# High level Petri net modeling For railway safety critical scenarios

Zakaryae Boudi, El Miloudi El Koursi, Simon Collart-Dutilleul, Moha Khaddour

# High level Petri net modeling

# For railway safety critical scenarios

Boudi Zakaryae[1], El Koursi El Miloudi[1],

Collart-Simon Dutilleul[1], Khaddour Moha[2]

[1] French Institute of Science and Technology for Transport, Development, and Networks
IFSTTAR-COSYS-ESTAS
20, rue Elisée RECLUS BP 317, F-59666 Villeneuve d'Ascq Cedex
Zakaryae.boudi@gmail.com
{el-miloudi.el-koursi, simon.collart-dutilleul}@ifsttar.fr,
[2] National Office of Moroccan Railways – ONCF
khaddour@oncf.ma

**Abstract.** This paper presents a high level Petri net modeling methodology for railway systems safety critical scenarios. This methodology is based on modular high level Petri nets, including most relevant components of a railway safety system, as safety regulation procedures, interlocking and especially human factors, enabling more various gathering of information and allowing the study of diverse possibilities in a same global model. At first, this method was applied to the infrastructure and the regulation of the Moroccan Kenitra railway station. Afterward, a first approach of real accident scenario modeling was introduced for "Saint Romain en Gier" accident, taking account of human errors. Our goal is to bring formal tools in order to study weaknesses in shunting management within train stations and accidental scenarios, considering automatic mechanisms and human involvement.

## 1 Introduction

Signaling systems are heritage of railway history and may be multiple within the same country and from a country to another. In order to face this problem, a new control system "ERTMS/ETCS" (European Rail Traffic Management System/European Train Control System) is destined to become a common standard in Europe. For more complex areas, ground and other logical signaling rules defined within a national context such as the "pink instruction" (Consigne Rose) are used. They prevent any conflicting use of a given infrastructure.

Achieving railway interoperability allowed by ERTMS requires a common understanding of requirements by all involved parties. In this context a formal rigorous

model is an effective tool to identify and clarify ambiguities. The PERFECT project (Performing Enhanced Rail Formal Engineering Constraints Traceability) is a French scientific project that aims to formalize railway specifications and validate various systems. Systems Models will be developed and formally studied to determine, if possible, the compliance between ERTMS and National railway specifications [1].

In this context, railway safety research as the PERFECT project one is facing the complexity of real railway scenario modeling. In fact, railway safety systems are semi-automatic systems, including human manipulation, infrastructure requirements and automatic actions (interlocking, ERTMS control…), yet, it requests a full and comprehensive modeling, as expressed by so many researchers and operators [2]. One of the ultimate goals of this study is to bring a modular modeling methodology that is able to allow different experts and specialists of various fields to contribute independently in the scenario global model, especially for human factor.

## 2 High level Petri nets modeling methodology

Petri nets (PN) are a powerful tool for studying a wide variety of discrete event systems. They are useful for both static modeling thanks to their structure, and dynamic modeling through their operating rules. In this context some typical cases are modeled using the CPN-tools software platform. This software has been proposed by the PERFECT project, especially for its extensive use in the previous contribution works [3], especially in rail systems assessment [4, 5, 6 and 7].

However, the use of Petri nets until now does not cover all a complete railway system modeling needs. Indeed, railway system models should be used by a larger team of diverse railway abilities and skills. The present methodology focuses on creating modular high level Petri nets that separates safety stakeholders in a railway scenario and enables the introduce of human factor, which has an extremely important influence in railway operation. Those sub-models are then gathered using the hierarchical levels of Petri nets. In the following, this method application shows how a railway infrastructure, regulation, interlocking and human action can be represented by a modular approach for high level Petri nets.

## 3 Description of Kenitra railway switching station

Kenitra Station is a mainline station connecting this city that is located in the northern suburbs of the capital Rabat to other Moroccan cities through line trains and Rapid shuttles trains (TNR). It also receives and manages freight and work trains. The safety management on these routes for all traffic types is warranted through the PRS switching station [8]. But some movement cases are managed on the ground by safety agents.

PRS Station of KENITRA enables the control of 45 routes. The controls are handled by the security chief who is also responsible for trains' movement. Some moves require handling safety equipment on the ground via permissions.

The next sections will detail some modeling possibilities of railway station aspects considering the case of Kenitra station. Those models could be injected in larger railway scenarios models which take into account station features.

## 4 Modeling an interlocking aspect (a part of route formation)

This section will show the modeling of an interlocking aspect of the Kenitra station. The route formation is materialized by interlocking control of turnouts and, if appropriate, by the actuation of interlocking between routes in opposite directions. It forbids the formation of all incompatible routes and authorizations. In the model constructed (Fig. 1), as in [9, 10], three basic modes of transport are considered: the permanent plot (TP), automatic destruction (DA) and manual destruction or shunting routes which can't have AD. TP mode is used only on safe routes; therefore, whenever a route requests TP mode, it is necessary to verify that it is not prohibited by that mode. More detailed interlocking information and modeling are presented in [10, 11].

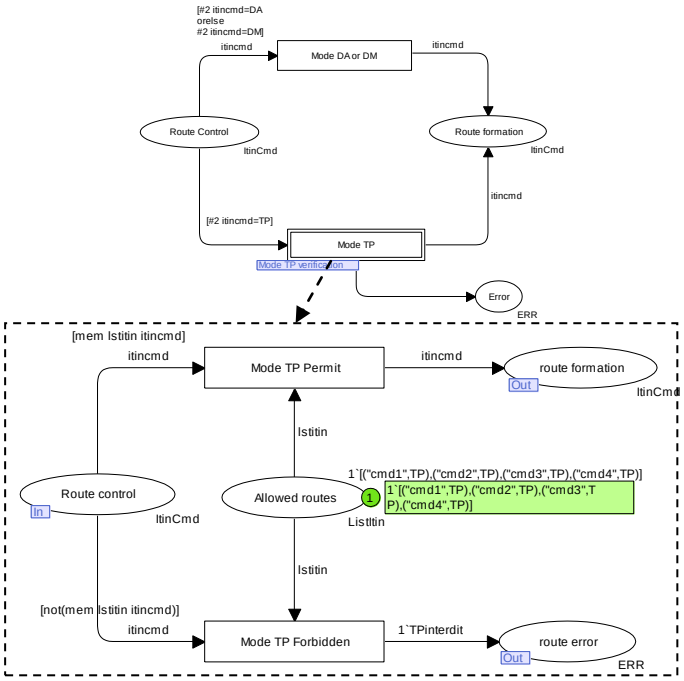


**Fig. 1.** Part of route formation

## 5 A representation of railway infrastructure and regulation (TS-RDS route of Kenitra station)

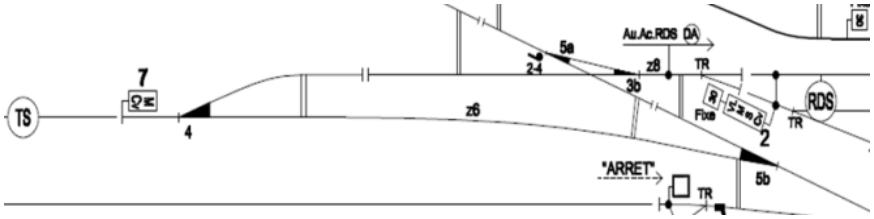


**Fig. 2.** Infrastructure to model

Still considering Kenitra station, and more specifically, the route “TS-RDS” (fig. 2) of the station, the present section describes the infrastructure and the regulation modeling in the scope of one global model. This model has three hierarchical levels. The first level represents the track section involved in the route (Fig. 3). In this study case, only the nominal direction movement is covered. The Petri net was composed by gathering elementary nets we had established for the infrastructure structures (zones, communication turnouts, signals…). This modular modeling method is one very interesting point in this work.

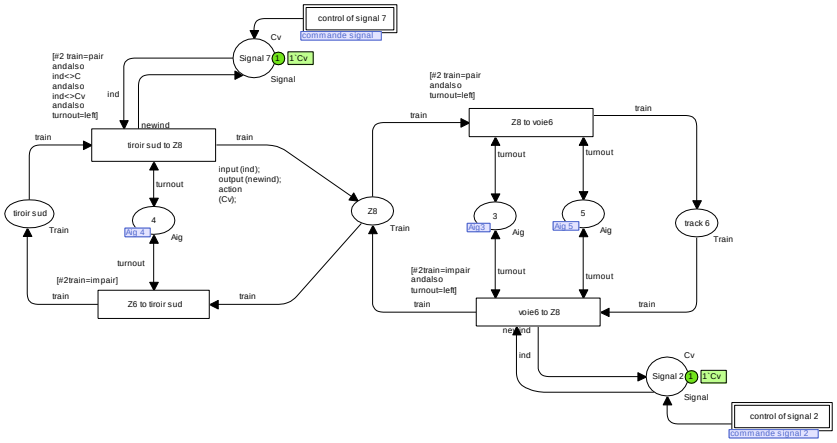


**Fig. 3.** First hierarchical level model

The traffic movement is allowed by the opening of the "signal 7". The second hierarchical level details the control of this signal. To simplify the modeling, certain open-

ing signal conditions have been shown in a simplified manner. This is the case of authorizations (Fig. 4). Turnouts control processes are modeled in the third level.

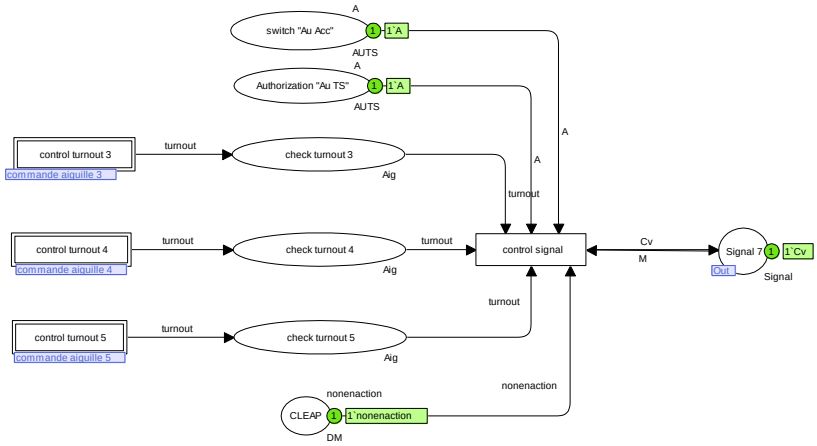


**Fig. 4.** Second hierarchical level model

## 6 Railway safety critical scenario modeling

As an important part of this work, real railway scenario modeling was studied. The concerned modeling methodology was applied to the case of the collision between a work train and a TGV in Saint Romain en Gier accident.

### 6.1 Circumstances and scenario of Saint Romain en Gier accident

The railway line from Lyon to Saint-Étienne is a double-track line, equipped with permanent installations of opposite direction (Installations Permanentes de Contre Sens-IPCS) between Terre Noire and Givors [12]. IPCS are specific signaling compounds that enable trains movement in the reverse direction. The line is regulated, rail traffic being subject to supervision by a regulator. Figure 5 shows the involved railway infrastructure.

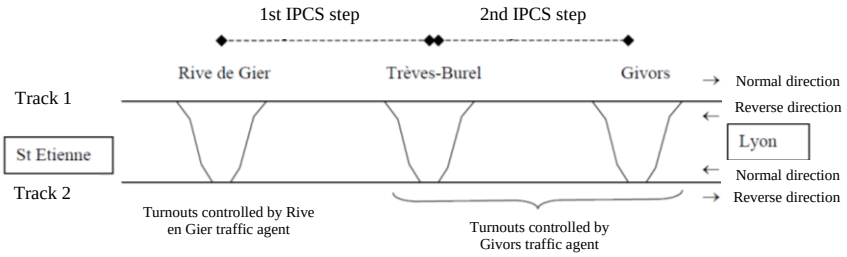


**Fig. 5.** Saint Romain en Gier accident infrastructure

Works are organized on infrastructure in the area Rive en Gier / Givors, both on the tracks 1 and 2. The Command Post of Lyon announces a circulation from Lyon to Saint -Étienne. The traffic agent of Givors city established route for engaging the TGV from its normal route within track 2 to Rive de Gier, and to Saint -Étienne. After crossing Givors city station, the TGV collides against the work train oncoming this track 2 to regain Givors station [8].

### 6.2 High level Petri nets Scenario Modeling

At first, we have modeled the scenario's related infrastructure, linking Givors and Rive en Gier railway stations. Fig. 6 presents this first level global infrastructure model. The stations are represented with places. Movements between these stations are covered by transitions in the model. The transition "TB -> Givors" is one that includes movements leading to the accident and will be detailed in another hierarchical level.

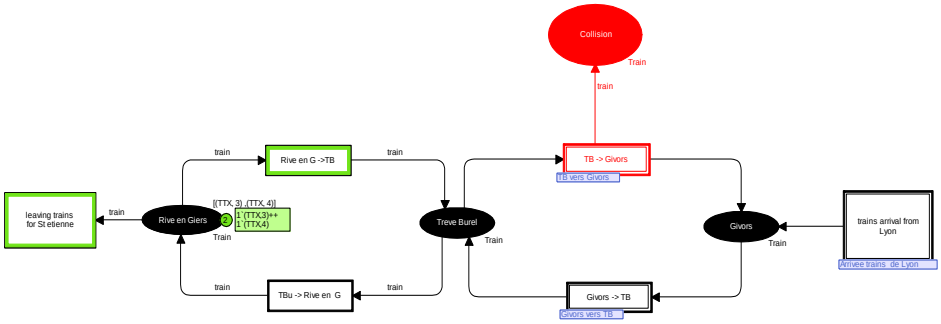


**Fig. 6.** Saint Romain en Gier accident infrastructure model

In this section, more detailed modeling of the infrastructure associated to the accident is presented, along with the work train "TTX 4" modeling of movements that led to the collision. Figure 7 shows the model of the accidental movement. The areas are modeled with places as well as signals. Here are introduced two types of transitions to

represent the movement of the work train between two areas. One type denoting the "regulatory crossing" signal and a second type for the "illegal crossing".

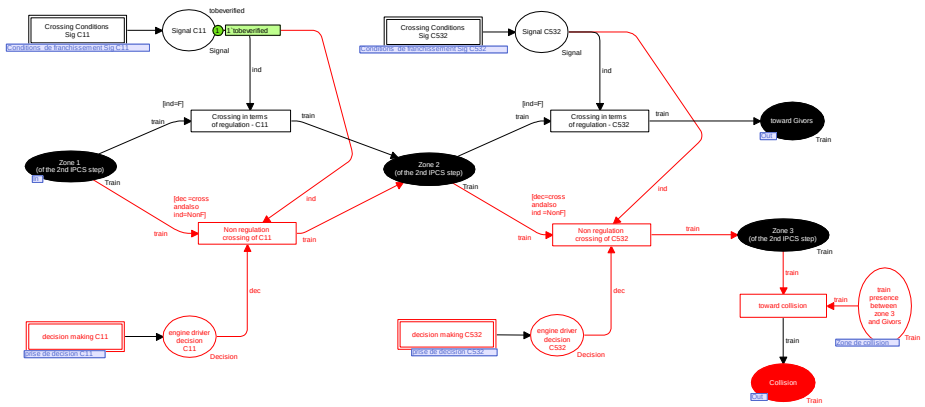


**Fig. 7.** Model of movements that led to the collision

At this point, the sub-model of regulatory crossing conditions of an intermediate signal in the intercepted track is shown. This modeling will visualize the Regulation abuse residing in the not allowed crossing of a signal that we have identified as a direct cause of the accident. Figure 8 illustrates this model for the case of the square signal C11, presented in another hierarchical level of the Petri net. Two main conditions determine the feasibility of such a signal crossing, namely, the establishment of direction in IPCS and bulletin I's authorization or the traffic agent's one. The two mentioned conditions are modeled with places.

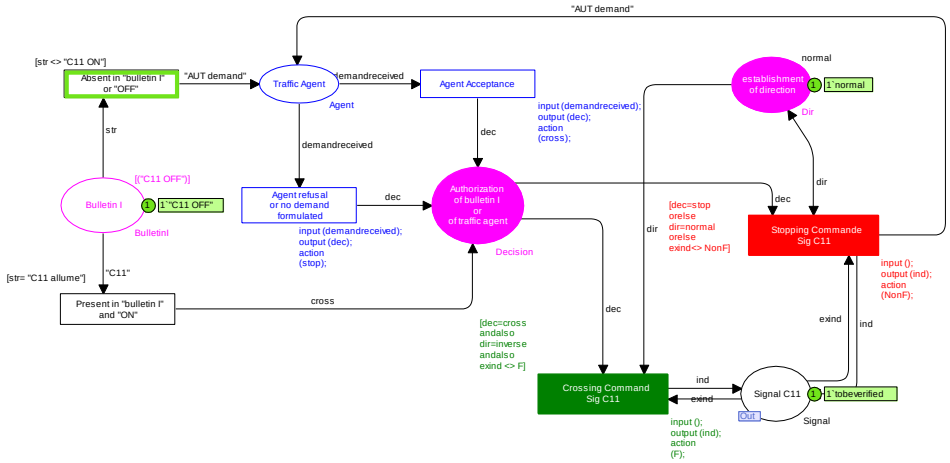


**Fig. 8.** Crossing a signal in terms of regulation

The next sub-model describes the behavior of the three driving agents of the work train towards the intermediate signal. The reaction of each agent is modeled with a place, and decision making in a transition. If no reaction is to point out, as in the real case of accident Saint Romain en Gier, the transition "decision crossing C11" will be validated (Fig. 9 - case of square C11).

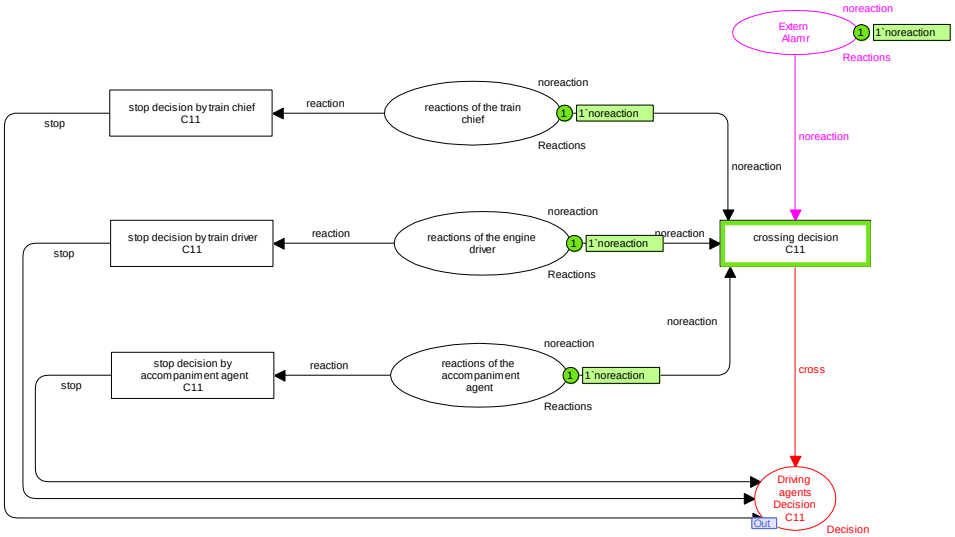


**Fig. 9.** Driving agents' decision making

## Conclusion and Perspectives

Under the PERFECT project (Performing Enhanced Rail Formal Engineering Constraints Traceability), a similar study to the one proposed on the French LGV-EST railway line is conducted on Kenitra railway station, being part of the future Moroccan high speed railway line linking Tangier and Casablanca within ETCS level 2. This is what makes this study a first interesting international perspective of this project.

In this respect, a modular approach for colored Petri net modeling was introduced for railway infrastructure and scenarios involving human decision, particularly accident scenario in order to provide formal tools both for checking railway rules consistency and accident analysis. This study enables more complete analysis of railway complex situations by creating the possibility of integrating all railway aspects, which could be modeled separately, in one global model. Therefore, this methodology is responding to the needs of railway researchers, experts and operators so that they could work together a complementary way.

## References


1. Bon, P., Collart-Dutilleul, S., Sun, P. (2013b): Study of implementation of ERTMS with respect to French national rules using a B centred methodology, International Conference on Industrial Engineering and Systems Management IESM'2013 October 28 - October 30 Rabat – Morocco.
2. Belmonte, F., Schon, W., Heurley, L., Capel, R.: Interdisciplinary safety analysis of complex socio technological systems based on the functional resonance accident model: An application to railway traffic supervision. Reliability Engineering and System Safety, num. 96, pp. 237-249, February, 2011
3. Jensen, K., Kristensen, L., M., Wells, L.: Colored Petri Nets and CPN Tools for modelling and validation of concurrent systems", Published online: 13 March 2007, Springer-Verlag 2007
4. Jensen, K.: Coloured Petri Nets - Basic Concepts, Analysis Methods and Practical Use, Vol. 1". Springer-Verlag, Berlin, 1992.
5. Lalouette, J., Brinzei, N., Malassé, O.: Evaluation des performances du système de signalisation ferroviaire européen superpose au système français, en présence de défaillances», Congrès Lambda- Mu 17, La Rochelle, Octobre 2010.
6. Ingrid, C., Y. : A Layered Approach to Automatic Construction of Large Scale Petri Nets Modelling Railway Systems. Thesis, University of Oslo, Department of Informatics, Cand. Scient., 25 august, 2004.
7. Lalouette, J., Brinzei, N., Malasse, O., Caron, R., Scherb, F., Aubry, J-F. : Modeling and performance assessment of a railway signaling system integrating ETCS and BAL using colored Petri nets (Modélisation et évaluation des performances d'un système de signalisation ferroviaire intégrant BAL et ETCS par réseaux de Petri colorés). Version 1, Sixth International French Conference of Automatic, CIFA 2010, Nancy, France, 2010.
8. ONCF Pink Instruction - signaling plans of Kenitra station – CG S6A n°8. : Poste tout relais à transit souple PRS", November 2000.
9. Collart-Dutilleul Simon, Lemaire Etienne, Livrable D11: Performing Enhanced Rail Formal Engineering Constraints Traceability" PROGRAMME ANR-TdM 2012, IFSTTAR, 2013.
10. Antoni, M.: Formal validation method for computerized railway interlocking systems. In Computers Industrial Engineering, 2009. CIE 2009. International Conference on, pages 1532–1541, 2009.
11. Sun, P., Collart-Dutilleul, S., Bon, P.: Formal modeling methodology of French railway interlocking system via HCPN, 2014
12. BEATT.: Rapport d'enquête technique sur l'accident ferroviaire du 5 avril 2004 à Saint-Romain-en-Gier. http://www.bea-tt.developpement-durable.gouv.fr/saint-romain-en-gier-r21.html. November 2004.