The Journal of Systems & Software 183 (2022) 111082

Contents lists available at ScienceDirect

The Journal of Systems & Software

journal homepage: www.elsevier.com/locate/jss

Model-based safety engineering for autonomous train map ☆,☆☆

Nadia Chouchani *, Sana Debbech, Matthieu Perin

Institut de Recherche Technologique Railenium, 180 Rue Joseph-Louis Lagrange, Valenciennes 59300, France

ARTICLE INFO

Article history:
Received 10 September 2020
Received in revised form 12 February 2021
Accepted 27 August 2021
Available online 10 September 2021

Keywords:
Model-based safety engineering
Safety ontology
Model-driven engineering
Safety/assurance case
Railway infrastructure model
Autonomous train

ABSTRACT

As a part of the digital revolution of railway systems, an autonomous driving train will use a complete and precise map of railway infrastructure to conduct operational actions. Nevertheless, the full autonomy of trains depends on the safety decisions management capacity both on-board and track-side. These decisions must be refined into safety requirements in order to continuously check the consistency between the perceived infrastructure and safety related properties. However, traditionally, the integration of safety analysis requires the intervention of human agent skills. This may be error-prone and in interference with the embedded aspect of the train map. In this paper, we propose a model-based approach to match between safety concepts expressed as an ontology, a derived safety model and a safety-extended railway infrastructure map model for autonomous trains. This approach is validated by railway safety case studies for autonomous train map. The integration of this model-based safety solution from the early stages of the map system design improves the safety decisions management process.

1. Introduction

The context of this research is the autonomous train project launched in 2016 as part of *Tech4Rail*, an ambitious technological program initiated by the direction of railway systems at *SNCF*, in France. The future system that follows from this vision is based on automatic train control (*ATC*) system. The latter is organized on the basis of three functional layers, i.e, (*i*) Automatic Train Protection, (*ii*) Automatic Train Operation (*ATO*) and (*iii*) Automatic Train Supervision. The second level of the *ATC* architecture aims to automate the driving functions of the train. Thus, the *ATO* performs railway driving by executing all the operational functions without human intervention. It is structured around several transverse and functional on-board subsystems like the train positioning, signaling recognition and environment monitoring. These main subsystems require a precise description of the rail network infrastructure. In this work, we propose a model-based approach to develop an on-board map for the autonomous train referring to the topology of the tracks and signaling. Indeed, the proposed model provides a topological description of the railway infrastructure and the signaling objects geo-located by a positioning system. However, the autonomous railway transportation are complex systems that require high safety integrity level. Traditionally, regular human interventions rely on the skills of human agents to ensure the integration of safety analysis. Nevertheless, these practices make the system verification difficult and challenging for safety assurance. Thus, to make the train become autonomous and safe, we identify the following research question (RQ) for this study:

RQ: How could the development of on-board map be enhanced by the integration of safety-related information for assisting the overall autonomous train subsystems ?

To avoid potential hazards, we provide a general framework for design and verification of the mapping system of the autonomous train. In order to have a consistent design process, domain ontologies are used to consider safety rules into system's components and to clarify safety management concepts. The main contribution is the proposal of a novel model-based safety approach which takes into account railway infrastructure information for autonomous train driving.

The outline of this paper is as follows. The next Section 2 introduces an overview and the motivations of our work. Section 3 details the proposed model-based approach. Section 4 is devoted to describe railway case studies for the autonomous train map. In Section 5, we present the related work. Finally, the paper concludes and introduces the future work.

☆ Editor: Raffaela Mirandola.

☆☆ This research work contributes to the french collaborative project TFA (autonomous freight train), with SNCF, Alstom Transport, Hitachi Rail STS, Capgemini and Apsys. It was carried out in the framework of IRT Railenium, Valenciennes, France, and therefore was granted public funds within the scope of the French Program "Investissements d'Avenir". Supported by French Driver-less Freight train project.

* Corresponding author.
E-mail addresses: nadia.chouchani@railenium.eu (N. Chouchani), sana.debbech@railenium.eu (S. Debbech), matthieu.perin@railenium.eu (M. Perin).

https://doi.org/10.1016/j.jss.2021.111082
0164-1212/

2. Overview and motivations

2.1. Safety ontologies

In order to deal with the complexity of safety management process, safety analysis results must be considered from the first design stages of critical systems (Debbech et al., 2018a). This practice is widely recommended by safety standards, e.g., *EN50129* (CENELEC, NF EN 50129, 2003) for railway systems and *ISO/DIS 26262-1* (ISO/DIS 26262-1, 2009) for the automotive domain. With the aim to provide a conceptualization of dysfunctional analysis, a reference domain ontology called *DAO* (Dysfunctional Analysis Ontology) was previously developed (Debbech et al., 2020). *DAO* is grounded on Unified Foundational Ontology (*UFO*) which is an upper-level ontology (Guizzardi, 2005). It establishes a common vocabulary for the knowledge sharing between safety engineers and system designers. *DAO* integrates both human errors and technical failures from both system and environment perspectives. It has been used on the safety analysis of railway systems. Based on the clarification of the ambiguous use of the failure concept, its causes, effects and related hazards, a set of safety measures may be identified in order to mitigate hazards. Otherwise, *DAO* is developed with the purpose of allowing a well-established formalization of a "Failure" and its surrounding concepts, which is used for the development of new safety critical systems, such as autonomous trains. In order to have an interoperable view of safety analysis methods, *DAO* is compliant with safety standards definitions of concepts. In other words, the proposed conceptual clarification aims to approximate the ideal conceptualization and to have an unambiguous interpretation of dysfunctional analysis concepts. As an example, we may refer to the proposed definition of the concept of Hazard from the standard EN50126 (CENELEC, NF EN 50126-1, 2017) as "a condition that may lead to accidents". In order to clarify the ambiguous use of these terms, we proposed to define a Hazard as a subtype of a situation (in regard to *UFO*), which is inherent to an exposure (it is activated by a hazardous state) and is prevented by safety measures. Furthermore, *DAO* has been formalized in Web Ontology Language (*OWL*) and evaluated using logic reasoning in order to have a knowledge basis.

Indeed, the development of safety measures requires a control organization which is integrated in adaptive socio-technical systems, such as railway systems. From this point of view, *GOSMO* – a Goal-Oriented Safety Management Ontology – was developed with the aim of matching the safety knowledge and the Goal Oriented Requirements Engineering (*GORE*) concepts (Debbech et al., 2019). The safety measures development process is proposed based on the Organization-Based Control Access (*Or-BAC*) model, which is traditionally used to ensure the information systems security (El Kalam et al., 2003). This contribution is motivated by the reinterpretation of *Or-BAC* concepts from a safety perspective and their alignment with safety and *GORE* concepts. Thus, *GOSMO* incorporates 3 main modules:

- *Or-BAC* concepts for the safety management process representation;
- *GORE* concepts for the semantic bridge between safety and requirements engineering phases;
- A set of *DAO* concepts for the matching between safety measures and safety goals and their management;

Furthermore, *GOSMO* is grounded on *UFO* in order to help the semantic matching with *DAO*. Otherwise, *UFO* provides a complete set of concepts and relations which is able to cope with the semantic heterogeneity induced by knowledge domains combination. Then, *GOSMO* is built using the Systematic Approach for Building Ontologies (*SABiO*) (de Almeida Falbo, 2014). *SABiO* methodology incorporates best practices of ontology engineering and ontological distinctions of foundational ontologies. In order to provide a high level of semantic expressivity and to have a reasoning support, *GOSMO* is formalized in *OWL* and evaluated using logic reasoning. Finally, the integrated railway knowledge is validated by the application of *GOSMO* to two real critical accidents and a remotely-operated task of autonomous trains (Debbech et al., 2018b). This ontological approach is used from the first design stages in order to integrate dysfunctional analysis and to support the safety decisions making process. The integrated safety measures are adaptive to contexts and they are defined to satisfy safety goals. The formalization of this semantic link between safety measures and safety goals is crucial since it improves the safety assurance and hazards mitigation. Further details about *DAO* and *GOSMO* development process may be found, respectively in Debbech et al. (2020, 2019). In the present study, *DAO* and *GOSMO* are used and combined with other models to have a structured safety model-based process. In order to fulfill autonomous system's needs, a specific fragment of *DAO* is extracted and used in this approach. The reused *DAO* and *GOSMO* concepts are defined in Section 3.

2.2. Railway infrastructure modeling

Upcoming autonomous transportation systems such as driverless trains, need a dense, coherent and high-definition representation of their surroundings in order to accomplish their mission safely and efficiently. Thus, digital maps are a key challenge for the railway industry, mainly because this topic has not been known as a core competence of manufacturers nor researchers until now. Especially, the autonomous train on-board mapping subsystem must be capable of gathering a wide variety of data and providing them to a set of different users, i.e the other subsystems, with a strong variation in the nature of needed information. In order to overcome these challenges and since traditional digital maps may not be optimal nor capable, our proposal is to design the autonomous train map following a Model-Based Engineering approach. The proposed solution is associated with state-of-the-art results from international initiatives on digital twin representation for railway infrastructures. In this paper, we propose the Autonomous Train Map Ontology (*ATMO*) which is a Conceptual Independent Model (see next section) representing all the infrastructure objects needed by the future train in order to provide safe and accurate service, based on users requirements. Some modeling research proposed to model the railway infrastructure but they are limited to a domain or a single use case. They are presented briefly in Section 5. Such limitations are incompatible in our opinion with the multiple map users such as perception, navigation, positioning, environment monitoring, and safety automation subsystems. *ATMO* is also aligned with existing standards like *RailTopoModel*[1] (RailTopoModel, 2016) for abstract and topological representation, *Eulynx*[2] for the physical and functional modeling of the signaling system and *IFC Rail*[3] for civil engineering-related elements such as track structures. Platform Independent and Platform Specific models can then be derived from *ATMO* through automatic processes to generate an implementation that will hold all the needed objects data.

[1] From UIC: International union of railways, https://uic.org/.

[2] https://www.eulynx.eu/.

[3] Industry Foundation Class, Rail part: https://www.buildingsmart.org/ifc-rail-candidate-standard-is-available-for-review-and-comment/.

2.3. Model-based engineering

In an attempt to ensure consistency between safety analysis and autonomous train map design, we propose to follow a model-based approach. In this multidisciplinary context, we opted for conceptual modeling with the aim to tackle the complexity of the system (Rodrigues da Silva, 2015). This modeling is a key element to generalize the use of *Model-Based Engineering* (*MBE*) and to clarify the semantic interpretation of domain concepts. But which architecture is suitable to build conceptual models for safety critical domains?

According to *OMG* (MDA Guide Revision 2, 2014), the *MBE* consists in using a set of complementary models, each corresponding to a specific aspect of the system. A model, being an abstraction of reality, makes it easier to understand the system to be developed. However, it does not represent all of reality but at best the aspect that we want to exploit. Therefore, a view is a representation of the model in a projection of an hyper space to simplify it. In this work, the representation is based on *UML* (Unified Modeling Language) (Unified Modeling Language v2.5, 2015), a semi-formal, enrichable and structured language. The modeling task is structured around the expertise knowledge and competency questions, and based on semantic formalisms, transformation rules and frameworks for transition from one model to another (Debbech et al., 2020). Indeed, the *MBE* can ensure the traceability of business and safety requirements which are modeled from the early stages of the development process, hence the minimization of the downstream design effort. Three main types of models are defined:

CIM (Computational Independent Model): represents the business model which is independent of any computer system. At this level, we used a safety and railway infrastructure ontologies.

PIM (Platform Independent Model): independent of the technical platform, this model is a partial view of a *CIM*. It represents the business functional logic and describes the system, using classes and *OCL* constraints (Object Constraint Language). At this level, two *PIM*s are derived from the ontologies.

PSM (Platform Specific Model): depending on the technical platform, it is used as a basis for code generation (Chouchani and Abed, 2020).

The transition from one model type to another is done by tools for model transformation according to user designed rules. A transformation is defined as an operation on a model that produces another one, and which conforms to formal syntax and semantics (Lano et al., 2018).

MBE is a valuable methodology to conceive system assurance cases argumentation. The assurance cases are claims, arguments and evidence concepts that justify and assess confidence in the system critical properties, such as safety and security (omg, 0000). For instance, assurance case reports can be generated by model-to-text transformation (Wei et al., 2019). Recently, model-based system assurance has attracted considerable research attention. In this context, the Structured Assurance Case Metamodel (*SACM*) (omg, 0000) was specified by the Object Management Group for representing structured assurance cases. This metamodel was intended to improve standardization and interoperability. Its specification evolved from experts collective safety/security knowledge and the associated experiences in the domain.

3. The safety model-based approach

The general architecture of our approach is given in Fig. 1. It is composed of three components: (*i*) safety analysis, (*ii*) model extension, and (*iii*) safety management. The subsections below provide details on these components.

3.1. Safety analysis

The first step is the extraction of relevant concepts from *DAO* in order to perform safety analysis for autonomous systems. Fig. 2 shows the *DAO* fragment which represents the required concepts and relations between them in *OntoUML* (Guizzardi, 2005). The latter is a *UML* profile for conceptual modeling and it incorporates foundational distinctions defined in *UFO*. The interpretation of *failure* and its related concepts in real-world semantics may be found in Debbech et al. (2020). The semantic interpretation of the main *DAO* concepts are detailed in Table 1, based on the knowledge acquisition step from safety engineering standards.

Once the autonomous system's structure is known, this *DAO* fragment may be applied in order to identify failures and their effects for each system's component. The obtained DAO instantiation is considered to be the *Safety Model* which depends on a specific dangerous event. This safety model is deduced from *DAO* and includes individuals of *DAO* concepts and relations between them.

Individuals of DAO concepts represent the safety analysis elements of the considered system. According to the performed safety analysis, a set of safety measures are defined in order to mitigate the perceived hazard. Safety rules are defined as a set of actions or safety measures to be realized within a task in order to achieve the required safety integrity level. Furthermore, safety rules are assumed to be available in a specific context which may be composed of sub-contexts. They are defined based on the railway expertise acquired from domain experts and referential. Thus, safety rules are considered as an aggregation of 3 concepts: safety measures, a specific context and conditions that validate the rules application. These safety rules are expressed from a high level of abstraction in order to prevent perceived hazards, such as collisions. Furthermore, they are integrated from the first design stages in order to prevent, as soon as possible, safety properties violation.

3.2. Model extension

As part of this approach, we are working on the modeling of a high definition on-board map or cartography, represented by *ATMO* and based on different standards including all information on infrastructure, signaling and even constructions such as tunnels and bridges, eventually in *3D* representation. Data integration and interoperability are complex challenges due to the heterogeneous nature of data and standards. To overcome this problem, we propose to apply semantic data modeling techniques to allow integration of heterogeneous information and make coherencies of cartographic elements in addition to the safety rules obtained from the previous step. The adopted methodology is structured around the following main steps:

3.2.1. Specification

The specification of the data model is defined by a set of functional and non-functional requirements derived from the established needs of the implementation of the autonomous train in the context of the project.

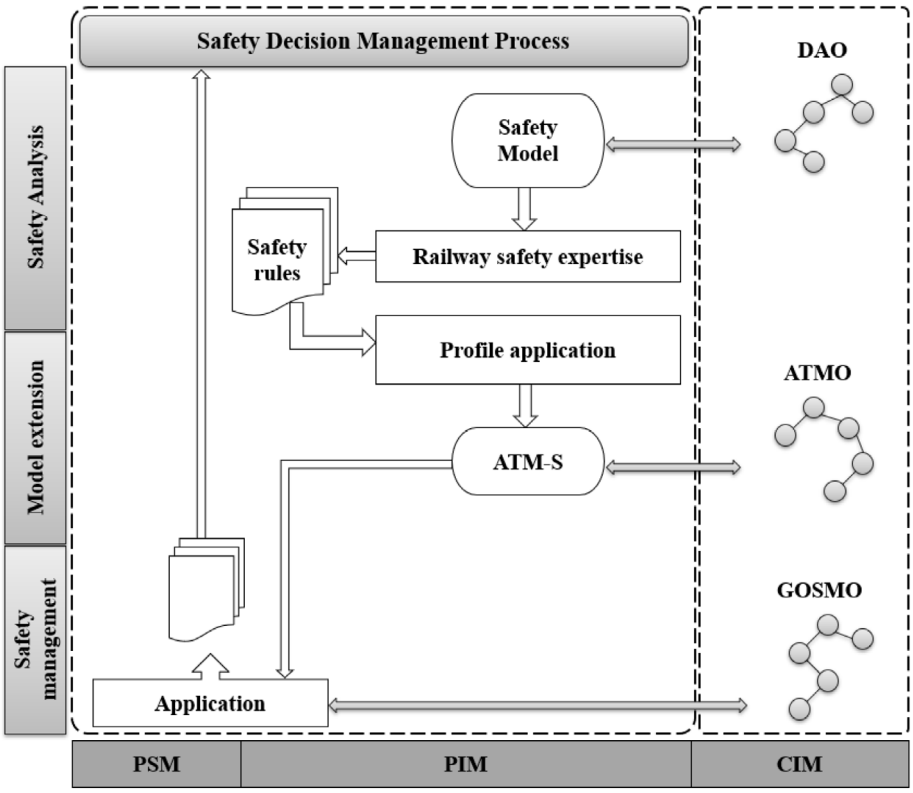

Fig. 1. General architecture.

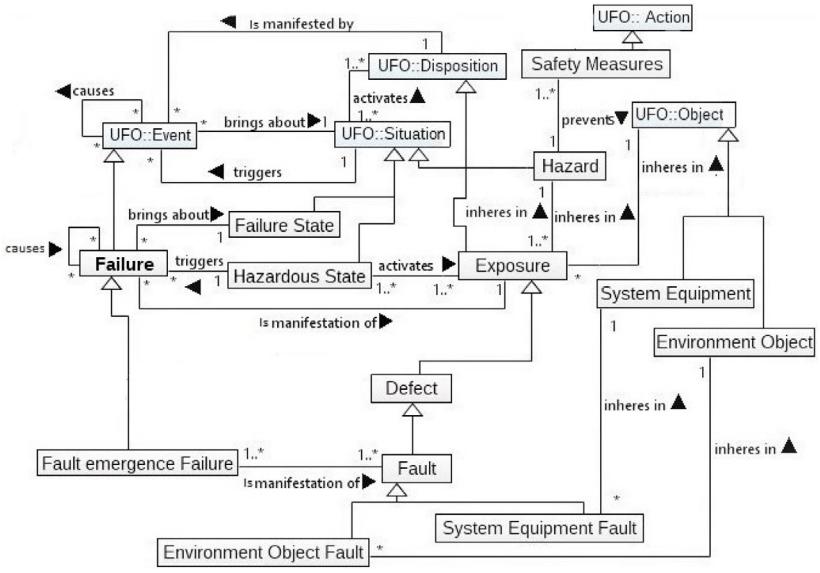

Fig. 2. A fragment of *DAO* conceptual model.

3.2.2. Knowledge acquisition

Several areas of knowledge are at the heart of this work. This step was carried out by defining Ontology Design Patterns (*ODP*s). It involves defining all the concepts to be used in the ontology, the relationships between them and also a documentation corresponding to the different concepts. In order to extract the domain knowledge of the ontology *ATMO*, we used three sources for explicit and implicit acquisitions. First bibliographic research of articles and books was necessary to form a background on the whole field and questions on more specific use cases. Then we collaborated with experts, especially in the signaling field. We had discussions around *EULYNX UML* model to which we had a read access. Finally, the reuse and re-engineering of non-ontological resources were applied to the model construction. The analysis of the various cited resources allowed to define data dictionary that meets the needs to be covered by *ATMO*.

3.2.3. Conceptualization

The vocabulary and the *ATMO* model are mainly based on the elements of *RTM*, *IFC Rail* and *EULYNX*, relying on both their *UML* models and natural language documentation. The designed model contains four packages, each one references one module of *ATMO*.

Table 1
The semantic interpretation of *DAO* concepts.

Concepts	Definitions	Source
Failure	A **Failure** is a *subtype of* **UFO::Event**. It *brings about* a **Failure State** and *is triggered by* a **Hazardous State**. A **Failure** *causes* another one (cascading failure) and *is manifestation* of an **Exposure**.	IEC 61508, Norme Internationale (2000)
Exposure	An **Exposure** is a *subtype of* **UFO::Disposition** (a special type of **Moment**). It denotes the **Exposure Moment** which *inheres in* **UFO::Object** and is *activated by* the **Hazardous State** (a *subtype of* **UFO::Situation**).	EN50126 (CENELEC, NF EN 50126-1, 2017)
Defect & Fault	A **Defect** is a *subtype of* **Exposure**. A **Defect** denotes a **Fault** when it is *manifested by* a **Fault emergence Failure**. A **Fault** *subsumes* an **Environment Object Fault** and a **System Equipment Fault**.	IEC 61508, Norme Internationale (2000)
Fault emergence Failure	A **Fault emergence Failure** is a *subtype of* a **Failure**. It represents any **Failure** caused by an **Object Fault**.	IEC 61508, Norme Internationale (2000)
Hazard	**Hazard** is a subtype of a **UFO::Situation**, which is inherent to an **Exposure** (it is activated by a Hazardous State) and *is prevented by* **Safety Measures**.	EN50126 (CENELEC, NF EN 50126-1, 2017)
Safety measure	**Safety Measure** is an **UFO::Action** which *prevents* a **Hazard** and *satisfies* a **Safety Goal**.	EN50126 (CENELEC, NF EN 50126-1, 2017)

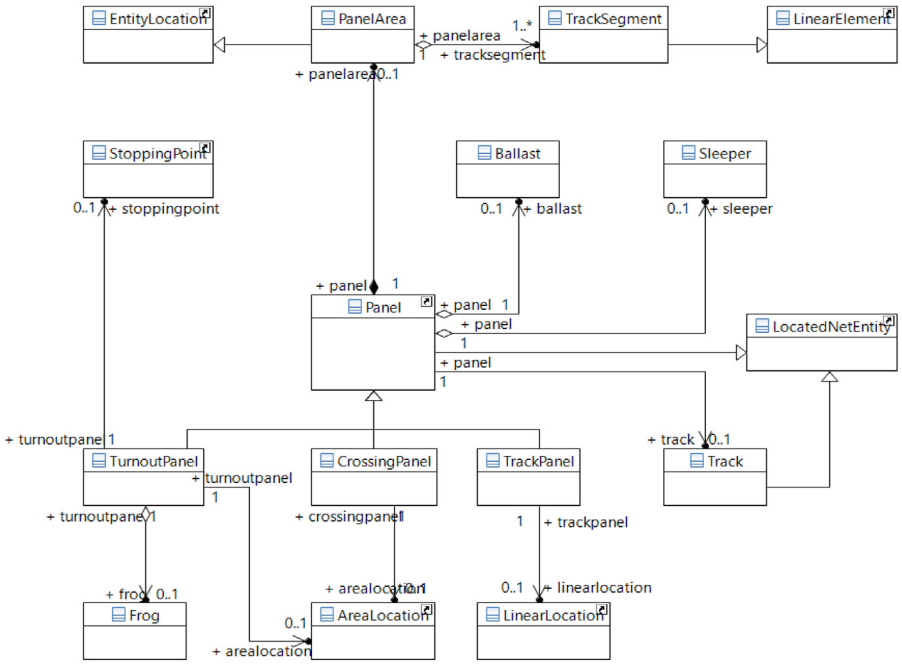

Fig. 3. An excerpt of the *UML* "Track" package of the map *PIM*.

An excerpt from the *UML* package of "Track" is shown in Fig. 3 and described in Table 2. Due to confidentiality restrictions linked to the project, not all packages can be detailed here.

The methodology of *ATMO* design follows a compositional approach. The different modules, each corresponding to a dimension of the railway map, are constructed and subsequently composed to constitute the global model.

3.2.4. Integration

The purpose of this step is to integrate the safety rules into the conceptual map model (*PIM*). The aim is to get a view of the rail infrastructure system coupled with safety measures in order to be able to take on-board safety decision actions in an autonomous way. The extracted safety rules from the previous component, are expressed in natural language. In order to have a safety decision-making framework, safety rules are transformed from natural language to a machine-readable language. In this work, the *SWRL* (Semantic Web Rule Language) (O'connor et al., 2005) is chosen thanks to its formal syntax and semantics and to its capabilities to express and integrate rules into ontologies.

For the safety decision management process, detailed in the following subsection, we relied on the safety actions ("DAO:: Safety Measures") associated to each context.

In order to integrate these safety measures into the map conceptual model, we defined and apply a *UML* profile, derived from *DAO*, to the *PIM* obtained from *ATMO*. The resulting *PIM* is *ATM-S*, the autonomous train map model integrating safety assurance aspect. The main aim of the profile is to capture the different situations related to the infrastructure objects and make the correspondence with the integrated safety rules.

For example, "Exposure", "Hazard" and "Hazardous State" are stereotypes applied to the "TurnoutPanel" entity of the "Track" *UML* package.

3.3. Safety management

Safety management is a crucial process for autonomous systems safety assessment since it is based on both perception and decision steps. In order to provide a structured safety management, safety measures derived from safety analysis must be linked to safety goals. This knowledge merging allows a shared

Table 2
UML "Track" package description.

Entity	Description
LocatedNetEntity	From *RTM*, it represents a functional object in the rail network located on the topology.
EntityLocation	From *RTM, it is the location of a network entity.*
LinearLocation	From *RTM*, a linear location consists on an ordered list of network elements.
AreaLocation	From *RTM*, it is an area located in the network.
Panel	It is a homogeneous section in configuration inheriting from "LocatedNetEntity" allowing a tiling of the infrastructure.
PanelArea	It is an area preempted by the functional object represented by the "Panel" which carries the topological objects. It is a geographic area ("EntityLocation")
TrackPanel	A simple, homogeneous track section, inheriting from "Panel"
CrossingPanel	A section representing a crossing of tracks inheriting from "Panel" linked to a geographical area "AreaLocation".
TurnoutPanel	A section of track representing a switch inheriting from "Panel" linked to a geographical area "AreaLocation".
Frog	Frog of turnout inheriting from "LocatedNetEntity".
Track	Functional and organizational object representing a channel inheriting from "LocatedNetEntity" and references "Panel" type objects.
TrackSegment	Functional cut-out of the train guidance which carries the *RTM* "LinearElement" topological object.
LinearElement	From *RTM*, a linear segment representing a network element.
StoppingPoint	Fouling point to stop the train.
Ballast	Track ballast.
Sleeper	Track sleepers.

view between safety and system objects with the aim of goals satisfaction. This is the subject of the third step of the proposed approach using *GOSMO* in order to orchestrate safety decisions management process. Fig. 4 shows the *GOSMO* fragment which includes pertinent concepts for autonomous systems safety management.

The organization-based control model allows the assignment of roles using the concept **Stakeholder Role** to *ATMO* components. Then, a **Permission** is assigned to perform a **Task** that realizes **Safety Measures** in a specific application **context**. Safety rules expressed in SWRL allow an allocation of safety measures to specific ATMO objects in a specific operational context.

This *Or-BAC* reinterpretation from a safety-perspective is suitable for the adaptive safety management of autonomous systems, such as railway systems. *GOSMO* conceptual model may be used to annotate the ATMO model as a profile in order to have a semantic link between them. This semantic annotation avoids ambiguities and allows consistency with system models. The considered goal-oriented perspective is useful for the requirements analysis process in a later stage of system development.

Table 3 shows *GOSMO* concepts definitions in order to improve readability. This ontology has been formalized in Ontology Web Language-Description Logic (OWL DL),[4] with the aim to reach a high level of semantic expressivity and to have a reasoning framework for safety decisions management. A set of DL axioms has been defined to constrain the proposed terminology and to help the data retrieval process (Debbech et al., 2019). Otherwise, the proposed framework aims to have an automatic safety decisions making process thanks to the predefined SWRL rules. It may be used from the first design stages of safety critical systems design.

4. Safety cases: Application for autonomous train map

The proposed map system performs critical functions thus requires safety justifications. In the following, we detail assurance cases, in particular, safety cases. As specified by Kelly and Weaver (2004), a safety case should communicate a clear, comprehensible and defensible argument that a system is acceptably safe to operate in a particular context.

Safety cases can be represented either textually, in natural language, or graphically. In this section, we refer to goal structuring notation in order to analyze ans validate the satisfaction of safety goals by the integration of safety rules. Then, the proposed approach is illustrated by two railway case studies.

4.1. Goal structuring notation

The Goal Structuring Notation (*GSN*) (Kelly and Weaver, 2004), widely adopted in the literature, is a graphical notation used to express system properties argumentations in a clear and well-structured way. Thanks to its powerful notation, *GSN* enables to represent structural system safety arguments. In order to produce a robust safety case, we followed the *GSN* metamodel which is compliant to *SACM* and represents the most popular approach for system assurance (Wei et al., 2019). An excerpt of the resulted goal structure is shown in Fig. 5.

The main goal (*G1*) of this structured safety case, is to operate the autonomous train map system safely with compliance to safety requirements. A sufficient mitigation and the avoidance of hazards are the key features to attend this goal. The latter is decomposed and sub-goals (*G2* and *G3*) are then identified. The demonstration of safety depends on contexts (*C1*, *C2* and *C3*) and is based on assumptions or justifications (*A1*). The solution (*Sn1*) guarantees to avoid hazards.

With the aim to show the attainability of the identified goal *G1* and therefore the safety of the proposed *ATM* system, the following sections present two case studies detailing the different hazards from *DAO* (*C3*) and safety rules (*Sn1*) application for each case.

4.2. Case study 1: Side collision

In order to validate the proposed approach, we refer to a railway case study which illustrates its three phases. As a potential risk related to infrastructure or rolling stock failures, the

[4] https://www.w3.org/2007/OWL/wiki/images/9/9a/Pfps-f2f1.pdf.

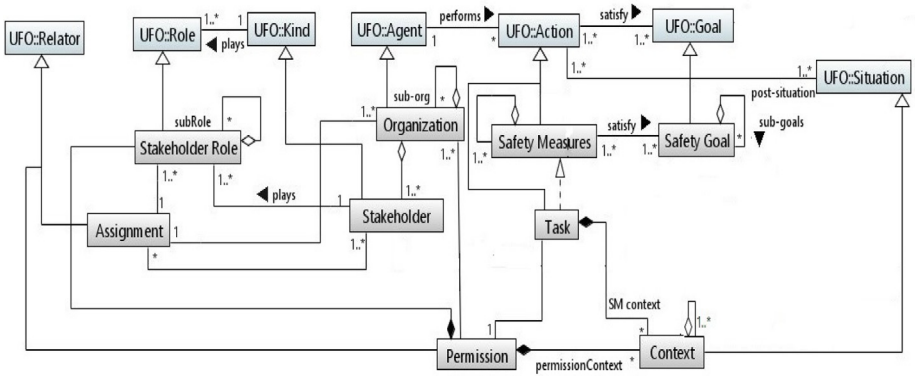

Fig. 4. A fragment of *GOSMO* conceptual model for autonomous systems safety management.

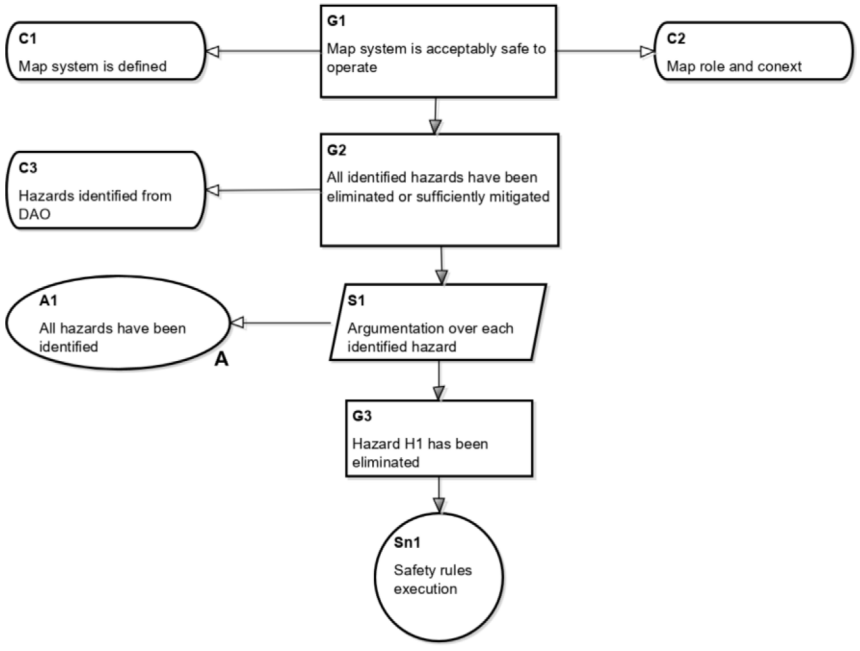

Fig. 5. An excerpt of the goal structure using *GSN*.

Table 3
GOSMO concepts definitions.

Concepts	Definitions
SafetyMeasure	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**).
Task	A **Task** is accomplished by a **Permission** assigned to **StakeholderRole** by an **Organization** according to a specific **Context**.
StakeholderRole	A **StakeholderRole** is a *subtypeOf* **Role**. It *is played by* a **Stakeholder** (a *subtypeOf* **Kind**).
Context	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**.
Organization	An **Organization** is a *subtype of* **Agent** and it *hasPart* **sub-organizations**. An **Organization** *hasPart* one or many **Stakeholders** that are a *subtypeOf* **Kind**.
Assignment	An **Assignment** is a *subtypeOf* **Relator** and it denotes the **StakeholderRole** assignment to a **Stakeholder** by an **Organization**.
Permission	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**.

side collision occurs when a train hurts another one at a track section which connects two tracks with different provenances. Fig. 6 represents the side collision between two trains that intend to join the same track and direction.

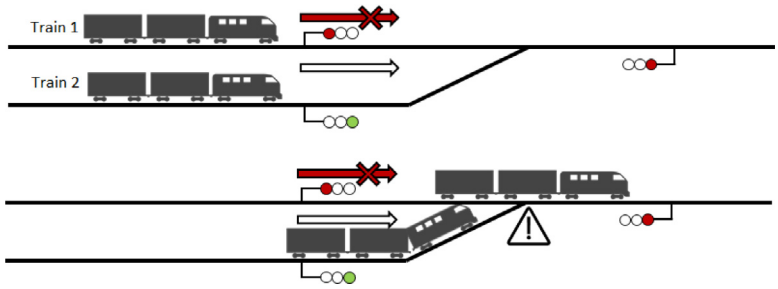

Fig. 6. Presentation of the side collision risk in railway operation. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

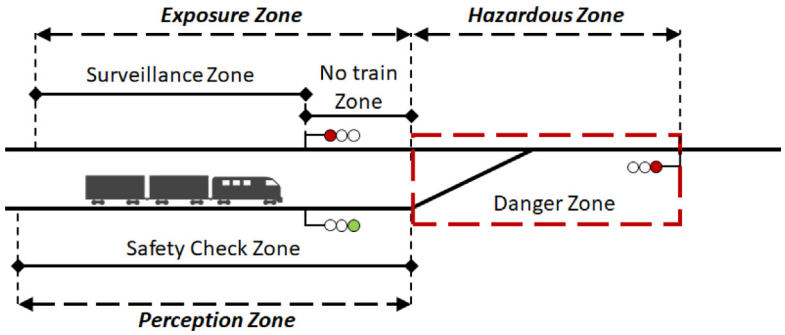

Fig. 7. Added Safety-related zones for a turnout related to the side collision hazard.

Indeed, train 1 crosses the first closed signal (red light) and keeps immobile at the merging track. Train 2 crosses the open signal (green light) and longitudinally hurts train 1.

The application of the proposed approach to this case-study allows representation of several zones to the infrastructure description in order to perform safety analysis. Side collision represents the "Hazard" concept in the *DAO* conceptual model. As depicted in Fig. 7, the extracted candidate concepts after matching with *DAO* are the following:

- **Exposure Zone** represents the zone which activates the hazard occurrence.
- **Danger Zone** represents the zone which inheres in the hazard (Side collision).
- **System Equipment** represents infrastructure components such as signal and tracks.
- **Hazardous Zone** represents the danger zone.
- **No train zone** represents the failure state.
- **Perception Zone** The perception of context to manage safety decisions.

The topological elements corresponding to this section of the infrastructure are:

- **Turnout** represented by "TurnoutPanel"
- **Signal** represented by a "LocatedNetEntity"
- **Area** represented by "AreaLocation"

This infrastructure decomposition allows the development of tailored safety rules. In order to avoid side collision, a set of safety rules are defined in natural language as follows:

1. The train must be in 30 km\h as a maximal speed in the surveillance zone in order to perceive the context.
2. In the case of crossing of a closed signal, a deployment of technical device of train protection system, such as crocodile must be performed in order to trigger the emergency stop before the danger zone.

```
Safety Rule 1:

<swrlx:classAtom>
   <owlx:Class owlx:name="SystemEquipment" />
   <ruleml:var>x1</ruleml:var>
</swrlx:classAtom>
<swrlx:classAtom>
   <owlx:Class owlx:name="Train" />
   <owlx:SubclassOf>
   <owlx:Class owlx:name="SystemEquipment">
   </owlx:SubclassOf>
</swrlx:classAtom>
<owlx:Class owlx:name="Train" />
        <owlx:ObjectRestriction owlx:property="hasSpeed">
        <swrlx:datarangeAtom>
        <owlx:DataValue owlx:datatype="&xsd;int">30</owlx:DataValue>
        <ruleml:var>x1</ruleml:var>
        </swrlx:datarangeAtom>
</swrlx:classAtom>
<swrlx:classAtom>
        <owlx:Class owlx:name="Task" />
        <ruleml:var>x1</ruleml:var>
        <swrlx:individualPropertyAtom  swrlx:property="hasContext">
        <ruleml:var>task</ruleml:var>
        <ruleml:var>theSurveillanceZone</ruleml:var>
        </swrlx:individualPropertyAtom>
</swrlx:classAtom>
```

Fig. 8. The first SWRL safety rule for case study 1.

In order to automatize the safety decisions management process, these safety rules are transformed in SWRL as shown in Figs. 8 and 9.

These safety decisions management is performed according to *GOSMO* conceptual model. Fig. 10 represents the safety management related to this case study. The permission is assigned to the technical device to trigger emergency stop if the speed curve profile is in state * or *KO* and the train position is close to the closed signal. These elements represent the perceived context related to this task.

The proposed case study illustrates the rigorous choice of *DAO* and *GOSMO* concepts for autonomous systems and their matching with ATMO. The proposed approach may be applied to other case studies in order to validate the flexibility to cover several critical situations.

```
Safety Rule 2:

<swrlx:classAtom>
            <owlx:Class owlx:name="Task" />
                  <ruleml:var>x1</ruleml:var>
          <swrlx:individualPropertyAtom  swrlx:property="realizes">
          <ruleml:var>task</ruleml:var>
          <ruleml:var>deploymentofTechnicalDeviceofTrainProtectionSystem</ruleml:var>
          </swrlx:individualPropertyAtom>
          <owlx:IntersectionOf>
        <swrlx:individualPropertyAtom  swrlx:property="hasContext">
        <ruleml:var>task</ruleml:var>
        <ruleml:var>crossingOfaClosedSignal</ruleml:var>
        </swrlx:individualPropertyAtom>
          </owlx:IntersectionOf>
</swrlx:classAtom>
<swrlx:classAtom>
            <owlx:Class owlx:name="SafetyMeasure" />
    <ruleml:var>x1</ruleml:var>
          <swrlx:individualPropertyAtom  swrlx:property="satisfy">
          <ruleml:var> deploymentofTechnical deviceofTrainProtectionSystem</ruleml:var>
          <ruleml:var> triggerTheEmergencyStopBeforeTheDangerZone </ruleml:var>
                    </swrlx:individualPropertyAtom>
</swrlx:classAtom>
```

Fig. 9. The second SWRL safety rule for case study 1.

4.3. Case study 2: Real railway accident of Saint-Romain-En-Gier

In order to validate the capability of the proposed solution to represent real critical scenario, we illustrate it by a railway accident of Saint-Romain-En-Gier (Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004). This accident denotes a frontal collision that occurred on April 5th, 2004 between an empty high speed train and a works train on the french line Lyon/Saint-Etienne. The accident was due to track works between the cities of Rive-de-Giers and Givors, in a railway section equipped with reverse signaling. The works carried out on the night of the 4th to 5th of April took longer than expected, and consequently the works trains were behind schedule on their return journey. The ballast works train return journey conflicted with the first commercial morning run between Lyon and Saint-Etienne. Due to series of human errors, these two trains were running in opposite directions but moving towards each other on the same track and a head-on collision could not be avoided. Consequently, both train drivers were injured and considerable damage impact rolling stock. Fig. 11 represents the infrastructure of the line Lyon/Saint-Etienne in which the accident occurred.

The first human error comes from the safety agent who did not protect this area. Furthermore, the traffic agent emitted an erroneous authorization to the works train due to a false interpretation of the situation. This works train crossed two closed signals which are out of its operating institution. More details about the accident factors and effects may be found in Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT) (2004).

The proposed approach aims to analyze and anticipate critical situations in order to improve safety from the first design stages. Indeed, the application of *DAO* to this accident scenario allows a thorough safety analysis which prevents the occurrence of this collision. In order to mitigate the frontal collision as Hazard, *DAO* concepts are instantiated and represent safety-related information of this accident. Fig. 12 depicts safety integrated concepts into the infrastructure section representation. Zones decomposition facilitates the safety decisions management process in order to ensure a safe system operation.

The alignment between topological concepts derived from *ATMO* and the presented infrastructure section, is performed as follows:

- **Turnout** represented by "TurnoutPanel"
- **Signal** represented by a "LocatedNetEntity"
- **Area** represented by "AreaLocation"
- **Rive de Giers/Trèves-Bruel segment** represented by "TrackSegment"
- **Trèves-Bruel/Givors segment** represented by "TrackSegment"

Once the safety analysis performed, a set of safety rules may be integrated in order to avoid frontal collision between commercial and works trains. These organizational rules are defined in order to mainly enforce the following railway procedures:

1. When the works train is running outside of its operating area, the verification of signaling instructions must be integrated in the on-board signaling detection subsystem.
2. In the presence of switches for both running directions and tracks interception devices, the running direction must be indicated on-board.

The first safety rule allows the capture of signaling data for the overall area in order to avoid the crossing of closed signals (**SafetyGoal1**). The second safety rule is proposed with the aim to prevent the traffic on the opposite direction (**SafetyGoal2**). Figs. 13 and 14 show the SWRL transformation of these safety rules in order to automate the safety decisions management process.

The illustration of the proposed approach by the accident of Saint-Romain-En-Gier shows that the integration of safety rules as soon as possible in the system development process could have avoided this collision. The matching between safety concepts and real data validates the powerful capabilities of semantics to represent, analyze and anticipate several critical scenarios.

5. Related work

This section represents existing approaches and studies which tackle the different perspectives of the proposed methodology, such as safety ontologies for safety-critical systems, railway infrastructure models and MBSE approaches. Then, a comparative discussion is presented in order to highlight the original contributions of this paper.

5.1. Safety analysis for critical systems

Developing automated driving systems faces safety challenges since verifying such critical systems represents a difficult task. Rangra et al. (2018) raises discussion on safety challenges in terms of normative requirements. However, the absence of autonomous trains in mainline railway results in technological and fundamental risk assessment challenges. These same challenges were also raised in the automotive field (Philip and Mickael,

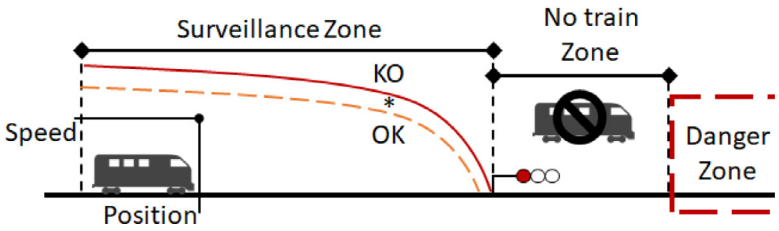

Fig. 10. Detail of the safety zone related to the presence and displacement of a train on the merging track.

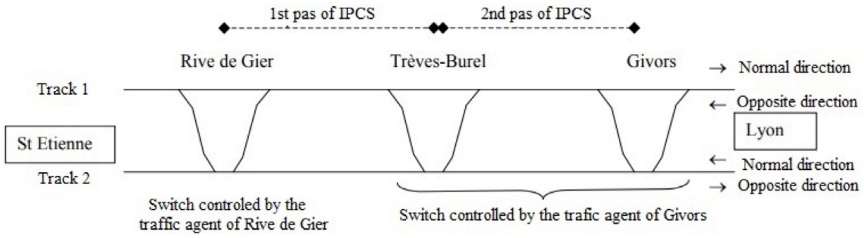

Fig. 11. The line infrastructure of Lyon/Saint-Etienne (Bureau d'Enquêtes sur les Accidents de Transport Terrestre, (BEA-TT), 2004).

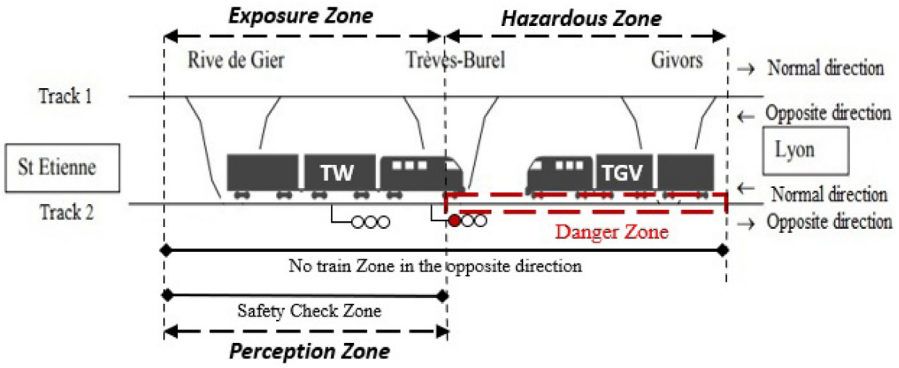

Fig. 12. Added safety-related zones for the turnout of the frontal collision.

Safety Rule 1:

```
<swrlx:classAtom>
  <owlx:Class owlx:name="SystemEquipment" />
  <ruleml:var>x1</ruleml:var>
</swrlx:classAtom>
<swrlx:classAtom>
  <owlx:Class owlx:name="OnboardSignallingDetectionSubsystem" />
  <owlx:SubclassOf>
  <owlx:Class owlx:name="SystemEquipment">
  </owlx:SubclassOf>
</swrlx:classAtom>
<swrlx:classAtom>
<owlx:Class owlx:name=" OnboardSignallingDetectionSubsystem " />
      <swrlx:individualPropertyAtom  swrlx:property="verifies">
       <ruleml:var> onboardsignallingdetectionsubsystem </ruleml:var>
       <ruleml:var>SignallingInstructions</ruleml:var>
       </swrlx:individualPropertyAtom>
</swrlx:classAtom>
<swrlx:classAtom>
      <owlx:Class owlx:name="Task" />
      <ruleml:var>x1</ruleml:var>
      <swrlx:individualPropertyAtom  swrlx:property="hasContext">
      <ruleml:var>task</ruleml:var>
      <ruleml:var>areaoutsideofitsoperatinginstitution</ruleml:var>
      </swrlx:individualPropertyAtom>
</swrlx:classAtom>
<swrlx:classAtom>
     <owlx:Class owlx:name="SafetyMeasure" />

      <ruleml:var>x1</ruleml:var>
      <swrlx:individualPropertyAtom  swrlx:property="satisfy">
      <ruleml:var> verificationofsignallinginstructions</ruleml:var>
      <ruleml:var>avoidthecrossingofclosedsignals </ruleml:var>
     </swrlx:individualPropertyAtom>

</swrlx:classAtom>
```

Fig. 13. The first SWRL safety rule for case study 2.

2017; Kianfar et al., 2013). Indeed, the *Safety Of The Intended Functionality* (*SOTIF*) standard, shorthand for *ISO/PAS 21448* (ISO/PAS 21448, 2019), testifies to the progress of the standardization of the autonomous vehicle safety. It provides design, verification and validation measures to achieve safety when identifying hazardous events. Unlike *ISO 26262* (ISO/DIS 26262-1, 2009), it is concerned with mitigating risks without a system failure.

In order to disambiguate safety analysis concepts and clarify their semantic from the first phases of the development cycle, knowledge representation is a key activity which facilitates this task. Indeed, ontologies have been widely used in the safety analysis of critical systems and their design. Authors of Zhang et al. (2015) proposed a safety ontology to formalize the safety knowledge and its link with information models. This ontology allows the automated safety planning for job hazard analysis using Building Information Modeling (*BIM*). In Rehman and Kifor (2016), an ontology was proposed to represent and manage Failure Modes and Effects Analysis (*FMEA*) knowledge in the automotive domain. Furthermore, it defines actions to mitigate the anticipated risk and allows the extraction of safety information using its operational version in OWL. On the other hand, a conceptualization of hazard-related knowledge (Hazard Ontology) (Zhou et al., 2017) was proposed. This ontology aims to identify hazards from the early design stages of safety critical systems and elicit safety requirements that mitigate them. From the same context, Tenbergen et al. (2018) proposed an approach to increase the validation of hazard-mitigating requirements based on an Ontology for Hazard Relation Diagrams. It allows to generate the Hazard Relations Diagram which satisfies a specific safety goal. This solution is built based on the same motivations and the identified research goal of our proposed approach. Nevertheless, authors did not use a specific ontology, such as *GOSMO* to establish and maintain the semantic link between safety concepts and goal-oriented requirements concepts.

In their study, Xing et al. (2019) developed a domain ontology to capitalize safety risk knowledge in metro construction. The built ontology is evaluated using case-studies and provides a decision-making support for safety risk identification. In order to provide a conceptualization of Functional Resonance Analysis Method (FRAM), Lališ et al. (2019) proposed a foundational

```
Safety Rule 2:
<swrlx:classAtom>
    <owlx:Class owlx:name="Task" />
   <ruleml:var>x1</ruleml:var>
    <swrlx:individualPropertyAtom swrlx:property="realizes">
    <ruleml:var>task</ruleml:var>
    <ruleml:var>IntegrationOfrunningdirectionOnboard</ruleml:var>
    </swrlx:individualPropertyAtom>
    <owlx:IntersectionOf>
    <swrlx:individualPropertyAtom swrlx:property="hasContext">
    <ruleml:var>task</ruleml:var>
    <ruleml:var>PresenceofswitchesforbothrunningdirectionandtracksinterceptiondevicesPresenceofswitchesforbothrunningdirectionandtracksinterceptiondevices</ruleml:var>
    </swrlx:individualPropertyAtom>
    </owlx:IntersectionOf>
</swrlx:classAtom>
<swrlx:classAtom>
    <owlx:Class owlx:name="SafetyMeasure" />
    <ruleml:var>x1</ruleml:var>
    <swrlx:individualPropertyAtom swrlx:property="satisfy">
    <ruleml:var> IntegrationOfrunningdirectionOnboard</ruleml:var>
    <ruleml:var>avoidthetrafficontheoppositedirection</ruleml:var>
   </swrlx:individualPropertyAtom>
</swrlx:classAtom>
```

Fig. 14. The second SWRL safety rule for case study 2.

ontology-based model using *UFO*. The conceptualization focused on the function concept and its surrounding aspects. The *FRAM* model is applied to a case study from the aviation domain in order to validate the integration of complex socio-technical system's features into this ontological analysis.

Most of these safety ontologies allow only the safety analysis by representing concepts of a specific method or based on a safety principle. However, none of them explored the overall dysfunctional analysis conceptualization which is independent of classic safety methods like *DAO*. Furthermore, their objectives are limited to safety analysis without a focus on how to exploit safety results and link them to the safety management process. This research goal is satisfied differently by other approaches (Clegg et al., 2019) to align safety and systems models without conceptual clarification of semantic links. An approach to validate safety of perception software and system in autonomous driving systems has been proposed based on fault injection but it did not consider the safety management (Rao et al., 2019). Finally, to the best of our knowledge, there is lack of an approach which integrates safety concerns with railway infrastructure ontologies. In this paper, we fill this gap and we propose a new approach which is able to deal with innovative industrial locks of future systems.

5.2. Infrastructure modeling

Previous works like Berkenkötter and Hannemann (2006) proposed modeling of railway infrastructure using *UML* and *UML* profiles. The aim was to obtain control-command models for signaling in tramway, but unlike *ATMO* only one usage for the infrastructure data is provided and no addition of safety-related information is present. Our approach differs because all the users of on-board mapping will benefit from the safety concepts added into *ATM-S*. The work presented in Bosschaart et al. (2015) focuses on the instance-level description of a railway infrastructure using *RailML*.[5] This study may be used by extending the scope of *RailML* to hold the safety information needed in order to instantiate *ATM-S* in a static file-based format. In Xiangxian et al. (2011), a component-based topology is used to model the infrastructure, as performed in *RailTopoModel* and subsequently *ATMO*. Therefore, the work presented in this paper may be seen as a follow-up of the proposed principle. Finally, Mecitoğlu and Söylemez (2013) presented a full method from *UML* model of the infrastructure down to *SCADA* implementation for railway interlocking, aside the limitation to a sole user. In Perin and Wouters (2014), an Ontlogies-based approach was proposed to support the integration of domain-specific models in the development process of critical systems. In a future work, the result of Perin and Wouters (2014) may be extended to link the system behavior with an ontological level.

"Ontorail"[6] is an ongoing project to support the scientific initiatives for implementing a shared railway dictionary using terminology adopted in several national and international standards, and technical specifications for interoperability. Their work is based on "MediaWiki"[7] and it semantic extension "Semantic MediaWiki".[8] It attempts to use the power of its semantics and extension tool-set to develop a *CIM* for railway field represented by an ontology.

Recent works from domains such as autonomous road vehicles are tackling infrastructure modeling, generally focusing on on-board mapping service, with interesting development in semantic layer (Eiter et al., 2019) to help manage dynamic information and graph-based layer (Ulbrich et al., 2014) to help autonomous control on road lane driving. These works show interesting ideas close to railway infrastructure modeling topics but are not taking into consideration safety-related properties.

Now, to the best of our knowledge, there is no scientific research work that has proposed a general framework for modeling the railway infrastructure and joint safety requirements for autonomous trains.

5.3. Model-based system assurance

The model management operations and its consequent automation capabilities provided by *MBE* have proven that the system consistency and efficiency are improved significantly. Several assurance cases tools have then adopted *MBE*, such as *CertWare* (Barry, 2011), *AdvoCATE* (Denney and Pai, 2018) and *D-Case Editor* (Matsuno et al., 2010).

5 https://www.railml.org/en/.

6 https://ontorail.org/ontorail/index.php?title=Main_Page.

7 https://www.mediawiki.org/wiki/MediaWiki.

8 https://www.semantic-mediawiki.org.

Historically, the safety cases expressed safety arguments in free texts using natural language. The main problem is that these texts are unstructured and can be unclear. To guarantee the production of clear and well-structured cases and avoid the problems issued by expressing safety arguments in natural language, graphical argumentation notations were proposed. *GSN* and Claims-Arguments-Evidence (*CAE*) (Bishop and Bloomfield, 1998) are examples of these notations. *CAE* presents assurance cases as a set of claims which are supported by safety arguments. However, *GSN* provides a more detailed decomposition of arguments. Furthermore, it supports additional features like modularity, controlled vocabulary and automated assurance case instantiation. These features are also adopted by *SACM*.

The use of *GSN* proved that the quality of argument approaches was improved, in addition to time development reduction (Wei et al., 2019). A major problem with the tools based on *GSN* is that they define their own metamodel. In Wei et al. (2019) a methodology was proposed to resolve interoperability problems by proposing a *GSN* metamodel compliant with *SACM*.

6. Conclusion

In order to make the trains become fully automated driverless, high precision embedded map of the railway infrastructure is required. Our proposal is being sought to consider safety engineering to design the autonomous train map. This paper proposes a solution allowing the safety requirements to be integrated inside a map conceptual model in order to be embedded onboard. Our work is based on a modeling approach using *MBE* and safety engineering. Two safety cases were presented and allowed to validate our solution. The first is expressed textually in natural language to describe a side collision case study. The second safety case provided a structural assurance case using *GSN* with compliance to *SACM* metamodel.

Safety rules are integrated to the map conceptual model and this allows are to automate their incorporation on-board and safety decisions management. Our solution offers an on-board safety-extended model for the railway infrastructure. The conceptual clarification and matching of different perspectives, namely safety analysis, railway infrastructure modeling and safety management allow a structured safety integration based on an ontological framework.

In future work, we intend to extend the proposed approach by integrating the requirement engineering concepts and to provide an operational solution for requirements traceability. This aspect is important in the system development process especially with dynamic aspect of safety requirements. Furthermore, we aim to reuse this approach for other components of future railway systems and validate the on-board application of the autonomous train map. Finally, we will investigate the formal verification aspect in order to check the safety rules consistency and the safety justification.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Barry, M.R., 2011. Certware: A workbench for safety case production and analysis. In: 2011 Aerospace Conference. pp. 1–10.

Berkenkötter, K., Hannemann, U., 2006. Modeling the railway control domain rigorously with a UML 2.0 profile. In: Górski, J. (Ed.), Computer Safety, Reliability, and Security. In: Lecture Notes in Computer Science, no. 4166, Springer Berlin Heidelberg, pp. 398–411.

Bishop, P., Bloomfield, R., 1998. A methodology for safety case development. In: Redmill, F., Anderson, T. (Eds.), Industrial Perspectives of Safety-Critical Systems. Springer London, London, pp. 194–203.

Bosschaart, M., Quaglietta, E., Janssen, B., Goverde, R.M.P., 2015. Efficient formalization of railway interlocking data in railml. Inf. Syst. 49, 126–141.

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. URL http://www.bea-tt.developpement-durable.gouv.fr/saint-romain-en-gier-english-summary-a15.html.

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.

CENELEC, NF EN 50129, 2003. Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement -Systèmes électroniques de sécurité pour la signalisation.

Chouchani, N., Abed, M., 2020. Automatic generation of personalized applications based on social media. Procedia Comput. Sci. 170, 825–830, The 11th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops.

Clegg, K., Li, M., Stamp, D., Grigg, A., McDermid, J., 2019. Integrating existing safety analyses into sysml. In: IMBSA.

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.

Debbech, S., Bon, P., Collart-Dutilleul, S., 2018a. Improving safety by integrating dysfunctional analysis into the design of railway systems. WIT Trans. Built Environ. 181, 399–411.

Debbech, S., Bon, P., Collart-Dutilleul, S., 2019. Conceptual modelling of the dynamic goal-oriented safety management for safety critical systems. In: ICSOFT 2019-14th International Conference on Software Technologies- Volume 1. pp. 287–297.

Debbech, S., Collart-Dutilleul, S., 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, URL https://hal.archives-ouvertes.fr/hal-02020997/l.

Debbech, S., Collart-Dutilleul, S., Bon, P., 2020. An ontological approach to support dysfunctional analysis for railway systems design. J. Univ. Comput. Sci. (J.UCS) 26 (5).

Denney, E., Pai, G., 2018. Tool support for assurance case development. Autom. Softw. Eng. 25 (3), 435–499.

Eiter, T., Füreder, H., Kasslatter, F., Parreira, J.X., Schneider, P., 2019. Towards a semantically enriched local dynamic map. Int. J. Intell. Transp. Syst. Res. 17 (1), 32–48.

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. IEEE, p. 120.

Guizzardi, G., 2005. Ontological Foundations for Structural Conceptual Models (Ph.D. thesis). University of Twente, Enschede, The Netherlands.

IEC 61508, Norme Internationale, 2000. Sécurité fonctionnelle des systèmes électriques électroniques programmables relatifs à la sécurité.

ISO/DIS 26262-1, 2009. Road vehicles - Functional safety - part 1 Glossary.

ISO/PAS 21448, 2019. Safety of the intended functionality.

Kelly, T., Weaver, R., 2004. The goal structuring notation–a safety argument notation. In: Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases.

Kianfar, R., Falcone, P., Fredriksson, J., 2013. Safety verification of automated driving systems. IEEE Intell. Transp. Syst. Mag. 5 (4), 73–86.

Lališ, A., Patriarca, R., Ahmad, J., Di Gravio, G., Kostov, B., 2019. Functional modeling in safety by means of foundational ontologies. Transp. Res. Procedia 43, 290–299.

Lano, K., Kolahdouz-Rahimi, S., Yassipour-Tehrani, S., Sharbaf, M., 2018. A survey of model transformation design patterns in practice. J. Syst. Softw. 140, 48–73.

Matsuno, Y., Takamura, H., Ishikawa, Y., 2010. A dependability case editor with pattern library. In: 2010 IEEE 12th International Symposium on High Assurance Systems Engineering. pp. 170–171.

MDA Guide Revision 2, 2014. OMG Document Ormsc/14-06-01. Object Managment Group.

Mecitoğlu, F., Söylemez, M.T., 2013. A UML modelling approach for a railway signalization system simulator and SCADA system. IFAC Proc. Vol. 46 (25), 77–82.

O'connor, M., Knublauch, H., Tu, S., Grosof, B., Dean, M., Grosso, W., Musen, M., 2005. Supporting rule system interoperability on the semantic web with SWRL. In: International Semantic Web Conference. Springer, pp. 974–986.

omg, Structured Assurance Case Metamodel V2.1, URL https://www.omg.org/spec/SACM/2.1.

Perin, M., Wouters, L., 2014. Using ontologies for solving cross-domain collaboration issues. In: IFAC Proceedings Volumes, 19th IFAC World Congress. 47, pp. 7837–7842.

Philip, K., Mickael, W., 2017. Autonomous vehicle safety: An interdisciplinary challenge. IEEE Intell. Transp. Syst. Mag. 9 (1), 90–96.
RailTopoModel, 2016. UIC International Railway Standard IRS 30100. UIC, The Worldwide Railway Organisation.
Rangra, S., Sallak, M., Schön, W., Belmonte, F., 2018. Risk and safety analysis of main line autonomous train operation: context, challenges and solutions. In: Congres Lambda Mu 21 de Maitrise Des Risques Et de Surete de Fonctionnement.
Rao, D., Pathrose, P., Huening, F., Sid, J., 2019. An approach for validating safety of perception software in autonomous driving systems. In: Papadopoulos, Y., Aslansefat, K., Katsaros, P., Bozzano, M. (Eds.), Model-Based Safety and Assessment. Springer International Publishing, Cham, pp. 303–316.
Rehman, Z., Kifor, C.V., 2016. An ontology to support semantic management of FMEA knowledge. Int. J. Comput. Commun. Control 11 (4).
Rodrigues da Silva, A., 2015. Model-driven engineering: A survey supported by the unified conceptual model. Comput. Lang. Syst. Struct. 43, 139–155.
Tenbergen, B., Weyer, T., Pohl, K., 2018. Hazard relation diagrams: a diagrammatic representation to increase validation objectivity of requirements-based hazard mitigations. Requir. Eng. 23 (2), 291–329.
Ulbrich, S., Nothdurft, T., Maurer, M., Hecker, P., 2014. Graph-based context representation, environment modeling and information aggregation for automated driving. In: 2014 IEEE Intelligent Vehicles Symposium Proceedings. pp. 541–547.
Unified Modeling Language v2.5, 2015. OMG Norm. Object Management Group.
Wei, R., Kelly, T.P., Dai, X., Zhao, S., Hawkins, R., 2019. Model based system assurance using the structured assurance case metamodel. CoRR abs/1905.02427.
Xiangxian, C., Yulin, H., hai, H., 2011. A component-based topology model for railway interlocking systems. Math. Comput. Simulation 81 (9), 1892–1900.
Xing, X., Zhong, B., Luo, H., Li, H., Wu, H., 2019. Ontology for safety risk identification in metro construction. Comput. Ind. 109, 14–30.
Zhang, S., Boukamp, F., Teizer, J., 2015. Ontology-based semantic modeling of construction safety knowledge: Towards automated safety planning for job hazard analysis (JHA). Autom. Constr. 52, 29–41.
Zhou, J., Hänninen, K., Lundqvist, K., 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. pp. 183–185.