Formalisation and simulation of operating rules using coloured Petri nets

O. Lahlou[1], P. Bon[1] & L. Allain[2]
[1]*INRETS, Villeneuve d'Ascq, France*
[2]*ISEN, Lille Cedex, France*

Abstract

The operational rules safety assessment of rail systems is a key element of the rail success to improve the competitiveness. In this context, the goal of this paper is to present a process for a safety analysis of operating rules. The first step of this process describes the operating rules and their formalisation using coloured Petri nets by means of a systematic method. The second step concerns the simulation of the resulting nets to check their properties.

A group of ERTMS (European Rail Traffic Management System) operating rules, stemmed from HEROE (Harmonization of European rail Rules for Operating) project concerning the departure of a train will be used as an example. These rules are "Departure", "Train preparation", "Permission of train movement authority" and "Written orders".

Starting with a reminder of our systematic method of description based on coloured Petri nets (CPN), we show that the main advantage of this method is to standardize the rules description.

Then, the properties of the resulting Petri nets are checked with appropriate tools, with a view to verifying liveness and to detecting possible deadlocks.

Finally, we think that the process of formalisation and simulation will allow to check the consistency and the integrity of operating rules.

1 Introduction

From the perspective to harmonize the European railway system, ERTMS (European Rail Traffic Management System) [1], which is the new European standard for train control systems, has been developed and must be implemented for upgrades of high-speed and conventional lines in accordance to the European Commission laws.

WIT Transactions on The Built Environment, Vol 88, © 2006 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR060341

In this way of harmonization, operating rules have an important role. Indeed, common operating rules in European railway will allow interoperability without constraint like knowledge of full regulations of each country for the driver or the presence of all country control systems on board the train.

Operating rules are regulations that drivers, railway staff and signalmen must apply to guarantee safety railway traffic. They define what must be done (or not) and the conditions to be applied.

Our aim in this paper is to present an approach for the verification of operating rules by the use of formal methods. Our case study depends on a group of ERTMS operating rules, stemmed from HEROE (Harmonization of European rail Rules for Operating project) [2], concerning the departure of a train. The first step of this approach describes the operating rules and their formalisation using coloured Petri nets (CPN) by means of a systematic method. The second step concerns the analysis of the resulting nets by means of simulation (which is equivalent to program execution and program debugging) or by means of more formal analysis methods to check the operating rules properties.

2 Context and problematic

Each country owns its operating rules. This implies that the traffic of trains between those countries is very difficult. To overcome this problem, common operating rules for the whole European railway network are the solution to allow a safety interoperability.

In this way, the HEROE project was launched in 1998 with the main objectives of harmonizing and assessing rules and regulations for the new ERTMS control-command system in normal and degraded modes. These common rules are mandatory upon all national railways undertaking using ERTMS. They will have to incorporate these rules, as applicable, within their national rules of operation.

The assessment approach developed during the HEROE project is based on the qualitative and quantitative analyses of ERTMS operating rules by using a common operational diagram to represent each rule.

The former analysis named qualitative assessment, checks that the safety will be fully effective if the rules are applied. The latter performs the quantitative analysis focused on the rules identified by the former as very critical. In fact, the quantitative assessment consists in evaluating the probability that the operators made errors in applying the rules (due to their complexity or for human errors) and evaluating the relevant consequences from the safety viewpoint.

This work identified some problems of inconsistency and incoherence, so it recommended to refine some rules [3]. Unfortunatly this approach requires experts of railway domain to analyse the rules. Even if rules formalisation requires experts, we propose the use of formal methods in order to prove operating rules.

The HEROE works allowed us to identify a particular semantics of rules. Indeed, we can find events, conjunctions, disjunctions, sequential and simultaneous actions. This semantics reminds the ECA rules notably used for the modelling of active databases [4].

ECA rules can be modelled with Petri nets [5, 6]. Thus, the Petri nets paradigm seems particularly revelant to describe the operating rules. Petri nets are a graphical and mathematical tool. They are a well established formalism for modelling and verifying concurrent and reactive systems. We invite the readers to refer to [7] for more explanation.

Nevertheless, simple place/transition Petri nets are insufficient because we have to model data transmission between events, actions and conditions. In order to answer this transmission problem, we use coloured Petri nets.

Coloured Petri nets (CPNs) [8] were introduced as an extension to Petri nets, allowing tokens to carry a data type and a value. The advantage of coloured Petri nets is the combination of the strength of Petri nets and the strength of programming languages. Indeed, Petri nets allow the description of the synchronization of concurrent processes, while programming languages provide the primitives for the definition of data types and the manipulation of data values.

We now present an example of operating rules description using a systematic method. It concerns a group of rules taken from the HEROE project.

3 Practical example

3.1 Group of rules

Our practical example concerns the group of rules applied for a safe departure of a train stemmed from the HEROE project (ERTMS/ETCS operating rules). It includes the rules “Departure”, “Train preparation”, “Permission for train movement” and “Written order”. Figure 1 shows the links between these rules.

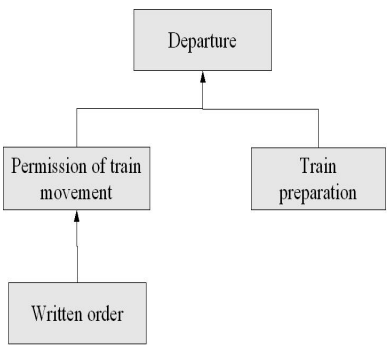

Figure 1: Relations between rules.

Figure 2 gives the text of the “Departure” rule. This rule requires five conditions to be performed. So, this is clearly a conjunction. We can also deduce that the rules for “Train preparation” (figure 3) and for “Permission for train movement” (figure 4) are called by the “Departure” rule. These relations between rules create

a link between their descriptions. Consequently, we use hierarchical coloured Petri nets to model the operating rules.

- The driver of a train is allowed to depart when :
  - he has information that conditions of "Train preparation" are met *and*;
  - he has information that the closing doors procedure has been completed and no passengers are in danger *and*;
  - the departure time is reached *and*;
  - he has received a "Permission for train movement" *and*;
  - the train is capable of clearing the platform.

Figure 2: Departure.

Figure 3 shows the "Train preparation" rule. A train must be prepared at the station (when it is composed) and in all cases when its composition or brake performance have been changed. This rule is also a conjunction.

- A train is prepared, when
  - all vehicles it consists of are coupled,
  - the train is equipped with train signals,
  - technical checks are successfully performed,
  - brake test is successfully performed,
  - brake performance is calculated,
  - train data are available,
  - data entry procedure has been performed,
  - information to check the integrity of the train is available.

Figure 3: Train preparation.

"Permission for train movement" rule is given in figure 4. We can see that signalman and driver actions are exclusive and only one of these should be executed at a time. All signalman and driver actions are obviously combine by disjunction operator.

- Signalman : when all required conditions are fulfilled, the signalman may permit a train movement by :
  - issuing a (full supervision or on sight) movement authority or
  - clearing a main signal or
  - issuing a written order
- Driver : If the driver receives :
  - a full supervision or on sight movement authority or,
  - a signal displaying a proceed aspect or
  - a written order

  he has permission to move his train.

Figure 4: Permission for train movement.

"Written order" rule (figure 5) is a safety related message issued by the signalman to the driver. It is used to convey an instruction that cannot be achieved by ERTMS. This rule is composed with parts that containing different semantics.

- Conditions :
  - train is stationary,
  - driver has identified his function, train number and location,
  - train has reached the last EOA in front of the section concerned.
- Content :
  - who issued it
  - from where it is issued
  - at what time and date
  - to which train it is intended
  - the instruction itself in an unambiguous manner
- Ways of transmission :
  - written orders may be transmitted physically written on paper, as text message or as a verbal message the driver must write it down.
- Permission of train movements :
  - the signalman must not permit a train movement until the written order has been received and confirmed by the driver.
- Precedence over DMI indication :
  - written orders take precedence over all relevant indications provided by the ERTMS DMI.

Figure 5: Written order.

Now we have four rules at our disposal in order to depict the systematic method of description presented in the next section.

3.2 Description method

In this section, we present the equivalent description of a rule referring to its semantics. Indeed, we give each rule semantics a description based on coloured Petri net. This systematic method of description allows to have a standardisation of rule translation, even if the description is done by different people.

We spotted that rules are based on events, conjunctions, disjunctions, sequential and simultaneous actions. Now we describe the translation method of these elements step by step.

- An event is represented by firing a corresponding transition of the CPN.
- Conditions combined by the conjunction operator may simply use a transition to synchronize all fulfilled sub-conditions as shown in Figure 6. This can be applied for instance to the "Departure" and the "Train preparation" rules.

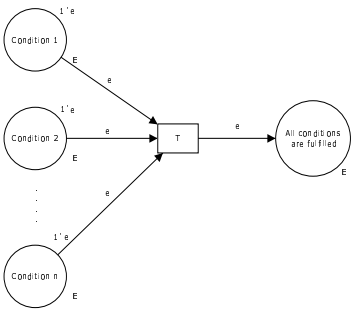

Figure 6: Conjunction.

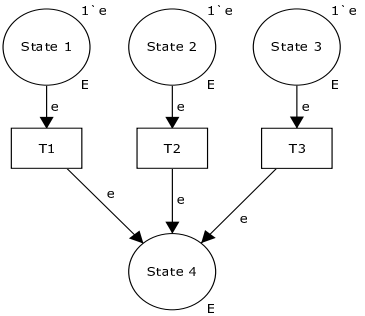

Figure 7: Disjunction.

- Conditions combined by the disjunction operator use multiple transitions as shown in figure 7. Each of them is related to one sub-condition. This translation assumes that all sub-conditions are exclusive.
- Sequenced actions are automatically described into a sequence of places and transitions as shown in figure 9.
- A rule called by another one, as for the "Train preparation" and "Permission for train movement" called by "Departure" rule, is described by a hierarchical net. An additional transition is added to depict the link (figure 8).

To understand the different annotations that we use in our models, we give here some details of CPN elements. We invite the readers to refer to [9] for more explanation.

- Each place has an associated type (colour set) determining the kind of data that the place may contain. In our example, we use E as colour. It is also possible to use complex type with several fields containing string, integer and other complex types.

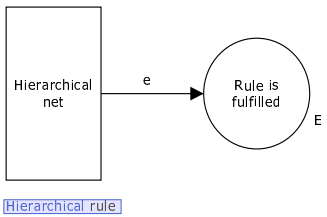

Figure 8: Hierarchical net.

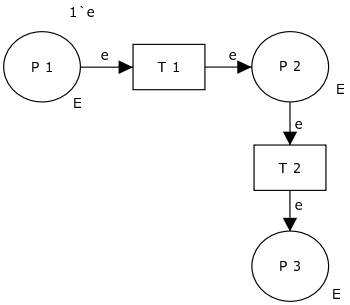

Figure 9: Sequenced actions.

- The marking of a place consists of the number of tokens this place contains. It is indicated as $1`e$ in our examples. Each token carries a value (colour), which belongs to the type of the place on which the token resides.
- To fire a transition, we need to assign data values to the variables occurring in the arc expressions. Then, we evaluate the arc expression to remove and add tokens respectively from input and output places. Either variable occurring in the arc and input-output places must have the same colour.

To complete the presentation of this systematic method of description, figure 10 shows the result of its application for the "Departure" rule (figure 2). To reach this aim, we used the conjunction translation to describe the five conditions listed on the rule. We also used two hierarchical nets to describe the call of "Train preparation" and "Permission for train movement" rules.

We presented here a systematic method of description of operating rules by means of coloured Petri nets. This method will allow a standardisation of coloured Petri nets describing operating rules. The use of hierarchical nets to describe a call of rule preserve the structure of operating rules and the link between them. It allows also to reuse Petri nets when the corresponding rule is called many times.

4 Discussion

CPN allows investigation of the system behaviour by making simulation of its model. Indeed, the simulation provides a great amount of detail, particularly for very large CPN models. Thus, in our case, we can follow the progress of operating rules execution with a view to observe message transmissions.

On the other hand, the state space method of coloured Petri nets makes it possible to validate and to verify the functional correctness of systems [10]. Indeed, with the state space method, it is possible to answer a set of analyses and verification questions concerning the behaviour of the system. Then we can verify the properties like the presence or not of deadlocks in the system. This can help us to detect scenarios which can affect the safety of railway system, using CPN-Tools for instance [11].

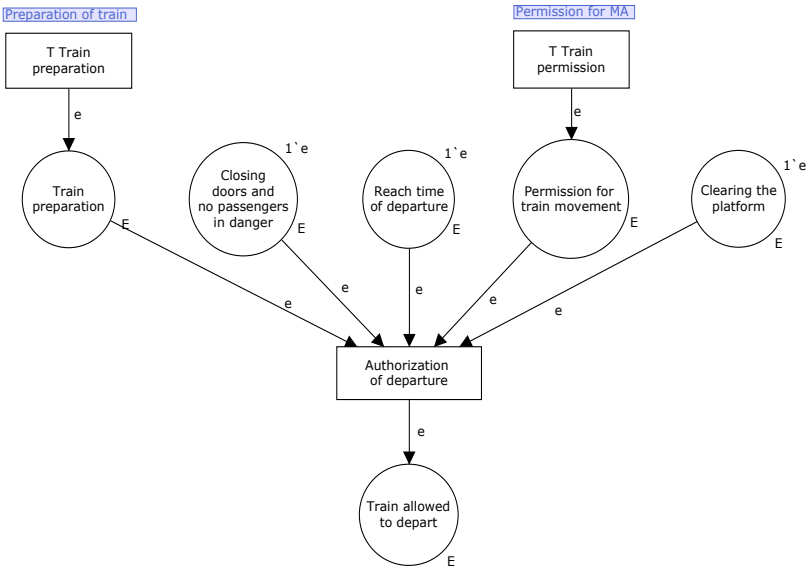

Figure 10: Complete CPN model for departure rule.

We can also use the work of [12] to translate the coloured Petri nets on an abstract B machine. Here the aim is to use the power of this method like the raffinement and well-established proof tools [13].

5 Conclusion

We presented in this paper an approach to verify the safety of operating rules. We chose coloured Petri nets because it seems particularly relevant depending on two points. The former is the similarity of the semantics of operating rules and ECA rules which can be modelled with Petri nets. The latter is to have a set of analysis methods and simulation tools at our disposal. For instance, coloured Petri nets paradigm can help us to verify a deadlock situation during execution of operating rules or to detect some dangerous scenarios.

References

[1] ERTMS, Functional requirements specification. **V4.29**, 1999.
[2] HEROE project WP A, Operational principles and rules. *The ERTMS Users Group*, p. 95, 2001.
[3] El-Koursi, E.M. & Kampmann, B., Qualitative and quantitative safety assessmenet of ERTMS operating rules. *CompRail VIII, Lemnos, Greece*, pp. 671–680, 2002.

[4] Hanson, E.N. & Widom, J., An overview of production rules in database systems. *The Knowledge Engineering Review*, **8(2)**, pp. 121–143, 1993.
[5] Allain, L. & Yim, P., Modeling information system behavior with dynamic relations nets. *JUCS*, **6(11)**, pp. 1109–1130, 2000.
[6] Gatziu, S. & Dittrich, K.R., Detecting composite events in active database systems using petri nets. *RIDE-ADS*, pp. 2–9, 1994.
[7] Murata, T., Petri nets: Properties, analysis and applications. *Proc IEEE*, **77(4)**, pp. 541–580, 1989.
[8] Jensen, K., *Coloured Petri Nets: Basic Concepts, Analysis Methods, and Practical Use*, volume 1 of *EATCS Monographs in Computer Science*. Springer-Verlag, 1992.
[9] Kristensen, L.M., Christensen, S. & Jensen, K., The practitioner's guide to coloured petri nets. *STTT*, **2(2)**, pp. 98–132, 1998.
[10] Huber, P., Jensen, A.M., Li, Jepsen, L.O. & Jensen, K., Reachability trees for high-level petri nets. *Theoretical Computer Science*, **45(3)**, pp. 261–292, 1986.
[11] CPN Group, University of Aarhus, Denmark, CPN tools home page. Http://wiki.daimi.au.dk/cpntools/.
[12] Bon, P., *Du cahier des charges aux spécifications formelles : une méthode basée sur les réseaux de Petri de haut niveau*. Ph.D. thesis, (in French), École Centrale de Lille, 2000.
[13] Abrial, J.R., *The B-Book: Assigning Programs to Meanings*. Cambridge University Press, 1996.