A study of railway ERTMS safety with Colored Petri Nets

Pavol Barger, Walter Schön, Mohamed Bouali

A study of railway ERTMS safety with Colored Petri Nets

P. Barger, W. Schön & M. Bouali
Heudiasyc UMR CNRS UTC 6599
Université de Technologie de Compiègne
France

ABSTRACT: European railway systems are in a constant technological progression combined with an international interoperability and standardization. This need gave birth to the European Rail Traffic Management System (ERTMS) with the goal to provide the basic framework to the interoperable rail signaling and train control. The analysis, verification and validation of such specifications are naturally crucial. These studies are done on models that are more or less formal. The presented work has chosen Colored Petri Nets (CPN) for the system modeling and analysis. CPN allow not only the modeling of the overall system structure but also its possible evolution in time. It is in this context, that they are applied in this paper to express both: 1. the ERTMS operational procedures as well as 2. the on-board and trackside component communication. The main goal of this work is to test the feasibility of the construction of the complete specification model using a unique modeling approach and to prepare the model for a further in-depth analysis for safety and/or performance proprieties.

1 INTRODUCTION

The ever increasing need for a high quality railway transport has brought together rail organizations from throughout Europe in order to resolve a challenging problem of providing a framework for the international rail traffic management. This activity gave birth to a new specification called European Rail Traffic Management System (ERTMS). The goal of this standard is to provide the rules for the interoperability of trains within all European continent on one side and on the other side to guarantee the safety and increase the cost effectiveness of all trains by introducing a unique trackside and on-board equipment in all participating countries. Of course, all of these changes have to contribute to the competitiveness of European rail.

ERTMS presents a very interesting study field for research initiatives and can serve as a benchmark for different modeling and analysis methods. All fundamental documents are freely available in their complete versions. Their volume is limited to several hundred pages which makes it possible for a small team to be able to fully integrate its contents but still enough voluminous to require a very pragmatic and industrializable approach using existing software tools. The use of a number of different expression formalisms (description text, tables, UML-like diagrams, (timed) automata, etc.) within the ERTMS specification makes this study even more challenging.

For reasons stated above, we have tried to approach the ERTMS modeling with Colored Petri Nets such as implemented in the CPN-tools software (available at http://wiki.daimi.au.dk/cpntools). The objective was to test whether this tool makes it possible to handle the modeling of the complete specification composed of communication subsystems, operating procedures, functional modes and their transitions, safety requirements, etc. The second objective is to construct a model using a unique formalism for a further evolution of safety and/or performance criteria under different context situations (on-board or trackside failures, driver behavior influence, etc.).

Another advantage of CPN is the possibility of a fully compliant modeling of communication subsystems including frames for transmission, frame structures, data contained and transmission delays. As communication is a central issue in both ETCS and GSM-R, this can be considered as an important advantage.

In order to present our work, this paper continues with the section 2 presenting the ERTMS standard with focus to the ETCS procedures, functions and equipments. Section 3 offers a concise presentation of Petri nets and Colored Petri Nets. Section 4 gives an overview of bibliography of past works related to

the application of Petri Nets to ERTMS modeling and evaluation. Our actual modeling experience is presented in section 5.

2 ERTMS PRESENTATION

The European Rail Traffic Management System (ERTMS) is the international answer to long distance train circulations often going across country borders. It aims to develop a complete, modular generic and interoperable system of rail traffic management shared by all national operators. This system includes:

- Automatic Train Control (ATC) functions
- Traffic Regulation and Management functions

ERTMS is the frame project for this standardization process and is composed of:

- European Train Control System (ETCS): unified system for Automatic Train Control
- GSM for Railway (GSM-R): radio-transmission system derived from GSM but specific for Railway applications
- European Train Management Layer (ETML): a system for management of traffic, train and signalization
- Harmonization of European rail Rules for Operation of ERTMS (HEROE): a set of operational procedures

Before ERTMS, were coexisting in Europe 23 different signaling systems in 15 countries causing international trains to have several onboard equipments (for example 6 different onboard a Thalys train).

The objectives of ERTMS are:

- To ensure the interoperability of high-speed lines (first priority) and then conventional lines throughout Europe, taking into account both:
  - Technical interoperability: same interfaces between equipments, in particular unified communication standards
  - Operational interoperability: same interfaces between equipments and the driver (Man Machine Interface: MMI, Figure 1)
- Standardize railway control systems
- Provide a complete solution for railway traffic management
- Reduce equipment and operational costs
- Increase line capacities by saving time of system's switching and by running on moving block
- Enhance global railway safety

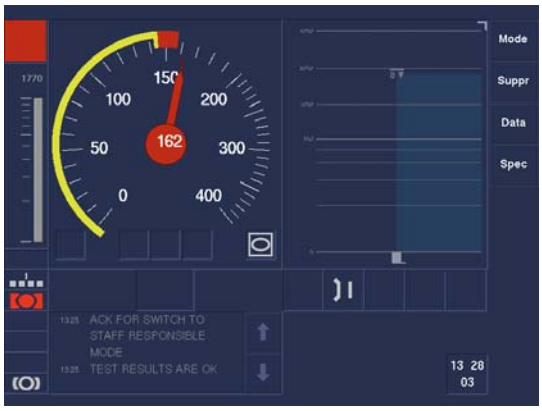

Figure 1. ERTMS Man Machine Interface.

ERTMS documentation is a set of European Directives, Technical Specifications for Interoperability (TSI), Functional Requirements Specifications (FRS) and System Requirements Specifications (SRS) fully available on the European Railway Agency (ERA) website (http://www.era.europa.eu)

The main ETCS functions are:

- Trackside equipments provide trains with "Movement Authorities" (speed settings to be respected at a specific track point), taking into account the positions of other trains, signals and switch point states as well as the physical line configuration (slopes, curves, etc.)
- Onboard equipments calculate a speed profile, taking into account the received movement authorities and the train characteristics (mass, length…). The speed limit as well as the current speed are displayed to the driver using a normalized interface (Figure 1), and are monitored by onboard equipments (Automatic Train Protection function with brake application in case of a speed excess).

ERTMS can operate in three levels (plus optional Level 0 and STM (Specific Transmission Module) Levels):

- Level 1 is designed to be compatible with national signaling systems, it provides an Automatic Train Protection functions using normalized balises (Eurobalises) and transmission loops (Euroloops)
- Level 2 provides cab signaling functions (lateral signals are not used) using GSM-R radio transmission to transmit movement authorities to trains. National train detection systems are still used.
- Level 3 provides a complete solution for train localization (calculated onboard using Eurobalises also and transmitted by radio to trackside equipments) transmission of movement authorities and ATP (Automatic Train Protection) functions. National train detection systems are no more useful and Level 3 can operate on a moving block. However a rigorous train integrity monitoring system must be put in place.

In order to guarantee the safety requirements compliance in all operation contexts, ERTMS specifies various train operation modes. Hereafter are the most important of them:

- Full Supervision (FS): is the "normal mode" providing a full protection against overspeed and overrun.
- On Sight (OS): is the mode used to run on an occupied block at limited speed. The driver has the full responsibility for the train maneuvers and safety
- Shunting (SH): is the mode used in situations other than normal circulations of trains along running lines (maneuver situations): vehicles in shunting mode can run without available train data
- Staff Responsible (SR): is used in some downgraded situation and at the beginning of missions. It allows running carefully at a limited speed.

ERTMS equipment architecture is represented on Figure 2.

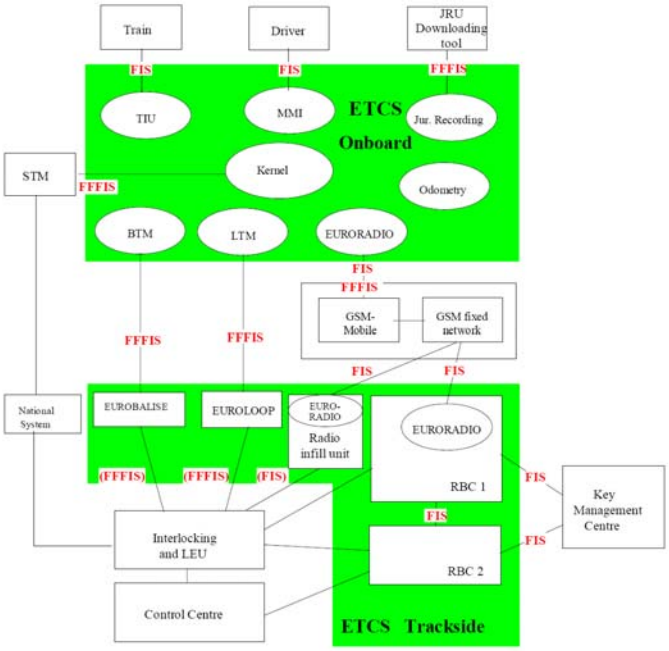

Figure 2. ERTMS equipment architecture.

The main equipments proposed in ERTMS can be separated in two groups: trackside and onboard. Their configuration determines the available ERTMS levels as described above.

The trackside equipments are:

- Eurobalises: transmission of fixed or variable data at a specific point of the line
- Lineside Equipment Unit (LEU) : calculates the variable data transmitted to the train by Eurobalises
- GSM-R: Radio Transmission System for Lineside / Onboard bidirectional communications.
- Radio Block Center (RBC): calculates the variable data (movement authorities…) transmitted to the train by radio.
- Euroloop or infill loop: A loop allowing a transmission of additional data not essential for safety but avoiding unnecessary delays (e.g. transmission at distance of a signal clearance).
- Radio infill: transmission of additional data by radio

The onboard equipments are:

- European Vital Computer (EVC) : implements the onboard ATP functions
- Transmission Modules (BTM, LTM, RTM, STM) for the transmission of respectively Balises, Loops, Radio and Specific (national system's) data to EVC)
- Train Interface Unit (TIU): Interface between EVC and the train
- Man (or Driver) Machine Interface (MMI or DMI): the interface between onboard equipments and the driver
- Odometry: speed measurements and distance / position calculation
- Juridical Recorder Unit: Records the mission data ("Black Box")

3 COLORED PETRI NETS

The Petri Nets are a powerful method to approach various kinds of discrete event systems. They allow expressing efficiently a variety of phenomena such as sequences, parallelism, synchronized start and stop, etc. They get the advantage to be able to be used both for the modelling of a static structure and the dynamic behaviour. They allow in this way to examine not only the system architecture but also its temporal evolution and reactions to stimuli. This makes them very suitable for the dependability, safety and performance evaluation. CPN can be employed throughout the complete process development cycle: one can thus preserve the same formalism to understand the architecture and the behaviour of the process (as well as the functional analysis). The driver model and various test scenarios can be also implemented in this formalism.

Although the Ordinary Petri Nets are a powerful modelling tool, many extensions and abbreviations exist. So for example Timed Petri Nets allow the incorporation of time attributes into the model. For modelling of various random phenomena Stochastic Petri Nets can be used. Colored Petri Nets (Jensen, K. 1997) allow the token differentiation due to the association of a color (value) with each token. They also give the possibility to model a system in which cooperate continuous-time variables and discrete events, which can occur on a stochastic basis. CPN allow thus to make the model more concise than the ordinary Petri Nets and also to include temporal and stochastic proprieties.

3.1 *Colored Petri Nets*

CPN belong to the group of high-level Petri nets. The relationship between CPN and ordinary Place/Transition Nets is analogous to the relationship between high–level programming languages and assembly code (Jensen, K. 1997).

Figure 3 shows an example of a CPN.

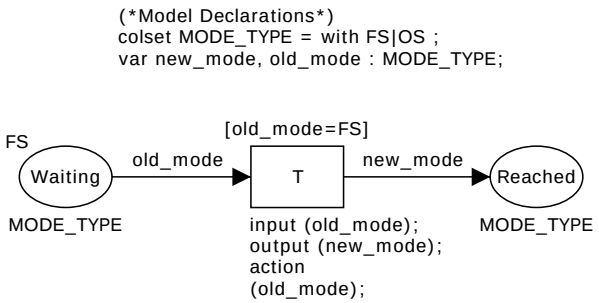

Figure 3. CPN example.

The presented model shows that each CPN model is composed of a net and a corresponding declaration section. Here, the declarations create an enumerated MODE_TYPE color which is used for the representation of the train functioning mode. On the figure one token FS is placed in the Waiting place of MODE_TYPE type. For the firing of T transition, this token will be attributed to the old_mode variable. The inscription above the transition is a guard function which allows the T firing only if it is evaluated as true. At the firing moment the code segment associated with the transition is executed. In this example it attributes the old_mode value to the new_mode variable.

Colored Petri Nets used in this example are modeled with the CPN-tools software which combines the power of CPN with the rigour of the ML programming language. This is a relatively new language which incorporates many modern programming-language ideas (Ullman, J. D. 1998). This is a strongly typed language based on declarative programming. Under certain conditions, mainly the language restriction, the CPN model can be considered as formal and be used directly or after an automatic transformation for certification proofs for example for safety and security criteria.

4 APPLICATIONS OF PETRI NETS TO ERMTS

4.1 *ETCS architecture modeling*

Meyer zu Hörste, M. & Schnieder, E. 1999. presents the global approach to be followed for the complete ERTMS going from the Functional Requirement Specification (FRS) through System Requirement Specification (SRS) down to the Architecture which then contains the functional code.

In order to deal with the model complexity a hierarchical approach is used defining 1.) Context, 2.) Process, 3.) Scenario and 4.) Function models.

The Context model is the most abstract level which interconnects the on-board and trackside interfaces through the air gap. The Process level specifies the general communication setup. The Scenario level is used to as a message generator. It sends messages both to the track and to the train. The function models are illustrated on the Movement Authority (MA) example.

This work makes clear of the use of Colored Petri Nets for such modeling but identifies the combinatorial explosion as the analysis problem. This is why, only a study of an isolated component procedure is presented. However a very interesting result in finding an ERMTS specification error is presented.

Lahlou, O. & El-Koursi, E. & Bon, Ph. & Yim, P. 2006. present CPN modeling of rules and requirements for the ERTMS specification. This work can be considered as a logical extension of the Meyer zu Hörste, M. & Schnieder, E. 1999. This paper draws a clear link between the specifications itself, CPN models, requirement management and proposes it as a possible approach for the certification procedure.

4.2 *Communication subsystem studies*

Petri Nets are also applied for the study of communication behavior of the ETCS. Many interesting papers can be found on the subject. Trowitzsch, J. & Zimmermann, A. 2006 can be an example for presentation of the transformation of an UML State Machine to Petri Nets in order to perform quantitative investigation of the ETCS communication subsystem. The detailed modeling examples of the communication procedure can be found in Zimmermann, A. & Hommel, G. 2005. This work also includes the modeling of failures which can occur in various phases of a transmission and a discussion of transmission delay influence is also included.

Kluge, O. 2003 completes the work on Petri net modeling in the rail traffic analysis with a detailed communication on the relationship of MSC (Message Sequence Charts) and Petri Nets applied to the safety management of railway level crossings.

5 ERTMS MODELING EXAMPLES

5.1 *Modeling of Mode transition table*

The Mode transition table is the fundamental part of Chapter 4 (Modes and transitions) of the SRS baseline 3. It presents all functioning modes the most important of which were presented in Section 2 of this paper.

The transition from one mode to the other is done according to a table whose extract is shown in Table 1.

Table 1. Extract from the Mode Transition table.

NP	<29 -p2-		<29 -p2-		<29 -p2-
4> -p2-	**SB**		<28 -p5-		<28 -p4-
		…			
	15> -p7-		**OS**		
				…	
			59> -p6-		**RV**

This table is to be read as follows. The transition from OS (On Sight) mode to the NP (Not Protected) mode is possible only if the condition number 29 is fulfilled. In cases where more conditions must be fulfilled at the same time, the priorities (e.g. -p1- represents the highest priority) give a clear solution on which transition should be done. A transition from one mode to the other is only possible if the corresponding field in the table is non empty.

The Mode transition table can easily be modeled with CPN. The model corresponding to Table 1 is shown on Figure 4. The train mode is expressed as a token present in the corresponding place (NP, SB, OS, RV). The token is present in the initial state in NP place. In this case for example, if the condition 4 is fulfilled then the train can switch to SB mode.

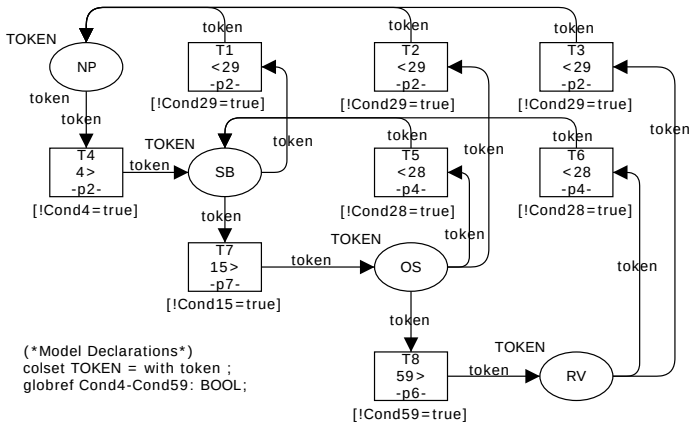

Figure 4. CPN model of the Mode Transition table.

After its construction, the stand-alone model is ready for its first analysis. The first information that can be obtained automatically from the CPN model is the possible reachability of one mode from another mode. For example the RV mode can only be reached from NP mode when traversing the SB and OS nodes with conditions 4, 15 and 59.

This information can be obtained automatically from the CPN model through the construction of an occurrence graph. Such graph contains all reachable states of the model from a given initial state. It can then be examined for a research of potentially parallel and concurrent paths from one state to the other. This information can be helpful for determining alternative operation procedures as well as for the detection of non determinism in the choice of possible paths. The occurrence graph for the presented model is shown on Figure 5.

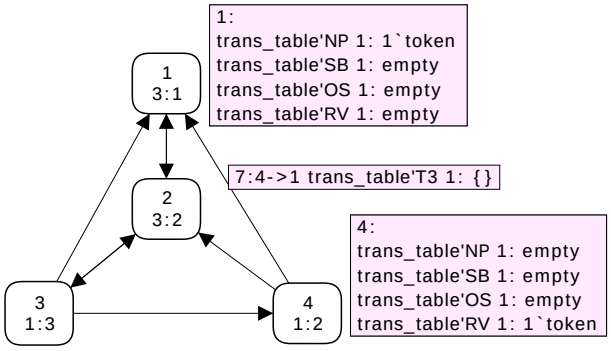

Figure 5. Occurrence graph of the CPN model.

The nodes of this graph represent train modes (e.g. node 1 stands for NP mode). Each node contains also its predecessors count (3 preceding states for node 1) and the successors count (1 succeeding states for node 1 and 2 successors for node 4). Each arc represents one transition firing (e.g. arc 7 represents the firing of T3 transition of the model). Such graph can of course be analyzed for blocking states, deadlock states, strongly connected components, etc. with the benefit of being more 'human-friendly' than the original Mode transition table.

The second information that can be obtained from the graph is an automatic priority management. Possible conflicts in transitions are, according to the specification, prevented by the table construction. The specification text contains a commentary that in case of the same priority levels, the associated conditions are mutually exclusive and cannot be true at the same time.

5.2 *Conditions modeling*

CPN propose different ways of representing conditions required for each transition. The standard and the most natural way, is to model each condition as a combination of input places for the given transition. The basic PN firing rule says that a transition can only be fired when each of its input places contains a 'valid' token. The advantage of this approach is that it keeps the model connected but the inconvenient is a graphical saturation and a decrease of model readability. For these reasons, this paper proposes the use of global references or variables to be used in the transition guard. The value of the global reference is determined in a separate part of the CPN model.

The condition for the transition between OS and RV modes can be taken as an example. Its number is 59 and it states: "(train is at standstill) and (driver has acknowledged the reversing)". The corresponding procedure can be found in §5.14 of the ERTMS/ETCS specification. It says that "*while the train is as standstill …, the driver shall be informed that reversing is possible. Upon the driver's intention to reverse, the on-board equipment shall ask the driver to acknowledge transition to RV mode. If positive, the on-board equipment shall switch to RV mode.*"

The condition 59 together with its procedure is represented on Figure 6.

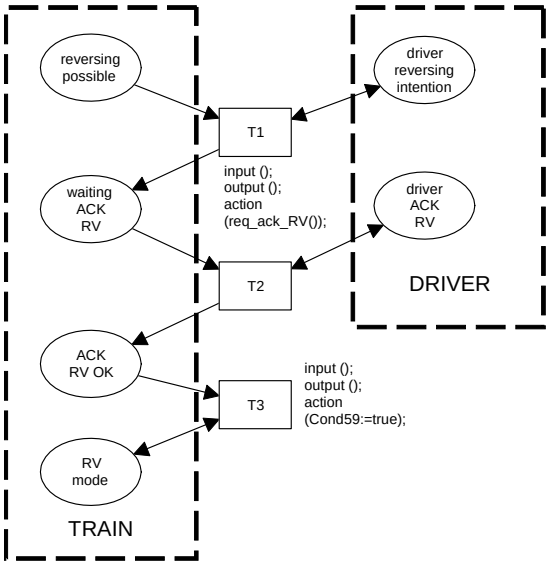

Figure 6. CPN model of the Train Reversing procedure.

The initial condition 59 value has to be set to FALSE.

This diagram shows a new aspect of the CPN model. It includes not only the automated procedures done either onboard or sidetrack but the model can include the driver model as well.

In the present model, the driver is only used as a precondition to certain transitions (T1 and T2). But CPN could be used for the modeling of human behavior. This is an interesting feature as it places the specification model in its context of use and allows the integration of human influence in safety and security analysis.

The conception of this model shows a certain number of questions which are not explicitly stated in the specification. One example is the treatment of the memory flag for the driver acknowledgement. There is a question whether the acknowledgement flag management. It can be reset after being used for the condition 59 set-up or its value can remain maintained for a certain time interval or even indefinitely. Answers to these questions were not found in the specification.

The two models given in this example cooperate and are closely linked. Thus the transition T8 from OS to RV mode shall not be possible unless the second model is executed which means that the driver needs to show his intention to reverse and then acknowledge the command. Of course, one of the advantages of such modeling is the automatic construction of paths in the model. And from paths can be derived the required preconditions on the driver behavior.

5.3 *Modeling of time constraints*

In the previous example, the time is not mentioned, meaning that the driver can acknowledge his intention at any moment. However in many other cases the reaction time is imposed. This can be found for example in the OS (On Sight), LS (Limited Supervision) or SH (Shunting) procedure where the driver has to acknowledge the imposed transition to OS mode from other modes. If he does so within 5 seconds from the acknowledgement request, the transition is considered valid. However if he fails to acknowledge in the given interval, service brake command is issued and can be only stopped by the drivers acknowledgement. This part of the procedure is shown on Figure 7.

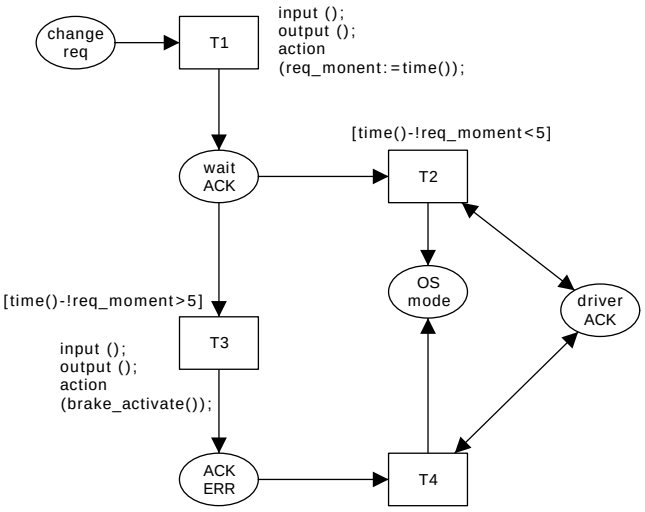

Figure 7. Timed CPN model.

This model uses global variable *req_moment* to memorize the date of the request occurrence. In this case, the request comes either from the train driver or from trackside equipment. This request has to be acknowledged within 5 seconds from its occurrence. This constraint is represented with a guard associated with transition T2. If the time limit overflows then the guard inhibits the T2 firing. In that case, T3 becomes valid for firing and is fired immediately. At the firing, the transition action code is executed and activates the braking function. According to the ETCS specification, the only way to continue in the procedure is to wait for the driver acknowledgement. No supplementary information is provided. So the

ACK_ERR has to be considered as a failure state and surveyed constantly.

6 CONCLUSION

This article presents a study concerning the modeling of ERTMS/ETCS. It is based on the publicly available ERTMS/ETCS baseline 3.

The chosen modeling approach is Colored Petri Nets as implemented in CPN tools. The model construction has confirmed the expressional power of CPN. All basic mechanisms and procedures can be modeled with sufficient level of detail and exactness. However some limits were identified. The most explicit one can be found in Subset-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2. This document gives very concrete values to be satisfied for safety assessments. These levels are standard SIL4 orders such as 10^{-11} dangerous failures/hour. Even though, these values can be integrated in the model, their in-depth analysis is harsh due to the lack of analytical calculus tools in the used software.

The main result of this work is a proposal for the approach on modeling of ERTMS/ETCS specification with a more formal tool. Such construction can be used later for analysis (and especially safety coherence verification) or for a future transformation to other formalisms. As it is more formal but still very readable and comprehensive, the model cans also serve for communication between various actors and the visual simulation can be used for educational purposes. The modeling process itself was highly inspiring and many questions and remarks were referenced. They could serve for potential future improvements in the specification documents.

As this is our first approach to ERTMS, the modeling work is still on-going. It is accompanied with a development of a new analysis method for diagnosability and safety assessment of models with the complexity of a complete specification. This method is based on a direct model backward reachability analysis. The goal is to provide a model with a method that proves that the model can never reach th accident state and is thus guaranteed safe and apt for the required certification level. The second perspective is to verify the feasibility of a CPN transformation to the standard safety evaluation approaches such as B method (Defossez, F. & Bon, P. & Collart-Dutilleul, S. 2008). This process is also useful for the future ERMTS equipment certification.

REFERENCES

Defossez, F. & Bon, P. & Collart-Dutilleul, S. 2008. Taking advantage of some complementary methods to meet critical system requirement specifications, *Computers in Railways XI*, ISBN 978-1-84564-126-9, Witpress: 153-161.

Jensen, K. 1997. Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use, Monographs in Theoretical Computer Science, *Springer Verlag*.

Kluge, O. 2003. Modelling a Railway Crossing with Message Sequence Charts and Petri Nets, *Petri Net Technology for Communication-Based Systems*, ISBN 978-3-540-20538-8: 197-218.

Lahlou, O. & El-Koursi, E. & Bon, Ph. & Yim, P. 2006. Evaluation des règles d'exploitation pour l'interopérabilité et la sécurité dans les transports ferroviaires, *Mosim'06*, Rabat, Maroco.

Meyer zu Hörste, M. & Schnieder, E. 1999. Formal modelling and simulation of train control systems using petri nets, *FM'99 — Formal Methods*, ISBN 978-3-540-66588-5.

Trowitzsch, J. & Zimmermann, A. 2006. Using UML state machines and petri nets for the quantitative investigation of ETCS, *Proceedings of the 1st international conference on Performance evaluation methodolgies and tools*, ACM International Conference Proceeding Series; Vol. 180.

Ullman, J. D. 1998. Elements of ML programming, ML97 Edition, Prentice Hall, 1998.

Zimmermann, A. & Hommel, G. 2005. Towards modeling and evaluation of ETCS real-time communication and operation. *Journal of Systems and Software* 77 (1): 47-54.