A formal modeling methodology of the French railway interlocking system via HCPN

P. Sun, S. Collart-Dutilleul & P. Bon
Université Nord de France and IFSTTAR/COSYS-ESTAS, France

Abstract

A railway interlocking system (RIS) plays a vital role in the safe transportation of a railway system. It is responsible for the safe routes of trains making sure that each train movement follows the other in a proper and safe sequence. Detailed verifications and evaluations are mandatory before deploying an RIS, since it is a safety critical system (SCS). But the increasing complexity of the RIS tends to limit the capability of the classic approval methods. As a result, the formalization of RIS becomes important to both the development of computer interlocking software and the third-party testing of the RIS facilities. Petri nets are a powerful formal tool that have been applied to many railway applications. Considering the large scale and the space complexity of interlocking systems, this paper introduces a feasible method for modeling the RIS by hierarchical colored Petri net (HCPN), which aim at providing a formal verification and logic evaluation of the French RIS. The paper describes how the signaling control logical and the railway road layout are specified and constructed into the HCPN. First, the architecture of RIS and the hierarchical structure of the model framework are introduced. Then, several basic RIS components are established as Petri nets to illustrate how to map RIS components into HCPN. As a case study, a section of a typical French station is modeled. It includes interlocking routes and signaling control principles. This paper takes place in the framework of the ANR project 'PERFECT'. As this method has already received recognition from French railway experts, the future research contains consistency checking with some other parts of the specification, such as operation rules, which allows us to find out the crux of some existing problems and to discover some potential safety hazards.

Keywords: railway interlocking system, modeling methodology, hierarchical colored Petri net.

WIT Transactions on The Built Environment, Vol 135, © 2014 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR140711

1 Introduction

To achieve interoperability throughout Europe's railways, the European Union provides a solution 'European rail traffic management system (ERTMS)' to create a seamless railway system. It ensures trains of different countries running through any other European countries without facing technical problems related to signaling.

Although the ERTMS has the advantage in cross-border competition, it is impossible to update all of the existing signaling systems into a new one. Moreover, a large number of non-border-crossing trains are not in urgent need of being equipped with ERTMS. Therefore, a 'mixed' solution is provided, as a type of ERTMS implementation, where ERTMS and local standards coexist. There are some critical aspects and many detailed application decisions that will have an impact on the railway network once the system is in service [1]. One of the main factors is the interlocking system which is pertaining to each country and not included in the ERTMS specifications.

An RIS is a set of associated devices, in accordance with particular interlocking principles, for the establishment of safe routes through a railway yard. RIS is one of the crucial parts of the railway system. It provides trains with safe routes, which guarantee that no train can be driven into a route occupied by another. At present, a large proportion of the practical applications in the railway system are still in the interlocking systems based on computer-controlled relays. They have the advantages of reduced dependence on human operators and rapid capacity for self-checking, but the complex sequences of checks and consequent actions makes RIS a large concurrent system, a system that has a potentially complex global behavior. Thus, detailed verifications and validations are essential before any changes are put into service.

The current signaling system and its RIS work well and have withstood the test of time. Before applying the new ERTMS system to an exiting railway line, a safety assessment must be done in order to prove safety equivalence between the former system and the new one. As a primary step, the formal modelisation of RIS is needed as a fundamental part of this task.

In this paper, we mainly investigate our experience of modeling of RIS by colored Petri net (CPN). This research coming from the French national project, named 'Performing Enhanced Railway Formal Engineering Constraints Traceability (PERFECT)', was launched by IFSTTAR. It aims at providing methodological tools for a comprehensive assessment for the consistency of the specifications and operating rules regarding safety requirements.

This paper is organized as follows: Section 2 gives a preliminary introduction of RIS; Section 3 first presents the architecture of RIS hierarchical structure of the model framework, then illustrates how to map the RIS components into CPN models, including interlocking routes and signaling control principles; as a case study, a section of a typical French station is modeled in Section 4.

2 Preliminary requirement

2.1 Interlocking system

In railway signaling, an interlocking system is an arrangement of signal apparatus that prevent conflicting movements through an arrangement of tracks such as junctions or crossings. Interlocking is generally considered as having two meanings [2]: first, ‘an interlocking’ is the interlocking plant where points and signals are interconnected in a way that each movement follows the other in a proper and safe sequence; second, the principles to achieve a safe interconnection between points and signals are also generally called ‘interlocking’.

To fulfill the safety principles, the simplest but most important rule is that each train runs in own route. The route for a train to pass through is called “Signal Route”, usually guarded by mechanical, electrical and computer systems. There are interactions between paths, but no overlaps; the absolute separation of each route is a basic condition for the safety of railway traffic. A signal route must meet the following conditions:

- all points must be set properly and locked;
- conflicting routes must be locked;
- the track must be clear.

A complete RIS consists of three essential elements: geographical route, signaling control and train.

The *geographical route* includes track sections, turnouts, signal lights, and other signal devices, such as the track circuit, KVB (French automatic block light control system), and BAL (balise speed control system). These signal devices could work automatically without help from a train controlling center, so they are classified in the category of geographical route.

Signaling control is a set of operating rules and control procedures of an interlocking system. It comprises computer automatic control and manual control. Normally, the computer processes are responsible for most of the device-oriented operations, such as route establishment, route auto-destruction, etc. while human despatchers deal with decision-making, such as route selection, mode selection, manual destruction, etc., and some non-regular operations, such as shunting operations.

The *train* runs on interlocking routes and are supervised by both route conditions and operating instructions.

These three elements proposed will be the top level in the hierarchical model structure (fig. 1). In the present architecture, trains communicate with signal control layers and interact with geographical route layers. The signal control layer directly controls the turnouts and signal lights according to its operating principles.

2.2 Colored Petri net

The Petri net is a powerful method to approach various kinds of discrete event systems. It has the advantage that it can be used both for modeling of a static

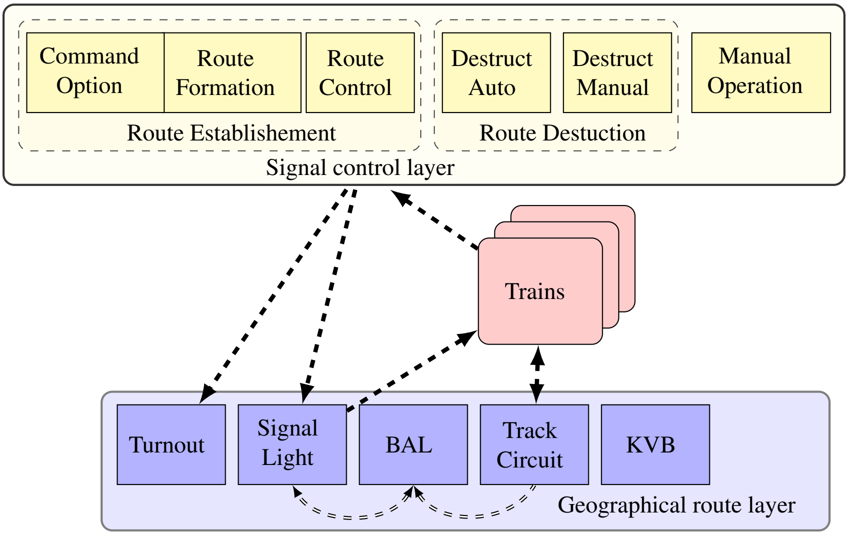
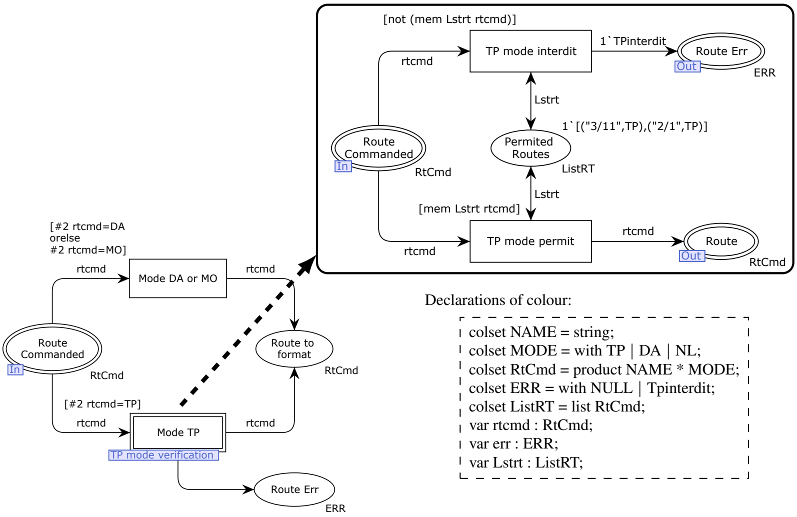


Figure 1: Top-level of interlocking system.

structure and the dynamic behavior. In the paper, the hierarchical colored Petri net is used [3], which is a backward compatible extension of Petri net. Its ‘colored’ property allows the token differentiation due to the association of a color (value) with it, and the value of a token can be manipulated and tested with ‘meta language’ in arcs, transitions and guards. Another ‘hierarchical’ property allows multiple levels in one model, where a low-level CPN module can be abstracted as a substituted transition in the high level. These two properties allow it to be feasible and convenient when applied to a large-scale system.

In addition, CPN have been widely accepted by railway researchers and engineers. There are already plenty of studies done in ERTMS based on CPN. Those works give sufficient background knowledge of applying Petri nets to the complex signaling system and ERTMS requirements to collaborate with in the future work. Meanwhile, the French National Railway Company (SNCF) is interested in the CPN as a formal tool in scientific research [4, 5]. French computerized RIS is also formally validated by CPN-based tools [6, 7].

The CPN model shown in Figure 2 is an example of a HCPN model. The model on the left is one of the initial steps of the interlocking route establishment. The model in the right is a substituted transition of ‘mode TP’. In this paper, three types of train movements are considered: trance permanent (TP), destruction automatic (DA) and maintenance operation (MO). TP mode is only available in certain routes, so each route command based on TP mode should be checked before its formation process.



Declarations of colour:

```
colset NAME = string;
colset MODE = with TP | DA | NL;
colset RtCmd = product NAME * MODE;
colset ERR = with NULL | Tpinterdit;
colset ListRT = list RtCmd;
var rtcmd : RtCmd;
var err : ERR;
var Lstrt : ListRT;
```

Figure 2: HCPN example (TP mode verification).

3 Modeling approach

3.1 Model framework

The hierarchy of our HCPN model framework is described in Figure 3.

The *Top level* of RIS is already mentioned in Section 2.1, which involves all of the function modules and the connections between them. It is possible (not obligatory) to substitute the transitions with other CPN nets that are models of each function component. The second level is the *Function level*, where the internal working procedure and principle of functions are mainly described. The *Decomposition level* is the function divisions and decompositions of the upper level, and consists of several *Detail level* Petri nets. The *Detail level* is an implementation of each particular action, and could be further decomposed, which depends on the complexity of the functions. The *Elementary* and *PrePost-procedure* levels are supplementary levels. The elementary net is used to change initial global conditions of the system. Pre/post-procedure net is the I/Os of the model structure, while pre-procedure is for inputting data or instructions from

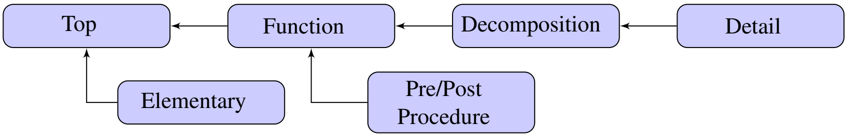


Figure 3: Generic structure of interlocking system.

third-part models or certain input sources, and post-procedure is for outputting data and results.

As the RIS is a complex system, a lot of features are closely combined. Some resources or statuses will be shared or accessed by several function nets or component nets. We have two methods to deal with such a situation:

(i) sharing a whole module by declaring all local places as fusion places in the shared net, which will effectively synchronize all its instances;

(ii) sharing a single place by storing sufficient information a fusion place, and implementing with calling and returning of functional block.

3.2 Mapping interlocking component to HCPN

The modeling principles are illustrated by two types of function components: the signaling control and the track layout.

3.2.1 Mapping signaling control

A signaling component is a sequence of commands and actions, similar to a working flow chart with determining, selecting, loops and execution of specific instructions. Figure 4 illustrates a part of the RIS route establishment, including command and formation processes.

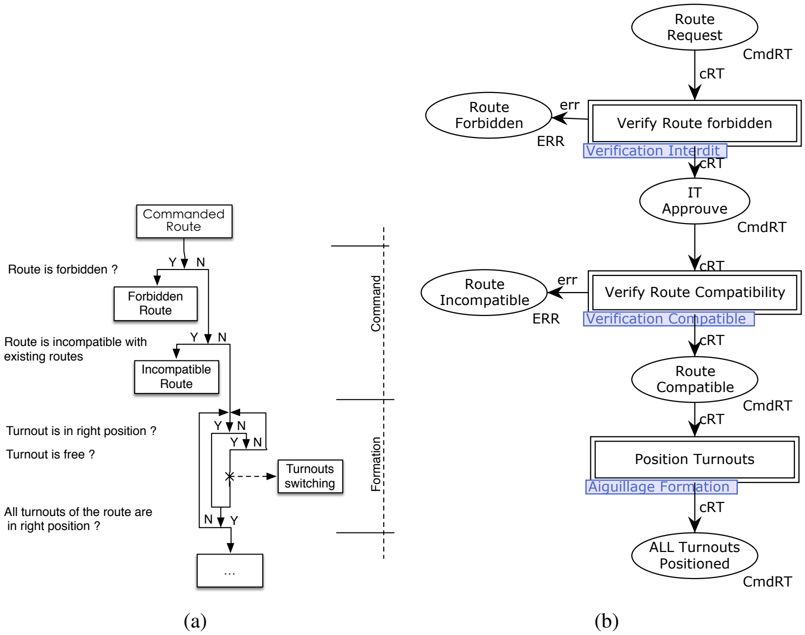
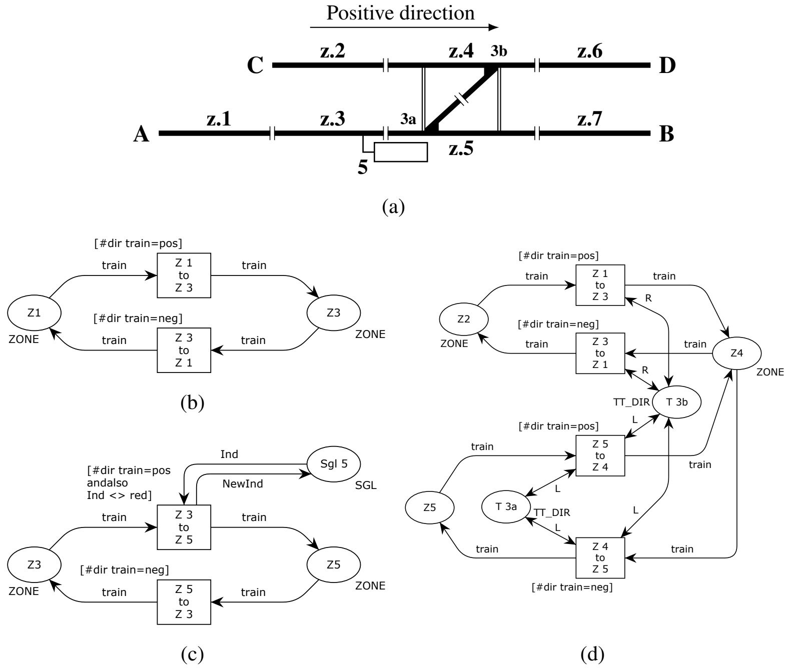


Figure 4: Example of mapping signaling control: (a) control flow chart; (b) corresponding HCPN model.

Figure 4(a) is the control flow chart. It receives the route commands, and checks whether those commands are feasible and compatible with existing ones. Then it will format the route according to the formation information stored in the model, such as the positions of turnouts. Figure 4(b) shows the corresponding model of route establishment. In this model, the determination nodes are considered as the decomposition nets containing further functions. It can ensure a clear structure corresponding with the flow chart.

3.2.2 Mapping track layout

A track layout is made up of track segments, turnouts and trackside signal lights. A track segment is a section of rail, which contains a complete track circuit. It is a simple straight or Y-shape with a turnout (3a, 3b in Figure 5(a)). A turnout is equipped with a moveable point. It allows trains to run on either side of the track, when facing the point. In general, an interlocking system is within a station yard, where the train runs at low speed, so train movement are partly directed by fixed signal lights installed along the rail. Signal lights mainly use 3 aspects: red (stop), yellow (approach, prepared to stop at next signal), green (clear).



(a)

(b)

(c)

(d)

Figure 5: Example of mapping track section: (a) track example; (b) movement between zone 1 and zone 3; (c) movement between zone 3 and zone 5; (d) movement at turnout 3a and 3b.

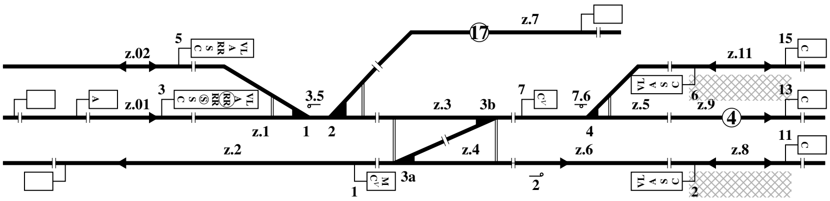


Figure 6: Case study of a typical station.

The model in fig. 5(b) shows a pair of train movements between zone 1 and zone 3, depending on the direction of the train. Here, the direction from left to right is defined as the *positive direction*. The movement from zone 3 to zone 5 is controlled by signal light 5 in fig. 5(c). As a necessary condition, unless the signal indicator is not ‘red’, trains cannot run through. Figure 5(d) is a turnout section, where the turnout direction is a constraint for all of the related train movements. Only one direction is available at one time.

4 Case study

In this section, a case of a typical station is brought in, from the book ‘French railway signalization’ [8] in fig. 6. This case is only a half-station, including 5 turnouts, 6 effective signal lights, 12 track segments, and 13 complete interlocking routes. The case has been chosen as an academic benchmark by experts involved with the PERFECT project [9].

The whole HCPN model is made up of 21 Petri nets. It can perform basic functions of an RIS by automatically arranging the routes according to different train commands, blocking the inverse path and signal light when a route is established, and enabling the route destruction function after a train passes through. The whole model is significantly large for a detailed demonstration, so only two examples are illustrated here. All of the other nets are modeled by the previous methodology.

The model in fig. 7 is a ‘decomposition component’ of the route establishment function. It opens the corresponding signal lights, by changing their indicators into green or yellow. The arc inscription ‘SepPack’ is used to extract the signal light commands from the static list and to assemble them into single signal tokens.

The route layout in fig. 8 presents all of the track connections and the functions of the station. There are four substitution transitions with the name of ‘. . . on DA’ are the ‘detail components’ for *Destruction Automatic*, which can destroy the route formations automatically after a train passes through a certain track segment. It is a basic function of the ‘flexible transit’ in the French railway system.

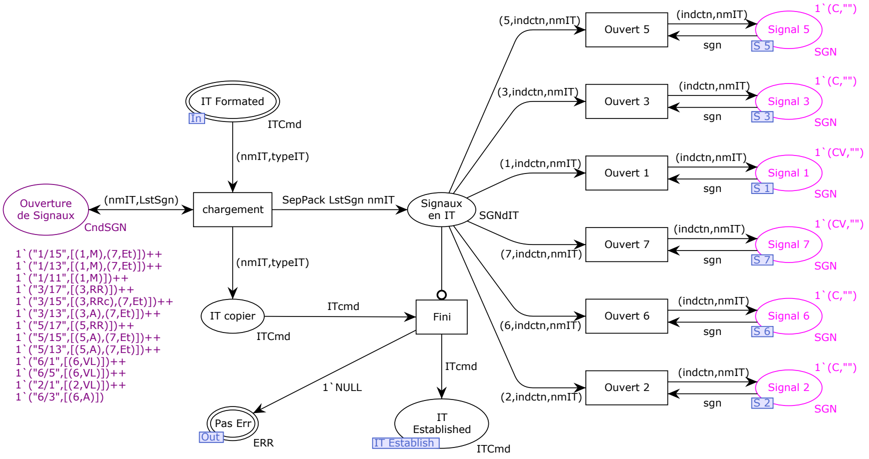


Figure 7: Case study example 1: open signal.

5 Conclusion

The goal of our research is to present a formal specification methodology for RIS. This work is achieved by the hierarchical colored Petri net. Its hierarchical and color features make it possible to propose a generic and compact structure which contains all high-level functions of RIS. The rigorous semantics of Petri nets could be applied for formal proofs in further research. This paper first introduces the architecture of RIS and the hierarchical structure of the model framework. Afterwards, two illustrations of mapping RIS components into HCPN specifications have been presented. As a case study, a particular station is modeled including track layout, basic signal control principles, and procedures.

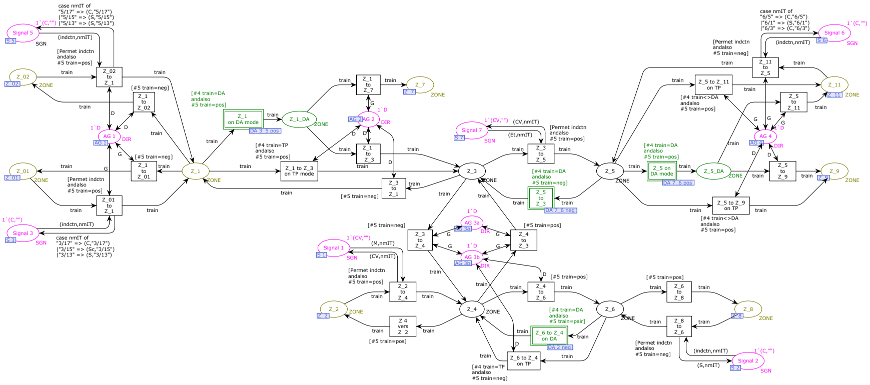


Figure 8: Case study example 2: route layout.

This research work is proceeding. While we still have to consider different scheduling modes, more complex or particular scenarios, the next step will consider with following works: integrating input interfaces of human influences, considering Time factors, and doing research into a more universal structure/form of models.

Acknowledgement

This research is funded by the PERFECT project (ANR-12-VPTT-0010).

References

[1] Murphy, E., The application of ertms/etcs systems. *Proc., Institution of Railway Signal Engineers (IRSE) Australasia Technical Meeting*, 2007.

[2] Pachl, J., *Railway operation and control*. VTD Rail Publishing, 2002.

[3] Jensen, K., Kristensen, L.M. & Wells, L., Coloured petri nets and cpn tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer*, **9(3-4)**, pp. 213–254, 2007.

[4] Lalouette, J., Caron, R., Scherb, F., Brinzei, N., Aubry, J.F., Malassé, O. et al., Evaluation des performances du système de signalisation ferroviaire européen superpose au système français, en présence de défaillances performance assessment of European railway signalling system superposed of the French system in the presence of failures. *17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2010*, 2010.

[5] Buchheit, G., Malassé, O., Brinzei, N., Lalouette, J., Walter, M. et al., Évaluation des performances d'un axe ferroviaire en fonction des caractéristiques fiabilistes de ses systèmes de signalisations. *9ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita'2011*, 2011.

[6] Antoni, M. & Ammad, N., Formal validation method and tools for French computerized railway interlocking systems. *Railway Condition Monitoring, 2008 4th IET International Conference on*, pp. 1–10, 2008.

[7] Antoni, M., Formal validation method for computerized railway interlocking systems. *Computers Industrial Engineering, 2009. CIE 2009. International Conference on*, pp. 1532–1541, 2009.

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

[9] Collart-Dutilleul, S., Bon, P., El Koursi, E. & Lemaire, É., Study of the implementation of ertms with respect to French national 'non on board rules' using a collaborative methodology based on formal methods and simulation. *Proc. Transport Research Arena 2014*, Paris, France, TRA'2014, 2014. To be published.