Conceptual Modelling of the Dynamic Goal-oriented Safety Management for Safety Critical Systems

Sana Debbech[a], Philippe Bon and Simon Collart-Dutilleul

Univ. Lille/Nord de France, IFSTTAR/COSYS/ESTAS, Villeneuve d'Ascq, France

Keywords: Ontology, GORE, Or-BAC, Safety Measures Development, UFO, Railway Safety.

Abstract: In the context of Safety Critical Systems (SCSs), safety measures derived from the dysfunctional analysis are generally expressed in an informal way. However, in an early phase of SCSs design, there is a need to link these safety measures to Goal-Oriented Requirements Engineering (GORE) concepts. Moreover, the current practice of the safety measures development is not based on a specific goal-oriented control model. Since there are different knowledge domains, there is a lack of a common vocabulary aiming to avoid the semantic heterogeneity between them. Consequently, a common model for an unambiguous knowledge sharing and a full semantic interoperability assurance is missing. In this paper, we propose the Goal-Oriented Safety Management Ontology (GOSMO), a domain ontology, which is grounded in the Unified Foundational Ontology (UFO) and provides a conceptualization and a real-world semantic interpretation of the knowledge matching for SCSs. Furthermore, the proposed safety measures development process is performed using a reinterpretation from the safety point of view of the Organization-Based Control Access (Or-BAC), which was initially developed for the Information Systems (IS) security. The GOSMO aims to capture the alignment between the considered domains concepts through the reference models reuse and the proposed taxonomy based on standards definitions. The proposed ontology is evaluated by the formalization of two cases studies from the railway domain, since it is the target application domain. Finally, the evaluation results show that GOSMO covers and analyses several real critical situations and fulfils its intended purpose.

1 INTRODUCTION

In the Safety Critical Systems (SCSs) context, safety is viewed as an emergent control issue. Therefore, safety management must be ensured by a control organization integrated in an adaptive socio-technical system. The aim of this control organization is to enforce safety constraints on the system behaviour in the first design stages (Debbech et al., 2018a). Furthermore, safety improvement must still be maintained and the system must keep its safe behaviour as changes occur. Consequently, there is a need to define the appropriate safety constraints according to the related context. From this perspective, SCSs suffer from a lack of control and development models of safety measures derived from dysfunctional analysis.

Moreover, these safety constraints must be integrated as a control structure of the adequate enforcement of components and their interactions. This safety knowledge has to be considered in the system design model and particularly in the Requirement Engineering (RE) practice. In other words, safety analysis should be strongly related to the system requirements elicitation. Ordinarily, safety measures derived from the safety analysis are directly considered as safety requirements: "*Safety requirements are the safety measures taken to mitigate hazards in safety-critical systems*" (Zhou et al., 2017). Then, safety requirements are defined as safety measures, that are taken to avoid, reduce or limit catastrophic failure consequences: "*safety requirements are defined based on a list of categorized hazards and associated safety risk analysis*" (Firesmith, 2005). Intuitively, this definition seems clear and easy to understand but there is a lack of consideration for the safety team efforts into the requirements specification process and "*this makes difficult to ensure that architecture incorporates the appropriate safety guards*" (Firesmith, 2005). From a further perspective, safety measures must be linked to Goal-Oriented Requirements Engineering (GORE) (Van Lamsweerde, 2001) concepts such as goal, agent, requirement and task.

In order to deal with the semantic heterogeneity and the knowledge domains combination, the aim of this study is to propose a conceptualization of the knowledge matching in order to provide a shared

[a] https://orcid.org/0000-0002-4003-6505

Debbech, S., Bon, P. and Collart-Dutilleul, S.
Conceptual Modelling of the Dynamic Goal-oriented Safety Management for Safety Critical Systems.
DOI: 10.5220/0007932502870297
In *Proceedings of the 14th International Conference on Software Technologies (ICSOFT 2019)*, pages 287-297
ISBN: 978-989-758-379-7

view between them. Furthermore, we define the safety measures development process for SCSs based on the Organization-Based Control Access (Or-BAC) Model (El Kalam et al., 2003). This control access model is normally used in order to ensure the Information Systems (IS) security. Nevertheless, the analogy between the security conditions to access to an information and the conditions in order to operate safely proposed by (Ben Ayed et al., 2014) is extended in this study. In the present paper, the matching between knowledge domains is considered through the concepts alignment and is driven by the Unified Foundational Ontology (UFO) (Guizzardi, 2005). Then, the proposed semantic interpretation and conceptualization is provided in real-world in order to provide a common vocabulary at a high level of abstraction.

Therefore, a domain ontology is proposed and is called the Goal-Oriented Safety Management Ontology (GOSMO). In this work, we focus on relevant concepts related to safety, GORE and Or-BAC knowledge. GOSMO aims to provide an unambiguous, complete and consistent set of the involved concepts, and to manage safety related decisions in the SCSs design process. In order to bridge the gaps mentioned above, two Research Questions (RQs) are defined:

- **RQ1:** How can we interpret and conceptualize safety measures and link them to GORE concepts in real-world semantics?

- **RQ2:** Which UFO-driven conceptualization of Or-BAC concepts would be able to provide a safety control model and to deal with the organizational aspect of SCSs?

These two RQs define the purpose of the proposed ontology and they will be refined in order to fulfil it. This paper is organized as follows. Section 2 defines the background on UFO, GORE, Or-BAC knowledge and discusses related works. Section 3 presents GOSMO and its evaluation by the railway knowledge is detailed in Section 4. Section 5 concludes the paper and outlines perspectives.

2 BACKGROUND

The present study is based on an extensive research on knowledge domains (knowledge acquisition) in order to extract, apply and connect them. In this section, we introduce relevant concepts of the considered domains, namely GORE, Or-BAC and the well-founded ontology UFO.

2.1 The Unified Foundational Ontology (UFO)

The Unified Foundational Ontology (UFO) is an upper-level ontology which provides a full and common set of generic concepts and relations for all domains (Guizzardi, 2005). The discussion around the choice of this foundational ontology has been made and argued in a previous work (Debbech et al., 2019b). Thanks to its ontological distinctions, it provides a complete and consistent set of concepts that cover pertinent aspects of safety, GORE and the organizational control model. Moreover, the reuse of foundational concepts aims to provide a real-world semantics interpretation of safety measures and its surrounding concepts. Figure 1 shows the Unified Modelling Language (UML) diagram representing a fragment of UFO concepts that will be reused in this study.

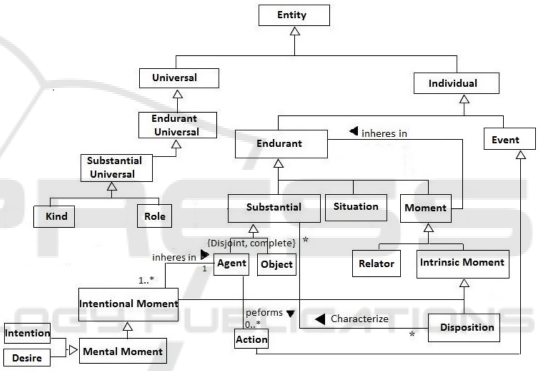

Figure 1: Fragment of UFO showing Individuals and Universals.

More details about these UFO concepts and their interpretation and illustration by railway examples may be respectively found in (Guizzardi, 2005; Falbo and Bertollo, 2009) and (Debbech et al., 2019b). Table 1 summarizes definitions of the UFO concepts considered in this study. In the remainder of this paper, concepts and relations between them are respectively represented in bold and italic styles in order to improve readability.

2.2 Goal-Oriented Requirements Engineering (GORE)

Several benefits of GORE are defined in the RE practice such as the clarity and the completeness of requirements specification, a clearer way to manage requirements complexity and resolve conflicts among them (Van Lamsweerde, 2001). These advantages have been the aim of many GORE approaches such as

Table 1: Definitions of the considered UFO concepts.

UFO Concepts	Definitions
Kind	A **Kind** is *a subtype of* **Substantial Universal**. It denotes a substantial universal with rigidity and a unique identity permanently.
Role	A **Role** is *a subtype of* **Substantial Universal**. It denotes non-rigid **Substantial Universal** and its identity changes as new situation (circumstances) occurs.
Agent	An **Agent** is a *a subtype of* **Substantial**. It denotes **Individuals** with a unique identity and its existence is independent of other **Individuals**.
Action	An **Action** is a *a subtype of* **Event** and it is *caused by* an **Intention**.
Relator	A **Relator** is *a subtype of* **Moment**. Its existence depends on many **Individuals**.
Situation	A **Situation** denotes a state-of-affairs existing in reality.
Intention	An **Intention** is a *subtype of* **Mental Moment**. It *inheres in* an **Agent** and it denotes a consideration of a plan to accomplish the goal.
Desire	A **Desire** is a *subtype of* **Mental Moment**. It denotes the willingness of the **Agent** towards a **Goal**.

the i*/iStar framework (Yu, 2011), KAOS (Dardenne et al., 1993), Techne (Borgida et al., 2009) and Goal Oriented Requirements Ontology (GORO), which is grounded in UFO (Negri et al., 2017). The purpose of this paper is neither to make a comparative study of these approaches nor to use one over the others, but it is to propose a new conceptual model to link safety measures derived from safety analysis to GORE concepts based on a real-world semantics.

As GORO is a reference domain ontology grounded in UFO, it seems interesting to be re-used for the alignment of both safety analysis and GORE concepts. It provides a common vocabulary of GORE concepts through the analysis and the interoperability of well-known languages mentioned above.

According to GORO (Negri et al., 2017), there is a distinction of the **Goal** type as a *propositional content of* two **Mental Moments**: the **Intention** or the **Desire** of the **Agent**. In the present study, these concepts are reused in order to elicit goals during the integration of safety measures in the RE process. In this way, a goal is considered as a set of intended statements to be achieved. The GORO fragment representing the **Goal**-related UFO concepts and relations between them, is illustrated by Figure 2.

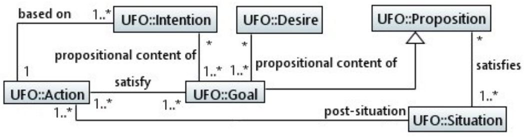

Figure 2: GORO fragment focusing on Mental Moments and Goals (Negri et al., 2017).

In this study, we assume that goals can be composed into sub-goals to be satisfied in a given state-of-affairs in reality. The composition is a whole-part formal relation which can be expressed as satisfying a goal (G) is achieved by satisfying at least one sub-goal:

$$Satisfy(G) \Leftrightarrow Satisfy(G_1) \vee ... \vee Satisfy(G_n) \quad (1)$$

From a lower level of abstraction, (Wang et al., 2014) defined a requirement as an intended behaviour in the environment independently of the machine. GORO considers the **Requirement** as a subtype of **Goal** in the context of a specific problem. It describes environmental conditions to be achieved through a desired solution to satisfy the underlying strategic goals.

In this paper, we refer to IEEE standards which define the requirement as a condition or a capacity of a system to satisfy a policy, a standard, a specification or any formal imposed document (IEEE 610.12, 1990) and (ISO/IEC/IEEE 29148, 2011). By this definition, we consider a **Requirement** as a refinement of a **Goal** to satisfy a specification. A specification may be an artefact, a formal document of statements to be satisfied or an agent's judgement to satisfy a specific situation. The requirement and its relations with other concepts is detailed in Section 3.

2.3 Organization-based Control Access (Or-BAC)

The Organization-Based Control Access (Or-BAC) is an access control model based on the organization concept and it is generally used in order to improve the IS security. In Or-BAC, an organization is an entity that manages a set of security policies. This security rules management is based on several entities such as *Organization, Role, Activity, View, Subject, Action, Object and Context*. Moreover, a set of predicates are defined aiming to model relationships between these entities. More details about Or-BAC may be found in (El Kalam et al., 2003). A formal definition of Or-BAC concepts and relations between them is detailed in (Méry and Merz, 2007). Figure 3 illustrates the Or-BAC concepts (rectangles) and relations between them (oval).

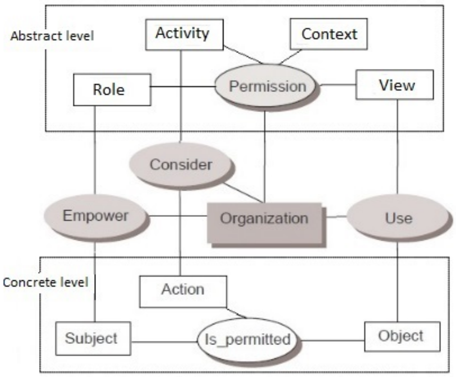

Figure 3: Or-BAC concepts and relations between them.

In Or-BAC, the hierarchy aspect is considered for the Role and the Organization concepts in order to ensure the permission inheritance of roles and security policies by sub-organizations. This aspect is relevant in the context of the present study since it spotlights the organizational aspect of SCSs and the interoperability criterion. On the one hand, this access model allows a structured security decisions management in order to access to information within an organization. On the other hand, it defines relevant concepts and relations between them that may be reinterpreted for other domains such as SCSs in this study.

In the SCSs terminology, safety operations management requires a consistent model aiming to manage safety conditions. In (Debbech et al., 2019a; Debbech et al., 2019b), we proposed a complete semantic interpretation of some Or-BAC concepts namely, organization, role and subject from the safety perspective. Furthermore, we discussed the difference of requirements between both domains and we defined the analogy between them by introducing new concepts. In this study, a full consistent conceptualization of Or-BAC concepts from the safety perspective is proposed in real-world semantics. The socio-technical aspect of SCSs enforces their view as hierarchical structures with specific imposed constraints on each level. The organization concept highlights the organizational aspect of railway systems and its integration in the conceptual model enhances the safety-related control. In the present study, Or-BAC concepts are reinterpreted in a safety-oriented way. Furthermore, they are extended regarding the railway knowledge and aligned with both UFO and GORE concepts.

2.4 Related Work

Ontologies are widely used in the Information Systems (IS) and software development. In (Souag et al., 2015), authors provide a security ontology to elicit security requirements through an interactive environment between security knowledge and requirements engineering. Nevertheless, the dynamic aspect of the security management and the security requirements analysis according to GORE approaches are not considered. The security measures development are not based on a structured control access model. Then, the conceptualization was not provided in real-world semantics in order to allow a better communication with a common vocabulary. With the analogy between safety and security properties, these aspects are considered in the present study.

In (Zhou et al., 2015), the proposed safety requirements elicitation approach is based on the safety-related environment knowledge representation, as a set of assumptions, and a set of defined reasoning rules. However, their work is limited to domain assumptions which does not cover all possible contexts for SCSs and the dynamic safety requirements elicitation is not satisfied. In (Provenzano et al., 2017), authors propose an ontological approach to elicit safety requirements based on the hazard knowledge conceptualization. The proposed heuristic approach describes the hazard components analysis according to their properties, roles and relations between them. Then, the safety requirements elicitation is performed by extracting this knowledge and managing relations between components. However, they did not consider the semantic link interpretation between safety measures derived from the hazard knowledge and safety requirements. Moreover, the safety requirements elicitation is not based on a specific GORE approach in order to deal with the complexity and the dynamic aspect of this activity.

To the best of our knowledge, the SCSs-related literature suffers from a lack of a shared and structured knowledge representation considering several issues simultaneously, and aiming to answer them. Furthermore, the dynamic aspect of the safety constraints management process must be considered in the first design stages. Therefore, the need to formalize a shared goal-oriented safety decisions management model emerges. In this paper, we try to fill the gaps mentioned above and we propose GOSMO, which aims to support the conceptual clarification of the considered domains and the safety decision-making management for the SCSs design. Then, it provides a new terminological interpretation of concepts based on reference models and standards. The development of the proposed ontology is detailed in next Section.

3 THE PROPOSED GOAL-ORIENTED SAFETY MANAGEMENT ONTOLOGY (GOSMO)

In order to build the Goal-Oriented Safety Management Ontology (GOSMO), we chose the Systematic Approach for Building Ontologies (SABiO) (de Almeida Falbo, 2014). The choice of the SABiO approach has been made because it supports the domain ontologies development process and incorporates best practices from Ontology Engineering and Software Engineering. Moreover, it has been widely used for building several domain ontologies and admit the relevance of using foundational ontologies in the ontology development process. In this paper, only the first two phases of SABiO are considered. The first one consists in the purpose identification and the ontology requirements elicitation. The second one denotes the capture of the domain conceptualization and the formalization of axioms. For the purpose of defining the GOSMO purpose, a set of Competency Questions (CQs) are elicited and are considered as the ontology requirements from the RE view. The raised CQs listed below consist in the high level of granularity of the proposed RQs and they are used to refine the GOSMO scope and then for its evaluation process:

- CQ1: What are safety measures and how to link them to GORE concepts?
- CQ2: How to operationalise these safety measures?
- CQ3: How to semantically align the role concept proposed by Or-BAC with the **Role** concept of UFO ?
- CQ4: How to conceptualize the dynamic context related to the Or-BAC permissions from the UFO perspective?
- CQ5: Which UFO-driven implementation of the organization concept is able to deal with the organizational aspect of SCSs?
- CQ6: What is the reinterpretation of the roles assignment proposed by Or-BAC that would be suitable for SCSs?
- CQ7: How to make better safety decisions management in the SCSs design based on the interpretation of the permission concept of Or-BAC?

After the CQs elicitation, the conceptual modelling may be performed by providing a specific taxonomy and using the UFO ontological pattern. In order to have a better approximation of the proposed ontology to the ideal knowledge domain representation, the ontology must be represented with highly-expressive languages such as OntoUML, which is a UML extension for the conceptual modelling. It incorporates the foundational features proposed by UFO and is used in this study in order to ensure the ontology representation adequacy. Then, some axioms specifying constraints and inferences rules are formalized using First-Order Logic (FOL) in order to provide an unambiguous and expressive description.

Figure 4 represents the conceptual model of GOSMO using the OntoUML diagram. It shows the interpretation and the conceptualization of relations between **Safety Measures**, GORE and Or-BAC concepts. In safety critical domains, safety measures are defined as the operationalization of safety policies imposed by organizations. As **Actions** are a *subtype of* **Events**, **Safety Measures** will change the state of affairs of reality from the **Hazard** situation to another safe **post-situation**. The central concept in the proposed ontology is **Safety Measures** (*sm*). They are composed of sub-measures. The composition relation is denoted by the *part_of* predicate and is declared to be transitive, non reflexive and anti-symmetric as respectively enforced by Axioms 2, 3 and 4 using the FOL. In the same way, these axioms are defined for the composition relation for other related concepts, but they will not repeated in order to improve readability. This relation is considered in order to satisfy both the constraint assumed in this study considering the **Safety Goal** composition (see Section 2.2) and the organizational aspect of SCSs.

$$(\forall sm_1, sm_2, sm_3) part\_of(sm_1, sm_2) \wedge part\_of(sm_2, sm_3) \Rightarrow part\_of(sm_1, sm_3) \quad (2)$$

$$(\forall sm) \neg part\_of(sm, sm) \quad (3)$$

$$(\forall sm_1, sm) part\_of(sm_1, sm) \Rightarrow \neg part\_of(sm, sm_1) \quad (4)$$

Then, we assume that a sub-measure may be a *part_of* two measures and may contribute to satisfy two sub-goals. Therefore, each organizational level provides its own **Sub-Safety Measures** and a sub-measure *satisfies* a sub-goal and partially *satisfies* a **Safety Goal**. This interpretation is formalized as follows:

Let *SM*={ $sm_i \mid i = 1, 2, ..., n$ } be the set of safety measures.

Let *SG*={ $sg_i \mid i = 1, 2, ..., n$ } be the set of safety goals.

$$Satisfy(sm, sg) \Leftrightarrow Satisfy(sm_1, sg_1) \vee \cdots \vee Satisfy(sm_n, sg_n) \quad (5)$$

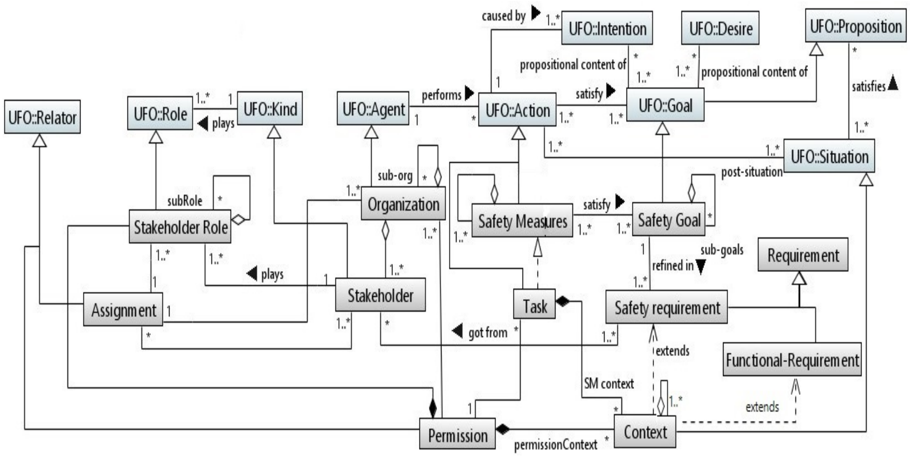

Figure 4: Conceptual Model of GOSMO focusing on relations between **Safety Measures**, **Or-BAC** and **GORE** concepts.

When the **Safety Goal** is achieved, a **post-situation** occurs in order to *satisfy* a **Proposition** (a goal). Then, the **Safety Goal** *is refined in* **Safety requirement** which is realized by a **Stakeholder** into an **Organization**. The central concept of the proposed safety measures management model is the **Organization**. In the proposed conceptual model, the **Organization** concept, which is inspired by the Or-BAC model, is aligned with the **Agent** UFO concept. Moreover, the hierarchy aspect of the **Organization** is considered in the proposed conceptualization by its aggregation to sub-organizations. In order to satisfy the socio-technical aspect of railway systems, the **Organization** (*o*) is considered as a *subtype of* the **Agent** and an aggregation of **Stakeholders** (*st*), which is denoted by the predicate *has_a(o, st)*.

Moreover, the **Stakeholder** (*st*) *plays* a **Stakeholder Role** (*str*) within an **Organization** (*o*). The **Assignment** (*a*) concept is a *subtype of* **Relator** since it is a relational property connecting several concepts. According to Or-BAC, an organization assigns a role to a user through the *empower* predicate. This interpretation is extended regarding UFO and GORE concepts by considering the **Stakeholder** concept and the subsumption relation of the **Role** and **Kind** concepts of UFO. It provides the concretisation of the safety management process when changes occur in order to deal with the dynamic aspect. The assignment of roles is constrained by Axiom 6 using the containment relation denoted by the *member_of* predicate.

$$\begin{aligned}(\forall o,str,a,st)&member\_of(str,a) \wedge member\_of(st,a)\\ &\wedge has\_a(o,st) \wedge member\_of(o,a) \Rightarrow plays(st,str)\end{aligned} \tag{6}$$

Likewise, as a **Relator**, the **Permission** (*p*) concept denotes the authorization assignment to a **Stakeholder Role** (*str*) to perform a **Task** (*t*) according to a specific **Context** (*c*). The role hierarchy aspect is considered in order to factor the permissions associated to roles. Hence, this formalism ensures the inheritance of permissions of **Stakeholder Role** to subroles. The conceptualization pattern of these concepts is justified and illustrated in (Debbech et al., 2019b). The permission process is enforced by Axiom 7 in order to provide a structured control model of safety decisions.

$$\begin{aligned}(\forall str,p,c,t)&part\_of(str,p) \wedge part\_of(p,c)\\ &\wedge part\_of(c,t) \wedge member\_of(o,p)\\ &\Rightarrow member\_of(p,t)\end{aligned} \tag{7}$$

Furthermore, we define the **Context** concept as a specific **Situation**, that determines the validity of a **Safety requirement** and of a **Functional Requirement**. A **Context** can be classified into many types such as the spatial and temporal boundaries, chronological events, domain constraints or the history of previous tasks. Consequently, the aggregation of the **Context** is considered in order to satisfy some situations in reality such as the remotely operated **Task** as illustrated in (Debbech et al., 2018b). This notion is important because it highly impacts safety-related decisions and the **Task** implementation. The matching between the context concept (from the Or-BAC model) and the railway knowledge was tackled and evaluated by a case study from the real accident of Saint-Romain-En-Gier in a previous work (Debbech et al., 2019a). In the present study, we propose the alignment between the context concept and UFO concepts in order to provide an abstract view in real-world semantics. This interpretation is illustrated by the *extends* relation between the **Safety requirement** and the **Context**. In the same way, a **Context** *extends* a **Functional Requirement**. The introduced relation called *extends* considers that validity or the execution of a requirement is potentially related to a context. It underlines the "extend" relation defined by UML.

The **Task** concept is considered as a concrete view of one or more **Safety Measures**. It denotes the *realization* of **Safety Measures**. Indeed, a **Task** is composed of a **Context** characterizing circumstances or the specific **Situation** in which the **Permission** is granted by the **Organization** to a **Stakeholder Role** in order to perform this **Task**. Moreover, this concept provides the related concepts encapsulation in order to ensure the information integrity.

Both **Functional Requirement** and **Safety requirement** are considered in the proposed conceptual model in order to tackle the requirement traceability mechanism. This aspect is relevant to ensure the requirements consistency and completeness, and to support the requirement management process after the safety requirements change. It is difficult to deal with the **Task** criticity when there are several requirements that dynamically change according to a **Context**. Furthermore, requirements change during the SCSs design process due to the continuous rise of safety constraints to enforce component interactions. This aspect will be tackled in future works in order to capture the requirement engineering knowledge and to provide a common model with a complete, consistent and traceable view.

The proposed ontology, grounded in UFO, aims to capture the goal-oriented safety decisions knowledge. It provides a consistent and unambiguous taxonomy of safety decisions management based on Or-BAC and GORE concepts in order to provide a reusable shared view between knowledge domains. Furthermore, GOSMO may be reused for other safety critical domains since it is a domain ontology founded in UFO. Otherwise, the proposed conceptualization is based on several criteria such as the clarity, the coherence and the extendibility since it aims to represent a knowledge sharing (Gruber, 1995).

4 EVALUATION

In this section, the evaluation of the Goal-Oriented Safety Management Ontology (GOSMO) is performed using verification and validation methods proposed by SABiO (de Almeida Falbo, 2014). The first step consists in the verification of the capability of GOSMO to answer to the raised CQs. The verification results are summarized in a table in order to verify that the ontology fulfils its requirements (purpose). Then, the validation of GOSMO is performed through its instantiation in order to represent real situations. This verification step is primordial in order to demonstrate the completeness and the validity of GOSMO and its ability to analyse different real-world aspects.

4.1 The GOSMO Verification

Table 2 illustrates the GOSMO verification results regarding the predefined CQs. This table may be used as an ontology management support in order to keep track of its changes. This traceability tool is particularly useful for the GOSMO reuse for other domains. The table displays that the ontology answers all of the CQs.

4.2 The GOSMO Validation

Case 1: For the validation purpose, we took a real rail accident scenario (d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), 2005). The rail accident occurred on February 16^{th}, 2005 at Longueville (France). It denotes a side collision when the train 117710 from Provins (Seine-et-Marne) hit the train 117578 sidelong at Longueville station (Seine-et-Marne). The scenario is due to the fault of the reversibility system which was not locked on the operating position. Consequently, the brakes were deactivated. Then, the driver had an insufficient behaviour knowledge in critical situations and only used the locomotive's handbrake to stop the train. However, it was not powerful enough because of the brakes deactivation, which causes a crossing of a closed signal. Consequently, the accident is due to cascading failures that seems to be triggered by a lack of an efficient safety measures development model able to deal with the criticality of railway systems as SCSs. More details about the scenario description and the safety investigation may be found in (d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), 2005). In this section, the graphic representation of the semantic annotation is used for the goal-oriented safety management process in order to improve the visualisation of the GOSMO illustration and to validate its semantic scope without modifications. In the graphic notation, ovals denote the GOSMO concepts and rectangles denote the linked individuals.

According to the accident scenario, safety constraints are violated and this causes the accident due to the lack of an efficient safety control model. In order to show the relevance of the GOSMO pattern design for the design of SCSs, the safety-oriented Or-BAC model is used to analyse the safety constraints, that could have been able to avoid this accident. Then, the safety measures development process, which has to be considered as flexible solutions to avoid this critical situation, is performed as detailed below in order to ensure their validity for all contexts. Here, it is im-

Table 2: Verification table: GOSMO's CQs and how to fulfil them.

CQs	Concepts and Relations
CQ1	A **Safety Measure** is a *subtype of* **Action**. It *satisfies* a **Safety Goal** that is *composed of* sub-goals. A **Safety Goal** is *refined in* **Safety requirement** *got from* a **Stakeholder**. When the **Task** is performed, a **post-Situation** occurs that *satisfies* a **Proposition** (**Goal**).
CQ2	A **Task** is accomplished according to a **Stakeholder Role Permission** by an **Organization** related to a specific **Context**.
CQ3	A **Stakeholder Role** is a *subtype of* **Role**. It is played by a **Stakeholder** (a *subtype of* **Kind**).
CQ4	A **Context** is a *subtype of* **Situation**. It denotes the specific **Situation** (circumstances) in which the **Permission** is according to a **Stakeholder Role** to perform the **Task**. Moreover, it **extends** a **Safety requirement** and a **Functional Requirement**.
CQ5	An **Organization** is a *subtype of* **Agent** and it is *composed of* **sub-organizations**. An **Organization** is *composed of* one or many **Stakeholders** that are a *subtype of* **Kind**.
CQ6	An **Assignment** is a *subtype of* **Relator** and it denotes the **Stakeholder Role** (a *subtype of* **Role**) assignment to a **Stakeholder** by an **Organization**.
CQ7	A **Permission** is a *subtype of* **Relator** and it denotes the **Stakeholder Role** authorization to accomplish the **Task** according to a **Context** , which is a specific *subtype of* **Situation**.

portant to mention that safety measures are proposed intuitively based on the railway knowledge for the illustration purpose.

The first **Safety Measure** can be the deployment of an electric control of the reversibility system to *satisfy* the correct switch of locomotives and correctly activate brakes (**Safety Goal**). This safety measure provides an enforcement of the system behaviour in order to avoid technical failures.

The driver as a **Stakeholder Role** assigned by the SNCF (**Organization**), has the **Permission** in his **Task** to use the emergency braking systems (**Safety Measure**), in the case of emergency situations such as the failure of brakes (**Context**), in order to stop the train (sub-goal) and then avoid a collision (**Safety Goal**). This recommendation was proposed in the BEA-TT report (d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), 2005). In this scenario, the driver did not use the emergency brakes, even if he should do it. Figure 5 represents the semantic annotation of the accident data related to the goal-oriented safety control process for the driver behaviour.

The second **Safety Measure** consists in a reinforcement of the braking control or of the driver behaviour. This **Safety Measure** may be the deployment of a technical device (a component of the train protection system) to *satisfy* the driver alertness when he cross a closed signal by alerting him on-board and he has to acquit (**Safety Goal**). If he did not acquit, the emergency stop is automatically triggered. It is a **post-situation** that *satisfies* a **Proposition** (a Goal). Another simple solution could be the use of low-level automatic control devices like crocodiles. This safety measure may be adequate in the context of this scenario, however it could be not efficient for all possible contexts in order to stop a train crossing a closed signal. A more flexible device could be able to be a tailored solution to different contexts.

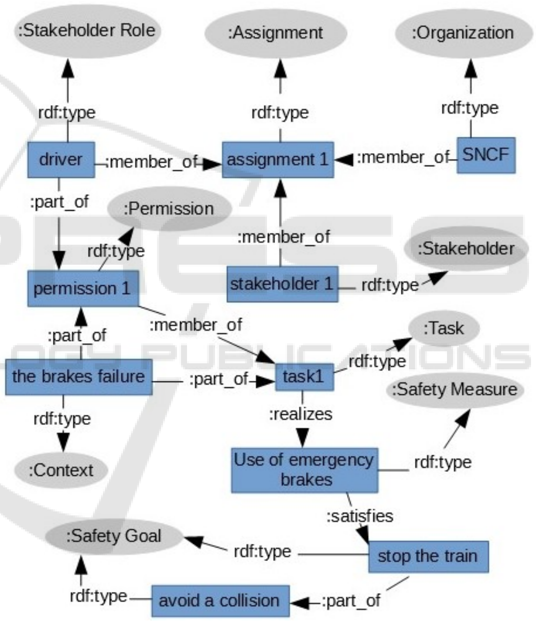

Figure 5: Semantic annotation of the safety-oriented Or-BAC model for driver behaviour in the Longueville accident.

The train agent as a **Stakeholder Role** assigned by the SNCF (**Organization**), has the **Permission** in his **Task** to communicate with the driver (**Safety Measure**), if he perceives a critical situation of the driver's behaviour (**Context**), in order to prevent a collision (**Safety Goal**). However, the train was not equipped by the inter-phony communication between the train agent and the driver. It could be efficient to avoid this collision if a communication had been established between them in order to have a full view of the critical situation. The semantic annotation for train agent behaviour is performed in the same way but it is not shown in this paper due to the space constraint.

Figure 6 depicts the semantic annotation of the proposed goal-oriented safety measures for this accident. The proposed **Safety Measures** are considered in order to deal with failures due to components fault (the reversibility system) and others due to human errors. These aspects can be transformed to architectural constraints in the design model of SCSs in order to improve goal-oriented safety decisions in the first stages.

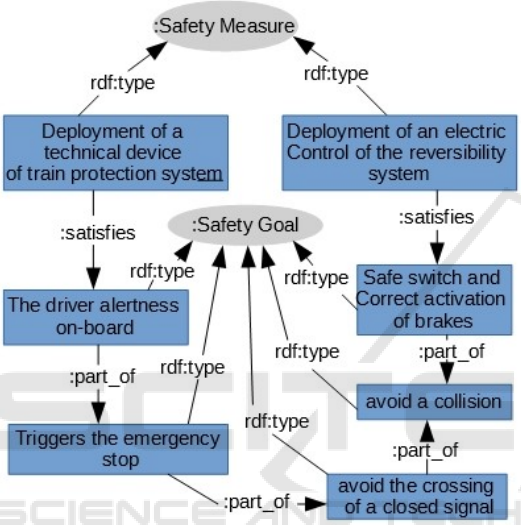
:Safety Measure
rdf:type
rdf:type
Deployment of a technical device of train protection system
Deployment of an electric Control of the reversibility system
:satisfies
:Safety Goal
:satisfies
rdf:type
rdf:type
The driver alertness on-board
Safe switch and Correct activation of brakes
:part_of
rdf:type
rdf:type
:part_of
avoid a collision
Triggers the emergency stop
rdf:type
:part_of
:part_of
avoid the crossing of a closed signal

Figure 6: Semantic annotation for the proposed goal-oriented safety measures development process of the Longueville accident.

Case 2: Another rail accident scenario is considered in order to instantiate and validate GOSMO from another perspective. We refer to the Saint Romain-En-Gier accident (d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), 2004) which denotes a frontal collision and occurred on April 5^{th}, 2004 between an empty high speed train and a works train on the line between Lyon and Saint-Etienne (France). It is due to a set of human errors and to maintenance works on tracks in a railway section. Firstly, the site was not protected by the safety agent in order to prevent the trains traffic in this area. Due to a false belief of the situation, the other human error consists in the erroneous authorization by the traffic agent to the works train that cross a closed signal which is out of its operating institution. Moreover, there is a lack of a full instructions document that indicates the signalling and the traffic direction for works train drivers. Consequently, a combination of these human errors bring about the frontal collision between trains, since they are running in the opposite direction but moving towards each other on the same track. Figure 6 shows the semantic annotation of the accident data in order to illustrate the GOSMO relevance for the safety related decision-making.

This accident scenario was tackled and analysed in a previous work (Debbech et al., 2019a) in order to illustrate the **Context** concept. More details about the scenario description and its analysis may be found in (d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), 2004). The accident was due to failures caused by **Stakeholders** such as the traffic agent and the works train driver. Moreover, both **Stakeholders** performed erroneous actions in their **Task** because there was no **Permission** granted to these **Stakeholder Roles** in a specific **Context** to carry out a safe **Task**. Then, the organized **Task** and its related parts did not consider all **Contexts**, especially the train works movement, the signalling and lists of instructions when the area changes. Consequently, the accident occurred due to the lack of the **Context** perception within the **Task** and the lack of a organizational control model for every **Stakeholder Role Permission** in a specific **Context**. Figure 7 shows the safety-control model annotation that could have been efficient to avoid this accident.

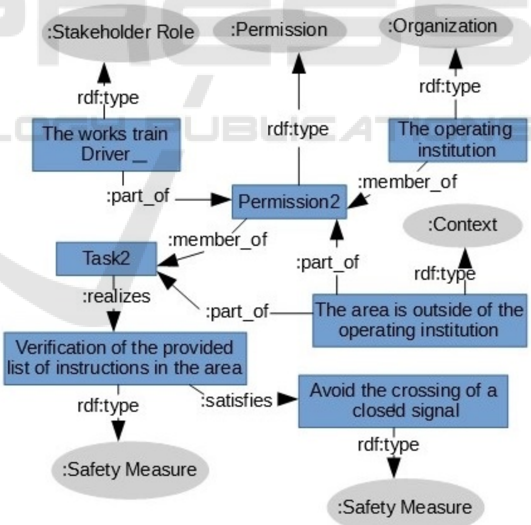

Figure 7: The annotation of the proposed safety control model for the Saint Romain-En-Gier accident.

These two accident scenarios demonstrate the GOSMO semantics flexibility in terms of the of concepts and relations between them. GOSMO shows its capability to annotate data and cover several aspects. Moreover, it shows the concepts polymorphism and their completeness regarding a set of real-world situations. The completeness of the defined semantics lies in their capability to interpret different critical notions. Then, GOSMO provides a high level of abstraction of goal-oriented safety management model, that can be adapted to a context.

5 CONCLUSION & FUTURE WORK

The main contribution in this paper consists in proposing a Goal-Oriented Safety Management Ontology (GOSMO), which is grounded in UFO, developed using the SABiO approach and based on standards and a thorough knowledge acquisition of involved knowledge domains such as GORE, Or-BAC and safety. Moreover, it establishes a semantic link between several domains for the purpose of identifying safety needs and refining them until the formalism implementation and the fulfilment of the GOSMO intended requirements. The proposed ontology contributes to the knowledge sharing, the conceptual modelling and the management of safety decisions from several perspectives which make it original. The considered issues in this study are summarized as follows.

Firstly, GOSMO provides a conceptualization of safety measures nature, its development from a goal oriented view and by a safety reinterpretation of Or-BAC concepts in order to improve safety decisions management. This conceptual analysis is based on the use of UFO's foundational concepts and relations between them. Then, it systematizes the ambiguous use of the term *safety measures* and its surrounding concepts in the safety critical systems terminology. Moreover, the safety oriented reinterpretation of Or-BAC concepts (such as organization, role, permission, context) aims to support safety measures development and it provides a structured and consistent safety control model for the SCSs design. Furthermore, GOSMO can be used as a reference model to support the ontological analysis and the conceptual clarification of real-world critical situations.

Secondly, the safety management is performed from a GORE perspective in order to deal with the complexity of the requirements engineering activity. Then, this aspect is relevant since the aim of GOSMO is to support safety management as soon as possible in the first design stages. Besides, a conceptual analysis of GORE concepts such as goal, requirement agent is provided with a matching between safety measures and Or-BAC concepts. In other words, safety notions are considered and integrated from the first design phases of SCSs for the purpose of obtaining a safe system behaviour. Then, it contributes to the RE process through the goals conceptualization and the safety constraints capture and specification.

Thirdly, GOSMO establishes a common vocabulary for the knowledge sharing in order to improve communication between actors domains and avoiding the semantic heterogeneity between them. Moreover, the proposed ontology provides a complete and consistent taxonomy which is able to represent and analyse several real situations. Then, the semantic annotation of real data set is performed using the GOSMO pattern design with any modification. It demonstrates the adaptability and the flexibility criteria of GOSMO, regarding different critical situations. The proposed concepts can be used interchangeably in order to refer to different aspects and types of phenomena. As a reference domain model, GOSMO may be reused for other safety critical domains since it is based on widely used standards and real-world semantics.

Finally, we are convinced that an operational version of GOSMO (implemented in OWL) can be used to make a semantic annotation of safety concerns in the system design model and components related to the occurrence of failures. In fact, we intend to strongly connect GOSMO to the proposed Dysfunctional Analysis Ontology (DAO) in future works. Then, the OWL formalization will improve the reuse of the GOSMO thanks to its powerful capacities in terms of expressiveness. Therefore, it will allow the development of a requirements traceability tool relating requirements and stakeholders goals with change requests that are tracked during the context-adaptive safety management process. This aspect will be the subject of future works. Finally, we will provide a formal characterization of GOSMO in order to allow the reasoning and the data retrieval related to safety and design aspects. Then, we intend to evaluate GOSMO by comparing it with results obtained by safety analysis integration methods and requirements elicitation tools. These contributions intend to provide a full safety-control methodology for the design of future autonomous systems.

REFERENCES

Ben Ayed, R., Collart-Dutilleul, S., Bon, P., Idani, A., and Ledru, Y. (2014). B formal validation of ERTMS/ETCS railway operating rules. In *International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z*, pages 124–129. Springer.

Borgida, A., Ernst, N., Jureta, I. J., Lapouchnian, A., Liaskos, S., and Mylopoulos, J. (2009). Techne: A (nother) requirements modeling language. *Computer Systems Research Group. Toronto, Canada: University of Toronto*.

Dardenne, A., Van Lamsweerde, A., and Fickas, S. (1993).

Goal-directed requirements acquisition. *Science of computer programming*, 20(1-2):3–50.

de Almeida Falbo, R. (2014). Sabio: Systematic approach for building ontologies. In *1^{st} Joint Workshop ONTO.COM / ODISE on Ontologies in Conceptual Modeling and Information Systems Engineering. FOIS, Rio de Janeiro*.

Debbech, S., Bon, P., and Collart-Dutilleul, S. (2018a). Improving safety by integrating dysfunctional analysis into the design of railway systems. *WIT Transactions on The Built Environment*, 181:399–411.

Debbech, S., Bon, P., and 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.

Debbech, S., Bon, P., and Collart-Dutilleul, S. (2019b). Towards semantic interpretation of goal-oriented safety decisions based on foundational ontology. *Journal of Computers*, 14(4):257–267.

Debbech, S., Collart-Dutilleul, S., and Bon, P. (2018b). 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.

d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), B. (2004). The saint-romain-en-gier accident bea-tt report (french version), rapport d'enquête technique sur l'accident ferroviaire survenu à saint-romain-en-gier le 5 avril 2004. Technical report, Ministère de l'Équipement, des Transports, de l'Aménagement du Territoire, du Tourisme et de la Mer, METATTM.

d'Enquêtes sur les Accidents de Transport Terrestres (BEA-TT), B. (2005). The longueville accident BEA-TT report (french version), rapport d'enquête technique sur l'accident ferroviaire survenu à longueville le 16 février 2005. Technical report, Ministère de l'Équipement, des Transports, de l'Aménagement du Territoire, du Tourisme et de la Mer, METATTM.

El Kalam, A. A., Benferhat, S., El Baida, R., Saurel, C., Balbiani, P., Deswarte, Y., Trouessin, G., et al. (2003). Organization based access control. In *The IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Come, Italy, June*, page 120. IEEE.

Falbo, R. D. A. and Bertollo, G. (2009). A software process ontology as a common vocabulary about software processes. *International Journal of Business Process Integration and Management*, 4(4):239–250.

Firesmith, D. G. (2005). A taxonomy of safety-related requirements. In *International Workshop on High Assurance Systems (RHAS'05)*.

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.

Guizzardi, G. (2005). *Ontological foundations for structural conceptual models*. PhD thesis, University of Twente, Enschede, The Netherlands.

IEEE 610.12 (1990). Standard glossary of software engineering terminology. Std, IEEE.

ISO/IEC/IEEE 29148 (2011). ISO/IEC/IEEE 29148: Systems and software engineering – Life cycle processes –Requirements engineering. Std, IEEE.

Méry, D. and Merz, S. (2007). Specification and refinement of access control. *J. UCS*, 13(8):1073–1093.

Negri, P. P., Souza, V. E. S., de Castro Leal, A. L., de Almeida Falbo, R., and Guizzardi, G. (2017). Towards an ontology of goal-oriented requirements. In *CIbSE*, pages 469–482.

Provenzano, L., Hanninen, K., Zhou, J., and Lundqvist, K. (2017). An ontological approach to elicit safety requirements. In *2017 24th Asia-Pacific Software Engineering Conference (APSEC)*, pages 713–718. IEEE.

Souag, A., Salinesi, C., Mazo, R., and Comyn-Wattiau, I. (2015). A security ontology for security requirements elicitation. In *International symposium on engineering secure software and systems*, pages 157–177. Springer.

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

Wang, X., Guarino, N., Guizzardi, G., and Mylopoulos, J. (2014). Towards an ontology of software: a requirements engineering perspective. In *8^{th} International Conference on Formal Ontology in Information Systems (FOIS), Rio de Janeiro*, pages 317–329.

Yu, E. (2011). Modelling strategic relationships for process reengineering. *Social Modeling for Requirements Engineering*, 11:2011.

Zhou, J., Hanninen, K., Lundqvist, K., Lu, Y., Provenzano, L., and 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.

Zhou, J., Hänninen, K., Lundqvist, K., and Provenzano, L. (2017). An ontological interpretation of the hazard concept for safety-critical systems. In *The 27th European Safety and Reliability Conference ESREL'17, 18-22 Jun 2017, Portoroz, Slovenia*, pages 183–185.