Simon Collart-Dutilleul *Editor*

Operating Rules and Interoperability in Trans-National High-Speed Rail

Springer

Operating Rules and Interoperability in Trans-National High-Speed Rail

Simon Collart-Dutilleul
Editor

Operating Rules and Interoperability in Trans-National High-Speed Rail

Springer

Editor
Simon Collart-Dutilleul
COSYS/ESTAS
Université Gustave Eiffel
Villeneuve d'Ascq, France

ISBN 978-3-030-72002-5 ISBN 978-3-030-72003-2 (eBook)
https://doi.org/10.1007/978-3-030-72003-2

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book is the result of many years of collaborative work on concepts and tooled experiments. Some of them were performed in a framework of projects, like ANR-TVM PERFECT, FUI21 LCHIP, IRT RAILENIUM ≪ ERTMS-Regional/Nextregio ≫... An important part is provided by academic works, mainly in the context of PhD co-supervisions. Last but not least, I want to mention the challenging discussions exchanged during amazing conferences. First, the FORMS/FORMAT conference takes an important place; it now belongs to the RSSRAIL conference to raise up ambitious propositions for the use of formal methods in railways. Formal methods are proved to be efficient to assess interlocking signalling devices. Nevertheless, railway systems are complex sociotechnical systems involving many actors including humans. In low traffic lines, many signalling functions are executed by human workers. In this case, the underlying logic has to be assessed by procedures as rigorous as the CBTC ones. The application of the above philosophy—assessing the human operation specified in operating rules for international lines, and integrating various national context and building on European technical specification for interoperability (TSI)—is the core technical contribution. This book is only a step forward, but many other steps are needed for providing efficiency to the numeric transition that the railway domain aims to achieve.

Villeneuve d'Ascq, France — Simon Collart-Dutilleul

Acknowledgements

I have greatly benefited from the challenging spirit of Marc Antoni from the SNCF/UIC. He led me to undertake all these ERTMS projects.

I want to thank Doctor Hela Kadri for her careful proofreading of this book. Her help with this project has been invaluable.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Simon Collart-Dutilleul

1.1 Introduction

Before detailing various aspects of the global growing phenomenon relative to railway high-speed lines, let us present it in few words. The global length of high-speed lines is increasing fast, in Europe and outside Europe (see Fig. 1.1). The commercial speed is gradually increasing as well (Fig. 1.2). Considering both these aspects leads to investigate seriously new railway services. Actually, going faster means going further using the same quantity of time. This quantity of time has a social meaning. As an example, it can be the travel time that people are able to use daily to go to their work. It can be the travel duration accepted for holidays, etc.

Providing high-speed railway services to a large amount of people should naturally lead to innovative uses from a societal point of view. For this reason, the first chapter of this book is an economical point of view on these international passenger lines.

Nevertheless, when we arrive to a frontier, the national laws are changing. This book aims to answer whether this legislative gap between two neighboring countries is an unbreakable wall or not. As the first answer of a legislative problem is a legislative answer, the second chapter of this book presents a European initiative normalizing on-board systems of trains through Europe and sharply defining their communications with the track-side part of the system. This is the ERTMS (European Railway Traffic Management System) specification.

Is ERTMS a solution that may be applied only in Europe? The first answer comes from the use of ERTMS in Australian high-speed lines (Katie 2016), for example. Another argument is the industrial use of CTCS in China, which is shortly presented

S. Collart-Dutilleul (✉)
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_1

in the third chapter of this book. The reader may consider whether this technical specification is far from the ERTMS one.

The fourth chapter of this book is devoted to a state of the art of modeling effort in the railway area. It closes the first part of this book devoted to an economical and technological context documentation.

The second part of this book provides a particular point of view leading to a methodological solution proposal.

Before going deeper, the basic data related to the above presentation are presented.

1.2 Fast Growing of High-Speed Lines Leading to New Paradigms

High-speed train development is increasingly growing, when you consider the number of lines or the number of trains. Let us consider the breakdown of the length of high speed lines in march 2011 (the exploitation speed is bigger than 250 km/h) in all the world (UIC source, 2011)

- 15,231 km of exploited lines,
- 9172 km of being built lines,
- 17,594 km of project of line.

It is easy to see that the total length of the projects of lines represents 15% more than the already exploited lines. Moreover, concerning the total length of work in progress of new lines building, it is a little bit less than 60% of the exploited lines. It is not surprising to see that the prospective evolution of high speed lines is a rapid increase (see Fig. 1.1). Focusing on Europe, the length of railway's high-speed lines is expected to double in less than 15 years.

All the data show that the high-speed train is entering a new dimension. All these new lines will need some operating and safety rules. The current safety expertise pertains to smaller sized systems. Anyway, a lot of new lines mean new particular case studies ensuing from new particular infrastructures and new contexts: as an example in Fig. 1.1 until 2000 years, there are some high-speed lines in other places than Europe and Asia (see the green curve in Fig. 1.1).

The last aspect to be integrated is the speed evolution (see Fig. 1.2). Increasing more than 15% starting from the maximal high speed in 2000 means that you can go further using the same time. Focusing on the French country further means mainly somewhere outside of France. Another state means another legislative context, another safety culture, etc. In other words, high speed makes possible new kinds of services, bringing new kind of problems.

Considering the line Paris-Marseille that corresponds to a real need and is well functioning, it is possible to imagine the possibility of reaching other European towns, even assuming that the commercial speed does not increase.

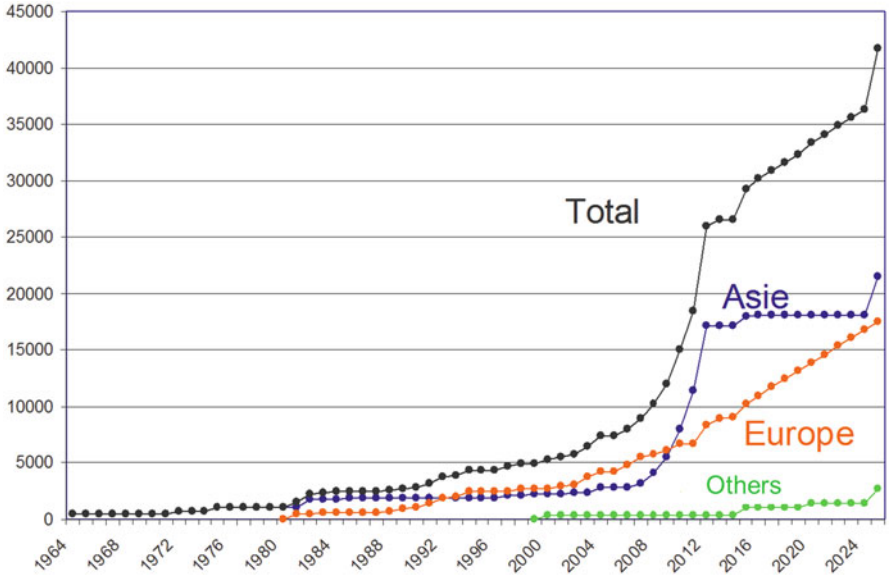


Fig. 1.1 Prospective evolution of high-speed line kilometers in the world (UIC source, 2011) (Color figure online)

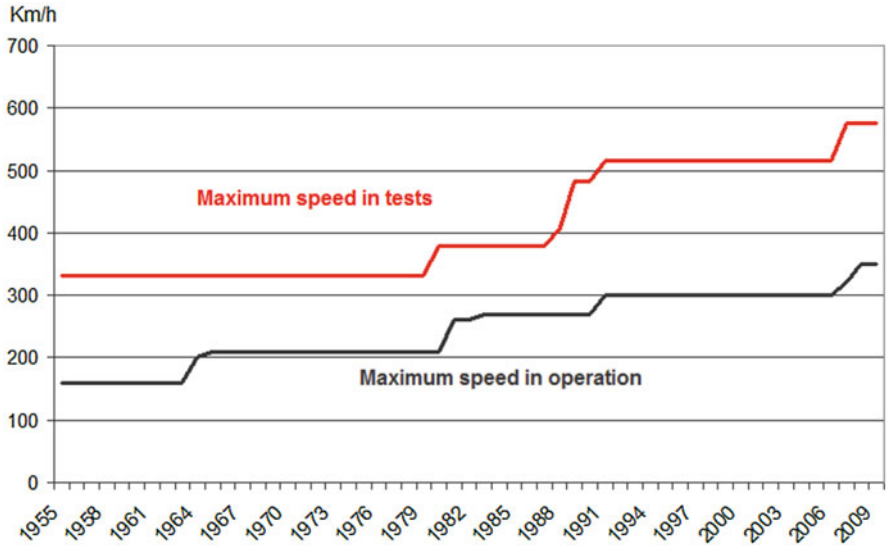


Fig. 1.2 Maximal speed evolution (UIC source, 2011)

Paris is actually the capital of France, but it is probably not true for every point of view. Making the strong assumption that crossing a national frontier costs nothing,

Fig. 1.3 A prospective vision centered on the Town of Paris (Color figure online)

the red circle in Fig. 1.3 may be moved to the right, to the north, or to the south, connecting more European economical capitals altogether.

Moving this red circle is useful to build a vision of what may be achieved in the following years, taking into account the run of the technology and assuming that the legislative wall does not exist.

The next section focuses on legislative aspects.

1.3 National Specific Rules: Framework Characterization

Trans-national high-speed lines have to tackle with the interoperability task. ERTMS/ETCS is the European proposed solution for on-board systems, whereas this technological and legislative context has to be integrated in all the different European countries. New operating rules have to respect both European interoperability directives and national safety rules (Fig. 1.4).

Aligning national safety rules may seem to be an easy solution. It is true considering that a rule is only a piece of paper, but when you integrate the fact that a rule is a list of actions of technical disposition relative to a given context, to be executed in order to achieve the needed level of safety, it becomes less simple (Fig. 1.5).

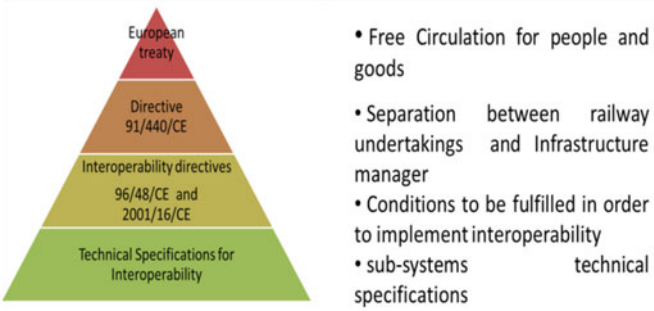


Fig. 1.4 ERTMS legislative context

Fig. 1.5 Operating rules positioning in a legislative hierarchy

The following section provides the basics of safety rules engineering.

1.3.1 Safety Rules

1.3.1.1 Definition

A safety rule is a set of coordinated actions to be made in order to make the set of all operations reach an acceptable level of safety. It includes

1. an application context (location, date, type of operation),
2. some conditions (constraint to be fulfilled for a valid application of the rule, as an example, a train arrival has to be signaled before a given distance from the concerned zone), and
3. a list of action to be made (as an example, moving the team to a non-dangerous zone).

Two kinds of safety rules may be identified:

– The first one imposes some actions preventing from an accident occurrence: this is the barrier concept.
– The second one demands an organization that decreases the occurrence probability of an accident or attenuates its severity.

A superficial analysis could directly demand first-type rules rather than second one. Anyway, the real pragmatic question, tacking the context into account, is What can be done?

Actually, a combination of the two types of rules may be used to reach the acceptable safety level. The question of which kind of rule should be applied becomes critical when a higher level rule requires a barrier kind of rule. In this case, applying a rule that rather decreases the severity does not correspond to the specification. Locally, the level of safety may be correct but form a global system safety point of view, some dangerous occurrence chains may be still allowed.

1.3.1.2 Bureaucratic Rule-Writing Approach in a Dynamic World

One of the more interesting contributions concerning safety rules in railway is Hale en 2003: *"Management of safety rules: the use of railways" Hale et al. (2003)*.

Nevertheless, this document claims that there is only a little quantity of scientific articles which deals with this subject.

A classical analysis considers that a given rule uses a collective knowledge to define some safe behaviors and some safe equipment. This knowledge is used to make them run safely (Baumard 1999).

Bureaucratic Approach and Safety

The assumption is that the rule editor has a general knowledge of all the possible contexts and overall knowledge of the global system. This top-down approach puts a high level of competency on the high-level layer of management (Hovden 1998). One of the goals is to make the behavior deterministic at the lowest level of the system.

Under this strong assumption, the rule can be edited using a simple process, because the editor must have a total knowledge. Using several-leveled rule decomposition is not mandatory, because the principle to be implemented is known by the editor.

The high responsibility-leveled editor writes the rules and defines the way it is applied. In this case, there are no real consistency problems. The lower levels only receive a delegation for controlling the rule application.

All these assumptions are difficult to meet in a dynamic world, as an example when there are some new technological environments and some new services.

Collective Knowledge?

When the knowledge is collective, it is useful to obtain all the needed information by the one who has a part of this knowledge in order to build a safety rule.

Using a purely knowledge approach, the knowledge increases in case of accident, because the scenario is added to the common knowledge.

In a fast-changing world, it is not possible, because we may build knowledge corresponding to a system that does not exist anymore. The preliminary risks analysis is a methodology to be considered (Rasmussen and Svedung 2000).

Anyway, there is a need for a predictive approach (Kirwan et al. 2002).

1.3.1.3 French Point of View

According to the directives from SNCF (IN3600), the text of a rule is both a product and a project.

A rule is a product because it has to be delivered to some clients who need it. By the consequence, the client satisfaction of these clients is an important parameter.

When the creator of a rule is not the client, one may think that the client understanding of the rule is the best because he/she is the one who applies the rule in a real context. Nevertheless, this assertion cannot be accepted for several reasons.

Accepting a misunderstanding as a solution is dangerous because it is building a gap between the the knowledge of the designers and that of the operators.

When they are several kinds of users for a given rule, their application context and technological culture may be different. In this case, the only way to build a safe collaboration is to make them apply the same rule (i.e. applying the same actions in the same situation).

Anyway, if there are several understandings of a text, who is right?

In order to propose a solution, the state of the art was consulted:

> The rule editor is the leader of its translation (Reason 1997).

By translation, one may understand, instantiating of principles included in a rule in some particular contexts.

As misunderstanding is not allowed, one man must be able to give a unique signification to the text. If this condition is respected, behavior becomes to be deterministic.

Moreover, the editor of a given rule is a client for higher level rules, which must be respected. As a consequence, when he/she orders an action in order to fulfill another rule, the interpretation of the current rule has to preserve the compatibility with a set of rules: this is typically the role of the rule editor.

Actually, when a rule does not respect the higher rule, it is just outlaw: the highest safety rule comes directly from the government of the concerned state.

1.4 National Rules and Interoperability: A Problem to be Solved

Writing safety rules is not an easy task, but many efficient safety rules have been written.

Standing a problem of rule alignment for several countries looks non-tractable. Anyway, half of the problem is solved by the use of an ERTMS like technological context.

The first part of this book presents ERTMS as a contribution to achieve interoperability, while the the second part of this book details a proposal based on ERTMS taking into account the national-specific contexts. It proposes to use model engineering as an abstraction layer aiming at aligning various needed knowledge. The main idea is to propose local alignments by the use of common functioning modes for border crossing.

References

Baumard, P. (1999). *Tacit knowledge in organizations*. London: Sage Publication.

Hale, A. R, Heijer, F., & Koormneeef, F. (2003). Management of safety rules: The case of railways. *Safety Science Monitor, 7*, 1–11.

Hovden, J. (1998). Models of organization versus safety management approach: A discussion based on studies of the "internal Control of the SHE". In B. Kirwan, A. R. Hale, & A. Hopkins (Eds.), *Changing regulation: Controlling risk in society*. Oxford: Pergamon.

Katie, S. (2016, June 29). *Australia receives its first ETCS Level 2 signalling system in Sydney*. News, Digital Content Producer, Global Railway Review.

Kirwan, B., Hale, A. R., & Hopkins, A. (2002). Insights into safety regulation. In *Changing regulation: Controlling risk in society*. Oxford: Pergamon.

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in dynamic society*. Karlstad: Räddningsverket.

Reason, J. (1997). *Managing the risk of organizational accident*. Aldershot: Ashgate Publishing Limited.

Part I
Technological and Economical Context

Chapter 2
The Performance of International Passenger Rail Transportation: A Statistical Assessment

Corinne Blanquart and Thomas Zeroual

2.1 Introduction

There are many advantages to taking the train. Unlike driving, rail allows travellers to avoid traffic, especially during rush hours. It also allows travellers to rest, especially over long distances. Moreover, there are 18 times fewer accidents by rail than by car. Unlike air travel, rail travel allows travellers to travel to and from a city centre or downtown area, as railroad stations are generally located within cities rather than on the outskirts, like airports. And rail travel does not involve arriving over an hour before departure. In terms of the environment, rail travel also has many advantages: a train uses on average 12 times less fuel per person than a car and 3 times less than an airplane (SNCF 2016). High-speed train (TGV) passengers reduce their CO2 emissions per kilometre by 50 compared to a car, by 25 compared to a carpool and by 8 compared to a bus[1] (Spinetta Report 2018).

For many years, the European Commission has therefore been working to promote international rail transportation, especially with the Fourth Railway Package of 2016, which aims to realize a single European market for rail. This commitment has had some positive results, including visible improvements in service quality (Von Arx et al. 2018). This progress on international lines has been supplemented by national efforts, especially in mass transit links between cities or major metropolitan areas.

[1] Only regional diesel trains emit more CO2 than busses because of their low occupancy rates.

C. Blanquart
Université Gustave Eiffel, AME-SPLOTT, Villeneuve d'Ascq, France
e-mail: corinne.blanquart@univ-eiffel.fr

T. Zeroual (✉)
ESCE, CIRCEE, Paris, France
e-mail: thomas.zeroual@esce.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_2

However, the results for international rail do not seem to have measured up in terms of commitments or benefits. In 2017, the European Commission inventoried 365 existing cross-border railway lines in Europe. Of these lines, 202 are operational and 156 are frequently used. Only 57 are classified as "fully utilized," 81 are "imperfectly utilized" and 18 are "not fully utilized" (Sipel 2018).

Just as rail has been overtaken in each country,[2] the same is happening in international travel. To understand these disheartening results for international rail travel, we will proceed in two steps. The first step will make a comparison at a time *t* (synchronous) and then compare the rate of progress (diachronic) of rail in European countries. Rankings will then be made to illustrate the diversity of European railways. These synchronous and diachronic comparisons will be put into perspective with the growth rates of rail's main competitors: bus and air travel. We will then analyse the reasons behind international rail's lacklustre performance.

Both of these steps require reliable data. The EU Eurostat database will be very useful for European comparisons. It will allow us to make a clear assessment through the use of percentages. This database will be supplemented primarily by data from ARAFER (the French government agency regulating rail and vehicle transport) for comparisons between modes of transportation and INSEE to look at the case of France.

2.2 Statistical Assessment: Comparisons in Europe and Between Modes of Transport

In this first step, we will assess passenger rail transport at time *t* (synchronous) in the first subsection, followed by a dynamic or diachronic assessment in the second subsection. Each subsection will include comparisons between European countries and between modes of transportation.

2.2.1 A First Synchronous Assessment

In passenger kilometres per inhabitant, Luxemburg, France, Czech Republic, Switzerland and Denmark had the most international rail travellers in the EU-18 in 2016, as can be seen in Fig. 2.1. These top five alone represent 63.7% of all rail passengers. To compare with transportation within the country, the countries with the most rail users per capita are, in order, Switzerland, Austria, the Netherlands,

[2] At the national level, the volume of vehicle transport is much higher than for rail: it is at least 10 times higher in the EU-28 from 1995 to 2015. Air travel is catching up, increasing by 86.5%, while the growth rate for rail in the same location over the same period was 26.1% . In international travel, rail made up 4.8% of total trips in Europe in 2016 (ARAFER 2018).

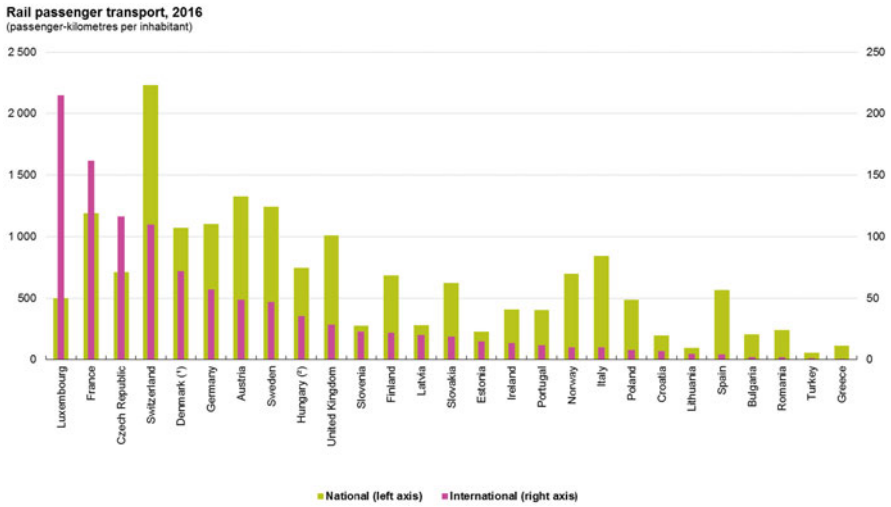


Fig. 2.1 International rail travellers in decreasing order of passenger kilometres per inhabitant, by European countries (Eurostat, 2018)

France and Sweden. These numbers can be explained by the geographic location of these countries, which have the most international borders, the number of cross-border workers and the speed offered by certain lines, as we will see in later sections.

More specifically, Table 2.1a presents a country ranking of passenger kilometres by inhabitant for domestic travel, in decreasing order. Table 2.1b presents a parallel ranking for international travel. It is interesting to note that among the 10 countries with the most national rail travel, nine of them are also in the top ten for international travel. Only Luxemburg is not in both rankings: it is the country with the most international travellers per inhabitant and also the country with the weakest multiplier between national and international travel. Besides this exception, the higher the amount of national travel, the more frequent international trips seem to be.

An analysis of how many thousands of international travellers enter and leave European countries can supplement this comparison of passenger kilometres by inhabitant. We first note the complete lack of data for five countries: Italy, Cyprus, Malta, the Netherlands and Austria. The lack of recent data is also problematic for our analysis (especially for France, where the Eurostat data end in 2009, and for Belgium, where there are no data after 2011). We have thus chosen to work with an average of the last 10 years. France is on average the country with the most travellers entering, followed by the UK, Germany and Switzerland, as seen in Fig. 2.2. France is also the country with the most travellers leaving the country, followed by the UK, Belgium, Germany and Switzerland. For comparison, bus travel carries an average of 4 million passengers from France to other countries (ARAFER 2018).

Table 2.1 Ranking of the top 10 European countries by national and international rail passengers, by passenger kilometre per inhabitant in 2016 (Eurostat, 2018)

(a) Country ranking for domestic travel

Rank	Country	Domestic	International	Multiplier
1	Switzerland	2231	110	20.32862
2	Austria	1328	49	27.35377
3	Sweden	1243	47	26.40899
4	France	1189	162	7.355597
5	Germany	1102	57	19.31191
6	Denmark (2015)	1073	72	14.94853
7	UK	1009	28	36.02232
8	Italy	843	10	87.55479
9	Hungary (2014)	746	35	21.34783
10	Czech Republic	711	116	6.109845

(b) Country ranking for international travel

N°	Country	Domestic.	Inter.	Multiplier
15	Luxemburg	502	215	2.336
4	France	1189	162	7.355597
10	Czech Republic	711	116	6.109845
1	Switzerland	2231	110	20.32862
6	Denmark (2015)	1073	72	14.94853
5	Germany	1102	57	19.31191
2	Austria	1328	49	27.35377
3	Sweden	1243	47	26.40899
9	Hungary (2014)	746	35	21.34783
7	UK	1009	28	36.02232

An analysis of the difference between those entering and leaving shows heterogeneity within the EU, as seen in Table 2.2. Belgium is the country with the highest negative balance, followed by Germany, France and Switzerland.

To supplement this average, a table of international travellers from each country reporting their destination country and a table of international travellers arriving in each country reporting which UE 28 country they are from would provide much valuable information. Unfortunately, the fragmentation of the data by year and country makes it impossible to build a reliable synthesis of this information.[3] We therefore mainly use international tourism numbers to narrow down the origin and destination of passengers from one country abroad and then from abroad to a country. We chose to look at France because it has the highest number of arrivals and departures: France has 11 border regions. The flow of migration differs depending

[3]Here, we have in mind the Eurostat databases "international transport of passengers from the reporting country to the country of disembarkation" and "international transport of passengers from the country of embarkation to the reporting country."

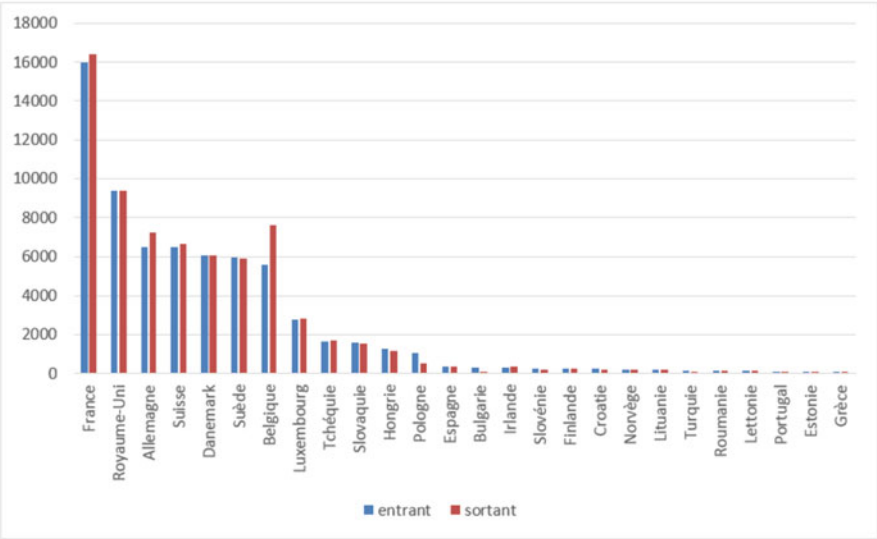


Fig. 2.2 Comparison of international rail travellers entering and leaving countries, on average, by thousands of passengers in Europe (Eurostat, 2018)

Table 2.2 Ranking of the top 10 European countries in terms of average number of international rail travellers entering and leaving, and the balance, in thousands of passengers (Eurostat, 2018)

Country	Average entering	Country	Average leaving	Country	Average balance
France	15,984	France	16,389	Belgium	−2070
UK	9389	UK	9389	Germany	−753
Germany	6463	Belgium	7616	France	−405
Switzerland	6461	Germany	7216	Switzerland	−188
Denmark	6040	Switzerland	6650	Ireland	−75
Sweden	5923	Denmark	6040	Czech Republic	−67
Belgium	5546	Sweden	5917	Luxemburg	−51
Luxemburg	2799	Luxemburg	2850	Romania	−13
Czech Republic	1644	Czech Republic	1711	Greece	−1
Slovakia	1601	Slovakia	1551	Spain	−1

on the country. In the case of France, we therefore distinguish between short and long trips and between business and leisure travel.

In 2012, 14% of business travel in France had an international destination. Short international trips (1–3 nights) made up 8% of all business travel and long trips abroad made up 6% (INSEE 2018). The estimated 350,000 commuters cross

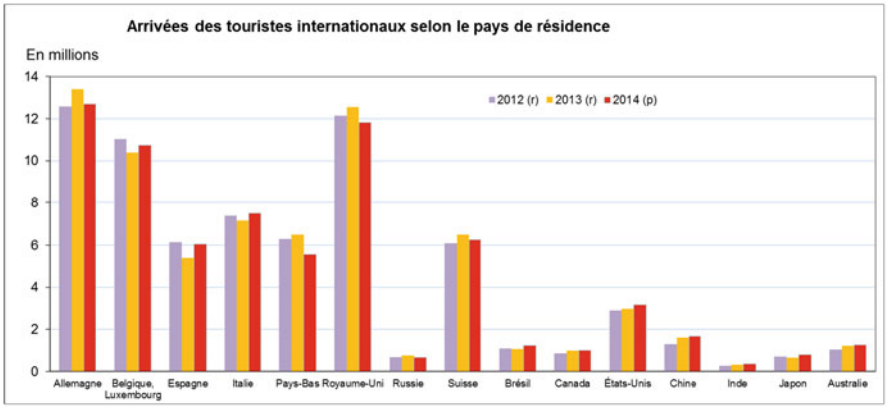


Fig. 2.3 Survey of visitors from abroad (DGE, Banque de France, 2013)

borders from France every day.[4] In comparison, in all of Europe, 2 million people work in another country at least once a week as of 2015. And the trend of cross-border professionals has more than tripled in the last 15 years.[5] In terms of mode of transportation, public transportation has a share of about 7% of cross-border mobility.

For leisure travel, 74.7% of trips had a destination in the EU: 17.2% to Spain and 11.6% to Italy. African countries were the second most popular destination (11.6%), followed by North and South America (8.2%) and Asia and Oceania (5.5%). At the same time, 84.8% of visitors to France came for leisure travel and 14.1% for business. Most of the international tourists arriving in France are travelling to France as their final destination (86.5%); France is not a transit country. Most of the most frequent visitors come from bordering countries as seen in Fig. 2.3.

The trips these international visitors take can also be analysed by mode of transportation. Worldwide in 2015, 54% of international arrivals came by air and 39% by vehicle (OMT 2017). In 2012, in France, 77.9% of international visitors came by vehicle, 14.5% by air, 4.9% by boat and 2.7% by train (DGCIS, Banque de France, EVE, 2013). At the same time, 58.8% of leisure trips from France to other countries were by air, 26.5% by car or motorbike and only 6.5% by train.

If we only look at cross-border travel, rail travel does not come out any more favourably. In fact, 90% of these trips are taken in private cars. On the other hand, rail travel makes up 80% of the remaining 10% of these trips. In France, there are over 20 rail lines that allow cross-border travel: the most popular go to Luxemburg,

[4]These flows should be qualified given the available databases as well as the flows clustered in these statistics due to factors like proximity or transit.

[5]http://www.observatoire-des-territoires.gouv.fr/observatoire-des-territoires/fr/dynamiques-de-lemploi-transfrontalier-en-europe-et-en-france.

Switzerland, Monaco, Italy and Germany. The distance between home and work, urban sprawl and traffic jams encourage people to use the railway (Forthoffer 2003).

Finally, within the railway offerings in France in 2014, international high-speed trains (TGV) made up 26 million kilometres of tracks, as opposed to 105 million for national TGV trains and 179 for regional trains (TER) (SNCF Network, ARAFER).

2.2.2 A Second Diachronic Assessment

We support the synchronous analysis with a diachronic analysis. Over the last 10 years, from 2008 to 2017, the Czech Republic and Spain have more than doubled the number of international rail passengers, followed by Norway with a growth rate of 80.64%. This trend is interesting because it shows the activity in these three countries that were ranked 10th, 14th and 11th in international rail travel in 2016 (Table 2.3).

If we compare this change to interior rail travel, the 10 countries where the number of passenger kilometres travelled by rail has grown the most between 2008 and 2015 are, in rank order, Poland, Bulgaria, Slovenia, France, Serbia, Croatia, Iceland, Latvia, Montenegro and Belgium (Fig. 2.4).

This progress is encouraging but should be seen in conjunction with other modes of transportation such as air travel. Air travel from France to other countries is clearly increasing: it grew by 379% from 1980 to 2017 and over 28% from 2008 to 2017. It is interesting to note that most of this travel is international and mostly within Europe, with the highest volume, 40.17 million passengers on average between 1980 and 2017, and the highest growth rate, over 588% in the same period, as well as one of the highest growth rates, over 38%, in the more recent period of 2008–2017 (Table 2.4).

Within Europe, 58.5% of international air travel from France goes to the UK, Spain, Italy and Germany (Table 2.5).

Table 2.3 Ranking of growth in the top 10 countries by international travellers, in thousands of passenger kilometres travelled by rail in Europe (Eurostat, 2018)

		2008	2010	2012	2014	2016	2017	% 2008–2017
1	Czech Republic	449	296	402	700	1229	1437	220.04
2	Spain	221	194	147	177	183	634	186.87
3	Norway	31	72	45	43	51	56	80.64
4	France	7546	–	10,698	10,810	10,810	9683	28.31
5	Finland	112	90	128	134	117	142	26.78
6	Germany	3870	4321	5124	5059	4700	4790	23.77
7	UK	1654	1720	1813	1905	1837	1872	13.18
8	Sweden	537	538	462	492	467	591	10.05
9	Portugal	120	103	90	111	120	124	3.33
10	Switzerland	912	998	1006	933	919	928	1.75

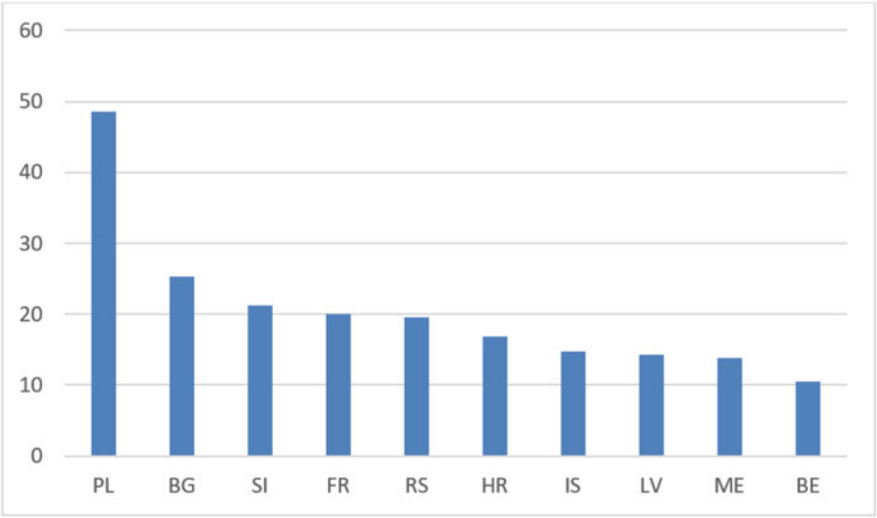


Fig. 2.4 Top 10 ranked countries of the EU-28 by growth rate in passenger rail travel, 2000–2015 (Eurostat, 2018)

Table 2.4 Air travel from France to other countries (DGAC 2018)

	% 1980–2017	% 2008–2017	Average 1980–2017
Total (mainland) France	379.29	28.31	87,304
France–International	488.17	32.11	63,562
France–Europe	588.91	38.80	40,172
France–Africa	200.78	13.34	10,317
France–America	575.63	15.83	7575
France–Asia	657.55	40.35	5483
France–Oceania	−99.97	-	14
France–France	144.33	12.42	21,047
Paris–Other Cities	91.66	−0.716	16,278
Other Cities–Other Cities	397.42	48.92	4769
Mainland France–French territories	474.05	25.44	2695
French territories–French territories	97.82	6.88	1703
French territories–International	166.57	25.48	1701
Total French territories	217.04	20.15	6099

Rail travel in France experienced four major phases in its development. The first phase extended from the Industrial Revolution to World War II: rail had a 90% share of transportation at the beginning of the twentieth century. The second phase took place between the 1930s and the 1970s. This period saw electrification in the 1930s and the beginnings of competition from private cars and air travel during the "trente glorieuses" period from the end of the war until the oil crisis of the 1970s. This new competition had clear effects: while over half the network was electrified in France,

Table 2.5 International air travel from France to Europe (DGAC 2018)

	% 2000–2017	Average 2000–2017
Europe	104.44	60,349
Spain	154.74	8663
UK	57.80	11,136
Italy	106.18	8151
Germany	58.23	7356
Portugal	312.96	3141
Netherlands	121.44	2620
Switzerland	15.38	2680

about 30,000 km of rail lines were deactivated between 1930 and 1970 (Spinetta Report 2018). The third phase, from the 1980s to the 2010s, was characterized by speed, with the development of the TGV and the construction of over thousands of kilometres of high-speed rails. The extension of the TGV network since the 1980s means that the TGV now carries half of all rail passengers (in passenger kilometres) even though the majority of trains in circulation are regional trains. The most recent development phase involves competition from new strategies and actors: budget air and bus travel as well as carpooling services. This competition explains in part the stagnation of TGV travel since 2011 (SDES 2016).

Looking at the passenger rail offerings in France in the last 3 years, one of the most significant declines is in international travel (−10%), as compared to domestic travel (−6%) and intercity trains (−13%).

2.3 The Performance of Rail and Its Competitors

To identify the difficulties rail travel is experiencing, we will analyse it with all the indicators traditionally used to evaluate the performance of modes of transport: cost, speed, punctuality, regularity and security. These indicators will be supplemented by environmental indicators such as greenhouse gas emissions, energy consumption and surface area.

2.3.1 The Question of Cost for Rail Users

Private cars are the preferred mode of transportation for most trips. At the same time, the cost of driving has gone up by about 34% over the past 40 years, adjusting for inflation, while public transportation prices have gone up by 12% (Beauvais Consultants 2013).

When this comparison includes the cost of rail transportation, the results are the same when compared to road transportation but differ when comparing rail transportation to other modes. More specifically, when looking at user costs for

short distances, the regional TER train costs 0.0794 € per passenger kilometre and public transportation costs 0.1145€ per passenger kilometre in the Paris metro area and 0.1282€ in the rest of France, while each kilometre of car travel costs 0.2694€. For long distances, rail travel costs 0.0911€ for intercity trains and 0.1098€ for the TGV, while budget air travel costs 0.0556€ and coaches 0.069€ per passenger kilometre. Only traditional air travel and private cars are more expensive than the train over long distances, costing 0.1511€ and 0.1921€, respectively, Beauvais Consultants (2013).

If we narrow the analysis to international rail travel, for French rail in 2015, we see that the average price per passenger for international travel is the highest: 46.1€ for the TGV, 22€ for the intercity trains and 3.8€ for the TER (ARAFER). It should be noted that it is difficult to make comparisons of rail prices across Europe. To compare the price of train tickets in two different countries, all of the services provided would have to be identical and rates would need to vary little over time. However, the services and prices offered by different rail companies are very different, and relying on an average price across European counties would hide too many disparities.[6]

Revenue earned from international rail lines is much lower than from domestic lines: international transportation generates only 15% of revenues. Profits from the TGV mostly come from same-day round trips between major cities (Spinetta Report 2018) (Tables 2.6 and 2.7).

Several factors could explain these prices. First of all, rail travel has less structural flexibility than air or bus travel, which does not allow it to adapt to demand much if at all (IRG-Rail 2015). Second, the average distance to international destinations is 309 km. Only the TGV has a higher average distance per trip of 445 km. However, rail travel is less competitive for long distances than budget air or bus travel. If we compare TGV prices with air travel, production costs per kilometre are much higher for rail as distances increase. For distances between 400 and 600 km, production costs are lower for rail, and for distances between 600 and 800 km, the rates are comparable for both types of travel. At distances over 800 km, the train becomes much more expensive than air travel (Spinetta Report 2018). In observing user

Table 2.6 Passenger transported from local, national and international rail lines (ARAFER 2016)

2015	Passenger kilometres transported (PKT)	Passengers transported
TER	13,418,267,929	267,500,000
Transilien	13,397,009,231	900,036,310
Intercités	7,175,684,263	28,900,000
TGV, domestic	45,945,391,552	103,167,355
International	7,390,411,856	23,915,895
Total	87,326,764,831	1,323,519,560

[6] GoEuro does offer a comparison of average prices.

Table 2.7 Revenue earned from local, national and international rail lines (ARAFER 2016)

2015	Sales revenue (€ H.T.)	Average passenger distance (km)	Average occupancy rate (%)	Revenue per PKT (€/100 PKT)	Revenue per train km. (€)	Average price per pass. (€)
TER	1,029,268,127	50	25%	7.7 €	5.9 €	3.8 €
Transilien	1,029,640,409	15	25%	7.7 €	17.3 €	1.1 €
Intercités	634,483,270	248	42%	8.8 €	19.3 €	22.0 €
TGV, domestic	4,470,306,341	445	61%	9.7 €	39.5 €	43.3 €
International	1,101,462,332	309	73%	14.9 €	44.0 €	**46.1** €
Total	8,265,160,479	66	42%	9.5 €	20.6 €	6.3 €

behaviour in comparing rail to bus travel, 38% of users chose the bus or carpooling because of the cost of rail travel (ARAFER). Third, business regulations are often less constraining for bus and air companies (IRG-Rail 2015). Finally, rail travel includes extra fees. Access fees are very high in international trips, especially for the TGV and night trains. In addition, unlike air travel, rail travel is not exempt from VAT.

2.3.1.1 Trip Duration

In this section, analysing travel time, we focus only on rail and air travel. To understand the potential market share trains could have as opposed to air travel, we have calculated the market share of each mode by rail travel time. Switching from rail to air travel seems to occur with trips that take 3 to 4 h by train; travellers prefer rail for trips that take less time. When the trip takes 3 h, the market share for business day trips is evenly distributed between rail and air. For trips over that duration, air travel is preferred to train by about 80% of this clientele (Spinetta Report 2018, p. 60). For trips over 5 h, for example, train travel has a 10–20% market share (Mignauw, 1998). It would thus seem necessary to focus on rail itineraries that take 2–3 h in order to compete with air travel (Klein and Claisse 1997) as this is the competitive distance for rail. It should be noted that this distance is limited to the domestic market between major cities, as seen in the figure below (OECD). In fact, when rail trips are international, the flow of passengers is sharply reduced (Spinetta Report 2018).

2.3.1.2 Service Quality: The Punctuality, Cancellation and Security Triangle

We now measure these three indicators for rail and air travel by comparing domestic and medium-haul flights[7] to domestic and international rail itineraries.

On average, rail travel always has fewer delays than does air travel. Within rail travel, delays are overall the same for international and TGV trips. Within air travel, there is always a higher delay rate for long-haul than for medium-haul flights and lower for domestic flights. If we focus on 2016 and 2017,[8] the increase in delays was primarily caused by the number of flights. We can also see a reduction

[7] Air France's medium-haul network includes flights in Europe between the following countries: Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Finland, France (not counting domestic flights in France), Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Norway, Poland, Portugal, Rumania, Russia, Serbia, Slovenia, Spain, Sweden, Switzerland, Turkey, the UK and Ukraine. It also includes flights between Europe and North Africa (Algeria, Morocco and Tunisia) and Israel. Source: www.airfrance.fr.

[8] For air travel, we prefer to focus on the last few years because the method of evaluating delays was changed in 2016.

in "passengers" and "airlines" as causes for delays and an increase in "security" causes, especially in medium-haul flights.

On average, the cancellation rate in rail is extremely variable and hides various discrepancies. The cancellation rate for air is clearer and seems to be inversely proportional to the delay rate: higher for domestic flights, followed by medium- and long-haul flights.

In terms of growth rate, delays are stable overall for air travel, with some improvement in long-haul flights. On the other hand, for rail travel, there has been significant growth in the delay rate for TGV and international travel. For international rail travel, the lowest delay rate is for trips between France and Switzerland. Cancellations have decreased for domestic and medium-haul flights but have increased for long-haul flights. For rail travel, cancellations have sharply increased for TGV and international trips (Table 2.8).

Comparing rail and coach travel, it seems that rail travel is more punctual: 21% of coaches arrived at their final destination at least 15 min late. These delays increase for international trips, with 44% of them having a delay of over 15 min.

Looking at delays across rail types, international trips are the bad apple, with 23% of trains delayed by more than 5 min 59 s, as opposed to 22% for intercity trains, 21% for TGV, 10% for TER and 9% for the Paris regional train Transilien (Tables 2.9 and 2.10).

Rail travel is extremely safe: in France, 54 people were killed over 87 billion passenger kilometres in 2015. In the same year, 3461 people were killed in road travel over 809 billion passenger kilometres, making rail travel seven times safer than driving (Sipel 2018). Comparing all modes of transportation, rail, with 0.10 fatalities per billion passenger kilometres, comes just behind air, with 0.06. The bus is half as safe, with a fatality rate of 0.19, followed by water travel (0.27), cars (passengers) (0.85), cars (drivers) (1.82) and motorcycles (37.80) according to the European Railway Agency. The increase in rail safety in Europe is encouraging: the

Table 2.8 Cancellation and delay rate (AQST 2018)

		2012	2013	2014	2015	2016	2017
Cancellation rate							
Air	Domestic	1.1	1.4	3	0.7	1.6	1.1
	Medium-haul	0.8	1.4	1.4	0.7	1.1	0.8
	Long-haul	0.8	0.6	1.6	0.4	0.5	0.5
Rail	International	0.2	3	0.3			1.2
	TGV	0.1	0.3	1.1	0.3	0.3	1
Delay rate							
Air	Domestic	13.1	13.3	13.1	11.1	17.1	17
	Medium-haul	16.8	17.6	18.3	19.4	22.4	22.4
	Long-haul	33.5	27.5	25.6	25.8	27.4	26.6
Rail	International	13.5	12.6	9.4	11.1	10.3	15.3
	TGV	10.6	11.7	9.6	10.8	11.5	15.4

Table 2.9 Cancellations across rail types (AQST 2018)

	Daily circulation	Advance cancellations	Trains scheduled as of the day before at 4:00 pm	Completely last-minute cancellations	Partial last-minute cancellations
TER	6182	61	6121	86	35
Transilien	4832	100	4732	127	54
Intercities	282	5	278	2	1
TGV, domestic	615	4	611	2	4
International	178	2	176	1	0
All passenger lines except non-contractual long-distance trains	12,089	172	11,917	218	95

Table 2.10 Delays across rail types (AQST 2018)

	Trains running	Trains running with a delay of over 5 min 59 s at terminus	Trains delayed less than 5 min
TER	5999	595	5285
Transilien	4551	423	4033
Intercities	275	60	207
TGV, domestic	604	129	457
International	175	40	131
All passenger lines except non-contractual long-distance trains	11,605	1247	10,113

number of fatalities dropped from 1517 in 2007 to 963 in 2015, and the number of serious injuries in the same time period dropped from 1367 to 684 (European Railway Agency 2017).

At the same time, there are great disparities among European countries in terms of number of fatalities by train kilometre. The safest countries for rail travel are Ireland, Norway, Luxemburg, Great Britain, Switzerland and the Netherlands, in that order. The least safe countries for rail are mostly in Eastern Europe, such as Poland and Greece and especially Slovakia, as can be seen in the map in Fig. 2.5 below.

2.3.2 The Environment, a Neglected Performance Indicator

On the environmental level, the advantages of rail are also numerous. A train consumes 12 times less energy than a car and three times less than an airplane

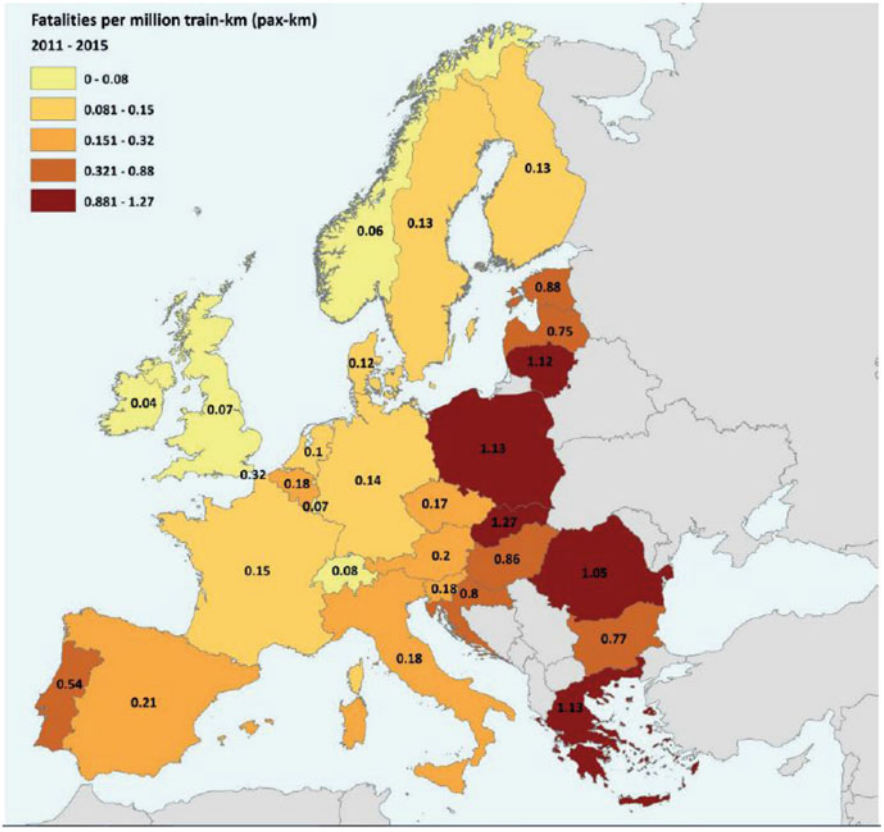


Fig. 2.5 Fatalities per million train kilometre (European Railway Agency 2017, Annual Report)

(SNCF, 2016). TGV passengers reduce their CO2 emissions per kilometre by 50 as compared to car travel, 25 compared to carpooling and 8 compared to bus (Spinetta Report 2018). And the average capacities of trains are well above other modes of transportation: a coach has an average of 20–80 seats and a domestic airplane has 40–220 seats, while a TGV has 380–1200 seats.

While energy consumption and greenhouse gas emissions are two important environmental indicators, land use should not be neglected as a factor, as it entails substantial negative externalities such as deforestation and loss of biodiversity. Rail travel uses much less land than does road travel. Considering the total surface area of the easement, a TGV line covers an average of 5–7 ha/km, while a motorway covers 9–10 ha/km for a 4-lane road and 10–11 for a 6-lane road (Setra). Overall volume is much lower for rail travel: 30,023 km in 2016 (including tracks used by the French rail company SNCF in conjunction with the Paris metro, regional commuter trains and trams) as opposed to the 1,103,366 km of roads in mainland France (SDES). There are 36 times more kilometres of road than of rail, and rail uses only 2.2

times more kilometres than do cycling and walking paths, estimated at 13,700 km. Of course, land use varies across Europe. Germany has the longest transportation network, with 37,775 km, followed by France with 28,987 km. Germany also has the highest density (0.47 km per 1000 inhabitants as opposed to 0.44 for France) according to Eurostat.

To compare land use between rail and air travel, it is clearly impossible to use the number of hectares covered by kilometre of roads or tracks. Rather, the comparison should be with the amount of land use for a similar number of passengers. Using this indicator, here too, rail expropriates less land: for a comparable number of passengers, the Paris-Lyon TGV line uses 2400 ha, while the Charles de Gaulle airport uses 3000 ha (source).

2.4 Conclusion

International rail travel faces a great deal of competition from coach and air travel. However, rail is safer and more environmentally friendly. Rail travel also avoids two future risks: it does not depend on variations in fuel prices and is not affected by road and flight path congestion. In this sense, the future success of international rail is contingent upon the failings of the other modes of transportation.

References

AQST. (2018). Bilan 2017 de la qualité de service des transports de voyageurs en France. http://www.qualitetransports.gouv.fr/IMG/pdf/bilan_annuel_de_la_qualite_de_service_dans_les_transports_28_08_2018.pdf

ARAFER. (2016). Les pratiques de mobilité de longue-distance des voyageurs sur les lignes régulières d'autocar librement organisées. http://www.arafer.fr/wp-content/uploads/2017/01/Enquete-2016-mobilite-des-voyageurs-en-autocar-Arafer.pdf

ARAFER. (2018). Marché du transport par autocar et gares routières. http://www.arafer.fr/wp-content/uploads/2018/07/rapport-annuel-sur-le-transport-routier-de-voyageurs-et-gares-routieres.pdf

Beauvais Consultants. (2013). Dépenses supportés par les voyageurs selon les différents modes de transport. Etude FNAUT multi-clients. 13 juin. https://www.statistiques.developpement-durable.gouv.fr/memento-de-statistiques-des-transports-2016

DGAC. (2018). Bulletin Statistique.Traffic aérien commercial. https://www.ecologique-solidaire.gouv.fr/sites/default/files/bulletin stat trafic aerien 2018.pdf

European Railway Agency. (2017). Annual Report. SNCF, 2016. https://erail.era. europa.eu/documents/SPR.pdf

Forthoffer, J. (2003). Transport ferroviaire et développement durable?. *Les Cahiers Nantais* (60), 133–140.

INSEE. (2018). Tableau de l'économie française. Collection Insee Références. Chapitre20.6. https://www.insee.fr/fr/statistiques/3303636?sommaire=3353488

Klein, O., & Claisse, G. (1997). *Le TGV-Atlantique : entre récession et concurrence, Etudes et Recherches*. Lyon: LET.

OMT. (2017). Faits saillants OMT du tourisme. https://www.e-unwto.org/doi/pdf/10.18111/9789284419050

IRG-Rail. (2015). Third Annual Market Monitoring Report 2014. https://www.irg-rail.eu/irg/documents/market-monitoring/39,2015.html

SDES. (2016). Enquête annuelle sur les transports collectif urbains.

SNCF. (2016). Les spécificités du transport ferroviaire. https://www.lnobpl.fr/sites/lnobpl.fr/files/telechargements/documents/mediatheque/NotespecificitéduferroviaireLNOBPL.pdf

Sippel, L., Nolte, J., Maarfield, S., Wolff, D., & Roux, L. (2018, March). Comprehensive analysis of the existing cross-border rail transport connections and missing links on the internal EU borders.

Spinetta, J. C. (2018). L'avenir du Transport ferroviaire. *Rapport remis au premier ministre Édouard Philippe le 15*.

von Arx, W., Thao, V. T., Wegelin, P., Maarfield, S., & Frölicher, J. (2018). The development of international passenger rail services from 2007 to 2016: The case of Switzerland. *Research in Transportation Economics, 69*, 326–336.

Chapter 3
Overview ERTMS/ETCS Baseline 3 and Beyond

Patrick Deutsch

3.1 Introduction

The purpose of the document is to describe the evolution of the ERTMS/ETCS specifications, starting from the first stable Baseline, i.e. Baseline 2. The various functions introduced in Baseline 3 for the two current versions (B3 MR1 and B3 R2) are briefly described. There will be in the future (planned in 2022) a new version of the specifications, which will introduce a variety of new functions, known to be the game changers. Errors detected in the current specifications will also lead to changes in the specifications. Moreover, there are also several European projects emerging with the ambition to improve the ERTMS/ETCS specifications and thus facilitate the deployment of ERTMS/ETCS in Europe.

In several parts of the document, the term "Agency" is used. The meaning of "Agency" in this context is "EU Agency for Railways".

This document is only an overview of several topics. To get more precise and detailed information, the reader shall look at Sect. 3.18.

3.1.1 Structure of the Document

The document starts with a general introduction about the main concepts: TSI, system version, definition of a Baseline and the process related to the introduction of Change Requests (CR) within a specification.

P. Deutsch (✉)
ERTMS, Clearsy, Strassbourg, France
e-mail: patrick.deutsch@clearsy.com

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_3

Then the various CRs, starting from Baseline 2 will be listed:

- CRs from 2.3.0d to 3.0.0;
- CRs from 3.0.0 to 3.4.0, leading to Baseline 3 Maintenance Release # 1;
- CRs from 3.4.0 to 3.6.0, leading to Baseline 3 Release # 2.

Article 10 (error CRs) and the Game Changers are briefly described.

In the latest sections of the document, the various projects which are using and influencing the specifications are described.

3.2 Technical Specification for Interoperability (TSI)

3.2.1 Introduction

The Technical Specifications for Interoperability (TSIs) define the technical and operational standards to be met by each subsystem or part of subsystems in order to meet the essential requirements and ensure the interoperability of the railway system of the European Union.

Directive (EU) 2016/797 defines the subsystems, either structural or functional, forming part of the railway system of the European Union.

For each of those subsystems, the essential requirements need to be specified and the technical specifications determined, particularly in respect of constituents and interfaces, in order to meet those essential requirements. The essential requirements can be summarised as safety, reliability and availability, health, environmental protection, technical compatibility and accessibility.

3.2.2 Control-Command and Signalling TSI

This TSI concerns the control-command and signalling on-board and trackside subsystems. It applies to control-command and signalling on-board subsystems of vehicles which are operated on and control-command and signalling trackside subsystems of the rail network of the European Union.

Different ERTMS baselines, as specified in Annex A to the TSI CCS, may coexist in vehicles and trackside equipment:

1. ETCS baseline 2 and GSM-R baseline 1;
2. ETCS baseline 3 maintenance release 1 (MR1) and GSM-R baseline 1, correcting numerous errors in ETCS baseline 2 and adding new functionalities;
3. ETCS baseline 3 release 2 (R2) and GSM-R baseline 1, with the inclusion of EGPRS (GPRS with mandatory EDGE support) in the GSM-R specification and

the correction of errors to ensure backwards and forwards compatibility with ETCS baseline 3 MR1.

Each baseline includes a set of **mandatory ERTMS specifications** (e.g. Subset-026) and a set of **informative ERTMS specifications**.

Backwards compatibility is also provided between vehicles equipped with ETCS baseline 3 and trackside equipped with ETCS baseline 2. More info on backwards and forwards compatibility of ETCS baselines can be found in Sect. 8.3.

3.3 ERTMS/ETCS System Version

3.3.1 Definitions

The system version defines unambiguously the ETCS mandatory functions that ensure technical interoperability between ERTMS/ETCS on-board and trackside subsystems. The system version is used to prevent situations leading to an unacceptable reduction of safety or performance, due to changes in the ERTMS/ETCS specifications.

Therefore, any technical change having the potential to change the behaviour, the performance or the safety of the ERTMS/ETCS system shall be considered as impacting the system version. Note: as a matter a fact, the version number of the SRS is incremented each time there is a new system version, at least because the definition of the variable M_VERSION (in SRS Chap. 7) has to be changed.

The system version can potentially be impacted by several of the mandatory specification documents which are listed in the TSI Annex A: SUBSET-026, SUBSET-035, SUBSET-036, SUBSET-037, SUBSET-040, SUBSET-041, SUBSET-044, SUBSET-047, SUBSET-048, SUBSET-091, EIRENE FRS, EIRENE SRS, A11T6001.

3.3.2 Identification/Evolution of System Versions

The version of the ERTMS/ETCS system is identified by a number which complies with the following:

- Each version number has the following format: X.Y, where X is any number between 1 and 7 and Y is any number between 0 and 15.
- The first number distinguishes incompatible versions.
- The second number indicates compatibility within a version X.

3.3.3 Compatibility Between System Versions

The compatibility/incompatibility between two consecutive ERTMS/ETCS system versions is established by analysing the relationship between an ERTMS/ETCS on-board equipment operating one system version and an ERTMS/ETCS trackside infrastructure operated with the other one.

In the following sections, version A is the existing system version, while version B is the subsequent system version, for which the compatibility/incompatibility is to be determined.

The version B is compatible with version A if both following conditions are met (see Fig. 3.1):

1. a train operating version A can run a normal service on trackside infrastructure operated with version B;
2. a train operating version B can run a normal service on trackside infrastructure operated with version A.

Conversely, the version B is incompatible with version A if one of the following conditions is met (see Fig. 3.2):

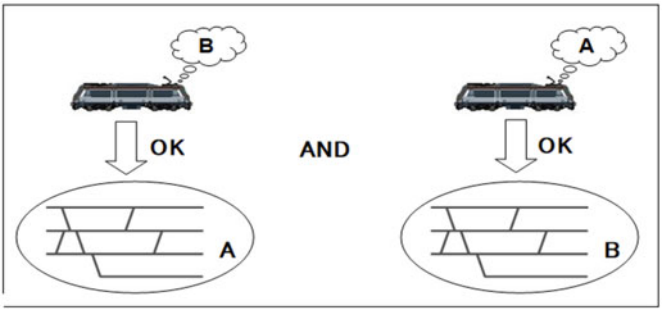


Fig. 3.1 Compatibility of system versions A & B

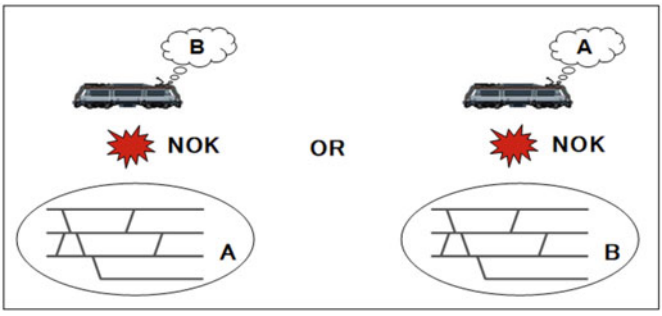


Fig. 3.2 Incompatibility of system versions A & B

1. there is a technical, operational or safety related obstacle preventing a train operating version A from running a normal service on a trackside infrastructure operated with version B;
2. there is a technical, operational or safety related obstacle preventing a train operating version B from running a normal service on a trackside infrastructure operated with version A.

3.3.4 Coexistence of System Versions

Each time any value of the system version number X.Y is incremented, the consequences will be, at a given time:

1. The coexistence of distinct trackside infrastructures operated with different system versions.
2. The existence of trackside infrastructures (e.g. level 2/3 areas) where ERTMS/ETCS constituents transmit information marked with a system version different from the one operated.

If the increments relate to system version number X, then:

1. the on-board equipment must be able to operate with at least two incompatible system versions, in order to run on trackside infrastructures operated with different system version numbers X (see Fig. 3.3);
2. the on-board equipment must be able to interpret (i.e. to translate) information received from trackside constituents, which is marked with a system version different from the one operated in the concerned trackside infrastructure.

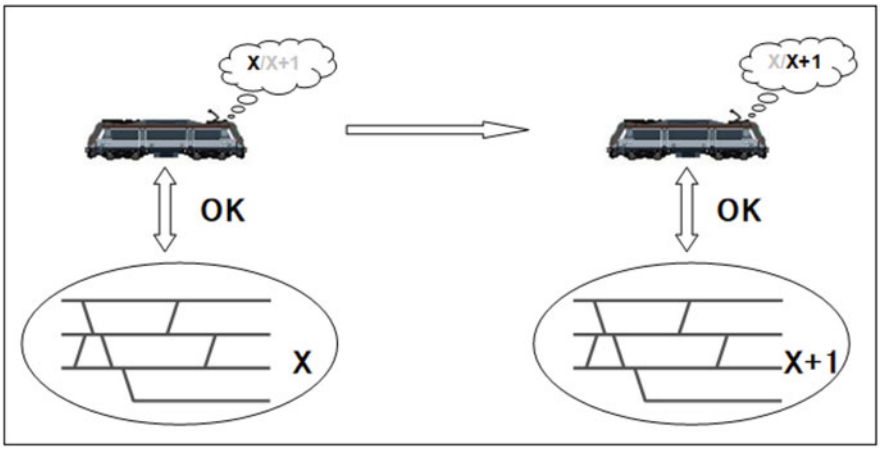


Fig. 3.3 On-board capable to operate with different X system versions

3.4 Baseline

A baseline is defined by a stable kernel in terms of system functionality, performance and other non-functional characteristics.

The definition of a new baseline implies that significant changes are implemented in the above-mentioned kernel: an enhancement may consist in adding a new function, keeping the functionality of the previous baseline unchanged, or may consist in changing some functionality, performance or non-functional characteristics of the previous baseline.

If a system version management exists for the concerned system, the system version number (X.Y) is always incremented when defining a new baseline: in case of X increment only the train to track backward compatibility is ensured, while in case of Y increment, both the train to track forward and backward compatibilities are ensured.

3.4.1 Baseline Release

A baseline release is defined by a specific version of each of the legally binding TSI documents that are relevant for the concerned system. During the whole lifetime of the system, several releases of the same baseline are issued:

1. the first draft release, including the first subset of the documents of a baseline in which an agreed set of changes to the stable kernel of the previous baseline is specified;
2. optionally, several consolidation releases, consisting of intermediate releases in order to progressively build the full and coherent set of documents attached to the baseline;
3. the first legal release, which is enforced in the Official Journal or other publication mean (e.g. Agency's website) once the consolidation phase is completed;
4. further on, one or more maintenance releases published in the Official Journal or other publication mean (e.g. Agency's website). They consist only of errors fixed after the publication of the first legal release.

3.4.2 Change Control Management

The Change Control Management (CCM) consists of the management of activities which allow moving from one baseline release to another one. The Change Requests (CRs) offer a transparent, formal and ordered processing of the changes leading to new releases.

The CCM process defined hereafter is baseline independent, i.e. it is valid for any step made in the lifetime of a given baseline, starting from the last legal release of

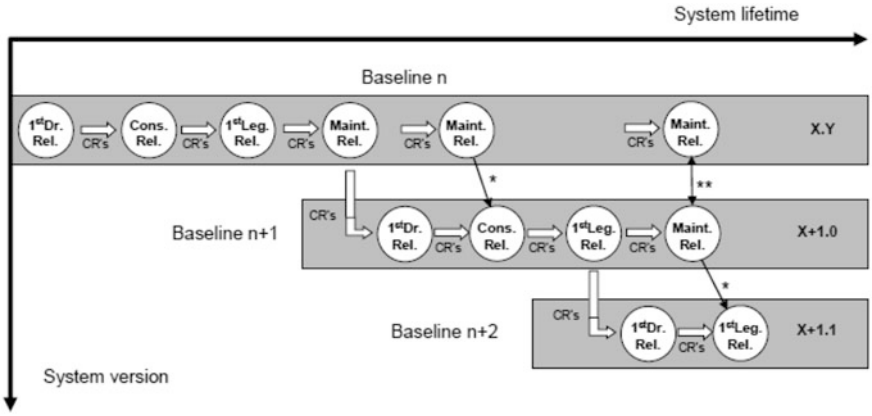


Fig. 3.4 Example of evolution of baselines and baseline releases

the previous baseline to the first draft release, the consolidation release(s), the first legal release and the further maintenance release(s) (see example in Fig. 3.4).

$*$: arrows indicate that updated documents in the maintenance release of a baseline are incorporated in the newer baseline
$**$: synchronised releases in the frame of the maintenance of different baselines

3.5 Organisation of the CCM

3.5.1 Overall Structure

The organisational structure shown in Fig. 3.5 outlines the main information flows and the interactions of the parties involved in the CCM; their tasks and interfaces are briefly described below.

3.5.2 CR Submitter

The following parties can submit a CR:

1. The representative bodies;
2. The National Safety Authorities (representing the Member States);
3. Each Member State;
4. The European Commission;
5. The Agency itself.

The list of representative bodies can be found at the Agency's website: https://www.era.europa.eu/agency/stakeholder-relations/representative-bodies_en.

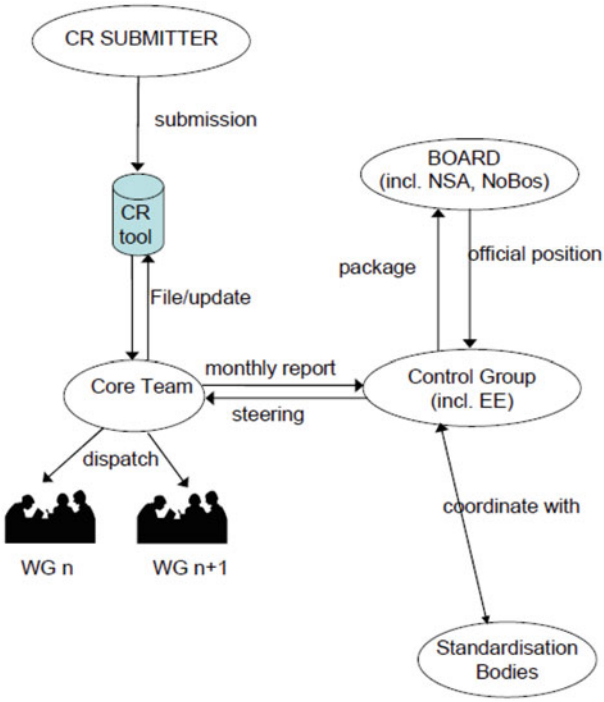


Fig. 3.5 Organisational structure of the CCM

3.5.3 Board

The Board is composed of persons mandated by the representative bodies, of representatives of the Network of National Safety Authorities and players of the Agency.

3.5.4 Control Group

The Control Group can be composed of experts invited by the Agency, of persons mandated by the representative bodies and of Agency staff.

The Control Group ensures the steering of the activities, identifying the most effective actions to deal with the outstanding issues in coherence with the overall system planning, resources and priorities.

Depending on the specific issue, the development of the detailed solution for a CR could entail a significant amount of time/resources. In this case, the Control Group will seek the endorsement of the Board before committing to the additional activities.

The Control Group defines the aggregation of different CRs in packages, proposed for specific baseline release and or deadlines.

The Control Group will submit a CR package to the Board, for endorsement.

3.5.5 Core Team

It is composed of Agency staff members and, when needed, ad-hoc sector representatives providing key system competence.

It receives, filters and classifies the CRs received from the submitters via the ERA CCM tool. To be accepted into the CCM process, the CRs must be formally correct; they are then provisionally assigned to one of the existing technical WGs when possible, and properly filed in the Agency database.

The Core Team reports at each meeting of the Control Group about the current state of the CRs, their progress, the workload of the different technical WGs.

3.5.6 Technical Working Groups

Each technical Working Group comprises external experts and is chaired or followed up by a representative of the Agency staff.

3.5.7 Standardisation Bodies

The Standardisation Bodies mentioned in Fig. 3.5 are the CEN, CENELEC and ETSI. They do not have any direct role or responsibility in the ERA CCM process, but they coordinate with the Control Group, allowing this latter to ensure that:

1. new standards are considered properly;
2. if new standards are needed, the requests are properly initiated and the result of the work verified.

3.6 Change Request Process

The following CR workflow describes the whole life cycle of a Change Request, from its submission to its final acceptance by the Board.

After a package of CRs has been forwarded to the Commission as a supporting part of an Agency recommendation, the further steps until the final approval of the baseline release by EC are not under the control of the Agency. They are therefore not covered by this CR process description.

This CR workflow is applicable to individual CRs only.

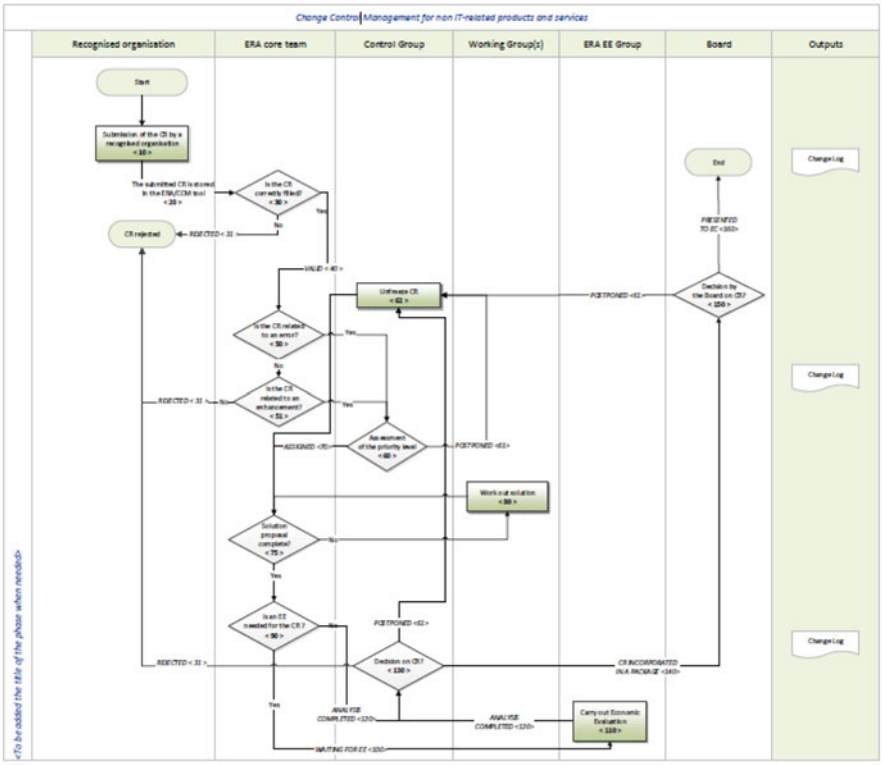


Fig. 3.6 CR workflow

The management of the editorial work for updating the TSI related documents is considered as not being part of the CR process itself, but only a consequence of it (Fig. 3.6).

3.7 Evaluation of a New Baseline

3.7.1 Impact of Changes

When it is envisaged by the ERA CCM to bring changes to the ERTMS/ETCS system, it must be assessed whether they impact the system version and, if yes, whether to increment the system version number X or Y.

Compatibility/incompatibility between two consecutive ERTMS/ETCS system versions is evaluated with regard to a set of agreed CRs.

Each CR from this set shall impact at least one of the TSI annex A documents that are identified as impacting the ERTMS/ETCS system version (see Sect. 3.3).

Each CR, regardless of the number of modifications distributed in the different impacted TSI annex A documents, shall be evaluated as a whole, leading to an individual decision with regard to its compatibility/incompatibility. For that purpose, the definitions given in Sect. 3.3 shall be used by assuming that the CR represents the difference between version B and version A.

If all the evaluated CRs are declared compatible, the new ERTMS/ETCS system version shall be declared compatible with regard to the existing one (Y increment).

If at least one CR, out of the set of evaluated CRs, is declared incompatible, the new ERTMS/ETCS system version shall be declared incompatible with regard to the existing one (X increment).

Note: to avoid incompatibility, the ERA CCM could decide to reassess, postpone or even rework one or more CRs, thus possibly keeping the versions compatible.

3.7.2 Evaluation of a Single CR

See Fig. 3.7.

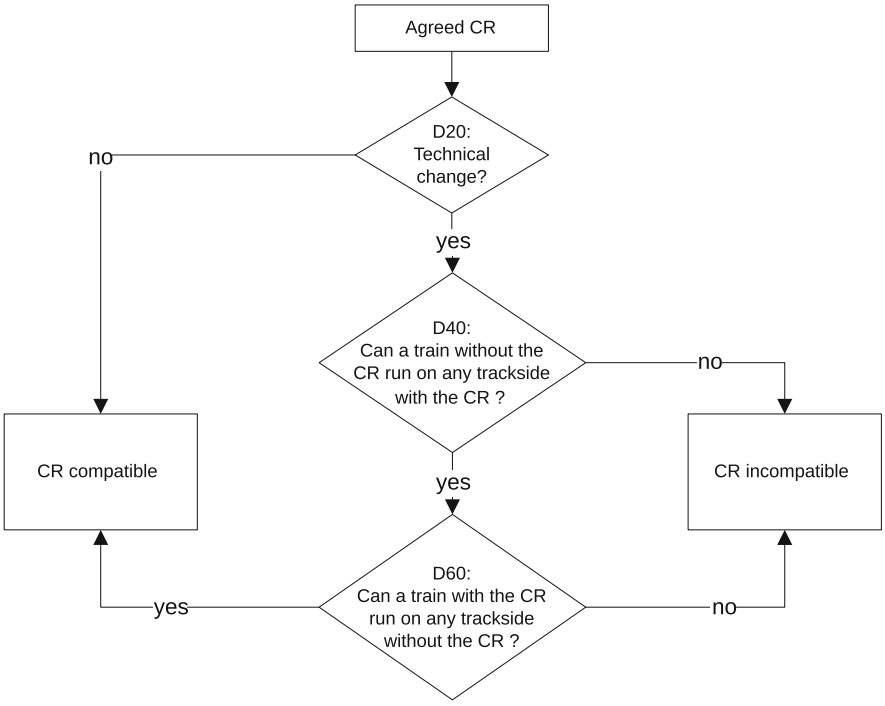


Fig. 3.7 Single CR evaluation

3.7.3 Explanatory Table for Compatibility/Incompatibility Decision Chart

#	Description
D20	If at least one of the modifications decided in the CR affects the behaviour or the implementation of either ERTMS/ETCS on-board or ERTMS/ETCS trackside, the CR shall be identified as a technical change and the process shall go to **D40**. Conversely, if all the modifications brought by the CR are purely editorial (wording) or explanatory, the CR shall be identified as an editorial change and shall be declared as compatible.
D40	A technical change shall be evaluated by addressing the following question: "Can a train without the CR run a normal service on any trackside infrastructure where the CR is implemented?" 1. If there is no technical, operational or safety related obstacle preventing a train without the CR from running a normal service within any trackside infrastructure, the CR shall go to **D60** 2. if there is at least one technical, operational or safety related obstacle, the CR shall be declared as incompatible. Note: to take into consideration operational and safety aspects for all concerned infrastructures is relevant as long as operational and safety rules are not harmonised.
D60	The evaluation shall be continued by addressing the following question: "Can a train with the CR run a normal service on any trackside infrastructure where the CR is not implemented?" 1. If there is no technical, operational or safety related obstacle preventing a train with the CR from running a normal service within any trackside infrastructure, the CR shall be declared as compatible; 2. if there is at least one technical, operational or safety related obstacle, the CR shall be declared as incompatible Note: to take into consideration operational and safety aspects for all concerned infrastructures is relevant as long as operational and safety rules are not harmonised.

3.8 Forwards and Backwards Compatibility

Backwards Compatibility between Baseline 2 and Baseline 3 (Maintenance Release 1—MR1 and Release 2—R2) has been agreed by all stakeholders. This backwards compatibility means that any Baseline 3 R2/MR1 ERTMS on-board subsystem will be able to work with no technical or operational impact on a B3 R2/B3MR1/Baseline 2 ERTMS trackside.

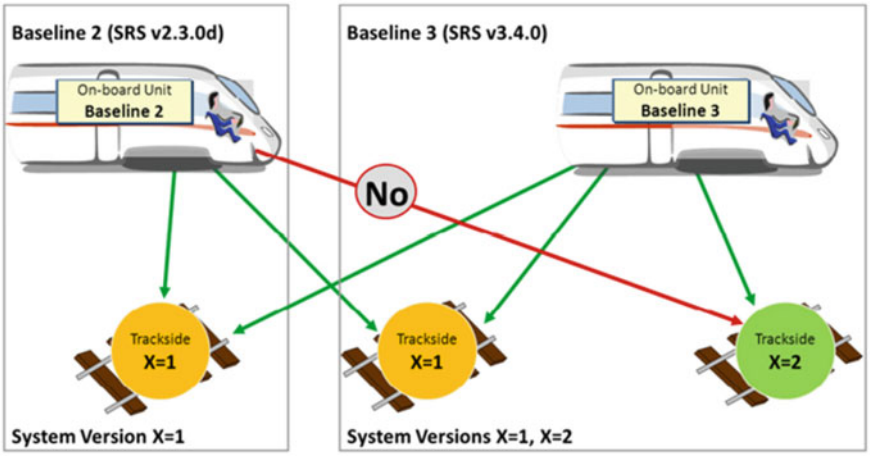


Fig. 3.8 Compatibility/incompatibility between B2 and B3

3.8.1 First Compatibility Assessment

A first baseline compatibility assessment undertaken by the sector (UNIFE/ UNISIG and ERTMS Users Group) has checked the compatibility between ETCS baseline 3 MR1 and ETCS baseline 2 (release 230d) (Fig. 3.8).

Within the scope of this assessment and provided that its recommendations are taken into account, the ETCS baseline 3 MR1 is backwards compatible with ETCS baseline 2.

3.8.2 Second Compatibility Assessment

A second baseline compatibility assessment has checked that:

- ETCS baseline 3 R2 is fully backward/forward compatible with ETCS baseline 3 MR1;
- Both the backward compatibility between ETCS baseline 3 R2 vehicles and ETCS Baseline 2 trackside and the compatibility between ETCS baseline 3 R2 trackside operated with system version X=1 (i.e. ETCS Baseline 3 R2 trackside using only baseline 2 functions) and ETCS baseline 2 vehicles.

The second baseline compatibility assessment also includes the analysis of the compatibility between trackside and on-board both within ETCS baseline 3 MR1 and within ETCS baseline 2, in the light of the problem description of the CRs included in ETCS baseline 3 R2.

This second baseline compatibility assessment confirms that the ETCS baseline 3 R2 is fully backwards and forwards compatible with the ETCS baseline 3 MR1, i.e. that ETCS baseline 3 R2 vehicles can run a normal service on ETCS baseline 3 MR1 trackside and ETCS baseline 3 MR1 vehicles can run a normal service on ETCS baseline 3 R2 trackside.

3.9 From Baseline 2 to Baseline 3

3.9.1 Starting Point: Baseline 2

The starting point is Baseline 2. It is identified by a complete set of stable documents. The documentation includes two types of documents:

- Mandatory: https://www.era.europa.eu/content/set-specifications-1-etcs-b2-gsm-r-b1
- Informative: https://www.era.europa.eu/content/informative-set-specifications-1-etcs-b2-gsm-r-b1

The two main documents in the mandatory part are:

Reference	Version	Issue date	Title
SUBSET-026	2.3.0	24.02.2006	System Requirement Specification
SUBSET-108	1.2.0	17.01.2008	Interoperability-related consolidation on TSI annex A documents

M_VERSION = 001 0000, meaning X.Y = 1.0 (X = 1 Y = 0)

3.9.2 Identified CRs

About 107 CRs have been identified to be part of version 3.0.0.

3.9.3 Main Changes

The main changes introduced in version 3.0.0 are the following:

- Clarification of functions;
- Correction of errors;
- mandatory DMI layout;
- backwards compatibility;
- implementation of braking curves;
- introduction of LS (Limited Supervision) mode;
- introduction of PS (Passive Shunting) mode;
- safety increase of the transition to NL (Non-Leading) mode (new signal from TIU);
- supervision of non-protected level crossings;
- update of train categories;
- new track conditions (current consumption limitation, platforms);
- display of permitted stops in tunnels;
- on-board speed limit calculated from allowed braking distance;
- . . .

3.9.4 Issue Date

Version 3.0.0 of the System Requirement Specification was issued on 23.12.2008.

3.9.5 Architecture

The architecture of the system in baseline 3 can be found (Fig. 3.9).

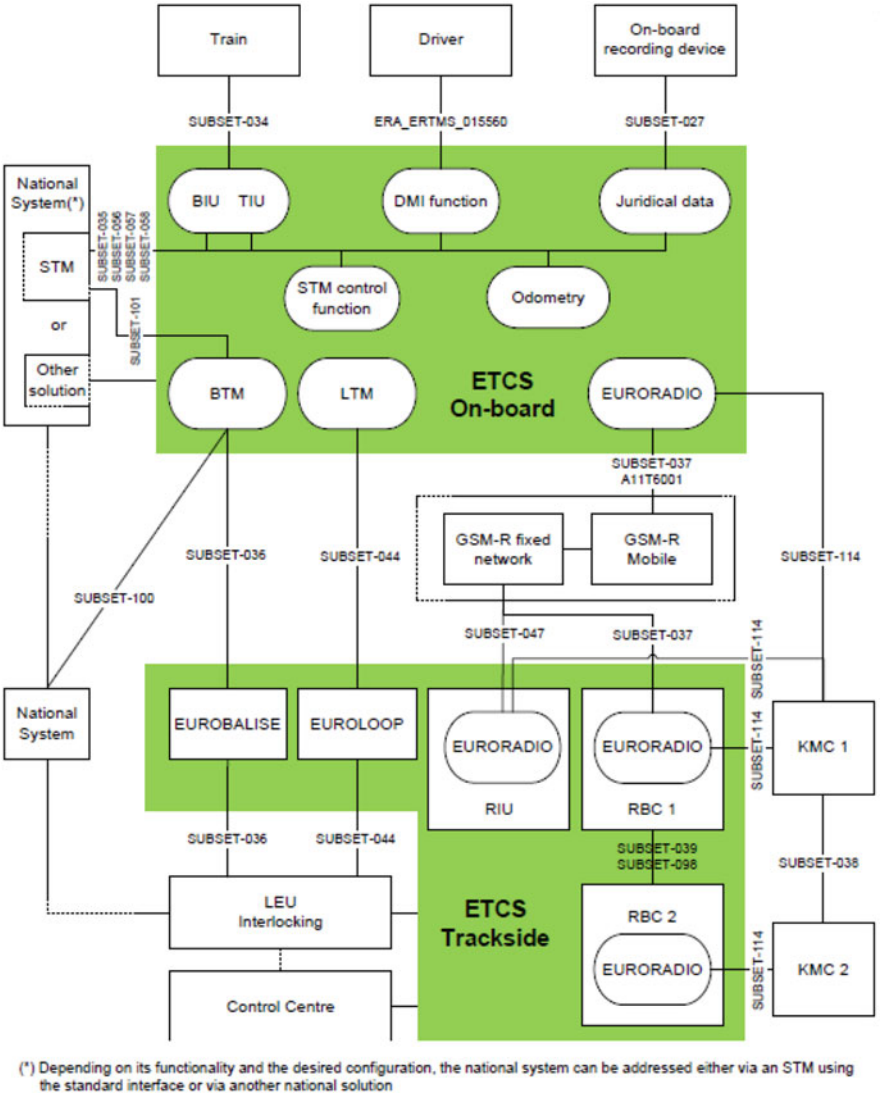


Fig. 3.9 ERTMS/ETCS reference architecture

3.9.6 Summary of CRs from B2 to 3.0.0

CR Id	Headline	Impacted documents
CR 0020	Pending communication session	SUBSET-026
CR 0070	Acknowledgement of STM transitions	SUBSET-26
CR 0123	TSR in L2/L1	SUBSET-026
CR 0124	Passing a signal in SR mode	SUBSET-026
CR 0138	Brakes release after max reversing distance overpassed	SUBSET-026
CR 0170	Indication of track conditions	SUBSET-026 SUBSET-040
CR 0232	Unknown text message	SUBSET-026
CR 0240	JRU changes	SUBSET-027
CR 0241	RBC/RBC interface specification	SUBSET-097 SUBSET-098
CR 0265	Information to driver about reason of train trip	Moved to CR 0760
CR 0284	ETCS accepted information from STM X (SE)	SUBSET-026
CR 0298	Level selection by driver	SUBSET-026
CR 0299	Version compatibility check	SUBSET-026 partly moved to CR 0757
CR 0319	LRBG orientation for special position report	SUBSET-026
CR 0338	Some Errors in Active Functions Table	SUBSET-026
CR 0342	Redefinition of the international train categories	SUBSET-026
CR 0346	List of trackside supported levels	SUBSET-026
CR 0372	FIS EVC - EIRENE Voice Radio	ERA_FFFIS_HaPELv1.pdf ERA_FFFIS_TNTNv1.pdf (creation)
CR 0393	Message “JRU State”	SUBSET-027
CR 0397	Conditions for Start/End of Text Indication	SUBSET-026 SUBSET-040
CR 0410	Shunting in STM areas	SUBSET-026 SUBSET-035
CR 0413	Level crossing modification	SUBSET-026 SUBSET-039 SUBSET-040
CR 0453	National/Default values	SUBSET-026
CR 0481	Supervision of the Radio Link	SUBSET-026

(continued)

CR 0485	Review of SRS by STM WG	SUBSET-026 SUBSET-035
CR 0494	Communication of SR balise list on the RBC/RBC interface	SUBSET-026
CR 0500	Change of Train Data from sources different from the driver	SUBSET-026
CR 0513	Non-Leading mode	SUBSET-026 SUBSET-034
CR 0514	Cold movement detection	SUBSET-026
CR 0535	Door control supervision	SUBSET-026 SUBSET-040 SUBSET-034
CR 0544	Unclear definition of big metal masses	SUBSET-036 Guidelines related to Metallic Masses
CR 0559	Inconsistencies in procedure “Shunting initiated by driver”	SUBSET-026
CR 0583	Indications on DMI in SR/OS mode	SUBSET-026 ERA_ERTMS_015560
CR 0584	STM max speed	SUBSET-035
CR 0593	Awakening on loops	SUBSET-026
CR 0594	Speed definitions	SUBSET-026
CR 0595	Braking curve calculation	SUBSET-026
CR 0601	OS acknowledgement	SUBSET-026
CR 0619	Message Acknowledgement	SUBSET-026
CR 0623	ETCS communication session	SUBSET-026
CR 0637	Limited Supervision	SUBSET-026
CR 0638	Selection of Static Speed Profile according to Train Categories	SUBSET-026
CR 0654	Unsuited wording of variable description	SUBSET-026 SUBSET-040
CR 0656	Follow-up of CR126	SUBSET-026
CR 0657	Unsuitability of RBC-RBC handover procedure in case of radio network change	SUBSET-026
CR 0660	Non ETCS airgap data for STM	SUBSET-026 SUBSET-035 SUBSET-058
CR 0664	Unclear requirements for Route suitability	SUBSET-026
CR 0676	Allowed current consumption	SUBSET-026 SUBSET-034 SUBSET-040
CR 0680	Definition of expectation window	SUBSET-026 SUBSET-023
CR 0686	Ambiguities regarding reversing information in SRS v230	SUBSET-026

(continued)

CR 0689	M_LOADINGGAUGE value 0	SUBSET-026
CR 0692	Subset 040 Consolidation 3/3 (New Rules)	SUBSET-040
CR 0706	Mismatch between announced and read balise group direction	SUBSET-026
CR 0710	Clarify if received but not yet applicable National Values shall be deleted in NP	SUBSET-026
CR 0712	Confusion in packets not transmitted by infill devices	SUBSET-026 SUBSET-040
CR 0713	PT distance D_NVPOTRP origin	SUBSET-026
CR 0719	Ambiguity on Text Message Conditions	SUBSET-026
CR 0729	Single balises, assignment of a coordinate system	SUBSET-026
CR 0732	Follow-up CR151: Eddy current brake switch off	SUBSET-026 SUBSET-034 SUBSET-040
CR 0741	Packet data transmission for ETCS	In order to enable ETCS operation over GPRS, the following standards would require an update: • The ERTMS/ETCS Specifications • FFFIS for EuroRadio • EIRENE Specifications • ETSI GPRS Standards
CR 0742	Change Requests for an optimised use of the Radio Infill function	SUBSET-026
CR 0745	Permitted braking distance	SUBSET-026 SUBSET-039 SUBSET-040
CR 0749	Number of keys per on-board	SUBSET-038 SUBSET-114 SUBSET-040
CR 0751	Start of mission in Level 2	SUBSET-026 A11T6001
CR 0756	Solution for ETCS to pass line sections under construction or refurbishment without isolation of ETCS.	SUBSET-026

(continued)

CR 0757	Insufficient provisions for management of future ERTMS/ETCS system versions	SUBSET-026 SUBSET-104
CR 0758	KMC-ERTMS entity interface specification	08E187-03 ETCS Key Management FRS (new SUBSET to be created)
CR 0760	DMI harmonisation (including data entry)	ERA_ERTMS_015560
CR 0763	Ack feedback to RBC	SUBSET-026
CR 0764	Reconnection time limited	SUBSET-026
CR 0767	Shunting and level transitions	SUBSET-026 SUBSET-040
CR 0768	Harmonised Network Registration	A11T6001
CR 0770	Train category spare values	SUBSET-026 SUBSET-108
CR 0771	Value NID_RBC is unknown	SUBSET-026 SUBSET-040
CR 0778	Geographical position reference balise groups	SUBSET-026
CR 0782	Reset of confidence interval	SUBSET-026
CR 0792	Storage of information in case of level transition announcement or RBC/RBC handover	SUBSET-026
CR 0800	Conditional level transition order overrides normal level transition order	SUBSET-026 SUBSET-023
CR 0804	National value for default location accuracy of balise group	SUBSET-026
CR 0814	Key validity period	05E537-1C *(Off line key management FIS)*
CR 0821	Removal of the STM European from the ETCS specifications	SUBSET-026 SUBSET-108 SUBSET-035
CR 0823	Delete route suitability function	SUBSET-026 SUBSET-027 SUBSET-035 SUBSET-040
CR 0824	Jumping braking curves (follow-up of CR601)	SUBSET-026
CR 0833	Consistency of Subset-039 with Subset-026, Subset-108 and Subset-040	SUBSET-039
CR 0835	Hazard of message deletion on Adjacent RBC interface	SUBSET-039
CR 0849	Configuration data for RBC-RBC Handover	SUBSET-039

(continued)

CR 0858	Inappropriate driver's indications	Postponed
CR 0861	SUBSET-040 update for baseline 2	SUBSET-040
CR 0876	SUBSET-039 update for baseline 2	SUBSET-039
CR 0877	DMI specification update for baseline 3	ERA_ERTMS_015560
CR 0878	Improvements for Passive Shunting (follow-up of CR751)	SUBSET-026
CR 0880	Gaps/inconsistencies in speed/distance monitoring chapter	SUBSET-026
CR 0881	findings from DMI WG (mainly SRS table 4.7.2)	SUBSET-026
CR 0884	Missing train category	SUBSET-026
CR 0885	RRI Confirmation message	SUBSET-039
CR 0894	Driver selection of Level in SoM opens second radio session	SUBSET-026
CR 0895	Unintended extension of the permitted distance to run in Reversing due to filtering of info On-board.	SUBSET-026
CR 0897	End Section/Overlap Timer	SUBSET-026
CR 0899	Replacement of track description and linking information	SUBSET-026
CR 0900	Fixed text messages	ERA_ERTMS_015560
CR 0901	Braking curves correction factors	SUBSET-026
CR 0902	Conversion model and brake build up time related issues	SUBSET-026
CR 0903	Driver confirmation of Train Data received from External Sources	SUBSET-026
CR 0904	V_LOA for STM	SUBSET-035
CR 0906	Findings from SRS 3.0.0 editorial review	SUBSET-026

3.10 Within B3: From 3.0.0 to 3.2.0

3.10.1 Identified CRs

About 72 CRs have been identified to be part of version 3.2.0.

3.10.2 Main Changes

The main changes introduced in version 3.2.0 are the following:

- Clarification of functions;
- Correction of errors;
- Improvement of braking curves;
- ...

3.10.3 Date of Issue

Version 3.1.0 of the System Requirement Specification was issued on 22.02.2010.
Version 3.2.0 of the System Requirement Specification was issued on 22.12.2010.

3.10.4 Summary of CRs from 3.0.0 to 3.2.0

CR Id	Headline	Impacted documents
CR 0680	Definition of expectation window	SUBSET-026 SUBSET-023
CR 0689	M_LOADINGGAUGE value 0	SUBSET-026, ERA_ERTMS_015560
CR 0712	Confusion in packets not transmitted by infill devices	SUBSET-026, SUBSET-040
CR 0731	Inconsistencies between SRS chapter 7 and SUBSET-054	SUBSET-026, SUBSET-027, SUBSET-039, SUBSET-040, ERA_ERTMS_015560
CR 0733	Button protection	SUBSET-026
CR 0802	Controversial on-board implementations	SUBSET-026, SUBSET-027, SUBSET-034, SUBSET-035, SUBSET-036, SUBSET-040, SUBSET-041, SUBSET-054, SUBSET-091, SUBSET-094, ERA_ERTMS_015560, ERA_ERTMS_003204
CR 0809	Direction of balise arrows in figures	SUBSET-026, SUBSET-035, SUBSET-039
CR 0828	Add language as stored information	SUBSET-026

(continued)

CR 0842	Activation of supervision of safe radio connection /Follow-up 787	SUBSET-026
CR 0844	Unspecified train movement supervision after PT or RV distance is overpassed	SUBSET-026
CR 0847	Handling of direction dependent data from RBC without coordinate system	SUBSET-026
CR 0866	Entry into Level 2 questions	SUBSET-026
CR 0873	Discrepancies between Level and RBC id/phone number selections	SUBSET-026
CR 0878	Improvements for Passive Shunting (follow-up of CR751)	SUBSET-026 ERA_ERTMS_015560 SUBSET-034
CR 0897	End Section/Overlap Timer	SUBSET-026
CR 0899	Replacement of track description and linking information	SUBSET-026
CR 0907	Hazardous brake command in RV	SUBSET-026
CR 0909	New text message to be confirmed with the same ID (Follow-up CR763	SUBSET-026
CR 0910	Location dependent Speed Restrictions to be deleted behind the train rear (Follow-up of CR798)	SUBSET-026
CR 0911	Contradictions in the display of track conditions (Follow-up of CR170)	SUBSET-026
CR 0912	Train speed in position report	SUBSET-026
CR 0913	Misleading remarks in message description	SUBSET-026 SUBSET-023
CR 0914	Missing repeat condition	SUBSET-026 ERA_ERTMS_015560
CR 0915	Start/End conditions for SoM	SUBSET-026 ERA_ERTMS_015560
CR 0916	Traceability 4.7.2	SUBSET-026
CR 0917	Display of permitted speed in RV	SUBSET-026 ERA_ERTMS_015560
CR 0918	Clause 5.8.2.1 a) vs a speed limit for triggering the override function equal to 0	SUBSET-026 ERA_ERTMS_015560

(continued)

CR 0919	Rejection of List of balises for SH area, error in solution of CR 650	SUBSET-026 SUBSET-040
CR 0922	Reduce 5 min on loss of connection	SUBSET-026 ERA_ERTMS_015560
CR 0924	Inappropriate definition of the speed monitoring	SUBSET-026
CR 0925	Missing transition from TR mode	SUBSET-026
CR 0927	Safe speed supervision for calculation of EBI	SUBSET-026 SUBSET-023 SUBSET-041 SUBSET-091
CR 0928	Driver's indication of brake command(s)	SUBSET-026
CR 0929	Indication of the reasons of non-stopping areas	SUBSET-026
CR 0942	Requirement for text display ambiguous in case start and end conditions are fulfilled	SUBSET-026
CR 0943	Standstill while capturing data	SUBSET-026 ERA_ERTMS_015560
CR 0945	Incorrect SoM start condition	SUBSET-026 ERA_ERTMS_015560
CR 0946	Train category 210 mm cant deficiency	SUBSET-026 ERA_ERTMS_015560
CR 0947	Data view for fixed train data entry	SUBSET-026 ERA_ERTMS_015560
CR 0948	Change of Driver ID in SH mode	SUBSET-026 ERA_ERTMS_015560
CR 0949	"Balise read error" indication in NL mode	SUBSET-026 ERA_ERTMS_015560
CR 0951	Train Data entry mechanism	SUBSET-026 ERA_ERTMS_015560
CR 0953	Train related speed restriction	SUBSET-026 SUBSET-079-1&2 SUBSET-035 SUBSET-058 SUBSET-74-3
CR 0955	Availability for use of level 2/3	SUBSET-026
CR 0956	Override when override is active	SUBSET-026
CR 0957	Overlapping of CR solutions	SUBSET-026
CR 0958	Ambiguous exception	SUBSET-026
CR 0959	Braking curve problems	SUBSET-026

(continued)

CR 0961	Standardised balise IDs for LS projects	SUBSET-026 SUBSET-054
CR 0963	Ambiguities in case of shortening of MA to the current position of the train	SUBSET-026
CR 0964	Computation of distances displayed on the planning information	SUBSET-026
CR 0965	Inconsistency in LS–>OS and OS–>LS transitions	SUBSET-026
CR 0966	Inconsistencies related to Track Conditions “Door Control” and “Current Consumption”	SUBSET-026
CR 0969	Clarification chapter 6 table headings	SUBSET-026
CR 0972	Safe areas management	SUBSET-026 ERA_ERTMS_015560
CR 0976	Isolation mode inconsistency	SUBSET-026
CR 0986	Start of Reversing movement	SUBSET-026
CR 0989	Unclear LX icon display conditions	SUBSET-026
CR 0995	Feedback from the review of document for early implementation of braking curves in baseline 2	SUBSET-026
CR 0996	Service brake build up time	SUBSET-026
CR 1000	Sound horn	SUBSET-026 ERA_ERTMS_015560
CR 1001	Editorial improvements to procedure	SUBSET-026
CR 1002	M_NVEBCL=0 (follow-up CR901)	SUBSET-026
CR 1003	Miscellaneous editorial findings in SRS 3.1.0	SUBSET-026
CR 1004	Wrong definition for M_AXLELOAD	SUBSET-026 ERA_ERTMS_015560
CR 1008	Inconsistency between clauses 3.18.3.8 and A3.6.2.1	SUBSET-026
CR 1009	Ambiguity in conditional transition order: can it be sent by an RBC or not	SUBSET-026

(continued)

CR 1015	Unsuitability of non-stopping areas announcement mechanism	SUBSET-026 ERA_ERTMS_015560
CR 1018	Obtaining list of available networks	SUBSET-026 ERA_ERTMS_015560 SUBSET-037 SUBSET-092-1 A11T6001
CR 1019	System version management in reversing	SUBSET-026 SUBSET-040
CR 1020	Unnecessary brake reaction at SoM	SUBSET-026 SUBSET-040 SUBSET-091
CR 1022	Communication Session/Safe radio connection request in radio hole	SUBSET-026

3.11 Within B3: From 3.2.0 to 3.3.0

3.11.1 Identified CRs

About 30 CRs have been identified to be part of version 3.3.0.

3.11.2 System Version

Introduction of new values of M_VERSION:
M_VERSION = 001 0001, meaning X.Y = 1.1 (X = 1 Y = 1)
M_VERSION = 010 0000, meaning X.Y = 2.0 (X = 2 Y = 0)

3.11.3 Main Changes

The main changes introduced in version 3.3.0 are the following:

- Clarification of functions;
- Correction of errors;
- Improvement of braking curves;
- Removal of FRS from TSI;
- . . .

3.11.4 Date of Issue

Version 3.3.0 of the System Requirement Specification was issued on 07.03.2012.

3.11.5 Summary of CRs from 3.2.0 to 3.3.0

CR Id	Headline	Impacted documents
CR 0752	ERTMS-reference architecture	SUBSET-026 SUBSET-091 ERA_ERTMS_015560
CR 0772	Overlap between SRS and Subset 027	SUBSET-026 0SUBSET-027
CR 0818	ETCS-STM Header Issue	SUBSET-026
CR 0904	V_LOA for STM	SUBSET-026 SUBSET-035 SUBSET-058
CR 0923	Danger for SH in level 0 and STM	SUBSET-026
CR 0977	Impact of message processing time	SUBSET-026 SUBSET-040 SUBSET-041
CR 0992	LUC completion	SUBSET-023 SUBSET-026 SUBSET-027 SUBSET-040 ERA_ERTMS_015560
CR 1024	Maximum value for M_POSITION	SUBSET-026
CR 1025	Missing condition for start in SR	SUBSET-026
CR 1027	Change of Train Data in RV mode	SUBSET-026
CR 1030	Reduced adhesion areas	SUBSET-026
CR 1032	Management of Balises transmitting system version number X equal to 0	SUBSET-026
CR 1036	Unclarities regarding the ETCS function change of traction system	SUBSET-026 SUBSET-040 ERA_ERTMS_015560
CR 1038	Mismanagement of Packet 39 in B3	SUBSET-026
CR 1050	Inconsistency regarding ack for SR mode	SUBSET-026
CR 1053	Trip situation is reported by STM	SUBSET-026 SUBSET-035
CR 1068	STM National Trip Procedure use for ETCS DMI Shunting and Level buttons	SUBSET-026 SUBSET-035 ERA_ERTMS_015560

(continued)

CR 1079	Inconsistent definition of leaving the indication status	SUBSET-026
CR 1092	Errors in formula for release speed calculation	SUBSET-026
CR 1096	Unclear brake release conditions after an unwanted further movement in PT/RV mode	SUBSET-026 ERA_ERTMS_015560
CR 1097	Miscellaneous editorial findings in SRS&DMI spec 3.2.0	SUBSET-026 ERA_ERTMS_015560
CR 1098	Handling of "No track conditions will be received" message in NL mode	SUBSET-026 ERA_ERTMS_015560
CR 1108	ETCS FRS removal from TSI annex A	Removal of document
CR 1121	Unsafe handling of track conditions inhibiting special brakes	SUBSET-026
CR 1131	Unnecessary reset of V_NVLIMSUPERV	SUBSET-026
CR 1133	Tunnel stopping area functionality on B2 lines	SUBSET-026 SUBSET-040 SUBSET-039
CR 1135	SUBSET-023 upgrade to baseline 3	SUBSET-023 SUBSET-026
CR 1140	Translation of M_AXLELOAD in SRS chapter 6	SUBSET-026
CR 1141	Conversion model for long trains	SUBSET-026
CR 1143	Freezing of ETCS variables not reflected in chapter 6	SUBSET-026

3.12 Within B3: From 3.3.0 to 3.4.0

3.12.1 Identified CRs

About 24 CRs have been identified to be part of version 3.4.0.

3.12.2 Main Changes

The main changes introduced in version 3.4.0 are the following:

- Clarification of functions;
- Correction of errors;

- Improvement of braking curves;
- Major changes to LS mode;
- . . .

3.12.3 Issue Date

Version 3.4.0 of the System Requirement Specification was issued on 06.05.2014. This version is stable, identified as Baseline 3 Maintenance Release 1 (B3 MR1). The documentation includes two types of documents:

- CCS TSI Annex A—Mandatory specifications: https://www.era.europa.eu/content/set-specifications-2-etcs-b3-mr1-gsm-r-b1
- CCS TSI Application Guide—Informative specifications: https://www.era.europa.eu/content/informative-set-specifications-2-etcs-b3-mr1-gsm-r-b1

3.12.4 Summary of CRs from 3.3.0 to 3.4.0

CR Id	Headline	Impacted documents
CR 0944	Data unit/resolution/size	SUBSET-026 SUBSET-040 ERA_ERTMS_015560
CR 1088	Subset-039 upgrade to Baseline 3	SUBSET-039
CR 1104	Subset-094 upgrade to baseline 3	SUBSET-094
CR 1109	error non-stopping areas (Follow-up CR 1015)	SUBSET-026
CR 1124	Findings on SRS section 3.13 "Speed and distance monitoring"	SUBSET-023 SUBSET-026 SUBSET-027 ERA_ERTMS_015560
CR 1127	Non convergence of the release speed calculated on-board	SUBSET-026
CR 1147	DMI text message handling	ERA_ERTMS_015560
CR 1148	Trigger of specific NTC data entry	SUBSET-035 SUBSET-074
CR 1149	Alignment of PBD SR requirements with the new braking curve model	SUBSET-026
CR 1150	Incomplete V_MRSP definition vs train position	SUBSET-026
CR 1151	Error in Subset-037 Table 11	SUBSET-037
CR 1153	Train interface passive shunting input simplification	SUBSET-034

(continued)

CR 1154	Train interface - clarification of isolation output	SUBSET-034
CR 1155	CR712 follow-up: packets sent as non-infill information from infill device	SUBSET-026 SUBSET-040
CR 1157	SUBSET-076 upgrade to Baseline 3	SUBSET-076
CR 1158	SUBSET-074 upgrade to Baseline 3	SUBSET-074
CR 1159	Missing train-to-track message specification for RBC X=1	SUBSET-026 SUBSET-039
CR 1168	Unspecified ACC RBC behaviour when receiving new pre-announcement messages in ongoing transaction	SUBSET-039
CR 1173	Miscellaneous problems with STM specifications	SUBSET-027 SUBSET-035 SUBSET-058 ERA_ERTMS_015560
CR 1176	Feedback on SRS chapter 6 from Baselines compatibility assessment	SUBSET-026 SUBSET-040
CR 1183	Unclear use of telegram header info when a balise telegram or BG message is ignored/rejected	SUBSET-026
CR 1185	Miscellaneous editorial findings in SRS&DMI spec 3.3.0	SUBSET-026 ERA_ERTMS_015560
CR 1223	Display in Limited Supervision	SUBSET-023 SUBSET-026 SUBSET-027 SUBSET-040 ERA_ERTMS_015560
CR 1231	Miscellaneous editorial findings in SUBSET-027 v3.0.0	SUBSET-027

3.13 Within B3: From 3.4.0 to 3.5.0

3.13.1 Identified CRs

About 55 CRs have been identified to be part of version 3.5.0.

3.13.2 System Version

Introduction of a new value of M_VERSION:
M_VERSION = 001 0001, meaning X.Y = 1.1 (X = 1 Y = 1)
M_VERSION = 010 0001, meaning X.Y = 2.1 (X = 2 Y = 2)

3.13.3 Main Changes

The main changes introduced in version 3.4.0 are the following:

- Clarification of functions;
- Correction of errors;
- Improvement of braking curves;
- Set speed indication;
- Suppression of the pre-indication;
- ...

3.13.4 Issue Date

Version 3.5.0 of the System Requirement Specification was issued on 18.12.20115.

3.13.5 Summary of CRs from 3.4.0 to 3.5.0

CR Id	Headline	Impacted documents
CR 0239	Train data on TIU	SUBSET-026 SUBSET-034
CR 0299	Version compatibility check	SUBSET-023 SUBSET-026 SUBSET-039 SUBSET-104
CR 0539	Set speed indication for driver	SUBSET-023 SUBSET-026 SUBSET-027 SUBSET-034 ERA_ERTMS_015560
CR 0740	Unclear requirements concerning functions active in L2/L3 only	SUBSET-026
CR 0741	Packet data transmission for ETCS	SUBSET-037 EIRENE SRS A11T6001
CR 0852	Definition of level 2/3 area and level transition border	SUBSET-023 SUBSET-026

(continued)

CR 0933	Storing of RBC contact information	SUBSET-026
CR 1014	Duplicated balises ambiguities	SUBSET-026
CR 1033	Disable Start in SR if no safe connection	SUBSET-026 ERA_ERTMS_015560
CR 1084	Target speed masking	SUBSET-026 SUBSET-023
CR 1086	Unknown L1 LRBG reported to RBC	SUBSET-026
CR 1087	Manual network selection	SUBSET-026 SUBSET-027 ERA_ERTMS_015560
CR 1089	Ack for text messages in NL mode	SUBSET-026
CR 1091	Insufficient driver information in OS	SUBSET-026 ERA_ERTMS_015560
CR 1094	Unclear stop conditions for display of some DMI objects	SUBSET-026 SUBSET-035 ERA_ERTMS_015560
CR 1107	Status planning information on the DMI in FS mode	SUBSET-026 ERA_ERTMS_015560
CR 1117	Reception of an order to terminate a communication session while session is being established	SUBSET-026
CR 1122	Communication session establishment to report change to SL mode	SUBSET-026
CR 1125	Clarification of human role in ETCS safety analysis	SUBSET-091
CR 1129	DMI indication of level announcement in SB	SUBSET-026
CR 1152	Avoid increase of permitted speed and target distance	SUBSET-026
CR 1163	Train interface—Track conditions related outputs to be harmonised	SUBSET-023 SUBSET-026 SUBSET-027 SUBSET-034 SUBSET-040
CR 1164	Ambiguity in assignment of coordinate system	SUBSET-026
CR 1167	Juridical data for the equivalent brake build up time	SUBSET-027
CR 1169	Ambiguity about the variable L_STMPACKET in juridical data STM INFORMATION	SUBSET-027
CR 1172	Problems related to level crossing supervision	SUBSET-026

(continued)

CR 1180	Guard rails and cables in the vicinity of balises	SUBSET-036
CR 1184	Missing requirement for the number of communication sessions an OBU must be capable to handle simultaneously	.SUBSET-026 EIRENE FRS EIRENE SRS
CR 1187	Indication marker inconsistency	SUBSET-026 ERA_ERTMS_015560
CR 1188	Balises in Multi-Rail Track	SUBSET-036
CR 1190	UES text message end condition	SUBSET-026 ERA_ERTMS_015560
CR 1197	Ambiguity regarding the temporary EOAs and SvLs	SUBSET-026 ERA_ERTMS_015560
CR 1213	SUBSET-091 upgrade to Baseline 3 Release 2 (B3R2)	SUBSET-091
CR 1221	Availability of Override and Start buttons	SUBSET-026 ERA_ERTMS_015560
CR 1222	Inconsistency regarding list of BGs for SH area	SUBSET-026
CR 1229	Age requirement for estimated speed	SUBSET-041
CR 1236	Criteria for Levels in train unclear	SUBSET-026
CR 1237	KMS evolution	SUBSET-137 SUBSET-023 SUBSET-026 SUBSET-104 SUBSET-038 SUBSET-114
CR 1242	Several problems with STM specifications	SUBSET-035 SUBSET-057 SUBSET-058 SUBSET-059 ERA_ERTMS_015560
CR 1245	Display of ETCS override in level NTC	SUBSET-026 ERA_ERTMS_015560
CR 1249	Problems with pre-indication	SUBSET-026 SUBSET-027 ERA_ERTMS_015560
CR 1250	Incorrect description in gradient profile	SUBSET-026
CR 1254	Session establishment attempts to report mode change	SUBSET-026
CR 1255	Impossibility to transmit unknown values in the message “Additional data”	SUBSET-027

(continued)

CR 1260	Inconsistent set of clauses regarding the service brake interface in SH mode	SUBSET-023 SUBSET-026 SUBSET-027
CR 1262	Issues related to the initiation of a communication session by an RBC	SUBSET-026 SUBSET-037 EIRENE FRS EIRENE SRS A11T6001
CR 1265	Miscellaneous editorial findings in B3 MR1	SUBSET-026 ERA_ERTMS_015560 SUBSET-027 SUBSET-034 SUBSET-035 SUBSET-036 SUBSET-037 SUBSET-039 SUBSET-091
CR 1266	Classification of SRS clauses	SUBSET-026
CR 1273	Impact of UIC 544-1 new version	SUBSET-026 SUBSET-040
CR 1275	Eurobalise transmission susceptibility requirements not linked to interoperability	SUBSET-036
CR 1277	D7 of SoM procedure is reached while no Mobile Terminal is registered yet	SUBSET-026 ERA_ERTMS_015560
CR 1278	SUBSET-074 upgrade to Baseline 3 Release 2 (B3R2)	SUBSET-074-2
CR 1280	System version number increment for B3R2	SUBSET-026 SUBSET-039

3.14 Within B3: From 3.5.0 to 3.6.0

3.14.1 Identified CRs

Two CRs have been identified to be part of version 3.6.9.

3.14.2 Issue Date

Version 3.6.0 of the System Requirement Specification was issued on 13.05.2016. This version is stable, identified as Baseline 3 Release 2 (B3 R2).
The documentation includes two types of documents:

- CCS TSI Annex A—Mandatory specifications: https://www.era.europa.eu/ content/set-specifications-3-etcs-b3-r2-gsm-r-b1

- CCS TSI Application Guide—Informative specifications: https://www.era.europa.eu/content/informative-set-specifications-3-etcs-b3-r2-gsm-r-b1

3.14.3 Summary of CRs from 3.5.0 to 3.6.0

CR Id	Headline	Impacted documents
CR 1283	Inconsistent use of the terms EOA and LOA	SUBSET-023 SUBSET-026 SUBSET-040 SUBSET-041 SUBSET-091
CR 1284	SUBSET-092 upgrade to Baseline 3 Release 2 (B3R2)	SUBSET-092-1 SUBSET-092-2

3.15 Beyond Baseline 3 R2

3.15.1 Article 10

The Commission Regulation (EU) 2016/919 enforcing Baseline 3 Release 2 (B3R2) of the ERTMS/ETCS specifications states in its article 10 that: *"If errors that do not allow the system to provide a normal service are detected, the Agency shall publish as early as possible the respective solutions to correct them as well as the evaluation of their impact in the compatibility and stability of the existing ERTMS deployment. Within one year of the date of application of this Regulation, the Agency shall send to the Commission a technical opinion on the state of the findings logged in the ERTMS Change Request Database. The Commission shall analyse the technical opinion, assisted by the committee referred to in Article 29(1) of Directive 2008/57/EC. As set out in the second paragraph of Article 7 of Directive 2008/57/EC, if these errors do not justify immediate revision, the Commission may recommend that the technical opinion be used pending the review of the TSI"* .

3.15.2 Identified Error CRs

A number of error CRs (18) have been identified by the Agency since the enforcement of B3R2. Solutions have been sought for errors preventing normal service.

A compatibility analysis took place: on the one hand between a "B3R2 + Art10SP" trackside and an on-board compliant with an existing baseline (B3R2, B3MR1 or B2) and on the other hand between a "B3R2 + Art10SP" on-board and a trackside compliant with an existing baseline (B3R2, B3MR1 or B2).

3.15.3 New List of Error CRs

In addition to this first list related to Article 10, a new list of error CRs with their solutions has been published by the Agency on their website in spring 2020. Some solutions from the first list have been updated as well.

3.15.4 Summary of (Known) Error CRs Beyond 3.6.0

CR Id	Headline	Impacted documents
CR 0887	Position Report Consistency (Follow-up of CR556)	SUBSET-026
CR 0940	Minimum Safe Rear End position and position reporting ambiguities	SUBSET-026 ERA_ERTMS_015560 SUBSET-027 SUBSET-034 SUBSET-039
CR 0994	Text message start conditions	SUBSET-026
CR 1120	Uncertain handling of some infill information	SUBSET-026 SUBSET-040
CR 1146	Euroradio HDLC parameters	SUBSET-037
CR 1166	Ambiguities in driver acknowledgement requirements	SUBSET-026 SUBSET-027 ERA_ERTMS_015560
CR 1170	Ambiguity about the list of traction systems accepted by a diesel engine	SUBSET-026
CR 1251	Use of inconsistent or incomplete terms for the cooperative MA shortening function	SUBSET-026
CR 1252	Ambiguities about release speed and application of A.3.4 in case a train accepts a CES	SUBSET-026
CR 1259	Accuracy of distances measured on-board not considered when determining Release Speed from MRSP	SUBSET-026
CR 1263	MA request condition when LoA speed is above MRSP	SUBSET-026
CR 1264	Exhaustiveness of the list of actions not to be reverted or executed twice	SUBSET-026

(continued)

CR 1267	Acquiring the list of available networks whilst communication session is established	SUBSET-026
CR 1282	Subset-044 chapter on safety is inconsistent with Subset-026 regarding handling of EOLM info	SUBSET-023 SUBSET-026
CR 1288	Shortcomings due to specific locations temporarily considered as the EOA/SvL	SUBSET-026
CR 1293	Ambiguity about clauses to be applied to messages containing high priority data	SUBSET-026
CR 1295	TSR inhibition in SB and SR modes	SUBSET-026
CR 1296	Wrong assumption in on-board calculation of release speed	SUBSET-026
CR 1300	Follow-up to CR977	SUBSET-026 SUBSET-041
CR 1306	Undefined sequence of actions following the filtering of trackside information as per SRS 4.8	SUBSET-026 SUBSET-040
CR 1309	Enhancement of HDLC to handle retransmission of SABME message	SUBSET-037 SUBSET-092
CR 1310	DNS/ETCS on-board communication handling	A11T6001 SUBSET-037 SUBSET-092-1
CR 1311	Inconsistency in Subset-026 regarding the relevance of Q_SLEEPSESSION for session termination orders	SUBSET-026
CR 1312	Undefined sequence of actions following the filtering of trackside information as per SRS 4.8 (part 2)	SUBSET-026 SUBSET-040 ERA_ERTMS_015560
CR 1313	Unclear management of train position status on passing unlinked BG(s)	SUBSET-023 SUBSET-026 SUBSET-027 SUBSET-040 SUBSET-041
CR 1318	Ambiguity in determination of location accuracy	SUBSET-026
CR 1319	Support of different transmission speeds (ETCS data)	SUBSET-037 EIRENE SRS A11T6001

(continued)

CR 1324	Problems with applying SRS clauses related to the supervision of an unprotected LX	SUBSET-026
CR 1325	Rejection of safety relevant information due to pending acknowledgement of validated train data	SUBSET-026
CR 1326	Display conflict in area D of ETCS DMI	ERA_ERTMS_015560
CR 1327	Reset of confidence interval	SUBSET-026 ERA_ERTMS_015560
CR 1332	Release speed calculated on-board while a LTO in rear of the EOA is stored on-board	SUBSET-026
CR 1333	Subset-026 clause 3.12.4.4 does not cover the case of reception of a new MA without mode profile	SUBSET-026
CR 1334	Ambiguity regarding the mode and level end events for the display of a text message	SUBSET-026
CR 1335	Train categories B3 on B2	SUBSET-026 SUBSET-039
CR 1338	Issues regarding the forwarding of data to a National System	SUBSET-026 SUBSET-035 SUBSET-058
CR 1340	Maximum D_LRBG exceeded	SUBSET-026
CR 1347	Unclear specification of “balise detection degradation” function	SUBSET-026
CR 1348	No change of speed and distance monitoring supervision status	SUBSET-026
CR 1353	Undefined term “the level is configured on-board”	SUBSET-026
CR 5049	PPP Activation timeout is not defined and ETCS DNS query repetition is missing	SUBSET-037 A11T6001

3.15.5 Game Changers

With the adoption of the latest B3 revision promising stability for the core ETCS functions, research is focusing on innovations that can bring additional functionality without affecting backwards compatibility, to protect the investments already made by member states.

The signalling sector has identified four Game Changers offering significant benefit in terms of additional functions and/or lower costs: automatic train operation

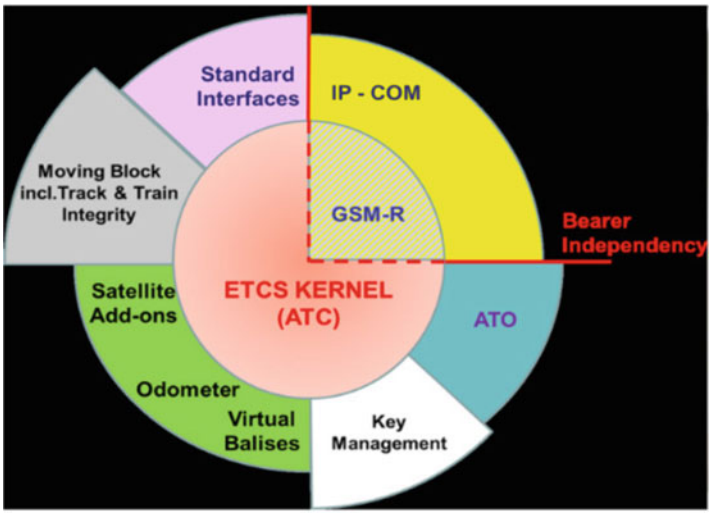


Fig. 3.10 Game Changers for ERTMS/ETCS

(ATO), ETCS Level 3, satellite positioning (GNSS) and the next generation telecommunication system (FRMCS).

Some of these initiatives have been incorporated into the IP2 workstream of the Shift2Rail research programme (Fig. 3.10).

3.15.5.1 Automatic Train Operation (ATO)

Automation is increasingly common in the urban rail sector. The Agency is looking for ATO functionality that can be applicable for urban rail, high speed and freight trains, in a mixed traffic environment. The purpose of this activity is the development of European ATO over ETCS specifications (AoE). The intention is to have ETCS as the Automatic Train Protection (ATP) system, which supervises the train movement from a safety point of view. The ATO on-board is able to drive the train automatically, based on timetable information transmitted by the trackside. It will attempt to meet the timetable and, where possible, do this in an energy efficient way. The ATO on-board has an interface with the ETCS on-board.

AoE provides a set of non-safety functions related to speed control, accurate stopping, door opening and closing, and other functions traditionally assigned to a driver. The safety of operation is ensured by ETCS or other safe systems.

AoE covers a wide range of applications from manually assisted to fully automated train operation. Possible actual operation depends on the desired grade of automation (GoA) and the automation level supported by Infrastructure Managers on a specific route.

Table 3.1 defines the operation principles for each GoA level:

ATO over ETCS is already implemented in several commercial projects: Thameslink, Mexico city - Toluca suburban line.

Table 3.1 Grades of automation

GoA	GoA name	Train operator	Description
GoA1	Non automated train operation	Train driver in the cab	The train is driven manually; but protected by automatic train protection (ATP) This GoA can also include providing advisory information to assist manual driving.
GoA2	Semi-automated train operation	Train driver in the cab	The train is driven automatically, stopping is automated but a driver in the cab is required to start automatic driving of the train, the driver can operate the doors (although this can also be done automatically) the driver is still in the cab to check the track ahead is clear and carry out other manual functions The driver can take over in emergency or degraded situations.
GoA3	Driverless train operation	Train attendant on-board the train	The train is operated automatically including automatic departure a train attendant has some operational tasks, e.g. operating the train doors (although this can also be done automatically) and can assume control in case of emergency or degraded situations.
GoA4	Unattended train operation	No staff on-board competent to operate the train	Unattended train operation all functions of train operation are automatic with no staff on-board to assume control in case of emergencies or degraded situations.

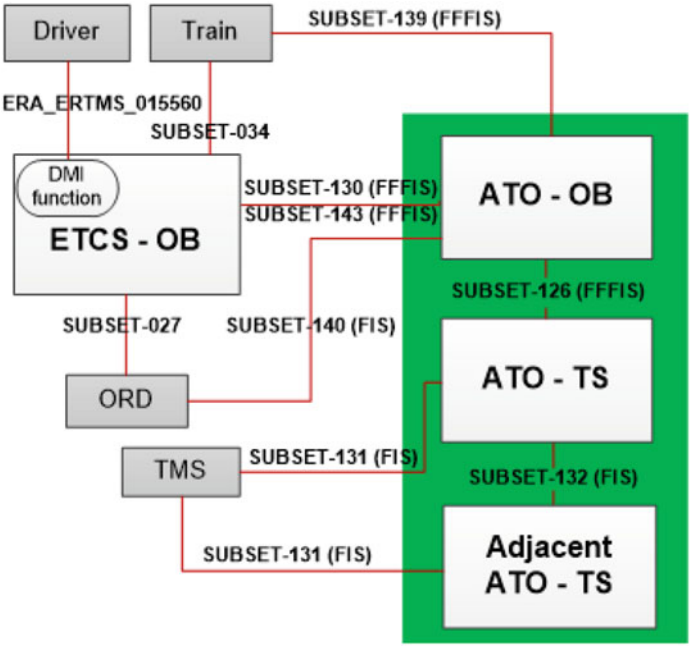


Fig. 3.11 ATO over ETCS reference architecture

With the introduction of AoE, Automated Train Operation (GoA2 to GoA4) will be beneficial for the different kinds of railway operation:

1. For High Speed Lines, Intercity lines and Regional lines, AoE will enhance the timetable adherence, provide high performance and enable the introduction of train traction energy saving functions fully managed by the ATO.
2. For Freight lines, AoE is supporting a smoother operation (e.g. allowing efficient conflict management and minimising unexpected train stops, support loading/unloading operations…) which lead to energy savings, but also to improved line capacity.
3. For Urban and Suburban applications, AoE will permit to provide high performance for lines carrying intensive inner suburban and cross-city traffic. ATO will also bring energy saving for these types of operation (Fig. 3.11).

The following interfaces are specified:

3.15.5.2 ETCS Level 3

This development stream intends to reduce the trackside fixed train detection systems, with the consequence to reduce both the cost of maintenance and the safety risk to the staff undertaking that work.

A key driver for research in this area is the need to increase capacity on busy routes, where train operators are looking at introducing moving block to optimise

SUBSET ID	Document title
SUBSET-126	ATO-OB / ATO-TS Interface (FFFIS application layer)
SUBSET-130	ETCS-OB / ATO-OB Interface (FFFIS application layer)
SUBSET-131	ATO-TS / TMS Interface (FIS)
SUBSET-132	ATO-TS / ATO-TS Interface (FIS)
SUBSET-139	ATO-OB / Train Interface (FFFIS)
SUBSET-140	ATO-OB / ORD Interface (FIS)
SUBSET-143	ETCS-OB / ATO-OB Interface (FFFIS low level layers)

headways. Although the Level 3 architecture does not explicitly specify moving block, the reduction of fixed train detection systems is a key step towards that objective.

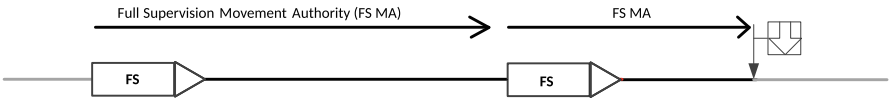
In Level 2, the train separation function is based on occupation status reported by trackside train detection devices. In Level 3 the train separation function, which is performed by the trackside, is based on train position and train integrity confirmation, both reported by the on-board to the trackside.

The SRS does not refer to moving block in the definition of Level 3. In a Level 3 implementation the block sections exist in a logical form in the trackside system. They can be fixed (virtual) blocks as well as moving (virtual) blocks. Both are possible and both are considered as Level 3 implementations.

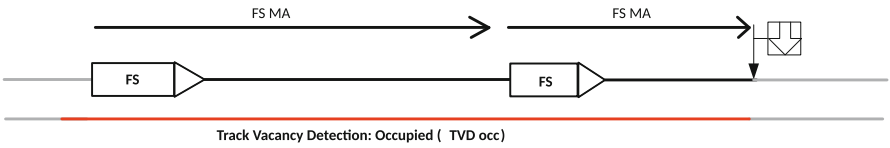
Several Infrastructure Managers have opted to install a form of Level 2+, by splitting the sections between fixed signals. Some are using separate track circuits or axle counters, others have opted for “virtual blocks” based on the train reporting its own location and train integrity.

Level 3 covers four different variants:

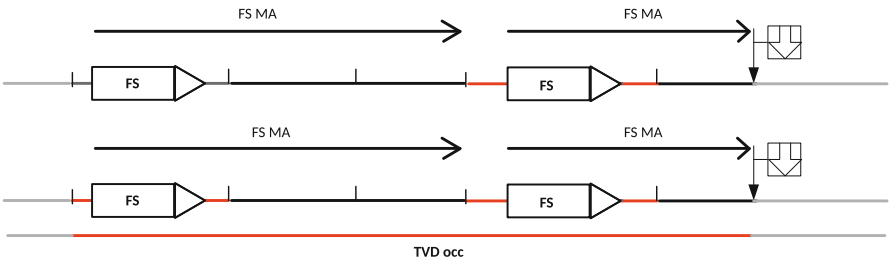
Variant 1: Moving Block without trackside train detection



Variant 2: Moving Block with trackside train detection



Variant 3: Fixed Virtual Block without trackside train detection
Variant 4: Fixed Virtual Block with trackside train detection



3.15.5.3 The Hybrid Level 3 Concept

Prior to the start of the Shift2Rail Level 3 work, the ERTMS Users Group had developed the so called Hybrid Level 3 (HL3) concept. It is a detailed description of variant 4 of the Shift2Rail Level 3 work.

The HL3 concept allows to reduce the trackside train detection substantially compared to ETCS Level 2. The advantage of keeping a limited implementation of trackside train detection is that this mitigates the disadvantages of the "pure" Level 3. It allows, for instance, to run trains without an integrity monitoring function and it mitigates the potential problems with trains which are not connected to the RBC, either due to communication failure or due to End of Mission.

The main characteristic of the concept is that it uses fixed virtual blocks for the separation of trains which are fitted with a train integrity monitoring system (TIMS), while a limited installation of trackside train detection is used for the separation of trains without TIMS, as well as for the handling of degraded situations.

The concept is defined in a generic way, which makes it applicable for all kinds of lines, from high density, high performance lines to low density lines.

The Hybrid Level 3 concept is based on the following features:

It is based on the existing Baseline 3 Release 2 set of specifications, with corrections defined in the agreed solution of CR940. These corrected specifications can be used without any additional functions or features.

It uses fixed virtual blocks. In comparison to moving blocks, fixed virtual blocks have in several implementations less impact on the existing trackside systems such as the RBC, interlocking and traffic control centre as well as on the operational procedures. By reducing the length of the virtual blocks the performance can be similar to moving blocks.

It uses a limited implementation of trackside train detection. Trains which are not reporting confirmed integrity can still be authorised to run on the line, albeit with longer headways. Trains which are disconnected from the Hybrid Level 3 (HL3) trackside are no longer lost. They are still visible by means of the trackside train detection, which facilitates operational movements of disconnected trains, protection against unauthorised disconnected trains, and recovery after a crash of the HL3 trackside system. In addition, trackside train detection can improve performance by providing a faster release of critical infrastructure (e.g. points) than what can be achieved on the basis of the position reports.

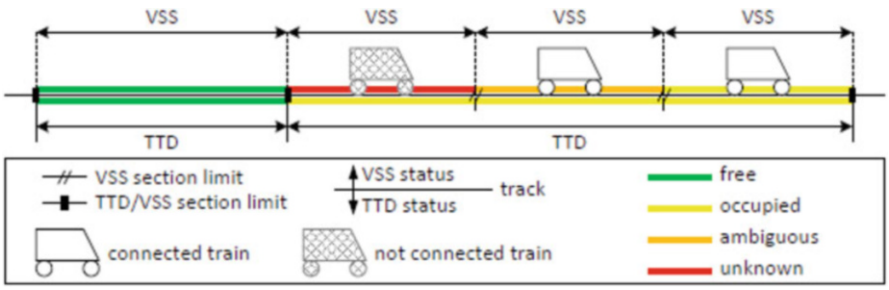


Fig. 3.12 Hybrid level 3

It uses the status of the virtual blocks for the train separation function. The underlying trackside train detection is only used, together with the position reports, to determine the status of the virtual blocks.

It aims to minimise any possible impact on the harmonised operational rules which are defined for Level 2 (by using a limited implementation of trackside train detection).

If the installation of trackside train detection is implemented by axle counters, which are restricted to the areas where the points are located, and possibly the level crossings, the cost will be only a fraction of the cost to fit the whole line with train detection (axle counter heads). The whole stretch of track between the point areas is implemented as one large trackside train detection section. This large physical section is then split into as many virtual sections as necessary for the intended performance. In the points area, power and cables are present anyway to operate the points.

It can be used on existing lines, which are already fitted with train detection, to provide a cost-effective way to increase the capacity of the line, specifically in the peak hours.

It can also be used on low density lines, where the fitment of a few train detection devices around the points (e.g. axle counters) together with a HL3 trackside system would provide a cost-effective way to achieve an ETCS implementation.

Since there are no easy solutions for the problems related to Level 3 without any trackside train detection, the Hybrid Level 3 concept is a pragmatic and flexible solution to start with the implementation of Level 3 (Fig. 3.12).

3.15.5.4 Global Navigation Satellite System (GNSS)

The ERTMS Users Group has created a WG named Localisation Working Group (LWG) to settle common railways requirements on the expected behaviour of a train localisation system in an ERTMS and RCA environment to tackle current criticalities and possible future needs and to explore innovative solutions to fulfil such requirements in a cost-effective way.

The objectives of the LWG are:

- To set and provide users' requirements (functional, performance, architectural, interfaces) for the evolution of the train localisation system with regard to the ERTMS and RCA environment.
- To share, learn, secure experiences of members or other players and support the members regarding train localisation projects to compare different technologies and solutions to fulfil the users' requirements.
- To establish relationship with all players involved in the topic (ERA, GSA, ESA, EC, UNISIG, CER, S2R, UIC . . .) to share and propose train localisation system users input.
- To become one of the key players of the satellite positioning game changer.
- To support the possible CBA analysis that the sector may carry out on the introduction of new technologies for train localisation.
- To support the development of the train localisation system architecture and its interfaces based on innovative solutions.
- To support the setting of common standards (possible CRs to ERTMS specification) and develop a legal framework (Fig. 3.13).

Several European R & D projects have investigated the possibility to use GNSS to improve the current train localisation principles of ERTMS. The main projects in this area were ERSAT EAV, ERSAT GGC, STARS, RHINOS and NGTC. A current continuation project is GATE4RAIL (Fig. 3.14).

ERSAT GGC impacts primarily on the evolution of ERTMS that thanks to the use of satellite assets will become more efficient and economically advantageous

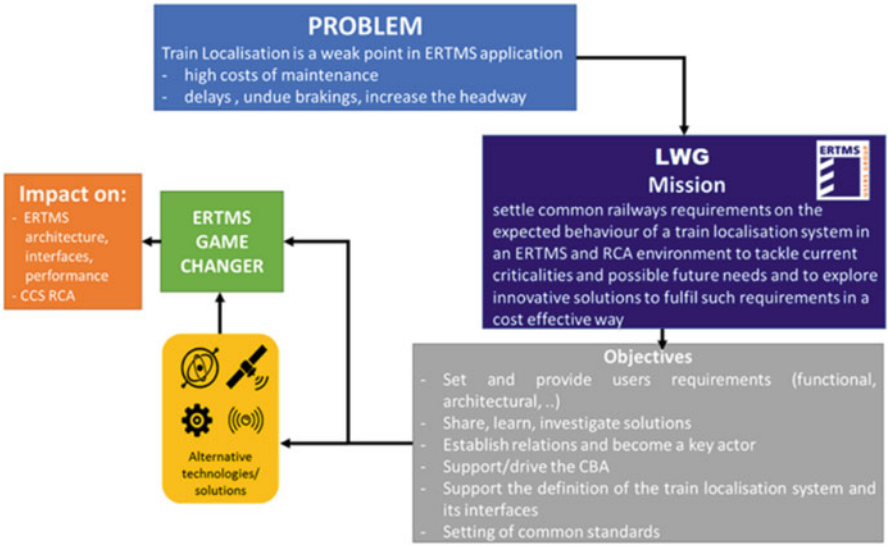


Fig. 3.13 Game changer GNSS

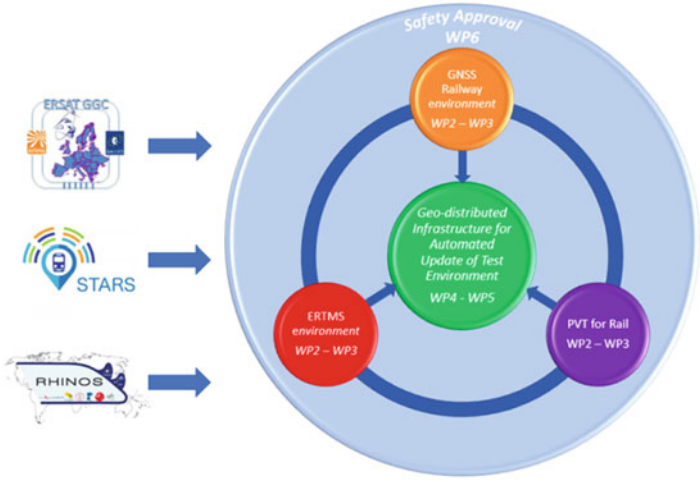


Fig. 3.14 Starting point for GATE4RAIL

for its deployment on local and regional lines, contributing to the EC policy on the adoption of the ERTMS on the European railways. At the same time the project will be impacting on the utilisation of EGNOS and GALILEO, primarily designed for aviation application, in the demanding rail operational environment.

A further contribution of ERSAT GGC with the introduction of new technologies lies on linking together ERTMS and EGNOS-GALILEO, both pillars of the European Commission industrial policy with the promise to impact on the rail and satellite sectors, creating unprecedented mutual benefits, rail being the highest potential user of EGNSS.

The ERSAT GGC (Galileo Game Changer) innovation project represents a fundamental contribution to the roadmap of ERTMS for the adoption of the EGNSS satellite technology, already identified as one of the game changer technologies of the ERTMS evolution. Particular focus is given to the certification process of the satellite assets to allow the ERTMS to operate seamlessly with Virtual Balises which are functionally equivalent to physical balises in order to ensure the end-to-end compatibility with ERTMS. ERSAT GGC is linked with previous projects achievements co-funded by GSA and EC.

The Project's high-level objectives are the following:

- Validation of EGNSS assets and relevant certification process compatible with the ERTMS Standards.
- Definition and certification of a standard process, methodology and the related toolset for classifying track areas as "Suitable" or "Not Suitable" for locating Virtual Balises.
- Consolidation and certification of the enhancement of the functional ERTMS architecture

  integrated with satellite-based Location Determination Systems.

Furthermore, ERSAT GGC contributes to the standardisation process and dissemination of results on the satellite and rail stakeholders which will be impacting on:

- the definition of new ERTMS TSI;
- the evolution of EGNSS requirements to implement efficiently virtual balises.

The following guidelines inspired the High-Level Functional Architecture produced by ERSAT GGC:

- Minimising the impact on current ERTMS/ETCS specification;
- Avoiding unnecessary constraints in order to let each supplier design its own Virtual Balise Transmission system and the Virtual Balise Reader (VBR);
- Concentrating on the introduction of the Virtual Balise Concept and Public Radio TLC Communication Network, and all the impacts on the ERTMS functions, and safety analysis;
- Defining the main properties of the Augmentation Network required for completing the definition of the enhanced ERTMS functional architecture, and executing the system functional hazard analysis.

The Virtual Balise is an abstract data type capable of storing the fixed Eurobalise user bits associated with a balise telegram. Signalling designers, during the design phase, shall establish the track location, where such a virtual balise would be logically installed, and the user bits (i.e. the information) that the virtual balise must send to the on-board system, in the same way to what the signalling designer does for the physical balise.

That information must be sent to the on-board system, when the estimated GNSS-based position of the GNSS Antenna mounted on the train roof and projected to the track (Virtual Antenna reference mark) matches the location established by the signalling designer.

The BTM function and the VBR function can be implemented on a unique safe platform, and both functions can be active at the same time, independent from each other.

During the train run:

1. the BTM generates the tele-powering signal to energise any Eurobalise that it can encounter.
2. the VBR periodically computes the estimated GNSS-based position of the GNSS Antenna, mounted on the train roof and projected to the track (Virtual Antenna reference mark), and compares it with the locations associated with the virtual balises stored in the on-board track database.

After passing over a physical balise, and for each correctly decoded telegram, the BTM provides both the user bits of the decoded telegram and the reference position of the physical balise to the ERTMS/ETCS Kernel. On the other hand, when the estimated GNSS position matches the stored position in the on-board track database, VBR provides both the user bits associated with the virtual balise and the reference position of the virtual balise to the ERTMS/ETCS Kernel.

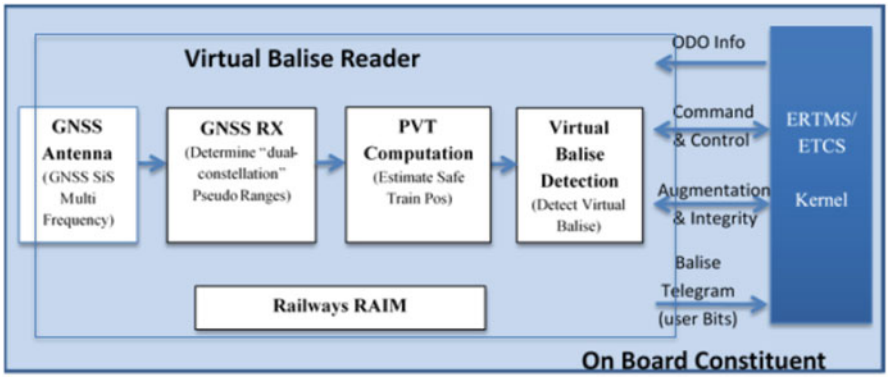


Fig. 3.15 High-level virtual balise reader architecture

Therefore, the ERTMS/ETCS kernel logically receives the same information (i.e. user bits and the reference location) independently from the type of medium through which this information is sent (physical or virtual balise).

The ERTMS/ETCS kernel remains responsible for implementing all the ERTMS/ETCS functions related to balises (e.g. LRBG, Linking, Expectation window, balise message consistency checks, etc.).

The VBR architecture can be found (Figs. 3.15 and 3.16).

3.15.5.5 Future Rail Mobile Communication System (FRMCS)

Globally, many railway infrastructure managers and railway undertakings currently use an interoperable radio communications network, GSM-R (Global System for Mobile Communications—Rail), for operational voice communications and to provide the data bearer for ETCS. In the European Union this is legally mandated in the Technical Specifications for Interoperability that are applicable in the European Member States. Voice and data communications are also used for various other applications.

GSM-R is a MOTS (modified off the shelf technology) system based around manufacturers' commercial GSM (Global System for Mobile Communications) offerings, enhanced to deliver specific "R" (railway) functionality. Due to the product modifications required to provide "R" functionality, and the need to utilise non-commercial radio spectrum, much of the equipment utilised for GSM-R comprises manufacturers' special-build equipment and/or software variants. The use of MOTS technology for GSM-R has proven expensive for the railways, both in terms of capital and operational expenditure.

The predicted obsolescence of GSM-R by 2030, combined with the deployment plan of ETCS and the Railway business needs, have led to the European Railway community initiating work to identify a successor for GSM-R. The successor has

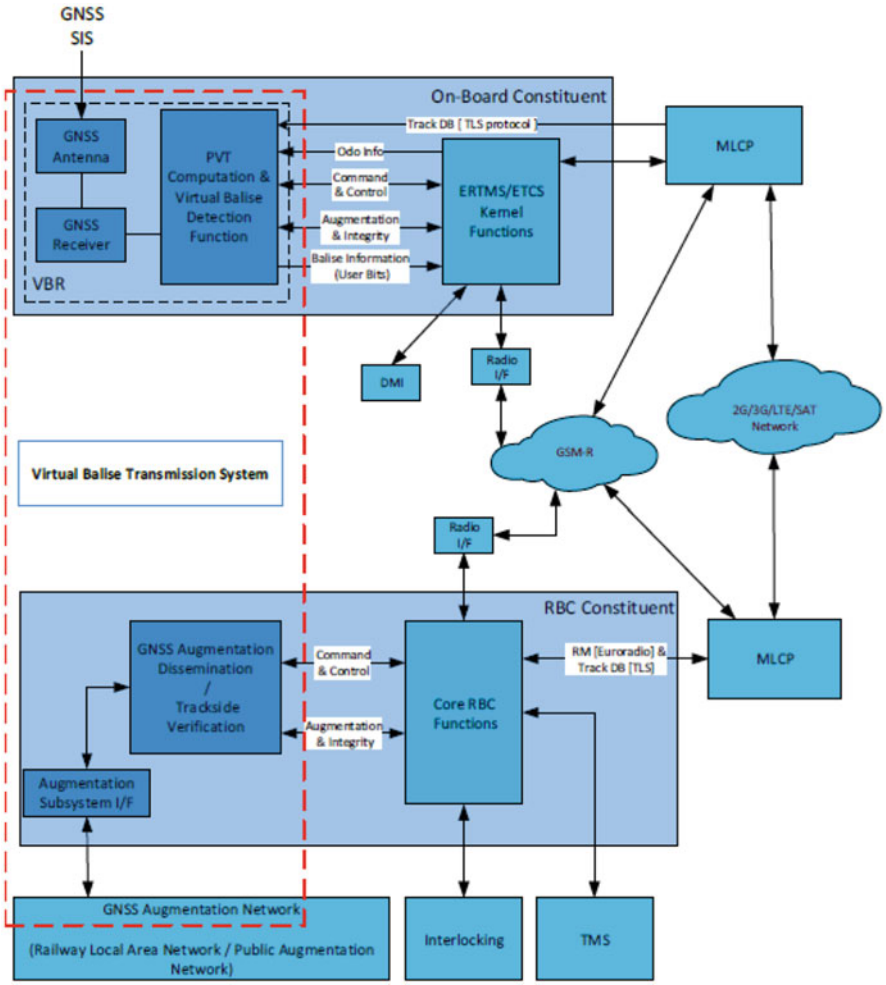


Fig. 3.16 High-level functional architecture for the introduction of the virtual balise concept

to be future proof, learn from past experiences/lessons and comply with Railway requirements. Those requirements are one of the first steps in this process, where the railways' needs are identified and defined in a consistent and technology independent way, the foundation for next steps on defining the Future Railway Mobile Communications System (FRMCS).

The FRMCS Project was formally initiated by UIC in 2014, after 4 years of previous activities in this field.

The Project Scope is to provide overall technical conditions for the successor of GSM-R.

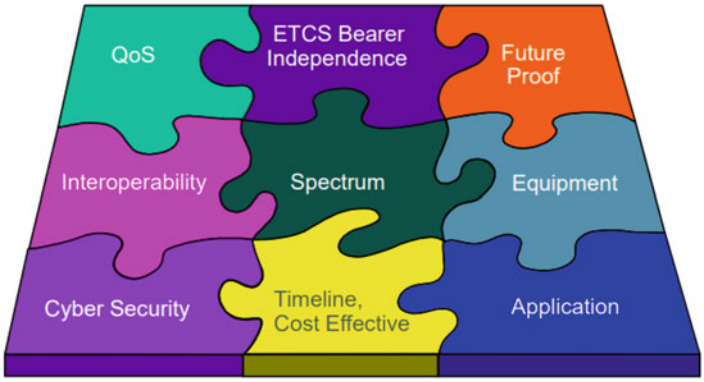


Fig. 3.17 FRMCS challenges

Three main work directions are identified to provide the baseline platform for the system definition and delivery:

- User Requirements;
- System architecture, interfacing with trackside and on-board equipment;
- Frequency Spectrum.

The project aims at providing an appropriate replacement to EIRENE FRS:

- Based on the User Requirements;
- Investigate future needs and add new functionalities;
- Technology independent;
- Future proof;
- Application layer approach;
- Enabling interoperability.

The project aims at providing an appropriate replacement to EIRENE SRS:

- Based on 3GPP and ETSI specifications;
- Define building blocks and interfaces;
- Provide communication service to the application layer;
- Ensure interoperability.

The project is facing a number of challenges as described (Fig. 3.17):

The project defines a Migration Strategy:

- Migration spectrum needs;
- Network model;
- Technical conditions for interoperability—interoperability with GSM-R;
- Flexible FRMCS implementation plans.

The project plan can be found (Fig. 3.18).

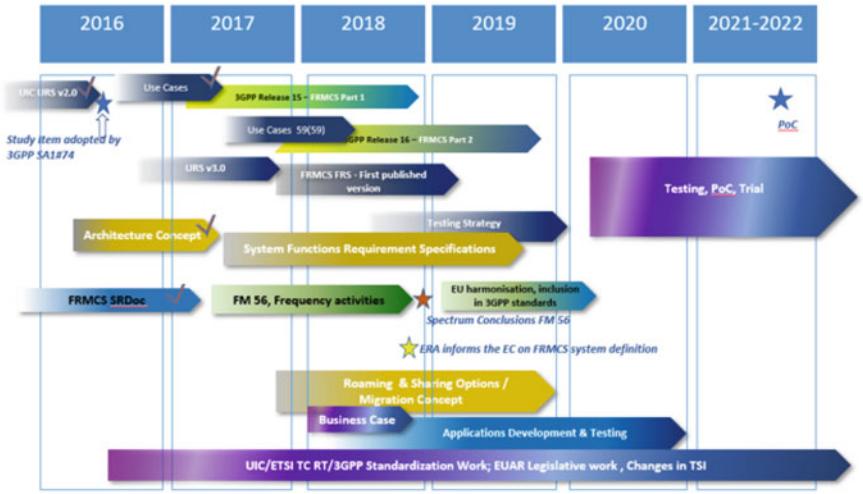


Fig. 3.18 FRMCS plan

3.15.6 CCRCC ERTMS Conference 2019

The EU Agency for Railways organised the Control-Command and Railway Communication Conference (CCRCC2019/ERTMS conference) which took place the 15–17 October 2019 in Valenciennes.

The conference focused on:

- ERTMS deployment and expectation for the TSI CCS 2022/2023 release;
- Vehicle Upgrade and vehicle authorisation topics > experience and challenges from current projects;
- ERTMS regulatory and funding framework > status quo, first experience and outlook;
- Communication > future railway mobile communication system (FRMCS) and GSM-R migration;
- Future transport system—Rail and CCS evolution > digitalisation and big data shaping the future rail system.

3.15.7 Next TSI Release

The new TSI release will include the results of the various work streams:

- Correction of error CRs (Article 10)
- Game changers:
  - ATO;
  - ETCS level 3;

  - GNSS;
  - FRMCS and its interfaces (FIS, FFFIS).
- Other improvements:
  - Supervision of shunting movements;
  - ETCS DMI optimisations;
  - Braking curves (conversion model, low adhesion, gradients under the train, target speed extension);
  - Extended diagnostics reported from train to track;
  - Etc.

The planned date of issue of the next TSI is 2022/2023.

3.16 Projects and Initiatives—European R & D

3.16.1 Shift2toRail Under Horizon 2020

The Shift2Rail Joint Undertaking (S2R JU) is a Public-Private Partnership in the rail sector, established under Horizon 2020, to provide a platform for coordinating research activities with a view to driving innovation in the rail sector.

The vision of the S2R JU is to deliver, through railway research and innovation, the capabilities to bring about the most sustainable, cost-efficient, high-performing, time driven, digital and competitive customer-centred transport mode for Europe (Fig. 3.19).

Rising traffic demand, congestion, security of energy supply and climate change are some of the major issues that the European Union and the wider world are facing. Tackling these challenges call for the railway sector to take on a larger share of transport demand in the next few decades.

The European Commission is working towards the creation of a Single European Railway Area (SERA), and has promoted a modal shift from road to rail in order to achieve a more competitive and resource-efficient European transport system. However, rail's share in the European freight and passenger transport markets is still not satisfactory. EU research and innovation therefore helps rail to play a new, broader role in global transport markets, both by addressing pressing short-term problems that drain rail business operations, and by helping the sector to gain a stronger market position.

Shift2Rail fosters the introduction of better trains to the market (quieter, more comfortable, more dependable, etc.), which operate on an innovative rail network infrastructure reliably from the first day of service introduction, at a lower life cycle cost, with more capacity to cope with growing passenger and freight mobility demand. All research activities are developed by European companies, thereby increasing their competitiveness in the global marketplace.

The aim is to benefit from all initiatives to bring new products on the market (Fig. 3.20).

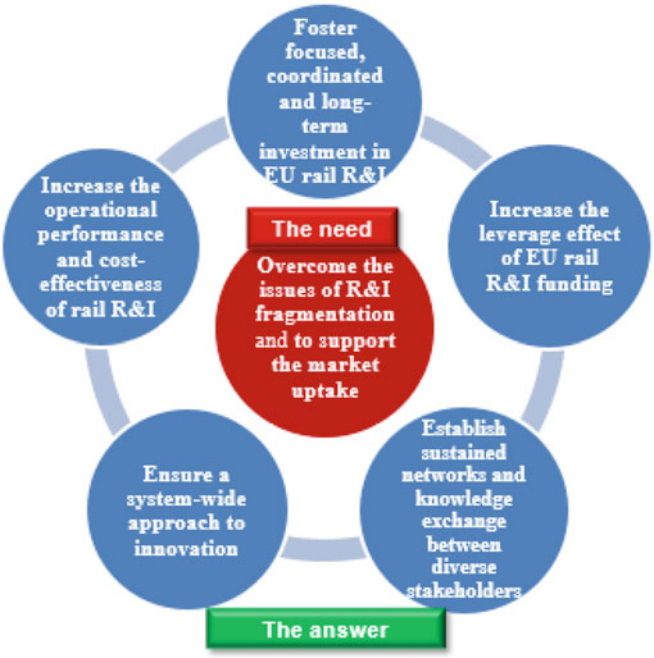


Fig. 3.19 Missions of Shift2Rail

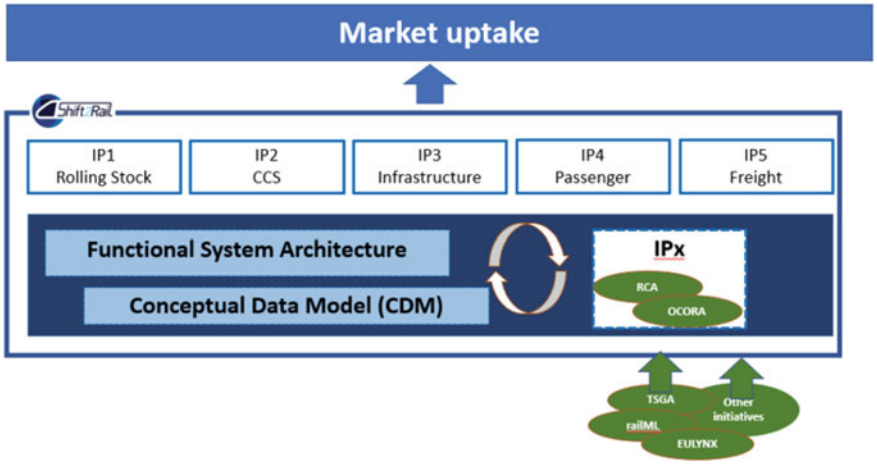


Fig. 3.20 Shift2Rail—"System of Systems" approach

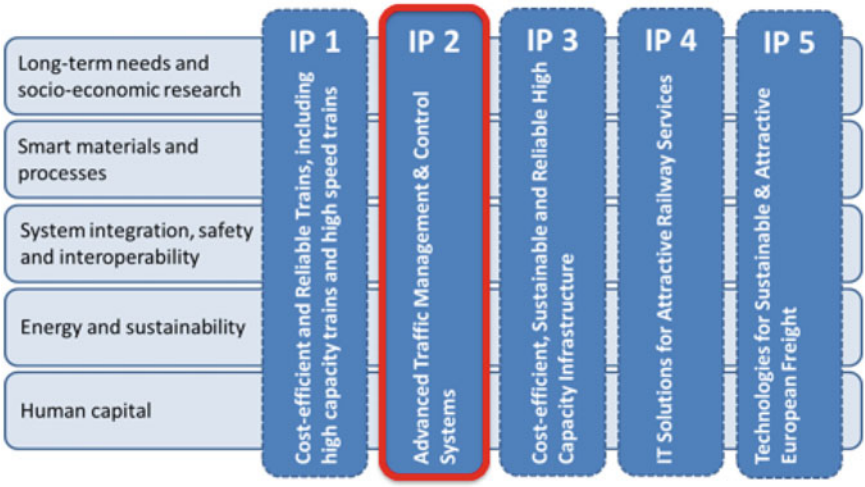


Fig. 3.21 Shift2Rail—five innovation programmes

The R & D work coordinated by Shift2Rail is organised in five innovation programs (Fig. 3.21).

Shift2Rail is offering applications to its **Call for Proposal 2020**. 19 topics worth in total €146.6 million will be funded under the Shift2Rail Joint Undertaking 2020 Call for Proposals for Research & Innovation activities. The application period is open since January 2020 and submissions will be accepted until 21 April 2020.

Details about IP 2 are summarised below (Fig. 3.22).

3.16.2 EULYNX

EULYNX provides the framework for close cooperation between Infrastructure Managers to support the aim of standardisation.

Standardisation of technical systems particularly on a European level is one of the most powerful measures to manage interoperability, improve efficiency and therefore reduce costs of the entire ecosystem. For signalling systems this standardisation takes into consideration different national operational rules, commercial interests, languages and other differences.

Life cycle cost targets and a shared market approach are the objectives of the European Infrastructure Managers (IM). The need is to change, maintain, renew and update the technical systems in a competitive way whilst converging the individual IMs' needs towards European harmonised requirements. This places the Infrastructure Managers as the system integrators into a position which provides them with a choice of various suppliers for different subsystems during the systems life cycle. This approach should be followed in new projects or when modifying

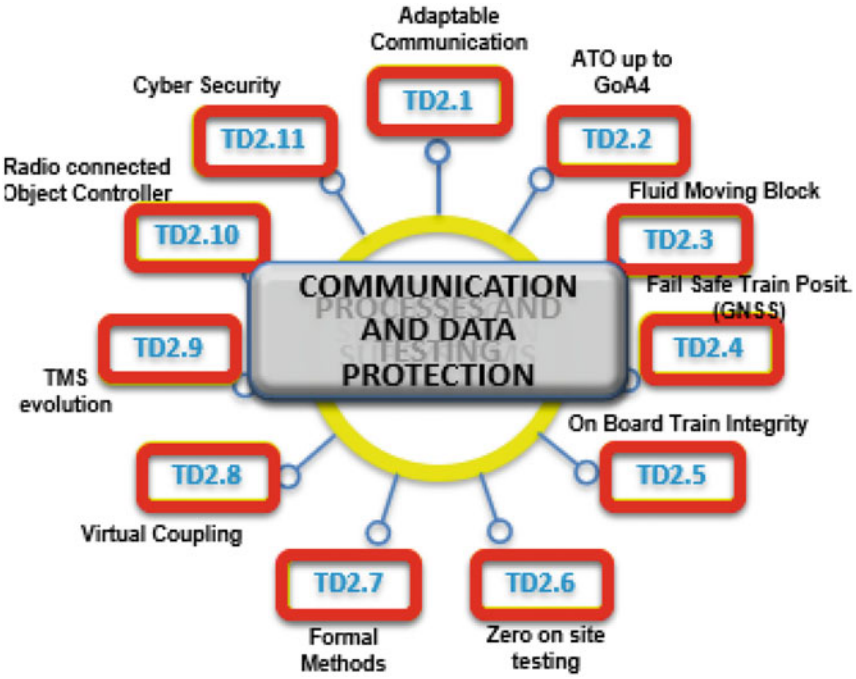


Fig. 3.22 Shift2Rail—focus on IP2 tasks

existing system functionality or infrastructure layouts. Also maintenance related activities will benefit from this. IM's join their market force in order to improve competition between suppliers and accelerate innovations for signalling systems, with the purpose of reducing life cycle costs. Due to different life expectancy of individual subsystems, the replacement shall be allowed on individual basis.

Results of previous European initiatives concerning interlocking system standardisation (e.g. Euro-Interlocking, INESS and ERTMS) provide a basis. This also provides an opportunity for the supply industry, as results can be reused in several markets. This creates a win-win situation for all involved (Fig. 3.23).

EULYNX provides the generic reference architecture of the control-command and signalling subsystems. This reference architecture is specified by infrastructure managers as well as consultation with certain suppliers through involvement in similar projects in Europe. In this architecture, processes are considered with the aim of the system accomplishing its intended functions, the exchange of data between the subsystems. Where needed, the definition also comprises the subsystems that will be implemented in the design (hardware, software, facilities, a.o.). The scope also includes security. The reference architecture applies in the whole life cycle of the system according to CENELEC standard EN 50126.

The reference architecture addresses the needs and concerns of the stakeholders: the European infrastructure managers; the suppliers of signalling systems and

Fig. 3.23 EULYNX partners

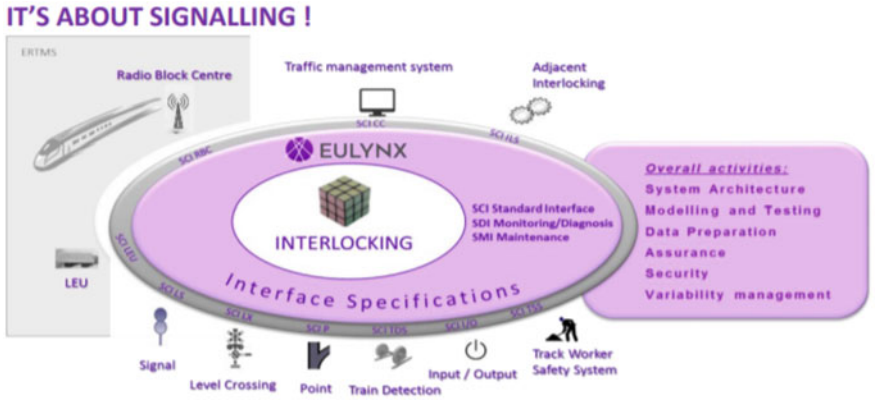


Fig. 3.24 5: EULYNX architecture

subsystems; the train operators; the safety authorities; the EU Agency for Railways; others (users, notified bodies, independent safety assessors, engineering bureaus, further standardisation organisations, contractors, etc.) (Fig. 3.24).

3.16.3 Smartrail 4.0

Swiss railway companies are working together on the development and implementation of the smartrail 4.0 traffic management system. The new solution will integrate interlocking, control technology, trackside installations, data transmission systems and traffic control systems to provide improved traffic management, more efficient

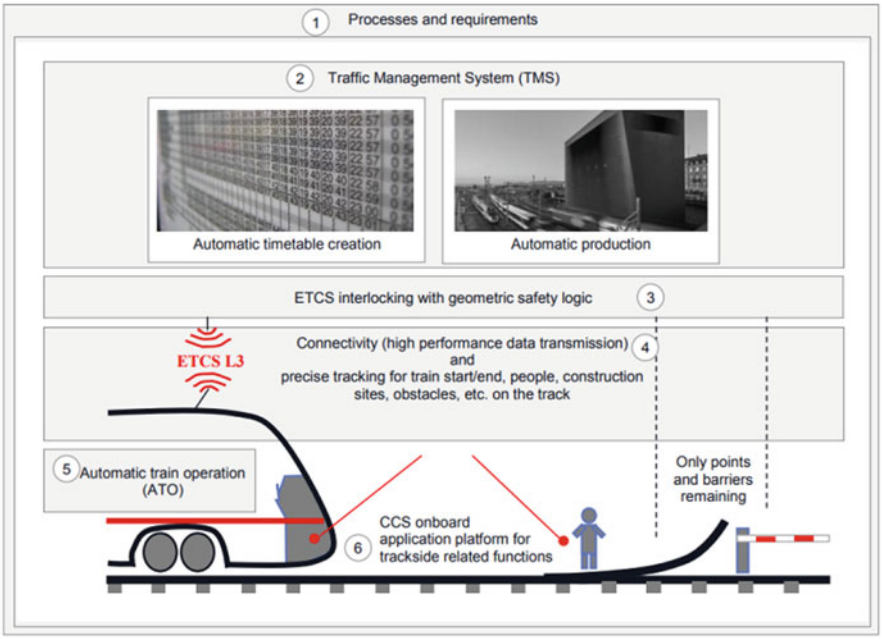


Fig. 3.25 Smartrail 4.0

use of railway infrastructure and to increase capacity of the network. The smartrail 4.0 programme will replace today's traffic management systems by 2038.

The project started in 2017. Four Swiss rail operators SBB, BLS, Schweizerische Südostbahn (SOB), Rhaetian Railway (RhB) and the Swiss Public Transport Union (Verband öffentlicher Verkehr, VöV) combined their forces to develop the smartrail 4.0 programme. The solution was successfully tested using a simulation in late 2018. The next intermediate target is short-term timetable planning with the use of a new traffic management system from late 2022. The final stage of the project is scheduled for 2027–2038, including the industrialised rollout of the smartrail 4.0 programme that is expected to replace the existing traffic management systems (Fig. 3.25).

The smartrail 4.0 solution is divided into six sub-programmes. The first element is the Traffic Management System (TMS). Today, it consists of five train-control centres covering almost the entire Swiss railway network. As a part of smartrail 4.0, TMS will be unified and automated. The unification will provide more efficient use of railway infrastructure by the operators. The second sub-programme is European Train-Control System (ETCS), that is a key component of the future unified European railway traffic management system. Switzerland started implementation of the ETCS Level 2 system in 2006 when it was installed on the first route in Switzerland (Mattstetten–Rothrist line). The country will complete its migration to the new train-control system by 2025.

The upgraded ETCS system is a foundation for another element of the smartrail 4.0—Automatic Train Operation (ATO). In August 2018, SBB tested automated trains on the Lausanne-Villeneuve route. The trial ATO has the second grade of automation (GoA 2). During the journey, a driver handed control of the train to the autopilot. Smartrail 4.0 provides the implementation of the fourth grade of automation (GoA 4) when the entire journey (including departure, stopping at stations, door closure, disruption management) is performed by ATO. The ATO implementation is impossible without two other components—on-board equipment and communication systems. The last sub-programme is "Processes and Requirements". It creates a framework around the other mentioned above sub-programmes and ensures them with the same functional architecture.

3.16.4 Reference CCS Architecture (RCA)

When considering the business challenges facing the railways and recognising the opportunities provided by a collaborative approach to Command and Control Systems (CCS), Infrastructure Managers consider that a joint development of a future "Reference CCS Architecture" (RCA) will have many benefits. A White Paper has therefore been developed to express the thoughts of the members of the ERTMS Users Group and the EULYNX Consortium.

The RCA White Paper and related communication strategy are aimed at:

- Highlighting the opportunities associated with Infrastructure Managers working together to develop a single modular framework for future CCS where the interfaces that are being developed within EULYNX are a vital cornerstone;
- Providing a common understanding for Infrastructure Managers, industry partners and other stakeholders on the RCA initiative;
- Providing the background and justification for the RCA initiative;
- Providing direction to industry partners and other stakeholders, including recognition of the benefits associated with building upon and aligning existing developments such as ETCS, ETCS Game Changers, EULYNX and Shift2Rail;
- Providing assurance that the RCA initiative will respect existing CCS investments by recognising the need for a flexible migration approach;
- The White Paper also highlights how the Infrastructure Managers will organise their collaborative approach, utilising the existing ERTMS Users Group and EULYNX Consortium to provide the technical direction and development activities. It also identifies the need for engagement with Railway Undertakings and Suppliers (Fig. 3.26).

The RCA initiative strives for a substantial improvement in cost, capacity, safety, reliability of the CCS (command, control, signalling) system. RCA starts with radio-based ETCS cab-signalling and EULYNX interfaces and adds a harmonised architecture with clearly defined interfaces leading to an upgradable system with

Fig. 3.26 RCA initiative

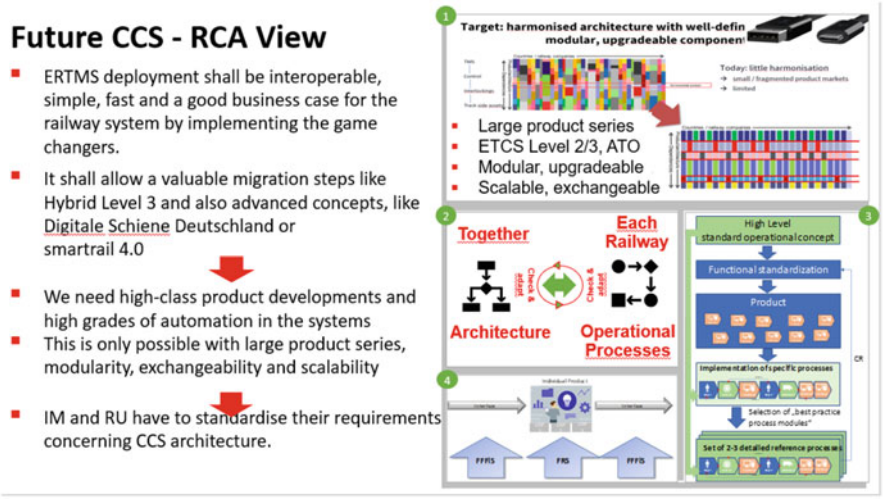


Fig. 3.27 RCA view

interchangeable components. RCA includes the game changers such as ATO, ETCS Level 3, satellite localisation, FRMCS.

The RCA view is summarised (Fig. 3.27):

A first draft of RCA has been released in February 2019. This RCA Alpha describes the RCA concepts to allow further discussion and feedback from railways, suppliers, regulators. Based on the feedback the RCA concepts will be incrementally developed into full specifications.

Several workshops have been organised and the resulting feedback (from railways, suppliers, sector organisations) has been used to produce the RCA Beta, which was released in August 2019. RCA Beta mostly deals with corrections, misunderstandings and frequently asked questions.

RCA Beta is released in the form of an updated set of documents from RCA Alpha and with a few additional "Beta chapters" on topics which had generated a lot

of interest. New "Beta chapters" include: Platform Independence, Modular Safety, Capacity Effects, Architectural Approach.

RCA Gamma has been released in January 2020. It is an update taking into account feedback from railways, suppliers and sector organisations. RCA Gamma provides new topics and reorganises the existing material to be able to move to model-based specifications.
New topics include: Migration with RCA, Principles of the Safety Logic, Business case of RCA for IMs, LSL (Enhanced L3, Supervision, Localisation). The first "development snapshots" of the model-based specifications will be made available starting March 2020.

As described previously, the focus of RCA is on the architecture of the CCS trackside. There is a similar initiative, called OCORA, which addresses the architecture of the CCS on-board side. An overview can be found in the next section.

3.16.5 OCORA

OCORA stands for **O**pen **C**CS **O**n-board **R**eference **A**rchitecture. OCORA is a collaboration of railway companies with five founding members that decided to combine **engineering resources** in the CCS domain to work on **ERTMS and beyond: SNCF, NS, SBB, ÖBB, DB**.

OCORA is an open collaboration. The "openness" of OCORA is defined as the principle based upon **collaboration and sharing, publicly available standards and models, facilitating cost-effective industrialisation** without any barrier and in line with the competition laws.

OCORA intends to remain a **collaborative platform**. The OCORA activities are:

- To define standardised interfaces and a reference architecture for all major evolvable on-board CCS components.
- To analyse the need to improve the regulatory framework.
- To bring new technology and to ensure that technological progress from other sectors reaches the railways.
- To provide proven solutions, which will be validated by, e.g. demonstrators. To ensure a cost-effective migration, the OCORA results should be promoted within the sector to be applied under voluntary basis.

The OCORA collaboration has no intent to substitute sectorial representative bodies. For instance, Change Requests will be proposed by OCORA through the regular sectorial representative bodies.

OCORA currently focuses on the internal communication backbone and interfaces of the CCS on-board subsystem of existing and new rolling stocks.

OCORA has the ambition to feed the railway sector with proven specifications along with their economical assessment to attain cost-effective, reliable, safe and secure CCS on-board subsystems over the life cycle of vehicles (Fig. 3.28).

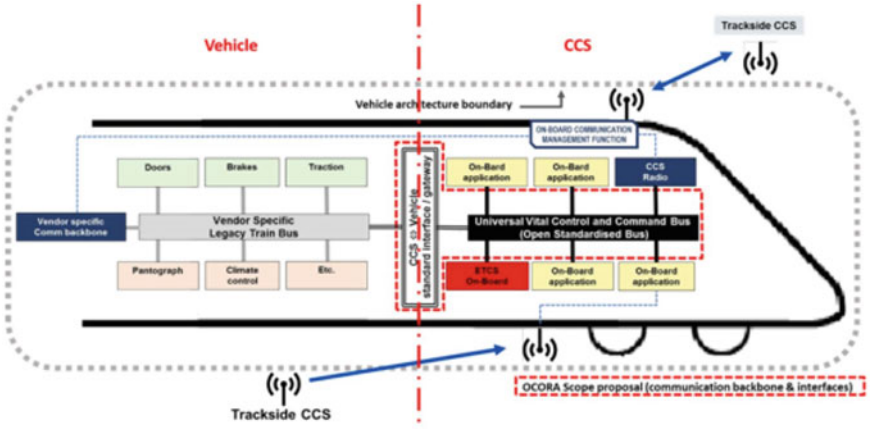


Fig. 3.28 OCORA reference architecture

Anticipated deliverables of OCORA are **specifications**. For the short term, OCORA aims at providing a comprehensive and coherent set of interface specification for a modular OCORA on-board CCS environment to serve as **voluntary tender templates.**

Additional deliverables include supporting material for **IVV (Integration, Verification and Validation)**. Also, part of OCORA is material helping to plan for an OCORA-based system (such as business case mechanics, supported reference architecture etc.) and material to help the decomposition of the OCORA subsystem. Although OCORA aims at standardisation of the on-board CCS, it does not envisage to set up a formal standard. OCORA will develop specifications serving procurement and innovation purposes.

In the short term, OCORA aims at preparing solutions for six major problems identified in the current CCS TSI. These include the lack of modularity (including the lack of an open CCS bus), hardware-software independence, regulations that prevent innovation, and the lack of non-functional requirements (e.g. performance indicators). These will be formulated as problem statements for an alternative Open CCS On-board Reference Architecture (Fig. 3.29).

The main objectives of OCORA:

1. **To define an Open CCS On-board Reference Architecture—which is referred to as OCORA, by e.g.:**
   - **Open standardisation** of the ETCS/ATP and ATO train-interfaces and -functions and other on-board subsystems as plug and play solution.
   - Establishing the principles and necessary requirements of the OCORA initiative.
   - Aligning initiatives and ideas already started and finding synergies to combine scarce resources.

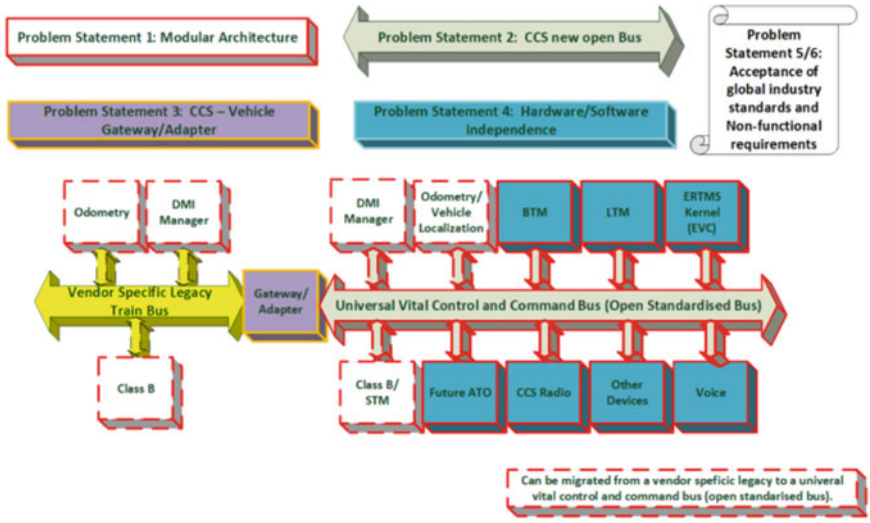


Fig. 3.29 Problem statements by OCORA

- Streamlining industrialisation processes in particular the certification.

2. To foster and develop the open ETCS/ATP source initiative by utilising and benefitting from the existing results of the "openETCS" initiative and sharing common understanding on this initiative.
3. To validate the viability and relevance of the OCORA approach by using demonstrators.
4. To promote the use of OCORA for the CCS on-board solutions in Europe in order to make them more cost effective, reliable, safe and secure by e.g.:

   - Ensuring consistency and complementary on a railway system scale between OCORA and other similar initiatives. This will be done in close coordination with sectoral organisations (e.g. CER, EPTTOLA, ...) and in close cooperation with joint undertakings already in charge of the definition of certain aspects of ERTMS (e.g. Shift2Rail, ERTMS Users Group, EULYNX, UNISIG, UIC, ...).
   - Building consensus and getting support from railway companies through regular information towards sectoral associations (e.g. members of the group of representative bodies).
   - Facilitating the industrialisation of OCORA results notably certification, through input to and discussions with associations sectorial organisations, manufacturing companies and joint undertakings (for instance UNIFE, UNISIG, Shift2Rail, ERL—European Reference laboratories, ...)

3.17 Conclusions

3.17.1 In Europe

The ERTMS/ETCS project was launched by EU and the UIC in the early 90s. The main achievement was the production of preliminary specifications. The first pilot projects appeared in Europe in the early 2000s in several countries, such as Spain or Italy. The first stable specification was baseline 2 (system version 2.3.0d) issued in January 2008. At the same time, the sector started to work on the next versions of the specifications. As a result a first version of baseline 3 appeared (B3 MR 1) in May 2014 and then a second one (B3 R2) in May 2016. Most countries of Europe are preparing and implementing a migration plan to ERTMS. In addition, EU is promoting the acceleration of the deployment of ERTMS on corridors (Core Network Corridors) and the replacement of class B legacy systems.

The European R & D coordinated by Shift2Rail is very active, the Game Changers will bring a lot of new functions for the next TSI to be issued in 2022 or 2023. Many initiatives are happening in parallel (RCA, OCORA), with the aim to improve the system, make it more modular and optimise his cost, by standardising the architecture of the trackside and the on-board parts. The sector is extremely dynamic.

The figure below shows the ambition of the ERTMS deployment as presented by EU at the CCRCC conference which took place in Valenciennes in October 2019 (Fig. 3.30).

The introduction of ERTMS in Europe has been very slow in Europe but it is now happening. There are still many challenges, but it is now becoming a success story.

Fig. 3.30 ERTMS deployment plan

3.17.2 Outside of Europe

ERTMS/ETCS becomes a de facto worldwide standard. In the first years, only the UNISIG members were able to provide such systems. Now there are many suppliers capable to offer the products. It happens on all continents.

The systems delivered outside Europe are quasi-identical to those installed in Europe. In China, CTCS is the name of the system which is deployed. It is also similar to ETCS. A description of this system can be found in another chapter.

The website of UNIFE shows the countries where ERTMS/ETCS is implemented.

3.17.2.1 Africa

See Fig. 3.31.

Fig. 3.31 ERTMS/ETCS in Africa

3.17.2.2 Asia

See Fig. 3.32.

Fig. 3.32 ERTMS/ETCS in Asia

3.17.2.3 Oceania

See Fig. 3.33.

Fig. 3.33 ERTMS/ETCS in Australia

3.17.2.4 America

See Fig. 3.34.

Fig. 3.34 ERTMS/ETCS in America

3.18 References and Resources

EU Agency for Railways: https://www.era.europa.eu/
ERTMS Users Group: https://ertms.be/
UNIFE/ERTMS http://unife.org/; http://www.ertms.net/
UIC (International Union of Railways): https://uic.org/
Site SBB – Smart Rail 4.0: https://smartrail40.ch/
Site EULYNX: https://www.eulynx.eu/
Site OCORA: https://github.com/OCORA-Public
RCA: https://ertms.be/workgroups/ccs_architecture
Shift2Rail (S2R): https://shift2rail.org/
GNSS: http://www.ersat-ggc.eu/; http://gate4rail.eu/
CCRCC 2019: https://www.era.europa.eu/content/ertms-ccrcc-%E2%80%93-ertms-conference_en

Chapter 4
Chinese Train Control System

Jidong Lv and Tao Tang

4.1 Introduction

4.1.1 Development Background

Train control system, as the core of railway signal system, is responsible for ensuring the safety of train operation and improving its efficiency. With the existing line speed-up and high-speed railway construction, the Chinese train control technology is confronted with new challenges. Traditional train control system including automatic block, cab signal, and automatic stop cannot meet the requirements of the existing line speed-up and high-speed railway. Developing Chinese train control system based on the requirements of high-speed railway and formulating an appropriate developing plan are the important tasks.

Several countries have developed train control system based on their own national conditions. Now, there are lots of train control systems being used in the world, such as UM2000/TVM430 of France, LZB of Germany, and ATC of Japan. Developing China train control system not only need drawing lessons from other countries in technologies, management, and practical application, but also taking care of our own national conditions.

According to what we mentioned above, the Chinese train control system should meet several requirements as follows:

- Satisfying transportation requirements of different level lines
- Realizing interoperability and ensuring safety when train operates in the across lines

J. Lv · T. Tang (✉)
School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China

State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
e-mail: 8438@bjtu.edu.cn; ttang@bjtu.edu.cn

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_4

- High-speed trains can run into the low-speed existing lines
- Standardizing to adapt the sustainable development of Chinese Railway

The purpose of CTCS (Ministry of Railways 2009) is to define a train control system for Chinese Railways to realize interoperability of train control system in the railway networks. In the future, all the train control systems, imported systems or local systems, wayside systems or on-board systems must be up to the CTCS standard. Apart from interoperability, the interface standard between the signaling systems, migration from the existing signaling to CTCS, data transmission format between the subsystems, safety and reliability, capacity increase, easy maintenance, lower investment, open market, etc. are considered during CTCS working.

The principles of CTCS are as follows:

- The different equipment of same level from different manufacturers should realize interconnection and interworking.
- The on-board system working on higher levels can be compatible with lower CTCS.
- Level transition should be completed automatically when transition conditions are met.
- Different levels of system should have clear layers; driver and equipment should have their own responsibilities.

Based on the current structure of signaling system on Chinese Railway Network, referring to ETCS (E. U. G. UNISIG 2012), CTCS is divided into the following five levels.

1. CTCS-0
   It consists of the existing track circuits, universal cab signaling (the digital), and microprocessors-based cab signaling that are compatible with the six kinds of track circuits on Chinese Railway Network and train operation supervision system. With level 0, wayside signals are the main signals, and cab signals are the auxiliary signals. It is the most basic mode for CTCS. It is not necessary to upgrade the wayside systems for CTCS level 0. The only way to realize the level 0 is to equip with the on-board system. CTCS level 0 is only for the trains with the speed less than 120 km/h.
2. CTCS-1
   It consists of the existing track circuits, transponders (or balises), and ATP system. It is for the train with the speed between 120 and 160 km/h. For this level, the block signals could be removed, and the train operation is based on the on-board system ATP that is called as the main signals. Balises must be installed on the line. The requirements for track circuit in blocks and at stations are higher than those in level 0. The control mode for ATP could be the distance to go.
3. CTCS-2
   It consists of track circuits with multi-information, balise, and ATP system. It is used for the trains with the speed higher than 160 km/h. There may be no wayside signaling in block for level 2 anymore. The control mode for ATP is the distance to go. The digital track circuit can transmit more information than

analog track circuit. ATP system can get all the necessary information for train control. With this level, fixed block mode is still applied. The system indicates the special feature of Chinese railway signaling. It is also called "a points and continuous system."

4. CTCS-3

   It consists of track circuits, balises, and ATP with GSM-R. In level 3, the function of the track circuit is only for train occupation and train integrity checking. Track circuits no longer transmit information concerning train operation. All the data concerning train operation information is transmitted by GSM-R. GSM-R is the core of the level. At this level, the philosophy of fixed block system is still applied.

5. CTCS-4

   It is the highest level for CTCS. Moving block principle can be realized by level 4. The information transmission between trains and wayside devices is made by GSM-R. GPS or balises are used for train position. Train integrity checking is carried out by on-board system. The wayside equipment is reduced in order to lower the maintenance cost of the system. Train dispatching can be made to be very flexible for the different densities of train operation on the same line.

Relationships between different levels of CTCS are clear. Level transition should be completed automatically. An automatic train protection system should meet the whole operation of a train, and the on-board system working on different levels should be compatible with lower levels. The trackside system and on-board system can work on lower levels when system breaks down, in which the level transition process should not have influence on the normal operation of train.

Note that, the division of CTCS is only preliminary. It could be changed a little bit during CTCS working. According to the above definitions, the function requirements specification (FRS) and the system requirements specification (SRS) have been started by the Chinese colleagues.

4.1.2 Hierarchical Structure of CTCS

The CTCS includes three layers: the traffic management layer, the network layer, and the control layer (ground device layer and on-board device layer), as shown in Table 4.1.

Table 4.1 Hierarchical structure of CTCS

Traffic management layer	
Network layer	
Trackside device layer	On-board device layer

1. Traffic management layer

   Traffic management of railway transport is the center controlling the operation of train. It completes the centralized control functions related to the operation of train. It synthesizes the analysis of factual conditions about train's operation, lines, devices, meteorology, etc. and completes the real-time control and management of train via communication network.
2. The network layer

   The transport network of CTCS lies in every layer, transporting data among ground and on-board systems through wire link or radio. Different layers have different requirements on the real time, reliability and safety of transport network.
3. The control layer

   - Trackside devices mainly include radio block center (RBC, for short), train control center, track circuit, point type device (balise), radio communication module, etc. According to different levels of CTCS, the configuration of trackside devices should be varied. The RBC (CTCS-3) or TCC (CTCS-2) is the core of trackside devices that generate movement authority according to the safe logical calculation, train control command, train routes, train operation conditions, and state of devices.
   - The on-board device layer is the key part of train control system, which has several kinds of control modes. It mainly includes on-board vital computer, track circuit reader (TCR), balise transmission module (BTM), radio transmission unit (RTU), driver–machine interface (DMI), train interface unit, judicial record unit, etc. The core of the control part within on-board system is the on-board vital computer.

Next, we will introduce CTCS-2 and CTCS-3 that are widely used during the development of Chinese high-speed railway in detail combining the abstract principles and knowledge mentioned above with concrete system application.

4.2 CTCS-2

4.2.1 The Main Features of CTCS-2

4.2.1.1 Information Transmission

Information transmission medium is the track circuit and the balise. Track circuit provides the cab signal, while balise supplies the route information in the station, the line data, and the temporary speed restriction.

1. It is the main difference to apply the unified format of track circuit between China and the ERTMS. The CTCS-2 makes full use of the existing information of track circuit.

2. Applying the balise's data and the temporary speed restriction information to meet the needs of locomotives and motor trains running across the railway lines. Chinese locomotive and motor trains run in long crossing road, and the ways are not fixed. The way of Japan's ATC system that the on-board system storages track data is not suitable; the balise can make full use of the mature equipment and specifications.

4.2.1.2 Control Method

The CTCS-2 uses the "distance-to-go" mode curve to control:

1. The existing main line signal distribution is designed in accordance with the speed difference. The target distance signal distribution method of CTCS-2 avoids the adjustment of the signal distribution.
2. The distance-to-go mode conforms to the international development trend of train control system.

4.2.1.3 Control Mode

The CTCS-2 uses "ATP with high priority control mode":

1. Europe uses "The driver's braking is preferred" mode and Japan uses "ATP with high Priority" mode.
2. The on-board system of CTCS-2 uses "ATP with high Priority" mode.

4.2.1.4 Mixed Transportation

1. The train equipped with CTCS-0 on-board system and low-speed train can run in CTCS-2 lines according to CTCS-0.
2. The EMU equipped CTCS-2 on-board system can run in CTCS-0 lines according to CTCS-0 mode.

4.2.2 Basic Functions of CTCS-2

The CTCS-2 is a new generation of automatic train control system, consulting the advanced technologies of other train control systems, based on the specification of CTCS (Ministry of Railways 2008). It is designed to meet the requirements of high-speed train whose speed is 200 km/h.

It is based on the multi-information track circuit (ZPW2000, for example) and point devices (balise, for example). Its trackside equipment and on-board equipment are designed integrated, and the basic functions of CTCS-2 are described as follows:

1. Information of the on-board equipment is from track circuit and point devices and recorded within the on-board database.
2. The on-board device can choose the highest level of running speed.
3. When running across railway lines, it should meet the requirements of controlling train at all time, and trackside device should be corresponded modified.
4. The on-board should have the function of checking the direction of the train running (upward or downward).
5. Protecting train from overrun a signal, and a safe protection distance should be used according to system's safe requirements.
6. Preventing train's speed from being higher than permitted speed, static speed restriction, and transient speed restriction; a command of temporary speed restriction is given by centralized traffic control system or local temporary limit speed unit; level and field of limit speed should meet the operation requirements.
7. Protect train's speed higher than permitted speed when it is in shunting mode.
8. Wheel slide and wheelspin should not affect the operation of the on-board system.

4.2.2.1 Main Functions of CTCS-2 On-board System

The basic functions of CTCS-2 are full filled by trackside system and on-board system integrated. Basic functions of CTCS-2 on-board system need to be mentioned according to the factual requirements of system. Main functions of CTCS-2 on-board system are as follows:

1. Reading information from track circuit

   The on-board system has the ability of receiving several carrier frequencies. Within the section of CTCS-2, the on-board system locks the carrier frequency through information of balise.
2. Reading information from balise

   The on-board system can receive information from balise according to the specification named "Message definition and application rules of balise within CTCS-2's field."
3. Measuring speed and calculating distance

   The on-board system monitors train's speed and calculates the distance of train and corrects the deviation brought by wheelspin or wheel slide.

   The on-board system can compute train's position according to the information from balise; position correction between two balises can be completed by checking the border of track circuit.
4. Interactive with driver and machine

   Driver–machine interface (DMI) of the on-board system displays train's current speed, permitted speed, target speed, and target distance to driver. DMI has audible and visual alarm function and can generate alarm or display the corresponding state for over-speed, losing traction, braking, breaking down, break releasing, or failure states.

DMI has data input function, and some information of train-related parameters can be input through it; the input operation shall be concise and clearly. The on-board system shall make rationality and correctness checking to the crew input data and operation process.

5. Over-speed protection

   The over-speed protection function of the on-board system takes the measures of audible and visual alarm, traction removal, service braking, and emergency braking. When the train speed exceeds the speed restriction of service braking or emergency braking, the service braking or emergency braking will be applied to slow down or stop the train (here, the electric braking force cannot be removed when the locomotive is in electric braking). After the implementation of the service braking, it can be artificially released only when the train speed is below the permitted speed. While once the emergency brake is implemented, it cannot be artificially intervened until the train stops completely.

6. Runaway protection

   Standstill detection function will be done when the train speed is below a pre-set speed value for some time. The speed value and duration time should be determined based on the characteristics of the device and meet the application requirements.

   In standstill detection state, the on-board system shall take some measurements to prevent the movement of the train and apply brake command sustainability.

7. Record function

   The recording unit can record the input, output, and operation states of the on-board system and reproduce the working states of the on-board system by using the recorded data.

4.2.2.2 Main Functions of CTCS-2 Trackside System

The CTCS-2 trackside system consists of equipment providing continuous train control information: ZPW-2000 (UM series) simulative track circuit, digital track circuit, and reserved wireless communication transmission system (GSM-R) and equipment providing spot information: analog loop, digital loop, and balise. Intermittent transmission device shall be installed in station or in the approaching and leaving sections of a station. Failure and error of the trackside system should not lead to dangerous consequences.

The main functions of the trackside system are:

1. Continuously monitoring the state of information transmission channel; safety measures must be taken when the channel interrupted.
2. Intermittent transmission device is set in position of the home/starting signal; emergency brake will be triggered when the train aggress stop signal.

3. In order to avoid collision, a protection distance should be reserved between locomotive and the home/starting signal; when the distance condition is not satisfied, it is must be ensured by setting another extended route.
4. The train control center sets MA, calculates static speed curve according to train's occupancy and route state, and then transmits them to the train.
5. The train control center shall be provided with a local monitoring station to record the working state of the trackside system and realize dynamic monitoring.

4.2.3 The System Structure of CTCS-2

- The main functions of the CTCS-2 are jointly realized by the trackside system and on-board system. The trackside system is composed of train control center, track circuit, and intermittent transmission device. The main functions are as follows: the train control center (TCC) encodes active balise according to temporary speed restriction (TSR) and route state.
- Track circuit (TC) checks the track occupancy and train integrity and continuously transmits the number of non-occupied sections in front of the train.
- Intermittent transmission device transfers the positioning information, route information, line parameters, and temporary speed restriction information to the on-board system.
- The on-board system generates distance to go according to the information from the track circuit and intermittent transmission device.

The CTCS-2 includes the on-board system and the trackside system. The trackside system is composed of lineside equipment unit (LEU), TC, interlocking (IL), TCC, centralized traffic control (CTC), TSR, and microcomputer monitor (MM). The on-board system is composed of special transmission module (STM), balise transmission module (BTM), train interface unit (TIU), data recording unit (DRU), on-board vital computer (VC), and driver–machine interface (DMI). The main functions are as follows:

1. STM receives and handles the track circuit information.
2. BTM receives and handles the balise information.
3. DRU records the received messages, system states, and control actions.
4. VC handles train operation control information, generates distance-to-go curve and controls the train running by commands.
5. DMI is a platform for the interaction between the on-board system and locomotive crew.

CTCS-2 system structure shown in Fig. 4.1:

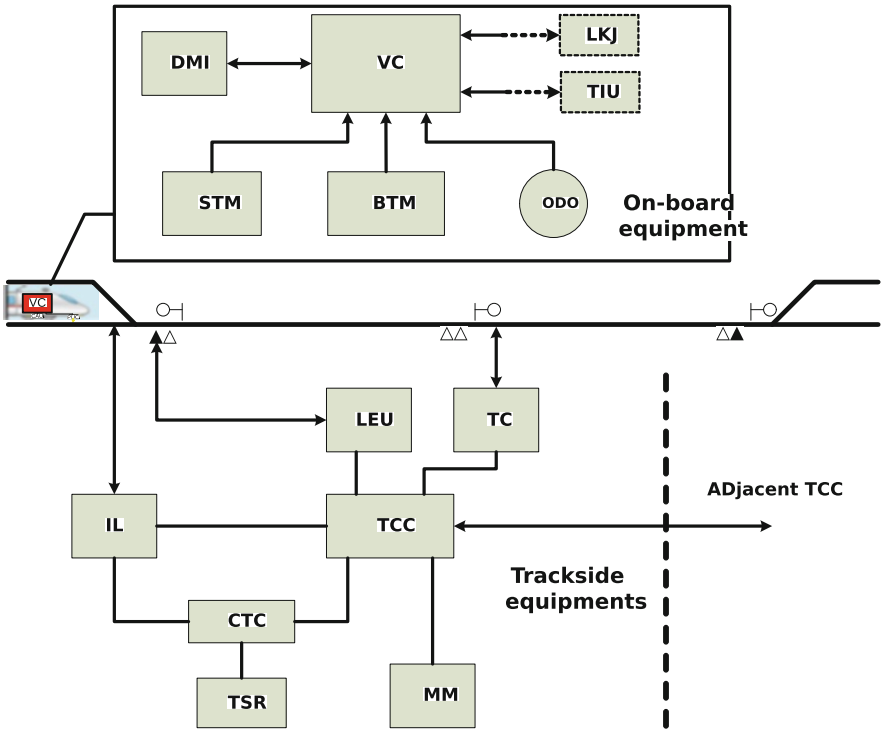


Fig. 4.1 The structure of CTCS-2

4.2.4 The Modes of CTCS-2

According to the operational requirements of CTCS-2, the on-board system has several working modes to meet all the operational requirements efficiently. The CTCS-2 on-board system has standby mode (SB), full supervision mode (FS), partial supervision mode (PS), shunting mode (SH), on-sight mode (OS), isolation mode (IS), etc. The modes are introduced below:

1. Full supervision (FS)

   The on-board system shall generate the distance-to-go curve to control train running safely when all basic data (track circuit information, balise information, and train data) are available. DMI shall display the train speed, permitted speed, and the target speed to the driver.
2. Partial supervision (PS)

   The on-board system shall generate fixed speed restriction to control train running when track circuit permitting is available. The PS mode contains the following two conditions:

(a) When two or more consecutive balise information lose, the on-board system shall trigger service brake immediately. When the train speed is dropped less than 120 km/h, it offers tips to allow us to release the brake. After the driver releases, the on-board system generates speed monitoring curve (the maximum restriction speed is 120 km/h) according to the most unfavorable conditions to control the train.
(b) When a train departs from the side line, the on-board system forms and maintains a fixed speed restriction according to the track circuit information to control the train.

3. On-sight (OS)
   When the on-board system displays stop signal, the driver makes special operation (such as pressing a dedicated button) according to the train operation rules; meanwhile, the on-board system shall generate a fixed speed restriction (20 km/h) to control the train safety running.
4. Shunting (SH)
   According to the shunting operation, it will convert into shunting mode after the driver takes some special operation (such as pressing a dedicated button), and the on-board system shall generate shunting speed restriction for the train controlling.
5. Isolation (IS)
   When the on-board system fails, brake command shall be triggered and the train will enter this mode; the driver makes some special operations by scheduled orders, while control function of on-board system is deactivated.

4.3 CTCS-3

4.3.1 Main Features of CTCS-3

4.3.1.1 High technical Integration

The CTCS-3 integrates the general technical solutions, from a technical proposal of high-speed train control system that meets China's national conditions and railway conditions:

1. integrating the communication signal system, establishing the CTCS-3 train control system based on the wireless communication technology, and forming the high-speed railway communication network;
2. The integration of CTCS-2 and CTCS-3 meets the command of the across-line operation under "a net" planning. When the GSM-R network fails, CTCS-3 degrades to CTCS-2 automatically, which improves the usability of the system.

4.3.1.2 High-Quality Development

It makes a breakthrough in 350 km/h high-speed train control system simulation test technology and sets up all fronts, panoramic, full-speed comprehensive simulation test platform, and the whole test method.

1. Researching and establishing CTCS-3 train control system platform based on the semi-physical simulation automatically. This platform can verify the project, research, and develop the key equipment, integrate the system, test the engineering data, test interconnection and interworking, and test failure of CTCS-3 train control system.
2. Providing long-term technical support for the research of train control technology, product development, and sustainable development of maintenance.

4.3.1.3 Well Standardization

It creates a complete technical standard system of CTCS-3 train control system:

1. Creating a technical standard system of high-speed rail CTCS-3 train control system that meets the national conditions, railway conditions, interconnects, and interworks and has the world first-class level
2. Setting down a standard specification for all aspects including research and development, production, construction, and maintenance and, according to the standard of first principles, carrying out technical innovation
3. Laying a solid foundation for China's high-speed railway train control technology rapid development

4.3.2 Basic Functions of CTCS-3

Different from CTCS-2, in CTCS-3, the trackside system transfers track data, interlock routing, and temporary speed restriction through GSM-R radio network. It has significantly improved the performance as the trackside system can receive train data and train state through bi-directional trackside-on-board communication on real time to supervise the train.

The basic functions of CTCS-3 are as follows:

1. It displays necessary information to the driver for safety driving.
2. It supervises train operating and shunting.
3. Train controlled by (RBC) can only run in RBC area with the authority of RBC.
4. It satisfies the requirements of 350 km/h and more for operation speed, 3 min for minimum tracking interval.
5. It satisfies operation demands of line crossing.
6. It tracks occupation checking.

7. It adopts fixed automatic block and uses distance-to-go mode curve to control train.
8. It contains two control modes, device braking priority and driver braking priority.
9. It contains the function of service brake and emergency brake to supervise train speed.
10. The trackside system can set temporary speed restriction and send it to the on-board system.
11. It is compatible with CTCS-2 functions.

Technical characteristics of the CTCS-3:

1. GSM-R radio is for bi-directional trackside-on-board communication.
2. RBC is for MA generation.
3. Track circuit is used for train occupation.
4. Balise is used for location referencing.
5. It is compatible with CTCS-2 functions.

4.3.2.1 Main Functions of CTCS-3 On-board System

The CTCS-3 on-board system shall realize the following functions:

1. Speed/distance measurement
   The on-board system cooperates with speed/distance measurement unit (SDU) to get the train's speed and distance by processing the output of speed sensor and radar signal. By comparing the current train acceleration and the maximum acceleration of the train, the wheel slide and wheelspin can be judged.
2. Wireless communication management
   The on-board system shall communicate with RBC, report its train data, train position and receive MA, and track parameters through GSM-R. And also, the on-board system shall manage the link of wireless communication, which contains several processes including registering to the wireless network, establishing a session, maintaining a session, and terminating a session.
3. Handling of balise information
   The on-board system gets track information from balise through BTM antenna, which includes wireless registration, level transition, communication management, and RBC/RBC handover information.
4. Speed monitoring
   Speed monitoring function of the on-board system is responsible for monitoring the permitted speed of the train, including: train construction speed, track limit speed, and temporary speed restriction. The train construction speed is obtained through the on-board system configuration file; track limit speed and temporary speed restriction are obtained from RBC. The on-board system generates the distance-to-go curve according to the speed restriction information.
5. Forward and backward movement protection

Forward protection means that the on-board system shall protect against inappropriate movement after the train stops. If an unexpected forward or backward movement happens, the on-board system shall apply the brake command.

6. Level transition

   The level transition is a specific function between CTCS-3 and CTCS-2. The on-board system should manage level transition between CTCS-3 and CTCS-2 according to the level transition command and wireless information from RBC. The level transition may happen when train runs from CTCS-3 area to CTCS-2 area or vice versa.

7. Driver–machine interface

   The driver inputs some information such as driver ID, train ID, train length, etc. It can display the train's current speed, target speed, permitted speed, geographic information, target distance, and text messages and warning messages to the driver in graphic, text, and sound ways.

8. Emergency brake message processing

   The emergency stop message can be divided into conditional emergency brake message and unconditional emergency brake message. When an unconditional emergency brake message is received, the on-board system shall output emergency braking command immediately; when a conditional emergency brake message is received, the on-board system shall accept or reject according to actual situations and then output the corresponding control command.

9. Data storage

   Juridical recorder unit, an equipment of the on-board system, can record information such as driver behaviors, trackside-on-board interact information, braking output, and working status of the on-board system.

4.3.2.2 Main Functions of CTCS-3 Trackside System

The main functions of the trackside system can be divided into the following several aspects according to different realization devices:

1. Train management function

   When a train enters into a CTCS-3 area, the CTCS-3 trackside system completes the registration and initialization of the train according to the current state. And also, when a train leaves, it shall complete the logout process interacted with the on-board system.

2. Level transition function

   When a train enters or leaves its CTCS-3 control area, the CTCS-3 trackside system shall activate level transition function to control the train to upgrade or degrade its levels.

3. RBC handover function

   The CTCS-3 trackside system can handle the handover of train control right from one RBC to an adjacent RBC through the communication between RBC

and the trackside-on-board interaction, letting the train running through RBC boundary without stops.

4. MA function

   The CTCS-3 trackside system generates MA and sends it to a specific on-board system to control the train running safely.

5. Temporary speed restriction function

   The temporary speed restriction commands are managed and maintained intensively by the trackside system of CTCS-3. The trackside system can check the consistency of the CTCS-2's temporary speed restriction and CTCS-3's.

4.3.3 The Structure of CTCS-3 System

According to the classification of the train control system, the CTCS-3 train control system is divided into two parts: trackside system and on-board system. On the basis of CTCS-2, the radio block center (RBC) and GSM-Railway (GSM-R) are added into the CTCS-3 trackside system. RBC generates movement authorities based on the track occupation information and the route information and sends it to the specific trains through GSM-R network. The external environment of CTCS-3 includes: train, driver, GSM-R radio communication system, on-board system interface, interlocking and centralized traffic control, and so on. The GSM-R radio communication system is the bi-directional transmission channel between the on-board system and the trackside system.

The structure and the interfaces of CTCS-3 are shown in Fig. 4.2.

4.3.3.1 Trackside System of CTCS-3

The trackside system of CTCS-3 train control system is comprised of the radio block center (RBC), temporary speed restriction server (TSRS), track circuit, train control center (TCC), balise/lineside electronic unit (LEU), the GSM-R interface, and so on. The functions of each unit are as follows:

1. Radio block center (RBC): The RBC generates messages based on the information received from external trackside system; the main objective of these messages is to provide movement authorities to allow the train to move safely in the RBC control area.
2. Temporary speed restriction server (TSRS): The TSRS manages the temporary speed restriction commands and transfers them to RBC and TCC respectively.
3. Track circuit: Track circuit detects the occupation of a track section by a train provides the free-occupation information for the on-board equipment responses for coding track circuit, and then sends them to RBC; and finallysends temporary speed restriction information and route information to the on-board system of CTCS-2 train control system via lineside electronic unit (LEU).

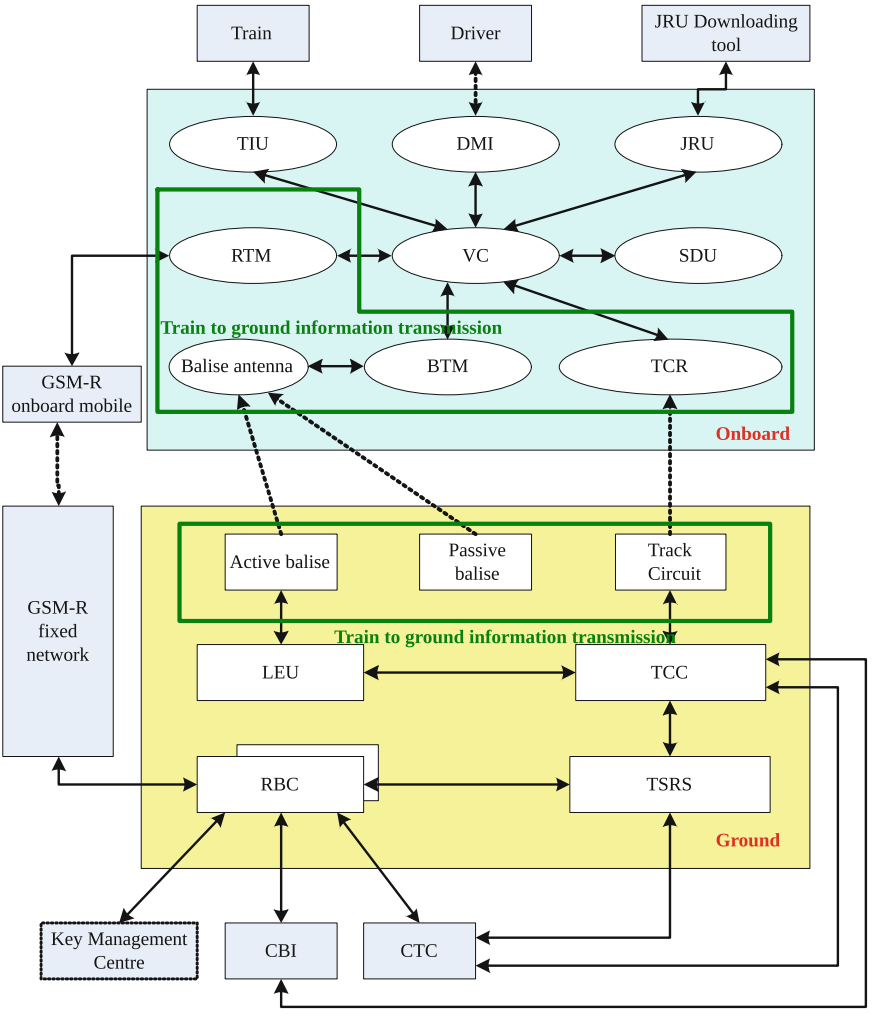


Fig. 4.2 Structure and interfaces of CTCS-3

4. Balise: It is an intermittent transmission device that can send messages to the on-board system. It provides the uplink for messages from the trackside system to the on-board system. It can provide fixed message to the on-board system and programmable messages to track circuit center.
5. Lineside electronic unit (LEU): Lineside electronic unit is an electronic device that generates messages to be sent by balise.

4.3.3.2 On-board System of CTCS-3

The on-board system of CTCS-3 consists of vital computer (VC), track circuit reader (TCR), balise transmission module (BTM), radio transmission module (RTM), driver–machine interface (DMI), train interface unit (TIU), speed and distance unit (SDU), juridical recorder unit (JRU), and so on. The functions of each unit are as follows:

1. Vital computer: Supervises the movement of the train on the basis of information exchanged with the trackside system
2. Track circuit reader: Receives the information from the track circuit
3. Balise transmission module and balise antenna: Connects with the balise antenna and receiving the information from the balise
4. Radio transmission module: Connects with the GSM-R on-board radio to realize trackside-on-board information transmission
5. Driver–machine interface: Exchanges interaction information between driver and the on-board system
6. Train interface unit: Provides the interface between on-board equipment and vehicle's related equipment
7. Speed and distance unit: Receives the signal from the speed and distance sensors, measuring the speed and distance of the train
8. Juridical recorder unit: Records the data of the train and provides data to analysis when it needed

4.3.4 Operation Scenarios and Driving Modes of CTCS-3 System

4.3.4.1 Operation Scenarios of CTCS-3 System

The difference between the CTCS-3 and CTCS-2 is the different information transmission methods between on-board equipment and trackside system. The CTCS-2 train control system transmits the train control information via track circuit and balise. The CTCS-3 train control system transmits train control information via GSM-R network.

According to the railway transportation's characteristics and the actual situations in China, 14 operation scenarios have been proposed with a full consideration of the requirement train operation in normal situation, special situation, and also fault or disaster situation (Shuguang 2008).

The Operation Scenarios in Normal Situations

The operation scenarios in normal situation contains: mission start, logout, movement authority, RBC handover, auto-passing phase-separated section, and so on.

1. Mission start

   This scenario describes the operation process of the on-board system by powering on, activating the platform, and starting the train when conditions are met.
2. Logout

   This scenario describes the operation process from RBC's logging out information of the train to shut down the power of the on-board system when the train stops.
3. Level transition

   This scenario describes the process of level transition when the train is on the boundary of CTCS-3 section and CTCS-2 section.

   In the level transition process, the CTCS-3 control unit and the CTCS-2 control unit shall communicate with each other to avoid triggering the emergency braking of the train, as shown in Fig. 4.3.
4. Movement authority

   Movement authority scenario describes the process that a train obtains the MA in CTCS-3 control area.

   MA is the authority for safe movement of a train. In the CTCS-3 control area, RBC receives signal authorization (SA) from interlocking to generate MA and sends it to the on-board system.
5. RBC handover

   RBC handover scenario describes the process to realize the safe handover of train's movement authority between two RBCs in the boundary of different RBCs, as shown in Fig. 4.4.
6. Auto-passing phase-separated section

   This scenario describes that the on-board system sends related commands to the phase-separated section device in the proper position for auto-passing phase-

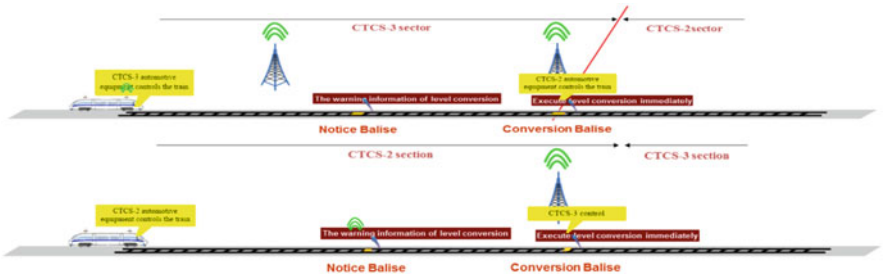


Fig. 4.3 Level transition scenario

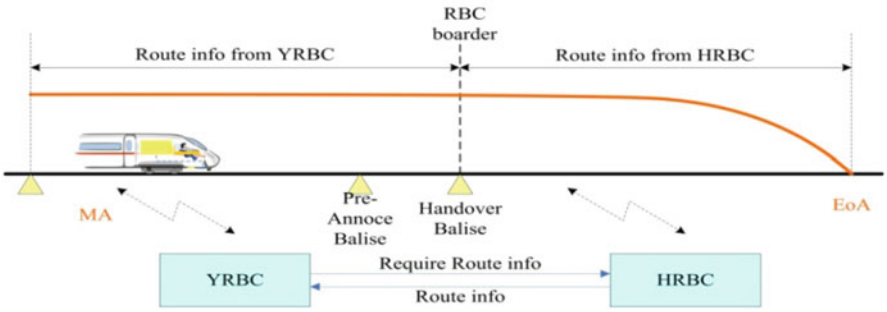


Fig. 4.4 RBC handover scenario

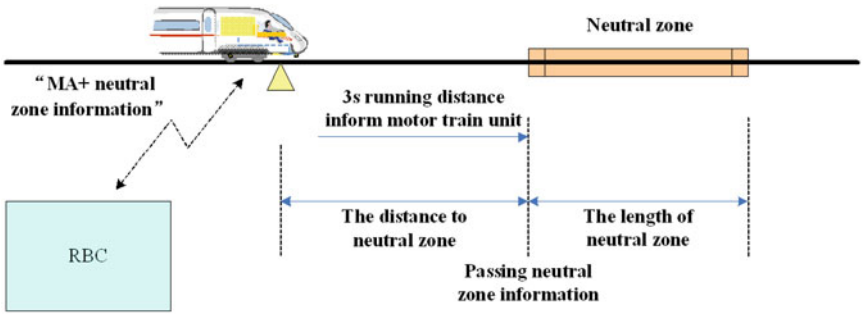


Fig. 4.5 Auto-passing phase-separated section scenario

separated section according to the phase-separated section information provided by the trackside system, as shown in Fig. 4.5.

The Operation Scenarios in Special Situations

The operation scenarios in special situations include multiple and breakup, temporary speed restriction, shunting, and releasing route manually.

1. Multiple and breakup

   The multiple of trains is the process of two EMUs with the same type that are sent to the same track station to build up a new train.

   The breakup of train is to divide the train parking in a station track into two trains. The two divided trains could go to the section or transfer to other lines in the same or opposite direction.
2. Temporary speed restriction

   Temporary speed restriction scenario describes the process of setting, issuing, and canceling the temporary command in the dispatching station.

The setting and canceling of the temporary speed restriction are carried out in the dispatching station. The principles of setting and canceling the temporary speed restriction are the same.

3. Shunting

   The shunting scenario describes the process of entering into the shunting mode, shunting protection, and exiting from the shunting mode.

4. Route releasing manually

   This scenario describes the process of canceling routes that have been set for train's arriving or dispatching.

The Scenarios in the Fault and Disaster Situations

The operation scenarios in fault or disaster situations include: degraded situation, disaster protection, and special route scenarios.

1. Degraded situation

   This scenario describes the process of entering into the backup mode of the train control system after the trackside system or on-board system breaks down.

   The fault conditions include: the abnormal occupation of track circuit in blocks and station, the failed display of switch, the broken filament of signal, and network failures.

2. Disaster protection

   This scenario describes the emergency reaction of the signal system when unforeseen situations happen. It includes the protection of wind, rain, snow, landslide, falling object, and emergency of the station platform.

3. Special route

   This scenario describes the running process based on the block between railway stations.

4.3.4.2 Driving Modes of CTCS-3 System

According to the operation requirements of the CTCS-3 train control system, the driving modes of the CTCS-3 on-board system are set up to achieve different functions in different modes. The modes of CTCS-3 on-board system include standby mode (SB), full supervision mode (FS), shunting mode (SH), sleeping mode (SL), isolation mode (IS), call-on mode (CO), and on-sight mode (OS). The application of each mode and the transitions between modes are introduced as follows.

1. Standby (SB)

   When the on-board system is powered on, the system shall enter into standby mode initially. In this mode, the train is not allowed to move.

2. Full supervision (FS)

   The on-board system shall enter into the full supervision mode automatically when all basic data (including train data, movement authority, and track data) are

available. In this mode, the on-board system should generate the dynamic train speed profile to supervise train safe movements and display the train speed, the permitted speed, the target distance, and the target speed to the driver via DMI as shown in Fig. 4.6.

The speed profile and other information that DMI shows in the FS mode are stated as Fig. 4.7.

3. Call-on (CO)

When the calling-on signal is given, the on-board system enters into the CO mode. As is shown in Fig. 4.8, in the CO mode, the on-board system generates the dynamic train speed profile and DMI shows the train speed, the permitted speed, the target distance, and the target speed, and so on. The on-board system supervises the train with the fixed 40 km/h speed restriction, and the driver is responsible for checking the track occupation.

4. On-sight (OS)

When the trackside system is failed, the on-board system shall enter into the OS mode. In the OS mode, the on-board system supervises the train with the fixed 40 km/h speed restriction that needs to be acknowledged once at intervals (300 m or 60 s), as shown in Fig. 4.9.

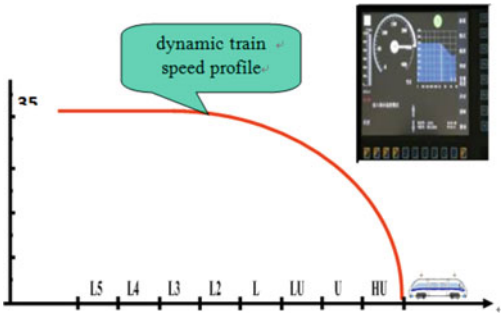


Fig. 4.6 The control profile of the train in the FS mode

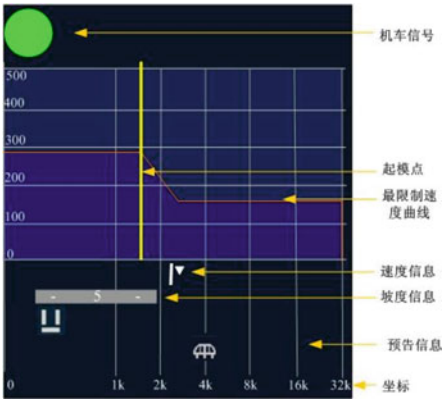


Fig. 4.7 The speed profile in the FS mode

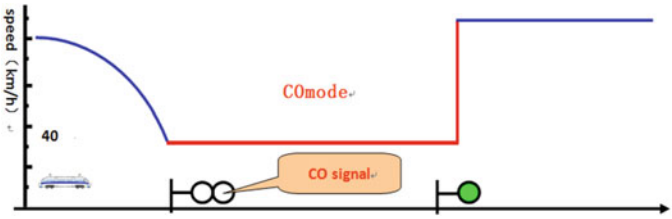


Fig. 4.8 CO mode

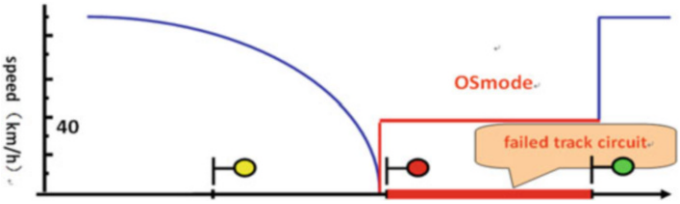


Fig. 4.9 OS mode

5. Shunting (SH)
   When the train stops, the driver chooses shunting command in the SB, FS, OS, CO, and PT modes, and the system shall go into the shunting mode. The on-board system supervises the train with the fixed 40 km/h speed restriction, and the driver is responsible for checking the track occupation.
6. Isolation (IS)
   The on-board system shall be in the isolation mode when the system is out of service. In this mode, the braking function is isolated, and the on-board system does not realize the safety supervising function.

4.3.5 The Comparison of the CTCS-3 and ETCS-2

The principles for ETCS-2 and CTCS-3 are very similar. They are, respectively, the development requirements of the European Railway Network and Chinese Railway Network. The key technical issues, such as interoperability, safety, reliability, vital computers for on-board system and control center, and easy and moderate investment and maintenance, are the same as in ETCS-2 and CTCS-3. This is the result of modern mobile communication development. Based on the reliable and fail-safe communication, train control system becomes a closed-loop safety control system to ensure train operation safety and efficiency (Ning et al. 2004).

4.3.5.1 Differences from Static Structure

From a static construction perspective view, the main difference between the CTCS-3 and ETCS-2 is that the CTCS-2 may be used as a backup mode of CTCS-3. The train from a high-speed railway line can run to a lower-speed existing railway line. Even more, when the GSM-R network fails, the CTCS-3 can be degraded to CTCS-2 automatically. In this way, the usability of the system can be improved.

In CTCS-3, track circuits still play a very important role. On Chinese Railway Network, track circuit is mostly used and is the basis of train control systems. It is not possible to construct CTCS-3 without track circuit. This is the reality of Chinese Railway.

4.3.5.2 Differences in the Control Mode

Intuitively, some of the dynamic operation scenario behaviors are not the same; here, we mainly focus on the differences of control modes using between ETCS-2 and CTCS-3.

There are 11 control modes (including CTCS-2 as a backup mode) in CTCS-3 as listed above, which are FS, OS, CO, SH, SB, TR, PT, IS, and SL (in CTCS-3) and PS and CS (in CTCS-2); whereas there are 13 control modes in ETCS-2, which are FS, OS, SR, SH, SL, SB, TR, PT, SF, IS, NP, NL, and RV.

- Specific control modes in ETCS-2

  NP (before power on) and SF (fail-safe) control modes are the specific modes in ETCS-2 for on-board equipment. In CTCS-3, these control modes are not considered as control modes but intermediate states. NL and RV are the specific control modes related to specific operation scenarios in European countries, whereas these scenarios are not operated in China.
- Specific control modes in CTCS-3

  As the CTCS-2 is the backup mode of CTCS-3, the PS and CS control modes are the specific control modes in CTCS-3. The PS and CS control modes are merely in CTCS-2 on a lower-speed limitation restriction when the GSM-R network fails or a train runs to an existing railway line.
- Control modes with different conditions

  There are some control modes with same functions but with different conditions to use, like OS, CO, SR, and SL.

  The OS control mode in CTCS-3 is the same as the SR control mode in ETCS-2, whereas the OS control mode in ETCS-2 is the same as the CO control mode in CTCS-3. But different functions are designed in spite of the same name. For example, although in SR control mode in ETCS-2 (response to OS in CTCS-3), the train will be supervised under 40 km/h, wherever the train can be transferred to other control modes like CO due to the signal telegrams received from track circuit, which is not permitted in ETCS-2.

SL control mode has the same name in both CTCS-3 and ETCS-2, but with different functions. When in SL control mode in CTCS-3, the DMI will continuously display movement authorities (received from its backup mode CTCS-2), while in ETCS-2, the SL control mode is used to control its non-leading on-board equipment.

In a word, there are a lot of common points between ETCS and CTCS. However, they are different. CTCS is a standardization of railway signaling system for Chinese Railway. Anyhow, it is true that CTCS could learn from ETCS during its construction process. It is hard and too early to say that ETCS and CTCS would come as a standard for railway signaling system in the world in the future.

References

E. U. G. UNISIG. (2012). System Requirements Specification (SRS) version 3.2.0, E. R. Agency, Ed. [Online]. http://www.era.europa.eu

Ministry of Railways. (2008). *CTCS Level 2 train control system requirements specification (SRS) VI.O[M]*. Beijing: China Railway Publishing House.

Ministry of Railways. (2009). *CTCS Level 3 train control system requirements specification (SRS) VI.O[M]*. Beijing: China Railway Publishing House.

Ning, B., Tang, T., Qui, C., et al. (2004). *CTCS-Chinese train control system*[J]. Southampton: WIT Press.

Shuguang, Z. (2008). *The general technical programme of CTCS-3 level train control system in railways for passengers* (pp. 103–108). Beijing: China Railway Publishing House.

Chapter 5
Modelling of High-Speed European Railway Systems

Matthieu Perin

5.1 Introduction

Railways systems have increased in complexity during the last two decades due to two factors: the arrival of new modern and complex systems such as (ERTMS European Union Agency for Railways 2016), and the obligation of collaboration for such systems with aged legacy systems such as relay-based block logic controllers. High-speed train infrastructure and operation are the pinnacle of such complexity because they impose an even higher level of safety and quality to ensure correct and safe operations.

The usage of models has clearly helped in tackling the complexity of such system, especially in the domain of the control logic of train operation (Banci et al. 2004; Brownsword 2014). But to handle the ever-growing needs of safety (Liu et al. 2011), the modelling of the infrastructure needs also to be taken into account to ensure a complete modelling, validation and even verification of the whole system.

This chapter proposes an overview of some promising initiative of railway system modelling—including infrastructure and control system—to bring solutions for high-speed train infrastructure modelling. Section 5.1 is a quick presentation of UML and SysML destined for non-experts. Section 5.2 focuses on some direct modelling approaches that have provided dedicated model for railway infrastructure.

M. Perin (✉)
Institut de Recherche Technologique Railenium, Famars, France
e-mail: matthieu.perin@railenium.eu

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_5

5.2 Overview of UML and SysML Norms

In this section, a quick overview of both UML and SysML norms is given. Curious reader should read carefully the two related norms (Object Management Group 2015a,b) for a complete view of these modelling languages.

5.2.1 UML: The Base

As expressed in the defining norm (Object Management Group 2015b),

> The objective of UML is to provide system architects, software engineers, and software developers with tools for analysis, design, and implementation of software-based systems as well as for modeling business and similar processes.

Thus, UML is clearly software oriented and based on programme modelling—but in any case limited to that—using object-oriented principles.

UML is most known through its diagrams, and they are divided into two categories: *Structure Diagram*, which shows the static structure of the objects in the system, and *Behaviour Diagrams*, which show the dynamic behaviour of a system.

Figure 5.1 presents the list of all diagrams proposed by UML 2.5 norms. None of them are mandatory to be used, but in the rest of this chapter mainly *Class Diagram*

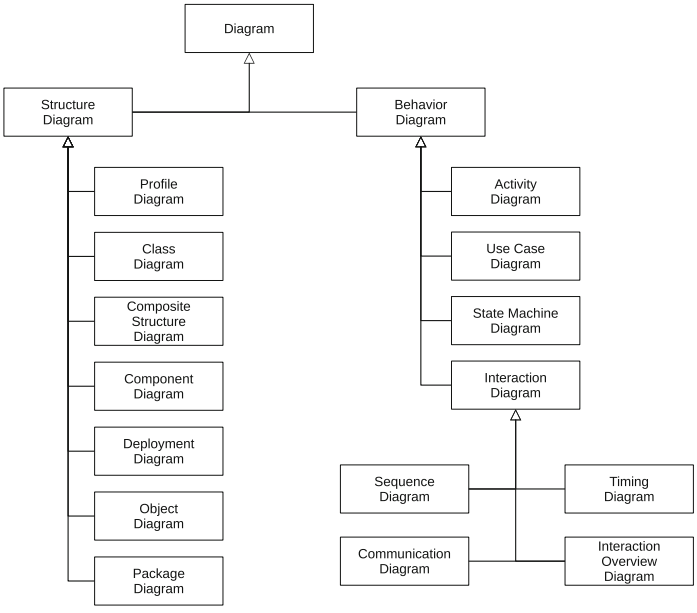


Fig. 5.1 Overview of proposed diagrams in UML 2.5 norm

will be used with sometimes some *Object Diagram*, *Profile Diagram* or *Sequence Diagrams*.

In the modelling community, UML *Classes* and *Association* are often used as an ontology to represent concepts and their interactions in a form of a meta-model like presented in Fig. 5.2.

Some works use *Profile* and associated *Stereotypes* to further define and specialise UML Object, as shown in Fig. 5.3.

Then, *Instance Specification* is sometimes used, as presented in Fig. 5.4, to represent a specific configuration of the infrastructure as a model form from the defined meta-model. For precision on these UML concepts and their usage, interested readers are proposed to carefully read UML norm (Object Management Group 2015b).

5.2.2 SysML: Addition for System Modelling

In Object Management Group (2015a), the objective of SysML is made clear:

> SysML is designed to provide simple but powerful constructs for modeling a wide range of systems engineering problems. It is particularly effective in specifying requirements, structure, behavior, allocations, and constraints on system properties to support engineering analysis.

This is achieved by the addition on UML of several diagrams: *Requirement Diagram*, *Parametric Diagram*, *Block Definition Diagram* and *Internal Block Diagram*, plus some modelling elements like *Block*,*ValueType*, *FlowProperty*, *Requirement* and the modification of existing ones such as *Association* and *Port*. All these objects are meant to help user to model and conduct analysis on cyber-physical system, such as train and railway infrastructure.

5.3 Modelling Railways and Trains

5.3.1 Component-Based Models

A direct approach towards modelling railway infrastructure is to decompose the network in portion and to model these using component-based approach. In Xiangxian et al. (2011), this methodology is coupled with a topology decomposition of the network, allowing to obtain an oriented graph as presented in Fig. 5.5. This representation is a powerful base to handle routing and interlocking algorithms but may lack some precision for other usages.

In Sun (2015), the infrastructure is directly modelled as tokens in a coloured Petri net. The resulting net is a straightforward implementation of the interlocking logic that handle route opening algorithm through token manipulation as partially

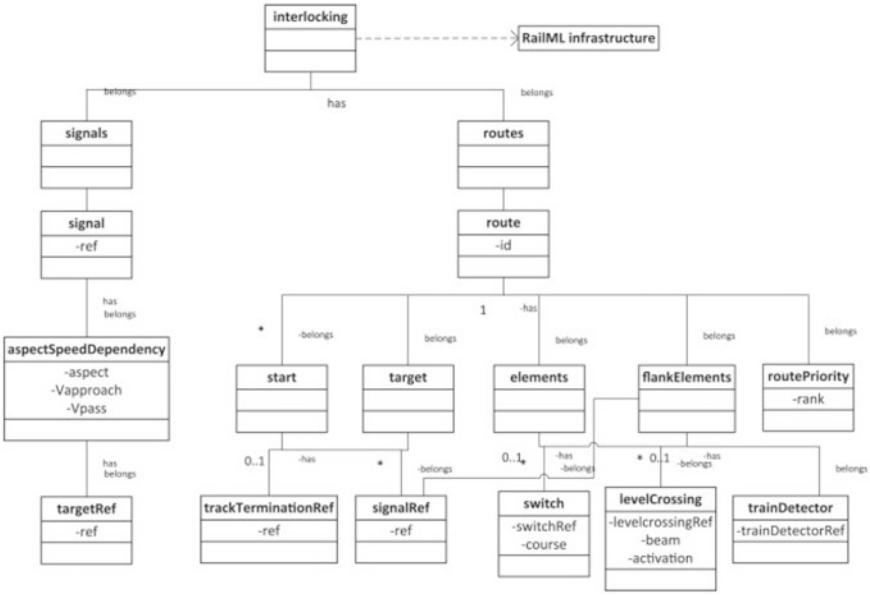


Fig. 5.2 Example of Class Diagram proposed in Bosschaart et al. (2015)

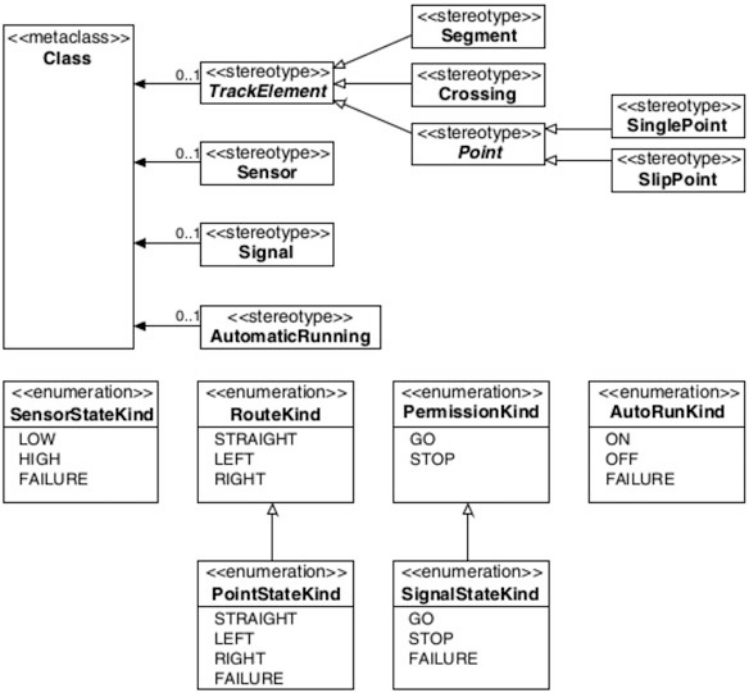


Fig. 5.3 Example of Profile Diagram from Berkenkötter and Hannemann (2006)

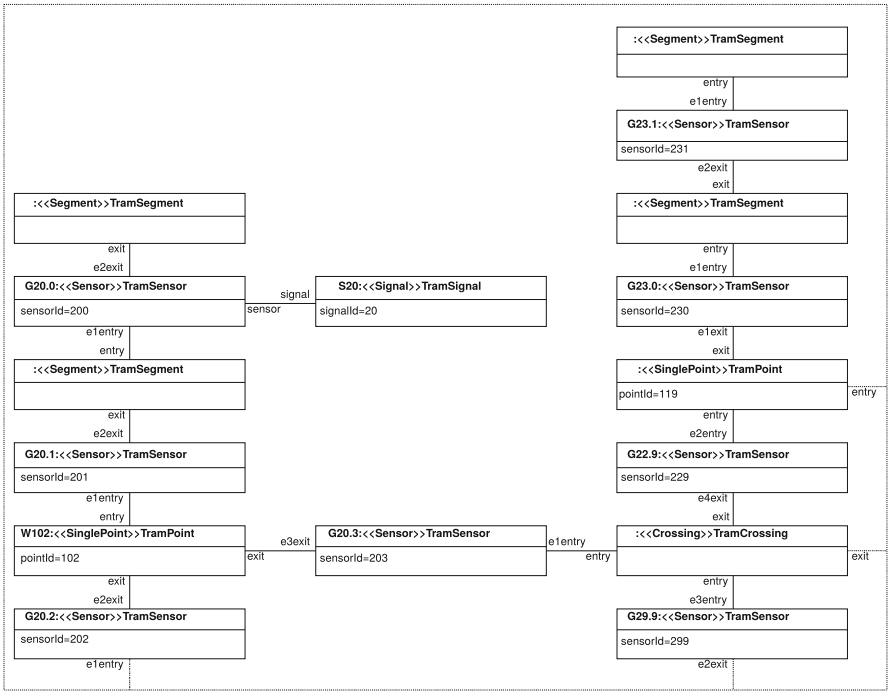


Fig. 5.4 Example of Instance Specification use from Berkenkötter and Hannemann (2006)

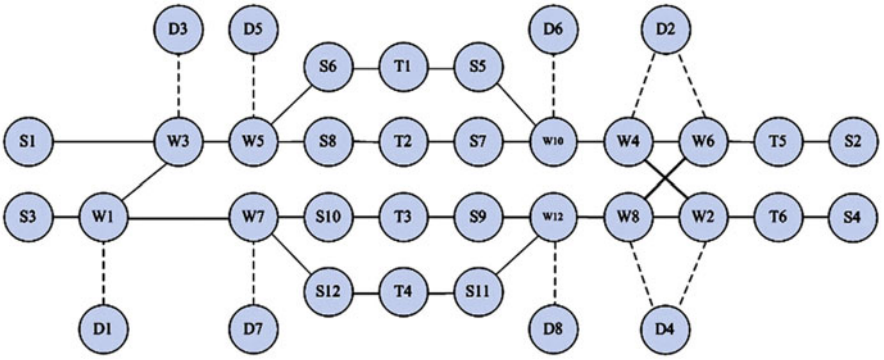


Fig. 5.5 The topological view of the network proposed in citeXiangxian11Componnent

presented in Sect. 5.3.1 (Fig. 5.6). Again, such modelling has obvious advantage in terms of calculation efficiency but may lack some detail for other usage such a safety analysis as the network is modelled in a set of coloured tokens and not directly.

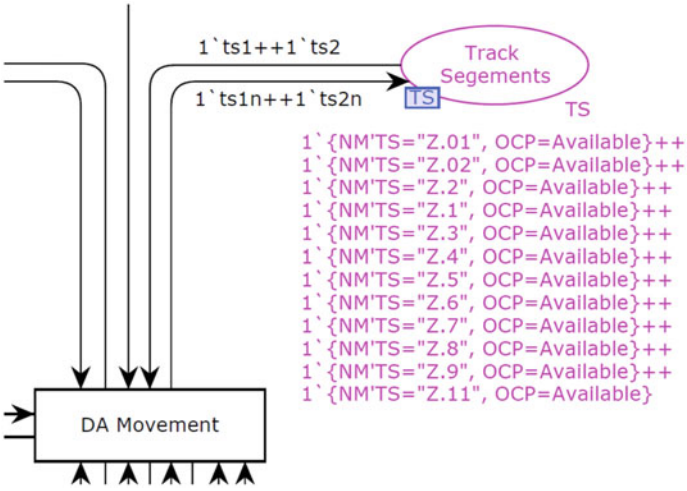


Fig. 5.6 Usage of coloured Petri nets for infrastructure modelling presented in Sun (2015)

5.3.2 Infrastructure Modelling Using UML SysML

The proposal of Hon et al. (2006) is to model the network in UML and to add some behaviours in state machine using Rhapsody. For a given network, the resulting model is then used to produce a NuSMV formal model to check against concurrent routes in the infrastructure. The strength of such approach is to allow flexibility using object-based language for the infrastructure description and to rely on formal language to handle the behavioural part using a well-known tool in this domain (Fig. 5.7).

Another way of exploiting UML description of the infrastructure is presented in Mecitoğlu and Söylemez (2013). In this work, the aim is to check SCADA application used for railway interlocking systems. The infrastructure is described in UML, and the behaviour is expressed using UML Statechart despite the fact that this formalism may be seen as *weak* because of the discrepancy in implementation (see Crane and Dingel (2007) for more details). An interesting fact of this proposal is the will to model the PLC to also consider a model of the implementation of the control algorithms. In order to check the complete behaviour, a translation to C++ coding language is performed, and the result code is then assessed (Fig. 5.8).

5.3.3 Control Modelling Using UML SysML

Marcano et al. (2004) used UML and especially OCL notation to model the behaviour of railway control system with pre- and post-conditions on evolution,

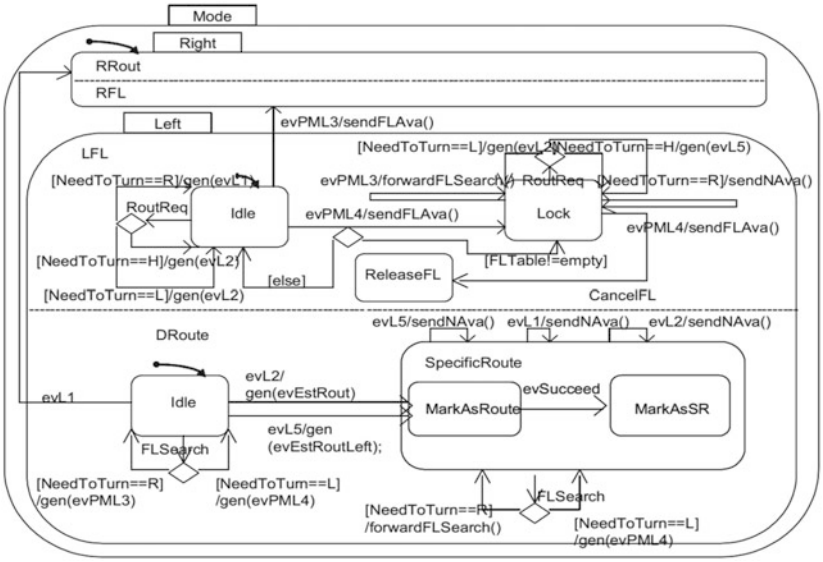


Fig. 5.7 Substate *mode* of the state machine associated with *point* presented in Hon et al. (2006)

making an advance towards B-method (Abrial 1996) linking. This approach relays heavily on state machine and interaction diagrams, as presented in Fig. 5.9, to model in a graphical way the behaviour of the control system, on top of a simple UML Class model for the physical part with operations.

The approach presented in Berkenkötter and Hannemann (2006) is to have UML Classes stereotyped using a specific profile dedicated to the description of railway infrastructure—presented in Fig. 5.3. Such profile allows the modeller a fine tuning of the modelling paradigm used in the modelling process, thus enabling a precise yet effective model of the railway system to be created. Nevertheless, the instance level is still hand-produced, inducing a great effort in the modelling of a large-scale network—like the high-speed one—as show for a small example in Fig. 5.4.

5.4 Industry Model-Based Modelling of Railway System

5.4.1 RailTopoModel: Modelling of Rail Infrastructure

UIC[1] is proposing a model of infrastructure using UML: RailtopoModel (UIC International Railway Standard 2016). This model focuses heavily on a topological description of the network, with the ability to add some positioning and geograph-

[1] International Union of Railways, https://uic.org/.

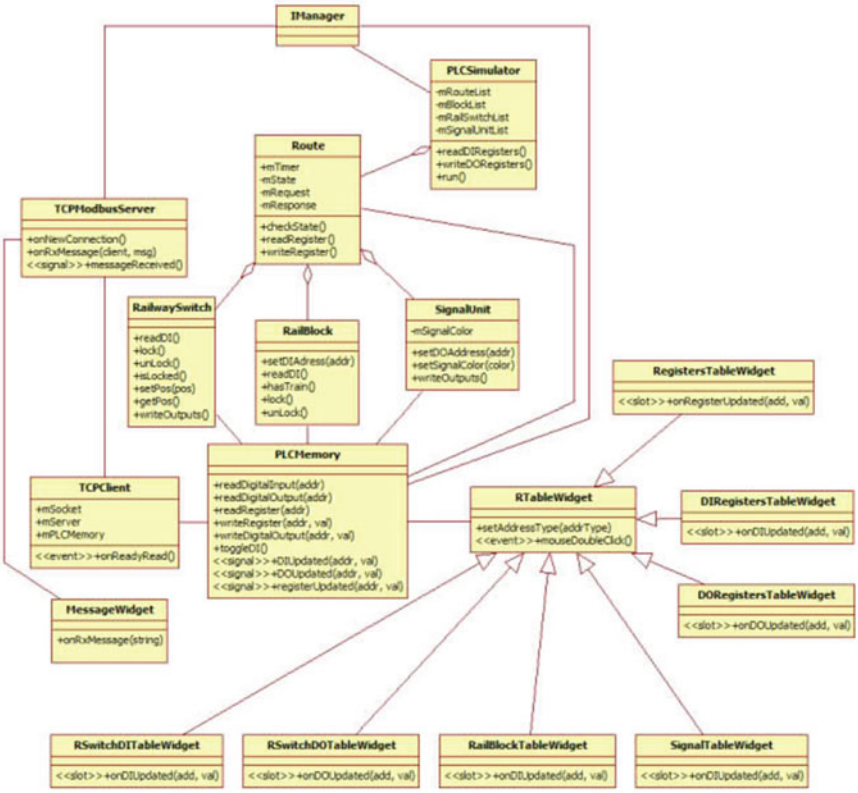


Fig. 5.8 UML model of the PLC used in Mecitoğlu and Söylemez (2013)

ical information. The aim of this model is to be the basis for further extension towards concrete objects—the model is quite abstract—in order to build a common and exchangeable layer to ease future business relations between railway operator, infrastructure and provider companies.

Figure 5.10 presents an overview of the topology package where the topology of the network is expressed as a graph using NetElement and Relations. Such graph may be link to a positioning system to have GIS-related information and may also be used as a structure to place some location (area, linear and point) that will be associated with physical objects.

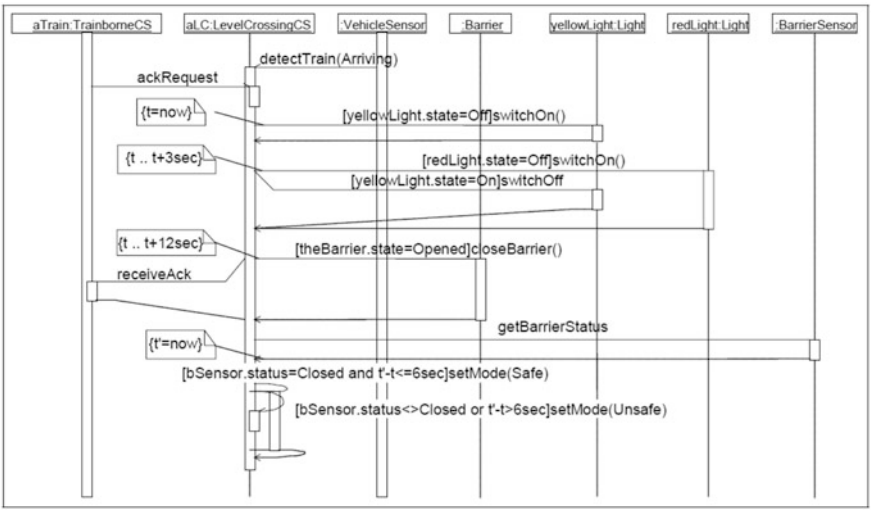


Fig. 5.9 UML model behaviour presented in Marcano et al. (2004)

5.4.2 Eulynx: Modelling of the Signalling System

Some of European railway infrastructure stockholders have grouped within the Eulynx[2] project in order to produce a model for specification of signalling. This model is also UML based by focusing more on the operational objects and is limited to the signalling domain, with an interesting mechanism of extension in order to handle the national specific signalling norms and standard used in Europe. Figure 5.11 presents a part of the platform description. The idea is to have all the necessary objects to completely define specification linked to signalling (e.g. place to stop with specific signal in a station) according to the placement of a specific access on the platform.

5.4.3 IFC Rail: Modelling for Construction and Maintenance

Digitisation of the rail infrastructure also needs to tackle the issue of construction and maintenance. IFC[3] standards are becoming the main modelling and digital standard for construction. Recently, an expert group composed of European and Chinese railway companies undertakes the work to propose an IFC/BIM standard

[2] https://www.eulynx.eu/.

[3] Industry Foundation Class, Rail Part: https://www.buildingsmart.org/ifc-rail-candidate-standard-is-available-for-review-and-comment/.

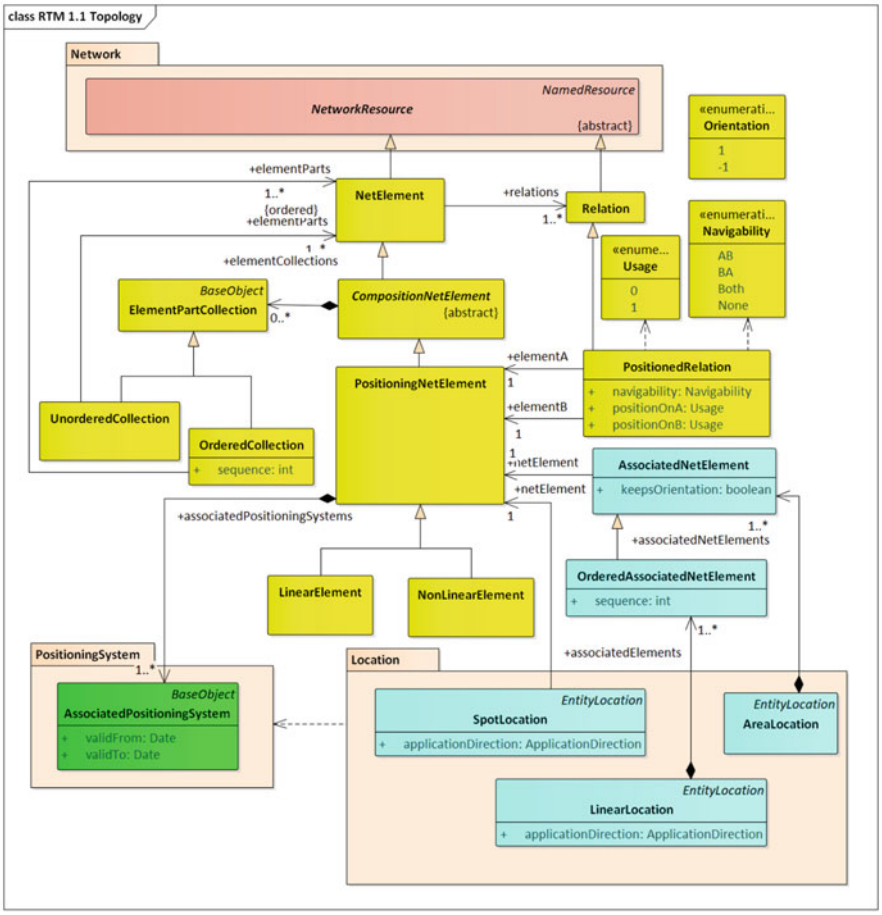


Fig. 5.10 Topology package of RailTopoModel model of UIC (UIC International Railway Standard 2016)

for railway infrastructure. Focusing more on physical object modelling, placement and spatial description, such model might be used as basis for further modelling activities. Figure 5.12 represents the conceptual model for a Track Panel that uses a composition of both spatial structures and physical objects.

5.5 Conclusion and Perspectives

As presented in this chapter, multiples initiatives in academic and industrial world propose solutions to model the infrastructure and control logic of railway systems. Such modelling effort is mandatory when the complexity and size of the systems at hand enforce the usage of automated tools—e.g. formal method—to ensure

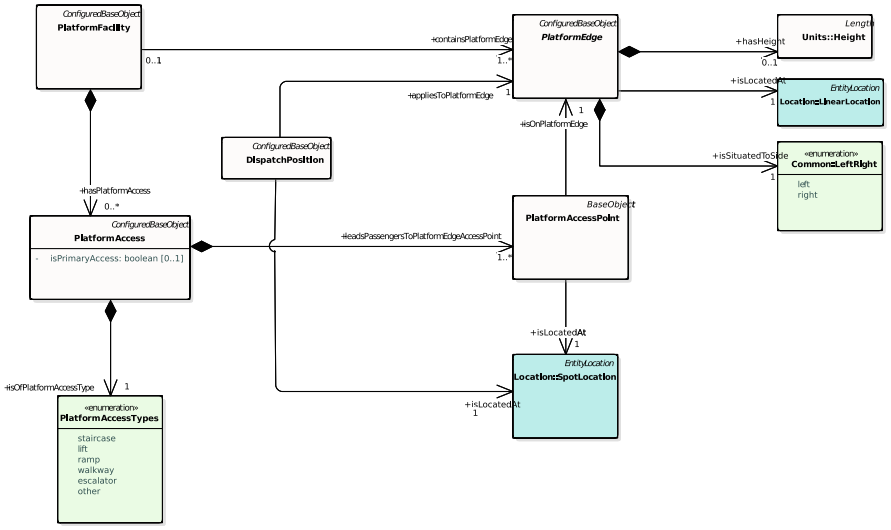


Fig. 5.11 Partial platform description from EULYNX project

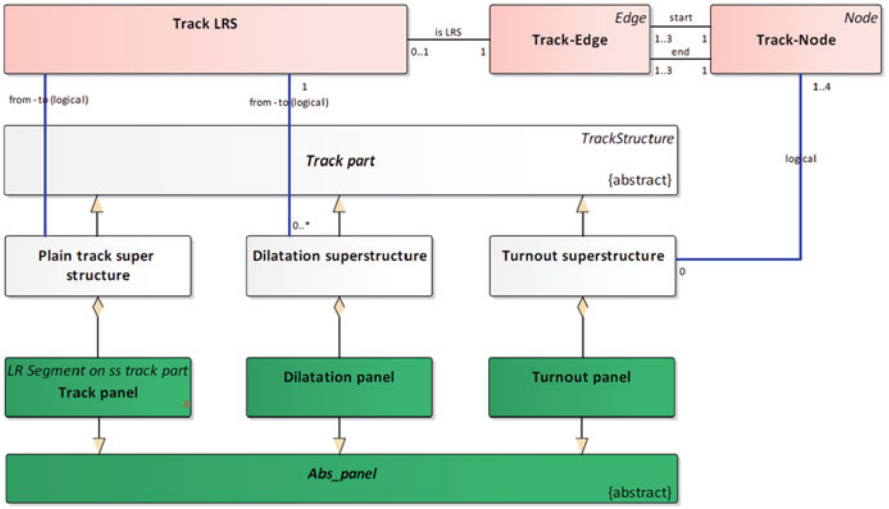


Fig. 5.12 Panel-related model of IFC Rail standard

operation capability and safety. As high-speed train infrastructure combines the complexity and size factor, this domain inevitably will rely more and more on formalised models for description of both the infrastructure and its behaviour. The real next upcoming challenge is to make the formal modelling paradigm and the descriptive model to work together in order to attain a so-called digital twin that fully models the infrastructure to develop and unable future usage of (very) high-

speed train operation of the near future. UIC is pushing a proposal to have a global railway ontology named OntoRail[4] to tackle this issue while preserving domain-specific models where it is needed the model: at domain expert level and usage.

References

Abrial, J.-R. (1996). *The B-book: Assigning programs to meanings*. New York, NY: Cambridge University Press. ISBN 0-521-49619-5.

Banci, M., Fantechi, A., & Gnesi, S. (2004). The role of formal methods in developing a distributed railway interlocking system. In *Proc. of the 5th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2004), Braunschweig, Germany* (pp. 220–230). Technical University of Braunschweig, Institute for Traffic Safety and Automation Engineering.

Berkenkötter, K., & Hannemann, U. (2006, September). Modeling the railway control domain rigorously with a UML 2.0 profile. In J. Górski (Ed.), *International Conference on Computer Safety, Reliability, and Security. Lecture Notes in Computer Science* (pp. 398–411). Berlin: Springer. ISBN 978-3-540-45762-6 978-3-540-45763-3

Bosschaart, M., Quaglietta, E., Janssen, B., & Goverde, R. M. (2015). Efficient formalization of railway interlocking data in RailML. *Information Systems, 49*, 126–141. ISSN 0306-4379.

Brownsword, M. (2014, January). How MBSE is used in rail. In *INCOSE IW 2014 MBSE Workshop, Los Angeles, CAL, USA*.

Crane, M. L., & Dingel, J. (2007, December). UML vs. classical vs. rhapsody statecharts: Not all models are created equal. *Software & Systems Modeling, 6*(4), 415–435. ISSN 1619-1374, https://doi.org/10.1007/s10270-006-0042-8

European Union Agency for Railways. (2016, February). ERTMS/ETCS SUBSET-026, System Requirements Specification v2.3.0.

Hon, Y. M., & Kollmann, M. (2006, September). Simulation and verification of UML-based railway interlocking designs. In *Automatic Verification of Critical Systems* (pp. 168–172).

Liu, C., Tang, T., & Lisagor, O. (2011, July). Challenge to introduce MBSA approaches into CBTC safety analysis. In *Proceedings of 2011 IEEE International Conference on Service Operations, Logistics and Informatics* (pp. 501–506). https://doi.org/10.1109/SOLI.2011.5986612

Marcano, R., Colin, S., & Mariano, G. (2004, October). A formal framework for UML modelling with timed constraints: Application to railway control systems. In *SVERTS: Specification and Validation of UML models for Real time and embedded systems* (p. 20).

Mecitoğlu, F., & Söylemez, M. T. (2013). A UML modelling approach for a railway signalization system simulator and SCADA system. *IFAC Proceedings Volumes, 46*(25), 77–82. ISSN 1474-6670, https://doi.org/10.3182/20130916-2-TR-4042.00030. 1st IFAC Workshop on Advances in Control and Automation Theory for Transportation Applications.

Object Management Group. (2015a, June). OMG Norm, Systems Modeling Language (SysML) v1.4.

Object Management Group. (2015b). OMG Norm, Unified Modeling Language (UML) v2.5.

Sun, P. (2015, July). Model based system engineering for safety of railway critical systems. Ecole Centrale de Lille.

UIC International Railway Standard. (2016). RailTOPOMODEL, RTM IRS 30100.

Xiangxian, C., Yulin, H., & Hai, H. (2011). A component-based topology model for railway interlocking systems. *Mathematics and Computers in Simulation, 81*(9), 1892–1900.

[4] https://ontorail.org/.

Part II
Proposal of a Model Engineering Approach for Border Crossing Assessment

Chapter 6
Designing Operating Rules for ERTMS Transnational Lines

Simon Collart-Dutilleul, Dalay Israel de Almeida Pereira, and Philippe Bon

6.1 Introduction

The process of designing the operating rules of an ERTMS line crossing a border is broken out into three different sub-problems (as depicted in Fig. 6.1):

1. implementing ERTMS in the first country, taking into account the specific national safety rules for specifying the first operating rule,
2. implementing ERTMS in the second country using a different legal and technological context,
3. designing the operating rules of a safe transient mode able to cross the border.

The following chapter describes the specification of operating rules in a given country (Fig. 6.2), knowing that this task has to be executed for all countries visited by the considered international line.

Formalising the design of operating rules is an important step before the safe transient mode implementation. However, the ERTMS specification itself is broken out into several functioning modes providing a first functional structure.

Keeping in mind that crossing a border is one of the aims of this type of lines, the following chapter considers operating rules as particular safety rules. This chapter presents a motivation for using model engineering in this context. Thus, a general proposition of model-based rule synthesis is proposed:

1. starting from UML as a universal language and
2. using (when existing) or producing a path towards obtaining abstract B-machines.

S. Collart-Dutilleul (✉) · D. I. de Almeida Pereira · P. Bon
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr; dalay-israel.de-almeida-pereira@ifsttar.fr; philippe.bon@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_6

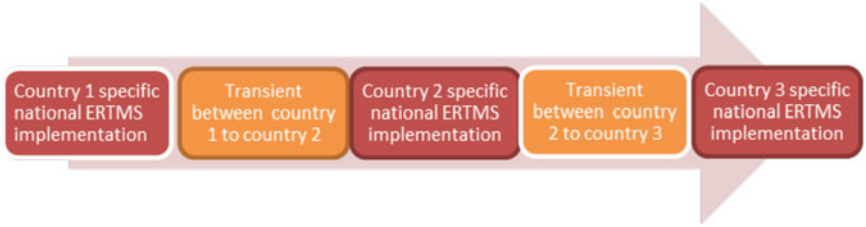


Fig. 6.1 Operating rule framework for international ERTMS lines

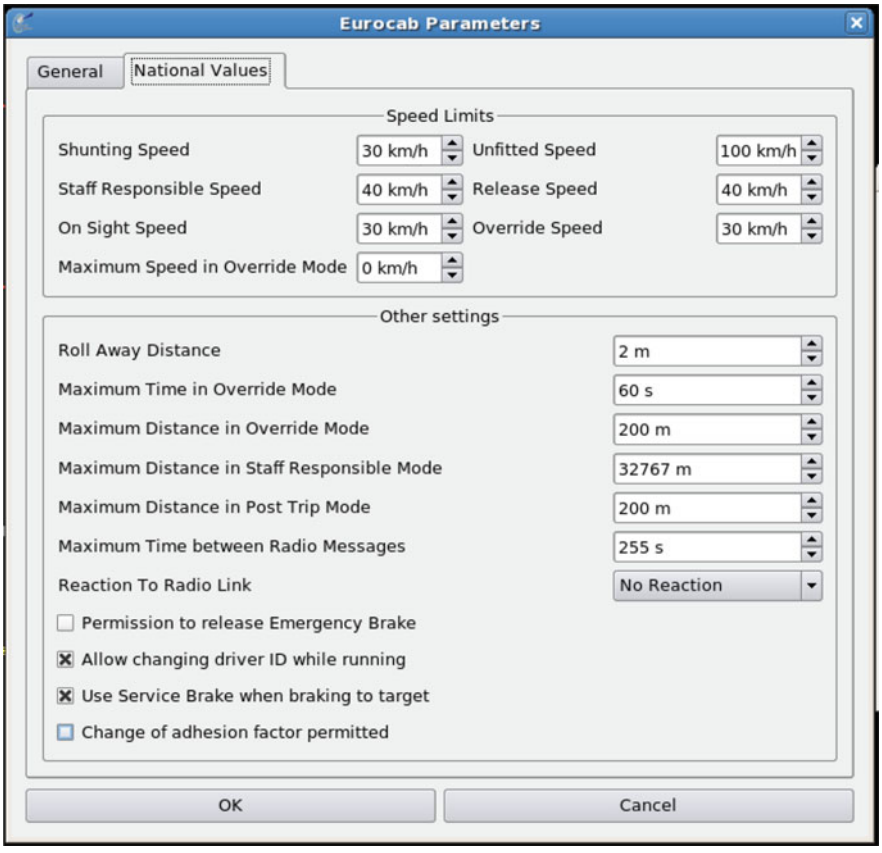


Fig. 6.2 ERSA ERTMS simulator screenshot showing national specific value setting

The B-method efficiency is recognised in the safety railway domain in order to formally specify the logical conditions that an operating rule is expected to fulfil.

The final textual rule document is not the aim of this study, since it only focuses on the logical design. Being at the border between system engineering and safety engineering, the use of a specific UML profile seems to be the most efficient

approach in order to model these systems. The potential contribution of the RBAC profile is studied, some limitations are identified and future solutions are proposed at the end of this chapter. Finally, the discussion extends the point of view from the scientific and proof of concept to industrial and certification aspects.

6.1.1 Safety Aspects of Operating Rules

It is really important to notice that operating rules target functional aims but must respect a set of high-level safety rules. Unfortunately, scientific literature concerning construction and management of safety rules is not very well provided. Nevertheless, one of the most relevant contributions is Hale's 2003 publication: "Management of safety rules: the use of railways" (Hale et al. 2003). However, this publication itself mentions the poverty of the literature in this field.

It is commonly accepted that a rule relies on collective knowledge to define and implement safe behaviour and equipment (Baumard 1999). As the knowledge is collective, it is recommended to consult the various stakeholders of a parcel of this knowledge to constitute a rule. Indeed, a rule is based on the perception and representation of the system from the point of view of the one who makes the rule. It is therefore important that there is a fit between the conceptual model used and the considered system.

6.1.2 The Life Cycle of a Rule

Various contexts of application rules are difficult to foresee. Moreover, the existing gaps between the initial intellectual representation and the reality of the field can be taken into account in a second phase, called an "adaptation phase".

This last consideration leads us to identify two strategies for the construction of rules adapted to very different contexts:

1. The first strategy is to introduce initial margins in relation to the level of abstraction in which the rule is expressed. In this case, the rule is considered to be a refinement, according to the different contexts.
2. The second strategy is to integrate a validation phase in the field by competent experts of a given domain of knowledge. In this case, the expression of the initial rule must be readjusted.

It has to be noted that the two procedures of adaptation to the local context are not incompatible with each other. It is still necessary to define criteria to switch from one behaviour to another and to rigorously identify components of the rule which are validated by an expert knowledge and other ones that still embed abstraction and margin allowing a later refinement.

The above sentence is a simplification of the real situation, because a given component of the rule may have a critical link with several knowledge domains. In this last case, the validation of a rule component represents one of the major issues.

An approach proposed by the literature is to apply the bureaucratic approach. A presentation of this approach can be found in the PhD thesis of Helene Cecilie Blakstad (2006). It means that you have to find a human mastering all the connected knowledge and able to make synthesis and compromise. One of the drawbacks of this solution is that it prevents the use of a radically new technology.

Actually, it is not possible to find an expert of railway technology mastering all the connected knowledge, like, for instance, mastering the knowledge of railway safety. Another proposition is to use a set of dedicated experts. Then, it is necessary to face a classical problem of knowledge alignment. Furthermore, dedicated experts do not have a mental representation of the impact of choices they made in the connected domain knowledge.

In this context, a possible solution may be in using a dedicated model in order to formally represent the knowledge about a given aspect. A definition of model is presented below.

Definition 6.1 (Model) A model is a simplification of a system built with an intended goal in mind. The model should be able to answer questions in place of the actual system (Bézivin and Olivier 2001).

Thus, based on the definition above, the model-based strategy seems an efficient solution. Building a model means representing the real world focusing on specific aspects. It is relevant because it provides an operational abstraction of a given knowledge, focusing on impacts on a given structure.

6.1.3 A Model-Based Proposition

The main objective of this chapter is to describe this methodological approach. The basic principle is that a rule specifies a set of tasks to be executed by a human like a software code specifies a list of instructions to be executed by a computer.

Obviously, a human does not behave like automatons facing an instruction list. Nevertheless, it is not impossible to specify a behaviour for a human. Defining the appropriate behaviour with regard to the system constraints is a challenging task on its own.

When this target behaviour is logically described, writing a document such a way that humans in a sociotechnical system will behave the right way is another challenging work. In this context, writing such document is not one of the objectives of this chapter, which only puts efforts on logically specifying a good design allowing a good behaviour.

As a consequence, the proposed work does not provide a written document as a result but only a discrete event model, which may be used as a core input information for the writing task.

The main proposition is based on formal modelling of the railway system, which is carried out in a joint UML and B-method approach. Moreover, two basic activities may allow the system implementation using a formal methodology: formal specification and formal verification. The formal specification is the expression, by means of a formal language, of an expected result. The formal verification is the production of evidence to show that the product effectively respects the formal specification.

The verification activity is not completely discussed in this book. The verification process includes technical aspects, like the choice of the proof methodology (model checking, theorem proving, simulation, etc.). The reader interested in going deeper concerning these aspects may consult (Boulanger 2013).

6.1.3.1 The Normative Context

The set of rules to be fulfilled comes from documents of the European specifications (Union Industry of Signalling (UNISIG) 2009) and railway operating rules on a national line (Réseau ferré 2012). The former is a document that explains the unified ETCS standard from a technical point of view. This specification often offers multiple solutions for the way to implement a specific function. The latter is a document created for the purpose of commissioning the system Level 2 of ETCS on the East European high-speed line. It repeats the principles and provisions relating to the use of this system resulting from the technical specification of interoperability (TSI) (ALCATEL, ALSTOM, ANSALDO SIGNAL, BOMBARDIER, INVENSYS RAIL, SIEMENS 2006) and provides useful details for a pragmatic implementation on this line. With respect to these two documents, the specification phase must include

1. analysis of European specifications according to national railway rules via operating rules and
2. formalisation and modelling of scenarios derived from railway operating rules.

6.1.3.2 Basics of the Formal Validation Process

This chapter details our modelling approach and focuses on specification by means of combining various modelling tools and techniques. The expression of safety requirements that must be respected by the produced model is discussed, but the proof production is not technically detailed.

Regarding this proof, models obtained now in B formalism and in Event-B[1] (Wakrime et al. 2018) in the future (Bougacha et al. 2019) are formally validated with regard to the security properties governing the system. This phase focuses on formal techniques such as Atelier B[2] logical proofs and model checking with ProB. In the case where the model is not 100% proved or verified by the model checker, two procedures may be followed:

1. at the modelling level, it is possible to improve the system specification, and
2. at the formal verification level, it is possible to make an intervention inside the prover in order to complete the logical proof.

Indeed, in the case of a failed verification of the model with the model checking approach, a counterexample that violates an invariant of the model must be generated. Therefore, we will be able to return to the models and correct them in order to avoid the invariant violations. In addition, in the case where the Atelier B automatic prover fails to demonstrate all proof obligations, it is advisable to use the interactive prover to finalise the proof and demonstrate the rest of the obligation proofs not solved by the automatic proof assistant.

6.2 ERTMS Operating Rule Modelling

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 modelling language may not be a formal language. In this context, the literature presents some propositions for using the Unified Modelling Language (UML) (Jaber et al. 2012; Laleau et al. 2010; Qiu et al. 2013; Milhau et al. 2011) and more precisely its specialisation for system descriptions: SysML (Collart-Dutilleul et al. 2011; Snook and Michael 2006). The main idea is to use UML notations to describe requirements using a unique language (Fig. 6.3). Another proposition is to integrate formal modellling analysis tool in order to perform specific requirements checking. B-method is used to assess the global consistency of the added constraints ensuing from the previous analysis (Fig. 6.4).

[1] http://www.event-b.org/.

[2] http://www.atelierb.eu/en/.

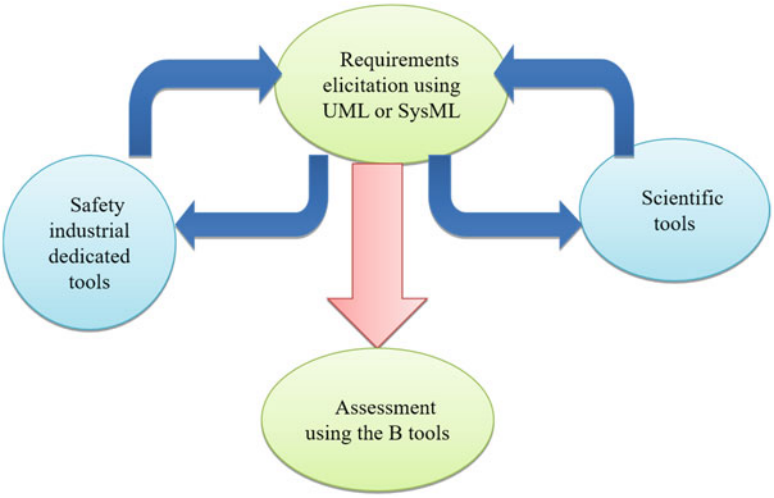


Fig. 6.3 UML centred requirement engineering approach (Collart-Dutilleul et al. 2011)

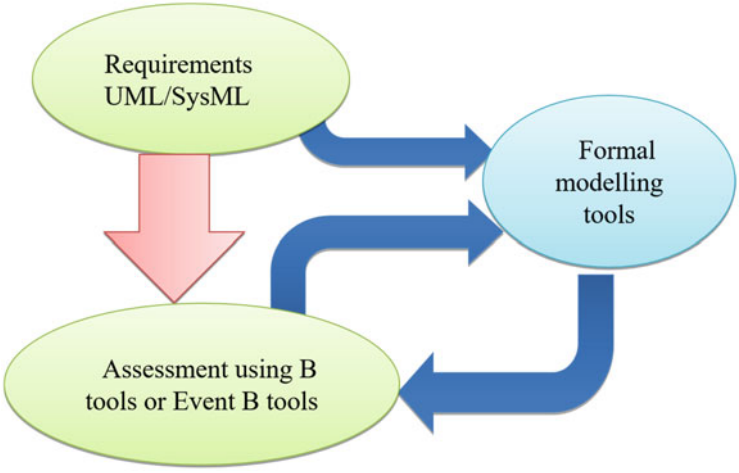


Fig. 6.4 B centred theorem proving for requirement checking

6.3 Using the Appropriate Tools at the Appropriate Level

6.3.1 B-method and Railway Automatism

The B-method has been used for industrial big-sized applications in various fields such as information systems (Ledru et al. 2011), databases (Mammar and Régine 2006) and mainly in the railway field for years (Arago 1997). Its extension, Event-B (Abrial 2010), is an evolution to the specification language dedicated to the

verification of many different types of systems, like discrete, distributed (Butler 2009) and railway systems, for instance.

In order to avoid the manual verification, some efforts have been made in order to formally specify railway automatisms. B-method is an example of language that has been increasingly used in the railway field.

Actually, for urban railway systems, which are more independent and closed systems, the B-method has been accepted and has been industrially applied in the global system (Sabatier 2016) or at a component level. Some early success stories are KVB, an Automatic Train Protection system for SNCF since 1993; SAET-METEOR (Behm et al. 1999), a driverless Train Automation and Operation system in metro line 14 in Paris in 1998; and Roissy VAL, a Section Automatic Pilot system for light driverless shuttle for Paris-Roissy airport in 2006 and now is operating in Taipei, Toulouse, Rennes and Turin (Erbin and Soulas 2003). A recent application is the COPPILOT system (Patin et al. 2006; Lecomte 2008), which is a metro platform screen door controlling system from the ClearSy company. It has been installed in the Paris Metro and the São Paulo Metro. Some reasons of the B-method success are the existence of rigorous mathematical foundations, the well-developed underlying methodology and the existence of reasonably advanced support tools.

The B language provides a high-level specification formalism called abstract B-machine. The specifications are then manipulated through a progressive development process that evolves the abstract B-machines into implementable programme codes. Each development process is called a refinement, which "refines" the previous specification into a more concrete one.

The basic building block of a specification in B-method is a B-machine. Inside a machine, the specification is divided into many clauses, like VARIABLES, INVARIANT and OPERATIONS.

B-method disposes of a set of proof obligations based on the defined clauses, which allows the analysis of the specification consistency.

The consistency of all the abstract B-machines and the correctness of each development step are validated by a set of proof obligations (POs). New POs are generated along with the refinement processes in order to enable the B-method to build error-free proven systems.

6.3.2 Modelling the Railway Infrastructure and Its Signalling System with High-Level Petri Nets

A Petri net-based modelling approach is proposed in (Sun 2015; Bon et al. 2013). This approach is exploited using two different methodologies:

1. transforming the Petri net model into abstract B-machines in order to use the B-tooling support, and
2. using the ERTMS UML specification in order to define some scenario to be validated through the Petri net model of the infrastructure.

A whole chapter is dedicated to this particular subject entitled "Formal Validation of Interlocking Systems under National Railway Signalling Rules." Thus, this chapter will not focus on the modelling of National Railway Signalling Systems based on this approach.

6.3.3 Issues of Producing a B-specification from a Different Formalism: A Relay-Based DSL Example

Some infrastructure managers consider relay diagrams as a Domain-Specific Language suitable for modelling a part of the railway systems: Railway Interlocking Systems (RISs). With the objective of ensuring safety by controlling the movements of trains in a track, RISs are considered as safety-critical systems. The RISs used nowadays resulted from the evolution of the technology used in the railway field. The first built RIS was purely mechanical, and then it evolved to use new technologies, becoming electrical–mechanical systems, relay-based systems and, more recently, computer-controlled systems (Hansen 1998).

A relay diagram models the physical connection between the electrical components of a Railway Interlocking System. Based on the knowledge about the behaviour of each component, a manual analysis of the diagram may be performed in order to evaluate the existence of dangerous situations. However, this verification tends to be error prone, since humans may make mistakes when dealing with relay diagrams with a high level of complexity.

In the context of the FUI21 LCHIP project, a proposition of traducing relay-based diagrams into abstract B-machines was presented in de Almeida et al. (2019b). Based on the connections between the components as described inside the relay diagrams, this work proposed to specify the conditions for each electrical component to be activated. The result of this specification is the description of the complete behaviour of the system, which may be animated, analysed, verified, refined and implemented.

Actually, when the specification language is also the implementation language, the problem of guaranteeing the correct implementation is simplified. Nevertheless, it does not mean that the creation and validation of a global invariant are easy. In fact, the proposed translation allows the specification of the system behaviour, but it cannot create the safety conditions, since it depends on the system context. Furthermore, each country has specific safety rules for the RIS behaviour in a way that the knowledge and the contextual information plays an important part on the specification of safety conditions and, by consequence, on the definition of the specification invariant.

6.3.4 *Industrial Example*

Railway Interlocking Systems are responsible for controlling the trains movements by managing the signals and switches. Considering that trains may go in both directions on the tracks and the possibility of a train to go from one track to another, the RIS must intervene in order to guarantee safety. The track plan in Fig. 6.5 is one example of a dangerous situation. When a train that comes from a Control Area A needs to change to the other track because of problems on its own track, it begins to go in the "wrong way," which may cause a collision with a train that comes from Control Area C. The RIS must control the signals in these control areas in order to avoid this collision.

Part of the relay diagram representing the system in Control Area A is presented in Fig. 6.6. Many different components may be used inside a relay diagram, which increases the complexity of the logic behind its behaviour. In this diagram,

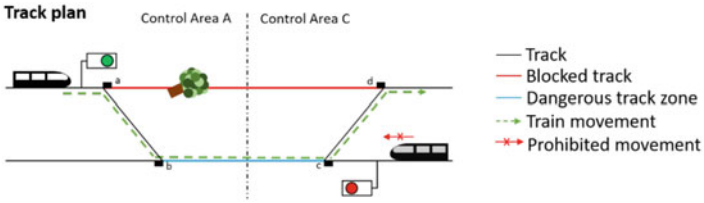


Fig. 6.5 Example of a track plan from Control Area A to Control Area C

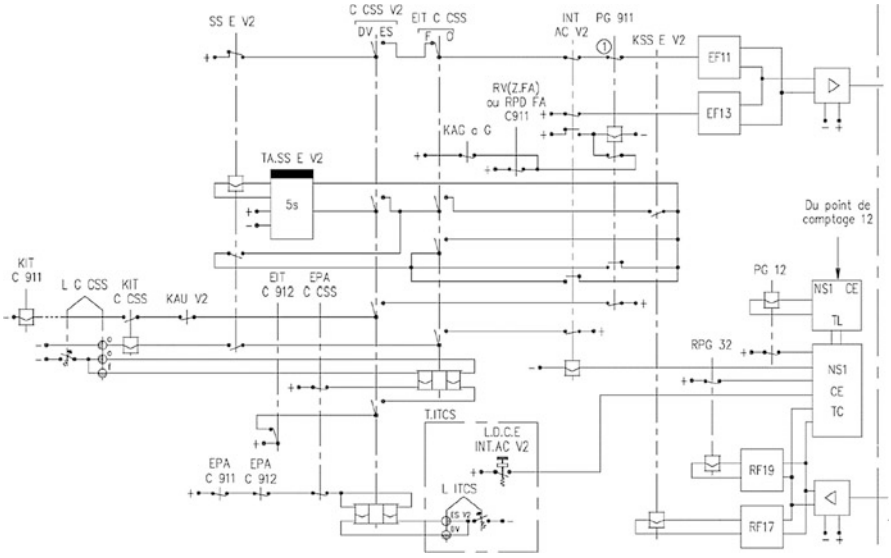


Fig. 6.6 Relay diagram of the system in Control Area A

the component "KIT C 911" is responsible for allowing the train to change its tracks in the Control Area A. Contrarily, the component EF11 informs the Control Area C that the train in this area is allowed to enter in this portion of the track. Evidently, in order to guarantee safety in this case, these two components may never be activated at the same time. The complete B-specification of this example is presented in Fig. 6.7. Nevertheless, this safety condition is not explicitly modelled in the diagram. Furthermore, this is only one example of a safety condition in a specific context, since many other conditions must be considered in order to guarantee safety in this same system and any contextual changes must be taken in consideration when analysing other similar systems.

In this example, the user of this proposed approach must have knowledge about the environmental context of the system. Besides, it is essential to expertise the implicit relation between components in order to specify the safety conditions based on how components may affect each other. More precisely, the link between the environment knowledge and the specification has to be studied carefully.

6.3.5 Firsts Steps on Contextual Specification

In order to try to specify contextual environmental information about the Railway Interlocking Systems, a study has been performed in this same project, as presented in de Almeida et al. (2019a). In this study, the knowledge about the relation between components and the environment was modelled in a higher level of abstraction: conceptual modelling. At this level of abstraction, it is possible to model the domain knowledge with a set of concepts and the relations between them. Based on a conceptual model, the specification of the industrial example presented in Sect. 6.3.4 has been improved and many other safety conditions were specified.

Nonetheless, despite the good result, this represents only a small step towards specifying the knowledge about the system. Besides, it is still not clear if it is possible to model all possible different RIS contexts and how these models may be used as basis in order to specify different Railway Interlocking Systems. Until, now it represents a good idea that must be studied carefully in the next years.

6.4 The Role-Based Formalism for Rule Modelling

6.4.1 The Genesis of RBAC and B4MSecure and Their Use for Railway Safety

6.4.1.1 UML as a Starting Modelling Language

Much of the ERTMS specification is written deliberately leaving possibilities of various interpretations of the text. One of the known justifications is the willingness

```
MACHINE
  itcs
SETS
  O_OU_F = {POS_O, POS_F};
  DV_OU_ES = {POS_ES, POS_DV}

VARIABLES
  KIT_C_CSS,
  SS_E_V2,
  TA_SS_E_V2,
  EIT_C_CSS,
  C_CSS_V2,
  PG_911,
  EF11,
  PLUS_KIT_C_911

INVARIANT

  KIT_C_CSS : BOOL &
  SS_E_V2 : BOOL &
  TA_SS_E_V2 : BOOL &
  EIT_C_CSS : O_OU_F &
  C_CSS_V2 : DV_OU_ES &
  PG_911 : BOOL &

  EF11 : BOOL &

  PLUS_KIT_C_911 : BOOL &

not(PLUS_KIT_C_911 = TRUE & EF11 = TRUE)

INITIALISATION
  KIT_C_CSS := FALSE ||
  SS_E_V2 := FALSE ||
  EIT_C_CSS := POS_F ||
  C_CSS_V2 := POS_DV ||
  PG_911 := TRUE ||
  TA_SS_E_V2 := FALSE ||
  EF11 := FALSE ||
  PLUS_KIT_C_911 := FALSE

OPERATIONS

  mise_a_jour_poste_A(L_C_CSS, INT_AC_V2, EPA_C_CSS, EIT_C_912, KAG_a_G, RPD_FA_C_911, L_ITCS, KAU_V2,
    KSS_E_V2, EPA_C_911, TA_SS_E_V2_echue) =
  PRE
    L_C_CSS : O_OU_F & INT_AC_V2 : BOOL & EPA_C_CSS : BOOL & EIT_C_912 : BOOL & KAG_a_G : BOOL &
    RPD_FA_C_911 : BOOL & L_ITCS : DV_OU_ES & KAU_V2 : BOOL & KSS_E_V2 : BOOL & EPA_C_911 : BOOL &
    TA_SS_E_V2_echue : BOOL
  THEN
    KIT_C_CSS, PLUS_KIT_C_911, EIT_C_CSS, PG_911, C_CSS_V2, EF11, TA_SS_E_V2, SS_E_V2:(

      KIT_C_CSS : BOOL & PLUS_KIT_C_911 : BOOL & EIT_C_CSS : O_OU_F & PG_911 : BOOL &
      C_CSS_V2 : DV_OU_ES & EF11 : BOOL & SS_E_V2 : BOOL & TA_SS_E_V2 : BOOL &

      KIT_C_CSS = bool(SS_E_V2 = TRUE &  EIT_C_CSS = POS_O & INT_AC_V2 = TRUE & L_C_CSS = POS_O) &

      PLUS_KIT_C_911 = bool(KIT_C_CSS = TRUE & KAU_V2 = TRUE & C_CSS_V2 = POS_ES & PG_911 = TRUE) &

      (EIT_C_CSS$0 = POS_O =>
        EIT_C_CSS = { TRUE |-> POS_F, FALSE |-> POS_O }(bool(L_C_CSS = POS_F & EPA_C_CSS = TRUE))) &
      (EIT_C_CSS$0 = POS_F =>
        EIT_C_CSS = { TRUE |-> POS_O, FALSE |-> POS_F }(bool(L_C_CSS = POS_O & C_CSS_V2 = POS_ES &
          EIT_C_912 = FALSE))) &

      (PG_911$0 = FALSE => PG_911 = bool(INT_AC_V2 = FALSE)) &
      (PG_911$0 = TRUE => PG_911 = bool(RPD_FA_C_911 = TRUE or KAG_a_G = TRUE or INT_AC_V2 = FALSE)) &

      (C_CSS_V2$0 = POS_ES =>
        C_CSS_V2 = { TRUE |-> POS_DV, FALSE |-> POS_ES }(bool(L_ITCS = POS_DV & EPA_C_CSS = TRUE &
          EPA_C_911 = TRUE))) &
      (C_CSS_V2$0 = POS_DV =>
        C_CSS_V2 = { TRUE |-> POS_ES, FALSE |-> POS_DV }(bool(L_ITCS = POS_ES & EPA_C_CSS = TRUE &
          EPA_C_911 = TRUE))) &

      EF11 = bool(SS_E_V2 = FALSE & C_CSS_V2 = POS_ES & EIT_C_CSS = POS_F & INT_AC_V2 = TRUE &
        PG_911 = TRUE) &

      (SS_E_V2$0 = TRUE =>
        SS_E_V2 = bool(
          (C_CSS_V2 = POS_ES & (EIT_C_CSS = POS_O or PG_911 = FALSE or INT_AC_V2 = FALSE)) or
          (C_CSS_V2 = POS_ES & EIT_C_CSS = POS_O & KSS_E_V2 = TRUE))
      ) &
      (SS_E_V2$0 = FALSE =>
        SS_E_V2 = bool(TA_SS_E_V2$0 = TRUE & TA_SS_E_V2_echue = TRUE & (C_CSS_V2 = POS_ES &
          EIT_C_CSS = POS_O & KSS_E_V2 = TRUE))) &

      TA_SS_E_V2 = bool(SS_E_V2$0 = FALSE & (C_CSS_V2 = POS_ES & EIT_C_CSS = POS_O &
        KSS_E_V2 = TRUE) & TA_SS_E_V2_echue = FALSE)
  )
  END

END
```

Fig. 6.7 Behavioural specification of the system in the Control Area A

to leave the possibility of technological innovation, while a too strict specification could freeze the architecture. This looks like a paradox for providing a service of interoperability.

In this context, the Unified Modelling Language (UML), although semi-formal, seems quite appropriate. In fact, the state of the art regarding the use of UML is quite provided (Lodderstedt et al. 2002; Ayed et al. 2014). This is even stronger when you consider the specialisation of UML named SysML (Ayed et al. 2016; Kraibi et al. 2019) and the formalism of Statecharts (Fotso et al. 2018a,b).

Another key argument around the use of UML/SysML notations for the collection of requirements is the language universality. Indeed, this language is taught in most engineering schools in the world.

6.4.1.2 The RBAC Profile

The extension mechanism called UML profile has been proposed to overcome the UML particular weaknesses. A UML profile, standardised by the OMG, is a set of techniques and mechanisms to define UML extensions to fit a particular domain. This adaptation is possible on any UML model with respect to the UML metamodel. This technique was used to define RBAC access control policies and Or-Bac to guide UML modelling to role-based modelling. RBAC model was published as NIST RBAC (Ferraiolo and Richard 1992) and then standardised by ANSI (American National Standard Institute)/INCITS in 2004 (ANSI INCITS 359-2004) and revised in 2012 (INCITS 359-2012). Figure 6.8 depicts the following different entities of the model as well as the relations between them:

- USERS: A user represents a human agent (human being or person) or software (including intelligent machines, networks or autonomous agents) that can access system resources. Access to resources by users must be controlled by permissions.
- PERMISSIONS (PERMS): Permission is a privilege to perform operation on one or more protected RBAC objects.

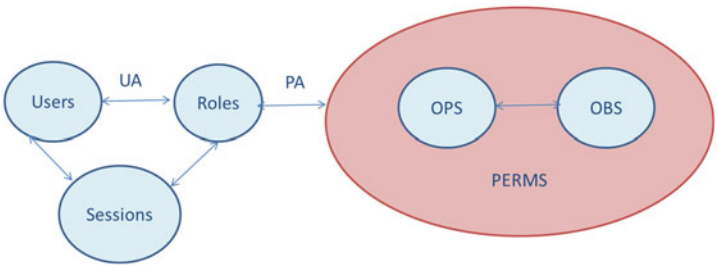


Fig. 6.8 RBAC core model

- OBJECTS (OBS): An object may be a system resource in which an access control can be performed such as a file, printer, database, etc.
- OPERATIONS (OPS): An operation is an access type (action) that can be invoked by a system user on a resource. An operation can correspond to any action of the system that retrieves or communicates information to an object.
- ROLES: A role is a function of an organisation associated with its authority and its responsibility. An RBAC role regroups permissions related to this function and grants them to users playing this role. The concept of role is central in RBAC model since it is the bridge between users and permissions. Indeed, two relationships are defined: one (PA: PermissionAssignment) to grant permissions to roles and a relationship (UA: UserAssignment) to assign these roles to users.
- SESSIONS: A session matches a user to an active subset of roles assigned to it.

6.4.2 Changing the RBAC Interpretation from Security to Safety

In what follows, we briefly distinguish security–safety (safety) from security of information systems (security):

- Safety expresses that catastrophic consequences never occur during execution. It defines the properties according to which a system is said to be safe. This has been standardised by a regulatory reference for safety: the 61508 standard. Several versions of this standard have emerged, each defining the standards that make EN 61508 applicable for different sectors concerned, like Std, EN50126 (2000), Std, EN50128 (2001) and Std, EN50129 (2019) for the railway sector.
- Information systems security addresses vulnerabilities or malicious attacks on information systems. Several techniques can be employed such as access control and cryptography. We focus on access control, which is a process that protects attempts to access system resources against unwanted access while determining authorised activities of legitimate users and ensuring security–privacy properties.

The study of the role-based access control (RBAC) model, its SecureUML metamodel and the modelling approach by B4MSecure are used in order to ensure information confidentiality. Furthermore, the similarities of their basic mechanisms lead us to propose a safety strategy based on context conditions that are mandatory for triggering a given procedure. This new strategy is built on a new interpretation of the basic concepts:

- the actors correspond to the users;
- the responsibilities given to actors correspond to the roles granted to users;
- the notion of authorisation is the safe notion of permission;
- authorised actions are operations;
- the resources involved correspond to the objects;

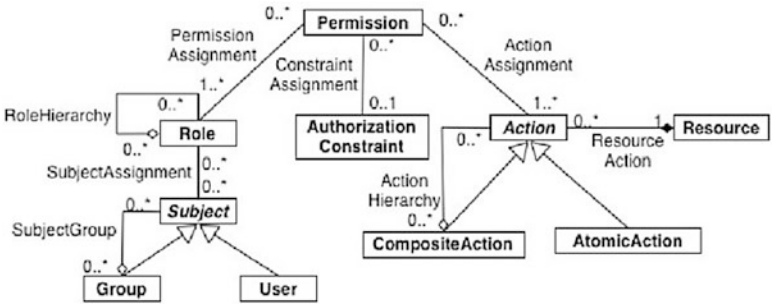


Fig. 6.9 A SecureUML meta-model (Lodderstedt et al. 2002)

- the constraints for issuing an authorisation correspond to the authorisation constraints

The used RBAC profile is inspired from SecureUML (Lodderstedt et al. 2002) (Fig. 6.9), which is a graphical modelling language specifying information related to access control with additional support for specifying authorisation constraints in order to model roles and their permissions. Research works done in the Selkis project (Laleau et al. 2010; Qiu et al. 2013; Ledru et al. 2011) show the efficiency of this platform and its different steps leading to the formal validation of scenario in healthcare domain by seeking for malicious sequences of operations. B4MSecure acts in three steps:

- graphical modelling using the Papyrus tool of a functional UML class diagram,
- graphical modelling of an access control policy using the RBAC UML profile and
- translation of both models into B-specifications in order to formally validate them.

In addition to the RBAC model, it turned out that the organisation-based access control (OR-Bac) model, an extension of RBAC, can be used in our industrial context according to the following findings:

- RBAC is a role-based access control model such that a user is granted permissions based on the roles they play (Fig. 6.10);
- Or-Bac is an organisation-based access control model that aims to define a richer and more modular security policy compared to RBAC, so it extends RBAC with notions of context and hierarchy of organisations.

The concepts of these two models facilitate the modelling of railway operating rules and the control of the complexity of these rules while ensuring a separation of concerns.

The first concern is the functional aspects of the system, and the second one is the safety aspects based on the responsibilities and the authorisations granted to the actors of the system. The modelling analysis structures the railway system in

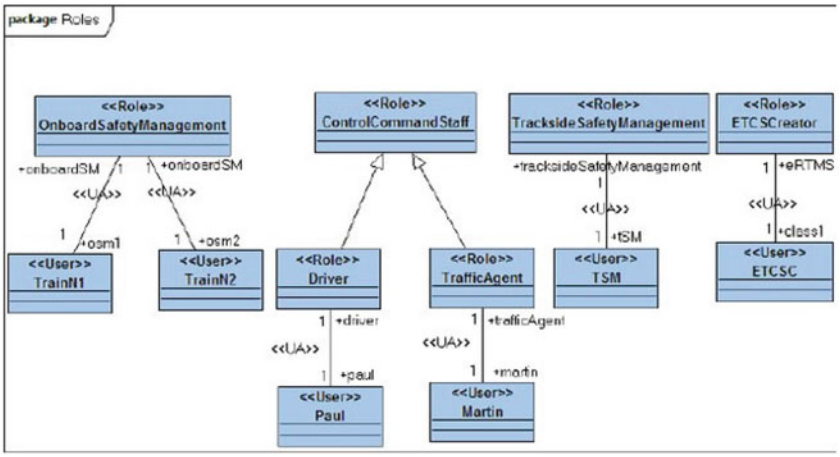


Fig. 6.10 UML model corresponding to roles

two levels: a functional level, which manages train movements, and a "safe" level that manages the travel authorisations and the operations carried out by the various actors of the system.

6.4.3 Rule Modelling

The train is supposed to own a movement authority (Ayed et al. 2014). A movement authority (MA) is an authorisation given to a train to move to a given point as a supervised movement. Some features can be used to define an MA.

The functional model (see Fig. 6.11) contains MA and ETCSOrder (including Override EOA, for example). The ETCSSystem class is composed of OnboardSystem class and TracksideSystem class corresponding to on-board sub-system and track-side sub-system, respectively. The on-board system is a part of the ERTMS/ETCS train, hence the relationship of aggregation between TrainETCS class and OnboardSystem class. The DMI allows the display of information about distance, speeds, ERTMS/ETCS level, ERTMS/ETCS mode and instructions as textual messages. Features of MA and Override EOA appear as attributes of MA and ETCSOrder classes. The Override EOA function is modelled as an ETCSOrder class since it is a particular kind of ERTMS/ETCS written order. For this reason, the AuthorizationType attribute of type Enumeration ETCSOrderNumber is initialised to ETCS01.

The MA function unfolds with interactions between the OnboardSafetyManagement (the on-board computer-based machine), the TracksideSafetyManagement (the track-side computer-based machine) and the Driver, as follows:

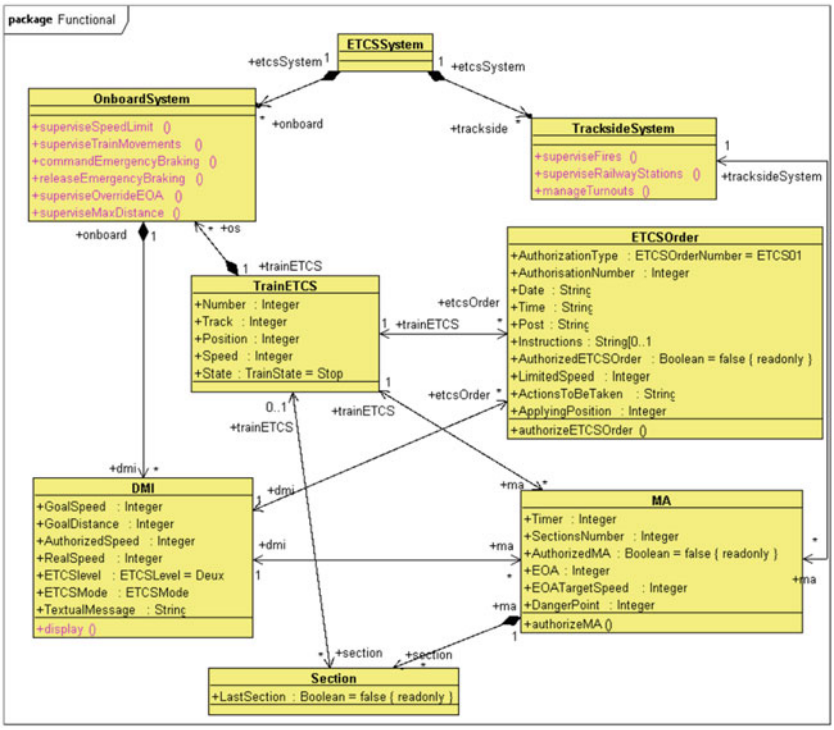


Fig. 6.11 Functional model

- MA.1: the OnboardSafetyManagement requests an MA to the TracksideSystem;
- MA.2: the TracksideSafetyManagement receives the MA request from the TracksideSystem;
- MA.3: the TracksideSafetyManagement proposes an MA to the TracksideSystem after creating it. It can also modify and/or delete the MA;
- MA.4: the OnboardSafetyManagement receives the proposed MA from the TracksideSystem, authorises it and processes the MA authorisation in order to be displayed in the Driver Machine Interface (DMI);
- MA.5: the Driver reads the authorised MA.

Each step of this scenario represents a permission to do an action on an entity by a role (Ayed et al. 2014). The assignment of the permission to the role is presented in Fig. 6.12.

UML models are automatically translated into abstract B-machines (see Fig. 6.13). The consistency of the corresponding model can be proved using the proof assistant of the Atelier B (or Rodin tool, Butler and Hallerstede 2007). Moreover, some safety invariants may be introduced in this global authorisation oriented B-model. The next section presents an example of safety invariant

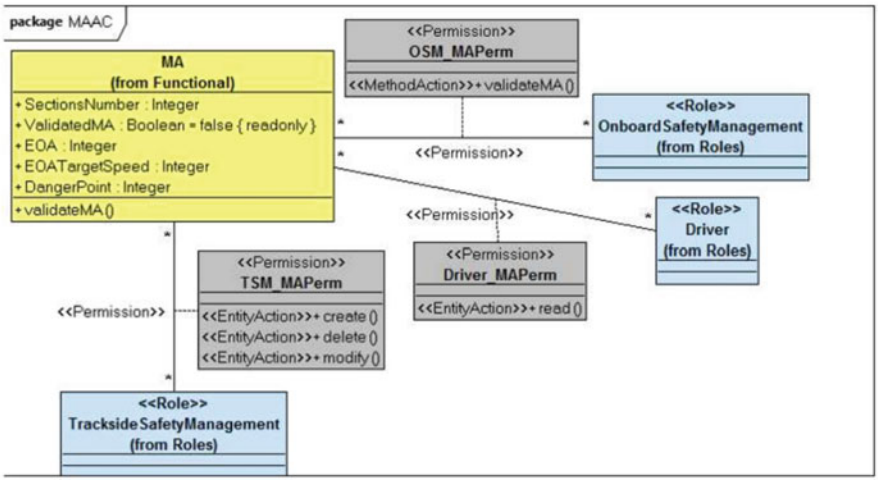


Fig. 6.12 UML model of permissions associated with MA

```
1 Machine
2     Functional
3 SETS
4     MA_AS;
5     ETCSORDER; ...
6 ABSTRACT_VARIABLES
7     MA,
8     ETCSOrder,
9     MA_ValidatedMA,
10     ETCSOrder_AuthorizedETCSOrder,
11     MAOfTrainETCS,
12     ETCSOrderOfTrainETCS,
13     ...
14 INVARIANT
15     MA ⊆ MA_AS
16     ∧ ETCSOrder ⊆ ETCSORDER
17     ∧ MA_ValidatedMA ∈ MA → BOOL
18   ∧ ETCSOrder_AuthorizedETCSOrder ∈ ETCSOrder → BOOL
19     ∧ MAOfTrainETCS ∈ MA ⤖ TrainETCS
20     ∧ ETCSOrderOfTrainETCS ∈ ETCSOrder ⤖ TrainETCS
21     ∧ ...
22 INITIALISATION
23     MA := ∅
24     || ETCSOrder := ∅
25     || MA_ValidatedMA := ∅
26     || ETCSOrder_AuthorizedETCSOrder := ∅
27     ||...
28 OPERATIONS
29 MA_validateMA(Instance)=
30   PRE Instance ∈ MA
31     ∧ MA_ValidatedMA(Instance) = FALSE
32   THEN MA_ValidatedMA(Instance) := TRUE
33   END;
34 ETCSOrder_authorizeETCSOrder(Instance)=
35   PRE Instance ∈ ETCSOrder
36     ∧ ETCSOrder_AuthorizedETCSOrder(Instance) = FALSE
37   THEN ETCSOrder_AuthorizedETCSOrder(Instance) := TRUE
38   END; ...
39 END
```

```
1 Machine
2     RBAC_Model
3 INCLUDES
4     Functional, UserAssignments
5 SEES
6     ContextMachine
7 SETS
8     ENTITIES={MA_Label, ETCSOrder_Label, ...};
9  Attributes={MA_ValidatedMA_Label,ETCSOrder_AuthorizedETCSOrder_Label...};
10 Operations={MA_validateMA_Label, ETCSOrder_authorizeETCSOrder_Label...};
11 PERMISSIONS={OSM_MAPerm,Driver_MAPerm,TSM_MAPerm,TA_ETCSOrderPerm}
12 VARIABLES
13     PermissionAssignment, isPermitted, ...
14 INVARIANT
15     PermissionAssignment ∈ PERMISSIONS → (ROLES *ENTITIES)
16     ∧ isPermitted ∈ ROLES ↔ Operations ...
17 INITIAISATION
18     PermissionAssignment :=
19     {(OSM_MAPerm↦(OnboardSafetyManagement↦MA_Label)),
20     (Driver_MAPerm↦(Driver↦MA_Label)),
21     (TSM_MAPerm↦(TracksideSafetyManagement↦MA_Label)),
22     (TA_ETCSOrderPerm↦(TrafficAgent↦ETCSOrder_Label)),...}
23 OPERATIONS
24 secure_MA_validateMA(Instance)=
25   PRE Instance ∈ MA ∧ MA_ValidatedMA(Instance) = FALSE
26   THEN SELECT MA_validateMA_Label ∈ isPermitted[currentRole]
27     THEN MA_validateMA(Instance)
28     END
29   END;
30 secure_ETCSOrder_authorizeETCSOrder(Instance)=
31   PRE Instance ∈ ETCSOrder ∧
32     ETCSOrder_AuthorizedETCSOrder(Instance)= FALSE
33 THEN SELECT ETCSOrder_authorizeETCSOrder_Label∈isPermitted[currentRole]
34     THEN ETCSOrder_authorizeETCSOrder(Instance)
35     END
36   END; ...
37 END
```

Fig. 6.13 Abstract B-machines corresponding to functional and RBAC models of MA

expression. When the safety invariant is proved, this means that the global design respects the corresponding safety constraints.

6.4.4 Proposed Approach for Modelling Operating Rules

On the basis of the separation of the concerns, we proceeded to the functional and safety modelling of the exploitation rules by relying on the coupling of the formal methods, in this case the B-method, and semi-formal ones such as UML. This type of coupling is a subject studied for years thanks to their complementarity. Using the proposed methodology, three steps are needed:

1. a first step of analysis of the specification,
2. a second stage of semi-formal modelling in UML with the integration of profiles for the modelling of domain-specific concepts and
3. a third step of formal modelling with B-method and possibly its extension Event-B for verification of security properties and validation of case study scenarios.

6.5 Model Verification and Validation

6.5.1 ProB Animation for Checking

The transformation of UML models into B-specifications generates B operations which respect the type invariants (the types of class attributes, the multiplicity of inter-class associations, etc.) in the functional model and the safety policy (roles, permissions, etc.) in the security model.

Animation with ProB allows validating, according to the rights of each role, certain operations of the functional model and verifying the sequence of operations that builds the two scenarios. For the validation of rail-specific safety requirements, it is wise to add constraints to the safety model and/or to the functional model in order to ensure the conformance of the B-specification.

The animation of the sequence of operations with ProB reveals the need to add railway safety constraints to given operations in the form of preconditions or to the specification as a whole in the form of invariants. These constraints can be expressed as B annotations in UML models so that they are automatically transformed by the B4MSecure platform into the specifications generated in B.

This first step of model verification requires involving a railway expert in order to assess that the behaviour simulated in ProB really corresponds to the informal specification provided by the textual specifications (according to textual description

provided by the Subset 26[3]). Actually, a preliminary verification checks that classes that have been designed to be able to execute some needed scenario are really able to execute them in ProB animations without breaking invariants.

6.5.2 *Safety Invariant Checking*

Now, at a system level, let us consider the safety invariant expressing that, in a normal running mode, there must be only one train on a given section or block of the railway track whatever the technology used to locate trains or to ensure that they left a given area. It corresponds to a nominal scenario like a train owning an MA running in SR mode (Staff Responsible) and FS mode (Full Supervision, the mode providing the highest speeds), for example.

Let us express the non-collision constraint: considering two trains t1 and t2 belonging to instances of class TrainETCS and co-domain of the function TrainETCSSection, and such that train t1 is different from train t2, implies that corresponding images of reverse function of TrainETCSSection function are different. This constraint is formally expressed in Fig. 6.14. TrainETCSSection is a partial function from all Section to all TrainETCS which corresponds to an association between class Section and class TrainETCS.

The above constraint is expressed as a B invariant which has to be fulfilled by the global model. On this case study, the MA procedure was modelled, since the specification around an ERTMS MA is well defined. On the other hand, the topology of the railway infrastructure and the signalling technologies are not yet defined. The non-collision constraint is expressed here with no technological dependencies, and thus there is a need for the study to be performed.

Actually, proving this invariant on a specific railway infrastructure requires at least adding a gluing invariant between the variable belonging to the B code generated from the infrastructure model and the B code generated from the "complemented ERTMS Model." In this case, we assume that the infrastructure and ERTMS B-models must "be included" in a global abstract B-machine.

Actually, managing the coherency between the state of the track-side system and the state of the on-board system of an ETCS train is a task devoted to the RBC (see the ERTMS chapter to get a global view). Gluing the ETCSSection variable

$$\forall\ (t1,t2).(t1 \in \text{TrainETCS} \wedge t2 \in \text{TrainETCS} \wedge t1 \in \text{ran}(\text{TrainETCSSection}) \wedge t2 \in \text{ran}(\text{TrainETCSSection}) \wedge t1 \neq t2 \Rightarrow \text{TrainETCSSection}^{-1}(t1) \neq \text{TrainETCSSection}^{-1}(t2))$$

Fig. 6.14 Non-collision constraint

[3] https://www.era.europa.eu/.

with a variable corresponding physically to a block section in the model of a French high-speed line infrastructure provides correct results in this particular case.

When the line is a partition of physical track-circuits, and when there are ERTMS balises corresponding to track-circuit limits, there must exist a direct simple mapping between ERTMS objects ETCSSection and objects corresponding to infrastructure track-circuits.

This last remark is rather technical, but it illustrates that it is not reasonable to align two models without the knowledge of experts of the respective domains. Roughly speaking, this step requires the validation by an ERTMS expert, a national interlocking expert and a safety expert. Moreover, when the discussion includes the use of B-method in the alignment process, these experts must have an adequate level of expertise related to this technology.

Clearly, a difficult point is reached, as a round table between experts is to be organised on the respective B-models aiming at aligning variables and expressing global safety invariants on these variables. The alignment of the knowledge of different experts with different viewpoints is known to be a challenge (Fig. 6.15). Furthermore, B-method may not be the best formalist in order to achieve this goal.

6.6 Operating Rule Synthesis

6.6.1 Dealing with Particular Cases

As a counterexample of easy variable alignment, let us consider the example presented in Fig. 6.5, assuming that there is only a wheel counter between the points *b* and *c*.

This example represents a situation where a track of a double-track section is inoperative. In this case, a single track must be used in both directions, which requires the use of a complementary signalling system in order to manage the train movements. This signalling system may be considered as "light" when it is used only one wheel counter and the driver must apply a procedure called "approaching procedure." In fact, there is a zone between the green light and the point *b* where there is no permanent train detection. For this reason, the track vacancy in this undetected zone depends on the procedure applied by the driver. The correspondence between ETCSSection ERTMS objects and track-side objects is now broken.

The vacancy of the track is guaranteed by a procedure that should be mentioned in the operating rule of the line.

One may think that it is a particular case. But the fact is that a significant part of operating rules is dedicated to the management of various incidents, like

- what to do when the GSMR connection is broken;
- what to do when the DMI remains black;
- what to do after an emergency break (Post-Trip mode);

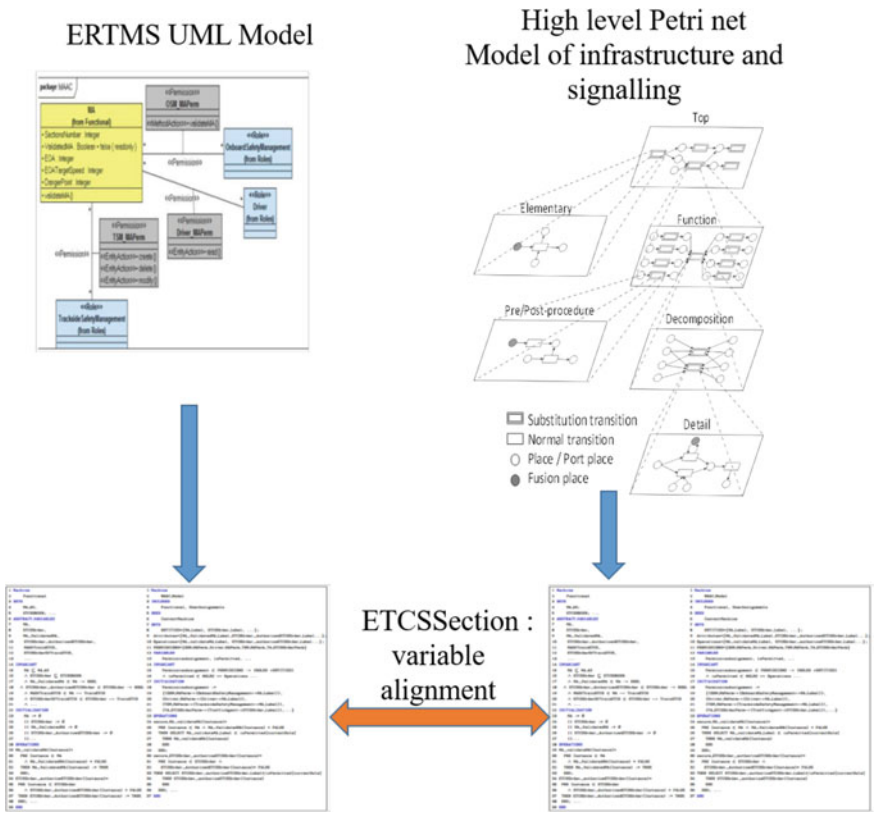


Fig. 6.15 B-model variable alignments

- what to do after a supposed collision with a non-identified object;
- etc.

A fact to be considered in a transnational line is that non-adaptive reflex actions may occur, as there are two different national contexts to be tackled. In this case, one may question: if the non-permanent signalling system is the same in the other country, does it use a similar approaching procedure to guaranty that a part of the track is free? If the procedure is similar, but a safety incidence occurs when the approaching procedure of the other country is applied, then it should probably be mentioned in the operating rule.

Finally, the border of the subject of this chapter is reached, as the discussion is related to human factor (i.e., on the probability to apply the bad procedure if they are similar). In this case, a work related to the conceptual modelling of intentional properties related to the human errors may be found in Debbech et al. (2019a,b) and Debbech (2019). Furthermore, writing the rule in order to avoid a mistake is a matter of specialists. This chapter only aims at specifying the logic to be fulfilled.

6.6.2 *Discussion on the RBAC Profile: Present and Future Contributions*

An advantage of the use of RBAC is that it provides an abstraction layer. When a procedure ensuring that a track section is free is to be executed by the driver, the task (and its context) is just added at the level of the driver role (see Fig. 6.9). Then, the B-specification is generated and the safety invariants must be proved in order to guarantee that the logical specification of the procedure is correct.

This approach was used in a Railenium[4] project focusing on French regional law traffic lines named NExTRegio (Ayed et al. 2016). The main idea is to let the traffic agent or the train driver execute a set of tasks when the volume of traffic does not allow investing in track-side automatism or in on-board devices. Actually, the same global safety services have to be provided, but the tasks are allocated in a different way to the various roles. Furthermore, this reallocation does not modify the safety reasoning, besides, proving the same system safety invariants is a strong argument that allows us to claim that a design modification does not impact the system safety.

6.6.2.1 Event-B Rather Than Classical B for System Engineering

Considering the limits of the proposed tool chain, it is relevant to discuss about the framework B4MSecure.

Considering the legal context influencing the rule in different countries, it seems not so adapted to only trigger the execution with regard to a set of static conditions. The OR-Bac profile proposes to integrate the organisation context, including the history of the system and it looks more appropriate.

Using classical B-models when B system exists seems not to be the best choice for a system engineering problem.

In the context of the ANR-VTT Perfect project, two PhDs thesis were defended. They both integrate a classical B generation from the UML RBAC profile or from high-level Petri nets. Up to now, the main applications produced in these works are based on classical B.

6.6.2.2 From RBAC to Or-Bac

Nevertheless, in the results of the Railenium project NExTRegio, there is a railway specific upgrade of the tool B4MSecure embedding a new UML profile inspired by Or-Bac (Bougacha et al. 2019). This profile is based on a new meta-model that adds a “Mode” class which associated with the “Context” class. “Mode” is specialised into two main classes: “nominal” and “failure” (Fig. 6.16).

[4] https://railenium.eu/en/.

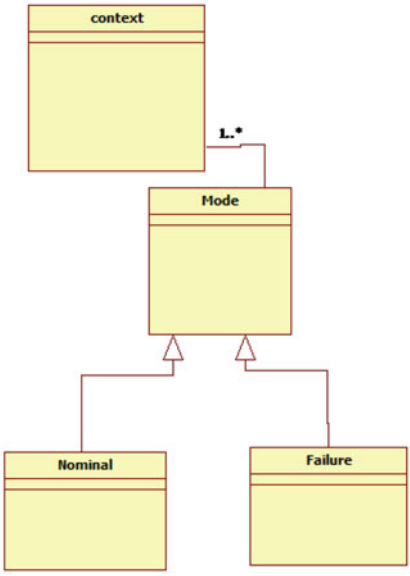


Fig. 6.16 The railway safety specific ad-on to a meta-model proposed for B4Msecure

The semantic of these two classes is still not validated by a systematic experimental feedback analysis. One of the motivations comes from the fact that specific analyses are needed in order to manage with all the failure modes. Failure modes depend on technologies and legal or industrial contexts. It means that national specific procedures are needed in the logical design of operating rules.

6.6.2.3 Motivation for a Railway Specific Meta-Model Specialisation

Let us propose a more subtle illustration of the justification of the "Failure" class being a specialisation of the "Mode" class, based on a real example.

In the French railway station of "Gare du Nord" in Paris, which is the biggest European station in terms of passenger traffic, the traffic capacity is a critical element. In this industrial context, some peak-hour trains are made assembling two TGV trains. The main motivation is to transfer twice the capacity of passenger using a unique object which is seen as a single train in the global signalling system. However, in order to make this double train, the following problem has to be solved: when a first TGV train is stopped at a quay, a second one must be able to approach it such a way that both trains can be coupled together.

The train stopped on a quay is protected by a closed signal, meaning that nobody is allowed to enter the quay zone. Let us assume that the second train is running under ETCS2. The second train arrives in front of the closed signal (corresponding to an EOA in the cab signal; see ERTMS chapter for more details) and contacts the traffic agent in order to receive a message authorising to process to an "Override EOA." Then, the second train can enter the quay zone using the "ON SIGHT" mode.

The use of "ON SIGHT" mode does not correspond to a nominal functioning, as its productivity does not correspond to the need in terms of commercial speed. Nevertheless, the above example has nothing to do with failure management, as it rather corresponds to a system adaptation to a high level of demand of passenger flows during peak hours. Rigorously, the class name should rather be something like "not nominal."

Another illustration can be found in the scenario of Fig. 6.4, when you assume that the second line is blocked, not by a tree fallen on the track, but by preventive maintenance works. This last scenario is not nominal, but it does not correspond to failure handling.

It must be noticed that crossing the border between two countries is considered as a specific phase or mode, and it must be checked that a procedure started in a first country can end safely in the second one. A dedicated chapter is focusing on this particular aspect.

6.6.2.4 A Multi-Component Refinement Proposition

Another step forward, the B4MSecure upgrade proposes to generate Event-B which is more efficient for dynamic system modelling (Wakrime et al. 2018). Industrial needs led to increase the Event-B semantic proposing a new REFSEES clause (Kraibi et al. 2019). The need corresponds to the possibility of refining a component which is coupled with other ones in order to allow an independent implementation synthesis. Identifying the proof obligations corresponding to this new clause in order to focus on a component design keeping the insurance of not braking global invariants is a work under progress (Fig. 6.17).

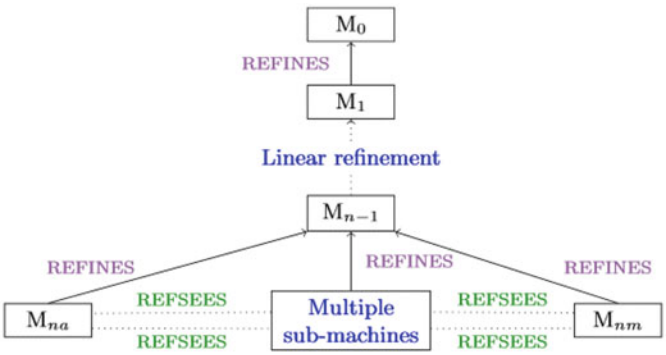


Fig. 6.17 The REFSEES proposition

6.6.2.5 Integrating the Requirement Engineering Tooling

The last difficulty identified in the tooled approach detailed in this chapter is at the level of the expression of the safety needs. More precisely, aligning B-models seems easier than aligning models using different formalisms. Nevertheless, the learning from experiments shows that expressing a B safety invariant and aligning variables in several generated B-specification are quite not easy. As a consequence, it may be error prone and this is actually not a good thing for a safety critical design process. An alternative can be found in the state of the art: applying the Kaos approach for the need engineering and proposing a SysML model capturing requirement and needs. Then, an original proposition of the FORMOSE project[5] is to federate the system ontology and ontology of the need in order to be able to generate obligation proof to be added in the B-model of the system in order to be able to prove that the needs are really met (Fotso et al. 2018a,b).

Making knowledge engineering with knowledge engineering tools like ontologies must be really more efficient. The principle looks good, but a real study is to be made in the context of the autonomous freight train project (Blin 2019) in order to validate this promising potential improvement of the present proposed approach.

6.7 Conclusion

Starting from challenges of rule synthesis and particularly safety rules, a model-based approach is presented. The main proposition is to model the rules using a UML centred approach on a first step. Then, the next step is the validation of the global design logic using a formal methodology and one of its supporting tools, B-method and Atelier B, which efficiency is demonstrated through the railway history.

It is proposed to generate B-specification corresponding to various automatisms using dedicated tools. The interlocking design is to be validated using Petri nets because this formalism is similar to the one familiar to automatism engineers (like the Grafcet formalism, for example). The interlocking design and Petri net are the subject to a particular chapter of this book.

Some particular signalling problems used to be specified with some particular DSLs (like relay-based specification). In this case, a translation of this DSL into B-machines is also presented as a proposed methodology. In this case, the benefits and the drawbacks of using this methodology are discussed, like the possibility of making automatic formal verification of the system and the need of modelling the system environmental aspects.

Concerning the rule modelling, the use of a role-based UML profile is proposed in order to allow specifying separately the functional part and the authorisation part. A modified semantic of the RBAC profile is proposed for railway safety analysis.

[5] https://anr.fr/Project-ANR-14-CE28-000.

Many times in this chapter, it was pointed out the need of system and/or language experts. Tracing the requirement from initial phases (from the expression of the need, for example) down to the proof of an Event-B model may provide to a real improvement of the methodology. In this case, some preliminary propositions were formulated in this chapter. Moreover, the refinement of multi-component architecture can be provided by a new semantic proposition for Event-B.

Nevertheless, through several scientific and industrial projects, the potential efficiency of an integrated multi-formalism formal method-based approach has been provided. The biggest step forward is probably to certify the tool chain, formally proving model transformations and qualifying the tool chain such a way that the final proof can be used not only as a help for safety experts, but as a part of safety demonstration.

References

Abrial, J.-R. (2010). *Modeling in Event-B: System and software engineering*. Cambridge, NY: Cambridge University Press.

ALCATEL, ALSTOM, ANSALDO SIGNAL, BOMBARDIER, INVENSYS RAIL, SIEMENS. (2006). ETCS-Baseline 2, system requirements specification.

Arago. (1997). Applications des méthodes formelles au logiciel. Observatoire Français des Techniques Avancées (OFTA) (Vol. 20), Masson.

Ayed, R. B., Collart-Dutilleul, S., Bon, P., Idani, A., & Ledru, Y. (2014). B formal validation of ERTMS/ETCS railway operating rules. In *International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z* (pp. 124–129). Berlin: Springer.

Ayed, R. B., Collart-Dutilleul, S., & Prun, E. (2016, October 2–7). Formal method to tailored solution for single track low traffic French lines. In *International Railway Safety Council (IRSC 2016)*. Paris: Springer.

Baumard, P. (1999). *Tacit knowledge in organizations*. Thousand Oaks, CA: Sage.

Behm, P., Benoit, P., Faivre, A., & Meynadier, J. M. (1999). METEOR: A successful application of B in a large project. In *International Symposium on Formal Methods* (pp. 369–387). Berlin: Springer.

Bézivin, J., & Gerbé, O. (2001). Towards a precise definition of the OMG/MDA framework. In *Proceedings 16th Annual International Conference on Automated Software Engineering (ASE 2001)* (pp. 273–280). Piscataway, NJ: IEEE.

Blakstad, H. C. (2006). Revising rules and reviving knowledge. Adapting hierarchical and risk based approaches to safety rule modifications in the Norwegian Railway System. Fakultet for samfunnsvitenskap og teknologiledelse.

Blin, C. (2019). Scientific and technological obstacles to achieve the autonomy. In *Keynote presentation at the International Conference on Reliability, Safety, and Security of Railway Systems - RSSRail2019, 4–6th June, Lille, France*.

Bon, P., Collart-Dutilleul, S., & Sun, P. (2013). Study of implementation of ERTMS with respect to French national rules using a B centred methodology. In *Proceedings of 2013 International Conference on Industrial Engineering and Systems Management (IESM)* (pp. 1–5). Piscataway, NJ: IEEE.

Bougacha, R., Ait, W. A., Kallel, S., Ben, A. R., & Collart-Dutilleul, S. (2019). A model-based approach for the modeling and the verification of railway signaling system. In *Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering* (pp. 367–376). SCITEPRESS-Science and Technology Publications, Lda.

Boulanger, J.-L. (2013). *Industrial use of formal methods: Formal verification*. New York: Wiley.
Butler, M. (2009). Incremental design of distributed systems with Event-B. *Engineering Methods and Tools for Software Safety and Security, 22*(131). IOS Press.
Butler, M., & Hallerstede, S. (2007). The Rodin formal modelling tool. In *BCS-FACS Christmas 2007 Meeting-Formal Methods in Industry, London*.
Collart-Dutilleul, S., Bon, P., & Petit, D. (2011). A set of design oriented scientific tools to assist abstract B machine specification. In *3rd IEEE International Symposium on Logistics and Industrial Informatics* (pp. 209–214). Piscataway, NJ: IEEE.
de Almeida Pereira, D. I., Debbech, S., Perin, M., Bon, P., & Collart-Dutilleul, S. (2019a). Formal specification of environmental aspects of a railway interlocking system based on a conceptual model. In *International Conference on Conceptual Modeling* (pp. 338–351). Cham: Springer.
de Almeida Pereira, D. I., Deharbe, D., Perin, M., & Bon, P. (2019b, June). B-specification of relay-based railway interlocking systems based on the propositional logic of the system state evolution. In *International Conference on Reliability, Safety, and Security of Railway Systems* (Vol. 2, No. 3, pp. 99–106, 242–258). Cham: Springer.
Debbech, S. (2019). Ontologies pour la gestion de sécurité ferroviaire : intégration de l'analyse dysfonctionnelle dans la conception. École Centrale de Lille.
Debbech, S., Bon, P., & Collart-Dutilleul, S. (2019a). Towards semantic interpretation of goal-oriented safety decisions based on foundational ontology. *Journal of Computers, 14*(4), 257–267.
Debbech, S., Bon, P., & Dutilleul, S. C. (2019b). Conceptual modelling of the dynamic goal-oriented safety management for safety critical systems. In *ICSOFT* (pp. 287–297).
Erbin, J. M., & Soulas, C. (2003). Twenty years of experiences with driverless metros in France. In *Proceedings of VWT19* (pp. 1–33).
Ferraiolo, D. F., & Kuhn, D. R. (1992). Role based access control. In *15th National Computer Security Conference* (pp. 13–16). Baltimore, MD: National Institute of Standards and Technology.
Fotso, S. J. T., Frappier, M., Laleau, R., Mammar, A., & Leuschel, M. (2018a). Formalisation of SysML/KAOS goal assignments with B system component decompositions. In *International Conference on Integrated Formal Methods* (pp. 377–397). Cham: Springer.
Fotso, S. J. T., Mammar, A., Laleau, R., & Frappier, M. (2018b). Event-B expression and verification of translation rules between SysML/KAOS domain models and B system specifications. In *International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z* (pp. 55–70). Cham: Springer.
Hale, A. R., Heijer, T., & Koornneef, F. (2003). Management of safety rules: The case of railways. *Safety Science Monitor, 7*(1), 1–11.
Hansen, K. M. (1998). Formalising railway interlocking systems. In *Nordic Seminar on Dependable Computing Systems* (pp. 83–94).
Jaber, H., Yakymets, N., Lanusse, A. (2012). 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)* (pp. 11–12).
Kraibi, K., Ayed, R. B., Rehm, J., Dutilleul, S. C., Bon, P., & Petit, D. (2019). Event-B decomposition analysis for systems behavior modeling. In *ICSOFT* (pp. 278–286).
Laleau, R., Semmak, F., Matoussi, A., Petit, D., Hammad, A., & Tatibouet, B. (2010). A first attempt to combine SysML requirements diagrams and B. *Innovations in Systems and Software Engineering, 6*(1–2), 47–54.
Lecomte, T. (2008). Safe and reliable metro platform screen doors control/command systems. In *International Symposium on Formal Methods* (pp. 430–434). Berlin: Springer.
Ledru, Y., Idani, A., Milhau, J., Qamar, N., Laleau, R., Richier, J. L., et al. (2011). Taking into account functional models in the validation of is security policies. In *International Conference on Advanced Information Systems Engineering* (pp. 592–606). Berlin: Springer.
Lodderstedt, T., Basin, D., & Doser, J. (2002). SecureUML: A UML-based modeling language for model-driven security. In *International Conference on the Unified Modeling Language* (pp. 426–441). Berlin: Springer.

Mammar, A., & Laleau, R. (2006). UB2SQL: A tool for building database applications using UML and B formal method. *Journal of Database Management (JDM), 17*(4), 70–89. IGI Global.

Milhau, J., Idani, A., Laleau, R., Labiadh, M. A., Ledru, Y., & Frappier, M. (2011). Combining UML, ASTD and B for the formal specification of an access control filter. *Innovations in Systems and Software Engineering, 7*(4), 303–313.

Patin, F., Pouzancre, G., & Servat, T. (2006). A formal approach in the implementation of a safety system for automatic control of platform doors. In *4th AFIS Conference on System Engineering*.

Qiu, S., Sallak, M., Schön, W., & Cherfi, Z. (2013). Modélisation et évaluation de la disponibilité d'un système de signalisation ferroviaire ERTMS niveau 2.

Réseau ferré de France (RFF). (2012). Principes et règles d'exploitation du système ETCS - Particularités en cas de superposition à un autre système de signalisation.

Sabatier, D. (2016). Using formal proof and B method at system level for industrial projects. In *International Conference on Reliability, Safety, and Security of Railway Systems* (pp. 20–31). Cham: Springer.

Snook, C., & Butler, M. (2006). UML-B: Formal modeling and design aided by UML. *ACM Transactions on Software Engineering and Methodology (TOSEM), 15*(1), 92–122.

Std, EN50126. (2000, January). Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS). European Committee for Electrotechnical Standardisation (CENELEC).

Std, EN50128. (2001, March). Railway applications - Communications, signalling and processing systems. European Committee for Electrotechnical Standardisation (CENELEC)

Std, EN50129. (2019, February). Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling. European Committee for Electrotechnical Standardisation (CENELEC).

Sun, P. (2015). Model based system engineering for safety of railway critical systems (Doctoral dissertation, Ecole Centrale de Lille).

Union Industry of Signalling (UNISIG). (2009). Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2.

Wakrime, A. A., Ayed, R. B., Collart-Dutilleul, S., Ledru, Y., & Idani, A. (2018). Formalizing railway signaling system ERTMS/ETCS using UML/Event-B. In *International Conference on Model and Data Engineering* (pp. 321–330). Cham: Springer.

Chapter 7
Formal Validation of Interlocking Under Signaling Rules

Pengfei Sun, Simon Collart-Dutilleul, and Philippe Bon

7.1 Introduction

The railway principles and standards used to be validated at the national level where each country has its own "language " for railway and its own requirements for managing trains on its network. Now, to promote the European rail market for passengers and freight, European Union has provided a solution called the ERTMS (European Railway Traffic Management System) that aims to create a common, harmonized, and standardized management of rail traffic and signaling in Europe in order to have a seamless network at the European level.

This brand new standard is easier to apply in the new lines, where wayside signaling cost is kept to a minimum, but all the vehicle fleets that operate on these lines must be equipped with the ERTMS on-board system. However, for the existing lines, there is an alternative "Mixed operation " solution. This is a strategy where the wayside signaling is equipped with both ERTMS and conventional systems. Normally, the conventional one is the legacy line used during the upgrade program. The main reasons for applying such a mixed solution are: financial and organizational constraints make it impossible to install ERTMS in the whole network in a short time. In addition, not every train has to go across the border line, and ERTMS-equipped trains sometimes have to run on the conventional lines. Most national companies prefer to gradually deploy the ERTMS in order to replace the conventional systems with a unified European system.

P. Sun (✉)
Southwest Jiaotong University Chengdu, Chengdu, China
e-mail: pengfeisun@home.swjtu.edu.cn

S. Collart-Dutilleul · P. Bon
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr; philippe.bon@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_7

Every conventional signaling system is the result of historical evolution, which was boosted by progressively technological development and lessons of accidents. Generally, its safety is ensured by engineering experiences, rather than by systematic methodology and their evaluations. So far, there has not been a lot of engineering experiences of ERTMS, which means it is impossible to evaluate the new system in the traditional way. Meanwhile, the management of railway signaling in ERTMS is based on the local rules pertaining to each country and not on global ones, which makes it difficult to evaluate the combined system in terms of safety. However, as a signaling system, its most important responsibility is to maintain transportation safety. Therefore, any implementations before being put into use should have detailed verification and validation (V&V), especially the compatibility of ERTMS and conventional signaling standards and systems.

One of the basic requirements of the railway safety is that a system must prevent trains from collision. For this reason, there is a mechanism, called railway interlocking system (RIS), which is a collection of associated devices, complying with explicit signaling principles. The purpose of the RIS is to maintain the transit safety by connecting and arranging the points and signals, so that a hazardous condition cannot arise. The specification and analysis of the RIS is an important part of the deployment of ERTMS. The evaluation of their global consistency is needed, which concerns the consistency between the conventional system and the ERTMS-equipped system, with regard to safety. This issue is crucial, and yet it has scarcely been covered by scientific literature. In fact, one of the difficulties of this problem comes from the lack of formal representations of both systems that could enable the validation of different aspects through test scenarios. So some new methodologies that are more systematic and formal need to be adopted.

In order to maintain high-level safety with deterministic scope, a project, called "PERFECT," was launched to develop the safety specification and verification of French railway interlocking systems in the context of national rules and the influence of implementing ERTMS laws on the original systems (Bon et al. 2013; Collart-Dutilleul et al. 2014; Sun et al. 2014). This chapter will introduce the low-level part and the fundamental phase of the project. It focuses on the formal validation approach of the French railway RIS based on the computer-controlled relay-based system. This study aims to provide a methodology for a comprehensive assessment of the consistency of the following two aspects: the operating rules of local signaling systems and the additional safety requirements (which means the ERTMS).

With this methodology, we are able to follow the safety analysis: the safety assessment of new systems, the analysis of given scenarios, and the evaluation of safety requirements of system updates. After this method is recognized by railway experts, we will develop the method in an automatic methodological tool easily applied in practice. Then, we will provide a methodology for translations between the exclusive model train and classical Petri net model. This will allow us the opportunity to apply our research results in actual practice.

7.2 State of Art

Nowadays, the design of railway systems increasingly benefits from advances in computer science, information technology, mathematics, and other engineering disciplines. Most of the railway devices are computer-related devices, which means either of these systems includes some software or is controlled by software. But software is notorious for having unpredictable bugs that may threaten its correct functioning. With the rising complexity, for a system that is composed of multiple computing elements, it is unfeasible to demonstrate the safety of a collection of behaviors with traditional safety assessments. "The employment of very stable technology and the quest for the highest possible guarantees have been key aspects in the adoption of computer-controlled equipment in railway applications" (Fantechi 2012; Fantechi et al. 2012). Therefore, the development and the implementation of formal proof and verification of system safety have been seen as a necessity for the railway domain.

So far, the railway signaling-related domain has been considered the most suitable and the most fruitful areas for formal methods (Fantechi et al. 2012). It is because railway signaling is safety critical. It has discrete nature and absence of hard real-time need. The broad use of FMs in this field has already been witnessed by over 182 references in an early review (Bjørner 2003). Some recent surveys and reviews (Bacherini et al. 2006; Fantechi 2012, 2014; Fantechi et al. 2014, 2012) focus on the advances in both formal method approaches and railway signaling applications. Still, lots of related work that has been performed by railway companies are not published because of confidentiality considerations.

In this chapter, our candidate is colored Petri net (CPN), a graphical modelling language, whose basic concept, Petri net, is first introduced by C. A. Petri (1966). The basic Petri net (or element Petri net) has the advantage of expressing discrete event control systems, and studies of Petri nets in railway can be traced back almost 20 years ago. However, the descriptive ability of basic Petri net seems not to meet the needs of complex systems. Many derivatives of Petri net have been introduced in this research area, such as colored Petri net (Jensen 1981, 1987).

With the help of such high-level Petri net, there comes a large-scale application—Oslo Subway (Bjørk 2006; Hagalisletto et al. 2007; Moen and Yu 2004; Yu 2004)—that integrates CPNs into the system development to simulate the Oslo subway and analyze schedules of trains. This project developed a specification tool for specifying and automatically constructing large CPN models of railroads. One of the important project experiences shows that CPN is a good specification language for communication because the research group collaborated with chief engineers from railroad infrastructure and traffic department. Although none were specialists in Petri nets nor formal methods, they understood the models and were able to provide suggestions for improving the system.

The specification, analysis, and implementation of railway control logic are always a hot research topic. In work, Fanti et al. (2006), Giua and Seatzu (2008) discuss the control of the railway network using CPNs. A resource-oriented CPN

method is introduced in Wu and Zhou (2004), which could deal with the deadlock of automated guided vehicle (AGV) systems. Cheng and Yang (2009) use a fuzzy Petri net for railway traffic control. A similar solution can be found in Kaakai et al. (2007) using a hybrid Petri net.

The level crossing (LC) is also a critical crux in both road and rail infrastructures. Stochastic Petri nets are applied in Ghazel (2009), Huang et al. (2010) in order to precisely reflect the system's dynamics. Furthermore, stochastic Petri nets could be used to evaluate the real-time system in railways, such as data processing (Zimmermann and Hommel 2003) and device-to-device communication (Lei et al. 2013).

Besides ETCS, there is another advanced train control system, called "communication-based train control (CBTC)," which has been applied to many metros. Its protocols and services have been studied by CPN (Chen et al. 2007; Xu and Tang 2007), deterministic and stochastic Petri net (Zhu et al. 2012), and timed Petri net (Wang and Bai 2010).

In France's railway domain, the French National Railway Company (SNCF) has initiated and participated in many projects. One of the most successful projects is to develop a formal validation method and tools for new computerized RISs and existing RISs (Antoni 2009a,b,c; Antoni and Ammad 2007, 2008). This project is led by Marc Antoni, the head of Innovation and technologic pole of SNCF Infra and director of the Rail System Department of UIC. This study developed four successive DSL tools (Antoni 2012b):

1. Tools A: general way for the definition of safety properties
2. Tools B: generation of the safety properties file
3. Tools C: proving tool: formal validation tool
4. Tools D: reached system state tree and execution certificate

In Tools A and B, the safety properties are specified with interpretable deterministic Petri nets, which will be later interpreted in the target machine. This method has been accepted by SNCF Infra. Now it has been applied in real RIS of "Noisy le Roy," situated next to Paris, and also applied in a new double-track level crossing. It is said that this method will be used by UIC and will be applied in the German system (Antoni 2012a).

Moreover, in order to verify the high-level systems' safety requirements, SNCF has made some performance assessments for both local signaling rules and European signaling standards, by specification and analysis of CPNs (Buchheit et al. 2011; Lalouette et al. 2010; Gregory et al. 2010).

7.3 Preliminary of Railway Safety and Interlocking System

This chapter aims to describe and to formalize some major safety properties and the control logic of interlocking systems in French railway. The reader who is familiar with the background can skip this section.

7.3.1 Safety Management of French Railway System

The concept of safety has different explanations depending on the nature of the systems and activities. The safety of rail traffic is particularly based on "the possibility of stopping." Most of the signaling rules take this concept as the primary requirement. If no train is moving, there will not be any danger to the traffic itself. So the basic system state can be simplified as the diagram shown in Fig. 7.1. This concept of safety is also widely used in the train control procedures, such as the ATP system, which stops the train according to the radio-based signals, in order to avoid a collision.

Any signaling rules and signaling-related procedures require a full explanation of safety properties. In French, they are historically based on *determinism*. Every system state has one or more causes. If a state is undesirable, removing its causes should help to avoid it.

One commonly used method is reasoning, which is necessary to exploit for every state, and especially to ensure that an undesirable event does not take place. The deterministic reasoning can only be applied to a closed system; otherwise, there will be a risk of unforeseen system state. Thus, the principle of the organization of the external environment is to limit the number of interactions, in order to avoid introducing chaos. As the external environment is one of the foundations of safety design, only those directly related to safety should be considered. This technique has already been used for operating safety and technical safety in French railway for a long time and its result proved to be safe.

Nowadays, with the development of the computer, the computer-controlled equipment plays an important role in many industrial areas. It has some advantages such as:

- Handling of complex new functions
- Ability of long distance remote control
- Reduction in staff

But everything has its two sides. It also has disadvantages such as:

- Long development cycle and hard to modify safely once the produce is finished.
- Require qualified operating and maintenance staffs.

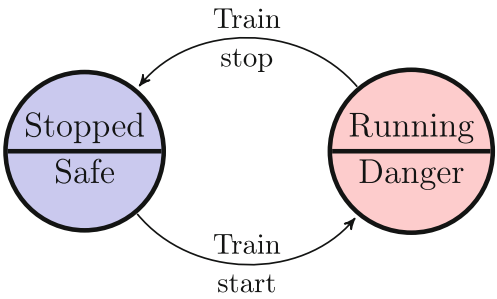


Fig. 7.1 Railway system state

- More difficult to validate and to integrate into the global system.
- The life cycle of computer devices is shorter than that of mechanical ones.

Unfortunately, many experiences show that the current development method cannot provide a safety guaranteed system according to SIL3 or SIL4. And the integration safety cannot be ensured under the global framework. A study has shown that "more than 3/4 accidents in relation with computerized systems are due to specification errors" (Antoni 2012a). Those accidents are caused by incorrect fiction descriptions, unthoughtful modifications, or improper maintenance.

In the traditional system, it was necessary to identify the failure events and to reduce their occurrence causes. When adopting the computer-controlled system, formal proof or verification is therefore regarded as a necessity. The following aspects should be taken into consideration.

- The functions and behaviors of such automated systems must be deterministic.
- Some properties should be specified rigorously:
  - Safety predicates
  - Functional predicates
  - Assumptions of interactions with the external environment
- For model checking-based formal proof, it is only possible when the reachable system states are finite.

The safety state of a computer-controlled signaling system is shown in Fig. 7.2. Transitions with red forbidden sign are the undesired system changes, which should

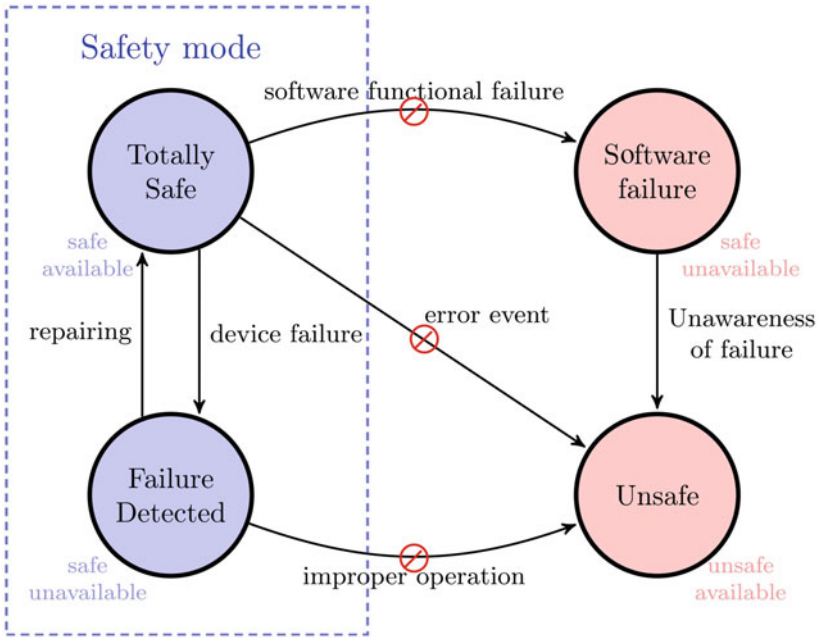


Fig. 7.2 The overall safety of a computer-controlled signaling system

be identified and reduced through formal specification & verification. In this way, the final system could operate as a “fail safe ” system.

7.3.2 *French Railway Interlocking System*

One of the basic requirements of the railway safety is that a system must prevent trains from collision. For this reason, there is a mechanism, called railway interlocking system (RIS), which is a collection of associated devices, complying with explicit signaling principles. The purpose of the RIS is to maintain the transit safety by connecting and arranging the points and signals, so that a hazardous condition cannot arise.

There is a simple example of an interlocking system, as illustrated in Fig. 7.3. Track segments are represented in a topology structure, and all of them have track circuits that detect the occupation of a train. Joints of different track lines represent the points. The sign-board-like symbols are signals of various types of transition control. This example is constituted by 2 allowed routes, 1 point, 2 signals, and 3 track circuits. The interlocking route that a train can go through safely must meet the following requirements:

- All points are properly positioned and are locked.
- Conflicting routes must be protected.
- All the tracks along the route must be clear.

When all of the above conditions are satisfied, the signals can be set to green to let the train enter the route. These rules express the fundamental principles that

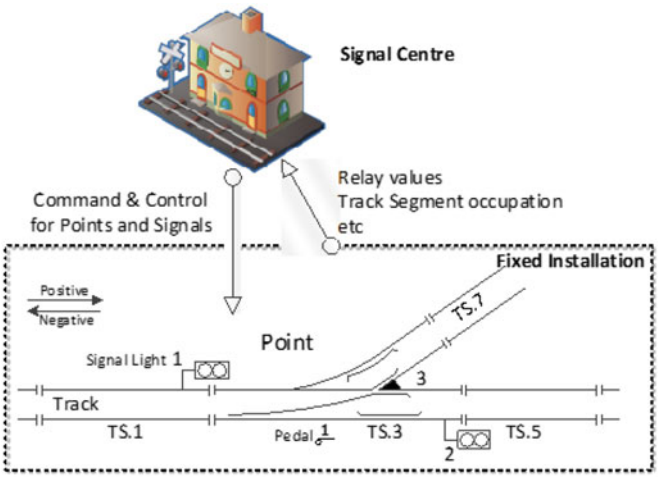


Fig. 7.3 An example of railway interlocking system

hold for all the RISs. Such rules ensure only the correct combinations of tracks, points, and signals, in order to avoid accidents. The signal indications authorize the movements of the train. They are handled by the interlocking system and can be considered as an indicator of the route establishment.

In our research, we restrict ourselves to the modelling of RISs. To better specify this complex system, we now introduce its composition and main components. In railway signaling, the term "interlocking" has two meanings (Pachl 2002). First, "an interlocking" is an arrangement of signal appliances that prevent conflicting movements through an arrangement of tracks. Second, principles to achieve a safety arrangement between signal appliances are also generally called "interlocking."

According to the above definition and considering the train and the operator as external interactions, the RIS could be roughly divided into two parts: the signaling operations and the fixed installations.

Signaling operations are a set of operating rules and procedures that can maintain safety and high efficiency of transits. It comprises computer automatic controls and human control processes. Normally, the computer responds to most of the device-oriented operations, such as route establishment, route auto-destruction, $\cdots$, while human control deals with decision-making, such as route selection, route mode selection, route manual destruction, $\cdots$, and some non-regular operations, such as shunting operations.

Fixed installations are a set of components of geographical routes that include straight track sections, points, signal lights, and some ground-based automatic signaling devices that could work automatically and do not need supervision from the signaling center. Thus, they should be treated as a component in the geographical route.

7.4 Formal Modelling of Railway Interlocking System via HCPN

In this section, we will study the modelling of the French railway interlocking system using hierarchical colored Petri net.

First, we describe the modelling structure of an interlocking system and its corresponding network, as well as a set of interlocking properties that this network should obey. Subsequently, we specify this interlocking system with colored Petri nets in a generic and compact structure. In this modelling framework, the high-level functions of RIS are modelled in terms of a hierarchical and modular point of view. The railway layout (networks) is modelled in a geographical perspective, in order to be easily understood by railway expert engineers. Then, for the high-level parts of RIS, we propose a modelling pattern of the French railway interlocking system, which is a parameterized model that respects the French national rules. It is a general reusable solution to this kind of problem and can be used in many different given contexts. Finally, for the low-level parts of RIS, we introduce an event-based concept

into the modelling process, in order to better describe the internal interaction of low-level interlocking logic. In this process, a reduction policy is applied both before and after the state space calculation to obtain a new compact graph with the same reliability for analysis.

7.4.1 GRAFCET and Petri Net

Petri net is a formal, mathematical, well-developed theory. However, French industry still prefers to use another informal tool—GRAFCET. In order to be close to industry usage habits, and to take advantage of formal methods, we make a little comparison of GRAFCET and Petri nets to discuss why the Petri net is our best solution for modelling the French railway system.

GRAphe Fonctionnel de Commande Étape/Transition (GRAFCET) is a method of representation and analysis of automation. This is a graphical tool for describing the behaviors of the control processes. It describes the informational interactions across the system boundary. This mode of representation is independent of the technology used in the automation and reflects a consistent specification of the automatism.

This method was proposed in 1977 by the Association Français pour la Cybernetique Economique et Technique (AFCET) as a standard to represent specifications for software control systems. It was accepted in 1982 as a French standard. Latter in 1987, it was accepted as an international standard IEC 1131.3 by the International Electrotechnical Commission. The GRAFCET is also known as DFS (Diagramme Fonctionnel en Séquence) or in English, the SFC (Sequential Function Chart).

The GRAFCET has many advantages, and it already has a wide range of applications. However, with the increasing safety need of the international standards, GRAFCET has also long been criticized because of its lack of a formal foundation that allows it to ensure correctness and safety requirements. On the other hand, "it lacks adequate methodology that allows an efficient development of high quality models in the case of complex systems on the other" (Zaytoon and Villermain-Lecolier 1999).

To compensate for its deficiency, researchers began to use other formal languages to describe GRAFCET. Particularly, formal design methods of state diagrams and Petri nets are available. State diagrams are easy to learn and can be converted into many existing programming languages of GRAFCET without any problem. However, some complex structures, such as a parallel, cannot be well represented. Petri nets can achieve almost all the structures of GRAFCET (René and Alla 1992, 1997). The models can be extensively analyzed by PNs in order to prove formally. Also, the model of PNs can be converted into GRAFCET. Furthermore, PNs are also accepted by some French industries. Here is a comparison of the structure of GRAFCET and PN in Table 7.1.

Based on Table 7.1, we can easily transform a GRAFCET model into a PN model as shown in Fig. 7.4. Their notation formalism is so close that the engineer who is

Table 7.1 Structure comparison between GRAFCET and Petri net

GRAFCET		Petri net
Step	⇔	Place
Transition	⇔	Transition
Link	⇔	Arc
Receptivity	⇔	Guard
Action	⇔	Auxiliary place

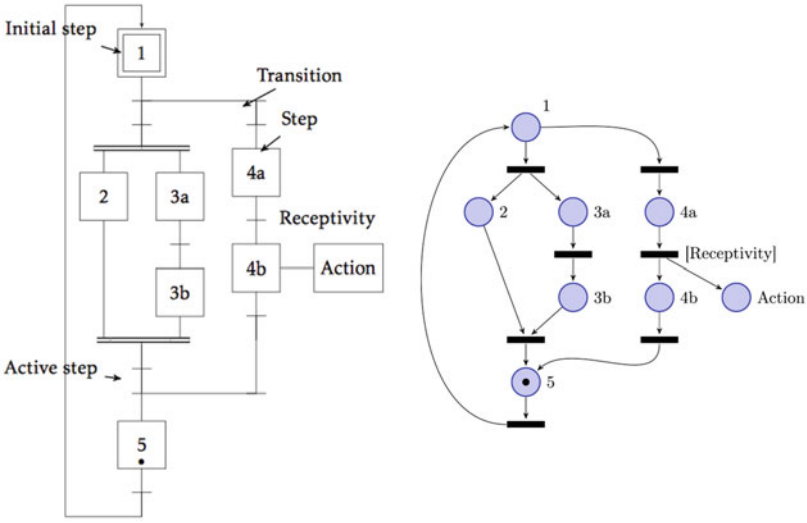


Fig. 7.4 Model comparison between GRAFCET and Petri net

familiar with the GRAFCET will easily understand the models of PNs. In other words, if a system is specified by PNs, it can be validated both by PN tools and by experienced expert engineers. In this way, the designed system can be considered as a strong formal proof. As a result, the PN is the most appropriate formal language to continue our research. Currently, the PNs are accepted by some French industries, such as the French National Railway Company (SNCF) (Antoni 2012b; Buchheit et al. 2011; Lalouette et al. 2010).

The major difference between these two languages is the mechanism of "concurrency." The GRAFCET allows all the enabled concurrent transitions to be fired at the same time, while in PNs, there will be a "choice" of firing one or another transition, thus reaching different new markings. Further information on the differences between GRAFCET and PNs can be found in Giua and DiCesare (1993).

7.4.2 *Initial Colored Petri Net Specification of Railway Interlocking System*

In our research, we focus on the traffic safety aspect and suppose that all the fixed infrastructures are both reliable and robust. The only threat to safety comes from the imperfect signaling rules or the incompatible international standards.

The modelling framework of the whole railway interlocking system could be divided into three parts: the signaling operations, the fixed installations, and rolling stock, as in Fig. 7.5. The train driver communicates with the dispatcher and requests an interlocking route. Train movement is a series of interactions with fixed installations (such as stopping at red lights and actions on track circuit). In response to train requests, the signaling operations send certain commands to fixed installations (such as points and signal lights) according to its operating principles:

- Signaling operations is a set of operating rules and control procedures of an interlocking system. It comprises computer automatic control and human manual control. Normally, the computer processes are responsible for most of the device-oriented operations, while human dispatchers deal with decision-making and non-regular operations.
- Fixed installations include track segments, points, signal lights, and other automatic facilities that could be self-acting without the instruction from the train controlling center. Whereas the critical safety results are always represented in the fixed installations, the safety verification for all the fixed ones' function is needed.
- Rolling stock runs on interlocking routes and is supervised by both route conditions and operating instructions.

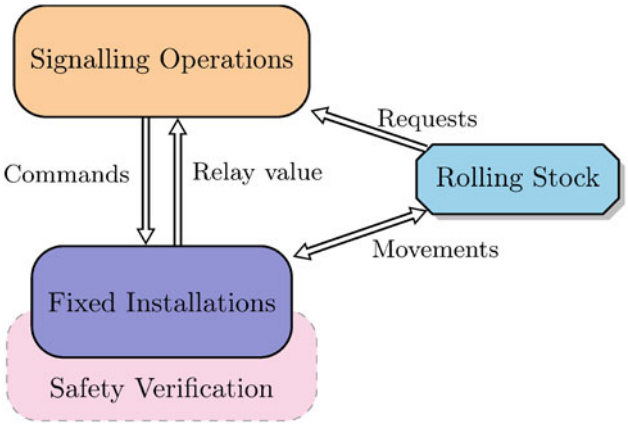


Fig. 7.5 Specification framework of railway interlocking system

Considering the large scale and the space complexity of interlocking systems, one feasible solution is to model the RIS by HCPN. The signaling operations and the fixed installations are represented by the topology structure of PN, in order to express complex connections and logical relations between different devices, while each train is defined as a colored token that can move along the network of track work.

To distinguish between various syntactic parts of a Petri net model, we classify different nets into 3 types. The first two basic types in RIS are the signaling operations and the fixed installations. The net $N^o = (T^o, P^o, A^o, \varepsilon^o)$ represents the operation part that implements the route management process and movement authority control. The net $N^i = \left(T^i, P^i, A^i, \varepsilon^i\right)$ represents the installation part where the train movements are realized by the transitions $t \in T^i$. The notation $N^s = (T^s, P^s, A^s, \varepsilon^s)$ denotes the supplemental part that is used to ensure the integrity of the model simulation and safety analysis. It could realize the initial simulation inputs or actions from the human operators, where $p \in P^s$ may be a compound place existing in other nets.

In order to standardize our modelling process, we have definitions below:

Definition 7.1 A basic unmarked RIS net is a connected Petri net

$$N_{RIS} = N^o \bigcup N^i \bigcup N^s,$$

where $N^o \cap N^i = P_{equip}$, N^o should not be an empty set $N^o \neq \varnothing_{pn}$ and N^i is strongly connected.

The common parts P_{equip} of the operation nets and the installation nets are signal equipment, such as signal lights and position of points. They perform the role of indicator in the operation nets and conduct the train movement in the installation nets.

7.4.3 A Geographical Approach of Railway Interlocking System

As a first approach, the RIS is specified into a CPN in a hierarchical and geographical perspective. This study can be found in our previous work (Sun et al. 2014). The basic hierarchy of the HCPN model framework is described in Fig. 7.6 The main net is the topmost net, which is the carrier of the whole model, "storing" all the subsystems and their interactions.

In the following subsections, we introduce the specifications of signaling part and installation part separately.

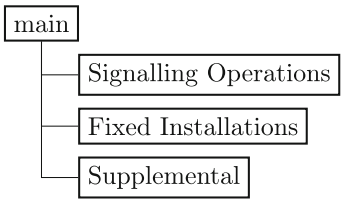


Fig. 7.6 Basic specification framework of railway interlocking system

7.4.3.1 Signaling Operation Specification

RIS signaling operations are a system with multi-input and multi-output. Their operating processes are involved with the functions in distributed levels. When modelling such a system, a specific model for system functionality seems not suitable for achieving the modelling objective. Successful experience in modelling the European Train Control System using CPN (Janhsen et al. 1997; Jansen et al. 1998) could give us some useful inspiration. In such systems, there are three aspects that should be integrated: *components*, *scenarios*, and *functions*.

When modelling the *component* view, the aim is to specify the communications and the interactions between different subsystems. A net of the component view shows a subsystem and its interfaces, and it could be further detailed in additional levels. The *scenario* view is the modelling of operational procedures. Its main elements are the sequence of events required to maintain operation, and the interactions between the signaling operations and the fixed installations. Individual scenarios are categorized into different groups, and in this way, they could be integrated into the corresponding component model. The *functions* represent the lower model level. They are involved in the process aspect and represent the activities or the response to interactions from the scenarios. Some of the functional modules can be used in different objects and the so-called functional blocks. These functional blocks are modelled as separate nets and can serve as functions in different scenarios, under the modelling principle of hierarchic decomposition. In this way, the subnets can be reused.

As the objective model framework needs to have so many features, an extensible framework is needed, which should also be readable, maintainable, and easy to accept by others. As a result, it should be modelled in a modular way. The hierarchical structure is the most consistent with the modelling requirements. It could integrate different functions of the system description and contain isolated modularity views in the model. Besides, their advantages are easy to comprehend and adapt and modular models can be reused. Meanwhile, the hierarchical ability of CPN provides a good basis for setting up the model in a straightforward way.

In order to structure the main component models of the signaling operations, a layered approach, proposed by Janhsen et al. (1997), Jansen et al. (1998), is adopted. Dynamics and functionality are expressed by both scenarios and functions. Scenarios show the behaviors of the system in its external environment, which means the railway operation context. Functions can process data received from external components or internal ones. The difference between scenarios and functions is that

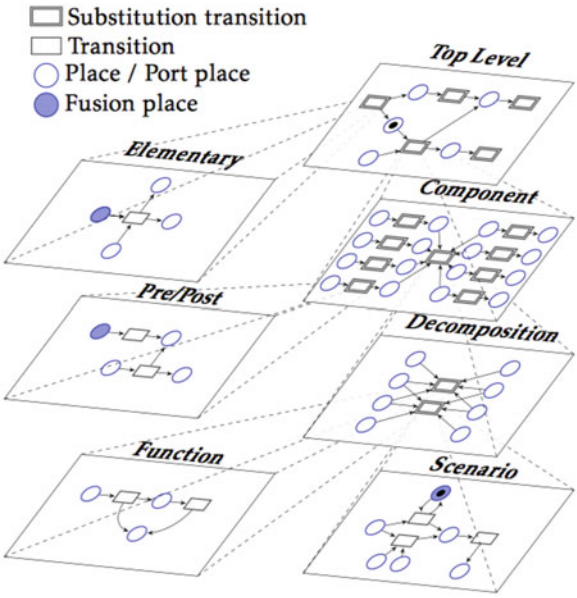


Fig. 7.7 Hierarchical model structure of signaling operation

functions are not subordinated to any scenarios. They are independent of scenarios and can be used within arbitrary scenarios.

Moreover, the concept of function in this thesis is not restricted to the very basis mathematical functions but can also represent procedures (may complex ones). To be more precise, each function represents a task. However, given the nature of their functionalities, we continue to use "functions" to refer to them. The corresponding vertical decomposition model is in Fig. 7.7 with several levels. The generic structure has a "Top Level" to store all the components. It shows the connections between components and their corresponding communications. The "Composition" layer shows the detail of the component models. The "Decomposition" layer represents the decomposition of the component model because some components are too complex to represent in one single model. The "Function" layers and the "Scenario" layers represent the function view and scenario view, respectively, and they may be further decomposed if necessary.

Moreover, for simulation purposes and compatibility reasons, two supplementary levels should be added into the hierarchical structure. The "Elementary" level is used to replace the preliminary transition of the top level. The "Pre/Post"-level concerns relations between components. They are used for preprocessing incoming messages and post-processing outgoing messages.

To illustrate how to map from signaling operation to the CPN model, here is a small demonstration of the route formation procedure, an important part of the interlocking operation. A complete process control always involves many aspects (see Page 392 in Rétiveau (1987)). As a demonstration example, only the core of the control flow will be presented. In Fig. 7.8a, there is the control flow chart. It

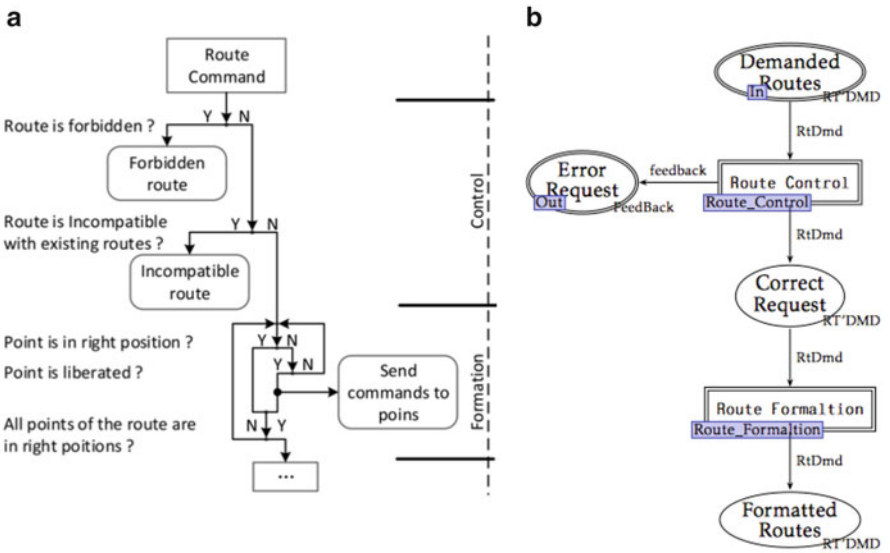


Fig. 7.8 Example of mapping signaling operations. (**a**) Route establishment flow chart. (**b**) Corresponding HCPN model

receives the route control instruction (route command) and checks whether this instruction is feasible and compatible with the existing ones. Then it will format the route according to its formation information, such as the positions of points.

The first 2 consecutive actions of interlocking route establishment are: control and formation. The control part validates the input of "Route control" instruction and acts as a filter. Only when the requested route is satisfied with current interlocking status, it is allowed to establish. Otherwise, an error message will be output and the process ends. In the French context, 2 aspects are checked concerning safety:

Forbidden route Inverse transit is forbidden and must be deactivated. When a track segment is acting as the destination of an established route, any new route originated from it is forbidden.

Incompatible route The region ahead of the signal must be free (in the case of a DA[1] route). This means that only when a route is partially destroyed because of the use of flexible transit 5, the corresponding initial signal can be used for another route. Otherwise, any new routes originating from the same signal are incompatible.

The formation part positions all the points of the commanded route. If the point is already in the expected position, no further action is performed. If the point

[1]Destruction automatic: A typical French interlocking route type that could be destructed by the passage of the train.

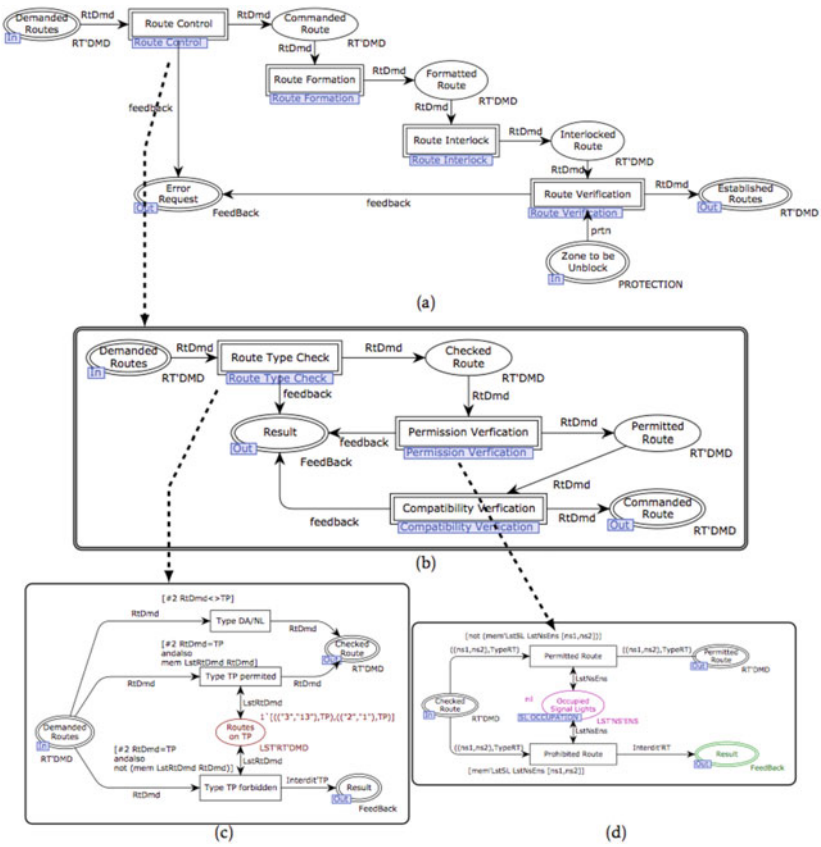


Fig. 7.9 Example of mapping signaling operations (2). (**a**) Composition net (route establishment). (**b**) Decomposition net (route control). (**c**) Scenario net (route type check). (**d**) Function net (permission verification)

is occupied by other routes, the process will wait until it is released. Only if a point is not in the right position and is liberated, an instruction will be sent to the fixed installation model to change the point. After receiving the new position, the procedure continues to confirm the next point of the route. When all the points are in the right position, this process is over.

The real corresponding model of the control flow is represented in Fig. 7.9.

Figure 7.9a represents a "Component level." It consists of hierarchical transitions for route control and route formation. The input place contains the token of route information. It could be passed through the model or output an error token. Figure 7.9b is the decomposition net of route command procedure. It still contains sequences of functions: route type check, permission verification, and compatibility verification. Figure 7.9c is a scenario net, because the place "Routes on TP" contains

the configuration of a certain scenario. Figure 7.9d is a function net, because its function is independent of the scenarios.

It should be noted that in this hierarchical structure, only the scenario nets reflect the localization of the stations by their configurations (the initial tokens), while the other parts of the model are the specifications of national railway standards and do not vary with different stations. Once we have completed a model of the signaling operations, the models of other stations under the same national standards could easily be derived from the previous model by only changing the initial tokens in each scenario net.

7.4.3.2 Geographical Railroad Layout Specification

The normal solution of modelling the fixed installations is the geographical approach. This approach can be considered as distributing the knowledge of the interlocking rules to objects modelling the geographic placement of physical elements (Banci et al. 2004). Its geographical structure allows us to slice the whole railway layout into independent and distributed components that can be individually modelled and physically located next to their relevant units.

Normally, an RIS route layout is made up of multiple similar components: tracks, points, and track-side signals. A track segment is a section of straight track that contains a complete track circuit for occupation detection. It is a simple straight or Y-shape with a point. A point is a railroad switch enabling railway trains to be guided from one track to another. The direction of the point is controlled by the signaling system according to the route requests. Generally, an interlocking system is within a station yard, where trains are running at low speed, so train movements are partly directed by fixed signal lights installed along the rail. A signal light mainly uses two aspects: red (stop intermediately) and green (route clear).

Both track and point are referenced as atomic components, which could form the geo-graphical structure of the whole railway layout and compose the route for transit. These journeys are also properly controlled by signal components along the railway layout, so the signal light could be regarded as constraints for train movement.

Track Segments

Figure 7.10 shows a demo of PN of two successive track segments. Each place represents a track segment. Two transitions move train tokens between the two segments, depending on the direction of the train and supervision by the guard function of the transitions. The direction from left to right is referred to as the “odd” direction (impair in French system), and the opposite direction is called the “even” (pair in French system) direction.

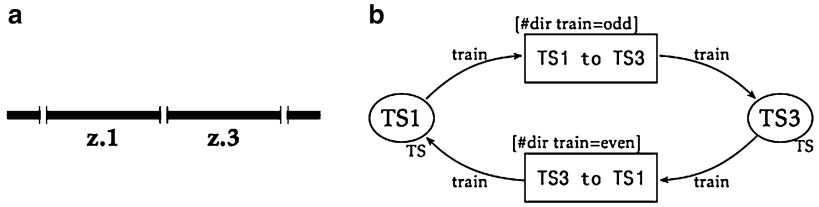


Fig. 7.10 A Petri net representation of track segments. (**a**) Track segment demo. (**b**) Corresponding CPN model

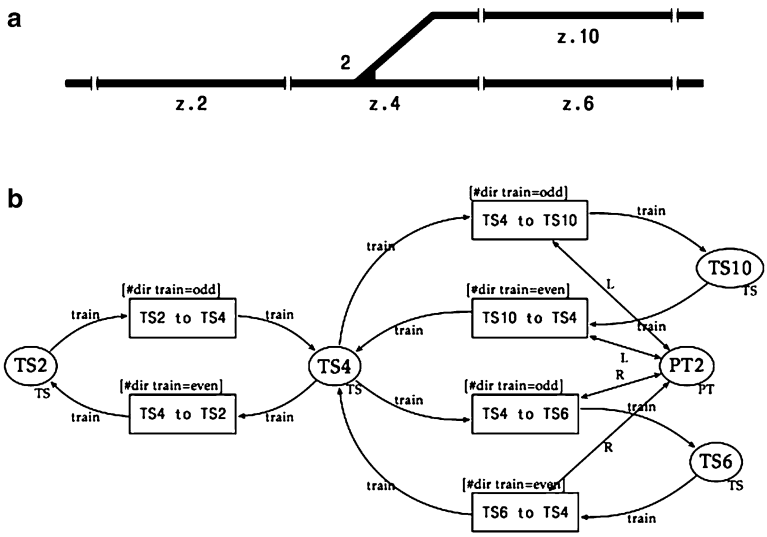


Fig. 7.11 A Petri net representation of point component. (**a**) Point demo. (**b**) Corresponding CPN model

Points

Figure 7.11 shows a CPN model of a point component. In the French railway system, a point is attached to a track segment, as shown in Fig. 7.11a. In its corresponding model, the point is represented by a single place that stores the current connection information (left or right). In the French system, the position "left" or "right" refers to the tracks on the left or right side when facing a point. This point place works as a condition place of 4 transitions (movements). However, its position will not affect the movements between TS2 and TS4 as they are constantly connected.

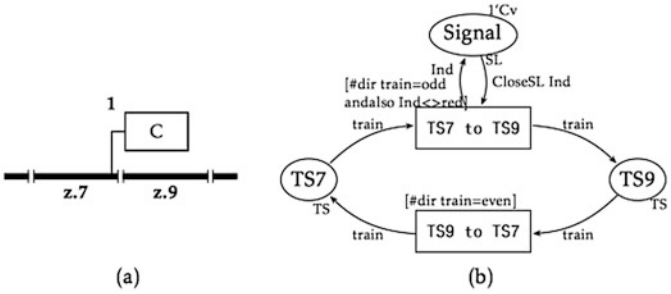


Fig. 7.12 A Petri net representation of signal light. (**a**) Signal light demo. (**b**) Corresponding CPN model

Signal Lights

Figure 7.12 shows a CPN model of a signal light component. Normally, a signal light can only be in charge of one direction of the transit. In Fig 7.12a, the movement from TS7 to TS9 is controlled by signal light. So, in Fig. 7.12b, signal place is only connected to the transition "TS7 to TS9." This transition is only enabled when the token (indicator color) of signal place is not "red." After a train passes the signal light (firing the transition), the signal light is switched off by setting the indicator to red. The operator "<>" in the guard function means "not equate to ($\neq$)."

Automatic Unlock Devices

In the French system, there is a ground-based automatic mechanism that could unlock the interlocked formation by the action of train passage (Rétiveau 1987). This mechanism is used for a flexible transit, and it is called the "DA" mode. This DA mode is fully automatic and ground-based, so we treat it as a fixed installation, rather than part of the signaling operations. The conditions of establishing a DA mode interlocking route are:

- There is a pedal (see in Fig. 7.13a.) on the track segment.
- The direction of the interlocking route is the same as the direction of the pedal.

If a route is established in DA mode, when a train passes and activates the pedal, all the upstream tracks will be automatically unlocked. Based on the original model in Fig. 7.11, this type of mechanism is represented with two additional parallel transitions. Each DA sub-model unlocks a track segment that is stored in the fusion place (see in Fig. 7.13c).

In our research, a typical station from the French railway signalization book (Rétiveau 1987) is studied, shown in Fig. 7.14. It is only half of the station that contains 5 points, 6 effective signal lights, 12 track segments, and 13 complete interlocking routes. The detailed information about this case study can be found

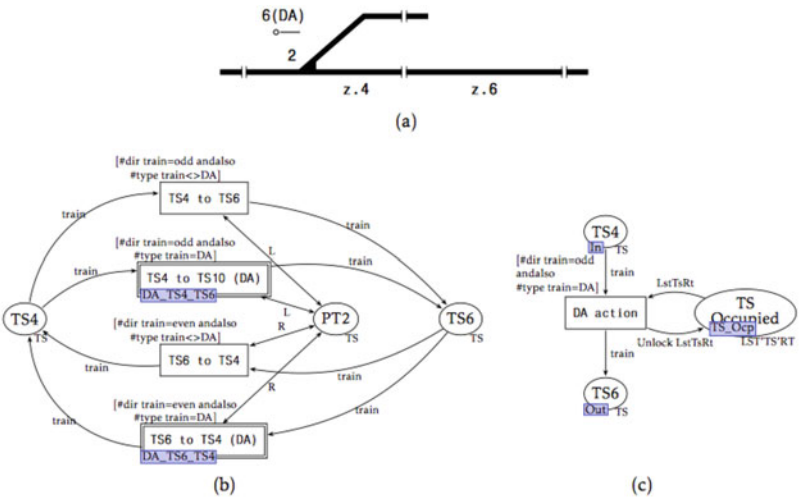


Fig. 7.13 A Petri net representation of "DA" mode. (**a**) DA mode. (**b**) Corresponding CPN model. (**c**) Sub-model of DS_TS4_TS6

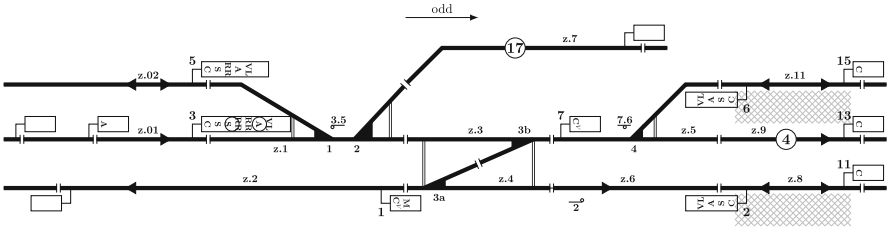


Fig. 7.14 Case study of a station layout

in Chapter 15 in (Rétiveau 1987). This case study example has been chosen as an academic benchmark by experts involved in the PERFECT project (Collart-Dutilleul et al. 2014; Sun et al. 2014).

The whole layout is represent by the CPN model in Fig. 7.15, using the basic components that have been discussed before. This layout allows all the train movements according to the interlocking routes.

Together with the signal operation parts in Sect. 4.3.1, the whole HCPN model is a complete RIS specification. 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 the train passes through. The whole model is too big and not necessary for a detailed demonstration in this section. However, all the other nets are modelled by the previous methodology.

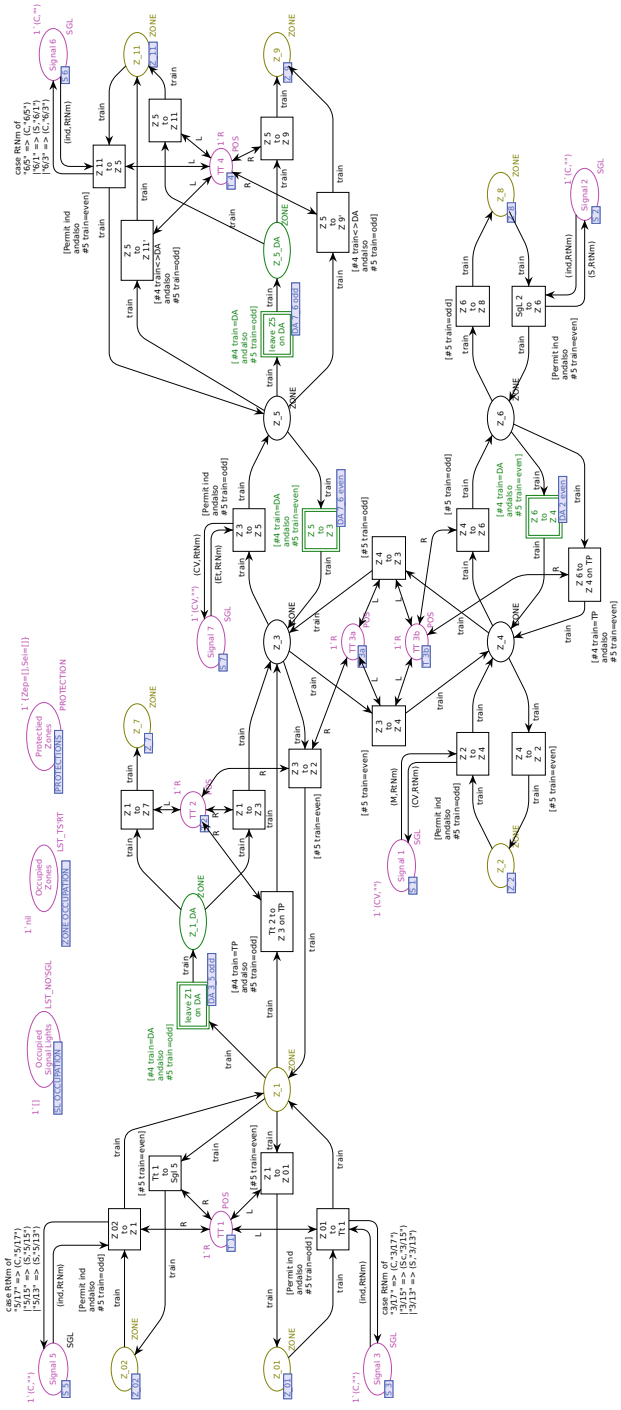


Fig. 7.15 The Petri net model of route layout

7.4.4 A Pattern of Railway Interlocking Modelling

An RIS has two main parts: the signaling operations and the fixed installations. In each station, signaling operations are localized instances of the national railway standards, which monitor and control the status of the fixed installations. It could be established via a hierarchical structure as we discussed in Sect. 4.3.1.

However, fixed installations consist of a series of track-side appliances, which are diverse in practice, as each station has its own rail route structure. Specification and evaluation of each station along a railway line is a repetitive and tedious job, and it has low efficiency and will probably introduce new errors from re-modelling processes. A feasible solution is to summarize all the common parts of the RIS and establish a parameterized model framework that can be applied to all stations. This study can be found in our previous work (Sun et al. 2015).

In this section, a generalization model pattern is presented, which is a reusable solution for the RIS with PIPC type. Models of different stations can be derived from this pattern without re-modelling, just changing the configurations in the pattern.

7.4.4.1 Generalization Concept

The stations that are equipped with the same type of RIS follow the same national rules. The only differences are the layouts of their fixed installations.

The expected structure should be both general and parameterized, which allows the specifications of stations to be derived from the same model with diverse configurations. That is to say, in this structure, the unmarked colored Petri net is a set of RIS functional rules, while the initial tokens are the concrete performance of stations. In such a model framework, the configurations (tokens) represent all the scenario information, based on the formation of the RIS layout and the "condition table" (or control table). When modelling a new station, the only job is to change the initial tokens on the expected structure.

To have this general structure, the railroad layouts cannot be performed by the physical location of places and connection of transitions. However, this information is indeed important for train movements, so all this diverse information must be represented in the token forms, ensuring the PN structure itself remains universal.

For a better understanding of the generalization concept, we use an incremental process and comparison examples to illustrate how to generalize the railroad structure.

Basis Track segments

Compared to Fig. 7.10, the new model in Fig. 7.16 has the same performance capabilities but in a parameterized form. A token in "train location" place indicates the train ID and its current location. Each time the transition occurs, the value of

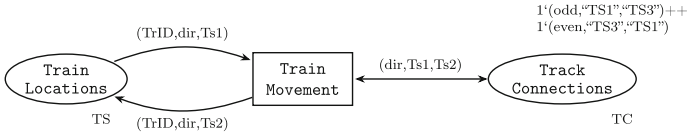


Fig. 7.16 Generalized representation of track segments

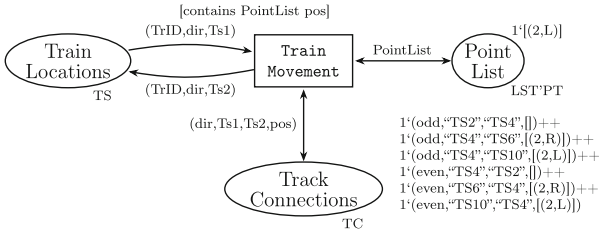


Fig. 7.17 Generalized representation including points

the train token will be refreshed according to the enabled binding elements. The “track connection” place is the constraint of train movement, which guides the train to move forward.

Adding Points

When we introduce the points into the generalized structure, it will first need a place to “store” all the point information, including point IDs and the positions. Meanwhile, the points will have an impact on the train movements, so the configuration of track connection should be modified. The new model in Fig. 7.17 is the corresponding model of the example in Fig. 7.11. The new color set of *TC* contains the point constraints. Only when the point stored in the point list place satisfies the point constraints, the train can move.

Adding Signal Lights

Similar to a point, a signal light is also the movement constraint. So the introduction of signal lights comes with a new place and a modification to the color set of *TC*. The new model in Fig. 7.18 is the corresponding model of the example in Fig. 7.19. The function *SL’Permit* checks the corresponding signal indicator. If the indicator is *red* (Cv in French), then it returns *false* to prevent train movement. Otherwise, it returns *true* to permit the transit. The function *SL’Close* switches off the corresponding signal lights after firing the transition.

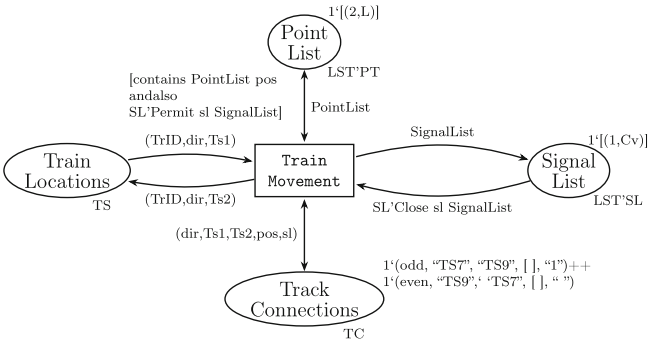


Fig. 7.18 Generalized representation including signal lights

From the above examples, we can conclude that the components of railroad and their combinations can be expressed by generalized structure, using constraint places and different transition conditions.

However, in a real practice, there are more constraints (appliances) and rules. First, we should list all the scenario-related elements and prepare their specification forms for the expected model.

In Table 7.2, train, track, point, and signal light are normal components that we have introduced in the previous parts. In this table, we give them several attributes to distinguish between each token. The *Track Connection* stores all the connection information between different tracks, considering the constraints of points, signal lights, and formation release triggers (the pedals). The *pedal* is the prerequisite condition for "DA" mode interlocking route. The "Destruct Auto" is the automatic unlock mechanism and its devices. It contains the related unlock conditions and the unlock actions.

With all these variables and their notations, the next step is to describe the movement of a train. Although the expected model does not have visible routes, we can determine train movement by token values. If the value of the train position changes, that means this train actually moves. Generally, there are two types of routing routes, DA and TP, in the French national context.[2] We also consider the route for shunting (OM), and the "staff responsible" mode (SR) for override operations. However, due to the space limitation, only DA mode will be discussed in this section.

The conditions for enabling DA movement are:

- There should be a pedal (passage detector for DA mode) in the current track.
- Points of the route must be proper positioned.
- Signal light (if any) in front of the train should be green.
- Train's movement authority allows it to move onto the next track.

[2]DA: Destruction automatique, TP: Tracé permanent.

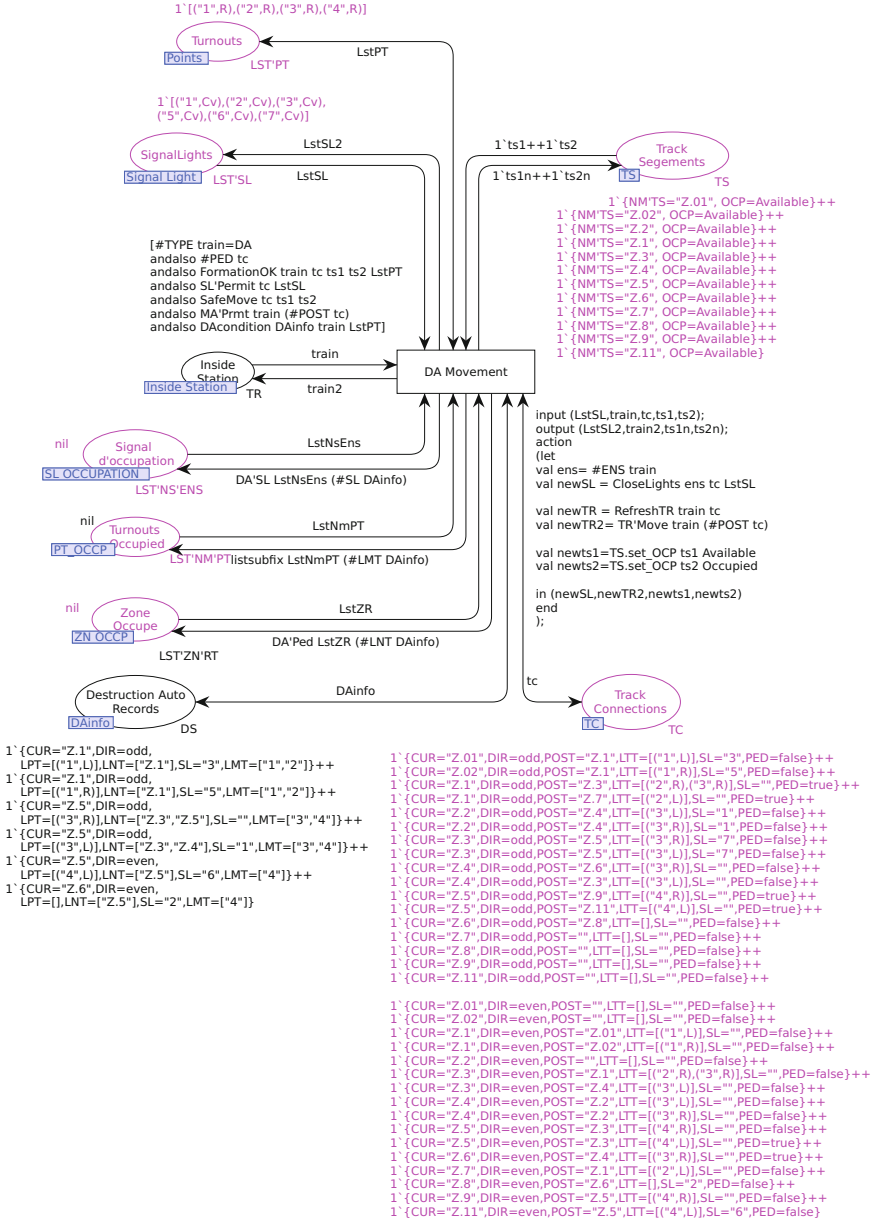


Fig. 7.19 Generalized Petri net model of "DA" route pattern

Table 7.2 Scenario-related elements in general structure

Element	Content	Notation
Train	Train name	NmTr
	Train direction	DirTr
	Route name	NmRt
	Route type (DA,TP,etc)	TpRt
	Train position	PosTr
	Movement authority	MA
Track	Track name	NmTs
	Occupation status	Ocp
Track connections	Current track	CurTs
	Connection direction	DirTs
	Post-track	PostTs
	Points (number varies [0,2]) (with name and its position)	PtTs
	Signal light name [0,1]	NmSl
	Indication of pedal	Ped
Point	Point list (contains name and its position)	LstPt
Signal light	Signal light list (contain name and its color)	LstSl
Destruct Auto	Exiting track (where DA takes place)	TsDa
	Effective direction of pedal	DirDa
	Tracks to be destructed	TsLstDa
	Signal light to release	SlDa
	Points to release	PtDa

The actions that release the formation of the route along with train movement:

- Release tracks of the route behind the train
- Release points of those tracks
- Switch off signal light (if any) after passing

For analysis purposes, we introduce a security guard function that constantly checks the occupation of the front track. The train's movement is safe provided that the front track is clear. Otherwise, if the front track is occupied, there will be a "face to face" or "face to tail" collision.

From what has been mentioned above, the more formal definition of the enabling rules of the DA movement is shown in Table 7.3. With the help of *CPN ML* language, all the conditions above can be embedded into one transition and can be combined into a single model to represent all the DA mode movements.

The study case of Fig. 7.15 is modelled by the generalization concept above. The complete CPN model provides a pattern that could be applied to all the relay-based computer-controlled RIS in the French national context. It can automatically arrange the routes for different trains, block the incompatible routes when a certain route is established, enable the route destruction function after a train passes, and support four types of route modes along with their mixed traffic operations. The

Table 7.3 Conditions and equations of "DA" movement

Condition	Equation
Route type	TpRt = DA
	Ped=TRUE
Route formation	PosTr = CurTs
	DirTr=DirTs
	PtTs ⊆ LstPt
Signal open	(NmSl,green) ⊆ LstSl
Movement authority	PostTs∈ MA
DA activated	TsDa = PosTr
	DirDa = DirTr
To release	TsLstDa
	SlDa
	PtDa
Security check	Ocp of CurTs = Occupied
	Ocp of PostTs = Clear

whole model is really large for a demonstration. Only one layer of the model and its results will be introduced. The other parts of the model are built by successive implementation.

Figure 7.19 shows the DA module of the general structure that includes all the necessary elements mentioned before: tokens of train, track segments, track connections, points, signals, and information of automatic destruction. Then, this transition is ordered by the conditions and fulfils the following actions. Train tokens are stored in an "Inside Station" place, with all the trains within this station. All tokens in this module do not really transit. They only "update" the data inside themselves.

Supposing we have the following initial parameters of simulation:

- Train demand route "3/15" : 1‘{ NmTr= "TER-0315" , DirTr= odd, NmRt= ("3" ,"15"), TpRt= DA, PosTr = "" , MA = []} ;
- List of all points: 1‘[("1" ,R),("2" ,R),("3" ,R),("4" ,R)];
- List of all signal lights: 1‘[("1" ,Cv), ("2" ,Cv), ("3" ,Cv), ("5" ,Cv), ("6" ,Cv), ("7" ,Cv)].

The simulation result of CPN tools is shown in Table 7.4. After the establishment of the route "3/15," related points change their position, and related track segments are blocked in memory. After switching on, signal lights change their indication and become blocked. After receiving an MA, the train can start with permission. As the train moves, its MA is gradually reduced and block components are released by the mechanism of automatic destruction. When MA equals zero, the train stops right away and triggers the route destruction. Finally, all the blocked components become free and the train exits the station.

Table 7.4 Result of route "3/15" simulation

Last action	Train token	Signal lights	Points Points	Tracks occupied	Signals occupied
Initial	Canton=Z.01 MA=()	(3,Cv) (7,Cv)	(1,R),(2,R) (3,R),(4,R)		
Route establish	Canton=Z.01, MA=()	(3,Cv) (7,Cv)	(1,L),(2,R) (3,R),(4,L)	Z.01, Z.1, Z.3, Z.5, Z.11	
Open signal lights	Canton=Z.01, MA=()	(3,VL) (7,Et)	(1,L), (2,R) (3,R),(4,L)	Z.01, Z.1, Z.3, Z.5, Z.11	3, 7
Generate MA	Canton=Z.01, MA=(Z.1,Z.3,Z.5,Z.11)	(3,VL) (7,Et)	(1,L), (2,R) (3,R),(4,L)	Z.01, Z.1, Z.3, Z.5, Z.11	3, 7
Z.01→ Z.1	Canton=Z.01, MA=(Z.3,Z.5,Z.11)	(3,Cv) (7,Et)	(1,L), (2,R) (3,R),(4,L)	Z.1, Z.3, Z.5, Z.11	3, 7
Z.1 → Z.3	Canton=Z.01, MA=(Z.5,Z.11)	(3,Cv) (7,Et)	(1,L), (2,R) (3,R),(4,L)	Z.3, Z.5, Z.11	7
Z.3→Z.5	Canton=Z.01, MA=(Z.11)	(3,Cv) (7,Cv)	(1,L), (2,R) (3,R),(4,L)	Z.5, Z.11	7
Z.5 →Z.11	Canton=Z.01, MA=()	(3,Cv) (7,Cv)	(1,L), (2,R) (3,R),(4,L)	Z.11	
Destruction		(3,Cv), (7,Cv)	(1,L), (2,R) (3,R),(4,L)		

Then we use the state space analysis function that is embedded in CPN tools to analyze the space state of this simulation. Its calculation result shows that this "single train" scenario has 26 states and 32 arcs. There is not any deadlock or live lock in the system. Then we perform another two simulations with 2 trains and 3 trains demanding for different interlocking routes. The sizes of the state space are 339 and 2025, and all the states are "safe."

7.4.5 An Event-Based Approach for Relay-Based Logic

In the previous two sections, we mainly focus on the high-level parts of the RIS. More precisely, we study and model the computer-controlled parts of the RIS. In this section, we analyze the low-level parts of RIS. That is the modelling methodology of the relay-based systems.

7.4.5.1 Background of Relay-Based Logic

All the controls and commands that come from the high-level part of RIS are implemented by a set of relays. They achieve the control procedures by changing their states. Most relays have two states, activated and deactivated, sometimes may be left and right. Because of different functional purposes, the relay circuit diagrams

can be divided into separate diagrams. For example, according to the book (Rétiveau 1987), the functional phases of the route establishment of the PRCI type have four stages:

- Route formation: receiving the route command from the dispatcher, and setting point to the right position by point machines.
- Formation verification for interlocking: verifying the positions of the points relay. If all the relays are properly positioned, the formation will be interlocked.
- Route verification: verifying the real point positions; if they are well positioned, then send a command to signal light control logic.
- Signal light control: switching on the lights and displaying different colors depending on the interlocking route itself.

For a better understanding, we create a small scenario with only one point. This example is designed on the basis of the control logic and the circuit diagram in Fig. 15.23, Fig. 15.27, Fig. 15.29, Fig. 15.39, Fig. 15.40, Fig. 15.46 in Rétiveau (1987), and it is shown in Fig 7.20. The example contains the main components for route establishment. It is realized by a set of relays and switches that are located

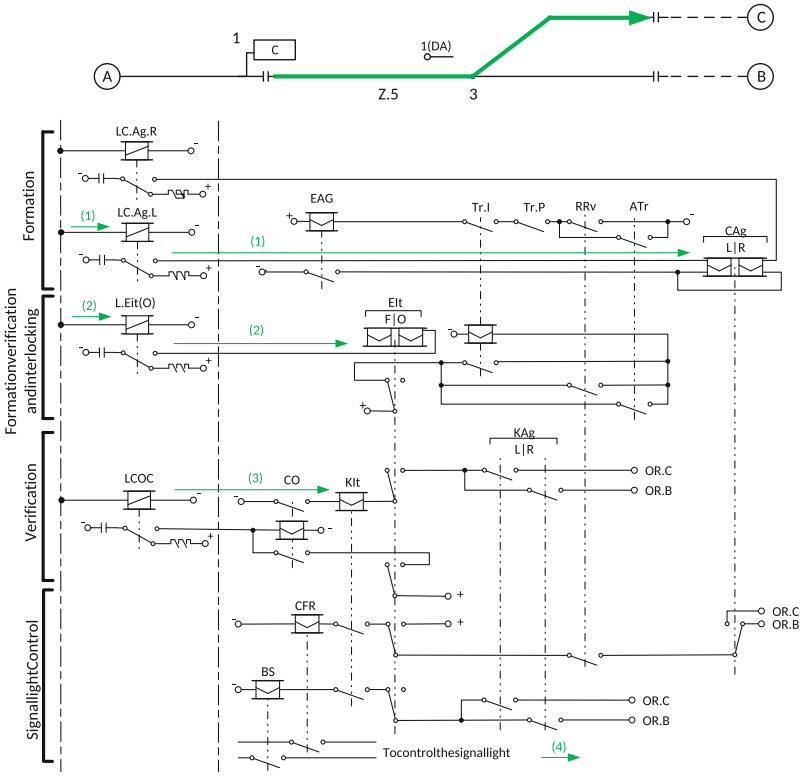


Fig. 7.20 An example of PRCI type system of a single point

in different layers (circuits diagram). However, as shown in Fig. 7.20, the dash-dotted line connected elements, in nature, are the same element. They are physically connected together, changing their states at the same time, but located in different circuits. The established procedures of this example are explained as follows:

- After receiving the formation command (*LC.Ag.L* => left or *LC.Ag.L* => right), the control relay *CAG* is going to change for the preparation of the route.
- After the point is well positioned, interlocking command *L.EIt(O)* is sent to interlock the enable relay *EAG* by locking its transit with *Tr.I* or *Tr.P*.
- When command *LCOC* is received, if the point is in the right position and well-locked, a further command will be sent to control the signal light.
- Switching on the signal light according to the relays *CFR* and *BS*.

From Fig. 7.20 and its procedures, we know that relays can be activated or deactivated in different layers by commands from the signaling center, occupation changes of the track segments, or the internal relay state changes. Moreover, each switches affiliated with these relays will be changed at the same time. Consequently, once a relay changes its values, all the related circuits will be refreshed simultaneously. However, this kind of concurrence is quite different from the rules in CPN. It has brought some problems in our early attempts. Nonetheless, all these problems are caused by the HCPN models that consist of several subnets. If all the logic connections are modelled in a single net, we can combine all the linked elements into one element (place), and there will be no further problem of concurrence. But, in that way, we will obviously lose the readability of the model and lose the description of the system's structure. So all the following problems, discussions, and their solutions are based on the model with multiple nets.

The following part begins with two simple examples to illustrate the problems. Then, we apply the event-driven concept to solve these problems.

Modelling Problem I: Synchronous Firing

In the envisioned model with the hierarchical structure, relays and switches are located in different nets. So if a relay changes its state, the related transitions cannot fire at the same time. As the states of the relays are closely coupled to each other, the dissynchronization of firing transitions fails to refresh the system simultaneously, and it may lead the system to uncertain states, such as standstill, livelock, deadlock, or even an unreasonable state. Such an example can be found in Fig. 7.21.

This example describes two logical processes that are controlled by relay A and relay C. Processes are placed in different nets, and each one has two transitions. Assuming the initial state is $S_{init} = [m, n|A, B, C] = [1, 1|1, 1, 1]$, the expected firing sequence is: $T_{1n}, T_{1m} \longrightarrow T_{2m}, T_{2n}$, and the expected final state is $S_{init} = [3, 3|1, 0, 1]$. But if the transition T_{2n} fires before T_{1m}, the result state is $[m, n|A, B, C] = [1, 3|1, 0, 1]$. This state does not exist in a real system, and it may cause unknown problems. This issue demands a transition management mechanism that could organize all the marking-enabled transitions to be fired in the right orders,

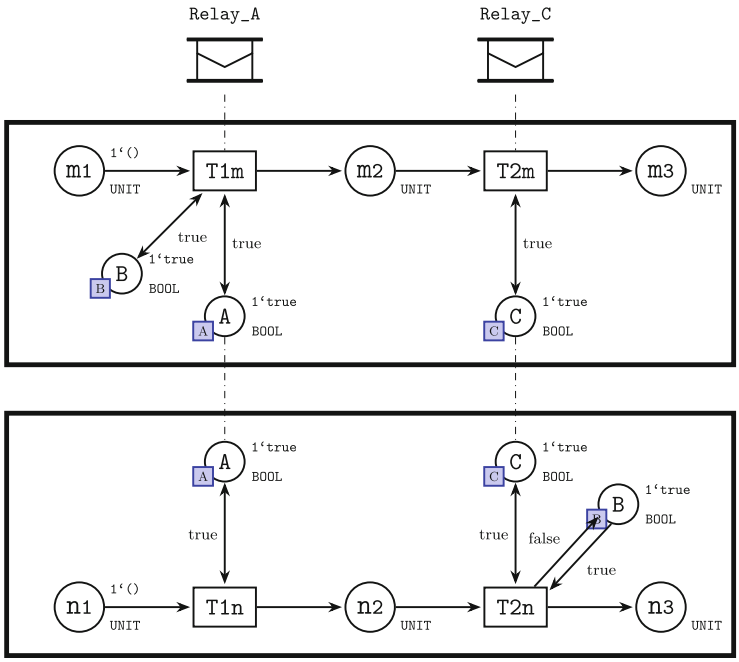


Fig. 7.21 Modelling problem I: synchronous firing

as they do in the real system. Moreover, considering the compatibility, the proposed solution should be achieved under the framework of CPN.

Modelling Problem II: Firing Conditions

Generally, a relay's status is controlled by several circuit elements, including electrical sources and switches. These elements can be considered as constant variables. If a relay is controlled by such constant variables, no matter the order, when all the elements meet the required conditions, the relay is activated. However, there is another "temporary" type of conditions. They are pulse signals that are a kind of instant variables. A relay connected to such pulse signals will only be activated at the "pulse" moment. For such a relay, we need to pay more attention to its activating condition order. The example is shown in Fig. 7.22a.

The *Cmd*_E is a command from signaling control and the *SW_F* is a controlled switch. Their states affect the value of *Relay_G*. If we have a corresponding model, as shown in Fig. 7.22b, we will encounter the unreasonable firing sequence: $E = true \rightarrow F = true \rightarrow t1$. In order to solve this problem, a reset mechanism (non-timed CPN approach) can be applied or time concept (timed CPN approach) can be introduced. Considering that an RIS is more like a continuous sequence event

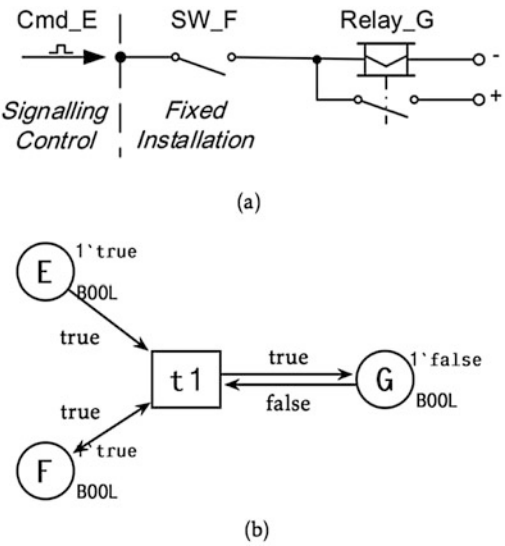


Fig. 7.22 Modelling problem II: firing conditions. (**a**) Example of different conditions. (**b**) Corresponding model

system, it is not necessary to add time factors into our models. The rest solution would be a new mechanism to differentiate two kinds of condition types with good readability.

7.4.5.2 Event-Driven Concept

In relay-based systems, every circuit state change is driven by an event, such as external commands or internal switch actions. Such a mechanism reminds us of a special PN—the controlled Petri net (CtlPN). It is a class of Petri nets with external enabling conditions called control places that allow an external controller to influence the progression of tokens in the net (Holloway and Krogh 1994; Holloway et al. 1997). Figure 7.23 illustrates a controlled Petri net, where the squares (*c1, c2, c3*) indicate the external control place.

As with the ordinary Petri nets, the state of a CtlPN is given by its marking, which is the distribution of tokens in places. A controlled transition can only be fired when this transition is marking-enabled and the connected control places are "TRUE."

Inspired by this occurrence rule, we design a similar mechanism to solve our previous problems under the framework of CPN without breaking any existing rules of CPN. This mechanism is achieved by introducing event-based enabling rules and an *event place* into ordinary CPN models. An event-driven model is a class of Petri nets with event conditions stored in the event place (fusion type place), which makes the connected transitions event-driven, in order to allow internal/external event to influence the progression of tokens. The event place contains an FIFO list that stores all the events in progress in their order of occurrence. This FIFO list has the following properties:

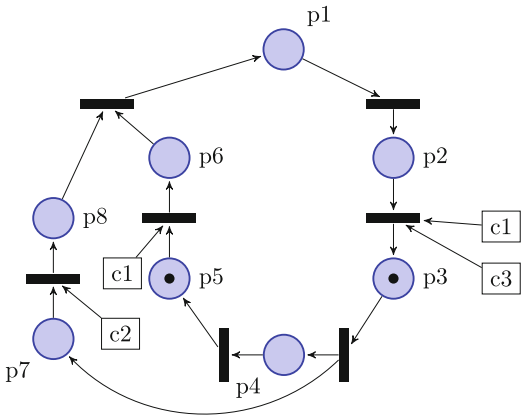


Fig. 7.23 An example of controlled Petri net

- Only the head (first element) of the list is referred as the current *activated* event and *tt* will activate its corresponding transitions.
- The tail (exception of the first element) of the list is considered as *deactivated* until the head of the list is removed. The new head will become activated.
- New events that are induced by internal actions are stored at the end of the list.
- Only when the system has no more events in this list, this system can accept an external command.

As in the Petri net literature, it is commonly assumed that only one transition can be fired at a given instant. So, parallel actions become "choices." If one transition introduces new internal events (relay status changes) before the last event is complete, the system status will appear confusing. However, with the help of event places, we can achieve a loose synchronization of firing the transitions. It continues firing all the enabled transitions related to the first event until there are no more enabled transitions. Then an event management function (transition) will be enabled. It removes the "useless" event (the first event), then moves on to the next event, and makes it the new head of the list. In this way, the whole system is gradually progressing forward, event by event, in order to imitate a synchronization system.

The expected event-driven model has 4 transition priorities: $P_{Event} > P_{Clear} > P_{normal} > P_{External}$.

P_{Event} belongs to the event-related transitions that are directly connected to event place.

P_{normal} belongs to the set of transitions that are not directly connected to event place.

P_{Clear} belongs to an event remove mechanism that will remove the "useless" event from the FIFO list if this event cannot fire any transitions.

$P_{External}$ belongs to external inputs for scenario analysis and state space calculation purposes.

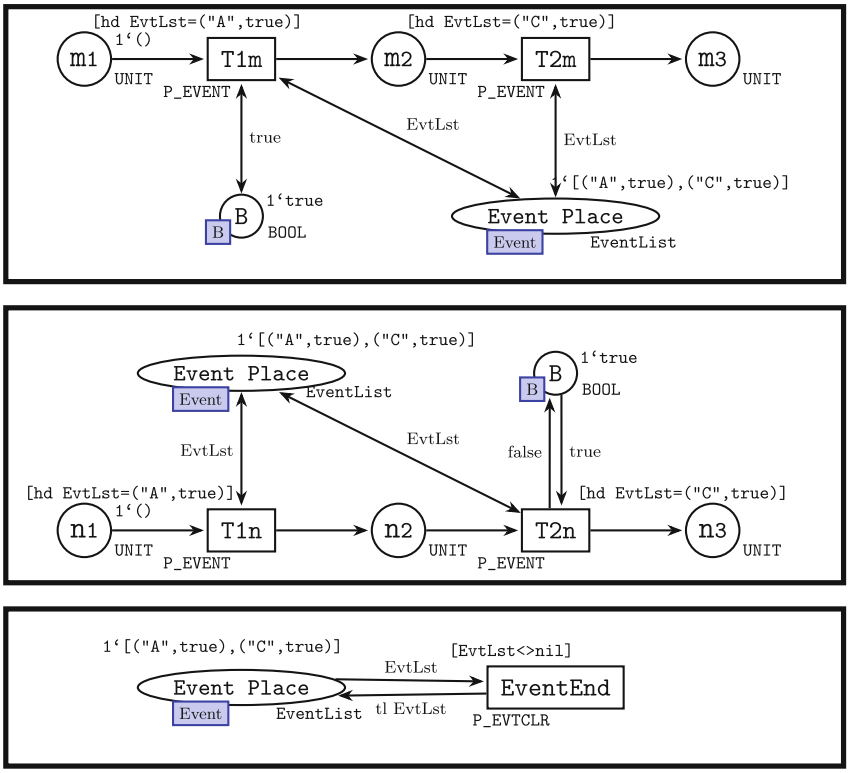


Fig. 7.24 Event-driven colored Petri net model of Fig. 7.21

Now, we can rebuild the example in modelling problem I: “the synchronous firing” with the event-driven concept. In Fig. 7.24, the color set of events is defined as *colset Event= STRINGxBOOL*. It contains the name of the event and its value, for example (“A,” true) means relay “A” is activated and (“B,” false) means relay “B” is inactivated. All the transitions are connected to an “Event Place” that stores the events to be triggered in their order of occurrence. Its color set is *colset EvntList= list Event*. The token in this place is in the form of *list* type. The head of the list (*hd* list, in meta language grammar, is to abstract the first element from the list) represents the event that is currently taking place in the system. The guard function checks the first element of the event list (*hd EvtLst*) and determines whether the transition is event-enabled or not. Any event-enabled transition has the ability to fire, and it can fire if it is also marking-enabled. Moreover, if a transition brings in a new event, then this new event will be stored at the end of the event list in “Event place,” and it can be triggered in later progress. After all the enabled high-priority transitions are fired, the transition with low priority is enabled. It will remove the current activated event from the list (*tl EvtLst* returns a new list with exception of the first element) and the second event becomes activated.

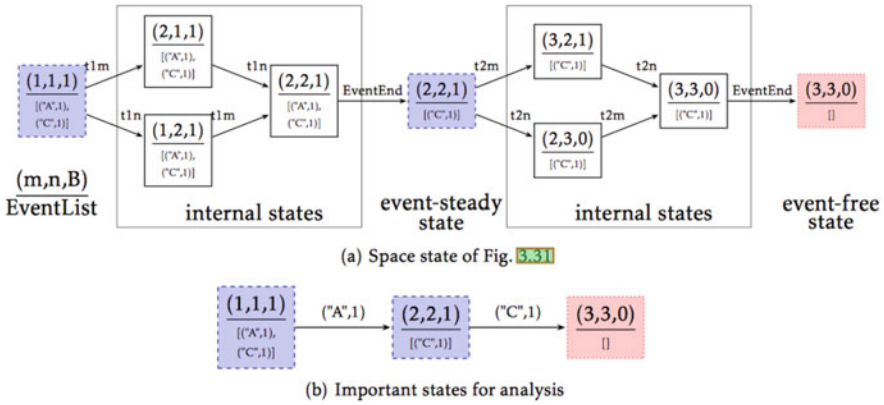


Fig. 7.25 Simplification rules of system space state. (**a**) Space state of Fig. 3.26. (**b**) Important states of analysis

The state space of this model is shown in Fig. 7.25. For a concise indication, in this state space graph, the system state is represented by the marking of the vector (m, n, B). Here, m is a mapping from markings of $(m1, m2, m3)$, and $m \rightarrow \{0, 1, 2\}$ represents the markings of $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Similarly, $n : (n1, n2, n3) \rightarrow \{0, 1, 2\}$. B indicates the marking in "B place " and 1/0 is used to represent "true/false." The inscriptions under the vector are the content of the FIFO event list. The label on the arcs between two states is the fired transition. The initial state of the system is $(m, n, B) = (1, 1, 1)$, $EventList = [("A", 1)("C", 1)]$. Each time the transition EventEnd is fired, an event will be removed from the event list.

The state in blue is called "event-steady" state. This means that a previous event is finished and begins to activate a new event. The state in red is an "event free" state. This means there are no more events and the system state is preserved until there is an external input event. The state in white is the internal state, or instantaneous state. Between two successive system-steady states, there may be more than one path, and the number of combinations of the path depends on the number of parallel transitions, which could result in a large number of system states. But no matter how the state changes, it will eventually be stabilized and finally reach the next steady state.

When we analyze this space state graph, we will find that not every state has equal importance. The event-steady and event-free states are more concise to describe the safety reachability of a system. Hence, an abstraction method to minimize the size of the system state will be demonstrated in Fig. 7.25b. From the perspective of analysis, the internal states are not useful because they have less value than the steady ones. Each internal state is a tiny change inside the fixed installations, only when the system finishes all the changes in a space state path, which means a complete response to the external input. While, from the modelling point of view, all the states and changes between two steady states should not exist in the real system,

because they are parallel at the same time, as in the modelling result, these states can be considered as transient states.

Therefore, the original state space in Fig. 7.25a can evolve into a quite simple one in Fig. 7.25b. The new state space has an initial state (1, 1, 1) and two external input events [("A", 1) , ("C", 1)] , and each event allows the system to advance into a new state. This method will effectively reduce the state space complexity caused by the relay-based components that act simultaneously in different layers.

Also the modelling problem II: the "firing condition" can be solved by the event-driven model in Fig. 7.26. The original pulse signal Cmd_E was replaced by a single event in the "Event Place," in order to achieve a similar instantaneous effect. From the simulation scenarios and results on the right side, it is clear that this model will fire transition "t1" only in the right action sequence "F=true → E=true → t1 fire."

From the above examples, we can have a general idea of an even-driven transition. It relies on both the condition places and the event place. However, in real systems, condition changes may call a new event. Moreover, an action could be either new condition change or new event. So the property (event, condition, action) of different system processes should be clearly defined. All the possible types we may use in fixed installations are summarized in Table 7.5.

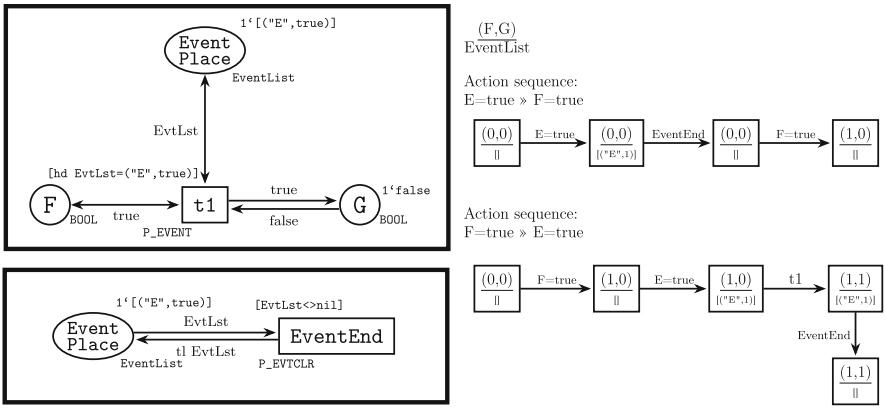


Fig. 7.26 Event-driven colored Petri net model of Fig. 7.22

Table 7.5 Type of logical variables ant its properties

Type	Description	Event	Condition	Action
Control	The status of relay (or switch)	X	X	
Command	The output command of relay	X		X
Indicator	Internal variable	X	X	X
Message	Command send by controlling center	X		
Action	Command or data send back to controlling center			X

7.4.5.3 System Validation of Event-Based Model

The final aim is to verify whether the system specification will hold the safety properties. Standard model checking algorithms are based on an exhaustive visit to all the reachable states of the specification. In our study, we chose CPN tools that integrate a powerful state space tool. It could generate the full state space of the PNs mode, and it could analyze the state space by means of a CTL-like temporal logic that allows user-defined searches and queries.

Model checking relies on the simulation environment. It determines which scenarios are going to be simulated and how each of the scenarios will be simulated. In each case study, we consider the original system to be a multi-input multi-output module. To be able to check its entire property, a test layer is added to provide external input events and variables and allows them to vary freely. In the system priority aspect, the test layer has the lowest priority. The test layer can give a new external input, but only when the original system reaches a new steady state. This assumption is also consistent with real practice, where RIS is a relay-based computer-controlled system. It has a faster processing cycle than its external inputs, such as human instruction or train movements. So it is reasonable to have a test layer with the lowest priority to simulate external input.

Safety performance of the system specification is "Safety property holds in every reachable state" or "danger case never happens." During the state exploring, if we meet an unsafe state, there is no need to exploit its successive states, because all post-states are potentially unsafe. With this selective exploring method, we can reduce the state space without loss of reliability of safety analysis. So, before starting the state space calculation, we use the safety properties to specify that, under certain circumstances (system not safe), the CPN tools do not need to calculate all the successors of a state.

Normally, after a state exploring, we will get a large number of states and their marking information. A lot of them are internal states caused by subsystems. From the perspective of the safety analysis, we are more interested in a concise state space and system counterexamples. So, we make our own queries (ML functions) to search for all the "event-steady" states and the unsafe states, to generate an event-based state space tree, and to list the event paths of all the counterexamples.

System Modelling

To illustrate a complete practical use, a model of RIS in Fig. 7.20 will be demonstrated. This case study is very simple in that it only contains one point and two interlocking routes. The signaling operations in this model are to send commands to establish or destroy an interlocking route. A reasonable modelling structure and its simulation environment are shown in Fig. 7.27.

It should be noted that in order to better illustrate the analysis capabilities, we need an imperfect system model. So, when modelling the signal system, we

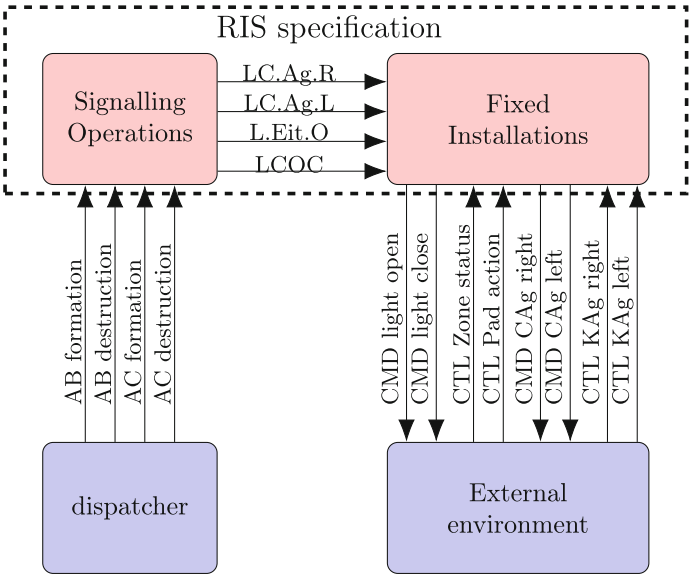


Fig. 7.27 Modelling structure and simulation environment

deliberately ignore a condition that is "System needs to wait 150ms, before sending command to switch on the signal light." Then, we get a potentially unsafe system.

The first part of the RIS model is the signaling operations as we discussed in Sect. 4.3.1. There is a simplified version of it in Fig. 7.28a, which contains different route phases (unformed, permitted, formed, etc.) and the corresponding transitions. Figure 7.28b is also a simplified version of route formation. As the signaling operations have been discussed before, considering the space restrictions, other sub-models of signaling operations are not shown here. The events in this model are defined in the form of (*Event type, Event name, value*), for example, the event to form the route "AB" is (*MSG, "AB " , form*). The event-trigger function is *fun* $EV : Eventlist * Event_x - > BOOL$. It is the guard function of event-related transitions and will return true if the $Event_x$ is at the top of the $Eventlist$.

The point control (in Fig. 7.29) contains two parts: 1. The point layer that could change the point's logical position by route command, interlock, or release point by shared resources and send commands to the point machine to change the rail connection (as shown in dashed line). 2. The transition layer is the necessary condition of route formation in flexible transition mode of the French context. The function "*gEV* " is a multi-event condition for transitions, which means any of the following events will enable this transition.

The final RIS layer is the signal light control (in Fig. 7.30) that could switch on signal lights if a route is established and the front zone is unoccupied. If the route is destroyed or if the front zone is occupied or if the point machine is not well positioned, then the light is switched off.

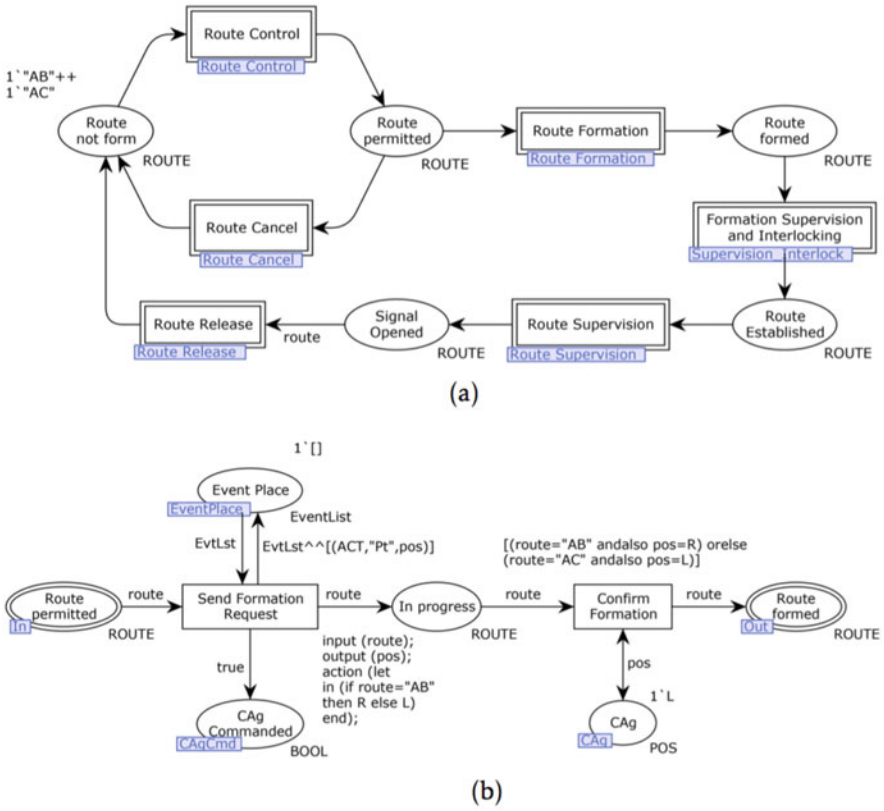


Fig. 7.28 Colored Petri net model of signaling operations. (**a**) Colored Petri net model of signaling operations layer. (**b**) Colored Petri net model of route formation

For model checking purposes, we need to add a test layer to simulate all the external input events in Fig. 7.27, and allow those events to vary freely. In this mode, the considered external inputs are route command (formation/destruction), zone occupation, pedal action, and point machine status *KAg*. (If a point is positioned to the right side, then relay *KAgR=true* else *KAgR=false*.) The outputs are signal light status and point machine command *CAg*. The model of simulation environment is shown in Fig. 7.31.

State Space Analysis

The safety statements of this system are:

φ_1: If any route is formed or zone is occupied, the relay CAg that controls the point cannot change.

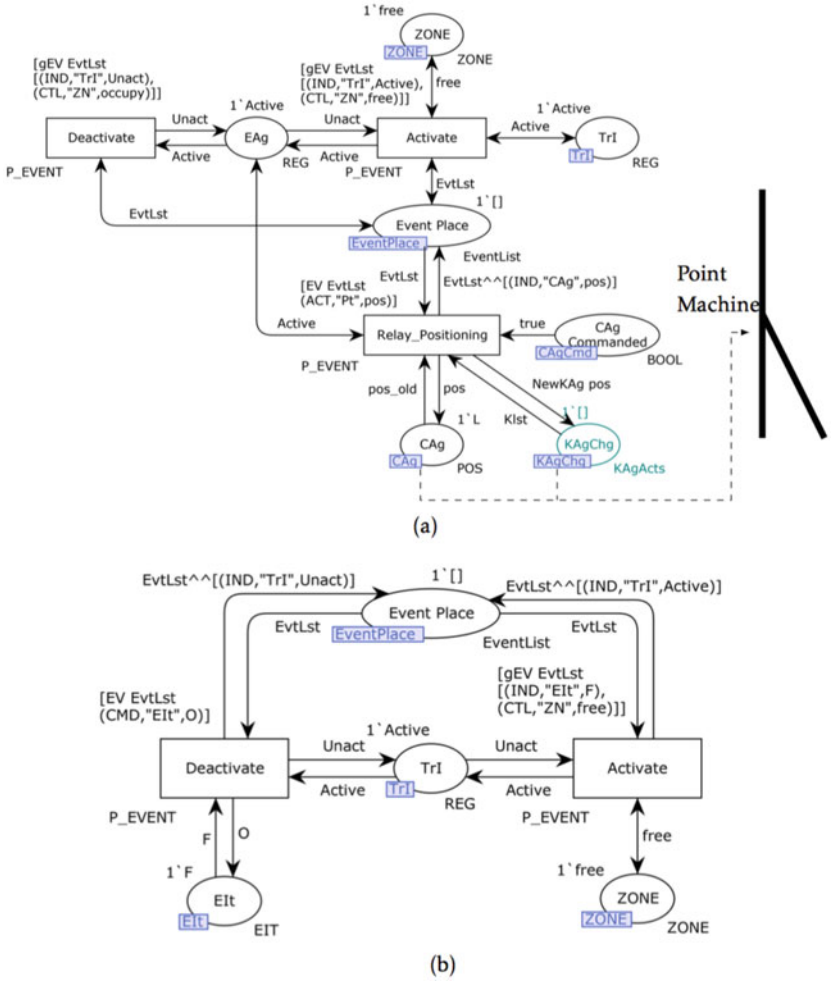


Fig. 7.29 Colored Petri net model of point control. (**a**) Colored Petri net of point layer. (**b**) Colored Petri net of transit layer

φ_2: If no route is formed or zone is occupied, signal light cannot be switched on.
φ_3: If the zone is occupied, the point machine must not act.

The selective branching option for exploiting the state space is designed as $\varphi_1(S) \wedge \varphi_2(S) \wedge \varphi_3(S) \rightarrow BOOL$, if the function returns *false* the state S will be a terminal state. With the result, we can start queries to examine if the state space will break any safety statements. The simulation result is shown in the second column of Table 7.6.

Although the size of the system state space has been simplified, it is still not readable. Moreover, too much information on CPN marking makes it difficult for

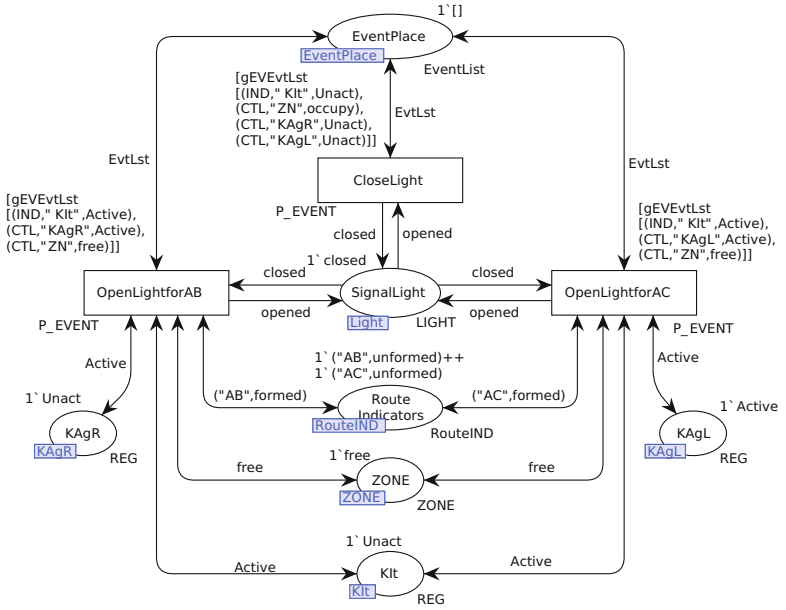


Fig. 7.30 Colored Petri net model of signal light control

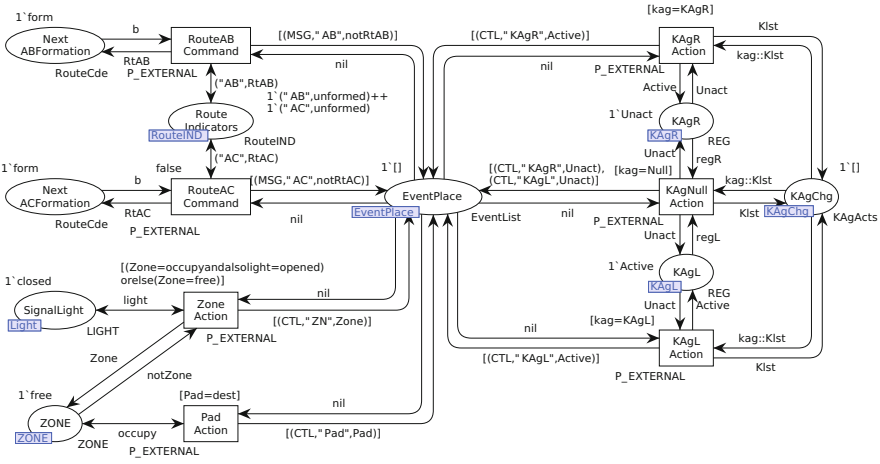


Fig. 7.31 Colored Petri net model of test layer

humans to compare each state. So another query is needed to transform the original state space into a more compatible form. Only event-free states and unsafe states will appear in the new state space. The original paths between each new state will be replaced by an external input event. So the new state space is an event-state graph, where each input event leads the system to a new state. Each of the new states

Table 7.6 State space calculation result

Exploring type	Default	Selective	Vectorization
State space size	366	301	76
Statement φ_1	Holds	Holds	Holds
Statement φ_2	Holds	Holds	Holds
Statement φ_3	Not holds (48 states)	Not holds (48 states)	Not holds (48 states)

is represented by a vector, $S_i = [A, B, C, D, E/F, G]$, each variable represents either a layer status or a relay value, and here, S_i.= *[Route progress, CAg, EAg, Tri, light / Zone, KAgR]*. The new state space graph has a total number of 76 states, where 29 are duplicates and 6 are danger states (third column of Table 7.6). Part of the graph is shown in Fig. 7.32, where the node in grey dashed style is the state already visited (duplicates) and the red node is the danger state.

The counterexamples of the verification are generated by giving the paths from initial state to each danger state. There are six paths in this example:

- Init → rAB=1 → LcAgR=1 → L.Eit=1 → L.Kit=1 → KAgL=0 → rAB=0 → KAgR=1 → rAB=1 → LcAgR=1 → L.Eit=1 → L.Kit=1 → Zon=0 → KAgR=0
- . . . → L.Kit=1 → Zon=0 → rAB=0 → KAgR=0
- . . . L.Kit=1 → Zon=0 → Pad=1 → KAgR=0
- . . . → L.Kit=1 → Zon=0 → Zon=1 → Zon=0 →KAgR=0
- . . . → L.Kit=1 → Zon=0 → Zon=1 → Zon=0 → rAB=0 → KAgR=0
- . . . → L.Kit=1 → Zon=0 → Zon=1 → Zon=0 → Pad=1 → KAgR=0.

All of the counterexamples violate the statement φ_3. The reason for this danger situation is that when a new command is sent from RIS to point machine, its feedback *KAg* will take some time. If the RIS does not wait for new *KAg* data and continue to perform subsequent processing programs, then the old *KAg* data may lead the RIS to switch on the signal light and allow the train to enter while the point machine is going to change the point's position. So we get a dangerous state. The point position is changing, but there is a train in this zone and this will probably cause derailment.

System Specification Improvement

The solution to this fault is to add a time constraint to the RIS route establishing process. When the logical position of point *CAg* is changed and the front light is not yet switched on, the RIS waits for a moment, which is longer than the operation cycle of a point machine, thereby ensuring that all the actions of the point machine will be accomplished before the light switches on.

After we applied this new constraint to the model and analyzed its safety property, it turns out that the new system holds all the safety statements for every state. The new model has 259 original states in CPN tools' state space calculation,

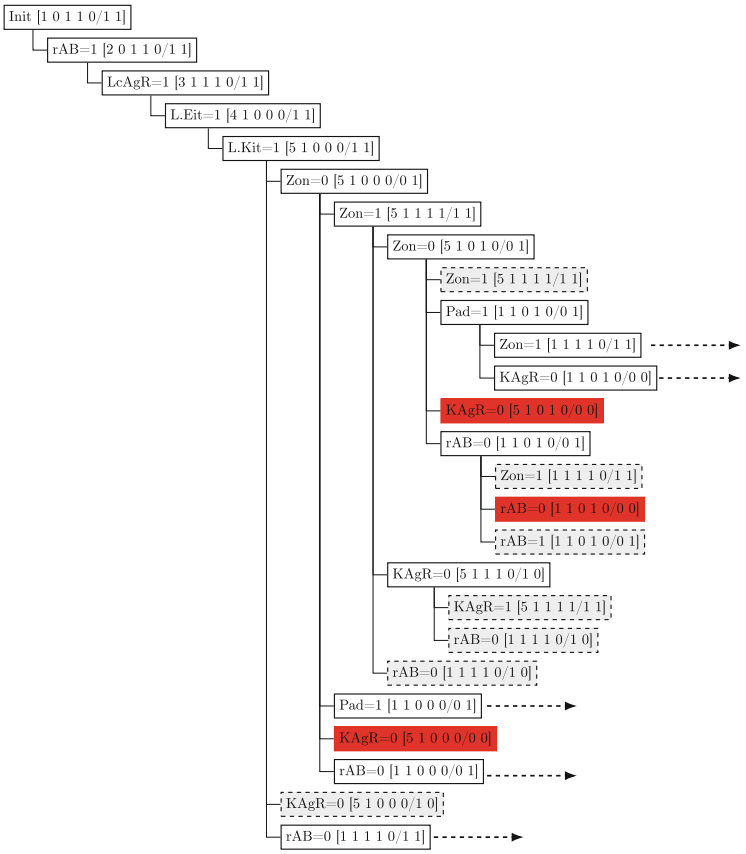


Fig. 7.32 Part of the state space tree

while after state abstraction, it has 65 states where 25 are duplicates, no danger state and no counterexample.

7.5 Conclusion and Perspectives

7.5.1 Conclusion

This chapter has been devoted to the model-based system engineering for safety of railway interlocking system. It provides a new approach via formal languages that aims to aid designers in effectively ensuring railway safety and improving the quality with system design and verification in railway industry. The study has focused on the formal modelling of French railway interlocking system. The nature

and its formal specifications of RIS have been studied. A hierarchical modelling framework is proposed via CPN to specify and verify properties and behaviors of the RISs. The work has been presented as follows.

Due to various reasons, the knowledge of railway is partly written in textual documents and partly unwritten while owned by engineers. So in the system design or development process, we always need the assistance and supervision of expert engineers who have got both the written and unwritten knowledge. Initially, a quick comparison of GRAFCET and CPN is given, which illustrates their similarity and the ability to be seamlessly converted. So CPN has been chosen as our formal specification language. Its hierarchy and color features make it possible to propose a generic and compact structure that contains all high-level functions of RIS. At the same time, PN's rigorous semantics allow us to implement formal proofs.

The RIS is one of the crucial parts of the railway transit safety. In the French railway domain, the computer-controlled relay-based RIS (PRCI type) is the dominant practice. Its complex sequences and consequent actions make it difficult to be verified and validated. For such systems, first we analysis the architecture of RIS and the hierarchical structure of modelling framework. After that, we introduce an intuitive modelling approach that could formally specify the constructions of the fixed installations and the signaling operations of the interlocking logic. As a multi-input multi-output system, the signaling part of RIS is suitable to be modelled in a vertical decomposition way. It should contain different aspects, including components, scenarios, and functions. The fixed installation part is represented by logical objects connected to each other in the form of the track layout. It is natural for us to model it in a geographic way. However, in practice, each station or yard in a single line has its own RIS, which respects the same national standards but has different facility layouts. Normally, to specify all the stations, we have to rebuild models. It has low efficiency and will probably introduce new errors during the rebuilding process. With the modelling power of CPN, a general solution is proposed by introducing a modelling pattern, which could be easily adapted to different stations with PRCI type RIS. It is a general solution in a parameterized form. The "place/transition" structure (unmarked CPN model) represents a set of RIS functional rules. The logical formation of railway layout (configuration) is represented by the information contained in tokens. Besides, models that are less compact can be derived from this generic one in order to validate various aspects while keeping the safety property. Finally, we analysis the low-level part of the RIS that is the relay-based logic circuits. The relay-based circuit components have the nature of concurrency. An event-based concept is introduced to better describe these internal interactions. All the relay-based transitions (actions) are supervised by an "event place," and different transition priorities realize their relative synchronization. Furthermore, this event-based model is compatible with the classic CPN.

7.5.2 Perspectives

7.5.2.1 Transformation from CPN to *B machine*

Since the formalism of Petri nets has the advantage of communicating and their models could be validated by some engineering experts, it is still a long distance from the final implementation. To bridge the gap between the specifications and the implementations, we carry out another study—a model transformation from colored Petri net to ***B*** language, which could help people to quickly shift from a valid design solution to a valid input of ***B*** development process in the design phase. Detailed references can be found in Bon and Collart-Dutilleul (2013), Sun et al. (2015), Sun (2015).

The ***B*** method can offer a formal software development. In the French railway context, the ***B*** method is industry recognized tool and already has some success implementations, such as Météor (Behm et al. 1999), the new metro line number 14 in Paris. These successful engineering stories convince people of the reliability of the ***B*** method because the final implementation code generated from abstract ***B*** machine is considered safe and is proved to be safe. So in the French railway context, ***B*** proved model is accepted as a strong safety proof (Boulanger 2013a,b).

In our study, after mapping colored Petri nets (CPNs) formalism into ***B*** language formalism, the transformed ***B*** machines will be the input of the ***B*** development process and could be automatically refined into the implementable codes. Moreover, considering the limitations of model checking, sometimes we want to apply a theorem-proving for the purpose of verification. As the ***B*** proved models are considered "safe" in French industry, the transformation from Petri net to ***B*** machine is needed by any means necessary.

In the transformation framework, we maintain the mechanism of multi-set behaviors, and the transformed machines can be automatically proved by Atelier ***B*** tool. Besides, we propose some mapping rules for different color sets, in favor of raising the compatibility.

Furthermore, the concept of hierarchy is integrated into the mapping process. A multi-system that is modelled in a hierarchical way can be translated into a set of abstract B machines. The hierarchy is expressed by the composition relations of the machines and the accessible operations. Then, the concept of prioritized transition is introduced into the transformation. It is achieved by giving each operation a priority and adding an operation to the machine for priority management. It maintains the same priority mechanism of as in Petri nets.

7.5.2.2 Transformation from UML to CPN

Nowadays, UML is considered to be the standardized language for object-oriented modelling and analysis. However, UML cannot be used for automatic analyses and simulation. In Kerkouche et al. (2010), they propose an approach for transforming

UML state chart and collaboration diagrams to colored Petri net models. It produces highly structured, graphical, and rigorously analyzable models that facilitate early detection of errors such as deadlock and livelock. This transformation helps to bridge the gap between informal notation (UML diagrams) and more formal notation (colored Petri net models) for analysis purposes.

All the model transformations above along with the formal modelling of RIS aim to contribute toward a global safe analysis framework.

References

Antoni, M. (2009a). Formal validation method and tools for French computerized railway interlocking systems. *International Journal of Railway, 2*(3), 99–106.

Antoni, M. (2009b). Formal validation method for computerized railway interlocking systems. In *International Conference on Computers Industrial Engineering, CIE 2009*, pp. 1532–1541.

Antoni, M. (2009c). Validation d'automatismes ferroviaires de sécurité à base de réseaux de Petri. Ph.D. thesis. Braunschweig, Allemagne: Technischen Universität Carolo-Wilhelmina zu Braunschweig.

Antoni, M. (2012a). Formal validation method and tools for computerized interlocking system. In *FM Industry Day*, pp. 1–44.

Antoni, M. (2012b). Méthode de validation formelle d'un poste d'aiguillage informatique. *Recherche Transports Sécurité, 28*(2), 101–118.

Antoni, M., & Ammad, N. (2007). Feasibility study for the implementation of a formal proof of interpretable specification (for an interlocking system). In *FORMS/FORMAT 2007, Formal Methods for Automation and Safety in Railway and Automotive Systems*, Braunschweig.

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

Bacherini, S., Fantechi, A., Tempestini, M., & Zingoni, N. (2006). A story about formal methods adoption by a railway signaling manufacturer. *FM 2006, Formal Methods* (pp. 179–189). Berlin, Heidelberg: Springer Berlin Heidelberg.

Banci, M., Fantechi, A., & Gnesi, S. (2004). The role of formal methods in developing a distributed railway interlocking system. In *FORM-S/FORMAT 2004*, pp. 220–230.

Behm, P., Benoit, P., Faivre, A., & Meynadier, J.-M. (1999). Météor: a successful application of B in a large project. *Petri nets: Central models and their properties* (pp. 369–387). Berlin, Heidelberg: Springer Berlin Heidelberg.

Bon, P., & Dutilleul, S.C. (2013). From a solution model to a B model for verification of safety properties. *Journal of Universal Computer Science, 19*(1), 2–24.

Bon, P., Collart-Dutilleul, S., & Sun, P. (2013). Study of implementation of ERTMS with respect to French national rules using a B centred methodology. In *Industrial Engineering and Systems Management (IESM 2013)*, pp. 1–5.

Boulanger, J.-L. (2013a). Formal methods: industrial use from model to the code. *ISTE*. Wiley.

Boulanger, J.-L. (2013b). Industrial use of formal methods: formal verification. *ISTE*. Wiley.

Bjørner, D. (2003). New results and trends in formal techniques & tools for the development of software for transportation systems – a review. In *Formal Methods for Railway Operation and Control Systems (FORMS03)*, pp. 1–20.

Bjørk, J. (2006). Executing large scale colored Petri nets by using Maude. Ph.D. thesis. Oslo, Norway: University of Oslo.

Buchheit, G., Malassé, O., Brinzei, N., Lalouette, J., Walter, M., et al. (2011). évaluation des performances d'un axe ferroviaire en fonction des caractéristiques fiabilistes de ses systèmes de signalisations. In *Qualita 2011, 9ème Congrès international pluridisciplinaire qualité et sûreté de fonctionnement*.

Chen, L., Ning, B., & Xu, T. (2007). Research on modeling and simulation of vehicle-on-board automatic train protection subsystem of communication based train control system. In *ICVES 2007, IEEE International Conference on Vehicular Electronics and Safety*, pp. 1–5.

Cheng, Y.-H., & Yang, L.-A. (2009). A fuzzy Petri nets approach for railway traffic control in case of abnormality: evidence from Taiwan railway system. *Expert Systems with Applications, 36*(4), 8040–8048.

Collart-Dutilleul, S., Bon, P., El-Koursi, E., & Lemaire, é. (2014). Study of the implementation of ERTMS with respect to French national on board rules using a collaborative methodology based on formal methods and simulation. In *TRA 2014, 5th Transport Research Arena 2014*, Paris, France.

Fantechi, A. (2012). The role of formal methods in software development for railway applications. In *Railway Safety, Reliability and Security: Technologies and System Engineering* (chapter 12), pp. 282–297.

Fantechi, A. (2014). Twenty-five years of formal methods and railways: what next? *Software engineering and formal methods* (pp. 167–183). Cham: Springer International Publishing.

Fantechi, A., Flammini, F., & Gnesi, S. (2014). Formal methods for railway control systems. *International Journal on Software Tools for Technology Transfer, 16*(6), 643–646.

Fantechi, A., Fokkink, W., & Morzenti, A. (2012). Some trends in formal methods applications to railway signaling. *Formal methods for industrial critical systems* (pp. 61–84). Hoboken, NJ, USA: John Wiley & Sons, Inc.

Fanti, M.P., Giua, A., & Seatzu, C. (2006). Monitor design for colored Petri nets: an application to deadlock prevention in railway networks. *Control Engineering Practice, 14*(10), 1231–1247.

Ghazel, M. (2009). Using stochastic Petri nets for level-crossing collision risk assessment. *IEEE Transactions on Intelligent Transportation Systems, 10*(4), 668–677.

Giua, A., & DiCesare, F. (1993). GRAFCET and Petri nets in manufacturing. *Intelligent manufacturing* (pp. 153–176). London: Springer London.

Giua, A., & Seatzu, C. (2008). Modeling and supervisory control of railway networks using Petri nets. *Automation Science and Engineering, 5*(3), 431–445.

Buchheit, G., Malassé, O., Brinzei, N., & Lalouette, J. (2010). Évaluation des performances d'un axe ferroviaire en fonction des caractéristiques fiabilistes de ses systèmes de signalisations. In *9ème Congrès International Pluridisciplinaire Qualitéet Sûreté de Fonctionnement, Qualita'2011*.

Hagalisletto, A.M., Bjørk, J., Yu, I.C., Yu, I.C., & Enger, P. (2007). Constructing and refining large-scale railway models represented by Petri nets. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37*(4), 440–460.

Holloway, L., & Krogh, B. (1994). Controlled Petri nets: A tutorial survey. English. In G. Cohen, & J.-P. Quadrat (Eds.), *11th International Conference on Analysis and Optimization of Systems Discrete Event Systems* (vol. 199). Lecture notes in control and information sciences (pp. 158–168.). Berlin, Heidelberg: Springer.

Holloway, L., Krogh, B., & Giua, A. (1997b). A survey of Petri net methods for controlled discrete event systems. English. *Discrete Event Dynamic Systems, 7*(2), 151–190.

Huang, Y.-S., Weng, Y.-S., & Zhou, M. (2010). Critical scenarios and their identification in parallel railroad level crossing traffic control systems. *IEEE Transactions on Intelligent Transportation Systems, 11*(4), 968–977.

Janhsen, A., Lemmer, K., Meyer zu Hörste, M., & Schnieder, E. (1997). Migration strategy for different level of the European train control system to existing railway environment. In *Proceedings of World Congress of Railway Research, volume C: Power Supply, Signaling, Telecommunications and Non-conventional Systems*, Florence, pp. 101–118.

Jansen, L., Meyer Zu Hörste, M., & Schnieder, E. (1998). Technical issues in modelling the European train control system (ETCS) using coloured Petri nets and the design/CPN tools. In *Workshop on Practical Use of Coloured Petri Nets and Design/CPN* (pp. 103–115). Aarhus, Denmark: Citeseer.

Jensen, K. (1981). Coloured Petri nets and the invariant-method. *Theoretical Computer Science, 14*(3), 317–336.

Jensen, K. (1987). Coloured Petri nets. *Petri nets: central models and their properties* (pp. 248–299). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kaakai, F., Hayat, S., & El Moudni, A. (2007). A hybrid Petri nets-based simulation model for evaluating the design of railway transit stations. *Simulation Modelling Practice and Theory, 15*(8), 935–969.

Kerkouche E, Chaoui, A.A., Bourennane, E.B., et al. (2010). A UML and colored Petri nets integrated modeling and analysis approach using graph transformation. *Journal of Object Technology, 9*(4), 25–43.

Lalouette, J., Caron, R., Scherb, F., Brinzei, N., Aubry, J.-F., Malassé, O., et al. (2010). évaluation des performances du système de signalisation ferroviaire européen superpose au système français, en présence de défaillances. In *Lambda-Mu 2010, 17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*.

Lei, L., Zhang, Y., Shen, X., Lin, C., & Zhong, Z. (2013). Performance analysis of device-to-device communications with dynamic interference using stochastic Petri nets. *IEEE Transactions on Wireless Communications, 12*(12), 6121–6141.

Moen, A., & Yu, I.C. (2004). Large scale construction of railroad models from specifications. In *IEEE International Conference on Systems, Man and Cybernetics*, pp. 6212–6219.

Pachl, J. (2002). *Railway operation and control*. VTSTD Rail Publishing.

Petri, C.A. (1966). *Communication with automata*, technical report RADC-TR-65–377 1 (2nd edn.). New York: Griffiss Air Force Base.

René, D., & Alla, H. (1992). *Petri nets and Grafcet: tools for modelling discrete event systems*. Prentice Hall (cit. on p. 56).

René, D., & Alla, H. (1997). Du grafcet aux réseaux de Petri. In *Ouvrage*. ISBN13: 978-2-86601-325 7.

Rétiveau, R. (1987). La signalisation ferroviaire. Presse de l'école nationale des Ponts et Chaussées.

Sun, P. (2015). Model based system engineering for safety of railway critical systems. Ph.D. thesis. Lille, France: école centrale de lille.

Sun, P., Collart-Dutilleul, S., & Bon, P. (2014). Formal modeling methodology of French railway interlocking system via HCPN. In *COMPRAIL 2014, International Conference on Railway Engineering Design and Optimization*, Rome, Italy.

Sun, P., Bon, P., & Collart-Dutilleul, S. (2015). A joint development of coloured Petri nets and B method in critical system. *Journal of Universal Computer Science, 21*(12), 1654–1683.

Sun, P., Collart-Dutilleul, S., & Bon, P. (2015). A model pattern of railway interlocking system by Petri nets. In *MT-ITS 2015, Models and Technologies for Intelligent Transportation Systems*, Budapest, Hungary.

Wang, F., & Bai, Z. (2010). Research for urban rail transit train regulation based on time Petri nets. In *CCTAE 2010, International Conference on Computer and Communication Technologies in Agriculture Engineering*, Chengdu, China, pp. 461–465.

Wu, N., & Zhou, M. (2004). Modeling and deadlock control of automated guided vehicle systems. *IEEE/ASME Transactions on Mechatronics, 9*(1), 50–57.

Xu, T., & Tang, T. (2007). The modeling and analysis of data communication system (DCS) in communication based train control (CBTC) with colored Petri nets. In *ISADS 2007, 8th International Symposium on Autonomous Decentralized Systems*, Sedona, AZ, pp. 83–92.

Yu, I.C. (2004). A layered approach to automatic construction of large scale Petri nets. Ph.D. thesis. Oslo, Norway: University of Oslo.

Zaytoon, J., & Villermain-Lecolier, G. (1999). Grafcet: methodological and formal issues. *Advances in manufacturing* (pp. 101–114). London: Springer London.

Zhu, L., Yu, F.R., Ning, B., & Tang, T. (2012). Service availability analysis in communication-based train control (CBTC) systems using WLANs. In *ICC 2012, IEEE International Conference on Communications*, Ottawa, ON, pp. 1383–1387.

Zimmermann, A., & Hommel, G. (2003). A train control system case study in model-based real time system design. In *IPDPS 2003, International Parallel and Distributed Processing Symposium*, 8 pp.

Chapter 8
Crossing Border in the European Railway System: Operating Modes Management by Colored Petri Nets

Hela Kadri, Simon Collart-Dutilleul, and Philippe Bon

8.1 Introduction

ERTMS is also a European specification that aims at providing a European interoperability. Nevertheless, it has been presented that this specification only defines the on-board automatism and their communication with the track, using some beacons and an RBC. That means that the signaling trackside rules are specific to each country.

It has been presented that the operating rules provide a bridge from the European specification toward the national trackside specification.

The current chapter points particular and specific aspects. Operating rules are written locally and commonly validated by a national safety authority. A national safety assessment of a global ERTMS implementation on a given line may lead to forbid several of the operating modes proposed by ERTMS.

One of the aims of the ERTMS specification is allowing us to go through national borders without stopping trains, without changing the staff, and without switching from a national control system to another one.

This chapter formally stands the problem for going through a border on a line where in each country there are some ERTMSs that have been eliminated for safety reasons.

The original version of this chapter was revised: The affiliation for Dr. Hela Kadri has been corrected. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-72003-2_10

H. Kadri (✉)
Université de Lille, Laboratoire Cristale, Lille, France
e-mail: hela.kadri@univ-lille.fr

S. Collart-Dutilleul · P. Bon
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr; philippe.bon@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_8

The problem of transnational line mode management is treated using several existing works concerning mode management applied to discrete-event systems. This efficient scientific framework allows to provide some recommendations for the local syntheses of transnational operating rules.

Many methods offering advantageous solutions to safe control include those based distinctively on the operating modes management. This technology involves matching each mode to specific system behavior (engagement or disengagement of different system components) and specific tasks and controlling the switching between the modes.

In this chapter, a multi-model approach is proposed, in which only one operating mode is activated at a time, while other modes must be deactivated. This allows us to define separate behavior of the system for each model under specific control based on the Supervisory Control Theory (initiated by Ramadge and Wonham 1989). However, in this theory, the size of the resulting model increases exponentially with the number of components, and controller synthesis becomes a difficult process.

Based on the colored Petri net (CP-net), our objective is to propose a formal model with a reasonable size to analyze the European railway system such as deadlock/livelock freeness and reachability properties (Kadri et al. 2014).

The remainder of this chapter is organized as follows. Section 8.2 is devoted to present an overview of the ERTMSs, while Sect. 8.3 presents the proposed CP-net model representing the adopted multi-model approach and related hypothesis. In Sect. 8.4, a case study is described and then the related CP-nets model is detailed. Finally, Sect. 8.5 sums up the paper and presents some ideas for future works.

8.2 ERTMS Crossing Border Problem

As explained before, the ERTMS global specification concerns rolling stocks and their interaction with trackside appliance. The infrastructure management is specific to each country.

Some specific contexts may never be instantiated in a given national context because of particular national infrastructure configuration correlated with particular national safety rules.

This detail leads to an interesting problem: is it possible to go through a border without stopping the train or without using a specific national functioning mode using a specific transmission module (STM)?

It is possible that a train, on a line crossing through a border, is running a functioning mode which is not allowed in the other country. Let us point out that if some functioning modes are forbidden, the transition of a given functioning mode to another may become sophisticated. In fact, there is a transition matrix for the global ERTMS functioning mode transition, but in a national context, a restricted version of the table is used.

In terms of a behavioral point of view, the model handled by the EVC is not the same in the two sides of a given border. It is also natural to consider a multi-model framework approach in order to deal with the ERTMS train cross-border problem.

8.2.1 The Different Modes of ERTMS

ERTMS can operate in three levels (plus optional level 0 and specific transmission module levels). This chapter focuses on ETCS level 2.

Level 2 provides cab signaling functions using GSM-R radio transmission to transmit Movement Authorities (MA) delivered by National train track systems to trains. A movement Authority specifies the speed to be respected at given track points until the end of Authority (EOA) is reached.

ERTMS defines several functioning modes in order to take into account the various operation contexts. Let us present some of them for the 2.3 release:

Full supervision (FS) is the nominal mode providing a full protection against overspeed and overrun.

On-sight (OS) is the mode used to run on an occupied block at a limited speed. The driver has the full responsibility for the train maneuvers safety.

Staff responsible (SR) is used at the beginning of missions and other degraded situations (e.g., when the position of the train is not sure). It allows running, under the responsibility of the driver, at a limited speed.

Shunting (SH) is the mode used in situations mostly for maneuver situations. Vehicles in shunting mode can run without the available train data.

No power (NP) occurs when no power is applied to the on-board ETCS equipment. It is accompanied by an emergency brake demand.

Standby (SB) is a default mode that is selected during the startup of ETCS or when the signal box is not in use.

Sleeping (SL). The train is remotely controlled by a leader locomotive.

Unfitted (UN). Train protection is left to older systems because the line is unfitted with ETCS. The system will only observe master speed limit.

Reversing (RV) mode allows the train to make an emergency backward movement, without any signaling condition or written order in a well-defined area.

Isolation (IS) occurs when the ETCS on-board equipment is disconnected from the train braking system.

Trip (TR) is automatically selected in the event of a movement authority being exceeded, until acknowledged by the driver. An emergency brake demand will occur.

Post-trip (PT) follows an emergency brake demand, once the driver has acknowledged the trip and the train has come to a stand.

System failure (SF) is associated with failure of the ERTMS and is accompanied by an emergency brake demand.

STM European (SE) allows the use of a national signaling system while applying the functions of ERTMS/ETCS. It is only used in the STM level.

STM National (SN) allows the use of a national system and applies national rules.

Limited supervision (LS) gives partial protection against overspeed and overrun. The driver has to observe and obey to lineside signals and operating rules when in limited supervision mode.

Non-leading (NL). The locomotive should be coupled to another one. The movement with a traction unit in NL is judged particularly unsafe because the engine in NL is free to move as soon as its driver has selected this mode.

Let us remark that some ERTMS modes are forbidden in some countries. As an example, SH, UN, RV, and NL are not available in France.

8.2.2 Transitions Between ERTMS Modes

Transition is the switching from one mode to another. However, it doesn't exist necessarily transitions between all modes, that is to say that some modes cannot be consecutive to the others. Different mandatory conditions are established for transitions between the modes are properly done (UNISIG, ERTMS Users Group 2008). These conditions are presented in list form.

Figure 8.1 represents the different transitions. It corresponds to the release 2.3.0*d* of ERTMS (UNISIG, ERTMS Users Group 2005). A new ERTMS line may have to fulfill the new specification ERTMS 3.4.0 (UNISIG, ERTMS Users Group 2014). In this specification, there is a new table of mode transitions, and a new Petri net can be systematically built using the same procedure.

The reading of this table is very simple. Various symbols appear in the table:

- The symbol "4 $>$ " means that the condition 4 must be met to trigger the transition.
- The direction of the symbol $>$, namely $>$ or $<$, is paramount; that is to say, we must respect the direction of the arrow in the reading of the table.
  For example, 1st line/2nd column: the transition from SB mode to NP mode will do if condition ♯29 is satisfied.
- Every transition gets a priority order, p ...to avoid conflict between different transitions that would occur simultaneously. Some transitions have received the same priority as it is obvious that they cannot take place in the same time.

More in detail, for the conditions to be respected, when it is indicated, for example, $<$ 5, 6, 50, 51, this means in fact $<$ 5 or 6 or 50 or 51, that is to say, to trigger the transition, the condition 5 or 6 or 50 or 51 must be satisfied.

8.3 A Multi-Model Control Problem for ERTMS

Colored Petri nets tool is wide used for operating rules management and ERTMS modelling (Barger et al. 2009; Lahlou et al. 2006; zuHörste and Schnieder 1999). On the other hand, switching from a discrete-event model to another is addressed in the scientific literature (Kamach et al. 2006; Faraut et al. 2009; Zouari et al. 2007; Kadri et al. 2013). Based on the supervisory control theory, the study of Kamach

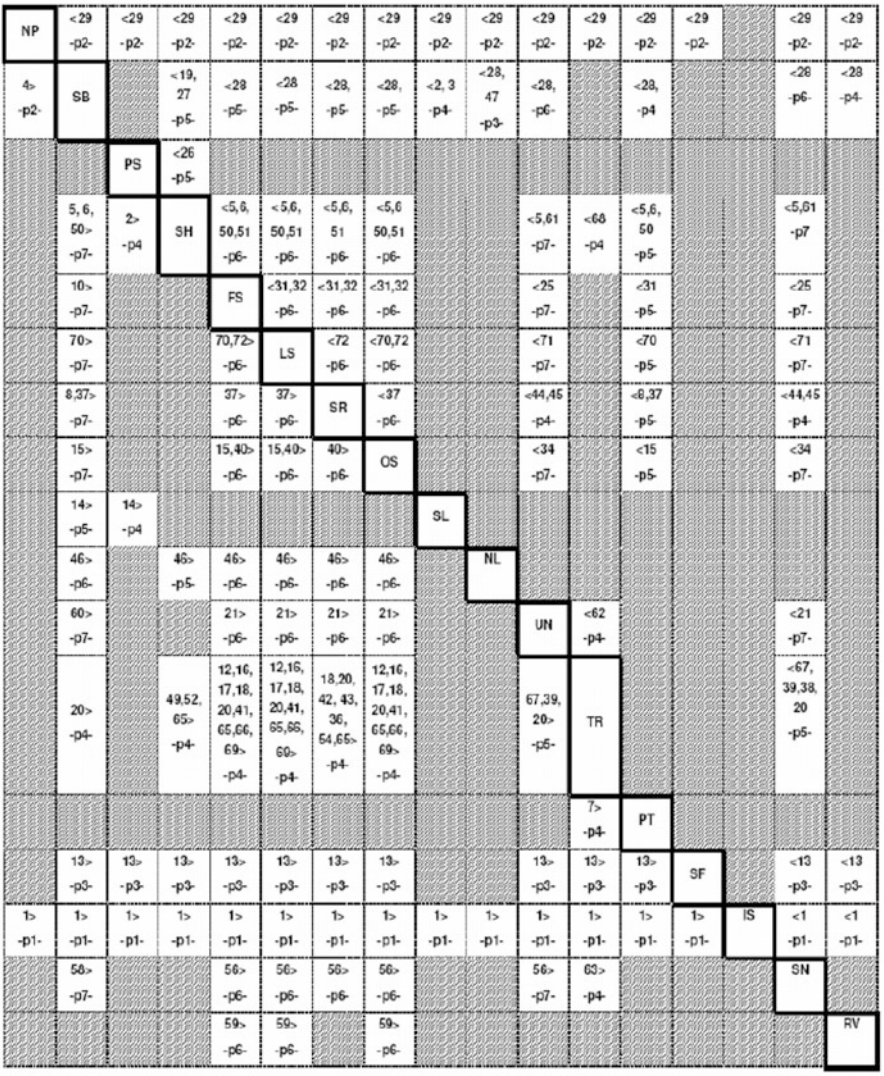


Fig. 8.1 Transition table between ERTMS modes

et al. (2006) and Faraut et al. (2009) associates the automata formalism with each operating mode and a switching mechanism inducing trace memorization. However, the same approach is formulated using a CP-nets formalism in Zouari et al. (2007) and Kadri et al. (2013). In this chapter, a method generalisation of Kadri et al. (2013) is proposed allowing the management of many systems at the same time having each one a set of operational modes. Then this method is applied to a railway system. In

fact, the system is highly specific, so that it can be regarded as a discrete-event system.

8.3.1 Supervisory Control Theory

Supervisory Control Theory (SCT) underpins the study of discrete-event system (DES) control. This theory has allowed us to introduce some important properties such as safety, liveliness, controllability, observability, and diagnosability in discrete-event system domain. SCT is based on the separation between the model representing what the system can do and the model of what the system should do. Applied to industrial applications, SCT has a problem of scalability because of state-space explosion: real system models may be too large to be computed and interpretation of models: larger models are difficult to understand even if computation is successful.

Several approaches have been proposed to solve scalability: modular (Nourelfath and Niel 2004), decentralized (Jiang and Kumar 2000), hierarchical (Chao and Xi 2003), and even hierarchical and distributed (Chafik and Niel 2000). Despite the decomposition is used to reduce the complexity, these approaches always handle the whole process and the whole specification involving a difficult interpretation of models, in particular about commutation between system's modes that are not clearly identified.

Moreover, numerous works focused on multi-model control law in DES. However, most of them apply compositional formalisms on modelling configurations: for instance, state charts (Harel 1987), mode charts (Jahanian and Mok 1994), hierarchical finite state machines, mode automata (Maraninchi and Rémond 2003), and more recently Petri nets model (Zouari et al. 2007).

Nevertheless, few approaches using SCT with modal point of view exist (e.g., Kamach et al. 2006; Kadri et al. 2013). These works allow to study the intramodal behavior of each mode independently and identify the incompatible states when a commutation could happen.

8.3.2 Colored Petri Nets

CP-nets are well adapted to the modelling of parametric systems, in which behaviors depend on the basic structure of the model rather than on the cardinalities of the color sets (Jensen 1997).

CP-net is a tuple $< P, T, K, D, W_-, W_+, \Phi, M_0 >$, where :

P is a finite set of places;
T is a set of transitions verifying $P \cap T = \varnothing$, $P \cup T \neq \varnothing$;

K $= \{C_1, \ldots, C_{|K|}\}$ is a set of object classes such that $\forall i \neq j \in \{1, \ldots k\}, C_i \cap C_j = \varnothing$;

D is the color *domain* function, defined from $P \cup T$ into the set of color domains. An element c of $D(s)$ is a tuple $< c_1, \ldots, c_k >$ and is called a color of s;

W^-, W^+ are the input and output functions (also called incidence functions) defined on $P \times T$, such that $W^-(p,t)$ and $W^+(p,t)$ $W^+(p,t)$ are color functions representing linear applications onto $Bag(D(p))$, for all $(p,t) \in P \times T$; in other words, $W^-(p,t)$ (respectively, $W^+(p,t)$) represents an input (respectively, output) colored arc of a CP-net;

Φ is a function that associates a guard with any transition. By default $\Phi(t)$ is true for any transition t;

M_0 the initial marking is a function defined on P, such that $M_0(p) \in Bag(D(p))$, for all $p \in P$.

The dynamic behavior of CP-nets is determined by the following firing rule :

- A guarded transition t is enabled for a color c and a marking M, denoted by $M[t,c\rangle$, if and only if $\forall p \in P$, $M(p) \geq W^-(p,t)(c)$, and the guard associated with t is evaluated to true.
- The marking M' obtained after the firing of (t,c) is computed as

$$\forall p \in P, M'(p) = M(p) + W^+(p,t)(c) - W^-(p,t)(c).$$

- The notation $M[t,c\rangle M'$ is used to indicate this reachability relation. The notation $[M\rangle$ indicates the set of all reachable markings from the marking M.

8.3.3 Multi-Model Approach for ERTMS

The multi-model approach involves representing a complex system by a set of simple models, each of which describes the system in a given operating mode. The adopted approach assumes that only one attempted operating mode is activated at a time, while other modes must be deactivated.

For the ERTMS, an operating mode *om* represents, for each train, its moving and its switching in set of functioning modes allowed in the corresponding country.

In the beginning, we denote the set of all modes representing the set of the engaged countries $O = \{om_1, om_2, \ldots, om_{|O|}\}$, where $|O| > 1$, the set of all trains $Trains = \{train_1, train_2, \ldots, train_{|Trains|}\}$, where $|Trains| > 1$, and for each mode om_i, we associate a CP-net $< P_i, T_i, K_i, D_i, W_i^-, W_i^+, \phi_i, M_{0,i} >$ representing a partial description of the system behavior.

8.3.3.1 Proper Component

We consider the following assumption: a process is made up of several components and not all components are used in every operating mode. For instance, European railway systems consist of several components (i.e., tracks, trains, etc.). In our adopted approach, a component represents a part of a CP-net related to one or more operating modes that we call *structure*.

Formally:

Definition 8.1 Let $om_i =< P_i, T_i, K_i, D_i, W_i^-, W_i^+, \phi_i, M_{0,i} >$ be an operating mode.

A CP-net structure $r =< P_r, T_r, W_r^-, W_r^+, M_{0,r} >$ is said to be a component of om_i if and only if $(Pr \subseteqq Pi)$ and $(Tr \subseteqq Ti)$ and $(M_{0,r} \subseteqq M_{0,i})$.

We can deduce:

$$\forall (p,t) \in Pr \times Tr, W_r^-(p,t) = W_i^-(p,t) \text{ and } W_r^+(p,t) = W_i^+(p,t).$$

8.3.3.2 Common Component

An important feature related to the concept of component is whether it is commonly used by several operating modes. Hence, if a component is used in more than one operating mode, it is called a *common component*; otherwise, it is a *proper component*.

In our adopted approach, a common component consists of a subset of tokens, transitions, and/or places, designed in at least two models, and we call it *common structure*.

Let us formally define the conditions to be fulfilled by any structure $r =< P_r, T_r, W_r^-, W_r^+, M_{0,r} >$ to be common.

Definition 8.2 Let O be the set of operating modes. $\forall (om_i, om_j) \in O \times O (om_i \neq om_j)$,

$$\text{if } \exists r =< P_r, T_r, W_r^-, W_r^+, M_{0,r} > \text{ such as}$$

$$(P_r = (P_i \cap P_j) \neq \emptyset) \text{ or } (T_r = (T_i \cap T_j) \neq \emptyset) \text{ or } (M_{0,r} = M_{0,i} \cap M_{0,j} \neq \emptyset),$$

$$\text{then } r \text{ is a common structure for the two modes } om_i \text{ and } om_j.$$

8.3.3.3 Switching Mechanism

A switching event occurs when a train is about to leave the territory of one country to another and leads to quitting the current operating mode and to entering into another one. It induces the deactivation of the current operating mode and the activation of a destination mode.

In our approach, the switching mechanism is modelled by specific CP-net transitions in a given mode that are activated at some distance before the train crosses the border. This distance will be specified by the designer. Firing such transition must disable the transitions of the source CP-net mode and enable firing the transitions of the destination CP-net mode. However, a switching transition holds additional information of the target operating mode and verifies that switching is in a common functioning mode.

To distinguish this type of transitions, we define an application noted:

"$target\_country$" whose role is to associate with each transition its destination mode corresponding to the destination country.

Formally:

Definition 8.3 Let om_i be an operating mode, and T_i be the related set of transitions and a train $Train_j$.

Let $target\_country : (T_i \times Train_j) \rightarrow (O \times Train_j)$ be a mapping such that $target\_country(t, train_j)$ indicates the active operating mode to the train $train_j$ after firing t.

Remark 8.1 $\forall t \in T_i$, if $target\_country(t, train_j) \neq (om_i, train_j)$, then t corresponds to a *switching mechanism* of mode om_i and for the train $train_j$ leading to mode $target\_country(t, train_j)$.

8.3.3.4 Global CP-net

On the basis of the previous concept, we are able now to construct the global CP-net that represents the whole management of the multi-model operating modes system.

Global CP-net is a tuple $< P, T, K, D, W_-, W_+, \Phi, M_0 >$ where :

$P \quad = \cup_{(i=1..|O|)} P_i \cup \{Countries\}$;

$T \quad = \cup_{(i=1..|O|)} T_i$;

$K \quad = \cup_{(i=1..|O|)} K_i \cup \{C_{Countries}\}$, where $C_{Countries} = O$;

D is the color domain function defined, by extension, from $P \cup T$ into the set of color domains;

$W^-, W^+ \quad :$

- $\forall om_i \in O, \forall (p,t) \in P_i \times T_i \wedge (p,t) \notin P_R \times T_R$,
  $W^-(p,t) = W_i^-(p,t)$ and $W^+(p,t) = W_i^+(p,t)$
- $\forall om_i \in O, \forall (p,t) \in P_R \times T_R$,
  - $W^-(p,t) = f(target\_country(t, train_i), p, t)$ where $f : (O \times Trains) \times P \times T \longrightarrow P \times T$
    $((Om_j, train_j), p, t) \mapsto W_j^-(p,t)$,
  - $W^+(p,t) = g(target\_country(t, train_i), p, t)$ where

$$g : (O \times Trains) \times P \times T \longrightarrow P \times T$$
$$((Om_j, train_j), p, t) \mapsto W_j^+(p, t);$$

- $\forall (om_i, om_j) \in O \times O (i \neq j), \forall (p, t) \in P_i \times T_j :$
  $p \notin P_j$ and $t \notin T_i$, $W^-(p, t) = W^+(p, t) = 0$;
- $\forall om_i \in O, \forall t \in T_i,$
  $W^-(Countries, t) = (c, n)$
  $W^+(Countries, t) = (c, n)$ if
  $target\_country(t, train_j) = (om_i, train_j)$
  $= target\_country(t, train_j)$ otherwise.

ϕ :

- $\forall om_i \in O, \forall t \in T_i$ and $t \notin T_R$,
  $\phi(t) = \phi_i(t) \wedge [(c, n) = (om_i, train_j)]$, where (c, n) is a variable defined on $C_{Countries}$
- $t \in T_R, \phi(t) = \vee_{(1..|o|)}(\phi(t) \wedge [Countries = (om_i, train_j)]$

M_0 :

- $M_0(Countries) = om_1$
- $\forall om_i \in O, \forall p \in P_i \wedge p \notin P_R$, $M_0(p) = M_{0,i}(p)$;
- $\forall p \in P_R$, $M(p) = \sum_{(j \in D(p))}[max_{(i=1..|o|)}(M_{0,i}(p)(j))]$
  where $M_{0,i}(p)(j)$ defines the number of instances of color j in $M_{0,i}(p)$.

8.3.3.5 Semantics of the Global CP-net

It is important to verify that the behavior of the global CP-net modelling the management of operating modes system fulfils the following rules.

Activated mode. A unique operating mode is activated at any given moment for any train.
Sketch of proof: It is easy to demonstrate that this rule is mainly ensured by the role of place $Countries$.

Mode switching. For each train, a switching mechanism deactivates its current mode and activates a new one.
Sketch of proof: As the firing of a switching transition modifies the value of tokens in $Countries$, and considering the mode activating principles, all transitions of the current mode become disabled and all the transitions of the target mode will get "true" as the value associated with their "mode" predicate.

Common component management. The state of a common component must be coherent after a switching mechanism.
Sketch of proof: As common components are represented without redundancy in the global CP-net, it is easy to see that the state of any common component is maintained by the marking of its common places.

8.4 Case Study

8.4.1 The Systems Description

To illustrate the modeling approach dedicated to the European rail system, this chapter considers the case of a train moving from France to a neighboring country "Country1" (see Fig. 8.2) on the itinerary [$Z1$, $Z2$, $Z3$, $Z7$, $Z8$] that is divided into cantons (Z_i) of about 3000 m. We remark that $Z1$, $Z2$ and a part of $Z3$ are situated in France, and the rest is in Country1.

In each country, trains move and switch from one mode to another in their set of allowed modes based on the profile of the line ahead. Let us remember that allowed modes in France are: FS, OS, and SR, and we suppose that in Country 1 the allowed modes are: FS, OS, UN,RV, NL, and SH. Before crossing the national border and to avoid stopping, trains have to go to a common mode between France and country1. The common mode chosen belongs to a set of common modes determined from the intersection of the modes of the two countries concerned (i.e., FS and OS).

Although the studied system has a limited size, the proposed approach can be easily applied to all the European rail networks.

8.4.2 CP-net Models

The following models of the management of operating modes are developed using the CPN Tools 4 environment (CPN Tools 2014).

To better understand the global model, let us first describe every operating mode in a separate sheet, by a CP-net model. Common components should be defined by giving same names to places, tokens, and transitions in different sheets, and the designer may indicate which transition is a switching one.

In this case study, $O = \{om_1, om_2\}$ (om_1 for the France mode and om_2 for country$_1$ mode) and $Train = \{T_1\}$.

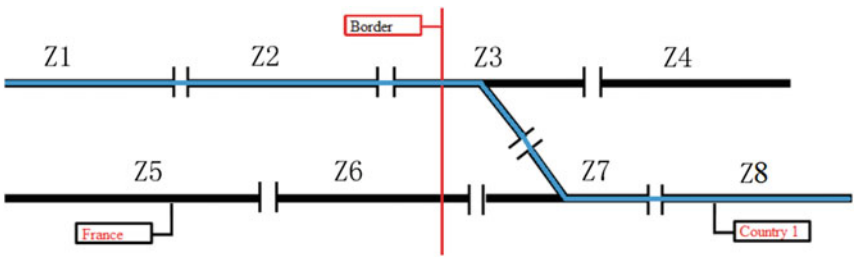


Fig. 8.2 Railway example between France and Country1

8.4.2.1 Operating Mode CP-net of France

In this CP-net (see Fig. 8.3), one may state:

- The functioning of the train $T1$ is represented by the state machine made up of places *{Trains, Modes of Countries}* and transitions {moving, mode changing}.
- The arcs labelled by variables (n, iti, m, c) and $(n, ct :: iti, m, c)$ that are defined on the color class $TrainIdentity \times Trajectory \times CurrentMode \times CurrentCountry$ allow the train movement. And the arcs labelled by variables $(n, iti, m1, c)$ and (c, lm) allow the changing modes train. (c, lm) is defined on the color class $Country \times AuthorizedModes$.
- $M_0(Trains) = 1`(T1, [Z1, Z2, Z3, Z7, Z8], SR, France)$, $M_0(Modes\ of\ Countries) = 1`(France, [FS, SR, OS])$.
- *transition'cross the Country1 border from France on Z3'*] is a switching transition (i.e., $target\_country(Train \times cross\ the\ Country1\ border\ from\ France\ on\ Z3) = (Train \times om_2)$). This transition, firstly, has a guard checking that the train is on the Z3 canton then on the Z7 canton; this will inform us of the position and direction of the train; and secondly, it is a high-priority transition in order to force it occurs before other transitions if it is enabled. When fired, the train crosses the Country1 border in a common functioning mode between France and Country1.

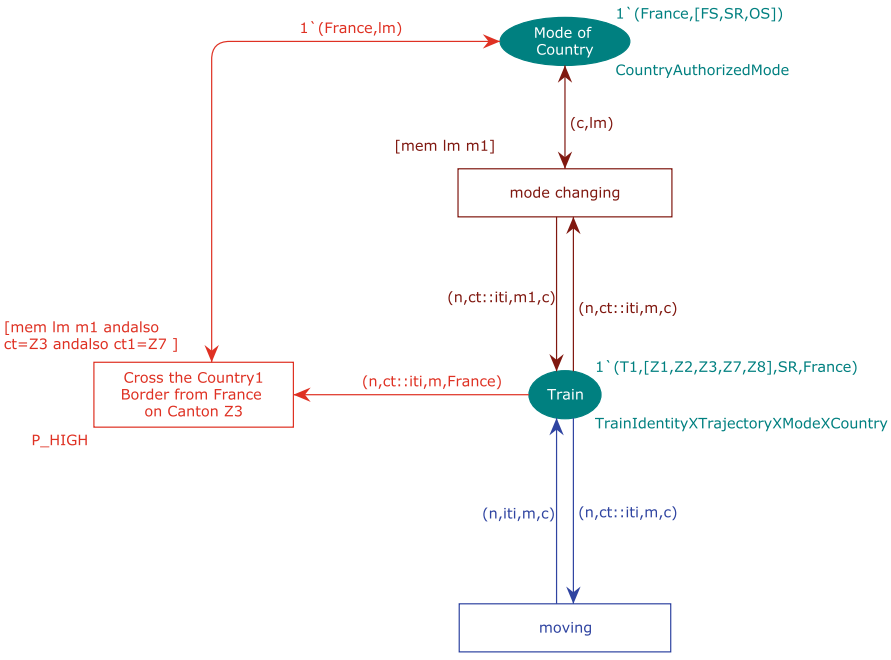


Fig. 8.3 Operating mode CP-net in France

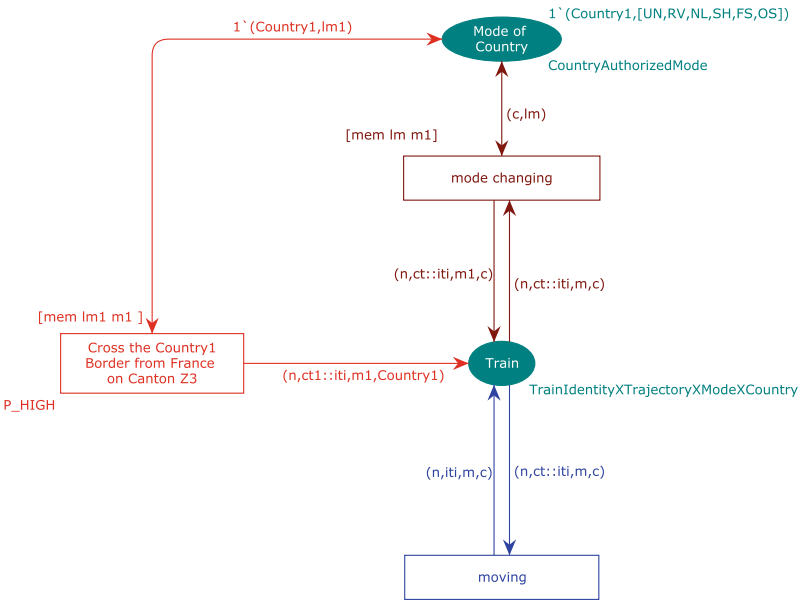


Fig. 8.4 Operating mode CP-net in Country1

8.4.2.2 Operating Mode CP-net of Country1

Figure 8.4 describes the behavior of the Country1 mode. One may note the following points:

- The train behavior is modelled in a similar way in Country 1 mode as in France mode.
- $M_0(Modes\ of\ Countries) = 1`(Country, [UN, RV, NL, SH, FS, OS])$.
- A *common component* appears through all the places, transitions, and arcs of the Country1 mode.

8.4.2.3 Global Model for the Management of Operating Modes

In this CP-net (see Fig. 8.5), all places, transitions, tokens, and arcs of the two modes are present without duplicating the common components.

Moreover, new elements are added in order to express the mode management:

- Place bears the name *Countries* and its associate initial marking is $(France, T1)$. This place is initialized by tokens as much as trains in the system.
- All arcs connecting *Countries* to non-switching transitions are labelled by (c, n).

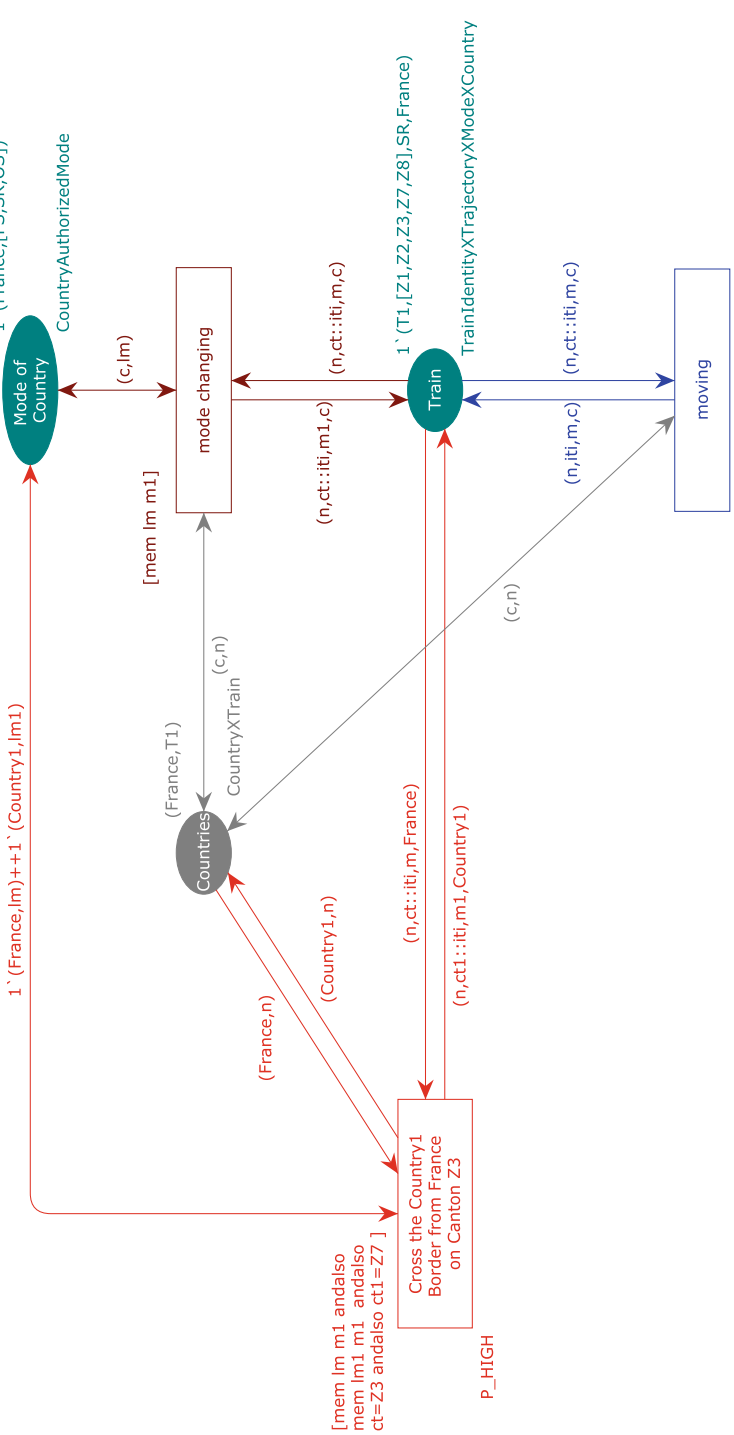


Fig. 8.5 Global model for the management of operating modes

- Any transition of a common component is assigned a predicate that is satisfied as soon as the token of *Countries* has the value of an operating mode including the component.
- Any other transition is assigned a predicate that is satisfied only when the appropriate token is in *Countries*.
- Any switching transition is connected to *Countries* with an input label (c, n), and with an output label set to its target mode.
- An arc is added to a switching transition permitting a commutation in a common functioning mode between the two concerned countries.
- $M_0(Modes\ of\ Countries) = 1`(Country, [UN, RV, NL, SH, FS, OS]) + + 1`(France, [FS, SR, OS])$.

8.4.3 The Case Study: Simulation and Formal Verification

During the simulation of the global model, we can observe the switching mechanism when any train crosses the border; and the proposed CP-net model allows validation of some properties of the studied system that are:

- *The deadlock-free states:* A deadlock is a situation wherein two or more components are waiting for the other to finish, and thus neither ever finishes. We have easily verified that the state spaces of a simple studied example do not include deadlock states.
- At any time and for each train, only one mode is activated and a productive cycle is always preserved.
- The system switches from one mode to another easily.

The validation is insured based on the standard report generated for the state space analysis of the railway system studied (see Fig. 8.6) that is directly generated by CPN tools.

We observe the absence of the home marking and the absence of dead and live transitions instances. There are two infinite firing sequences (IFS):

- *mode changing* that occurs infinitely often in every IFS;
- *cross the Country1 border from France on canton Z3* that occurs infinitely often in every IFS where it is enabled infinitely often.

However, the transition *moving* is with no fairness, that is, there is an IFS where it is continuously enabled from some point onward and does not fire anymore; and the train terminates in one of the six dead markings relating to the train stop in one of the six modes allowed in Country1.

8.5 Conclusion

We have presented a CP-net approach for the management of operating modes in ERTMSs. The proposed methodology provides a safe management of operating modes when trains cross borders. We adopted a multi-model approach not only to tackle the state explosion problem but also to offer an easy design tool. The use of CP-nets contributes by providing a formal framework at both the specification and analysis levels. We aim, in the future, to take into account a time measure as a parameter of operating mode management in order to conduct performance assessment.

```
 Statistics
------------------------------------------------------------------------

  State Space
     Nodes:  27
     Arcs:   114
     Secs:   0
     Status: Full

  Scc Graph
     Nodes:  13
     Arcs:   24
     Secs:   0


 Boundedness Properties
------------------------------------------------------------------------

  Best Integer Bounds
                              Upper      Lower
     New_Page'Countries 1     1          1
     New_Page'Modes_of_Countries 1
                              2          2
     New_Page'Trains 1        1          1

  Best Upper Multi-set Bounds
     New_Page'Countries 1
                         1`(France,T1)++
1`(Country1,T1)
     New_Page'Modes_of_Countries 1
                          1`(France,[FS,SR,OS])++
1`(Country1,[UN,RV,NL,SH,FS,OS])
     New_Page'Trains 1   1`(T1,[],UN,Country1)++
1`(T1,[],RV,Country1)++
1`(T1,[],NL,Country1)++
1`(T1,[],SH,Country1)++
1`(T1,[],OS,Country1)++
1`(T1,[],FS,Country1)++
1`(T1,[Z1,Z2,Z3,Z7,Z8],OS,France)++
1`(T1,[Z1,Z2,Z3,Z7,Z8],SR,France)++
1`(T1,[Z1,Z2,Z3,Z7,Z8],FS,France)++
1`(T1,[Z2,Z3,Z7,Z8],OS,France)++
1`(T1,[Z2,Z3,Z7,Z8],SR,France)++
1`(T1,[Z2,Z3,Z7,Z8],FS,France)++
1`(T1,[Z3,Z7,Z8],OS,France)++
1`(T1,[Z3,Z7,Z8],SR,France)++
1`(T1,[Z3,Z7,Z8],FS,France)++
1`(T1,[Z7,Z8],UN,Country1)++
1`(T1,[Z7,Z8],RV,Country1)++
1`(T1,[Z7,Z8],NL,Country1)++
1`(T1,[Z7,Z8],SH,Country1)++
```

Fig. 8.6 The standard report generated for the state-space analysis of the global CP-net model

```
1`(T1,[Z7,Z8],OS,Country1)++
1`(T1,[Z7,Z8],FS,Country1)++
1`(T1,[Z8],UN,Country1)++
1`(T1,[Z8],RV,Country1)++
1`(T1,[Z8],NL,Country1)++
1`(T1,[Z8],SH,Country1)++
1`(T1,[Z8],OS,Country1)++
1`(T1,[Z8],FS,Country1)

  Best Lower Multi-set Bounds
     New_Page'Countries 1
                        empty
     New_Page'Modes_of_Countries 1
                           1`(France,[FS,SR,OS])++
1`(Country1,[UN,RV,NL,SH,FS,OS])
     New_Page'Trains 1   empty


 Home Properties
------------------------------------------------------------------------

  Home Markings
     None


 Liveness Properties
------------------------------------------------------------------------

  Dead Markings
     6 [27,26,25,24,23,...]

  Dead Transition Instances
     None

  Live Transition Instances
     None


 Fairness Properties
------------------------------------------------------------------------

  Impartial Transition Instances
     New_Page'mode_changing 1

  Fair Transition Instances
     New_Page'Cross_the_Country1_border_from_France_on_canton_Z3 1

  Just Transition Instances
     None

  Transition Instances with No Fairness
     New_Page'moving 1
```

Fig. 8.6 (Continued)

References

Barger, P., Schön, W., & Bouali, M. (2009). A study of railway ERTMS safety with colored Petri nets. In *The European Safety and Reliability Conference (ESREL'09), Prague, Czech Republic*.

Chafik, S., & Niel, E. (2000). Hierarchical-decentralized solution of supervisory control. In *Proc. 3rd Int. Symp. Math. Modelling, MATHMOD, Vienna, Austria* (Vol. 2, pp. 787–790).

Chao, Z., & Xi, Y. (2003). Necessary conditions for control consistency in hierarchical control of discrete-event systems. *IEEE Transactions on Automatic Control, 48*(3), 465–468.

CPN Tools. (2014). CPN Tools Webpage, http://cpntools.org

Faraut, G., Piétrac, L., & Niel, E. (2009). Formal approach to multi-modal control design: Application to mode switching. *IEEE Transactions on Industrial Informatics, 5*(4), 443–453.

Harel, D. (1987). Statecharts: A visual formalism for complex systems. *Science of Computer Programming, 8*(3), 231–274.

Jahanian, F., & Mok, A. K. (1994). Modechart: A specification language for real-time systems. *IEEE Transactions on Software Engineering, 20*(12), 933–947.

Jensen, K. (1997). *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use*. *Monographs in Theoretical Computer Science* (Vol. 1). Berlin: Springer

Jiang, S., & Kumar, R. (2000). Decentralized control of discrete event systems with specializations to local control and concurrent systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 30*(5), 653–660.

Kadri, H., Zairi, S., & Zouari, B. (2013, September 11–13). Global model for the management of operating modes in discrete event systems. In *Management and Control of Production and Logistics, Fortaleza, Brazil* (Vol. 6, Part 1).

Kadri, H., Collart-Dutilleul, S., & Zouari, B. (2014). Crossing border in the european railway system: Operating modes management by colored Petri nets. In *Proceedings of the 10th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems, FORMS/FORMAT 2014* (pp. 244–252). Technische Universität Braunschweig. ISBN: 978-3-9816886-6-5.

Kamach, O., Piétrac, L., & Niel, E. (2006). Multi-Model approach to discrete events systems: Application to operating mode management. *Mathematics and Computers in Simulation, 70*(5–6), 394–407. Computational Engineering in Systems Applications.

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, Maroc.

Maraninchi, F., & Rémond, Y. (2003). Mode-automata: A new domain-specific construct for the development of safe critical systems. *Science of Computer Programming, 1*(46), 219–254.

Nourelfath, M., & Niel, E. (2004). Modular supervisory control of an experimental automated manufacturing system. *Control Engineering Practice, 12*(2), 205–216.

Ramadge, P. J., & Wonham, W. M. (1989). The control of discrete event systems. *Proceedings of the IEEE, 77*(1), 81–98.

UNISIG, ERTMS Users Group. (2005). Subset026, System Requirements Specification (SRS), version 2.3.0d.

UNISIG, ERTMS Users Group. (2008). Subset026, System Requirements Specification (SRS), version 3.0.0.

UNISIG, ERTMS Users Group. (2014). Subset026, System Requirements Specification (SRS), version 3.4.0

Zouari, B., Frefita, R., & Niel, E. (2007). A coloured Petri net approach for the management of operating modes in discrete event systems. In *Management and Control of Production and Logistics, 4th IFAC Conference on Management and Control of Production and Logistics* (Vol. 4, Part. 1, pp. 397–402).

zuHörste, M. M., & Schnieder, E. (1999). Formal modelling and simulation of train control systems using Petri nets. In *FM'99 – Formal Methods*. ISBN 978-3-540-66588-5.

Chapter 9
Conclusion

Simon Collart-Dutilleul

Starting from the fact that railway high-speed trains running at a speed higher than 300 km/h are becoming common, the first part of this book has presented a context integrating various parameters.

The first one is the diversity of safety national rules that must be considered while crossing borders. The second one is the economical interest of international passenger lines that correspond to a societal need. The third one is the technological framework provided by the European community, namely the ERTMS framework. The corresponding chapter of this book presents not only a current state of the ERTMS specification, but a strategic choice of preserving a stable kernel during a given amount of time in order to allow a commercial use. Moreover, the specification of retrocompatibility properties is presented too. It provides the possibility to use more recent ERTMS released rolling stocks on an older released infrastructure for example. These two properties are raising the specification to a life cycle compatible one. ERTMS specification is a living specification, made for accompanying future technological innovations, like moving blocks for instance, toward a commercial efficient use.

The ERTMS chapter is followed by a description of CTCS, which can be seen as an equivalent proposition in China. This proposition is aligned with the assumption that the ERTMS proposition is an alive specification that may be instantiated and may evolve differently, taking into account various contexts including specific needs or new technologies.

The last section of the first part devoted to the background of transnational high-speed railway lines is a short state of the art. It presents tools and approaches that have been successfully experimented. Perspectives associated with several European projects are explained. This section provides the core material that is used

S. Collart-Dutilleul (✉)
COSYS/ESTAS, Université Gustave Eiffel, Villeneuve d'Ascq, France
e-mail: simon.collart-dutilleul@univ-eiffel.fr

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_9

to build a systematic proposition to be used for designing a safe border crossing solution. This is the focus of the second part of this book. Moreover, the state of the art opens to future tooled approaches that promise more efficiency. Actually, it leads to the identification of the next scientific challenges.

Building on the technological and scientific fundamentals of the first part of the book, the second part argues and details a scientific and technological framework allowing addressing the border crossing problem while running ERTMS.

The problem is broken out into two different dimensions: the vertical one and the horizontal one. By vertical, we mean the problem of aligning the operating rule with the ERTMS specification while respecting national lines that are based on a safe interlocking layer.

The horizontal point is common to many cyber-physical systems : trains do not cross instantaneously the border, because they have a given length and because they move with a finite speed. Beyond this physical layer, trains crossing the border need to comply with the countries safety and technical laws. Commpliance with these laws is performed by automation and software services, which cannot simply be switched from one set of rules to another. Therefore, a transient mode must be implemented.

The first chapter provides a synthetic presentation of the global strategy. Then, it proposes a UML-centered approach to integrate UML models of national operating rules into the global railway system. The model engineering is presented as a key technology, as various models are well adapted to describe various types of knowledge. An example of relay-based specification corresponding to a real industrial system is presented. Then, the specification is translated in abstract B machines.

Formal methods-based proofs correspond to the second main proposition of this chapter: checking the global consistency using the B method. It leads us to introduce a systematic translation of UML models of operating rules in abstract B machines using the B4Msecure tools. One of the advantages of this framework is that it separates the functional part and the safety part in the model.

Nevertheless, Event B for system modelling seems to be more adapted. A new version of the tool proposes to translate the UML profile into Event B. Today, safety requirements are introduced at this stage in the model by the mean of safety invariants. Using the goal engineering tools to build these safety invariants independently from technical choices should be more appropriate.

The global safety approach assumes that the interlocking layer behaves correctly, while collaborating fairly with the ERTMS layer (by the mean of the RBC in ERTMS level 2). A whole chapter focuses on this subject. It mainly proposes a generic high-level Petri net model of a railway infrastructure that can be instantiated on a wide variety of infrastructures. This generic pattern embedded the classical French signaling rules to be respected as well as constraints for route forming or train itinerary tracing.

In this particular case, the safety constraints are well known, and they can be checked using the associated model-checking tools, when the corresponding model is not too large.

The translation of high-level Petri nets model into B machines is not presented in this chapter, while there are substantial works in the state of the art devoted to this task. This translation is needed in an approach based on the definition of a global model of the system fulfilling global safety invariants. The last chapter of the book details the border crossing. A proposition is to formalize the problem using a system of system approaches where various functioning modes can be applied when common functioning modes exist. The ERTMS structures use a quite compatible design philosophy, allowing an easy implementation of the approach. Nevertheless, a specific transient mode has to be introduced, fulfilling an intersection of the set of constraints imposed by the first and second countries. A high-level Petri net-based modelling approach is proposed, and some elementary properties insuring the global safe functioning of the system can be checked. A translation of the Petri net model is needed in order to allow proving global invariants while integrating the corresponding operating rule, but it is not presented in this book.

Even if all models are not presented or detailed, a global modelling approach that aims at specifying the problem of international railway lines is presented in this book. The proposed framework allows the use of specific dedicated formalisms when there exists a way of translating the model into abstract B machines.

Nevertheless, a lot of modelling works have to be performed by the experts in the current proposition. Using the BIM implementation provided by the initiative IFC-Rail will deliver a huge amount of structured data that may allow avoiding some repetitive modeling tasks. Moreover, through the OntoRail project, IFC-Rail is aligned with a functional model of the railway topology (this is the RailTopoModel contribution). This functional specification is to be used to feed the building process of formal models analyzed for safety assessment. The more promising element is the project to make RailTopoModel evolve to RailSYS, providing a global functional ontology of the railway system. When this goal will be achieved, a lot of difficult alignment tasks are avoided. Moreover, it will be possible to propose the automation of the formal modelling task.

Correction to: Crossing Border in the European Railway System: Operating Modes Management by Colored Petri Nets

Hela Kadri, Simon Collart-Dutilleul, and Philippe Bon

Correction to:
Chapter 8 in: S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_8

This book was inadvertently published with incorrect University name in the affiliation of Dr. Hela Kadri in Chapter 8.

The affiliation has been updated as follows:

Université de Lille, Laboratoire Cristale, Lille, France

The updated version of this chapter can be found at
https://doi.org/10.1007/978-3-030-72003-2_8

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2_10

Index

S. Collart-Dutilleul (ed.), *Operating Rules and Interoperability in Trans-National High-Speed Rail*, https://doi.org/10.1007/978-3-030-72003-2