Interoperability between Risk Assessment and System Design for Railway Safety Critical Signalling System Development *

Marielle Petit-Doche
Systerel
1090 rue René Descartes
Parc d'activités de la Duranne
13857 Aix-en-Provence cedex 3
marielle.petit-doche@systerel.fr

Frédéric Thomas
Obeo
2 route de la Noue - BP 76
91193 Gif-sur-Yvette
frederic.thomas@obeo.fr

Fabien Belmonte
Alstom Transport
48 rue Albert Dhalenne
93482 Saint-Ouen cedex
fabien.belmonte@transport.alstom.com

December 13, 2011

Abstract

The goal of this paper is mainly to show how it would be possible to improve collaboration between system designer and safety assurance manager. Both of them use models since long time but those are generally non interoperable because of their different viewpoints on the system.

In this work a tooled methodology has been developed allowing safety engineers to build their models by requesting directly the system design model. Hence, the risk assessment is strongly coupled with the designer production. Formal methods are used to complete the safety analysis to record rigorous reasoning about system safety properties proof in a formal model.

1 Introduction

Railway signalling system design on the one hand and risk and safety studies on the other should be strongly coupled. Today collaboration between these two disciplines is performed by a regulated process defined by CENELEC standards (EN 50126 [6], EN 50128 [7], EN 50129 [8]) and imposed by national authorities. It seems that this process shall be more tooled in order to improve the collaboration between safety and system engineers. Safety engineers perform risk assessments by reading and validating the work of system engineer. By applying the methodology from the previously mentioned standards, they aim to identify as exhaustively as possible the accident scenarios and the possible failures of the system and control their mitigation by validating the correct application of the safe development methodology done by system design (including risk control architecture and error free process development [4]). It follows that the collaboration between safety analysts and system designers shall allow designers to express a model of the system and the cues of its safe behavior. Today, system design is generally described with textual requirements in large documentation. Safety engineers validate these designs, by identifying safety related requirements and validating the risk control strategy. Up to now, this validation has been done on textual documentation. The documentation reveals the result of system design activity and the rationale of the retained solution is not recorded. Furthermore, the results included in documentation are difficult to reuse especially for the safety engineers. Recently,

*This paper is funded by the "Systematic Paris Region" cluster in the context of the IMOFIS project. Authors thank the Systematic cluster and all participants of the IMOFIS project. http://www.imofis.org

Alstom Transport introduced a model based system engineering methodology to tackle these limitations of the textual approach [9]. This approach is made of three viewpoints (Operational, Functional and Constructional) and supported by the so-called SysML notation.

Moreover, due to the growing complexity of the developed system, it becomes very difficult to demonstrate the behavioral safety of the system. In this domain, formal modeling techniques are helpful. It allows safety engineers to record rigorous reasoning about system safety properties proof in a formal model. Most of the formal techniques assist the safety engineers by providing formal proof assistant. Such reasoning are clues to justify trustworthiness of the system safety.

The goal of the work presented in this paper is to show how it would be possible to improve collaboration between system designer and safety assurance manager. Both of them use models since long time but those are generally non interoperable because of their different viewpoints on the system. Safety engineers use models that describe the dysfunctional behavior of the system in order to assess and better control the risks. Such models refer to specific formalisms: Fault Trees, Event Trees, Failure Modes and Effect Analysis (FMEA), see [5]. Until today, to build these models, safety engineer stem from documentation of the system.

In this work a tooled methodology has been developed allowing safety engineers to build their models by requesting directly the system design model. Hence, the risk assessment is strongly coupled with the designer production. Formal methods are used to complete the safety analysis by ensuring that safety requirements are verified on formal models of the system and reinforcing requirement traceability in regards of safety analysis.

2 Methodology

The major concern of safety engineers is to insure that the risks are exhaustively covered. To reach this goal, two processes are performed during the specification and design phases of the system. One is a deductive strategy where the safety assurance manager shall deduce the causes of accidental scenarios. The second is an inductive strategy, where the safety analyst shall infer the effects of local failures. These two strategies are complementary: causes of failure identified in the deductive risk assessment are corroborated by the effect given by the inductive risk assessment. Furthermore, problems forgotten in one approach should be seen in the second.

The risk assessment starts with the identification of accidental scenarios. This analysis is called Preliminary Hazard Analysis (PHA). Based on the definition of accidental scenarios, fault trees are built to identify the causes of the accidents, this is the deductive phase of the risk assessment called *System Hazard Analysis - Fault Tree or SHA-FT*. Then, the safety analysts take into account the elementary failures of the system one by one and identify their effects on the system. This is the inductive process named SHA-FMEA.

The PHA is modeled with event tree formalism, the SHA-FT with fault-trees and SHA-FMEAs are serialized within tables. PHA needs to be linked with structural and operational model elements of the system design model. And SHA are linked to structural and functional model elements of the system design model.

A domain specific language supported by semi-formal modeling tool for risk assessment has been developed. It is able to communicate with any system engineering modeling language as long as the model follows the Eclipse Modeling Framework format. The main features are:

- Graphical representation of PHA and SHA;
- One model serialized, many views are available;
- Serialization of the global risk analysis into one fault tree;
- Requests on system design model and references of model element into risk assessment;
- Customization of requests based on system engineering method used in system design (e.g. which model element represents function ?);
- Automatic layout of graphical representation (very usefull for large model);
- Requirements repository and traceability purpose;

3 Formal models for Safety analysis

The use of formal methods to support safety analysis by rigorous reasoning on models of the system allows to strengthen the processes described in the previous section. Due to the current practice of B method [3] in development of critical software in the railway industries, Event-B [1] a close language more suitable for system modeling, with a top-down approach following the system and safety steps

has been chosen. Hazard Analyses have highlighted safety requirements, however the usual manual demonstration that safety requirements are covered by the system can be difficult in some complex cases. Event-B models show that a safety property is verified on a formal model of the system, with system functional models and safety properties modeling in the same language. Several elements improve the safety analysis:

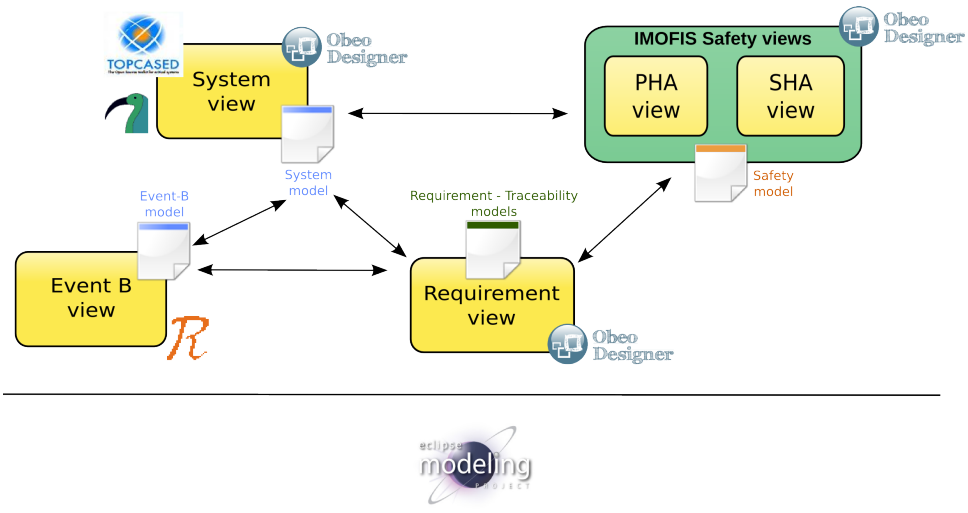
- Formal models highlight the functional concepts of the system models to ensure safety requirements;
- Formal proofs follow rigorous mathematical reasoning which ensures that the formal models and the safety requirements are consistent;
- Event-B approach allows a step by step refinement of the formal models, which can follow the system design and the safety analysis refinement steps. Formal models describes the safety properties that each functions of each subsystems shall cover. Formal proofs of the model shall strengthen completeness of the safety requirements during refinement steps;
- Formal model and proof structure shall strengthen fault tree analysis : the proofs highlight the functional elements of the system necessary for the mathematical reasoning;
- Formal models shall be animated to be validated in regards to informal system models and safety analysis;
- Formal models and proofs can be recorded and reused for an evolution of the system.

4 Tools

From a tool provider point of view, there are several challenges to tool up this system engineering methodology :

- interoperability : The key idea of the underneath implementation work is to provide a common framework in which both system engineers can model the system and safety ones can describe their analyses (PHA, SHA, FMEA, Event B models),
- adaptability : a tool in adequation with both the system and safety expert needs must been provided. It must be a unique tool with several viewpoints : safety and system design viewpoints.
- incrementallity : as any research and development tooling project, the needs are not static but they evolve.

Our current tooling approach is described on the next figure.



To be able to provide interoperability, the Eclipse Modeling framework has been used. This framework is opened, available and it is a common adopted framework for many meta-modeling tools based on Eclipse. It profits us to provide textual, graphical and web-based editors to the engineers. Those technologies allow us to implement specific metamodels for Safety, to reuse SysML implementation [1], to adapt incrementally our tools from the expert reviews, and to extend then to existing tools based on the same Eclipse Modeling framework (for example with Rodin [2] to edit and validate formal Event-B models). Firstly the required metamodels (safety, requirement management, traceability) is defined,

[1] the Topcased SysML implementation is used

secondly their Java API implementations is generated and finally editors are build upon this new API. Thus, with the viewpoint-based Obeo Designer technology, graphical and tabular views have been developped to describe Safety models. Such a tool allows us to customize a generic model editing tool for expert needs. It allows one to iteratively describe specific PHA viewpoint in order to adapt the editing framework to our methodology. At the end, all engineers works on the same set of models with several point of views : PHA view, SHA view, Requirement view, System view. Each view represents the same system but with a different concern.

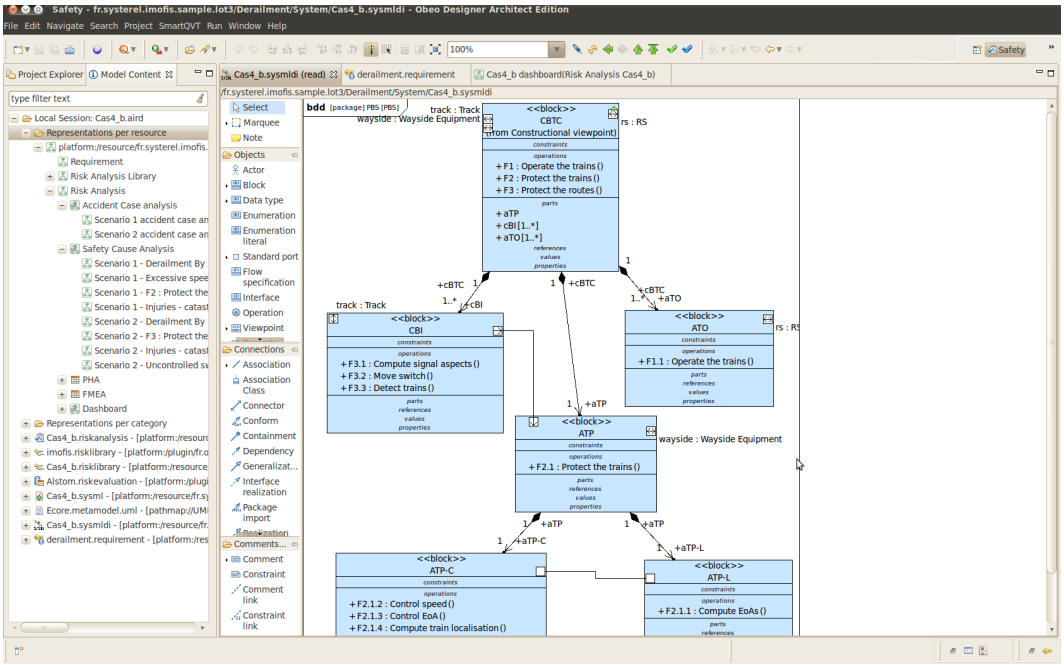
Thanks to a common modeling framework and a viewpoint based technology, the risk analysis models are coupled to the system design model in SysML. Indeed, it allows safety engineers to be fully compliant with the operational, functional and constructional viewpoints modeled by system design. Moreover, graphical representations of the risk analysis model synchronized with a tabular synthetic representation is provided. The graphical representation is more intuitive for the safety engineers since it is based on on-going work [9] for the update of the CENELEC standards (also discussed in MODSAFE and MODCONTROL European R&D programs). The tabular representation allows to publish the result of the risk analysis and also to accelerate the modelling activity when risk analysis is obvious. Finally, Rodin platform [2] has been embedded in the common platform. This allow to link directly formal model elements to the safety requirements defined by the safety analyses. Complementary tools have been developed to check the covering of the requirements by the formal models and to check the proof status.

5 Example

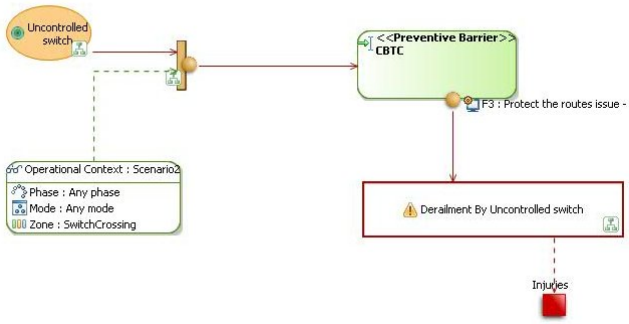
This approach is going to be described on a small example from the railway domain: apart of a signaling system. Such system shall protect against derailment. The objective of our model is to specify the elements of the system to avoid derailment.

The starting point of our approach is a system model, in our case a SysML model, which describes the structure and functions of the system via block, activity and sequence diagrams.

The following figure gives the block diagram for our example: a CBTC system to operate train movements and to protect train against derailment. A CBTC consists of three kinds of subsystems: CBI in charge of interlocking functions, ATP in charge of protection of train functions and ATC in charge of operation on train functions.

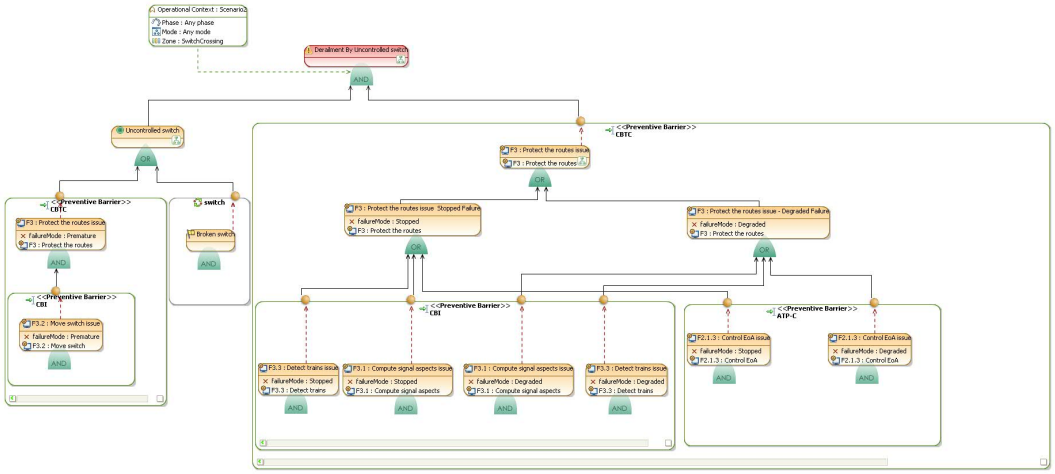


Safety engineers can start risk assessment with the preliminary risk analysis. Accidental scenarios are graphically defined as in figure: a safety hazard "Uncontrolled switch" is defined in a given context, the preventive barrier CBTC and its function "F3: Protect the route issues" prevent from the accident "Derailment by uncontrolled switch" and its consequence "Injuries".

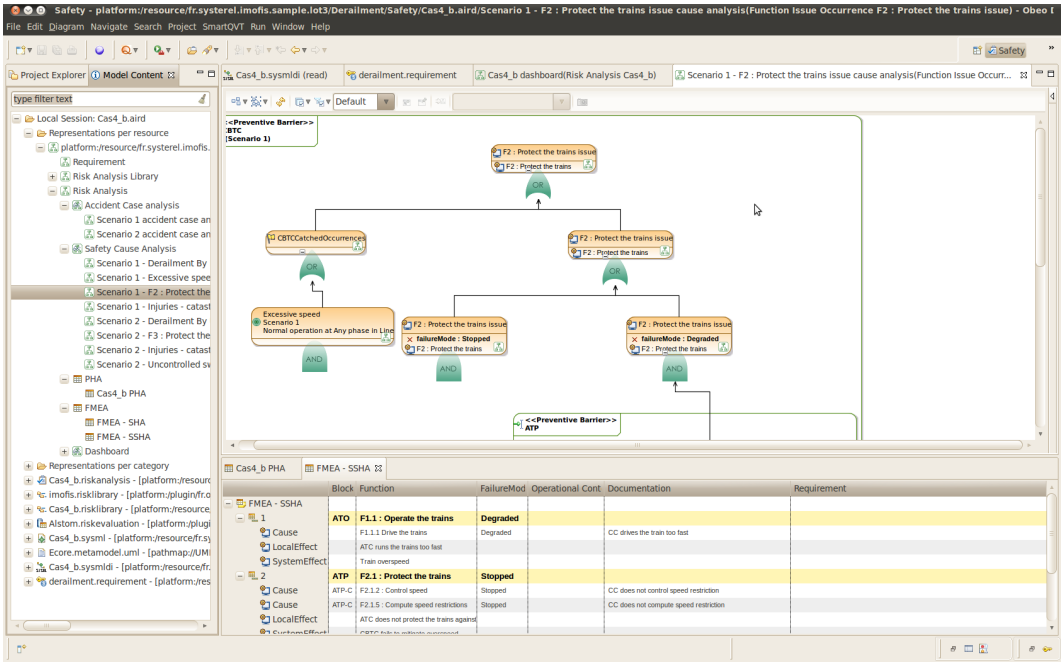


In this case, the preventive barrier is constituted of elements of the system. Thanks to tool integration, safety engineers can directly use elements of the SysML model during their analyses.

Then fault trees are built to identify the cause of each accident (see next figure): failures of functions and sub functions are analyzed for a given accident. Once again tool capabilities allow using directly the elements of the SysML models.

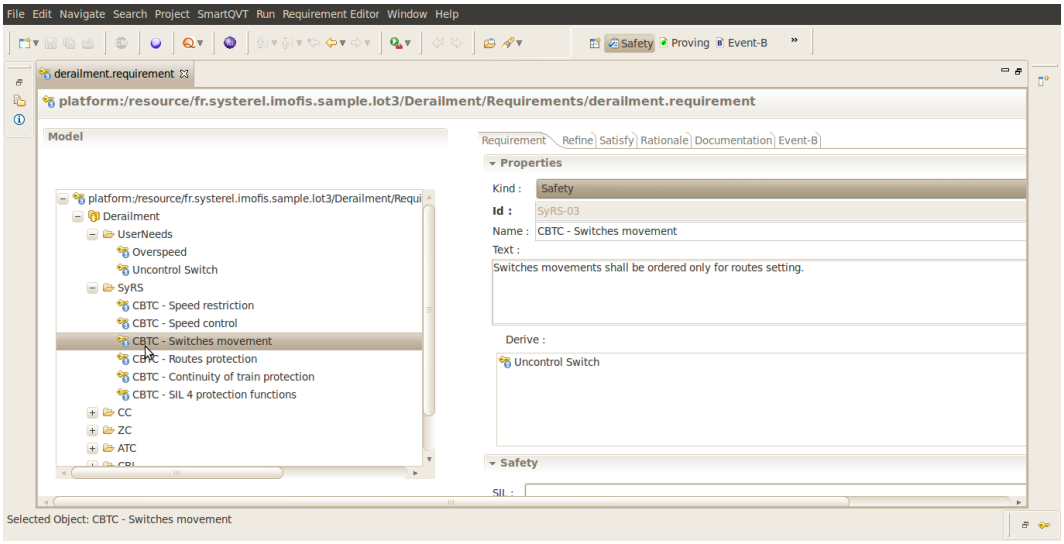


Tabular view of the PHA is also provided by the tool. The FMEA is currently defined in a tabular view as in the next figure.

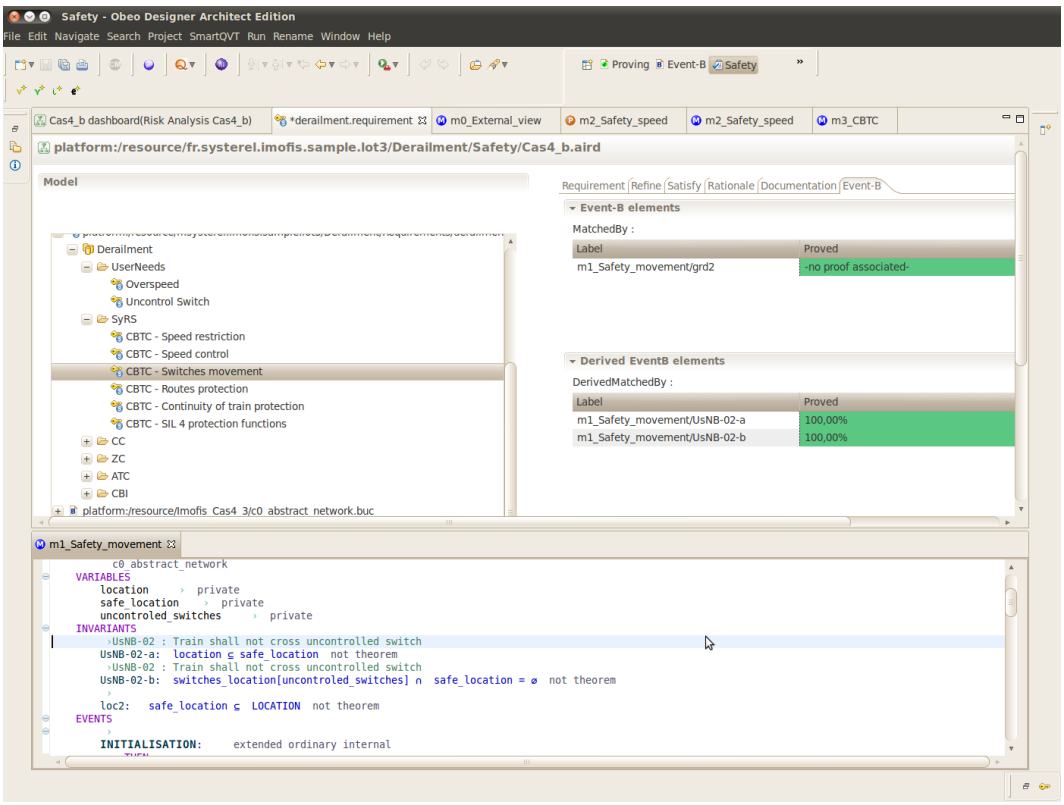


Main part shared by system design and safety process is the requirement repository. The specific requirement view (on the next figure) collects information on requirements:

- description of the requirement and traceability with other requirements
- traceability of the requirement on the system model (allocation on block and function)
- traceability on the safety analyses



Moreover the requirement view is linked to the Rodin tool to connect strongly the requirements to Event-B models as in the next figure. Tools dedicated to formal proof and animation can be used directly from the common platform, with report on proof status on the formal model.



6 Discussion

The model allows the users to analyze the risk analysis, perform verification by means of structural model verification provided by the modeling tool. The main benefits are to assist the verification tasks

(traceability, consistency and correction) and to put closer the system design engineering and safety engineering. Formal models strengthen the safety analysis and allow to reuse this analysis. Finally, model driven engineering improves confidence in system and safety analyses while providing reusable modeling concepts close to the different engineers' background and thus improve system design and safety activities.

The framework is going to be extended:

- to other formal methods like AltaRica to complete safety analysis means
- to other tools for requirement and analysis management
- to other activities around critical system development (software development, validation and verification, quality...)

References

[1] J-R. Abrial, *Modeling in Event-B*, Cambridge University Press 2010.

[2] Rodin platform : www.event-b.org

[3] J-R. Abrial, *The B-book: assigning programs to meanings*, Cambridge University Press 1996.

[4] M. Carnot, C. DaSilva, B. Dehbonei and F. Mejia, Error-free software development for critical systems using the B-Methodology in proceedings of the Third International Symposium of Software Reliability Engineering, Research Triangle Park, NC, USA, oct. 1992

[5] Villemeur, Alain, Reliability, availability, maintainability, and safety assessment, J. Wiley, 1992

[6] CENELEC, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS), EN50126.

[7] CENELEC, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems, EN50128.

[8] CENELEC, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling, EN50129.

[9] Belmonte F., Blas A. et Mejia L.-F. And Thomas F., *Risk Evaluation in Railway Systems Supported By Modeling Languages and Tools*. Lambda-Mu, 17ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement. La Rochelle : IMDR, 2010.