A model-based system engineering approach to manage railway safety-related decisions

Sana Debbech, Philippe Bon, Simon Collart-Dutilleul

A MODEL-BASED SYSTEM ENGINEERING APPROACH TO MANAGE RAILWAY SAFETY-RELATED DECISIONS

SANA DEBBECH, PHILIPPE BON & SIMON COLLART-DUTILLEUL
Université de Lille/Nord de France, IFSTTAR/COSYS/ESTAS, France

ABSTRACT

The safety assessment of Safety Critical Systems (SCSs) is a challenging task since it involves different actors and a combination of several knowledge domains. This increases the complexity of the integration of safety requirements into the design model. Consequently, there is a need for a shared model with an unambiguous terminology aiming to avoid misunderstandings between both safety and design teams. In this paper, we propose a model-based system engineering approach in order to support the goal-oriented safety reasoning and to provide a common model between both safety and requirement engineering driven by goals. Furthermore, the present study considers the safety rules development process based on the Organization-based Access Control (Or-BAC) model, which is normally used to improve the security of the information systems. Then, the common vocabulary proposed for the interpretation of the considered notions of domains is defined. Moreover, safety requirements are expressed with a high level of abstraction according to the required railway knowledge and the requirement traceability process is considered through an up-bottom reasoning using the Unified Modeling Language (UML) diagrams. The proposed approach aims to provide a methodology able to identify safety conditions in order to anticipate risks and to make better safety-related decisions. Finally, the proposed methodology is evaluated through a real accident scenario analysis in order to validate its adaptability to represent real critical situations.

Keywords: rail accident scenario, design model, dysfunctional analysis, model-based safety engineering, Or-BAC, safety requirements.

1 INTRODUCTION

Due to the increasing complexity and the ubiquitous deployment of safety critical systems (SCSs), new needs concerning safety methodologies and tools arise. In such interactive complex systems, there are many branching paths among components making the interactions unpredictable to system designers and users. Therefore, complex systems are error prone and safety critical since errors lead to accidents with potentially catastrophic effects. Consequently, the increasing complexity of transportation systems makes their development and safety analysis more difficult. The identification of necessary safety conditions to reduce the occurrence of dangerous situations is important to guarantee required safety integrity level (SIL) [1]. This parameter directly impacts the system architecture design and determines the risk reduction factor required for safety functions. Its possible values range between ‘0’ (less critical) and ‘4’ (most critical). The design of a specific system and its subsystems depends on the value of the SIL associated with each functionality of the system.

In railway systems, more and more functionalities are transferred from hardware to software components. Consequently, it becomes continuously harder to verify safety aspects. Model-based safety analysis can help solving this problem by finding causal connections between component failure modes and overall system hazards. Besides, taking advantage of these notions requires to build models combining both functional and dysfunctional aspects. Most of the current practices on the system safety assurance rely mainly on manual processes. Currently, the railway safety community refers to qualitative methods before the design process. Nevertheless, a tool-based methodology does not exist to allow the integration of the safety assessment earlier into the design stages. Moreover, the safety rule development

ISSN: 2058-8305 (paper format), ISSN: 2058-8313 (online), http://www.witpress.com/journals
DOI: 10.2495/TDI-V3-N1-30-43

process is not performed through a dedicated tool which combines both railway knowledge and requirement engineering.

In a previous work [2], we proposed a semantic interpretation of the safety-related concepts based on a foundational ontology (the Unified Foundation Ontology [UFO]) and the Organization-based Access Control (Or-BAC) which is inspired by the information systems (IS) security. This semantic interpretation provides a conceptualization of safety-related concepts in real-world semantics, with the aim of matching the different knowledge domains. Consequently, a conceptual model with a shared view of safety, Or-BAC and the goal-oriented requirement engineering (GORE) concepts is obtained.

In this paper, the proposed approach aims to integrate safety knowledge as soon as possible in the railway system architecture design. First, we define an ontology of the European Rail Traffic Management System (ERTMS) to have a structured and non-ambiguous representation of the system. The aim of this study is to propose a formalization of safety requirements that will be taken into account along the design phases. They are expressed with a high level of abstraction and related to Or-BAC concepts. Then, the traceability of their evolution and their impact on system's other requirements are considered. The paper starts with the description of the proposed methodology. Section 3 describes the considered case study and the safety-related analysis. Then, Section 4 discusses some related works and compares them to ours. Finally, Section 5 concludes the paper and outlines some perspectives.

2 DYSFUNCTIONAL ANALYSIS INTEGRATION INTO AN MBSE APPROACH WITH UNIFIED MODELING LANGUAGE

System engineering (SE) approaches provide relevant solutions for the purpose of formalizing and comprehending complex systems. Thus, big efforts are required to manage the complexity, to maintain the coherence and the consistency along the development and to deal with numerous requirements relevant to multiple domains. In order to prevent as many accidents as possible, efforts are being focused on safety in many domains. Development requirements and SCS life cycle present guidelines to make systems more and more fault-tolerant. However, a potential source of safety critical problems can only be anticipated if safety requirements are integrated as early as possible into the system architecture design. This problem is amplified by the fact that safety and system design engineering develop their own techniques and methodologies separately.

For the railway domain, safety analysis is executed through standard methods such as Fault Tree Analysis [3], Preliminary Risk Analysis [4] or Failure mode, effects and criticality analysis [5] and formal verification methods like the B method [6]. In order to avoid error-prone processes and to involve both safety engineering and system design, we employ a *model-based safety engineering* approach. This approach provides a shared view of the same model of the system between safety engineers and system designers. Indeed, model-driven engineering (MDE) [7] is being successfully adopted in many domains and industrial research projects [8]. For instance, the model-based system engineering (MBSE) approach proposed in [9] shows the utility of the MDE in order to integrate the dysfunctional analysis into the system design. This approach is evaluated by a case study from a real accident scenario of *Saint-Romain-En-Gier, France*.

As a contribution to this paper, we propose a methodology to integrate dysfunctional analysis into the design process from the first stages for railway systems. The aim of this study consists in defining the safety rule development process based on the Or-BAC model with a high level of abstraction. Then, their integration into the design model and their traceability are considered. The first step of the methodology is illustrated by examples from the ERTMS system. Moreover, the ERTMS-related concepts are formalized in a structured way in order to regroup and create a formal structure of this domain concept into a knowledge web. In this study, ontologies are used to model and formalize the ERTMS system requirement specifications (SRS).

Ontologies are structured representations of knowledge of a certain domain. Several definitions of the term ‘ontology’ have been provided in the literature. Ontologies present their own methodological and architectural peculiarities. On the methodological side, the main peculiarity is the adoption of a highly interdisciplinary approach, where philosophy and linguistics play a fundamental role in analyzing the structure of a given reality at a high level of generality and in formulating a clear and rigorous vocabulary [10]. On the architectural side, the most interesting aspect is the centrality of the role that an ontology can play in a complex system, leading to the perspective of *ontology-driven complex systems modeling*. The railway domain is an environment where numerous heterogeneous information sources exist. The ERTMS system basically relies on information exchange. Ontologies provide a number of useful features for intelligent systems, as well as for the knowledge representation [11]. In the railway domain, documents describing the SRS [12], provided by the European Railway Agency, were issued with the specific aim of explaining and clarifying the usage of a part of the terms/concepts used in this domain and of the system itself. The main idea of the proposed methodology is summarized in Fig. 1.

In this study, we choose an ontology creation tool using the Web Ontology Language, called the Protégé tool. Protégé 5.2.0 was developed by Mark Musen’s group at Stanford Medical Informatics. Its plug-in architecture can be adapted to build both simple and complex ontology-based applications. In this environment, concepts are formalized as classes together with their types of properties and relations between them. Our ERTMS ontology is composed of three layers, based on the ERTMS architecture: ETCS on-board, ETCS Trackside and Global System for Mobiles-Railway (GSM-R). Moreover, human actors and the train are considered for the system environment factors aspect. These subsystems are formalized as classes. Every subsystem (class) is composed of several components, where each one has its own functions, properties and communication interfaces (relations) with the other components. The classes’ view of the ERTMS ontology is presented in Fig. 2.

In the present paper, we use the SRS documents, written in natural language (English), and we build our ontology in French. The asserted class hierarchy view is one of the primary navigation devices in Protégé. It is presented as a tree where nodes represent *classes*. A child–parent relationship in the tree represents a sub/super class relationship in the class hierarchy. Moreover, a class will be shown as a child of another class in the tree (1) if it is asserted to be a *SubClassOf* that other class or (2) if it is asserted to be *EquivalentTo* a class expression that is an intersection containing that other class as an operand. For example, in

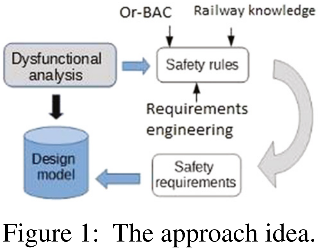
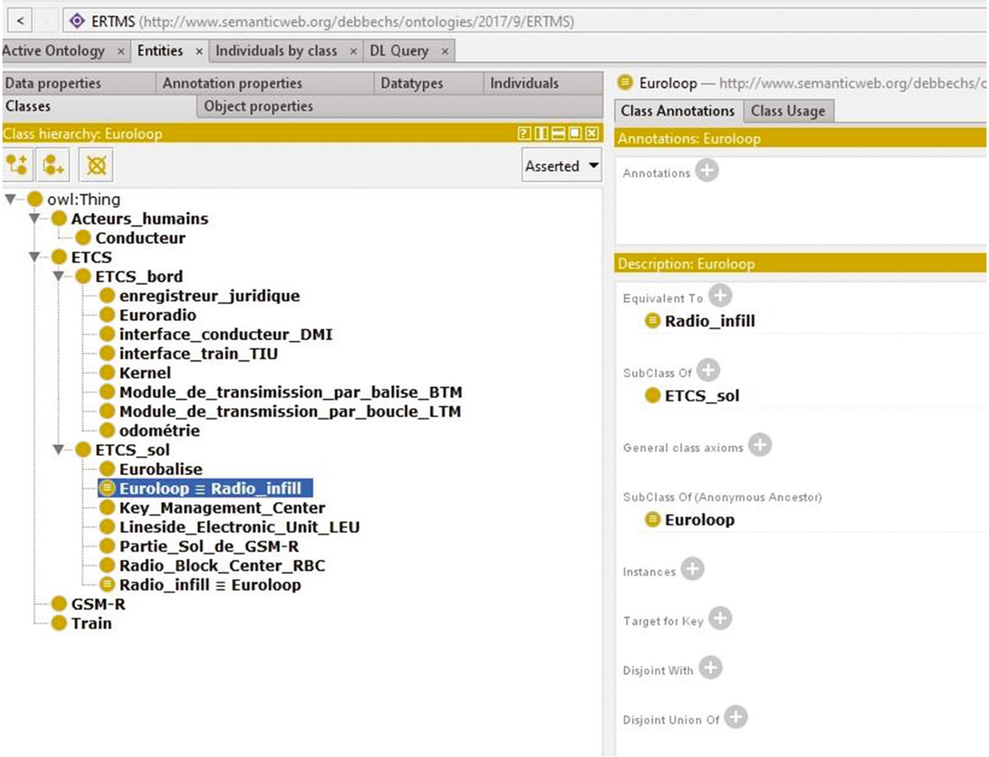


Figure 1: The approach idea.



- owl:Thing
  - Acteurs_humains
    - Conducteur
  - ETCS
    - ETCS_bord
      - enregistreur_juridique
      - Euroradio
      - interface_conducteur_DMI
      - interface_train_TIU
      - Kernel
      - Module_de_transimission_par_balise_BTM
      - Module_de_transmission_par_boucle_LTM
      - odométrie
    - ETCS_sol
      - Eurobalise
      - Euroloop ≡ Radio_infill
      - Key_Management_Center
      - Lineside_Electronic_Unit_LEU
      - Partie_Sol_de_GSM-R
      - Radio_Block_Center_RBC
      - Radio_infill ≡ Euroloop
  - GSM-R
  - Train

Equivalent To: Radio_infill

SubClass Of: ETCS_sol

SubClass Of (Anonymous Ancestor): Euroloop

Figure 2: The ERTMS ontology.

our ERTMS ontology, the *radio infill* is equivalent to *the euroloop* in the ETCS track-side. In order to have a non-ambiguous representation of the ERTMS system model, this ontology was translated to a Unified Modeling Language (UML) class diagram in [9], based on some defined rules. Moreover, this ontology may be represented using the Resource Description Framework (RDF), which is a model, associated with a syntax, whose purpose is to allow a community of users to share the same meta-data for shared resources. It was originally designed by the W3C in order to help the information structure accessibility on the web and effectively index it. This formalism provides the definition of the model (or even a diagram) of meta-data that allows:

- to make sense of the properties associated with a resource;
- to constrain on the values associated with a property to ensure its significance.

An RDF model is a statement represented by the threefold: property, resource and value. In this study, the RDF graph representation provides a better extraction of information through SPARQL Protocol and RDF Query Language. Furthermore, the dysfunctional analysis aspect considered in this study requires a thorough traceability of the failure causes and effects in order to help safety-related decisions. For instance, the failure propagation of a system component may be detected by specific queries and the mitigation measures may be integrated into the ontological model and then into the design model. Then, another component may be delegated for the purpose of accomplishing the failed task. This formalism has been widely

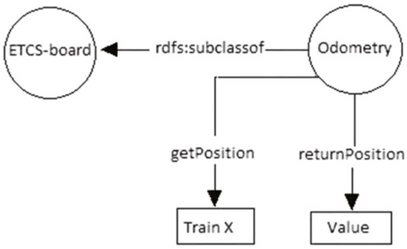


Figure 3: The RDF graph example.

used in order to enhance the IS security. For instance, it is employed in the authentication context for a specific IP address or in the network routing. Consequently, it provides a matching between subgraphs and the queried ontology graph. Besides, the other advantage of using this formalism consists in ensuring the matching between concepts and the interoperability between ontologies representing different knowledge domains. This aspect is interesting for our work since it allows a better information management and a matching between the system ontology concepts and the domain ontology (dysfunctional analysis ontology). This will be the subject of future work. Figure 3 represents the RDF graph of an example from the ERTMS ontology with the aim to illustrate this formalism utility.

For the purpose of supporting the SE approach, we must use a tool to model system requirements and the ERTMS system architecture and ensure the coherence between these different views. Indeed, we chose the UML, thanks to its several advantages, semi-formal capabilities of modeling and formal semantics [14]. Simultaneously, we use the Object Constraint Language (OCL) that is a formal language used to express side-effect-free constraints in the UML model. Semantics for OCL includes necessarily semantics for class diagrams [15]. Consequently, the ERTMS ontology is modeled in UML class diagrams and OCL constraints [9]. Moreover, UML is more and more applied in different academic and industrial projects because it provides a better communication and manipulation of the same system model by design engineers and safety engineers [16]. For example, UML class diagrams are used in order to represent ontologies and UML object diagrams to represent instance knowledge [13].

The approach proposed in [9] shows that safety measures derived from the dysfunctional analysis must be expressed with a high level of abstraction. In the present study, we propose a model of the safety rule development based on the Or-BAC model. It establishes relations between safety-related concepts and Or-BAC concepts and then the GORE concepts. As a preliminary step, we proposed a semantic interpretation of safety, Role-based Access Control (R-BAC) and GORE concepts based on the UFO foundational concepts [2]. This semantic interpretation of concepts in real-world semantics enhances the multi-view modeling with a common vocabulary. Furthermore, it ensures the interoperability between different knowledge domains and the analogy of concepts between the IS security and the railway safety. In this paper, we propose the UML class diagram, as presented in Fig. 4, showing relations between concepts (classes) in order to deduce the expression of safety rules regarding other concepts. In this diagram, we consider the SRS concepts such as scenario, goal, requirement and actors. Moreover, we introduce the Or-BAC concepts such as organization, role and context, and we define relation between them. This modeling process improves the clarity and the expressivity of safety rules. Then, the requirement engineering (RE) perspective is considered with the aim to ensure the requirement traceability. The proposed methodology is evaluated and illustrated by a real accident scenario in the next section.

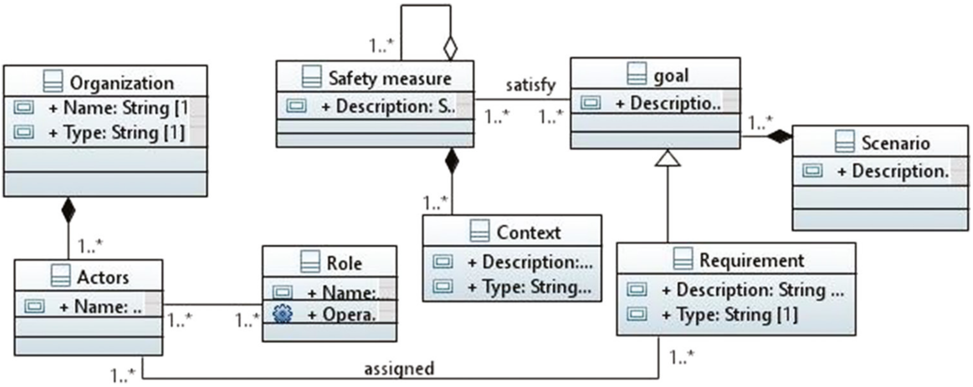


Figure 4: UML class diagram of safety rule-related concepts.

Requirement engineering is a primordial activity in the architecture system design. A requirement specifies the capability or condition that must (or should) be satisfied. A requirement may specify a function that a system must perform or a performance condition a system must achieve [17]. The aim of this study consists in integrating new safety requirements as soon as possible in the design stages. So, we have to formulate safety requirements with a high level of abstraction in order to have a flexible integration of requirements and have a good visibility of the requirement evolution. Safety requirements can be grouped into two categories [18]:

1. Requirements related to compliance and good practice;
2. Specific system performance-related requirements.

In this paper, the second category related to the system performance is considered. Safety requirements can be expressed according to the desired actor who is involved to accomplish the failed service. We have two methods to anticipate safety problems: *component redundancy* and *human interventions*. Component redundancy is the most applied protection measure in the hazard log. This mitigation measure is related to novel equipment, or new processes, or any novel environment states within which the regular *equipment* or *processes* have to operate. Once the safety requirement deduced from the hazard assessment and expressed with the high level of abstraction, it will be integrated into the system architecture. The second challenge of our study is to trace the requirement's evolution. Once the functional model is reliable, the required SIL is achieved. The inherent complexity of complex systems imposes the use of powerful tools for the implementation of the requirement traceability. In this study, we choose Systems Modeling Language (SysML), thanks to its advantages to model requirements explicitly [17].

SysML is a general-purpose modeling language for SE applications. It supports the specification, analysis, design, verification and validation of a broad range of systems and systems-of-systems. SysML is defined as an extension of a subset of the UML using an UML profile mechanism [19]. In this study, we are particularly interested by its ability to represent text-based requirements and relate them to other modeling elements. A standard requirement includes properties to specify its unique identifier and text requirement [15]. Thus, a generic trace requirement relationship provides a general-purpose relationship between a requirement and any other model element. Finally, we illustrate the proposed methodology based on a case study from the real accident scenario of Saint-Romain-En-Gier in France in the next section.

3 A CASE STUDY: SAINT-ROMAIN-EN-GIER ACCIDENT

In this paper, we present the accident scenario of Saint-Romain-En-Gier, in France, which consists in a railway collision on 5 April 2004, between an empty high-speed train and a works train at 532,730 km on track 2 of the main line between Lyon and Saint-Etienne as mentioned in Fig. 5. The accident was due to track works between the cities of Rive-de-Giers and Givors, in a railway section equipped with reverse signaling [20]. 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 path. The ballast works train return journey conflicted with the first commercial train in the morning run between Lyon and Saint-Etienne. Due to a series of errors, these two trains were running in opposite directions but moving towards each other on the same track, and a frontal collision could not be avoided. Two people were injured and considerable damage was done to the rolling stock. The BEA-TT report [20] describes the accident causes and circumstances, and it represents preventive recommendations in order to mitigate the risk level in these situations involving works trains.

In this study, this accident scenario is chosen because it highlights the utility of Or-BAC concepts in the definition of safety-related rules, particularly the *context* concept. Furthermore, the analysis of this scenario shows that there are at least three violated safety rules. In this paper, we discuss the safety rule development for this scenario, and a safety rule is proposed and formalized.

In order to help the safety reasoning and to analyze the system behavior regarding the critical information, we affirm that the safety rule is structurally related to a context. It may be spatiotemporal, a precondition or a chronological order of actions. From this point of view, we conclude that the aggregation relation between safety rules and its three aggregates such as the *context*, the *preconditions* and the *actions list* is primordial. The safety rule decomposition is considered in [21], but it is not formalized in terms of safety reasoning, modeling and requirement traceability. In this paper, we tackle these issues. According to the BEA-TT report [20], the preventive actions considered in this scenario are:

1. The request of track interception (DIV) which is defined as a procedure allowing the service responsible for the infrastructure maintenance to carry out work on a portion of line or track, depending on two traffic agents, with the guarantee of no commercial traffic for a specified time period.

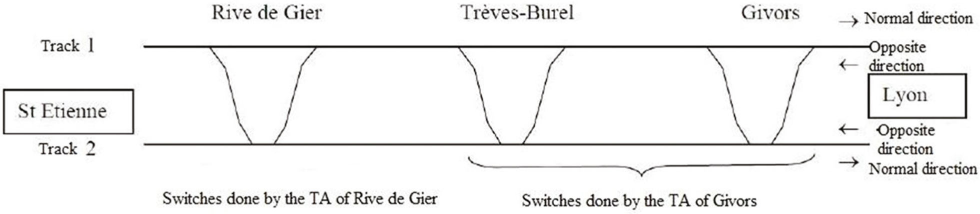


Figure 5: The infrastructure representation [20].

2. The site protection: The safety agent responsible for the site has to protect it. He should leave a flag across the track (it is called a manual stop signal SAM). Consequently, any train that enters in this site will be informed. Nevertheless, this action was not done by the safety agent in this scenario.
3. The permanent installation of the opposite direction (IPCS): railway lines may be equipped with signaling devices allowing trains running in both directions on every track. However, this equipment may be used in only one direction of the track. In this scenario, the works train driver crosses a turned-off signal. This signal is turned off because the traffic agent authorizes the crossing of the commercial train in the other direction. This collision occurred at a low speed (20 km/h for the works train and 10 km/h for the commercial train). The commercial train was slowed by the signaling which ensures that no collision in the same direction can happen. Unfortunately, the movement of trains in this scenario was in both directions. In this case, we may conclude that the works train driver considered that he was protected by the DIV.

After the analysis of the scenario, the BEA-TT experts conclude that the series of errors in this accident are due to a lack of appreciation of the context. Indeed, the whole safety reasoning considers all safety measures/actions. If the system actor has a partial view of the system, a partial analysis of the context leads to measures inconsistent in terms of safety. Consequently, it is judicious to use a formalism which provides a structured and non-ambiguous representation of critical data related to the context. Hence, the Or-BAC formalism is particularly interesting for safety rule development since it introduces the context concept. In this study, we propose a specialization for the railway application. In the present paper, we propose an intuitive safety reasoning (not definitive) in order to illustrate the proposed methodology.

According to the considered scenario, a DIV is deposited to track 1 and track 2.

In this case, there are two critical information to be considered:

1. This DIV is deposited to track 2 every night as always; however, on the night of the accident, it has been extended. Indeed, the DIV extends from *Rive de Gier* to *Givors* on this night. Contrarily, it covered *Rive de Gier* to *Trèves-Burel* previously.
2. At the time of the accident, the DIV of track 1 had been released.

According to the BEA-TT report [20], the agent supposed that the DIV position was the same and the section *Rive de Gier-Givors* was not occupied. Consequently, every modification should have been reported to the next agent. However, it is not the case in this scenario because the previous agent put a physical device against the opening of the route on track 2 from *Givors* to *Rive de Gier*. Furthermore, the interdiction of movement on track 2 was not lifted since these devices were not removed. Hence, the provisional context had to be considered in this case. From another point of view, the traffic agent did not consider the protection aspect. In other words, the critical information related to the DIV show that a DIV is planned for a specific period and the traffic is authorized *if and only if* the DIV is removed. In this case, the temporal context is useful only for the scheduling but not for the safety aspect.

The IPCS access may be done without stop through the opposite direction entry table (TECS), which is a luminous board indicating to the train driver that he start to circulate in the opposite direction. Consequently, the signals to be respected are then on the other side of the track [20]. In this scenario, the works train encountered the second IPCS of Trèves-Burel/Givors, which is out of its operating institution, and the TECS was turned off indicating that the train circulates through the wrong way. Indeed, the Trèves-Burel station and the IPCS Trèves-Burel/Givors fall within the institution of Lyon-Sud, while the zone under construction during the days of 4th and 5th April only concerns the institution of Saint-É tienne Loire. Consequently, the works train is engaged in the IPCS without respecting the signaling. According to the BEA-TT analysis, the lack to consider the number, the actual disposition and the procedures for using IPCS steps seem to have been the main source of misunderstandings between safety operators. Moreover, the inaccuracy of the list of intermediate signals weakens the strictness of attitude of the operators in the field. More details about installations on the line Saint-É tienne/Lyon may be found in Appendix 7 of the BEA-TT report [20]. In this study, a safety measure is proposed as an example in order to illustrate the proposed methodology and to assist safety-related decisions.

Intuitively, we can propose an automatism as an example: the deployment of a crocodile, which is a component of a train protection system used in France, Belgium and Luxembourg, on track 2. This safety measure may be considered in order to transmit on-board an authorization/interdiction to cross a signal and potentially to stop a train when passing a dangerous signal. In this case, this emergency stop may be envisaged as an IPCS reinforcement measure in order to avoid the non-respect of the signaling by the driver. Furthermore, this safety measure covers the *provisional context* aspect in this scenario. Consequently, its deployment provides the multi-view assessment aspect in terms of safety improvement, human error mitigation and automation of this task in order to ensure performance. Moreover, the device deployment may be considered as a tailor-made solution especially in the case of accidents due to human errors and climatic conditions. Nevertheless, it requires a high cost of deployment, in particular on high traffic lines, and hence a high cost of maintenance. However, this safety measure seems to be efficient in terms of the risk occurrence probability compared to human factors and reliability analysis. Since this study does not aim to assess human factors [22], it is interesting to consider it in future works in order to have a thorough qualitative and quantitative safety analyses. Then, a tool-based methodology will be proposed in future works in order to develop safety rules dynamically and justify the pattern regarding design constraints.

From an RE perspective, there are two sub-goals of safety improvement in this scenario: safety of the rolling stock traffic and safety of agents and passengers. In order to satisfy these sub-goals, there are two sub-measures to be considered, respectively: a crocodile transmitting a signal on-board for an emergency stop and also suspend the traffic of commercial trains when there is a works train in the area. Consequently, the proposed safety measures are related, respectively, to a specific provisional context and precondition. This interpretation is introduced in order to illustrate the proposed approach. The safety measure development based on Or-BAC is illustrated by the UML object diagram in Fig. 6. Then, it is important to consider another aspect of the safety rule definition into an organization and the role assignment process to actors considering a specific scenario. Indeed, it provides a shared view of the design model between actors in order to avoid the partial system view and the impacts they may cause. This aspect is important in the requirement elicitation process since it provides a consistent and a complete requirement specification.

The second challenge of the present study is the requirement's traceability in order to ensure the coherence in terms of the requirement's interactions and consequently

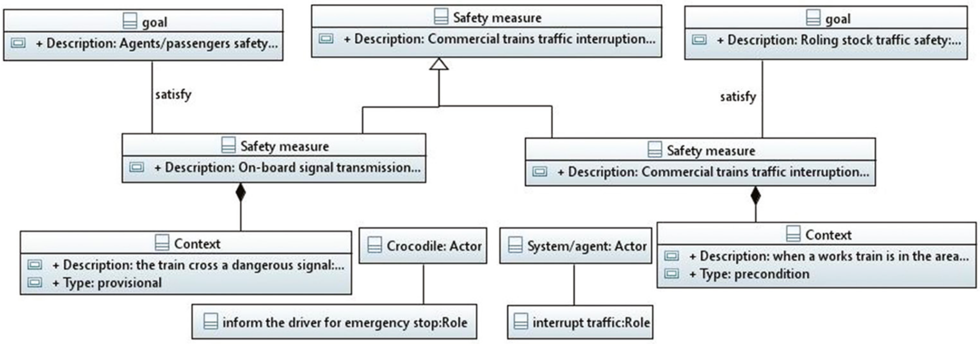

goal
+ Description: Agents/passengers safety...
Safety measure
+ Description: Commercial trains traffic interruption...
goal
+ Description: Roling stock traffic safety:...
satisfy
satisfy
Safety measure
+ Description: On-board signal transmission...
Safety measure
+ Description: Commercial trains traffic interruption...
Context
+ Description: the train cross a dangerous signal:...
+ Type: provisional
Crocodile: Actor
System/agent: Actor
Context
+ Description: when a works train is in the area...
+ Type: precondition
inform the driver for emergency stop:Role
interrupt traffic:Role

Figure 6: Safety rule illustration: UML object diagram.

the reliability of the system. For this purpose, the SysML-based *requirement diagram* is defined. Moreover, several requirement relationships can be specified and a trace of requirement's evolution can be stored. A particular focus is put on the mechanism of interactions between existing requirements and integrated requirements. Figure 7 shows the several relationships between requirements expressed with a high level of abstraction. The new safety requirement is integrated into the requirement's package model. OCL constraints are included in the requirement diagram in order to constrain relations between requirements. For instance, the 'lead to emergency stop' requirement is performed *if* the crossing of a dangerous signal is *true*. Finally, the requirement model is validated and the system performance is ensured.

In this study, this issue is considered for the illustration purpose to improve the effectiveness of the proposed methodology. Nevertheless, it will be based on dynamic tools in order to ensure the traceability management. This gap is the subject of future work. The requirement diagram shows that relations between requirements are improved and the traceability management is performed. Moreover, it improves the choice of the proposed safety measure and the requirement coherence and consistency.

The RE aspect considered in this study aims to ensure the consistency of the requirement package model from the first design stages. Moreover, it is primordial to consider it in the requirement elicitation process specially to enhance the requirement quality. That can be

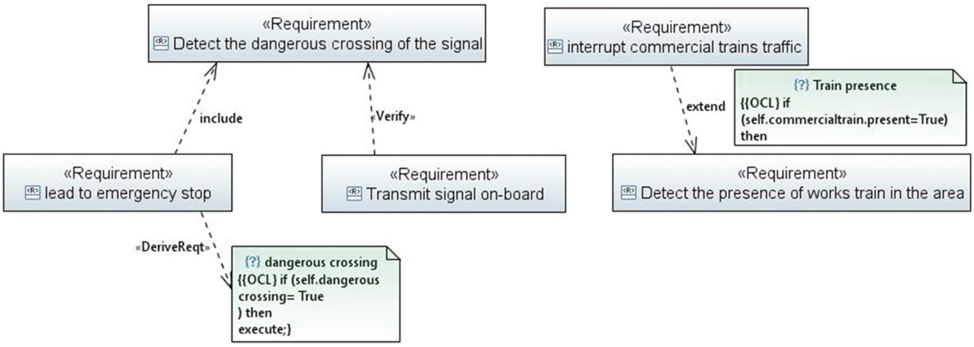


Figure 7: SysML requirement diagram with integrated safety requirement.

done through documenting interrelationships among requirements after brainstorming processes and use case models. In future work, requirement ontologies based on upper ontologies will be proposed in order to have non-ambiguous, structured and traceable requirements.

RELATED WORK & DISCUSSION

In the field of SE processes, the best practices are supported by a wide theoretical and technical documentation. The integration of the dysfunctional analysis or safety concerns in general-purpose modeling processes is a big challenge that has been explored in many directions. In this paper, we focus on previous works which are receiving specific attention in the SE community.

In [16], Cancila et al. proposed a UML profile to integrate some safety concerns in SE processes. This modeling language allows the risk analysis and defines automatically some safety attributes such as the SIL. Feiler et al. [23] proposed a framework to model the error state propagation in a hierarchical architecture. They demonstrate that error propagation may occur at the components level, at the hardware level and between the hardware and components. In order to limit or avoid the error propagation, the authors define adapted filters (guards), for example, between the interconnection of components. For the same purpose, some industries and academics defined an architecture description language called EAST-ADL [24] in order to specify component-based software infrastructures in automotive applications. In [25], the authors proposed a meta-model using UML class diagrams and OCL constraints to integrate safety concerns into SE processes. In addition, they defined redundancy policies to update the dynamical allocation of functions caused by dysfunctional events. In their paper [26], Guillerm et al. describe a method for declining safety requirements of complex systems. In their study, the refinement of requirements is a necessary step aiming to treat the safety ones and to achieve their integration. In [27], the authors proposed an approach to integrate safety requirements into the design process based on SysML. In order to maintain safety standards, the triplet requirement models, solution models and validation and verification (V&V) models are isolated. For this purpose, a SysML profile respecting safety standards called Requirement Profile for MeMVaTEX (RPM) was developed. In this work, traceability is assured between requirement models, between requirement and solution models and between requirement and V&V models by using their properties. However, only integration of safety requirements is considered in this work, but safety analysis techniques (from which safety requirements are derived) are performed separately. Table 1 summarizes the comparative discussion mentioned above based on the main contributions:

- (a) Taking into account the SE processes
- (b) Performing safety analysis methods jointly with design
- (c) Considering traceability of requirements
- (d) Developing safety rules based on control access models

However, these works do not consider the requirement traceability after the integration of safety requirements in the system architecture design. Then, none of them take into account the safety rule development based on control access models from IS and provide the analogy between domains. Hence, they did not employ a clear methodology or a predefined model to define safety rules for a specific scenario. Moreover, the dynamic and traceable aspect of requirements among this process is not considered in most studies. In this paper, we propose a methodology based on Or-BAC model of safety requirements to fill these gaps.

Table 1: Comparative study.

	a)	b)	c)	d)
Cancila	*	*		
Feiler	*	*		
Piriou	*	*		
Guillerm	*	*		
Dubois	*	*	*	

CONCLUSION AND OUTLOOKS

The aim of this study is the integration of dysfunctional analysis into the railway system design and the formalization of the safety reasoning. This paper presents an MBSE methodology to take into account safety analysis as early as possible during the design phases. Then, it is illustrated by a real accident scenario of Saint-Romain-En-Gier in France in order to highlight the criticality of safety-related information, in particular, the *context* concept. Moreover, the present study considers the safety rule development process based on the Or-BAC model which is normally used for the IS security. From this point of view, a design model of safety rules is proposed based on the Or-BAC concepts and reinterpreted for railway application from the safety perspective. Besides, the RE aspect is considered for the purpose of ensuring the requirement traceability. Consequently, safety rules derived from the dysfunctional analysis are expressed with a high level of abstraction and may be integrated into the design model.

The real accident scenario considered in this paper shows that the proposed approach is able to manage the design and safety-related decisions. Then, the proposed formalism is relevant in order to deal with the criticality of this task. Furthermore, the ERTMS ontology is proposed for the purpose of providing a structured representation of the system and a better tool management of its failures. Indeed, the proposed system ontology may be considered to ensure the interoperability between ontologies and then to provide a multi-view modeling between actors. This step will be the subject of future publication.

Nevertheless, the present study did not consider the interoperability between knowledge domains such as the railway domain, the GORE and Or-BAC through the matching between related concepts. Furthermore, there is a need to define a shared conceptual model in order to ensure the information management conceptualization and to provide a consistent model. Then, dysfunctional analysis is still dependent on dynamic system models such as sequence diagrams and automata in order to analyze the system behavior. However, these models may not be obtainable from the first design stages. Moreover, the requirement traceability needs to be performed through an enhanced tool in order to improve the requirement quality and avoid inconsistency issues. Future works will consider the gaps mentioned above.

Therefore, one of the aims of future work will be the conceptualization of dysfunctional analysis based on foundational ontologies in order to tackle the criticality of this task for SCSs. This study will provide a consistent and structured conceptual model in order to perform dysfunctional analysis independently from dynamic models representing system behavior. Furthermore, the interpretation of dysfunctional analysis concepts will be provided in real-world semantics in order to ensure the ontology reuse for other domains. The second challenge considered in future works is to provide a conceptualization of safety rule development based on upper ontologies in order to ensure the interoperability with Or-BAC concepts and GORE concepts. The proposed structured representation will manage the requirement elicitation process. It will also ensure the requirement traceability to deal with the dynamic and changing requirements among the dysfunctional analysis process from the first design steps. Furthermore, the proposed requirement ontology may be used in other domains since it will be grounded in top-level ontologies.

REFERENCES

[1] Summers, A.E., Techniques for assigning a target safety integrity level. *ISA transactions*, **37**(**2**), pp. 95–104, 1998.

[2] Debbech, S., Bon, P. & Collart-Dutilleul, S., Towards Semantic Interpretation of Goal-Oriented Safety Decision based on Foundational Ontology. *Proceedings of the 11 th International Conference of Computer Science and Information Technology*, Paris, 2018.

[3] Limnios, N., *Fault Trees*, John Wiley & Sons: USA, 2013.

[4] Mortureux, Y., *Preliminary risk analysis*, Techniques de l'ingénieur. Sécurité et gestion des risques, SE2 (SE4010): SE4010, 2002.

[5] Bouti, A. & Kadi, D.A., A state-of-the-art review of FMEA/FMECA. *International Journal of reliability, quality and safety engineering*, **1(04)**, pp. 515–543, 1994.

[6] Abrial, J.R., *The B-Book: Assigning Programs to Meanings*, Cambridge University Press: UK, 1996.

[7] Schmidt, D., Model-driven engineering, *IEEE computer*, 39(2), pp. 25–31, 2006.

[8] Ougier, F. & Terrier, F., ADONA: an open Integration Platform for automotiveSystems Development Tools, from Model-Driven Design to Resource Management for Distributed Embedded Systems. *IFIP TC 10 Working Conference on Distributed and Parallel Embedded Systems (DIPES), 2006.*

[9] Debbech, S., Bon, P. & Collart-Dutilleul, S., Improving safety by integrating dysfunctional analysis into the design of railway systems. *WIT Transactions on the Built Environment*, **181**, pp. 399–411, 2018.

[10] Guarino, N., Formal ontology and information systems. *Proceedings of FOIS*, **98**, pp. 81–97, 1998.

[11] Hoinaru, O., Mariano, G. and Gransart, C., Ontology for complex railway systems application to ERTMS/ETCS system. *FM-RAIL-BOK Workshop SEFM'2013 11 th International Conference on Software Engineering and Formal Methods*, 2013.

[12] E, U. G. UNISIG, System requirements Specification (SRS) version 3.4.0, E. R. Agency, available at http://www.era.europa.eu/Document-Register/Pages/Set-2-System-Requirements- Specification.aspx, 2016 (accessed 02 May 2017).

[13] Cranefield, S. & Purvis, M., UML as an Ontology Modeling Language. *Proceedings of the Workshop on Intelligent Information Integration, 16th Int. Joint Conference on AI (IJCAI-99)*, Germany, 1999.

[14] Manfred, B. & Cengarle, M.V., UML formal semantics: lessons learned. Software and Systems Modeling, **10(4)**, pp. 441–446, 2011.

[15] Richters, M. & Gogolla, M., On formalizing the UML Object Constraint Language OCL, *17th Int. Conf. Conceptual Modeling, eds*. T. W. Ling, s. Ram & M. L. Lee Lecture Notes in Computer Science, number 1507, Springer-Verlag, 1998.

[16] Cancila, D. et al., Sophia: a modeling language for model-based safety engineering, MoDE*LS ACE-MB*, Denver, Colardo, USA, pp. 11–25.

[17] Object Management Group: SysML v 1.5 Online. www.omg.org:spec/SysML/; p.161. (accessed 06 December 2017).

[18] Lucic, I., *Risk and Safety in Engineering Processes*, Cambridge Scholars Publishing: UK, 2015.

[19] Friedenthal, S., Moore, A., Steiner, R. *A practical guide to SysML: the systems modeling language*. Morgan Kaufmann, 2014.

[20] The Saint-Romain-En-Gier accident BEA-TT report, Rapport d'enqu ête technique sur l'accident ferroviaire du 5 avril 2004 à saint-romain-en-gier. Rapport technique, Ministère de l'É quipement, des Transports, de l'Aménagement du Terrioire, du Tourisme et de la Mer, METATTM. Online. http://www.bea-tt.developpement-durable.gouv.fr/saint-romain-en-gier-english-summary-a15.html. (accessed 09 September 2018).

[21] Ben Ayed, R., Modélisation UML/B pour la validation des exigences de sécurité des règles d'exploitation ferroviaires, Thèse de doctorat, IFSTTAR/COSYS/ESTAS, Univ. Lille, 2016.

[22] Rangra, S., Performance shaping factor based human reliability assessment using valuation-based systems – application to railway operations. Thèse de doctorat, Labex MS2T, Heudiasyc, UTC, 2017.

[23] Feiler, P. & Rugina, A., Dependability Modeling with the Architecture Analysis & Design Language (AADL). Technical report, Software Engineering Institute, Carnegie Mellon, 2007.

[24] ATESST Project. Advancing Traffic Efficiency and Safety through Software Technology. ATESST STREP - FP6 project Online. http://www.atesst.org. (accessed 09 March 2017).

[25] Piriou, P.Y., Faure, J.M. & Deleuze, G., A meta-model for integrating safety concerns into systems engineering processes. *7th Annual IEEE International Systems Conference (SysCon) 2013*, Orlando (Florida), pp. 298–304, 2013.

[26] Guillerm, R., Demmou, H. & Sadou, N., Combining FMECA and Fault Trees for declining safety requirements of complex systems. *Advances in Safety, Reliability and Risk Management: ESREL 2011*, pp. 207, 2011.

[27] Dubois, H., Gestion des exigences de sûreté de fonctionnement dans une approche IDM. *Journées Neptune n^{o}5*, Paris, 2008. (*in french*).