Towards Semantic Interpretation of Goal-Oriented Safety Decisions Based on Foundational Ontology

Sana Debbech, Philippe Bon, Simon Collart-Dutilleul

Towards Semantic Interpretation of Goal-Oriented Safety Decisions Based on Foundational Ontology

Sana Debbech*, Philippe Bon, Simon Collart-Dutilleul
Université de Lille/ Nord de France, IFSTTAR/COSYS/ESTAS, 59655, Lille, France.

* Corresponding author. Tel.: +33(0)320438407; email: sana.debbech@ifsttar.fr
Manuscript submitted January 15, 2019; accepted April 10, 2019.
doi: 10.17706/jcp.14.4.257-267

Abstract: Semantic interpretation of a knowledge domain is usually required to provide and formalize its common vocabulary. This task is challenging in the context of Safety Critical Systems (SCSs) development, since it involves both safety and design teams. In the railway domain, there is a lack of a common vocabulary aiming to avoid ambiguities in the safety-related decisions to satisfy goals. To cope with the complexity of this task, the aim of this study is to propose a semantic interpretation of the safety rules development process from a goal-oriented perspective. The safety rules development process is performed according to the Organization-Based Access Control (Or-BAC) model, which is normally used for the information systems security. The proposed approach is based on a foundational ontology in order to interpret safety-related concepts in real-world semantics. It provides relations between safety-related concepts and Unified Foundational Ontology (UFO) concepts. Furthermore, the matching between safety rules, Or-BAC and Goal-Oriented Requirements Engineering (GORE) concepts is considered and formalized in a structured way. The proposed interpretation is evaluated and progressively justified regarding the railway domain knowledge and the current literature.

Key words: Foundational ontology, GORE, knowledge domain, Or-BAC, railway systems, safety, semantic interpretation.

1. Introduction

The combination between two or more knowledge domains to accomplish an intended task requires a common vocabulary to provide a shared view between them. In this context, the integration of safety conditions, as early as possible, into the Safety-Critical Systems (SCSs) design process involves safety analysts, design actors and domain experts [1]. Hence, there is a need to provide a conceptual model of both dysfunctional analysis and safety rules development based on foundational concepts.

In a current work, we are proposing a reference ontology of dysfunctional analysis for SCSs. The obtained conceptual model is grounded in Unified Foundational Ontology (UFO) [2], which is a top-level ontology, to provide a real-world semantics. The highlighted safety measures in the dysfunctional analysis process must be linked to Goal-Oriented Requirement Engineering (GORE) in order to satisfy safety goals.

Railway systems, as socio-technical systems, require thorough safety-related decisions based on standards [3] and System Requirements Specification (SRS) [4]. In [5], authors proposed an approach based on Role-Based Access Control (R-BAC) [6] and Organization-Based Access Control (Or-BAC) [7] in order to help the railway operating rules modeling. However, the concepts used in this work such as role, user and action, are inspired by the information systems security. Hence, there is a need to interpret these

concepts according to the railway safety knowledge and the goal-oriented perspective.

In this study, we formalize a semantic interpretation of safety rules development related to GORE concepts such as goal and agent. The aim of this paper is to propose a common vocabulary to ensure the clarity, the completeness and the non-ambiguity of these concepts. This paper does not consider a thorough quantitative analysis to evaluate the conceptual model quality. The proposed interpretation is grounded in UFO, since this foundational ontology provides a wide set concepts, that are interesting to our work. Furthermore, the interpretation is performed in real-world semantics in order to obtain a reference conceptual model with a multi-shared view. This aspect is important since it combines several domain-specific views and it is suitable for our context.

This paper is structured as follows: Section 2 defines the problematic and the background of this study. Section 3 presents the proposed semantic interpretation and the formalization of relevant concepts for this study to satisfy some competency questions (CQs) defined in advance. Railway examples are considered to incrementally evaluate and illustrate the proposed interpretation. Finally, Section 4 concludes the paper and presents some perspectives.

2. Background

For the railway safety community, current practices to extract or integrate safety conditions suffer from several drawbacks such as:

a) The lack of semantic interpretation to assist the safety reasoning based on goal-oriented concepts,
b) The lack of a common vocabulary to provide a multi-view conceptual model,
c) The lack of a reference model grounded in well-founded ontology to link safety and GORE concepts.

Several industrial and academic projects, in the railway domain, have been made in order to formalize systems and improve railway safety. The aim of the Perfect project [8] was the validation of ERTMS operating rules through the B formal method and illustrated by a case study from the high-speed railway line LGV-EST. Moreover, it provided the modeling of these rules based on RBAC. Then, this study was extended in the Nextregio project with the aim to formalize and implement the ERTMS regional system for the low single-track traffic safety.

Nevertheless, they did not consider the expression of safety rules with a high level of abstraction in a structured way and from a goal-oriented view.

In order to anticipate safety problems as well as accidents, some assumptions have to be considered, in this study, to fill the gaps mentioned above. The first assumption considers that safety conditions must be defined according to a specific context to satisfy a given goal. Then, the realization of these safety rules is based on the assignment of a set of roles to actors respecting specific context constraints. Here, a matching between Or-BAC concepts, GORE concepts and UFO concepts is required to satisfy railway domain requirements.

In the next section, we present the well-founded ontology chosen in this study to interpret concepts in real-world semantics. Then, we define briefly the GORE concepts and their utility for this study.

2.1. The Unified Foundational Ontology (UFO)

Ontology is defined as *an explicit specification of a conceptualization* [9]. It provides a structured and an explicit representation of a knowledge domain. In recent years, ontologies have been widely used in several domains in order to provide their conceptual models. Besides, foundation ontologies (known as upper ontologies) provide a set of foundational concepts and relations between them with the aim to obtain a reference model of a knowledge domain.

Comparing it with other foundational ontologies such as GFO [10] and BFO [11], UFO proposes a complete set of concepts to cover important aspects of the safety rules development and GORE concepts. The benefit of using UFO consists in the observation of entities from a uniform perspective in real world.

Furthermore, UFO is the most foundational ontology used in conceptual modeling and this aspect increases the reusability of our work. Therefore, the proposed interpretation is grounded in UFO in order to provide a common vocabulary and to improve the safety-decision based on GORE concepts through a reference model.

The other advantage to use the foundational ontology UFO in this study consists in providing a multi-view interpretation and modeling with a common vocabulary. The (Unified Modeling Language) UML profile fragment presented in Fig. 1 illustrates the UFO foundational concepts suitable for this study. This UML profile (called Onto-UML) is an UML extension defining a conceptual modeling language based on UFO [2].

In this fragment, rectangles represent concepts, lines and arrows "▶" define associative relations. The subsumption relationship represented by "a white arrow" links the sub-concept to its super-concept.

In the remainder of this paper, we use this representation to illustrate the interpretation of concepts and relations between them. The full description of UFO concepts may be found in [2]. The proposed concepts related to safety rules development are presented in Section 3. In this paper, concepts are presented in bold.

UFO distinguishes two types of entities: **Individual** and **Universal**. The former is an entity with a unique identity and existing in reality (such as a person and a train). The latter denotes a pattern of features existing in a set of **Individuals**. For instance, the **Universal** *train passenger* instantiates the **Individual** *train*.

Endurant is a sub-type of **Individual**, it represents an entity with a unique identity and is maintaining it in time. A **Situation** is an **Endurant** which represents a state of affairs in reality and it is established by one or more **Endurants**. A **Moment** is existentially dependent on the presence of many **Endurants**.

Substantial is an **Endurant**, which is existentially independent of other endurants. **Substantial** is classified in two types: **Agent** and **Object**, which are more related to our work. An **Agen**t is an **Individual** existing in reality with a unique identity stable over time and existentially independent. Contrarily, **Object** represents every particular **Substantial** non-agentive.

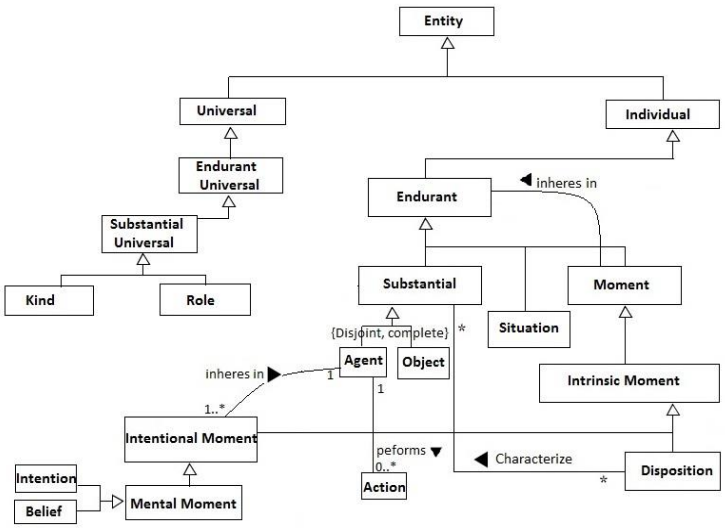

Fig. 1. UML fragment of UFO showing individuals and universals.

In the same level, the **Substantial Universal** entity is specialized into **Kind** and **Role** based on ontological aspects of rigidity and identity [2]. A **Kind** denotes a **Substantial Universal** with rigidity, keeping its identity in every situation. For instance, a person is a **Kind** with a unique identity. In contrast,

Role denotes non-rigid universals. For instance, a driver is a **Role** until next mission. In other words, a person (**Kind**) plays a driver **Role** while she/he is in the train. So a **Role** instantiates a **Kind** in some specific situations according to some constraints.

These two concepts are suitable for the safety rules development in railway domain since it is based on user roles to perform an action. The interpretation of these concepts and their adaptation to our context is presented in Section 3.

The second part of this study consists in the interpretation of the relation between safety rules and GORE concepts grounded in well-founded ontology, i.e., Goal-Oriented Requirements Ontology (GORO) [12]. The next section introduces relevant concepts in GORO.

2.2. Goal-Oriented Requirements Ontology (GORO)

The goal-oriented Requirements Ontology (GORO) [12] is a reference model grounded in UFO and providing a formal semantics to allow the interoperability between existing GORE approaches, such as i* framework [13], KAOS [14] and Techne [15]. As the main characteristic of foundational ontologies is the reusability, GORO is interesting to our work in order to provide a common vocabulary between safety concepts and GORE concepts.

In this paper, only the GORO fragment related to **Goals** and **Agent's mental moments** is considered. Intuitively, a goal denotes declarative statements intended to be achieved. A **Mental Moment** is an **Intentional Moment** characterizing an **Agent**. It is existentially dependent on one **Individual** (intrinsic), and it is intentional (inheres in **Agent**) [11]. It is classified into **Intentions**, **Beliefs** and **Desires**. In GORO, a **Goal** is a propositional content of an **Intention** or a **Desire** [11]. A **Desire** is the aim of the agent towards a specific situation in reality. An **Intention** represents the aim of the agent and the associated **Plan** to accomplish it. More details about GORO may be found in [11].

We interpret these concepts using as definition the first order language $\mathcal{L}$, as natural language is not the aim of this study.

Definition 1. (Goal). Let *G, I, D, P* be respectively a set of goals, intentions, desires and plans, and *R* a set of relations:

- "x Propositional Content of y" is represented by *Prop_ Cont (x,y)* ∈ *R,*
- "x is assigned to y" is represented by *assignment(x,y)* ∈ *R,*

Such that:

$$\forall g\ (\exists i\ \exists d\ (\text{Prop-Cont(g,i)} \vee \text{Prop-Cont(g,d)}) \wedge \exists p\ ((\text{Prop-Cont(g,i)} \rightarrow \text{assignement(p,g)}))$$

Moreover, according to GORO, a **Goal** is a sub-type of a **Proposition** when it is based on **Agent's assumption.** This situation is possible when the agent becomes a stakeholder and believes that a situation in the environment is true [11]. Therefore, an **Assumption**, as a propositional content of a **Belief**, can be wrong and lead, in this case, to accidents. These aspects are suitable for this study since the safety rules elicitation can be performed based on **Agent's assumptions**.

The proposed interpretation of these concepts for the railway safety domain and its justification are defined in the next section.

3. The Proposed Semantic Interpretation

The main contribution of this study consists in a semantic interpretation of concepts in order to propose a conceptual model of safety rules development. This paper does not consider a thorough quantitative analysis to evaluate the conceptual model quality. Nevertheless, the evaluation may be performed along three interesting dimensions: syntax, semantics and pragmatics. These aspects are discussed in Section 3.4.

Moreover, some metrics and attributes could be introduced to quantify the obtained model such as the reusability, the completeness and the expressiveness. This model quantification will be the subject of future work.

In order to provide a common vocabulary for safety-decision from a goal-oriented view, there is a need to define a uniform interpretation of safety related concepts. As information systems and railway systems are extremely different in terms of safety goals and system actors, a matching between Or-BAC concepts and the railway knowledge domain is required. In this paper, only user/subject, organization and role concepts are considered.

Furthermore, Or-BAC concepts, such as role and subject, need to be re-interpreted to satisfy the railway safety goals. In this context, some Competency Questions (CQs) are raised to refine the interpretation. The obtained concepts interpretation must be able to provide answers to these CQs :

- **CQ1**: What is a subject in Or-BAC from the GORE point of view and how is it adapted to the railway systems?
- **CQ2**: What is a role in Or-BAC and how is it re-interpreted based on the UFO concept for the railway safety?

3.1. Railway Systems vs Information Systems

Information Systems (IS) are a combination of hardware, software and telecommunication networks that people and organizations use to create, filter and distribute data [16]. In order to improve IS security, an organization employs a security policy to ensure confidentiality, availability and integrity of the information. The security policy is based on user authentication, access control method (to assign roles to users to restrict the access) and encryption.

Hence, information systems security is different from the railway safety, since the type of users is known and it is based on the role assignment to users in order to access to resources. The IS security involves only the user, the role and the system itself. Then, the subject (the actor) in information systems is a user (person or software). Based on UFO, it is a type of **Kind** concept keeping its identity in every situation.

However, railway systems, as socio-technical systems, may involve a technical device behavior, a human intervention or organizational systems, as *an implemented solution* to achieve safety goals. In other words, the type of system actors cannot be defined early to assign roles and permissions. In this context, the type of the actor involved in this *implemented solution* is unknown. It can be a combination of human operators and technical devices cooperating between them to achieve a safety goal. Consequently, the concept of role assignment is more complex since an organization is a complex aggregation of different users.

In this section, we try to solve this issue by providing a conceptualization of the concept subject for railway systems based on the UFO foundational concepts. Then, a semantic interpretation of this concept related to GORE concepts is proposed.

3.2. Agent vs Kind

According to GORO, "an **Agent** becomes a **Stakeholder** when the **Goal** becomes a **Requirement**". This *specific situation* is satisfied through an *implemented solution*. From this point of view, we consider the *specific situation* as the assignment of a **Role** to the **Agent** based on the concept role in R-BAC. In this situation, the **Agent** becomes a **Kind** which plays a **Role**. Besides, **Kind** plays a **Role** to satisfy a requirement through an *implemented solution*. This solution denotes a set of actions to be performed representing how to satisfy a safety requirement. This aspect underlines the **Task** concept in GORO, which defines how to reach a state-of-affairs in reality.

Consequently, according to railway safety knowledge, we define the subject defined in Or-BAC based on GORO and UFO foundational concepts as follows:

Definition 2. (Subject) a Subject is an **Agent**, which performs a **Task.** It becomes necessarily a **Kind** playing a **Role** in this **Task**. After the **Task** execution, a **post-situation** is reached by satisfying a **Goal** (a **Proposition**).

For instance, the traffic agent is a person (**Kind**) which plays a traffic supervisor (**Role**) in the detection of the area occupancy (**Task**) in order to have a safe traffic (**post-situation**) by preventing collisions between them (**Goal**). In order to provide a common conceptual model in real-world semantics of these concepts, the interpretation is based on UFO concepts. Fig. 2 illustrates the defined relations according to Or-BAC interpretation and GORE concepts. In railway systems, organizational systems can be involved in a **Task**. In this case, a **Task** is composed of **sub-Tasks** to be performed by **a set of Agents** belonging to the organizational system. Consequently, the execution of a **sub-task** satisfies a **sub-goal**. It is important to consider this aspect to satisfy a specific state-of-affairs in reality.

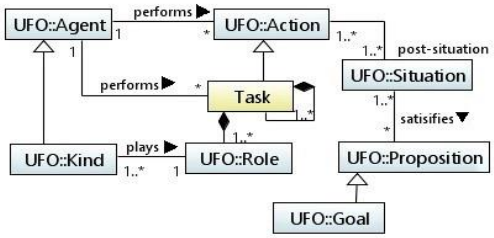

Fig. 2. UML fragment focusing on Roles and GORO concepts.

Railway Illustrative Example:

The function of detecting the presence or transit of the vehicle in a particular section is a safety critical function. It can be realized through a relay, which is an electromagnetic device and the main component of the track circuit, as it is illustrated by Fig. 3. The two rails of the track are used as conductors. The transit of a vehicle on the track causes the electrical contact between the two rails. When the circuit is closed, the relay is characterized by zero current and the block signal is set as danger or occupied (B).

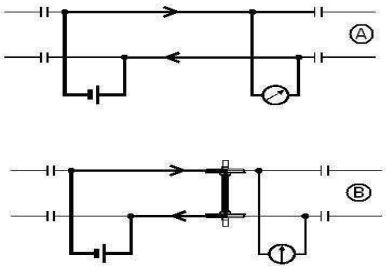

Fig. 3. Free (A) and occupied (B) track-circuit.

In some situations, the realization of this function may involve different **Kinds** such as a person, an automatism or the combination of them. As the context is related to an earlier stage of this system design, the polymorphism of this concept has to be considered to ensure some flexibility in safety-related decision.

For instance, in order to prevent the collision between two trains (**Goal**), the **Task** is composed of **two sub-tasks**: the *detection of the occupancy of the area by the track-circuit* (**Kind**) and *the interdiction of crossing the area to the driver delivered by the traffic agent* (**Kind)**.

Hence, we deduce the definition below:

Definition 3. (**Kind and Task**) Every **Kind** involved in the **sub-task** plays a **Role** in this **sub-task** to provide a **post-situation** satisfying a **sub-goal**.

Fig. 4 shows the UML fragment illustrating relations between concepts in the mentioned example. In this context, we deduce that while the composition (**Task**, **Role**) is true, the **Goal** is achieved. Alternatively,

Kinds becomes **Agents** without **Roles** and the assignment process needs to be incrementally performed.

For instance, in RBAC, a doctor can access to the patient's chart in the hospital **if** he/she is the referring physician. If the spatio-temporal constraints are not satisfied and the task is not performed, the doctor is deprived of the referring physician role for this patient. In order to answer to CQ2, a semantic interpretation of the concept Role in RBAC and the proposed constraints to extend this concept based on UFO is required. Next section details this interpretation.

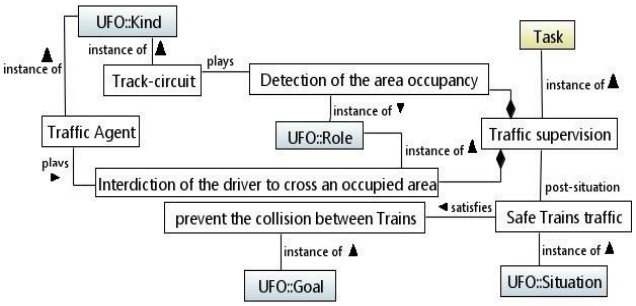

Fig. 4. The UML fragment for example illustration.

3.3. The *Role* Semantic Interpretation

The objective of this section consists in providing a semantic interpretation of the Role concept introduced in RBAC and a conceptualization based UFO concepts. This interpretation may extend this concept to be reused in the railway domain.

In RBAC, the access to a set of resources is based on the function (job) of the user in the enterprise hierarchy. The function of the user consists in its role related to its rights to perform an action. However, the security policy does not change when a user with a role leaves the enterprise. In this case, the new user should be able to activate the desired role. The role concept as defined in R-BAC is interesting in the case of the same enterprise or the same organization. Nevertheless, this aspect is not able to cover the case of multi-organizations cooperating between them or a complex organization composed by heterogeneous constituents.

According to this interpretation, the R-BAC model is not suitable to railway systems as socio-technical systems. In Or-BAC, this aspect is extended to satisfy complex situations. In this model, several concepts are introduced, such as organizations, their hierarchy and the context.

According to Or-BAC, the **context** concept is introduced to constrain the authorization assignment to execute an action. This concept is suitable for railway safety since it defines a spatio-temporal framework or a specific sequential order to perform actions in order to accomplish a task. The interpretation and conceptualization based on UFO of this concept are subject to future works.

Regarding the **Organization** concept, we define it, based on UFO, as an aggregation of **Agents**. The type of **Agents** is still always abstract in the railway safety context. Moreover, the organization hierarchy provides a set of sub-organizations with their own safety policy. This aspect satisfies the railway systems requirements.

For instance, the principal safety requirement of railway systems is the safety of the passengers and the safe traffic of the rolling stock. This generic safety policy needs to be refined in several safety policies. Hence, the safety team, the telecommunication team and the electronic team as **sub-organizations** inherit this safety policy. Therefore, they are able to activate or avoid some authorizations to define their own safety policies.

The **Role** concept as defined in UFO is a non-rigid entity. It is an entity with an identity changeable over

time. This dynamic character needs to be restrained by some constraints to provide the matching between UFO and Or-BAC concepts. In this respect, we deduce that the role in Or-BAC is considered as a sub-type of **Role** in UFO, related to a **Task** in a specific **Context** and valid only in the same **Organization** and the same **Context**.

Definition 4. (Role) According to this interpretation, we can define the role using the first order language as following:

- "A role *r* is permitted by an organization *o* to execute a task *t* for the related context *c*" is represented by *Permit (o,t,c,r)*,
- "In the organization *o*, the context *c* is true for the task *t* and the involved agent *a*" is represented by *Define (o,t,a,c)*,

Such that:

$$\forall\, o \forall\, a\, (\exists\, t \exists\, c\, (Define\ (o,t,a,c) \leftrightarrow \exists\, r \quad (Permit\ (o,t,c,r) \wedge c \in t\ )$$

This constraint can be included in the design model using the Object Constraints Language (OCL). In order to provide a conceptualization of this interpretation in real-world semantics, Fig. 5 illustrates this interpretation through an UML fragment.

An example from the railway domain is described below to illustrate this interpretation. A driver can cross an End of Authority (EOA) in an emergency situation and after the authorization delivered from the traffic agent. In this situation, relations between defined concepts should exist in order to accomplish the task. In this example, concepts consist of:

- **Role**: driver
- **Task** : cross an End of Authority (EoA)
- **Context**: After the traffic agent authorization

Here, a context is required to perform the task. If the task is executed without satisfying this condition, the post situation is dangerous and there is a violation of the safety goal. Consequently, it is required to define another concept able to verify this condition with the aim to avoid hazardous situations. This aspect is considered in Or-BAC by introducing the *context* concept. Nevertheless, it is necessary to provide a semantic interpretation of this concept for the railway domain. Furthermore, the intended conceptualization will be grounded in UFO. These aspects will be considered in future work.

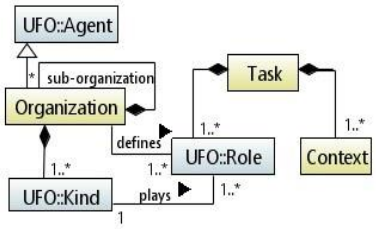

Fig. 5. UML fragment showing role relations with other concepts.

3.4. Evaluation

This step aims to evaluate the proposed interpretation by providing answers to the raised Competency Questions (CQs). Table 1 recapitulates the results of this step and shows that the proposed taxonomy answers to all its intended requirements.

The proposed interpretation provides a common vocabulary to conceptualize the railway domain knowledge and goal-oriented requirements engineering. It supports the conceptual modeling of the railway safety rules development based on UFO. This interpretation may be reused in other domains for the

purpose of improving safety reasoning. Besides, the verification table can be considered as a traceability tool to support the interpretation management.

The proposed semantic interpretation is a primordial step required to provide a full conceptual model of the safety rules development. The safety rules development must be performed and linked to the Goal-oriented Requirement Engineering process from the first design stages. Furthermore, the obtained common vocabulary based on well-founded concepts (UFO) helps the multi-view modeling of different knowledge domains.

The quality evaluation of the conceptual model may be done through several metrics such as the reusability degree [17], which refers to the ratio between the reused concepts and the total concepts. The principle of reusability is widely used to evaluate the quality of conceptual model in the software engineering domain and the information systems development. In our proposed conceptual model, the reusability degree is equal to 0.7. This result represents a high reusability degree (it ranges between 0 and 1). In other words, it improves the matching between safety-related concepts, Or-BAC concepts and GORE concepts. This metric shows the reusability of existing concepts and the future reusability of the conceptual model. However, a low value indicates that corrective actions are required with the aim of decomposing the model and improving its reusability.

Table 1. Verification of the Proposed Semantic Interpretation

CQs	Concepts and relations between them
CQ1	A subject is an **Agent**, which becomes a **Kind** in an **Organization** playing a **Role** to accomplish a **Task**. The **Task** is performed to satisfy a **Goal.**
CQ2	A **Role** is assigned to a **Kind** to accomplish a **Task** according to a related **Context.** The relation between **Task, Context** and **Role** is required to satisfy a **Goal.**

Besides, syntactic quality consists in the degree of correspondence of the conceptual schema and its representation. In this study, the proposed conceptual model is based on the foundational ontology UFO and it is represented in a structured and a semi-formal way. Moreover, the semantic quality refers to the rate of correspondence between the conceptual schema and the real world. Indeed, this aspect is considered in this study by providing a real-world semantics interpretation of safety related concepts. Finally, the pragmatic quality represents the degree of correspondence between the conceptual model and its interpretation. It defines the degree of understanding of the conceptual model. The proposed multi-view conceptual model is shared between different actors. The pragmatic quality is improved since the conceptual model is grounded in UFO, interpreted in real-world semantics and represented through the UML fragments.

4. Conclusion and Future Work

In this paper, a semantic interpretation of a part of safety rules development concepts is proposed regarding the well-founded UFO concepts. The aim of this interpretation is to provide a common vocabulary in real-world semantics in order to have a shared view between different knowledge domains. The shared view consists in a matching between GORE and R-BAC/Or-BAC concepts, and their refinement for the railway systems safety. This aspect is improved by the obtained reusability degree, which is adequate with the intended CQs to enhance the matching between different knowledge domains. Furthermore, this result justifies the good choice of foundational concepts reused for this study and improves the consistency and the completeness of the conceptual model. This study is a continuation of a proposed dysfunctional analysis conceptual model grounded in UFO. The conceptualization of safety measures derived from the dysfunctional analysis is required with a goal-oriented perspective in order to satisfy safety goals and help the requirements management.

With the aim of managing the safety-related decisions based on the accidentology knowledge, there is a need to link safety rules to GORE concepts and formulate them with a high level of abstraction. Moreover, the obtained interpretation may support the tool implementation development of safety rules for the railway domain. In this study, only subject, role and organization concepts are considered from the Or-BAC model. The interpretation of these concepts is based on UFO and its evaluation results are presented in a verification table, which can be reused as a traceability tool for the management of concepts and relations.

In future work, the semantic interpretation and the conceptualization based on UFO of other Or-BAC concepts such as context, authorization, prohibition and assignment is envisaged. Moreover, other concepts may be introduced such as safety requirements and functional requirements, with the objective of managing the requirements traceability mechanism based on a conceptual model. The intended solution aims to ensure the coherence in terms of the requirements interaction with the safety requirements adaptability according to different contexts. This process must be considered in order to have a whole view of the system requirements and the relations between them throughout the design process.

References

[1] Debbech, S., Collart-Dutilleul, S., & Bon, P. (2018). Improving safety by integrating dysfunctional analysis into the design of railway systems. *Proceedings of the 16th International Conference on Railway Engineering Design & Operation*. Lisbon.

[2] Guizzardi, G. (2005). *Ontological Foundations for Structural Conceptual Model.* Ph.D. thesis, Institute for Telematica and Information Technology, Twente Univ., Twente, Enschede, The Netherlands.

[3] EN-50129: Railway applications. (2003). Communication, signalling and processing systems. *Safety Related Electronic Systems for Signaling.*

[4] Unisig, E, U. G. (2016). *System Requirements Specification (SRS) Version 3.4.0, E. R. Agency.* Retrieved from http://www.era.europa.eu/Document-Register/Pages/Set-2-System-Requirements-Specification.aspx

[5] Ben-Ayed, R., Collart-Dutilleul, S., Bon, P., Idani, A., & Ledru, Y. (2014). B formal validation of ERTMS/ETCS railway operating rules. In Y. Ait Ameur & K. D. Schewe (Eds.), *Proccedings of ABZ*, LNCS: *Vol. 8477* (pp. 124-129). Heidelberg: Springer.

[6] Abou-El-Kalam, A. (2003). Or-BAC: Un modèle de contrôle d'accès basé sur les organisations. *Cahiers Francophones de la Recherche en Sécurité de L'Information 1,* 30-43.

[7] Ferraiolo, D. F., Cugini, J. A., & Kuhn, D. R. (2014). Role-based access control (RBAC): Features and motivations. *Proceedings of the 11th Annual Computer Security Application Conference*.

[8] Perfect Project Website. Retrieved from http://www.agence-nationale-recherche.fr/Projet-ANR-12-VPTT-0010

[9] Borst, W. (1997). *Construction of Engineering Ontologies.* Ph.D thesis, Institute for Telematica and Information Technology, Twente Univ., Enschede, The Netherlands.

[10] Herre, H. (2010). General Formal Ontology (GFO): A foundational ontology. *Theory and Applications of Ontology: Computer Applications*, 297-345. Springer: Dordrecht.

[11] Arp, R., Smith, B., & Spear. A. (2015). *Building Ontologies with Basic Formal Ontology*. MIT Press.

[12] Negri, P. P. (2017). Towards an ontology of goal-oriented requirements. *CIbSE*, 469-482.

[13] Yu, E. S. K. (1995). *Modelling Strategic Relationships for Process Reengineering.* Ph.D. thesis, Toronto. Univ, Canada,

[14] Dardenne, A., Lamsweerde, A., & Fickas, S. (1993). Goal-directed requirements acquisition. *Proceedings of 6th International Workshop on Software Specifcation and Design*. Elsevier Science Publishers B. V.

[15] Borgida, A. (2009). Techne: A (nother) requirements modeling language. *Computer Systems Research*

Group. Toronto Univ., Toronto, Canada.

[16] Jessup, L. M., & Valacich, J. S. (2008). Information systems today: Managing in the digital world. *Pearson Prentice Hal.*

[17] Mehmood, K., & Cherfi, S. S. (2009). Evaluating the functionality of conceptual models. In C. A. Heuser, & G. Pernul (Eds.). *Proceedings of ER 2009 Workshops* (pp. 222-231). Verlag Berlin Heidelberg: Springer.

Sana Debbech is a Ph.D student in computer science at Lille University, IFSTTAR/COSYS/ESTAS, Lille, France. In 2015, she graduated as an engineer from the National School of Computer Sciences (ENSI), Tunis, Tunisia. She has been working as an engineer at IFSTTAR and she was involved in research projects. Her research interests include ontology-driven system engineering, dysfunctional analysis and railway safety.

Philippe Bon received the Ph.D degree from Lille University in 2000. He is currently a senior researcher in the ESTAS Laboratory, COSYS Department, the French Institute of Science and Technology for Transport, Development and Net-works (IFSTTAR). His research focuses on the implementation requirements traceability throughout the design cycle of railway land systems. He was involved on several research projects related to the use of formal methods for traceability and validation.

Simon Collart Dutilleul received the Ph.D degree from University of Savoie in 1997 and the Habilitation degree from Lille University in 2008. In 1999, he was a lecturer at the Lagis Laboratory, Ecole Centrale de Lille. He was responsible for the teaching section in computer engineering at the Institute of Technology of Computer and Industrial Engineering from 2006 to 2012. He is currently a research director at IFSTTAR. He has supervised nine Ph.D. students. Since 2012, he has been involved in the IFSTTAR/COSYS/ESTAS laboratory dedicated to railway systems. He also leads the European Railway Management System Group in this laboratory.