholderRole** is a *subtypeOf* **Role**. It *is played by* a **Stakeholder** (a *subtypeOf* **Kind**).
QC4	A **Context** is a *subtypeOf* **Situation**. It denotes the specific **Situation** (circumstances) in which the **Permission** is assigned to a **StakeholderRole** to perform the **Task**. It *hasPart* **SubContexts**. It *extends* a **SafetyRequirement** and a **FunctionalRequirement**.
QC5	An **Organization** is a *subtype of* **Agent** and it *hasPart* **sub-organizations**. An **Organization** *hasPart* one or many **Stakeholders** that are a *subtypeOf* **Kind**.
QC6	An **Assignment** is a *subtypeOf* **Relator** and it denotes the **Stakeholder-Role** assignment to a **Stakeholder** by an **Organization**.
QC7	A **Permission** is a *subtypeOf* **Relator** and it denotes the **Stakeholder Role** authorization to accomplish the **Task** according to a **Context**, which is a specific *subtypeOf* **Situation**.

Tableau 4.2 – Table de vérification de GOMSO : QC et leurs réponses par GOSMO

L'alignement entre les connaissances est bien établi à travers la conceptualisation et la formalisation, et la taxinomie proposée répond aux objectifs attendus. Afin de valider la flexibilité de GOSMO à l'égard des connaissances métier, nous illustrons le processus de la gestion de sécurité de deux scénarios différents dans la section suivante. Le raisonneur Pellet a été utilisé pour vérifier la cohérence de GOSMO. La hiérarchie inférée de l'ontologie est illustrée par la figure 4.10.

4.5 Validation de GOSMO par des cas d'étude ferroviaires

Afin de valider l'adaptabilité de GOSMO pour représenter différentes situations réelles et annoter des données dans le cadre d'une aide à la prise de décisions de sécurité, nous entamons la phase de son instanciation à l'égard de trois scénarios différents tels que : le

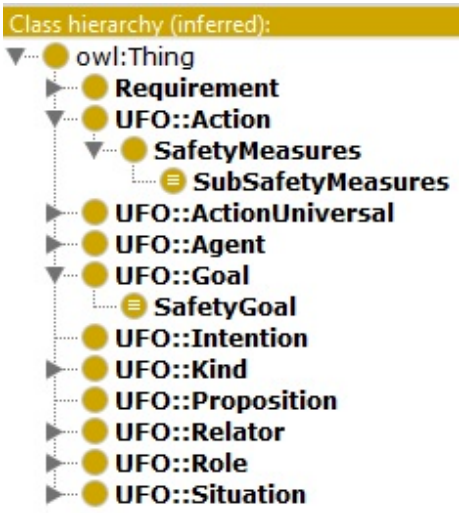

Figure 4.10 – Hiérarchie inférée de GOSMO à l'aide du raisonneur Pellet

scénario d'accident ferroviaire de Longueville, le scénario d'accident ferroviaire de Saint-Romain-En-Gier et un scénario de mission ferroviaire télé-opérée.

4.5.1 Scénario d'accident ferroviaire de Longueville

À l'issue de la description du scénario d'accident et l'illustration de son analyse dysfonctionnelle par DAO présentées dans le chapitre précédent, le processus de la gestion de décisions de sécurité est menée par l'instanciation de GOSMO. Le raisonnement de sécurité, introduit dans cette section, émane de l'analyse dysfonctionnelle réalisée auparavant ainsi que des connaissances métier acquises. Par conséquent, la représentation graphique de l'annotation sémantique est utilisée pour illustrer le processus de la gestion orientée-but de la sécurité afin d'améliorer la visualisation de l'illustration GOSMO et valider sa portée sémantique sans modifications.

Suite à l'analyse du scénario d'accident de Longueville, nous constatons que la violation des mesures de sécurité conduit à l'occurrence du danger de la prise en écharpe. En effet, le manque d'un formalisme pertinent de contrôle de sécurité intégré dans la conception des systèmes ferroviaires constitue un facteur majeur de cet accident. Afin de valider la pertinence du patron (pattern) de GOSMO pour la conception des SCS, le modèle Or-BAC orienté-but et réinterprété pour la sécurité est utilisé pour analyser les mesures de sécurité, qui auraient pu être en mesure d'éviter cet accident. Par ailleurs, le processus de développement des mesures de sécurité, qui doivent être considérées comme des solutions flexibles pour éviter cette situation dangereuse, est effectué comme indiqué ci-dessous pour assurer la validité de l'interprétation sémantique pour différents contextes.

Remarque 4.1 *Il est important mentionner que les mesures de sécurité sont proposées intuitivement en s'appuyant sur l'analyse dysfonctionnelle menée, les résultats d'enquête*

du BEA-TT [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005] et les connaissances ferroviaires dans l'optique de l'illustration.

La première **SubSafetyMeasure** peut être le déploiement d'une commande électrique du système de réversibilité pour *satisfaire* la commutation des locomotives et l'activation correcte des freins (**SubSafetyGoal**). Cette sous-mesure de sécurité du dispositif technique fournit un renforcement du comportement du système afin d'éviter la défaillance technique de la position instable de la serrure de réversibilité décrite dans la figure 3.14 du chapitre précédent. Ce **SubSafetyGoal** est *une partie du* **SafetyGoal** global qui consiste à éviter la collision entre deux trains comme le montre la figure 4.12.

Afin de faire face à l'erreur humaine du conducteur du train 117710, nous formalisons le geste métier préconisé par le référentiel « conducteur de ligne » et applicable par l'**Organization**. En effet, le formalisme de la gestion de sécurité basé sur Or-BAC permet de structurer ces règles de sécurité et de garantir la satisfaction du **SafetyGoal** global. Le conducteur en tant que **StakeholderRole** attribué par la SNCF (**Organization**), a la **Permission** accordée à sa tâche (**Task**) pour utiliser les systèmes de freinage d'urgence comme une **SubSafetyMeasure**, dans les situations d'urgence telles que la dérive du train (**Context**), afin d'arrêter le train (**SubSafetyGoal**) puis éviter la collision (**SafetyGoal**). Cette structuration permet de renforcer le mode opératoire du conducteur au sein de l'organisation. La figure 4.11 représente le graphe RDF des données d'accident liées au processus du contrôle orienté-but de la sécurité pour imposer les gestes métier du conducteur.

La deuxième **SubSafetyMeasure** est le déploiement d'un dispositif technique (un composant du système de protection du train) pour renforcer le comportement du contrôle de freinage ou du comportement du conducteur. Cette sous-mesure de sécurité *satisfait* l'alerte à bord du conducteur quand il franchit un signal fermé et il doit l'acquitter (**SubSafetyGoal**). S'il n'acquitte pas cette alerte, l'arrêt d'urgence est déclenché automatiquement. Ce déclenchement automatique d'arrêt d'urgence représente une **post-situation** qui satisfait le **SafetyGoal** global. Comme le montre la figure 4.12, cette sous-mesure de sécurité permet de traiter, à la fois, l'erreur humaine du conducteur, et la défaillance technique du système de réversibilité qui impacte le freinage.

Une autre solution simple et adéquate dans le cadre de ce scénario pourrait être l'utilisation de dispositifs de contrôle automatique comme les crocodiles [1]. Cependant, cette solution n'est pas efficace dans tous les contextes pour arrêter un train traversant un signal fermé. Un dispositif plus flexible pourrait être une solution sur mesure pour satisfaire différents contextes.

1. Le crocodile est un équipement utilisé sur les réseaux ferroviaires français, belge et luxembourgeois pour transmettre en cabine l'autorisation ou non de franchir un signal, et éventuellement arrêter le train en cas de franchissement dangereux d'un signal.

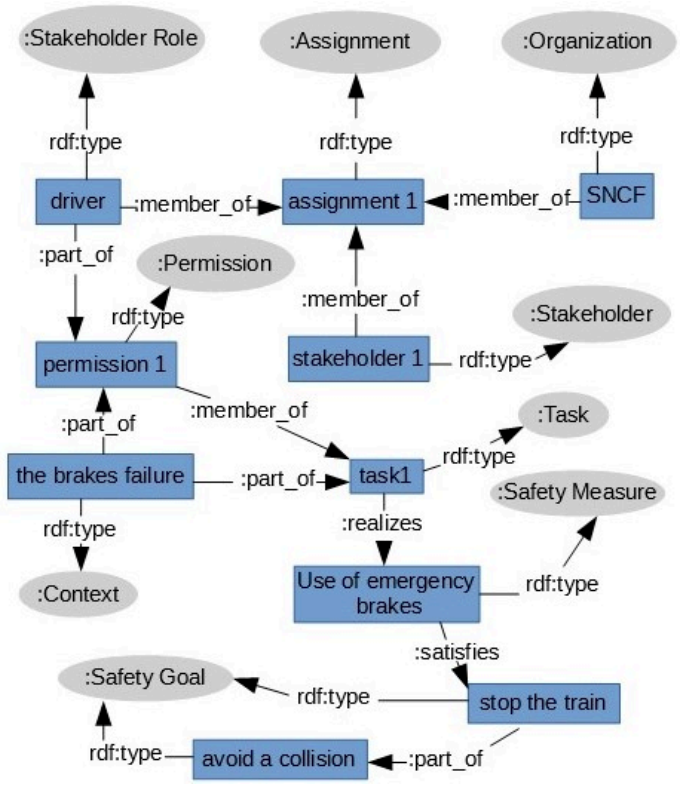

Figure 4.11 – Graphe RDF du comportement réglementé du conducteur par le modèle Or-BAC orienté-sécurité pour l'accident de Longueville

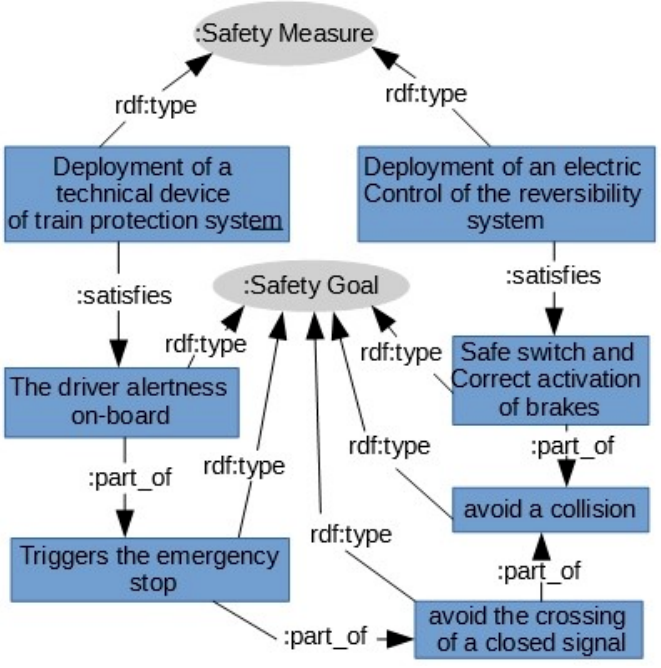

Figure 4.12 – Graphe RDF du développement des mesures de sécurité dirigé par les buts pour l'accident de Longueville

4.5.2 Scénario d'accident ferroviaire de Saint-Romain-En-Gier

Cet accident est dû à une combinaison de facteurs humains et organisationnels comme décrit et analysé dans le chapitre précédent. En effet, l'incohérence de la réglementation pour le trafic commercial et le trafic des trains de travaux a contribué à l'occurrence de la collision nez à nez de Saint-Romain-En-Gier. Cet aspect organisationnel doit être considéré pour assurer l'interopérabilité ferroviaire en ajoutant des documents d'organisation des travaux et de la signalisation à disposition des agents d'accompagnement notamment dans une section de ligne en dehors de leur établissement d'exploitation. Cette mesure de sécurité est illustrée par la figure 4.13 pour justifier la pertinence du modèle de contrôle organisationnel proposé dans GOSMO.

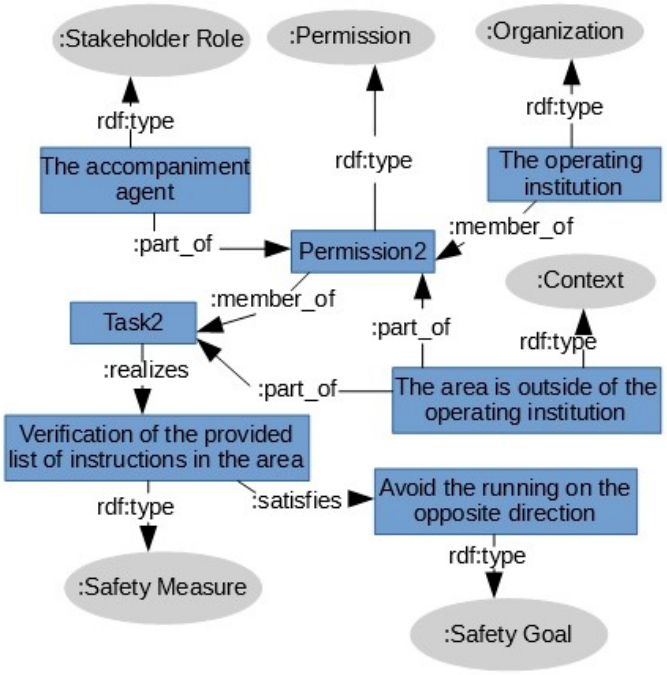

Figure 4.13 – Graphe RDF du contrôle organisationnel de la sécurité pour l'accident de Saint-Romain-En-Gier

D'autre part, le conducteur du train des travaux doit demander l'orientation de circulation et ne doit pas franchir un signal éteint sans l'autorisation explicite de l'agent de circulation, notamment en présence des installations permanente de contre sens IPCS et la protection des pas d'IPCS par des DIV. En imposant cette **SafetyMeasure**, le conducteur s'assure qu'il circule dans la bonne orientation et ne franchit pas un signal éteint pour éviter le collision nez à nez (**SafetyGoal**). Par ailleurs, l'hétérogénéité des éléments du **Contexte** a favorisé l'occurrence de cet accident. Il convient donc d'intégrer ce modèle de gestion de sécurité qui prend en considération l'appréciation du contexte comme une condition nécessaire pour accorder la **Permission** de réaliser une tâche. La figure 4.14 illustre le graphe RDF de cette mesure de sécurité.

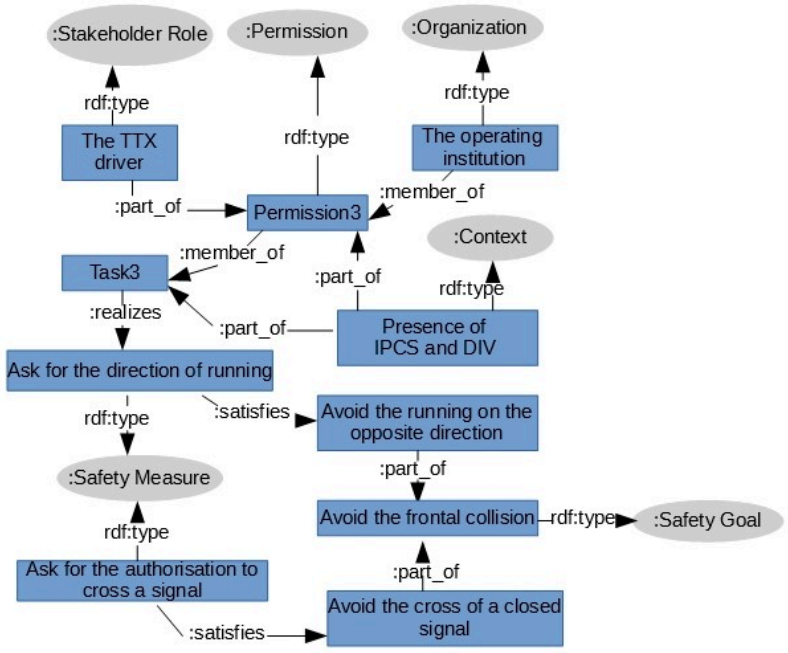

Figure 4.14 – Graphe RDF d'une mesure de sécurité sous forme d'une procédure pour l'accident de Saint-Romain-En-Gier

Ce scénario nous permet de constater que la prise de connaissance des différentes parties du contexte permet d'avoir une meilleure conduite de raisonnement de sécurité pour éviter les dangers. Cette conclusion est arguée aussi par les experts du BEA-TT lors de l'analyse du comportement erroné de l'agent de circulation du matin : « On se rend compte que cet agent s'est trouvé confronté à une situation délicate, face à plusieurs sources d'information dont il n'avait pas entièrement pris connaissance, et dont les indications n'étaient pas complètes ni cohérentes entre elles, sans que cette incohérence ait été clairement perçue par lui » [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004]. Par conséquent, l'intégration du modèle proposé par GOSMO qui prend en considération les différentes informations critiques du contexte s'avère nécessaire pour mener à les missions ferroviaires critiques en toute sécurité. La modélisation de ce scénario à l'aide d'une approche dirigée par les modèles ainsi que l'intégration des contraintes liées au contexte sont présentées dans [Debbech *et al.*, 2019a]. Cette modélisation nous a permis d'abstraire la représentation des connaissances et de les aligner par la suite avec les connaissances de l'IEDB et de la sécurité.

4.5.3 Mission ferroviaire télé-opérée

Dans les deux premiers cas d'étude, nous nous sommes focalisés sur l'analyse dysfonctionnelle ainsi que le processus de la gestion des décisions de sécurité en s'appuyant sur le modèle Or-BAC et l'IEDB. Ainsi, nous avons validé la capacité des ontologies proposées

à représenter des situations critiques de l'accidentologie et des systèmes existants. En effet, DAO et GOSMO présentent un véritable intérêt pour éviter les dangers et faire face à la complexité de la gestion des décisions de sécurité qui sont adaptatives au contexte et guidées par les buts. Étant donné que l'objectif principal de cette deuxième contribution est l'intégration de la gestion orientée-but et anticipée de la sécurité ferroviaire lors de la conception d'un nouveau SCS, il nous semble judicieux de valider GOSMO par un scénario inspiré du mode opératoire des **systèmes autonomes**. Dans cette section, nous présentons une instanciation de GOSMO pour annoter la gestion des décisions de sécurité lors de l'organisation d'une mission ferroviaire télé-opérée.

Description des scénarios de la mission

Cette mission télé-opérée représente le franchissement d'une rampe dans les conditions de sécurité raisonnables en s'appuyant sur la prise de connaissance des différents éléments du **contexte** d'évolution des infrastructures ferroviaires. La description et l'analyse des deux scénarios *nominal* et *dégradé* de la mission est détaillée dans le rapport de recherche [Debbech *et al.*, 2018c]. Le scénario nominal décrit la planification 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'essai des freins.
4. À l'issue de cette étape de prise de connaissance, le conducteur décide d'organiser la mission de manière classique.

À l'issue 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* définit 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 derniers.

Dans ce scénario, le danger est 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. Afin de valider la capacité de GOSMO à représenter les scénario décrits ci-dessus, nous avons décomposé les éléments du contexte 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 *part_of*(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 l'estimation de la probabilité faible du risque associé au non passage de la rampe 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.

Représentation du scénario nominal

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 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 (**SubSafetyMeasure 1**), la prise de connaissance des documents fournis (**SubSafetyMeasure 2**) et l'essai des freins (**SubSafetyMeasure 3**) constituent l'ensemble de sous-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 qui sont des parties de la **SafetyMeasure** globale : Prise de connaissance du contexte général de la mission. Cette dernière permet de satisfaire le **SafetyGoal** global,

le franchissement de la rampe en toute sécurité. La figure 4.15 représente le graphe RDF, basé sur un fragment de GOSMO pour la gestion des décisions de sécurité en fonction du contexte pour le scénario nominal de la mission télé-opérée.

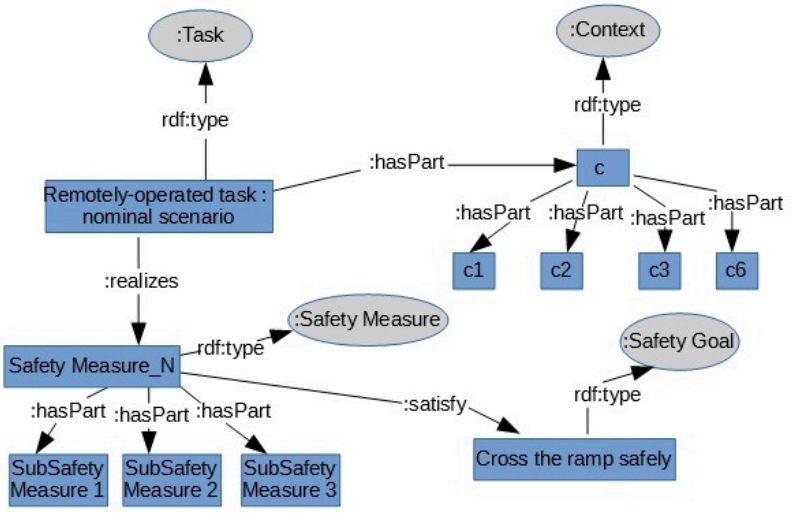

Figure 4.15 – Graphe RDF de la gestion adaptative au contexte des décisions de sécurité pour le scénario nominal de la mission télé-opérée

Représentation du scénario dégradé

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'issue de la prise de connaissance de ces deux éléments du contexte, le conducteur décide d'organiser normalement sa mission. Pour ce scénario dégradé 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 de l'union 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 (**SafetyMeasure**) qui peut être décomposée en deux sous-mesures de sécurité comme suit :

— **SubSafetyMeasure 4** : la mise à disposition d'une locomotive de remplacement ;
— **SubSafetyMeasure 5** : l'utilisation d'une deuxième locomotive ;

La disjonction de ces sous-mesures de sécurité permet de satisfaire le but de sécurité global pour franchir la rampe dans les conditions acceptables. Néanmoins, la **SubSafetyMeasure 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 4.16 représente le graphe du scénario

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

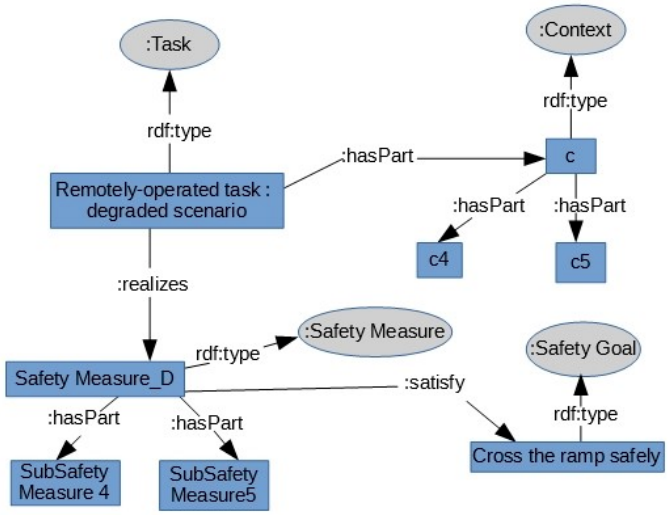

Figure 4.16 – Graphe RDF de la gestion adaptative au contexte des décisions de sécurité pour le scénario dégradé de la mission télé-opérée

La validation de GOSMO avec ce cas d'études met en exergue la pertinence du modèle conceptuel introduit et de la taxonomie définie dans la sémantique du monde réel, ainsi que sa capacité d'analyse des situations critiques des futurs systèmes autonomes. En effet, le modèle conceptuel met en relief le contexte et ses concepts environnants afin de systématiser le processus global de la gestion des décisions de sécurité lors de la préparation d'une mission de téléconduite avec un train de fret télécommandé.

L'interrogation de GOSMO avec des requêtes SPARQL permet de chercher les données qui remplissent certains critères de recherche. La figure 4.17 illustre l'exemple d'une requête SPARQL testée sur GOSMO. Cette requête permet d'obtenir les mesures de sécurité qui satisfont le but de sécurité « stop the train ».

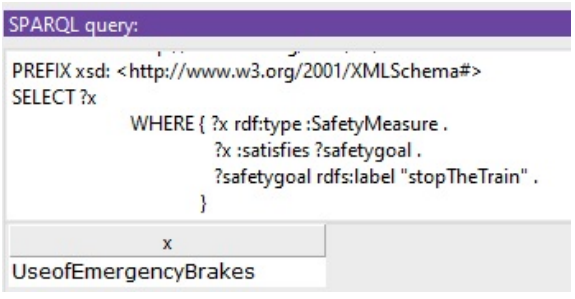

Figure 4.17 – Exemple de requête SPARQL et son résultat testée sur GOSMO

4.6 Discussion

L'ontologie proposée contribue au partage des connaissances, à la modélisation conceptuelle et à la gestion des décisions de sécurité. Les aspects considérés dans cette étude sont résumés comme suit.

Premièrement, GOSMO fournit une conceptualisation des mesures de sécurité, leur développement au regard de la satisfaction du but de sécurité et de la réinterprétation des concepts Or-BAC d'un point de vue sécurité, pour améliorer la gestion des décisions de sécurité. Cette analyse conceptuelle est basée sur l'utilisation des concepts de haut niveau et des relations fondamentales d'UFO. Ensuite, GOSMO systématise l'utilisation ambiguë du terme *mesures de sécurité* et des concepts associés dans la terminologie des SCS. De plus, la réinterprétation des concepts Or-BAC, tels que organisation, rôle, permission et contexte vise à assister le développement des mesures de sécurité et à fournir un modèle de contrôle organisationnel de sécurité structuré et cohérent. En outre, GOSMO peut être utilisé comme modèle de référence pour fournir l'analyse ontologique et la clarification des situations critiques comme validées par les scénarios d'accidents et la mission télé-opérée.

Deuxièmement, la gestion de la sécurité est effectuée d'un point de vue buts afin de faire face à la complexité de l'activité d'ingénierie des exigences. Cet aspect est pertinent puisque l'objectif de GOSMO est d'intégrer la gestion de la sécurité dans les premières phases de conception. De plus, une analyse conceptuelle des concepts de l'IEDB tels que but, agent, tâche et exigence est fournie avec un alignement entre les mesures de sécurité et les concepts Or-BAC. Cet alignement est guidé par le modèle de référence GORO et l'ontologie de haut niveau UFO. Ensuite, GOSMO contribue au processus de l'IE à travers la conceptualisation des buts ainsi que la capture et la spécification des mesures de sécurité.

Troisièmement, GOSMO établit un vocabulaire commun pour le partage des connaissances afin d'améliorer la communication entre les acteurs des domaines, en évitant l'hétérogénéité sémantique entre eux. En effet, l'ontologie proposée fournit une analyse terminologique complète et cohérente capable de représenter et d'analyser plusieurs situations réelles. Ensuite, les graphes des données réelles sont établis à l'aide du pattern de GOSMO sans effectuer de modifications. Cette validation justifie les critères d'adaptabilité et de flexibilité de GOSMO au regard des systèmes existants et des systèmes de demain.

Enfin, la version opérationnelle de GOSMO (implémentée en OWL) peut être utilisée pour faire une représentation des préoccupations de sécurité dans le modèle de conception du système ainsi que les éléments qui contribuent à l'occurrence du danger introduits dans DAO. En effet, le pont sémantique entre GOSMO et DAO fournit une méthodologie structurée d'analyse de sécurité et de gestion de ses décisions pour la conception des SCS. Ensuite, la formalisation OWL augmente la réutilisation de GOSMO pour d'autres domaines critiques grâce à son haut niveau d'expressivité. La validation de GOSMO à l'aide du raisonneur Pellet qui valide la cohérence de l'ontologie développée.

L'aspect adaptatif des décisions de sécurité conduit à l'évolution des exigences de sécurité et leurs relations avec les autres éléments du modèle de conception. Afin de faire face à la complexité de la gestion des exigences et leur traçabilité, nous proposons une série d'axiomes prenant en considération différents aspects de la phase de gestion des exigences. Ces axiomes sont appliqués à GOSMO et visent à fournir une base structurée pour raisonner concernant la cohérence des exigences entre elles, leur satisfaisabilité et leur traçabilité. Nous détaillons cette base structurée d'axiomes dans la section suivante.

4.7 Gestion structurée des exigences et leur traçabilité

En s'appuyant sur la taxonomie introduite par GOSMO, nous formalisons un ensemble de règles d'inférence ou d'axiomes qui permettent de vérifier certaines propriétés des exigences de sécurité et garder leur traçabilité lors du processus de gestion de sécurité. Cette structuration de la gestion de l'évolution des exigences vise à établir les relations entre les différentes niveaux des exigences et gérer les conflits entre elles. Ainsi, nous commençons par identifier les aspects à considérer dans la spécification des axiomes. La formalisation de ces axiomes représente un support de raisonnement pour GOMSO complémentaire à sa caractérisation terminologique.

4.7.1 Identification des aspects de la gestion des exigences

En tenant compte du type de relations définies entre les concepts de GOSMO et les besoins en terme de sécurité, nous identifions les aspects de gestion des exigences. Nous nous intéressons particulièrement aux exigences de sécurité et l'impact de leur évolution tout au long de la phase de conception. Afin de clarifier l'objectif à satisfaire dans chaque aspect identifié, un ensemble de questions est défini comme suit :

- **Raffinement des exigences** : Comment le raffinement des exigences est établi ? Quel est le type du but associé ?
- **Hiérarchie des exigences** : Est ce que l'exigence est de haut niveau (but) ? Est ce que l'exigence est de niveau inférieur ?
- **Satisfaisablité des exigences** : Est ce qu'une exigence est satisfaisante ?
- **Traçabilité des exigences** : Quelle est la racine de l'exigence ? Est ce que l'exigence dérive d'autres ?
- **Changements des exigences** : Comment les exigences évoluent ? Quel est l'impact de cette évolution ?
- **Relations entre les exigences et les éléments de conception** : Comment lier une exigence à un autre élément de conception ? Quel est l'impact d'évolution dans le modèle de conception ?

4.7.2 Formalisation des axiomes

Dans cette section, nous spécifions les axiomes en DL permettant de répondre aux questions prédéfinies pour satisfaire les différents aspects considérés. Ensuite, nous interprétons les axiomes et leur raisonnement au regard de l'ontologie GOSMO.

$$\textit{refinedIn} \circ \textit{refinedIn} \sqsubseteq \textit{refinedIn} \tag{4.19}$$

$$\top \sqsubseteq \neg\exists \textit{refinedIn}.\textit{Self} \tag{4.20}$$

$$\top \sqsubseteq \exists(\textit{refinedIn} \sqcap \textit{refinedIn}^{-}).\bot \tag{4.21}$$

$$\textit{Primitive} \equiv \neg\exists \textit{refinedIn}^{-}.\text{SafetyGoal} \tag{4.22}$$

$$\exists \textit{refinedIn}.\text{SafetyRequirement} \sqcap \forall \text{hasPart}.\textit{SubSafetyGoal} \sqsubseteq \text{Explicit} \tag{4.23}$$

$$\textit{TypeExplicit} \sqsubseteq \text{Explicit} \sqcap \text{Proposition} \sqcup \exists \textit{propositionalContent}.\text{Intention} \sqcup \exists \textit{propositionalContent}.\text{Desire} \tag{4.24}$$

$$\textit{Satisfiable} \equiv \exists(\textit{refinedIn}^{-} \circ \text{satisfy}^{-}).\text{SafetyGoal} \tag{4.25}$$

$$\textit{derived} \sqsubseteq \text{SafetyRequirement} \sqcap \exists \textit{refinedIn}^{-}.\text{SafetyGoal} \sqcap \exists \textit{extends}^{-}.\text{Context} \tag{4.26}$$

$$\top \sqsubseteq \leq 1 \textit{isreqRoot}.\top \tag{4.27}$$

$$\textit{hasPart} \circ \textit{refinedIn} \sqsubseteq \textit{isreqRoot} \tag{4.28}$$

$$\textit{hasPart} \circ \textit{extends} \circ \textit{refinedIn} \sqsubseteq \textit{extends} \tag{4.29}$$

$$\textit{plays} \circ \textit{partOf} \sqsubseteq \textit{allocate} \tag{4.30}$$

$$\textit{BlockTask} \sqsubseteq \exists \textit{allocate}^{-}.\textit{SystemBlocks} \tag{4.31}$$

Les Axiomes (4.19), (4.20) et (4.21) spécifient les caractéristiques de la propriété *refinedIn* pour être transitive, non réflexive et asymétrique. La relation de composition du **SafetyGoal** représentée par la propriété *PartOf* est également déclarée par les mêmes axiomes. Le processus de raffinement établit la hiérarchie des exigences partant des exigences **explicites** (**SafetyGoal**) aux exigences **primitives** de niveau inférieur (**SafetyRequirement**). Afin de distinguer chaque niveau de la hiérarchie des exigences, les exigences primitives sont considérées comme des exigences concrètes à attribuer aux acteurs du système. Autrement dit, ce sont les feuilles dans l'arbre des exigences et elles ne peuvent plus être raffinées. Les axiomes (4.22) et (4.23) permettent de raisonner à propos des concepts et des individus afin de distinguer les différents niveaux, tels que le but de haut niveau, le sous-but et l'exigence. Le type du but de haut niveau est déduit par l'axiome (4.24) pour toute exigence qui est un raffinement d'un but explicite. Un but peut être une proposition ou un contenu propositionnel d'un désir ou d'une intention. À partir des règles d'inférence, nous répondons aux requêtes formalisées sous forme de questions pour les aspects de raffinement et de la hiérarchie des exigences.

La satisfaisabilité d'une exigence de sécurité est inférée à partir de l'axiome (4.25) qui stipule la transitivité des propriétés *refined*$^-$ et *satisfy* pour toute instance d'exigence de sécurité. Nous introduisons le concept **satisfiable** qui stocke toute exigence satisfaisante si le but associé est liée à une mesure de sécurité par la propriété *satisfy*. En d'autres termes, lorsque le chemin ascendant partant de l'exigence primitive jusqu'au but explicite est établi et que ce dernier est satisfiable, la satisfaisabilité de l'exigence primitive est déduite. Cette règle d'inférence est en cohérence avec l'interprétation du concept **SafetyMeasures**, de la propriété *satisfy* ainsi que leurs axiomes introduits dans la phase de formalisation de GOSMO.

Afin de répondre aux aspects de la traçabilité des exigences, nous introduisons les Axiomes (4.26), (4.27) et (4.28). L'Axiome (4.26) considère les exigences qui sont dérivées d'autres pour accomplir une fonction du système. Ainsi, le concept **derived** est défini pour stocker toutes les exigences qui sont liées à d'autres exigences de niveaux différents et définit la relation *derive* qui a la même interprétation que celle proposée par les diagrammes des exigences SysML. De ce fait, toute exigence **derived** *extends*$^-$ un contexte spécifique. Contrairement à la relation *refinedIn* qui, par transitivité, établit un raffinement entre les exigences du même niveau où l'exigence raffinée ajoute des précisions par rapport à l'exigence principale. D'autre part, les Axiomes (4.27) et (4.28) définissent la propriété *isReqRoot* pour déduire la racine de l'exigence. Cette propriété est déclarée fonctionnelle à partir de la chaîne de rôles *hasPart* et *refinedIn* du but de sécurité associé à cette exigence.

Afin de garder la cohérence entre le exigences et les contextes associés, l'Axiome (4.29) spécifie la création de la propriété *extends* entre toute exigence **derived** ou déduite par raffinement et le nouveau contexte de dérivation. En effet, l'évolution des exigences par dérivation ou par raffinent nécessite la détermination du contexte associé qui détermine la validité de la nouvelle exigence. Mise à part les relations entre les exigences et la relation *extends*, nous proposons les Axiomes (4.30) et (4.31) pour gérer les mises à jour au niveau des éléments de conception lors de cette évolution. Ainsi, la propriété *allocate* est introduite pour allouer un bloc à la tâche dans laquelle un acteur joue un **StakeholderRole**. Le **BlockTask** représente l'ensemble des éléments de conception nécessaire pour réaliser l'exigence par le **StakeholderRole** dans sa tâche (**Task**). Afin de mettre en place et de garder la trace des évolutions dans le modèle de conception, les deux derniers axiomes indiquent que si l'acteur joue un rôle et que ce rôle est une partie de (*partOf*) la tâche, alors un bloc est alloué à cette tâche dans les blocs du système.

4.8 Synthèse

La contribution principale dans ce chapitre propose une ontologie de la gestion de la sécurité orientée par les buts (GOSMO), qui est fondée sur UFO et développée en utilisant l'approche SABiO. L'interprétation sémantique des concepts et des relations est basée sur

l'extraction des définitions fournies par les normes et l'acquisition des connaissances de domaines impliqués tels que GORE, Or-BAC et la sécurité ferroviaire. De plus, GOSMO établit un lien sémantique entre plusieurs domaines dans le but d'identifier les besoins de sécurité en terme de mesures de sécurité et les raffiner jusqu'à ce qu'à l'implémentation du formalisme Or-BAC orienté sécurité ferroviaire et l'accomplissement des exigences attendues de GOSMO.

Dans un premier temps, une réinterprétation des concepts Or-BAC est proposée pour chercher le compromis entre les définitions initiales fournies dans le contexte de la sécurité-confidentialité des systèmes d'information et les besoins en terme de sécurité ferroviaire. L'adaptation de la sémantique est établie à l'aide de l'alignement des connaissances au regard de l'ontologie de haut niveau UFO. Ce modèle de contrôle d'accès satisfait l'aspect organisationnel des systèmes ferroviaires pour gérer d'une manière structurée les décisions de sécurité. En partant des mesures de sécurité qui émanent de l'ontologie DAO proposée dans le premier chapitre, une adaptation de ces mesures au contexte dynamique des SCS est fournie en tenant compte de la satisfaction des buts de sécurité de haut niveau. Ce lien sémantique avec les concepts de l'IEDB est considéré pour intégrer ce processus de gestion de sécurité orienté but dès les premières phases de conception.

Ensuite, le modèle conceptuel de GOSMO ainsi que la formalisation en OWL sont fournis pour assurer une expressivité sémantique qui favorise une communication efficace entre les acteurs impliqués dans la phase de conception. Par ailleurs, GOSMO a été validée avec trois cas d'étude ferroviaires : deux scénarios d'accidents ferroviaires réels et une mission ferroviaire télé-opérée inspirée des futurs systèmes autonomes. Afin de gérer les évolutions des exigences de sécurité, un ensemble de règles d'inférence est fourni pour vérifier différents aspects tel que la traçabilité des exigences et leur satisfaisabilité.

CONCLUSION ET PERSPECTIVES

La conception des SCS, tels que les systèmes ferroviaires s'appuie sur la collaboration de plusieurs acteurs multi-disciplinaires pour délivrer une solution satisfaisante aux exigences fonctionnelles et non-fonctionnelles, comme la SdF. Dans le cadre de cette thèse, nous nous sommes focalisés sur l'attribut « sécurité-innocuité » qui constitue un enjeu majeur dans le cycle du développement des SCS. Nos contributions portent sur deux aspects importants liés à la conception des SCS, à savoir l'intégration de l'analyse dysfonctionnelle dans les premières phases de conception, et la gestion orientée-but des décisions de sécurité ainsi que la gestion des exigences de sécurité et leur traçabilité. Dans cette approche ontologique, nous avons commencé par étudier les besoins du contexte industriel des domaines critiques qui nous ont permis de faire converger nos choix méthodologiques. Afin de faire face aux ambiguïtés sémantiques et aux conflits de compréhension dans ce contexte de partage de connaissances, nous avons choisi de formaliser un cadre sémantique et structuré, fondé sur l'ontologie de haut niveau UFO. Il permet, d'une part, de systématiser le processus d'analyse dysfonctionnelle dans la sémantique du monde réel pour déduire les décisions de sécurité à intégrer. D'autre part, il fournit un support de raisonnement sur la gestion des décisions de sécurité dirigée par les buts de sécurité à un stade précoce de la conception. Ce cadre ontologique cohérent assistera efficacement une méthodologie d'innovation pour le développement sous contrainte de sécurité des systèmes de demain. En effet, il permet de résoudre les problèmes d'interprétation qui peuvent conduire à des choix de conception contradictoires avec les exigences de sécurité.

Afin de tirer profit des bonnes pratiques d'ingénierie ontologique, nous avons opté pour l'approche systématique SABiO du développement d'une ontologie de domaine. L'interprétation des concepts d'analyse de sécurité et de l'IEDB au regard d'UFO ainsi que l'acquisition de leurs définitions à partir des normes et des référentiels assurent l'harmonisation terminologique entre les différentes parties. Par ailleurs, la conceptualisation des connaissances en utilisant le langage de la modélisation conceptuelle, OntoUML, basé sur l'ontologie de haut niveau UFO fournit une base de communication non ambiguë. La formalisation du réseau sémantique en utilisant le langage formel d'ontologie OWL apporte l'interopérabilité sémantique et le raisonnement avec sa rigueur et sa précision. Nous avons poursuivi cette méthodologie par la vérification du cadre ontologique au regard des exigences attendues. La validation de l'aspect ferroviaire a été établie grâce à l'illustration de situations critiques des systèmes ferroviaires existants et futurs.

Dans un premier temps, nous avons proposé l'ontologie d'analyse dysfonctionnelle DAO

qui capitalise les connaissances liées aux défaillances techniques et aux erreurs humaines ainsi que leur causes et conséquences, du point de vue du système et de son environnement. Cette vue systématique d'analyse dysfonctionnelle permet de clarifier les relations entre les concepts qui contribuent à l'occurrence d'un danger pour pouvoir proposer des décisions de sécurité appropriées. La modularité du modèle conceptuel de DAO permet de raisonner sur les différents aspects techniques et humains tout en impliquant les caractéristiques cognitives de l'acteur humain et les fautes à l'origine des défaillances techniques. L'annotation ontologique des deux scénarios d'accidents ferroviaires justifie l'intérêt de DAO pour anticiper les dangers, dès les premières phases de conception, grâce à sa flexibilité et au polymorphisme de ses concepts.

Dans un deuxième temps, nous avons établi le lien sémantique de l'analyse de sécurité avec l'IEDB en développant l'ontologie de gestion de sécurité orientée-but GOSMO. Elle permet de traiter la gestion de décisions de sécurité grâce à la réinterprétation des concepts du modèle de contrôle d'accès Or-BAC d'un point de vue sécurité-innocuité. Le modèle Or-BAC, initialement conçu pour assurer la sécurité-confidentialité des systèmes d'information, a été adapté au service de la sécurité ferroviaire pour répondre à l'aspect émergent de la sécurité et à l'adaptabilité des décisions en fonction du contexte. Par ailleurs, les rôles sont affectés aux acteurs humains et aux dispositifs techniques au sein de l'organisation. À l'issue de cette affectation, des permissions sont accordées pour réaliser une tâche dans un contexte spécifique et satisfaire un but de sécurité. Ces buts de sécurité sont raffinés en exigences de sécurité pour établir une hiérarchie et garder la trace entre les différents niveaux. L'alignement des concepts d'Or-BAC avec les concepts de l'IEDB s'appuie sur la réutilisation du modèle de référence GORO qui fournit une vue interopérable des approches de l'IEDB. D'autre part, GOSMO a été validé avec des scénarios d'accidents réels de systèmes existants et de mission télé-opérée inspirée des trains du futur. Afin d'assurer la cohérence globale des exigences, un cadre structuré de gestion des évolutions des exigences et de leur traçabilité a été fourni. L'ensemble des axiomes spécifié représente un support d'inférence de nouvelles connaissances et de vérification de différents enjeux de la gestion des exigences tels que la satisfaisabilité, la traçabilité et la gestion des relations avec les éléments de conception.

À court terme, nous envisageons d'enrichir les axiomes de gestion des exigences pour considérer les autres types d'exigences et fournir un support de traçabilité de l'ensemble des exigences du système. Par ailleurs, une validation par le cas d'étude de mission télé-opérée permettra d'évaluer la cohérence entre les exigences de sécurité et les décisions de sécurité prises dans un contexte spécifique. Cet aspect reflétera l'adaptabilité des mesures de sécurité à la polyvalence des trains autonomes et à la diversification de leur environnement.

En outre, nous désirons ajouter les préoccupations fonctionnelles en plus de celles de

sécurité dans un processus avancé de spécification des exigences. L'objectif sera d'intégrer une entité organisationnelle de contrôle qui structure l'accomplissement des tâches et assure la cohérence du comportement global du système en liaison avec le formalisme de gestion de sécurité proposé par GOSMO. Cette entité s'occupera de la supervision de la satisfaction des buts fonctionnels et non-fonctionnels ainsi que de l'absence de conflits entre eux. D'autre part, le formalisme de gestion de sécurité basé sur Or-BAC, grâce à un ensemble de rôles agissant sur le comportement du système en terme de sécurité, s'intéressera au développement et à la spécification des décisions de sécurité de haut niveau. La séparation du modèle de gestion fonctionnel de celui de la sécurité facilitera l'abstraction des décisions de sécurité.

Dans GOSMO, seules les permissions ont été accordées aux activités qui implémentent les mesures de sécurité pour satisfaire les buts de sécurité. Néanmoins, le modèle Or-BAC propose d'autres types d'autorisations, tels que les interdictions, les obligations, les recommandations. Dans une prochaine étape, nous introduirons la notion d'interdiction dans GOSMO pour considérer les situations où une interdiction sur une activité est nécessaire pour empêcher le changement d'état vers un autre qui viole le but de sécurité. Cette notion représente un véritable intérêt dans le contexte opérationnel des SCS car elle évitera l'occurrence d'un état dangereux (**Hazardous State**), qui conduit à un danger tel que défini dans DAO. À la différence de la sécurité-confidentialité, la sécurité-innocuité se manifeste à ce niveau par l'activation de l'exposition au danger. Ainsi, les interdictions accordées à ce niveau permettront de couvrir les fautes et l'utilisation dangereuse.

Dans un contexte d'innovation du transport ferroviaire, nous désirons établir le lien sémantique entre les mesures de sécurité et les invariants de sécurité pour vérifier et valider la spécification des exigences, avec une méthode formelle telle que la méthode B. En effet, les invariants de sécurité représentent les propriétés qui doivent être toujours vraies en implémentant les mesures de sécurité. À partir des mesures de sécurité issues de l'analyse dysfonctionnelle, les règles de sécurité seront développées afin de mener l'ensemble des opérations à un niveau de sécurité acceptable. Ce dernier représente le niveau dans lequel les invariants de sécurité sont satisfaits. En procédant de cette manière, une première proposition intuitive sera la mise en œuvre d'un processus de synthèse de règles de sécurité qui sera transformé en un modèle formel pour vérifier ses propriétés en tenant compte des analogies suivantes :

— l'ensemble des mesures de sécurité à implémenter représente le comportement des rôles qui réalisent des opérations de sécurité,
— l'occurrence potentielle de l'état dangereux constitue la pré-condition qui déclenche l'application des règles pour amener le comportent du système au niveau de sécurité requis.
— les sous-contextes, qui sont des parties du contexte dans lequel la règle est appliquée,

correspondent à un domaine de valeurs pour des variables liées au système et à son environnement afin de structurer les interventions des rôles de sécurité.

Dans le cadre du développement des trains autonomes, il sera nécessaire d'assurer la capacité de ce processus de synthèse des règles de sécurité à garantir l'exécution des missions complexes en toute sécurité. Ces missions mettent en œuvre des fonctions critiques d'un haut niveau d'intégrité de sécurité (SIL). En effet, l'efficacité de ce processus réside dans les phases de perception du contexte et du déclenchement des interventions suivant la prise de connaissance des éléments critiques du système et de son environnement. En ce qui concerne les trains autonomes, un certain nombre de choix d'architectures ou de technologies ne sont pas encore fixés. Il est donc particulièrement judicieux de faire un raisonnement de sécurité sur les concepts de manière à fournir un ensemble de règles de sécurité qui seront adaptées aux différents contextes, états organisationnels et environnements technologiques. Le fait d'avoir très peu d'hypothèses sur le système permettrait aussi d'envisager des extensions de l'approche proposée dans le domaine de la robotique mobile ou des véhicules automobiles autonomes.

Bibliographie

[Abou EL Kalam, 2003] Abou EL Kalam, A. (2003). *Politiques et Modèles de Sécurité pour les domaines de la santé et des affaires sociales.* Thèse de doctorat, Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS-CNRS). (Cité dans les pages 9, 142 and 149.)

[Abrial, 1996] Abrial, J.-R. (1996). *The B Book-Assigning Meanings to Programs.* Cambridge University Press. (Cité dans la page 55.)

[Akers, 1978] Akers, S. B. (1978). Binary decision diagrams. *IEEE Transactions on computers*, (6):509–516. (Cité dans la page 38.)

[Alvarez-Rodríguez *et al.*, 2014] Alvarez-Rodríguez, J. M., Llorens, J., Alejandres, M. et Fuentes, J. (2014). Why avoiding how when defining what ? Towards an OSLC-based approach to support Model-Driven Requirements Engineering. *In INCOSE International Symposium*, volume 24, pages 990–1005. Wiley Online Library. (Cité dans la page 86.)

[Amari et Akers, 2004] Amari, S. V. et Akers, J. B. (2004). Reliability analysis of large fault trees using the vesely failure rate. *In Annual Symposium Reliability and Maintainability, 2004-RAMS*, pages 391–396. IEEE. (Cité dans la page 38.)

[Andrews et Henry, 1997] Andrews, J. D. et Henry, J. (1997). A computerized fault tree construction methodology. *Proceedings of the Institution of Mechanical Engineers, Part E : Journal of Process Mechanical Engineering*, 211(3):171–183. (Cité dans la page 38.)

[ANSI, EIA-632, 1999] ANSI, EIA-632 (1999). processes for engineering a system (R2003). (Cité dans la page 62.)

[Aries *et al.*, 2008] Aries, S., Le Blanc, B. et Ermine, J.-L. (2008). *MASK : une méthode d'ingénierie des connaissances pour l'analyse et la structuration des connaissances.* Hermes sciences. (Cité dans la page 74.)

[Arlat *et al.*, 1996] Arlat, J., Costes, A. et Blanquart, J.-P. (1996). *Guide de la sûreté de fonctionnement.* Cépaduès-éditions. (Cité dans la page 19.)

[Arp *et al.*, 2015] Arp, R., Smith, B. et Spear, A. D. (2015). *Building ontologies with basic formal ontology*. Mit Press. (Cité dans les pages 76 and 102.)

[Avdeenko et Pustovalova, 2015] Avdeenko, T. et Pustovalova, N. (2015). The ontology-based approach to support the completeness and consistency of the requirements specification. *In Control and Communications (SIBCON), 2015 International Siberian Conference on*, pages 1–4. IEEE. (Cité dans la page 86.)

[Badreau et Boulanger, 2014] Badreau, S. et Boulanger, J.-L. (2014). *Ingénierie des exigences : Méthodes et bonnes pratiques pour construire et maintenir un référentiel*. Dunod. (Cité dans les pages xi, 59, 60, 62 and 65.)

[Baier et Joost-Pieter, 2008] Baier, C. et Joost-Pieter, K. (2008). *Principles of model checking*. MIT press. (Cité dans la page 62.)

[Balmat *et al.*, 2009] Balmat, J.-F., Lafont, F., Maifret, R. et Pessel, N. (2009). MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor. *Ocean engineering*, 36(15-16):1278–1286. (Cité dans la page 32.)

[Baxter *et al.*, 2008] Baxter, D., Gao, J., Case, K., Harding, J., Young, B., Cochrane, S. et Dani, S. (2008). A framework to integrate design knowledge reuse and requirements management in engineering design. *Robotics and Computer-Integrated Manufacturing*, 24(4):585–593. (Cité dans les pages 86 and 88.)

[Baybutt, 2002] Baybutt, P. (2002). Layers of protection analysis for human factors (LOPA-HF). *Process Safety Progress*, 21(2):119–129. (Cité dans les pages 34 and 36.)

[Ben Ayed *et al.*, 2014] Ben Ayed, R., Collart-Dutilleul, S., Bon, P., Idani, A. et Ledru, Y. (2014). B Formal Validation of ERTMS/ETCS Railway Operating Rules. *In 4th International ABZ Conference*, pages 124–129, France. (Cité dans la page 152.)

[Ben-Ayed *et al.*, 2015] Ben-Ayed, R., Collart-Dutilleul, S., Bon, P., Ledru, Y. et Idani, A. (2015). Formalismes basés sur les rôles pour la modélisation et la validation des règles d'exploitation ferroviaires. *Technique et Science Informatiques (TSI)*, 34(5). (Cité dans la page 152.)

[Beugin *et al.*, 2016] Beugin, J., Ouedraogo, K. A., El-Koursi, E. M., Clarhaut, J., Renaux, D. et Lisiecki, F. (2016). Pratiques partagées ou divergentes d'allocation de niveaux d'intégrité de sécurité dans le domaine ferroviaire. *Congrès Lambda Mu 20 de*

Maîtrise des Risques et de Sûreté de Fonctionnement, 11-13 Octobre 2016, Saint Malo, France. (Cité dans les pages 25, 26 and 48.)

[Bijan *et al.*, 2013] Bijan, Y., Yu, J., Stracener, J. et Woods, T. (2013). Systems requirements engineering : State of the methodology. *Systems Engineering*, 16(3):267–276. (Cité dans la page 64.)

[Black et Koopman, 2009] Black, J. et Koopman, P. (2009). System safety as an emergent property in composite systems. *In 2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, pages 369–378. IEEE. (Cité dans la page 49.)

[Borgida *et al.*, 2009] Borgida, A., Ernst, N., Jureta, I. J., Lapouchnian, A., Liaskos, S. et Mylopoulos, J. (2009). Techne : A (nother) requirements modeling language. *Computer Systems Research Group. Toronto, Canada : University of Toronto*. (Cité dans les pages 66 and 145.)

[Borst, 1997] Borst, W. (1997). *Construction of Engineering Ontologies for Knowledge Sharing and Reuse*. Thèse de doctorat, University of Twente, Netherlands. (Cité dans la page 74.)

[Boudali *et al.*, 2007] Boudali, H., Crouzen, P. et Stoelinga, M. (2007). Dynamic fault tree analysis using input/output interactive markov chains. *In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*, pages 708–717. IEEE. (Cité dans la page 39.)

[Brachman et Levesque, 2004] Brachman, R. J. et Levesque, H. J. (2004). Knowledge representation and reasoning. *Morgan Kaufmann Publishers, Massachusetts, US*, 9:9. (Cité dans la page 81.)

[Bresciani *et al.*, 2004] Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F. et Mylopoulos, J. (2004). Tropos : An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3):203–236. (Cité dans la page 145.)

[Briones *et al.*, 2007] Briones, J. F., De Miguel, M. Á., Silva, J. P. et Alonso, A. (2007). Application of safety analyses in model driven development. *In IFIP International Workshop on Software Technolgies for Embedded and Ubiquitous Systems*, pages 93–104. Springer. (Cité dans la page 29.)

[Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004] Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT) (2004).

Rapport d'enquête technique sur l'accident ferroviaire survenu à Saint-Romain-En-Gier le 5 Avril 2004. (Cité dans les pages xii, 133, 134, 135 and 168.)

[Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005] Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT) (2005). Rapport d'enquête technique sur l'accident ferroviaire survenu à Longueville le 16 février 2005. (Cité dans les pages ix, xii, 127, 128, 130, 165, 205, 206, 207 and 208.)

[Burgazzi, 2004] Burgazzi, L. (2004). Evaluation of uncertainties related to passive systems performance. *Nuclear Engineering and Design*, 230(1-3):93–106. (Cité dans la page 36.)

[Cardoso, 2007] Cardoso, J. (2007). The semantic web vision : Where are we ? *IEEE Intelligent systems*, 22(5):84–88. (Cité dans la page 85.)

[Carral *et al.*, 2013] Carral, D., Scheider, S., Janowicz, K., Vardeman, C., Krisnadhi, A. A. et Hitzler, P. (2013). An ontology design pattern for cartographic map scaling. *In Extended Semantic Web Conference*, pages 76–93. Springer. (Cité dans les pages xii, 106 and 108.)

[CENELEC, NF EN 50126-1, 2017] CENELEC, NF EN 50126-1 (2017). Applications ferroviaires : Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FMDS)-partie 1. (Cité dans les pages xi, xv, 22, 23, 24, 25, 41, 43, 44, 47, 48, 49, 112 and 117.)

[CENELEC, NF EN 50128, 2011] CENELEC, NF EN 50128 (2011). Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire. (Cité dans la page 41.)

[CENELEC, NF EN 50129, 2003] CENELEC, NF EN 50129 (2003). Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement -Systèmes électroniques de sécurité pour la signalisation. (Cité dans les pages xv, 22, 24, 25, 41, 48, 49 and 97.)

[CENELEC, NF EN 50159, 2011] CENELEC, NF EN 50159 (2011). Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de communication. (Cité dans la page 41.)

[Charlet, 2003] Charlet, J. (2003). L'ingénierie des connaissances. *Développements, résultats et perspectives pour la gestion des connaissances médicales, Mémoire d'Ha-*

bilitation à Diriger des Recherches, université Pierre et Marie Curie. (Cité dans la page 70.)

[Charlet, 2004] Charlet, J. (2004). L'ingénierie des connaissances, entre science de l'information et science de gestion. (Cité dans les pages 70 and 71.)

[Charlet *et al.*, 2009] Charlet, J., Baneyx, A., Steichen, O., Alecu, I., Daniel-Le Bozec, C., Bousquet, C. et Jaulent, M.-C. (2009). Utiliser et construire des ontologies en médecine. le primat de la terminologie. *Technique et science informatiques*, 28(2):145–171. (Cité dans la page 76.)

[Chen, 2002] Chen, P. (2002). Entity-relationship modeling : historical events, future trends, and lessons learned. *In Software pioneers*, pages 296–310. Springer. (Cité dans la page 67.)

[Crawley et Tyler, 2015] Crawley, F. et Tyler, B. (2015). *HAZOP : Guide to best practice*. Elsevier. (Cité dans la page 34.)

[Cuppens et Miege, 2003] Cuppens, F. et Miege, A. (2003). Modelling contexts in the or-bac model. *In Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pages 416–425. (Cité dans la page 151.)

[Cuppens et Miège, 2004] Cuppens, F. et Miège, A. (2004). Or-bac. *Organization Based Access Control, Journées Druide, Le Croisic*. (Cité dans les pages xii and 150.)

[Cyganiak *et al.*, 2014] Cyganiak, R., Wood, D., Lanthaler, M., Klyne, G., Carroll, J. J. et McBride, B. (2014). Rdf 1.1 concepts and abstract syntax. *W3C recommendation*, 25(02). (Cité dans la page 106.)

[Dalpiaz *et al.*, 2016] Dalpiaz, F., Franch, X. et Horkoff, J. (2016). istar 2.0 language guide. *arXiv preprint arXiv :1605.07767*. (Cité dans la page 145.)

[Dardenne *et al.*, 1993] Dardenne, A., Van Lamsweerde, A. et Fickas, S. (1993). Goal-directed requirements acquisition. *Science of computer programming*, 20(1-2):3–50. (Cité dans les pages 66 and 145.)

[Davis, 2013] Davis, A. (2013). *Just enough requirements management : where software development meets marketing*. Addison-Wesley. (Cité dans les pages 58 and 67.)

[Davis *et al.*, 1993] Davis, R., Shrobe, H. et Szolovits, P. (1993). What is a knowledge representation ? *AI magazine*, 14(1):17–17. (Cité dans la page 77.)

[de Almeida Falbo, 2014] de Almeida Falbo, R. (2014). Sabio : Systematic approach for building ontologies. *In 1st Joint Workshop ONTO.COM / ODISE on Ontologies in Conceptual Modeling and Information Systems Engineering. FOIS, Rio de Janeiro.* (Cité dans les pages xi, 8, 86, 98, 100 and 110.)

[de Almeida Pereira *et al.*, 2019] de Almeida Pereira, D. I., Debbech, S., Perin, M., Bon, P. et Collart-Dutilleul, S. (2019). Formal Specification of Environmental Aspects of a Railway Interlocking System Based on a Conceptual Model. *In 38th International Conference on Conceptual Modeling (ER).* (Cité dans la page 138.)

[De Hoog *et al.*, 1993] De Hoog, R., Martil, R., Wielinga, B., Taylor, R., Bright, C. et Van De Velde, W. (1993). The Common KADS model set. *ESPRIT Project P5248 KADS-II M*, 1. (Cité dans la page 73.)

[Debbech *et al.*, 2018a] Debbech, S., Bon, P. et Collart-Dutilleul, S. (2018a). An Ontological Approach to Support Dysfunctional Analysis for Railway Systems Design (submitted). *Journal of Universal Computer Science (J.UCS).* (Cité dans les pages 75, 119 and 138.)

[Debbech *et al.*, 2018b] Debbech, S., Bon, P. et Collart-Dutilleul, S. (2018b). Improving Safety By Integrating Dysfunctional Analysis Into The Design Of Railway Systems. *WIT Transactions on The Built Environment*, 181:399–411. (Cité dans la page 97.)

[Debbech *et al.*, 2019a] Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019a). A Model-Based System Engineering Approach to Manage Railway Safety-Related Decisions. *International Journal of Transport Development and Integration*, 3(1):30–43. (Cité dans la page 168.)

[Debbech *et al.*, 2019b] Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019b). Conceptual Modelling of the Dynamic Goal-Oriented Safety Management for Safety Critical Systems. *In ICSOFT 2019-14th International Conference on Software Technologies- Volume 1*, pages 287–297. (Cité dans la page 154.)

[Debbech *et al.*, 2019c] Debbech, S., Bon, P. et Collart-Dutilleul, S. (2019c). Towards Semantic Interpretation of Goal-oriented Safety Decisions based on Foundational Ontology. *Journal of Computers*, 14(4):257–267. (Cité dans la page 154.)

[Debbech *et al.*, 2018c] Debbech, S., Collart-Dutilleul, S. et Bon, P. (2018c). Cas d'étude de mission ferroviaire télé-opérée. Rapport de recherche, IFSTTAR - Institut

Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux. (Cité dans les pages iii, 138 and 169.)

[Dentler *et al.*, 2011] Dentler, K., Cornet, R., Ten Teije, A. et De Keizer, N. (2011). Comparison of reasoners for large ontologies in the OWL 2 EL profile. *Semantic Web*, 2(2):71–87. (Cité dans la page 79.)

[Devadasan *et al.*, 2003] Devadasan, S., Muthu, S., Samson, R. N. et Sankaran, R. (2003). Design of total failure mode and effects analysis programme. *International Journal of Quality & Reliability Management*, 20(5):551–568. (Cité dans la page 31.)

[Dinmohammadi et Shafiee, 2013] Dinmohammadi, F. et Shafiee, M. (2013). A fuzzy-FMEA risk assessment approach for offshore wind turbines. *International Journal of Prognostics and Health Management*, 4(13):59–68. (Cité dans la page 32.)

[Dobson et Sawyer, 2006] Dobson, G. et Sawyer, P. (2006). Revisiting ontology-based requirements engineering in the age of the semantic web. *In Proceedings of the International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs*, pages 27–29. (Cité dans la page 86.)

[Duarte *et al.*, 2018] Duarte, B. B., Falbo, R. A., Guizzardi, G., Guizzardi, R. S. S. et Souza, V. E. S. (2018). Towards an ontology of software defects, errors and failures. *In 37th international conference on Conceptual Modeling ER 2018*. (Cité dans la page 108.)

[Duarte *et al.*, 2003] Duarte, R., Júnior, J. et A.Mota (2003). Precise Modeling with UML : Why OCL ? *In Workshop of Formal Methods*. (Cité dans la page 83.)

[Dunjó *et al.*, 2010] Dunjó, J., Fthenakis, V., Vílchez, J. A. et Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials*, 173(1-3):19–32. (Cité dans les pages 35 and 36.)

[Eizenberg *et al.*, 2006] Eizenberg, S., Shacham, M. et Brauner, N. (2006). Combining HAZOP with dynamic simulationâ[U+0080][U+0094]applications for safety education. *Journal of Loss Prevention in the Process Industries*, 19(6):754–761. (Cité dans la page 36.)

[El Ghosh *et al.*, 2017] El Ghosh, M., Abdulrab, H., Naja, H. et Khalil, M. (2017). Using the Unified Foundational Ontology (UFO) for Grounding Legal Domain Ontologies. *In KEOD*, pages 219–225. (Cité dans la page 102.)

[Ericson *et al.*, 2015] Ericson, C. A. *et al.* (2015). *Hazard analysis techniques for system safety*. John Wiley & Sons. (Cité dans la page 28.)

[Essame, 2002] Essame, D. (2002). La méthode B et l'ingénierie système. Réponse à un appel d'offre. Rapport technique, Technical report, IUT-Nantes, Université de Nantes, http ://www. iutnantes. univ-nantes. fr/habrias/dessGledn. (Cité dans la page 58.)

[Fernández-López *et al.*, 1997] Fernández-López, M., Gómez-Pérez, A. et Juristo, N. (1997). Methontology : from ontological art towards ontological engineering. (Cité dans la page 85.)

[Ferraiolo et Kuhn, 1992] Ferraiolo, D. F. et Kuhn, D. R. (1992). Role-based access controls. *In 15th National Computer Security Conference, Baltimore MD*, pages 554–563. (Cité dans la page 151.)

[Fockel et Holtmann, 2014] Fockel, M. et Holtmann, J. (2014). A requirements engineering methodology combining models and controlled natural language. *In 2014 IEEE 4th International Model-Driven Requirements Engineering Workshop (MoDRE)*, pages 67–76. IEEE. (Cité dans la page 64.)

[Galluzzo *et al.*, 1998] Galluzzo, M., Bartolozzi, V., Catiglione, L. et Taibi, G. (1998). HAST : a support system for HAZOP studies. *In Proceedings of CHISA*, volume 98. (Cité dans la page 36.)

[Gangemi *et al.*, 2006] Gangemi, A., Catenacci, C., Ciaramita, M. et Lehmann, J. (2006). Modelling ontology evaluation and validation. *In European Semantic Web Conference*, pages 140–154. Springer. (Cité dans la page 84.)

[Gangemi *et al.*, 2002] Gangemi, A., Guarino, N., Masolo, C., Oltramari, A. et Schneider, L. (2002). Sweetening ontologies with dolce. *In International Conference on Knowledge Engineering and Knowledge Management*, pages 166–181. Springer. (Cité dans la page 76.)

[Genesereth *et al.*, 1992] Genesereth, M. R., Fikes, R. E. *et al.* (1992). Knowledge interchange format-version 3.0 : reference manual. (Cité dans la page 79.)

[Giese *et al.*, 2004] Giese, H., Tichy, M. et Schilling, D. (2004). Compositional hazard analysis of UML component and deployment models. *In International Conference on Computer Safety, Reliability, and Security*, pages 166–179. Springer. (Cité dans la page 28.)

[Gilb, 2005] Gilb, T. (2005). *Competitive engineering : a handbook for systems engineering, requirements engineering, and software engineering using Planguage.* Elsevier. (Cité dans la page 55.)

[Glinz, 2011] Glinz, M. (2011). A glossary of requirements engineering terminology. *Standard Glossary of the Certified Professional for Requirements Engineering (CPRE) Studies and Exam, Version*, 1. (Cité dans les pages 56 and 144.)

[Group *et al.*, 2009] Group, O. W. *et al.* (2009). OWL 2 Web Ontology Language Document Overview : W3C Recommendation 27 October 2009. (Cité dans la page 79.)

[Gruber, 1993] Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge acquisition*, 5(2):199–220. (Cité dans les pages 8, 70, 74 and 84.)

[Gruber, 1995] Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing ? *International journal of human-computer studies*, 43(5-6):907–928. (Cité dans les pages 78 and 82.)

[Gruninger et Fox, 1994] Gruninger, M. et Fox, M. (1994). The Role of Competency Questions in Enterprise Engineering. IFIP WG5. *In 7th Workshop on Benchmarking-Theory and Practice, Trondheim, Norway.* (Cité dans la page 85.)

[Guarino, 1998] Guarino, N. (1998). *Formal ontology in information systems : Proceedings of the first international conference (FOIS'98), June 6-8, Trento, Italy*, volume 46. IOS press. (Cité dans les pages 8 and 76.)

[Guizzardi, 2005] Guizzardi, G. (2005). *Ontological foundations for structural conceptual models.* Thèse de doctorat, University of Twente, Enschede, The Netherlands. (Cité dans les pages 76, 102 and 103.)

[Guizzardi *et al.*, 2012] Guizzardi, G., Araujo Baião, F., Lopes, M. et de Almeida Falbo, R. (2012). The Role of Foundational Ontologies for Domain Ontology Engineering. *International Journal of Information System Modeling and Design*, 1(2):1–22. (Cité dans la page 8.)

[Guizzardi *et al.*, 2015] Guizzardi, G., Wagner, G., Almeida, J. P. A. et Guizzardi, R. S. (2015). Towards ontological foundations for conceptual modeling : The unified foundational ontology (UFO) story. *Applied ontology*, 10(3-4):259–271. (Cité dans les pages 102 and 103.)

[Guizzardi *et al.*, 2013] Guizzardi, G., Wagner, G., de Almeida Falbo, R., Guizzardi, R. S. et Almeida, J. P. A. (2013). Towards ontological foundations for the conceptual modeling of events. *In International Conference on Conceptual Modeling*, pages 327–341. Springer. (Cité dans la page 119.)

[Haasl, 1965] Haasl, D. F. (1965). Advanced concepts in fault tree analysis. *In System Safety Symposium*, volume 8. The Boeing Company Seattle. (Cité dans la page 38.)

[Heino *et al.*, 1988] Heino, P., Suokas, J. et Karvonen, I. (1988). An expert system in process design-analysis of process safety and reliability. *In Proceedings of the International Workshop on Artificial Intelligence for Industrial Applications*, pages 225–231. IEEE. (Cité dans la page 36.)

[Helvacioglu et Ozen, 2014] Helvacioglu, S. et Ozen, E. (2014). Fuzzy based failure modes and effect analysis for yacht system design. *Ocean Engineering*, 79:131–141. (Cité dans la page 32.)

[Herre, 2010] Herre, H. (2010). General Formal Ontology (GFO) : A foundational ontology for conceptual modelling. *In Theory and applications of ontology : computer applications*, pages 297–345. Springer. (Cité dans les pages 76 and 102.)

[Hoinaru *et al.*, 2013] Hoinaru, O., Mariano, G. et Gransart, C. (2013). Ontology for complex railway systems application to ERTMS/ETCS system. *In FM-RAIL-BOK Workshop in SEFM 2013, 11th International Conference on Software Engineering and Formal Methods*, page 6p. (Cité dans les pages 88 and 91.)

[IEC 61508, Norme Internationale, 2000] IEC 61508, Norme Internationale (2000). Sécurité fonctionnelle des systèmes électriques électroniques programmables relatifs à la sécurité. (Cité dans les pages xi, 20, 22, 24, 25, 41, 46 and 111.)

[IEC 61882, 2001] IEC 61882 (2001). Hazard and Operability Studies (HAZOP Studies)– Application Guide. (Cité dans la page 33.)

[IEC, IEC 50191, 1990] IEC, IEC 50191 (1990). Vocabulaire Elecrotechnique International, Chapitre 191-Sûreté de fonctionnement. (Cité dans la page 21.)

[IEEE 1012, 2016] IEEE 1012 (2016). Standard for System, Software, and Hardware Verification and Validation. (Cité dans la page 115.)

[IEEE 1220, 2005] IEEE 1220 (2005). IEEE Standard for Application and Management

of the Systems Engineering Process. (Cité dans les pages xi, 55 and 56.)

[IEEE 610.12, 1990] IEEE 610.12 (1990). IEEE Standard Glossary of Software Engineering Terminology. (Cité dans les pages 56, 115 and 155.)

[Iqbal *et al.*, 2013] Iqbal, R., Murad, M. A. A., Mustapha, A., Sharef, N. M. *et al.* (2013). An analysis of ontology engineering methodologies : A literature review. *Research journal of applied sciences, engineering and technology*, 6(16):2993–3000. (Cité dans la page 83.)

[ISO 10303-11, 2004] ISO 10303-11 (2004). Systèmes d'automatisation industrielle et intégration – représentation et échange de données de produits – partie 11 : Méthodes de description : Manuel de référence du langage express. (Cité dans la page 79.)

[ISO, 26262-2, 2018] ISO, 26262-2 (2018). Véhicules routiers – Sécurité fonctionnelle – Partie 2 : Gestion de la sécurité fonctionnelle. (Cité dans la page 41.)

[ISO 73 : 2009, 2009] ISO 73 : 2009 (2009). Risk management vocabulary. Std, International Organization for Standardization. (Cité dans la page 25.)

[ISO/IEC/IEEE, 29148, 2011] ISO/IEC/IEEE, 29148 (2011). ISO/IEC/IEEE 29148 : Systems and software engineering – Life cycle processes –Requirements engineering. (Cité dans la page 155.)

[Johannessen *et al.*, 2004] Johannessen, P., Törner, F. et Torin, J. (2004). Actuator based hazard analysis for safety critical systems. *In International Conference on Computer Safety, Reliability, and Security*, pages 130–141. Springer. (Cité dans la page 28.)

[Johnson, 2003] Johnson, C. (2003). A handbook of incident and accident reporting. (Cité dans la page 115.)

[Jureta *et al.*, 2009] Jureta, I. J., Mylopoulos, J. et Faulkner, S. (2009). A core ontology for requirements. *Applied Ontology*, 4(3-4):169–244. (Cité dans la page 145.)

[Kaminski et Kostylev, 2016] Kaminski, M. et Kostylev, E. V. (2016). Beyond well-designed sparql. *In 19th International Conference on Database Theory (ICDT 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. (Cité dans la page 106.)

[Kayser, 1997] Kayser, D. (1997). *La représentation des connaissances*. Hermes Paris. (Cité dans la page 74.)

[Khondoker et Mueller, 2010] Khondoker, M. R. et Mueller, P. (2010). Comparing ontology development tools based on an online survey. World Congress on Engineering 2010 (WCE 2010), London, UK. (Cité dans la page 86.)

[Kletz, 2001] Kletz, T. A. (2001). *HAZOP and HAZAN : identifying and assessing process industry hazards*. IChemE. (Cité dans la page 33.)

[Kossmann *et al.*, 2009] Kossmann, M., Gillies, A., Odeh, M. et Watts, S. (2009). Ontology-driven requirements engineering with reference to the aerospace industry. *In Applications of Digital Information and Web Technologies, 2009. ICADIWT'09. Second International Conference on the*, pages 95–103. IEEE. (Cité dans la page 86.)

[Kotek et Tabas, 2012] Kotek, L. et Tabas, M. (2012). HAZOP study with qualitative risk analysis for prioritization of corrective and preventive actions. *Procedia Engineering*, 42:808–815. (Cité dans les pages 33 and 35.)

[Kotonya et Sommerville, 1998] Kotonya, G. et Sommerville, I. (1998). Requirements engineering : processes and techniques. 1998. *J. Wiley*. (Cité dans la page 59.)

[Lanusse *et al.*, 2009] Lanusse, A., Tanguy, Y., Espinoza, H., Mraidha, C., Gerard, S., Tessier, P., Schnekenburger, R., Dubois, H. et Terrier, F. (2009). Papyrus UML : an open source toolset for MDA. *In Proc. of the Fifth European Conference on Model-Driven Architecture Foundations and Applications (ECMDA-FA 2009)*, pages 1–4. (Cité dans la page 28.)

[Laprie *et al.*, 1995] Laprie, J., Arlat, J., Blanquart, J., Costes, A., Crouzet, Y., Deswarte, Y., Fabre, J., Guillermain, H., Kaâniche, M., Kanoun, K. *et al.* (1995). *Guide de la Sûreté de Fonctionnement, 324 p.* Cépaduès Editions, Toulouse, France. (Cité dans les pages xi, 19, 20 and 22.)

[Laronde, 2011] Laronde, R. (2011). *Fiabilité et durabilité d'un système complexe dédié aux énergies renouvelables-Application à un système photovoltaïque*. Thèse de doctorat, Université d'Angers. (Cité dans les pages xi and 30.)

[Larouzée *et al.*, 2014] Larouzée, J., Guarnieri, F. et Besnard, D. (2014). *Le modèle de l'erreur humaine de James Reason*. Thèse de doctorat, MINES ParisTech. (Cité dans les pages 109 and 117.)

[Lee et Gandhi, 2005] Lee, S. W. et Gandhi, R. A. (2005). Ontology-based active requirements engineering framework. *In Software Engineering Conference, 2005. APSEC'05.*

12th Asia-Pacific, pages 8–pp. IEEE. (Cité dans la page 87.)

[Leveson, 2011] Leveson, N. (2011). *Engineering a safer world : Systems thinking applied to safety*. MIT press. (Cité dans la page 27.)

[Lewis, 2015] Lewis, R. (2015). *A semantic approach to railway data integration and decision support*. Thèse de doctorat, University of Birmingham. (Cité dans la page 87.)

[Liu, 2016] Liu, H.-C. (2016). FMEA using uncertainty theories and MCDM methods. *In FMEA using uncertainty theories and MCDM methods*, pages 13–27. Springer. (Cité dans la page 32.)

[Liu *et al.*, 2013] Liu, H.-C., Liu, L. et Lin, Q.-L. (2013). Fuzzy failure mode and effects analysis using fuzzy evidential reasoning and belief rule-based methodology. *IEEE Transactions on Reliability*, 62(1):23–36. (Cité dans la page 32.)

[Liu et Wang, 2007] Liu, S. et Wang, H. (2007). An automated approach to specification animation for validation. *Journal of Systems and Software*, 80(8):1271–1285. (Cité dans la page 62.)

[Lodgaard *et al.*, 2011] Lodgaard, E., Pellegård, Ø., Ringen, G., Klokkehaug, J. A. *et al.* (2011). Failure Mode and Effects Analysis in Combination with the Problem Solving A3. *In Proceedings of the 18th International Conference on Engineering Design (ICED 11), Impacting Society through Engineering Design, Vol. 9 : Design Methods and Tools pt. 1, Lyngby/Copenhagen, Denmark, 15.-19.08. 2011*, pages 71–79. (Cité dans la page 29.)

[Lozano-Tello et Gómez-Pérez, 2004] Lozano-Tello, A. et Gómez-Pérez, A. (2004). Ontometric : A method to choose the appropriate ontology. *Journal of Database Management (JDM)*, 15(2):1–18. (Cité dans la page 84.)

[Maalel *et al.*, 2012] Maalel, A., Mejri, L., Mabrouk, H. H. et Ghezela, H. B. (2012). Toward a knowledge management approach based on an ontology and case-based reasoning (cbr) : Application to railroad accidents. *In 2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*, pages 1–6. IEEE. (Cité dans la page 89.)

[Machado et Gomes, 2006] Machado, Renata Guanaes, M. R. B. et Gomes, J. O. (2006). Supporting the collaborative collection of user's requirements. *In Proceedings of the*

InternationalConference of Group decision and negotiation, pages 27–30. Universitat Karlsruhe, Karlsruhe, Germany. (Cité dans la page 60.)

[Machado et Gomes, 2008] Machado, Renata Guanaes, M. R. B. et Gomes, J. O. (2008). Supporting the system requirements elicitation through collaborative observations. *In Proceedings of the International Workshop of Groupware*, pages 364–379. Springer, Berlin, Heidelberg. (Cité dans la page 60.)

[Mader *et al.*, 2011] Mader, R., Griessnig, G., Leitner, A., Kreiner, C., Bourrouilh, Q., Armengaud, E., Steger, C. et Weiss, R. (2011). A computer-aided approach to preliminary hazard analysis for automotive embedded systems. *In 2011 18th IEEE International Conference and Workshops on Engineering of Computer-Based Systems*, pages 169–178. IEEE. (Cité dans la page 28.)

[Masson *et al.*, 2017] Masson, L., Guiochet, J., Waeselynck, H., Desfosses, A. et Laval, M. (2017). Synthesis of safety rules for active monitoring : application to an airport light measurement robot. *In 2017 First IEEE International Conference on Robotic Computing (IRC)*, pages 263–270. IEEE. (Cité dans la page 36.)

[Mekki, 2006] Mekki, K. S. (2006). Robust design failure mode and effects analysis in designing for six sigma. *International Journal of Product Development*, 3(3-4):292–304. (Cité dans la page 31.)

[MIL-STD, 2002] MIL-STD, M. S. (2002). 883e. (Cité dans la page 22.)

[MIL STD 882, 2002] MIL STD 882 (2002). System Safety Program for Systems ans associated subsystems and Equipement. (Cité dans la page 24.)

[Miller, 1995] Miller, G. A. (1995). Wordnet : a lexical database for english. *Communications of the ACM*, 38(11):39–41. (Cité dans la page 78.)

[Montgomery *et al.*, 1996] Montgomery, T. A., Pugh, D. R., Leedham, S. T. et Twitchett, S. R. (1996). FMEA automation for the complete design process. *In Proceedings of 1996 Annual Reliability and Maintainability Symposium*, pages 30–36. IEEE. (Cité dans la page 32.)

[Mortureux, 2005] Mortureux, Y. (2005). La sûreté de fonctionnement : méthodes pour maîtriser les risques. (Cité dans les pages 18, 19, 27, 37 and 38.)

[Musen *et al.*, 2015] Musen, M. A. *et al.* (2015). The protégé project : a look back and a

look forward. *AI matters*, 1(4):4. (Cité dans la page 86.)

[Nardi *et al.*, 2013] Nardi, J. C., de Almeida Falbo, R. et Almeida, J. P. A. (2013). Foundational ontologies for semantic integration in eai : a systematic literature review. *In Conference on e-Business, e-Services and e-Society*, pages 238–249. Springer. (Cité dans la page 8.)

[Negri *et al.*, 2017] Negri, P. P., Souza, V. E. S., de Castro Leal, A. L., de Almeida Falbo, R. et Guizzardi, G. (2017). Towards an ontology of goal-oriented requirements. *In CIbSE*, pages 469–482. (Cité dans les pages xii, 9, 76, 87, 88, 105, 117, 146 and 148.)

[Newell *et al.*, 1982] Newell, A. *et al.* (1982). The knowledge level. *Artificial intelligence*, 18(1):87–127. (Cité dans la page 72.)

[NF EN 60812, 2006] NF EN 60812 (2006). Techniques d'analyses de la fiabilité du système - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE). (Cité dans la page 29.)

[NF, EN 61513, 2013] NF, EN 61513 (2013). Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûretlé - Exigences glénlérales pour les systèmes. (Cité dans la page 41.)

[NF, ISO 21127, 2014] NF, ISO 21127 (2014). Information et documentation - une ontologie de référence pour l'échange d'informations du patrimoine culturel. (Cité dans la page 74.)

[Noy *et al.*, 2001] Noy, N. F., Sintek, M., Decker, S., Crubézy, M., Fergerson, R. W. et Musen, M. A. (2001). Creating semantic web contents with protege-2000. *IEEE intelligent systems*, 16(2):60–71. (Cité dans la page 86.)

[Nuseibeh et Easterbrook, 2000] Nuseibeh, B. et Easterbrook, S. (2000). Requirements engineering : a roadmap. *In Proceedings of the Conference on the Future of Software Engineering*, pages 35–46. ACM. (Cité dans les pages xi and 59.)

[Pinto et Martins, 2004] Pinto, H. S. et Martins, J. P. (2004). Ontologies : How can they be built ? *Knowledge and information systems*, 6(4):441–464. (Cité dans la page 84.)

[Pinto *et al.*, 2004] Pinto, H. S., Staab, S. et Tempich, C. (2004). Diligent : Towards a fine-grained methodology for distributed, loosely-controlled and evolving. *In Proceedings*

of the 16th European Conference on Artificial Intelligence (ECAI 2004), volume 110, page 393. (Cité dans la page 85.)

[Pohl, 2010] Pohl, K. (2010). *Requirements engineering : fundamentals, principles, and techniques*. Springer Publishing Company, Incorporated. (Cité dans la page 67.)

[Price *et al.*, 1995] Price, C. J., Pugh, D. R., Wilson, M. S. et Snooke, N. (1995). The flame system : automating electrical failure mode and effects analysis (FMEA). *In Annual Reliability and Maintainability Symposium 1995 Proceedings*, pages 90–95. IEEE. (Cité dans la page 32.)

[Provenzano *et al.*, 2017] Provenzano, L., Hanninen, K., Zhou, J. et Lundqvist, K. (2017). An ontological approach to elicit safety requirements. *In 2017 24th Asia-Pacific Software Engineering Conference (APSEC)*, pages 713–718. IEEE. (Cité dans la page 90.)

[Raiteri *et al.*, 2004] Raiteri, D. C., Franceschinis, G., Iacono, M. et Vittorini, V. (2004). Repairable fault tree for the automatic evaluation of repair policies. *In International Conference on Dependable Systems and Networks, 2004*, pages 659–668. IEEE. (Cité dans la page 40.)

[Rauzy, 2002] Rauzy, A. (2002). Mode automata and their compilation into fault trees. *Reliability Engineering & System Safety*, 78(1):1–12. (Cité dans la page 38.)

[Reason, 1987] Reason, J. (1987). Generic error-modelling system (gems) : A cognitive framework for locating common human error forms. *New technology and human error*, 63:86. (Cité dans la page 117.)

[Règlement d'exécution, 402/2013/UE, 2013] Règlement d'exécution, 402/2013/UE (2013). Méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques d'un système ferroviaire, Commission Européenne, modifications apportés dans le règlement d'exécution 2015/1136 au 13 juillet. (Cité dans la page 45.)

[Rehman et Kifor, 2016] Rehman, Z. et Kifor, C. V. (2016). An ontology to support semantic management of fmea knowledge. *International Journal of Computers, Communications & Control*, 11(4). (Cité dans la page 90.)

[Ren et Kong, 2011] Ren, Y. et Kong, L. (2011). Fuzzy multi-state fault tree analysis based on fuzzy expert system. *In The Proceedings of 2011 9th International Conference*

on Reliability, Maintainability and Safety, pages 920–925. IEEE. (Cité dans la page 39.)

[Rothenberg *et al.*, 1989] Rothenberg, J., Widman, L. E., Loparo, K. A. et Nielsen, N. R. (1989). The nature of modeling. *in Artificial Intelligence, Simulation and Modeling*. (Cité dans la page 64.)

[Ruijters et Stoelinga, 2015] Ruijters, E. et Stoelinga, M. (2015). Fault tree analysis : A survey of the state-of-the-art in modeling, analysis and tools. *Computer science review*, 15:29–62. (Cité dans la page 39.)

[Sandberg *et al.*, 2010] Sandberg, A., Chen, D., Lönn, H., Johansson, R., Feng, L., Törngren, M., Torchiaro, S., Tavakoli-Kolagari, R. et Abele, A. (2010). Model-based safety engineering of interdependent functions in automotive vehicles using EAST-ADL2. *In International Conference on Computer Safety, Reliability, and Security*, pages 332–346. Springer. (Cité dans la page 28.)

[Sango *et al.*, 2015] Sango, M., Hoinaru, O., Gransart, C. et Duchien, L. (2015). A temporal qos ontology for ertms/etcs. *International Journal of Computer, Information, Systems and Control Engineering*, 9(1):7. (Cité dans les pages 89 and 91.)

[Schenck et Wilson, 1994] Schenck, D. A. et Wilson, P. R. (1994). *Information modeling the EXPRESS way*. Oxford University Press. (Cité dans la page 79.)

[Schön, 2014] Schön, W., L. G. M. G. e. P. J. (2014). *Signalisation et automatismes ferroviaires Tome 3*. La vie du rail. (Cité dans la page 152.)

[Schulz, 2018] Schulz, S. (2018). The role of foundational ontologies for preventing bad ontology design. *In 10th Formal Ontology in Information Systems conference (FOIS)*. (Cité dans la page 8.)

[SE Handbook Working INCOSE and others, 2011] SE Handbook Working INCOSE and others (2011). INCOSE systems engineering handbook v. 3.2. 2. Rapport technique, INCOSE. (Cité dans les pages 63 and 64.)

[Siegemund *et al.*, 2011] Siegemund, K., Thomas, E. J., Zhao, Y., Pan, J. et Assmann, U. (2011). Towards ontology-driven requirements engineering. *In Workshop semantic web enabled software engineering at 10th international semantic web conference (ISWC), Bonn*. (Cité dans les pages 86 and 88.)

[Simperl et Luczak-Rösch, 2014] Simperl, E. et Luczak-Rösch, M. (2014). Collabora-

tive ontology engineering : a survey. *The Knowledge Engineering Review*, 29(1):101–131. (Cité dans la page 85.)

[Simperl *et al.*, 2009] Simperl, E., Mochol, M., Bürger, T. et Popov, I. O. (2009). Achieving maturity : the state of practice in ontology engineering in 2009. *In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 983–991. Springer. (Cité dans la page 85.)

[Sommerville, 2013] Sommerville, I. (2013). *Software Engineering : Pearson New International Edition*. Pearson Education Limited. (Cité dans la page 58.)

[Sowa, 2014] Sowa, J. F. (2014). *Principles of semantic networks : Explorations in the representation of knowledge*. Morgan Kaufmann. (Cité dans la page 74.)

[Stamatelatos *et al.*, 2002] Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J. et Railsback, J. (2002). Fault tree handbook with aerospace applications. (Cité dans la page 38.)

[STAN 00-56, 1996] STAN 00-56 (1996). Safety management requirements for defence systems, uk ministry of defence, defence standard 00-56. (Cité dans la page 25.)

[Stringfellow *et al.*, 2010] Stringfellow, M. V., Leveson, N. G. et Owens, B. D. (2010). Safety-driven design for software-intensive aerospace and automotive systems. *Proceedings of the IEEE*, 98(4):515–525. (Cité dans la page 28.)

[Stuckenschmidt *et al.*, 2009] Stuckenschmidt, H., Parent, C. et Spaccapietra, S. (2009). *Modular ontologies : concepts, theories and techniques for knowledge modularization*, volume 5445. Springer. (Cité dans la page 82.)

[Studer *et al.*, 1998] Studer, R., Benjamins, V. R. et Fensel, D. (1998). Knowledge engineering : principles and methods. *Data & knowledge engineering*, 25(1-2):161–197. (Cité dans la page 74.)

[Suárez-Figueroa *et al.*, 2012] Suárez-Figueroa, M. C., Gómez-Pérez, A. et Fernández-López, M. (2012). The NeOn methodology for ontology engineering. *In Ontology engineering in a networked world*, pages 9–34. Springer. (Cité dans la page 85.)

[Summers, 1998] Summers, A. E. (1998). Techniques for assigning a target safety integrity level. *ISA transactions*, 37(2):95–104. (Cité dans la page 25.)

[Sure *et al.*, 2004] Sure, Y., Staab, S. et Studer, R. (2004). On-to-knowledge methodology (otkm). *In Handbook on ontologies*, pages 117–132. Springer. (Cité dans la page 85.)

[Swain et Guttmann, 1983] Swain, A. D. et Guttmann, H. E. (1983). Handbook of human-reliability analysis with emphasis on nuclear power plant applications. final report. Rapport technique, Sandia National Labs. (Cité dans la page 34.)

[Taylor, 1982] Taylor, J. (1982). An algorithm for fault-tree construction. *IEEE Transactions on Reliability*, 31(2):137–146. (Cité dans la page 40.)

[Trammell *et al.*, 2004] Trammell, S. R., Lorenzo, D. K. et Davis, B. J. (2004). Integrated hazards analysis. *Professional Safety*, 49(5):29. (Cité dans la page 35.)

[Tueno *et al.*, 2017] Tueno, S., Laleau, R., Mammar, A. et Frappier, M. (2017). Towards using ontologies for domain modeling within the sysml/kaos approach. *In 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, pages 1–5. IEEE. (Cité dans les pages 87 and 88.)

[Tutcher, 2014] Tutcher, J. (2014). Ontology-driven data integration for railway asset monitoring applications. *In 2014 IEEE International Conference on Big Data (Big Data)*, pages 85–95. IEEE. (Cité dans les pages 87 and 91.)

[UIC RailTopoModel, 2016] UIC RailTopoModel (2016). Railway Network Description. Rapport technique, International Union Of Railways. (Cité dans les pages 88 and 91.)

[UML, OMG, 2003] UML, OMG (2003). 2.0 superstructure final adopted specification. (Cité dans les pages 55, 65 and 67.)

[Uschold, 1995] Uschold, M. (1995). King. m. towards a methodology for building ontologies. *In Proceedings of the IJCAI-95 Workshop on Basic Ontological Issues in Knowledge Sharing, Montreal, Canada*. (Cité dans la page 85.)

[Vaidhyanathan et Venkatasubramanian, 1996] Vaidhyanathan, R. et Venkatasubramanian, V. (1996). A semi-quantitative reasoning methodology for filtering and ranking hazop results in hazopexpert. *Reliability Engineering & System Safety*, 53(2):185–203. (Cité dans la page 36.)

[Van Gulijk *et al.*, 2015] Van Gulijk, C., Hughes, P., Figueres-Esteban, M., Dacre, M. et Harrison, C. (2015). Big data risk analysis for rail safety ? *In Proceedings of*

ESREL 2015. CRC/Balkema. (Cité dans les pages 87 and 91.)

[Van Lamsweerde, 2001] Van Lamsweerde, A. (2001). Goal-oriented requirements engineering : A guided tour. *In Requirements Engineering, 2001. Proceedings. 5th IEEE International Symposium on Requirements Engineering (RE'01)*, pages 249–262. IEEE. (Cité dans les pages 66, 144 and 145.)

[Vaurio, 2002] Vaurio, J. K. (2002). Treatment of general dependencies in system fault-tree and risk analysis. *IEEE Transactions on Reliability*, 51(3):278–287. (Cité dans la page 40.)

[Verstichel *et al.*, 2007] Verstichel, S., Van Hoecke, S., Strobbe, M., Van den Berghe, S., De Turck, F., Dhoedt, B., Demeester, P. et Vermeulen, F. (2007). Ontology-driven middleware for next-generation train backbones. *Science of Computer Programming*, 66(1):4–24. (Cité dans la page 89.)

[Villemeur, 1988] Villemeur, A. (1988). Sûreté de fonctionnement des systèmes industriels : fiabilité-facteurs humains, informatisation. (Cité dans les pages 18, 19, 21 and 32.)

[Vogel, 1988] Vogel, C. (1988). *Génie cognitif*. Masson. (Cité dans la page 73.)

[Walker et Papadopoulos, 2009] Walker, M. et Papadopoulos, Y. (2009). Qualitative temporal analysis : Towards a full implementation of the Fault Tree Handbook. *Control Engineering Practice*, 17(10):1115–1125. (Cité dans la page 38.)

[Wang *et al.*, 2002] Wang, Y., Teague, T., West, H. et Mannan, S. (2002). A new algorithm for computer-aided fault tree synthesis. *Journal of Loss Prevention in the Process Industries*, 15(4):265–277. (Cité dans la page 38.)

[Wang *et al.*, 2009] Wang, Y.-M., Chin, K.-S., Poon, G. K. K. et Yang, J.-B. (2009). Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean. *Expert systems with applications*, 36(2):1195–1207. (Cité dans la page 31.)

[Xing, 2007] Xing, L. (2007). Reliability evaluation of phased-mission systems with imperfect fault coverage and common-cause failures. *IEEE Transactions on Reliability*, 56(1):58–68. (Cité dans la page 38.)

[Yangui, 2016] Yangui, R. (2016). *Modélisation UML/B pour la validation des exigences de sécurité des règles d'exploitation ferroviaires*. Thèse de doctorat, Ecole centrale de Lille. (Cité dans la page 152.)

[Yu, 2011] Yu, E. (2011). Modelling strategic relationships for process reengineering. *Social Modeling for Requirements Engineering*, 11:2011. (Cité dans les pages 66, 87, 88 and 144.)

[Zang *et al.*, 2003] Zang, X., Wang, D., Sun, H. et Trivedi, K. S. (2003). A BDD-based algorithm for analysis of multistate systems with multistate components. *IEEE Transactions on computers*, 52(12):1608–1618. (Cité dans la page 39.)

[Zhi, 2000] Zhi, J. (2000). Ontology-based requirements elicitation. *Chinese Journal of Computers*, 5:5. (Cité dans la page 86.)

[Zhou *et al.*, 2015] Zhou, J., Hanninen, K., Lundqvist, K., Lu, Y., Provenzano, L. et Forsberg, K. (2015). An environment-driven ontological approach to requirements elicitation for safety-critical systems. *In 2015 IEEE 23rd International Requirements Engineering Conference (RE)*, pages 247–251. IEEE. (Cité dans la page 90.)

[Zhou *et al.*, 2017] Zhou, J., Hänninen, K., Lundqvist, K. et Provenzano, L. (2017). An ontological approach to hazard identification for safety-critical systems. *In 2017 Second International Conference on Reliability Systems Engineering (ICRSE)*, pages 1–7. IEEE. (Cité dans les pages 90 and 112.)

[Zhou *et al.*, 2002] Zhou, L., Booker, Q. E. et Zhang, D. (2002). Rod-toward rapid ontology development for underdeveloped domains. *In Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pages 957–965. IEEE. (Cité dans la page 86.)

Annexe A

Fonctionnement de la serrure de réversibilité et du système de freinage [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005]

Dans le cas d'un train constitué par une rame réversible, le conducteur se trouve évidemment toujours en tête, soit dans la locomotive –qui est menante- (cas de l'accident de Longueville), soit dans la cabine de conduite de la voiture pilote - la locomotive se situant en queue (locomotive menée). La locomotive concernée, du type « BB 66400 » a présenté un défaut au niveau de sa serrure mécanique de réversibilité qui n'a pas été verrouillée en position opérationnelle de marche. Les vibrations de l'engin ont alors provoqué une rotation de l'axe de cette serrure de réversibilité. Ce qui a entraîné l'inhibition de la commande du frein.

Les consignes de freinage ainsi que l'énergie de freinage sont acheminées à la commande du frein de chaque véhicule à l'aide d'une conduite pneumatique dite « conduite générale » (CG). Le conducteur peut régler la pression CG en tête grâce à un « robinet du mécanicien » en service, soit dans la locomotive (robinet de type « H7A »), soit dans la cabine de la voiture pilote (robinet à commande électrique de type « PBA2 SH »). L'action du robinet de mécanicien « H7A » est purement mécanique. La figure A.1, extraite du rapport [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005], montre le principe du fonctionnement du robinet de frein du mécanicien « H7A » de la locomotive. La poignée amovible tourne autour d'un axe vertical et établit les communications pneumatiques pour chaque position repérée qui correspond à une commande de freinage du train. Le « réservoir égalisateur », d'un petit volume d'air, donne la possibilité au conducteur d'ajuster avec précision la dépression dans la conduite générale CG. La pression de la CG se cale sur le niveau de celle produite dans le réservoir égalisateur.

Le robinet de frein H7A est manœuvré à l'aide d'une poignée amovible qui peut s'enclencher sur une serrure permettant de connecter le robinet de frein du mécanicien à la CG ou au contraire le déconnecter. La connexion du robinet de frein du mécanicien à

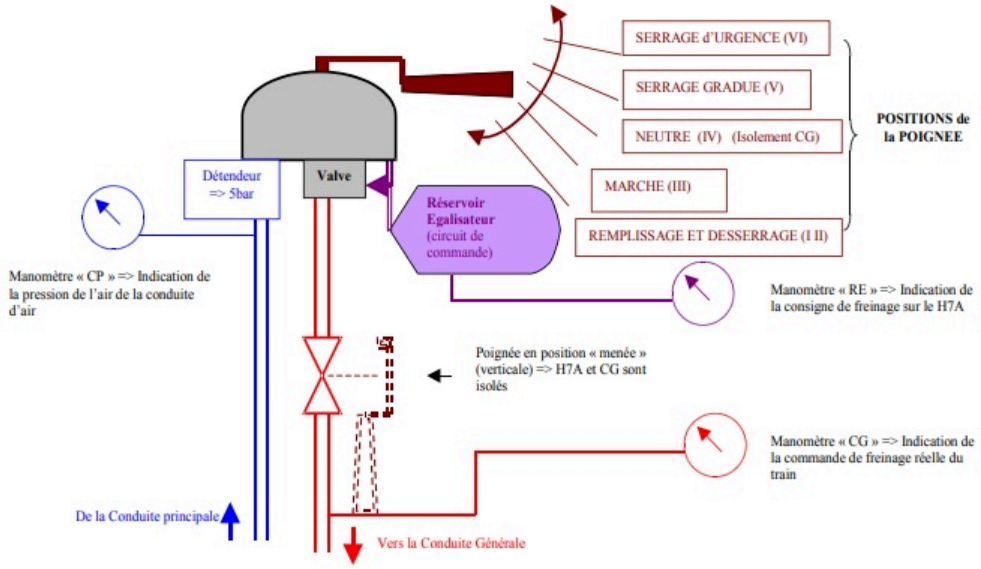

Figure A.1 – Fonctionnement du robinet de frein du mécanicien « H7A »

la CG confère à ce robinet le statut d'organe de commande du frein de tout le train. La déconnexion de ce robinet par rapport à la CG ôte à ce robinet toute fonction active ; la locomotive se comporte alors, du point de vue du frein, comme un simple véhicule remorqué de queue.

Les étapes s'enchaînent comme suit pour mettre le poste de conduite de la locomotive en position « menante » :

- Étape (0) : la poignée amovible est en position verticale sur la serrure ZG, bloquée par la barrette de retenue (position locomotive menée).
- Étape (1) : Pivotement de 90° autour de l'axe ZG pour libérer la poignée de la barrette de retenue.
- Étape (2) : Libération de la poignée de la serrure ZG.
- Étape (3) : Mise en place de la poignée sur le robinet de frein H7A.

Lorsque la locomotive est en configuration « menée » (acheminée en véhicule dans un train, poussant le train en réversibilité ou participant en unité multiple à la traction d'un train), la poignée amovible est en positon verticale et verrouillée par la barrette de retenue qui en interdit le retrait. Lorsque la locomotive est en configuration « menante », la poignée amovible a été d'abord positionnée à l'horizontale pour pouvoir être retirée de l'axe carré de la serrure. Cette poignée est ensuite enfilée sur l'axe vertical du robinet de frein du mécanicien « H7A », l'axe de la serrure restant en position « menante » (voir Annexe 6 du rapport [Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2005]).

Ontologies pour la gestion de sécurité ferroviaire : Intégration de l'analyse dysfonctionnelle dans la conception

Résumé : La sécurité-innocuité est une propriété émergente des systèmes critiques de sécurité (SCS), notamment les systèmes ferroviaires. Cet aspect émergent complexifie leur processus du développement et nécessite un raisonnement judicieux permettant de diminuer les dangers. Cette thèse propose une approche ontologique qui intègre les activités de sécurité dès les premières phases de conception des SCS. Ce cadre structuré offre une harmonisation sémantique entre les domaines impliqués, tels que l'ingénierie de sécurité et l'Ingénierie des Exigences Dirigée par les Buts (IEDB). La logique métier intégrée dans cette approche est validée par des cas d'étude ferroviaires d'accidents réels et d'une mission télé-opérée. Dans un premier temps, nous avons proposé une ontologie d'analyse dysfonctionnelle, appelée DAO et fondée sur l'ontologie de haut niveau UFO. DAO considère les aspects sociaux-techniques et environnementaux des SCS et intègre les différents types de fautes et de propriétés cognitives liés respectivement aux défaillances techniques et aux erreurs humaines. Le modèle conceptuel de DAO est exprimé en OntoUML et formalisé en langage OWL afin de fournir un support de raisonnement. Ensuite, un pont sémantique est établi entre les mesures de sécurité, les buts de sécurité et les exigences de sécurité par le développement d'une ontologie de gestion de sécurité orientée-but, appelée GOSMO. La gestion des décisions de sécurité s'appuie sur la réinterprétation du modèle de contrôle d'accès Or-BAC d'un point de vue sécurité-innocuité. Afin d'assurer la cohérence globale des exigences, GOSMO permet de structurer la gestion des évolutions des exigences et leur traçabilité.

Mots clés : Sécurité ferroviaire, Analyse dysfonctionnelle, ontologie, IEDB, Modélisation conceptuelle, UFO, OWL, Modèle Or-BAC.

Ontologies for railway safety management : integration of the dysfunctional analysis into the design

Abstract : Safety is an emergent property of safety critical systems (SCS), including railway systems. This emergent aspect exacerbates their development process and requires a thorough reasoning to reduce hazards. This thesis proposes an ontological approach that integrates safety activities from the early design stages of SCS. This structured framework provides a semantic harmonization between the involved domains, such as safety engineering and Goal Oriented Requirements Engineering (GORE). The business logic integrated in this approach is validated by real rail accident scenarios and a remotely operated task. At first, we proposed a dysfunctional analysis ontology called DAO and grounded in the high-level ontology UFO. DAO considers the socio-technical and environmental aspects of SCS and integrates the different types of faults and cognitive properties that are respectively related to technical failures and human errors. The DAO conceptual model is expressed in OntoUML and formalized in OWL language in order to provide a reasoning support. Then, a semantic bridge is established between safety measures, safety goals and safety requirements through the development of a goal-oriented security management ontology, called GOSMO. The management of safety decisions is based on the reinterpretation of the Or-BAC access control model from a safety point of view. In order to ensure the overall consistency of requirements, GOSMO allows structuring the management of requirements changes and their traceability.

Keywords : Railway safety, Dysfunctional analysis, ontologies, GORE, Conceptual modeling, UFO, OWL, Or-BAC model.