Study of implementation of ERTMS with respect to French national rules using a B centered methodology.

Philippe Bon, Simon Collart-Dutilleul, Pengfei Sun

International Conference
on Industrial Engineering and Systems Management
IESM'2013
October 28 - October 30
RABAT - MOROCCO

Study of implementation of ERTMS with respect to French national rules using a B centred methodology

Philippe Bon [a,b] Simon Collart-Dutilleul [a,b] Pengfei Sun [a,b]

[a] *Univ Nord de France, F-59000 Lille, France*

[b] *IFSTTAR-ESTAS, 20 rue lise Reclus, F-59650 Villeneuve d'Ascq, France*

Abstract

Interoperability of the rail system within Europe is a key to its competitiveness. It aims at creating a rail network allowing a transport that is safe, compliant with the required performance level of the lines, and which does not necessitate train transfers. This requires the compliance with a set of rules, of technical and operational conditions which ensure that all the safety requirements are met. The main proposition is to contribute to the implementation of a European system for railway signalling called "European Rail Traffic Management System" (ERTMS) using a methodology based on B framework tools.

The idea is to assist the writer of the national operating rules. The national operating rules are expected to define the precise implementation of the high level ERTMS Specification Requirement System (SRS). They fulfils the national rule and refines the ERTMS specification in the context of a particular infrastructure. Some parts of the specification may be considered as irrelevant in the context of some particular infrastructures.

A second step consists in refining the needed behaviour so that the national safety conditions and the ERTMS can be proved to be fulfilled. The methodology proposes to represent all the needed information using the B formalism in a three stepped methodology:

- The first step models the useful part of ERTMS specification in the context of the considered infrastructure. A requirements model is obtained.
- The second step consists in enriching the existing model with a precise description of the functioning of the infrastructure. More precisely, the interlocking implementation and the Automatic Train Protection (ATP) is taken into account and a process model is obtained.
- The third step consists in consistency checking between the two first models. The second model should be a refinement of the first one, because it is a particular instantiation of the ERTMS requirements. When it is not the case, some proof obligations will not be validated by the proof assistant included in the B framework. Then, the writer of the operating rules can try to introduce new logical propositions so that the proof obligations are fulfilled.

When these three tasks are achieved, the writer of the rule has the logical proof that his operation rule is a national instance of the ERTMS SRS. The focus of the paper will be mainly on the second step.

Key words: Railway, ERTMS, Safety, National rules, B method

Email addresses: philippe.bon@ifsttar.fr (Philippe Bon), simon.collart-dutilleul@ifsttar.fr (Simon Collart-Dutilleul), pengfei.sun@ifsttar.fr (Pengfei Sun).

1 Introduction

A change of the embedded signalling system during a border cross generates an important over cost. Interoperability of the rail system within Europe is therefore key to its competitiveness. The aim of interoperability is a railway system allowing a safe transport without train transfers and compliant with required performance level of the lines. Consequently, the system has to respect statutory, technical and operational conditions which ensure that all the safety requirements are met. The proposition of this paper is to contribute to the implementation of a European system for railway signalling called "European Rail Traffic Management System" (ERTMS) using a methodology based on B framework tools.

A first section describe the context of the study. It explains the ERTMS technological context, including difficulties identified in the previous ERTMS implementation projects . The second one presents the modelling aspects. The different level of accuracy and the needs of consistency are discuss taking into account some industrial feasibility constraints. The third section presents the proposed methodology. As there is a need of assessment, all the specification are checked using some B formal method, whereas they may be initially formulated using another formalism. This section focuses on the national context. A particular use case is presented and the methodology of the translation into B abstract machines is explained. The last section proposes some further ideas before concluding.

2 Context

The management of railway signalling in ERTMS is based on local rules pertaining to each country and not on global rules. This makes it difficult to evaluate the system in terms of safety. Thus, one of the main objectives of this study is to supply methodological tools for the evaluation of the global consistency between the specification and the operating rules, with regard to safety. This issue is crucial and yet it has scarcely been covered by scientific literature.

Nevertheless, an European project, named "Open ETCS" [1] , aims to develop an integrated modelling, development, validation and testing framework for leveraging the cost-efficient and reliable implementation of ETCS. Consequently, scientific community will have a common base of models of ETCS, which is a part of ERTMS. Or proposal is to use these models as requirements model.

A French national project, named Perfect [2] , aims at contributing to the validation and implementation of ERTMS by giving methodological tools to globally assess the compliance between the specifications and operating rules.

3 Modelling aspect

3.1 About using the appropriate tools at the appropriate level

The ERTMS specifications are written in a not so precise way. The assumed idea is to keep the possibility of allowing technological innovation while providing interoperability services. For this reason, the more appropriate modeling language may not be a formal language. In fact, there are some proposition in the state of the art for using the Unified Meta Language (UML)[7] and more precisely its specialization for system descriptions: SysML[10]. As it shown on Figure 1, when an exhaustive specification is built, it is transformed into B formalism for the assessment task using the proof assistant of the B tools.

The main idea is to use UML notations to centralize all, requirements using a unique language. One of the arguments is that UML notation are well known and it is easy to find engineers able to deal with this kind of models, teaching resources are available, etc. . . Another consequence is that there is a lot of modelling proposition based on UML in the state of the art (see figure 2).

Focusing more precisely on the model transformation aspects, this first proposition has some weakness. B is a formal model, and other formal models of the state of the arts are used for signalling system setting[2]. It

[1] `http://openetcs.org/`

[2] `http://www.agence$-$nationale$-$recherche.fr/projet$-$anr/?tx{\_}lwmsuivibilan{\_}pi2$[$CODE$]$=ANR$-$12$-$VPTT$-$0010`

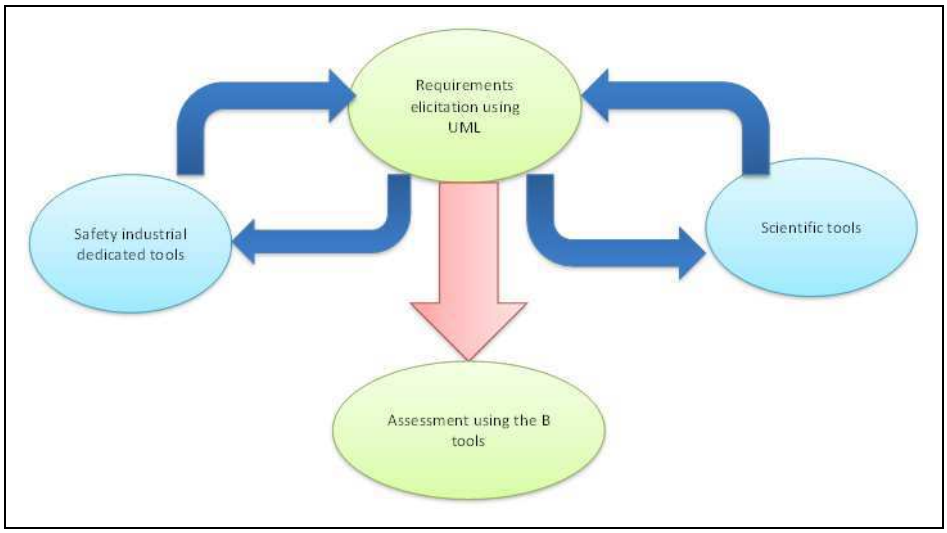

Fig. 1. *UML* centred requirement engineering approach

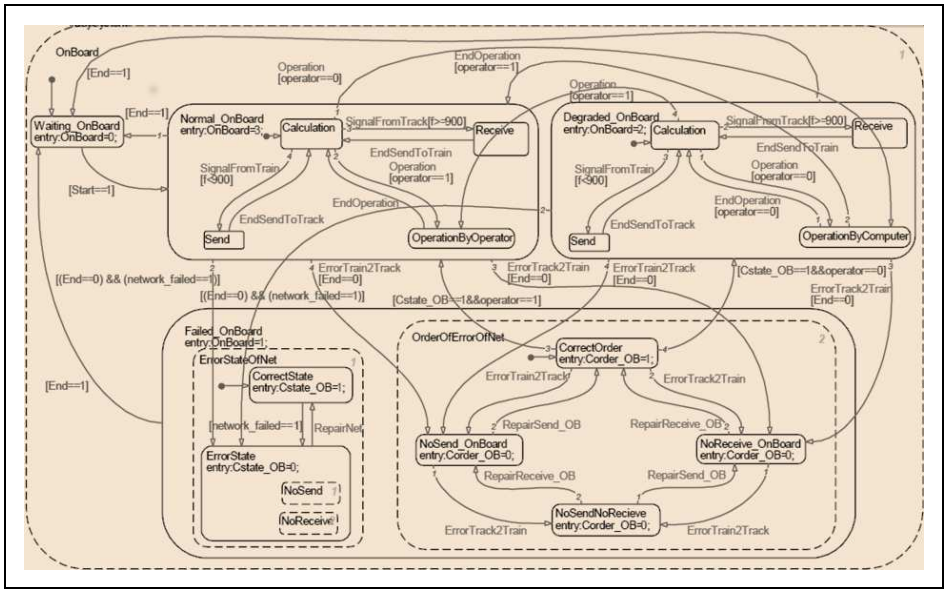

Fig. 2. *UML* State chart of the ERTMS on board system from [16]

does not seem really relevant to use a semi-formal language as an intermediate language for transforming a formal model into another one. The transformation task is of course easier to perform handling only some non-ambiguous semantics.

This first consideration is tempered by another strong argument: the need of consistency of the global specification. All the information must be expressed and put in a same referential in order to be able to identify contradictions and non-coherences.

In railway area, considering the ERTMS specification the following explanation may highlight some critical aspects: The interlocking system, like the communication system, like national rules, is not in the ERTMS specification. All these entities are sub systems which influence the safety analysis of a system using ERTMS/ETCS. Nevertheless, no direct contradictions can be found between the different specifications because the ERTMS does not directly talk about them.

This leads to the following proposition to introduce the low-level and formal specification directly in the *B* model when the concerned sub-systems are not mentioned in the ERTMS specification. Let us point out the need of proved transformation in the assessment process in order to be sure that no critical information is forgotten or modified.

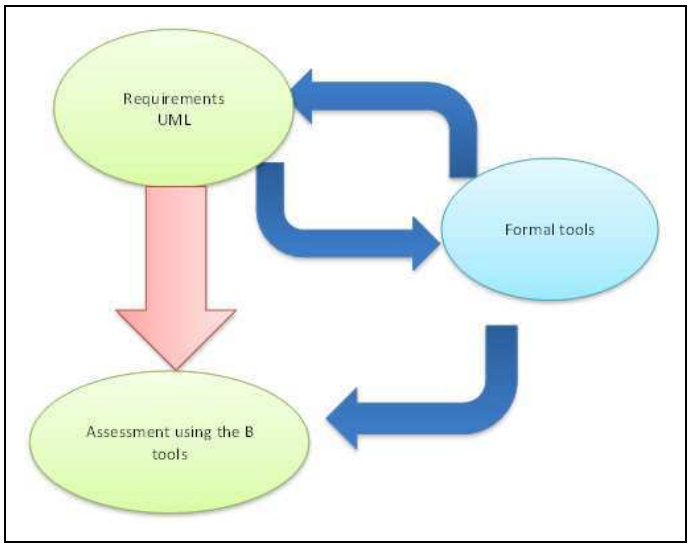

Fig. 3. B centred assessment process

3.2 Model based assessment process

From a formal point of view, the assessment activities can be described as proving that the proposed solution corresponds to the specification. In other words, focusing on safety aspects, it has to fulfil all the safety requirements included in the specification.

A first step towards solving this problem is to provide a formal model of the requirements[9]. A second step is to build a model of the proposed solution. The third step consists in consistency checking between the model of requirements and the model of a solution. Formally, the second model has to be a refinement of the first one.

This last consideration leads us to the proposition of translating all produced model into B formalism in order to use the embedded proofer[12,14]. To solve this kind of problem, there are some works in the state of the art describing some B centred approach[1,13,18].

The refinement is a process in the B method. It transforms an abstract specification into a concrete and deterministic one. This transformation preserves all the functionalities of the initial specification. During a refinement phase, some new variables and new event can be introduced. In this case, the corresponding new proof obligation are generated such a way that the coherency with the initial specification is maintain. In other words, some new conditions to be fulfilled are described, whereas the proof of this fulfilment implies the proof of the initial specification fulfilment. Using Event-B tools a open software platform, based on "Eclipse" one, allows to specify and prove. Its name is Rodin [3].

To decrease the dimension of the consistency checking problem, it may be interesting to use a projection of the model of the requirements on the state space of the proposed solution.

A formulation of this problem is given as follows[6]:

- Sr is the set of state classes generated from the requirements,
- Ss is the set of state classes generated from the potential solution,
- D is the range of requirements and
- $R(A, B)$ is an application which makes the projection from A towards B.

As a result, we want to check if: $R(Ss, D) \subset Sr$

Let us consider an example takes out of a ERTMS SRS. In the SRS, the functioning of a functioning mode called "shunting" is described. Considering the implementation of this SRS on a French infrastructure, the following fact has to be integrated: the shunting mode is not allowed in France. As a consequence, to propose a French implementation of the corresponding SRS, there is no need to model the shunting ERTMS mode because it

[3] Event B portal: `http://www.event-b.org/`

projection in a French context will be empty. Actually, there is nothing to be checked concerning the requirement model of the "shunting" procedure.

When all the functioning modes are distinct, a solution is valid if: $\bigwedge_i(A_i)$

where

- $SS = \{Ss_i\}$
- $DD = \{D_i\}$
- $SR = \{Sr_i\}$
- $A : SS \times DD \times SR \rightarrow \{True, False\}$
- $If D \neq \emptyset$:
  - $A : (Ss, D, Sr) \rightarrow (R(Ss, D) \subset Sr)$
- $If D = \emptyset$:
  - $A : (Ss, D, Sr) \rightarrow True$

Roughly speaking, experts have to identify the functioning mode first, and then the above condition has to be checked. Considering ERTMS SRS, functioning modes are clearly identified. There are described separately. Moreover, switching between different modes is documented too.

4 French context integration

4.1 System description

4.1.1 Railway System

A railway System consists of three essential elements:

- The 1st one is the infrastructure with the track work, the station, the signalling equipment and the catenary or third rail system with power supply (figure 4).
- The 2nd one is the rolling stock composed by cars and locomotives.
- The 3rd is a system of operating rules and procedures for a safe and efficient operation.

And this is what we concerned in the whole project.

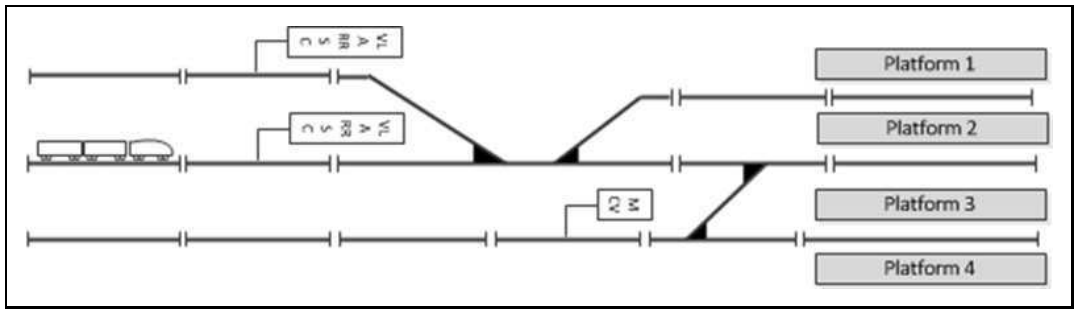

Fig. 4. Example of railway infrastructure

4.2 Interlocking

The term "interlocking" is used with two meanings:

- An interlocking is an arrangement of points and signals interconnected in a way that each movement follows the other in a proper and safe sequence,
- and the principles to achieve a safe interconnection between points and signals are also generally called "interlocking".

The route a train could go through is called signal routes that are usually interlocked with facilities related to the route. The signal and points with solid circles are essential parts of a signal route, and the dotted circle is the security protection to this route, in case other train rushes into the green route.

4.2.1 Signal Route Conditions

The Signal Route Conditions must meet the following conditions:

- All points must be set properly and locked,
- conflicting routes must be locked and
- the track must be clear.

This is provided by the following functions:

- Interlocking between points and signals,
- route locking,
- locking conflicting routes,
- flank protection and
- track clear detection.

4.2.2 Procedure of "Establish a route"

The flow diagram of figure 5 is part of Establishment of an interlocking route in [17].

This flow diagram contain 3 functions:

- Command a route,
- formation of the route and
- open signals.

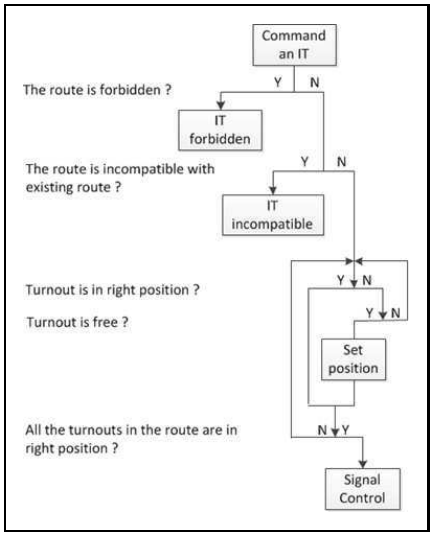

Fig. 5. Diagram of an itinerary formation and control

The conditions for an itinerary control are strict and precise, whereas they are safety critical. For these reason, a non-ambiguous semantic tool is needed for this modelling task. As National railway Society (SNCF) use to control new interlocking devices by the mean of Petri Net[2], this modelling tool is a natural choice.

4.3 Modelling using Petri nets

Petri Nets were introduced by C.A. Petri en documented in [15]. This model is well fitted to both mathematically and graphically represent the concept of asynchronous and concurrent actions. There is a huge scientific literature concerning the underlying mathematical properties of Petri Net. Nevertheless, when the system to be modelled has a big dimension, the size of the corresponding model becomes non tractable. For this reason some abbreviation and extension were introduced in order to provide more descriptive power to the model. Coloured Petri net is one of the proposed tools, which can produce more compact models. Moreover, it was successfully applied for ERTMS modelling[3].

CPN is a Petri net language developed by Professor Kurt Jensen [11]. It is Supports the extensions with time, color and hierarchy. The CPN language syntax is based on standard Meta language. In CPN tools Syntax, each place and token must have a color type. The CPN tolls adopted from the Standard ML [19], but it is not fully supported.

A coloured Petri net is a tuple $CPN = (\Sigma, P, T, A, N, C, G, E, I)$ as:

(1) Σ non-empty and finite set of types, called **colours**,
(2) P is a finite set of places,
(3) T is a finite set of transitions,
(4) A is a finite set of arcs, as: $P \cap T = P \cap A = T \cap A = \emptyset$,
(5) N is the **node** function, defined from A to $P \times T \cup T \times P$,
(6) C is the **color** function, defined from P to Σ,
(7) G is the **guard** function, defined, from P to expressions, as:

$$\forall t \in T : [Type(G(t)) = \mathbb{B} \wedge Type(Var(G(t))) \subseteq \Sigma],$$

(8) E is an **expression of arcs** function, defined from A to expressions, as:

$$\forall a \in A : [Type(E(a)) = C(p(a))_{MS} \wedge Type(Var(E(a))) \subseteq \Sigma]$$

where $p(a)$ is a place of $N(a)$,
(9) I is an **initialisation** function, defined from P to closed expressions, as:

$$\forall p \in P : [Type(I(p)) = C(p)_{MS}].$$

Using coloured Petri nets, the action of verifying that the itinerary to be traced is compatible with the infrastructure and the already existing one is described one the figure 6. Actually, his is only a part of the needed action demanded in the flow-diagram presented on figure 5.

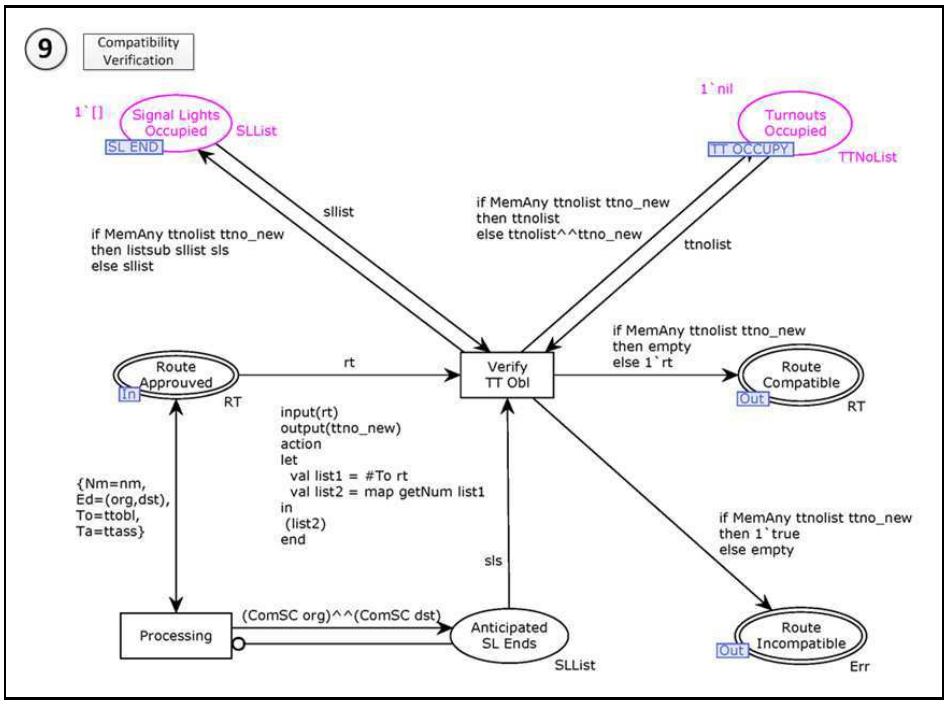

Fig. 6. Compatibility verification

This model, modelling verifications of compatibility, extracts the turnout number information and obviously the numbers of mandatory turnout. The mandatory turnouts are the directly participating in the formation of the considered route.

Then, corresponding numbers are compared with the global register named "TT OCCUPY". If any of the numbers are already in the register, this route is incompatible, the model will return an Error token, otherwise

the model will put these number into global register and return this route token. Moreover, if the route is incompatible, it will also cancel the operation from previous "forbidden verification" module.

4.4 Integration of the interlocking logic into a B methodology

Coloured Petri nets, or more generally speaking high level Petri nets, are formal tools build upon mathematically defined semantic. Nevertheless, consistency checking with a part of the specification which is described using B abstract machines is not direct. A proposed solution is to translate the high level Petri nets model into B abstract Machines [5].

When this first translation step is performed, the couplings between the several abstract machines are not taken into account in the obtained model. Then by link editing, it is also possible to obtain a single B component by implementing the algorithm described in [4].

The principle of the algorithm is to translate two B specifications (connected by a refinement or a composition link) into a single one. The properties are the properties of the originals specifications enriched with a specific part that expresses the nature of the link between the two different specifications. The algorithm which is implemented the "BRILLANT platform" [8], is detailed in [4].

5 Conclusions

In the presented paper, the ERTMS context of the study has been described. The need of non-ambiguous specification has led to a model engineering problem. The difference of specification which may be found in different kind of document was pointed out. For this reason a several modelling tool approach is proposed.

Focusing on low-level specification, formal model and formal proof are needed. An illustration on an itinerary control problem of an interlocking device was presented. A methodology, based on existing scientific works, aiming at integrating this new information into a global specification is shortly described.

The presented paper mainly focuses on the enrichment phase of the ERTMS specification with some national and specific to a given infrastructure information.

The next step to be performed in following works, starting from an existing B specification, is to document how B tools can be used in order to identify some lake of specification in safety operating rules.

References

[1] Yamine Aït Ameur and Mickaël Baron. Formal and experimental validation approaches in HCI systems design based on a shared event B model. *International Journal on Software Tools for Technology Transfer*, 8(6):547–563, 2006.

[2] Marc Antoni. Formal validation method for computerized railway interlocking systems. In *Computers Industrial Engineering, 2009. CIE 2009. International Conference on*, pages 1532–1541, 2009.

[3] Pavol Barger, Walter Schön, and Mohamed Bouali. A study of railway ERTMS safety with colored petri nets. In *The European Safety and Reliability Conference (ESREL'09)*, Prague, Czech Republic, 2009. HAL - CCSD.

[4] Salimeh Behnia. *Test de modèles formels en B : cadre théorique et critères de couvertures.* PhD thesis, Institut National Polytechnique de Toulouse, October 2000.

[5] Philippe Bon and Simon Collart-Dutilleul. From a solution model to a *b* model for verification of safety properties. *Journal of Universal Computer Science*, 19(1):2–24, jan 2013. `http://www.jucs.org/jucs_19_1/from_a_solution_model_to`.

[6] Philippe Bon, Simon Collart-Dutilleul, and Fran cois Defossez. Functioning mode management and formal assessment of safety. In Pierre Borne and Florin Gheorghe Filip, editors, *Large Scale Complex Systems Theory and Applications*, volume 9, Lille, France, July 2010.

[7] Philippe Bon, Simon Collart-Dutilleul, and Dorian Petit. A set of design-oriented scientific tools to assist abstract B machine specification. In *3rd IEEE International Symposium on Logistics and Industrial Informatics (LINDI 2011)*, pages 209–214, Budapest, Hungary, 25-27 August 2011.

[8] Samuel Colin, Dorian Petit, Georges Mariano, and Vincent Poirriez. BRILLANT: an open source platform for B, 2010.

[9] Fran cois Defossez, Simon Collart Dutilleul, and Philippe Bon. A formal model of requirements. *Open Transportation Journal*, 5:60–70, October 2011.

[10] Hadi Jaber, Nataliya Yakymets, and Agnes Lanusse. Model based system engineering for safety analysis of complex systems: the benefits of UML profile mechanisms implemented in papyrus. In *Model-Based Safety Assessment Workshop (MBSAW 2012)*, Bordeaux, France, 11-12 2012.

[11] K. Jensen. *Coloured Petri Nets - Basic Concepts, Analysis Methods and Practical Use, Vol. 1.* Springer-Verlag, Berlin, 1992.

[12] Régine Laleau and Amel Mammar. An overview of a method and its support tool for generating B specifications from UML notations. In *The 15st IEEE Int. Conf. on Automated Software Engineering,*, September11-15 2000.

[13] Régine Laleau, Farida Semmak, Abderrahman Matoussi, Dorian Petit, Ahmed Hammad, and Bruno Tatibouët. A first attempt to combine SysML requirements diagrams and B. *ISSE*, 6(1-2):47–54, 2010.

[14] Éric Meyer and Jeanine Souquières. Systematic approach to transform OMT diagrams to a B specification. In Jeannette M. Wing, Jim Woodcock, and Jim Davies, editors, *FM'99 – Formal Methods*, Lecture Notes in Computer Science (Springer-Verlag), pages 875–895. Springer-Verlag, September 1999.

[15] Carl Adam Petri. Kommunikation mit Automaten (in German). Internal Report 2, Institut fuer Instrumentelle Mathematik, University of Bonn, Bonn, FRG, 1962.

[16] Siqi QIU, Mohamed SALLAK, Walter SCHN, and Zohra CHERF. Modélisation et évaluation de la disponibilité d'un système de signalisation ferroviaire ertms niveau 2. In *QUALITA'2013, 10ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement*, Compiègne, France, March19-22 2013.

[17] Roger Rétiveau. *La signalisation ferroviaire.* Presse de l'École Nationale des Ponts et Chaussées, 1987.

[18] Colin Snook and Michael Butler. UML-B: Formal modeling and design aided by UML. *ACM Transactions on Software Engineering and Methodology*, 15(1):92–122, January 2006.

[19] J. D. Ullman. *Elements of ML programming.* Prentice Hall, 1994.