International Journal on Software Tools for Technology Transfer (2020) 22:249–255
https://doi.org/10.1007/s10009-020-00562-3

INTRODUCTION

Introduction to special section on the ABZ 2018 case study: Hybrid ERTMS/ETCS Level 3

Michael Butler[1] · Thai Son Hoang[1] · Alexander Raschke[2] · Klaus Reichl[3]

Published online: 31 March 2020

Abstract
This paper introduces the topic of the Special Section on the *ERTMS Level 3 Hybrid* case study. The European Rail Traffic Management System (ERTMS) is a system of standards for management and interoperation of signalling for railways. The case study focuses on the *ERTMS Level 3 Hybrid* principles, which accommodates different types of trains, including trains equipped for ERTMS and non-ERTMS trains. The Special Section contains seven contributed articles describing the application of a formal method to the case study and these contributions are outlined. A overview of the assumptions and requirements of the case study are presented at a level of detail sufficient for the reader to follow the contributed articles.

1 Introduction

This Special Section is devoted to various solutions to formal modelling and analysis of an important new development in railway signalling, namely *Hybrid ERTMS/ ETCS Level 3*. The European Rail Traffic Management System[1] (ERTMS) is the system of standards developed by the European Union for management and interoperation of railway signalling. The aim of ERTMS is to replace the different national train control and command systems in Europe with a seamless European railway system. The intended advantages of ERTMS include increased capacity, higher reliability rates, improved safety, and open supply market. ERTMS uses advanced communications and positional equipment, both trackside and onboard, to ensuring train safety. To cater for a transition period where some trains will be equipped for ERTMS and others will not, the *hybrid* standard concerns a version of ERTMS that caters for ERTMS-equipped trains and non-equipped trains running on the same railway infrastructure. The hybrid system can achieve greater throughput for ERTMS-equipped trains, while achieving conventional throughput for non-equipped trains. Of course, managing equipped and non-equipped trains simultaneously increases the complexity of the signalling scheme and makes for an interesting and challenging case study for formal methods.

The idea of inviting groups to apply formal methods to the case study developed out of the successful series of case studies promoted by the ABZ conference. The ABZ conference is dedicated to the cross-fertilization of six related state-based formal methods, Abstract State Machines (ASM), Alloy, B, TLA, VDM, and Z, that share a common conceptual foundation and are widely used in both academia and industry for the design and analysis of hardware and software systems. ABZ 2014 introduced the concept of an ABZ case study with a practical and real-life case study covering an aircraft *Landing Gear*. Researchers were invited to apply a formal method to the case study and submit a paper describing this. The conference dedicated special sessions to the accepted case study contributions which provided valuable comparison of the various formal methods used. The practice of the ABZ case study was also followed by the ABZ 2016 conference with the *Hemodialysis Machine* case study and by the ABZ 2018 conference with the ERTMS railway case study. The ABZ series of case studies has had the intended effect of enriching the set of case studies developed with ABZ and related methods.

[1] http://ertms.net.

✉ Michael Butler
mjb@ecs.soton.ac.uk

Thai Son Hoang
t.s.hoang@ecs.soton.ac.uk

Klaus Reichl
klaus.reichl@thalesgroup.com

[1] School of Electronics and Computer Science, University of Southampton, Highfield, Southampton SO17 1BJ, UK

[2] Ulm University, 89069 Ulm, Germany

[3] Thales Austria GmbH, Handelskai 92, 1200 Vienna, Austria

This special section of the International Journal on Software Tools for Technology Transfer contains seven articles all of which describe the application of a state-based formal method to the ERTMS case study. Shorter versions of these articles were presented at the ABZ 2018 conference held in Southampton on June 5–8, 2018 [4]. To avoid the authors of the articles having to repeat explanations of the standard, this introduction provides an overview of the key principles of Hybrid ERTMS/ETCS Level 3. The detailed principles of the system are described in a standard document [8].

The first article in this special issue, *The ABZ-2018 case study with Event-B*, by Abrial [1], is focused on re-writing and simplifying the presentation of the ERTMS case study requirements compared with the standard document [8] in a way that is intended to make the requirements more understandable and ease the formalisation process. The usual modelling style in Event-B is to present the details in a stepwise manner through a series of model refinements, and the article outlines the refinement strategy followed in the formalisation. Details of the Event-B formalisation itself are not presented in the article though a link to a machine readable version of the formalisation is provided. We believe that the systematic presentation of the requirements will help the reader understand the principles, allowing them to appreciate the contributions of the other articles more easily.

The article *Validation of the Hybrid ERTMS/ETCS Level 3 using SPIN*, by Arcaini et al. [2], presents a formalisation of the ERTMS case study using the Promela language and describes the validation of the model using the SPIN model checker. The authors highlight ambiguities in the standard that were identified through the model checking and also describe how they used SPIN to perform user-driven validation of the model.

The article *Validating the Hybrid ERTMS/ETCS Level 3 concept with Electrum*, by Cunha and Macedo [5], describes a formalisation of the ERTMS case study using Electrum. Electrum is an extension of the Alloy language that adds mutable relations and LTL to Alloy. The article shows how the Alloy Analyzer was used to validate the Electrum model through scenario execution and through verification of safety properties.

The article *Formalising the Hybrid ERTMS Level 3 specification in iUML-B and Event-B*, by Dghaym et al. [6], describes the use of UML-B for modelling and analysis of the ERTMS case study. UML-B is a graphical version of Event-B that provides class diagrams and state machine diagrams based on UML. UML-B supports refinement and the approach described uses refinement to gradually introduce features of the model while maintaining consistency through formal proof. The emphasis of the article is on the added-value provided by a formal language with diagrammatic syntax.

The article *Validation and Real-Life Demonstration of ETCS Hybrid Level 3 Principles Using a Formal B Model*, by Hansen et al. [12], describes the development of a B formal model of the ERTMS case study and the use of the ProB model checker for *model-in-the-loop* validation. As part of a field demonstration of the ERTMS concept on a real train running on a test track, ProB was used at runtime to execute the formal model in real time. In our view, this represents an impressive development in the use of formal modelling for control of safety critical systems. The authors of the article also worked closely with the authors of the Hybrid ERTMS Level 3 standard [8] which resulted in improvements in the standard through the elimination of ambiguities discovered through the formalisation [3].

The article *A formal refinement-based analysis of the hybrid ERTMS/ETCS level 3 standard*, by Mammar et al. [13], describes a formalisation of the ERTMS case study using the Event-B language and the Rodin tool to prove correctness of the chain of model refinements. A focus of the article is on proving the safety of ERTMS trains.

The article *Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach*, by Fotso et al. [10], addressed the application of the KAOS requirements analysis method to the ERTMS case study. The authors used a tool that automatically converts the KAOS models that they developed into B models. This provides a systematically derived template model that was then enriched manually to capture the behaviours of the system. The B models were proved using the Rodin tool.

To make it easier for readers to compare the different modelling solutions to the ERTMS case study presented in this special issue, we asked the authors to use the following common structure:

Introduction Here, the authors were asked to introduce the methods and tools they used, to outline any distinctive features of their approach and to provide an overview of the team who performed the development.

Requirements and Modelling strategy Here, the authors were asked to explain how their formal model is structured, how traceability between the formalisation and the requirements is provided, and to describe the most important properties addressed.

Model details Here, the authors were asked to provide insights into how they approached the formalisation of the requirements and to describe any modelling styles/idioms that were used.

Validation and verification Here, the authors were asked to describe strategies and tools used for validation and verification of their models, to describe changes to the model that resulted from the validation or verification, and to describe ways in which the verification capabilities of your chosen technology influenced the modelling itself.

Other observations Here, the authors were asked to identify improvements to the requirements suggested by their formalisation and to suggest improvements to tools that would have helped the case study.

Comparison Here, the authors were asked to outline the main differences between their solution and the other solutions to the case study solutions presented at the ABZ 2018 conference.

2 System overview

There are three signalling levels for European Rail Traffic Management System (ERTMS).[2]

Level 1 Communication between trains and trackside equipment by means of transponders called Euro-balises. Trackside equipment is needed for detecting train location and train integrity,[3] and lineside signals are required.

Level 2 Communication between trains and trackside equipment is provided by the Global System for Mobile Communications—Railway (GSM-R). Trackside equipment is needed for determining train location and integrity, while lineside signals are optional.

Level 3 The train determines its location using fixed positional transponders and supervises its integrity using the on-board Train Integrity Monitoring System (TIMS). This means that trackside detection equipment is not required.

There are different options depending on levels of maturity in terms of definition and development, leading to several ERTMS *Level 3* types. Our case study focuses on *Level 3 Hybrid* which is the most mature and is developed using existing technology solution augmented for optimisation [11].

Abbreviations Figure 1 shows the list of abbreviations used in this introduction. A more complete glossary of terms and abbreviations referenced here can be found in [9].

Requirements taxonomy In this introduction, we use ASM to indicate an *assumption* and REQ to indicate a *requirement* of the system. The list of requirements in this introduction is intended to provide a high level view of the system and does not cover all system details. We refer the reader to [8] for the detailed principles of the system under consideration.

It is expensive and challenging to fit trains with ERTMS and the Train Integrity Monitoring System (TIMS), so *Level 3 Hybrid* copes with different train configurations (TIMS-equipped, ERTMS without TIMS, and non-ERTMS). *Level 3 Hybrid* uses a limited amount of trackside detection. In the case of TIMS-equipped trains, the capacity of the line can be increased using *fixed virtual blocks*. In order to achieve this purpose, each Trackside Train Detection (TTD) is divided into several Virtual Sub-Sections (VSSes). The scope of the case study is the management of the VSSes (more detailed specification is in [7]). We will not consider the interlocking system, e.g. how train routes are set and unset. More specifically, we can consider that the trains travel on a straight line and in the same direction.

EoA	End of Authority
ERTMS	European Rail Traffic Management System
EU	European Union
GSM-R	Global System for Mobile Communications - Railway
MA	Movement Autority
TIMS	Train Integrity Monitoring System
TTD	Trackside Train Detection
VSS	Virtual Sub-Section

Fig. 1 List of abbreviations

ASM 1	The trains travel along a *straight line* track and in the *same direction*
ASM 2	The train track is partitioned into several fixed TTD sections
ASM 3	Each TTD is partitioned into one or more fixed VSS

The overview of the relevant part of the system is seen in Fig. 2. The trackside has a sub-system for managing the VSS, which communicates the VSS status information to the Movement Authority (MA) authorisation sub-system. The MA authorisation sub-system sends information related to the MAs to the trains and also informs the VSS management sub-system about the issued MAs. In order to decide the VSS status, the VSS management sub-system receives the TTD status from the interlocking system and the position reports from the trains (depending on the trains' type).

We describe in more detail the various aspects of the system in the next section.

3 Level 3 Hybrid with fixed virtual blocks

3.1 TTD sections and VSSes

We consider the TTD information as reliable and safe. In particular, a TTD section is reported as free only if there are no trains or no part of a train located on the TTD. Subsequently, the VSS on a free TTD can be regarded as "free".

[2] https://ec.europa.eu/transport/modes/rail/ertms/what-is-ertms/levels_and_modes_en.

[3] Train integrity means the train is complete and has not been accidentally split.

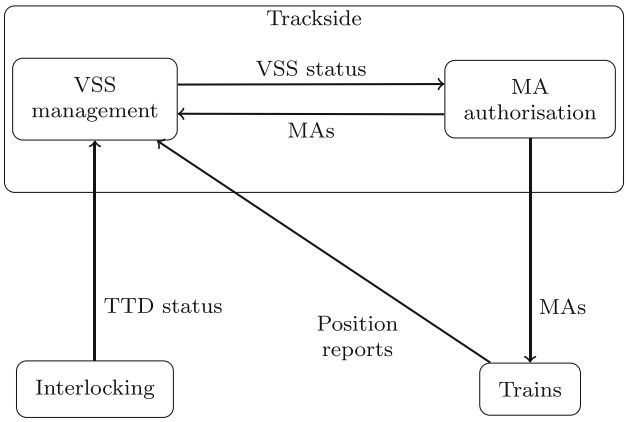

Fig. 2 System overview

ASM 4	A TTD can be reported as "free" or "occupied"
ASM 5	A TTD is reported as *free* if and only if there are no trains or a part of a train located on the TTD

Due to the discrepancy of the timing and spatial information of the trackside detection, two additional (internal) statuses of VSS are specified: "ambiguous" and "unknown". Status "ambiguous" indicates that a train is present, but its status is not known, whereas status "unknown" indicates that the occupancy sub-section is not proven.

REQ 1	A VSS can have one of the following statuses: "free", "occupied", "ambiguous", or "unknown"
REQ 2	A VSS is *free* when there are no trains or no part of a train located on the VSS
REQ 3	A VSS is *occupied* if there is exactly one train or a part of a train located on the VSS
REQ 4	A VSS is *ambiguous* if there is a train occupying the VSS, but its status is not known
REQ 5	A VSS is *unknown* if the occupancy of the VSS is not proven

3.2 Types of trains

Depending on the train's equipment, the status of a VSS is computed differently based on the train position information and the TTD information:

– A TIMS-equipped ERTMS train (an *integer* train) precisely occupies the relevant VSS in which it is located.
– An ERTMS train not fitted with TIMS also occupies the sections in the rear (until the end of the trackside detection section).
– A non-ERTMS train occupies the whole TTD section.

As a result, a non-TIMS train can follow an integer train on VSS sections, but other trains can only follow it on a separate trackside detection section. Capacity gain for *Level 3 Hybrid* can be achieved only for ERTMS trains, and full gain is achieved only for TIMS-fitted trains.

REQ 6	The system should accommodate three types of trains: TIMS-equipped ERTMS, ERTMS not fitted with TIMS, and non-ERTMS
REQ 7	A TIMS-fitted ERTMS train occupies the relevant VSSes that it is located on
REQ 8	An ERTMS train without TIMS occupies the relevant VSSes that it is located on, and also all the VSSes in the rear until the end of the TTD section
REQ 9	A non-ERTMS train occupies the whole TTD section that it is located on

The status of a VSS is computed based on the TTD status and the train position reports.

3.3 Movement authority

We will not need to consider *how* the MAs of the trains are computed or how they are related to routes. (A route is a contiguous sequence of connected sections). The MA of a train defines (beside other information) a position on the track, called the End of Authority (EoA), which must not be passed by the train. Depending on the type of a train and its location within the track, the EoA can be defined in terms of a VSS or of the trackside sections. However, since VSS status depends on a train's MA, we will need to consider what has been set as the train MA with the assumption that the trains will be safe from collision if they respect the provided MAs. For the purpose of issuing MAs, only "free" state of VSSes is required to be distinguished from the other states, i.e. "occupied", "ambiguous", or "unknown" (which will be treated as "occupied").

ASM 6	For non-ERTMS trains, their EoAs are defined in terms of TTD sections
ASM 7	For ERTMS trains, their EoAs are defined in terms of the VSSes
ASM 8	The MAs are disjoint, i.e. trains will be safe from collision if they respect the provided MAs

3.4 Timers

A timer can have one or more *start events* and zero or more *stop events*. Any start/stop event of a timer will start/stop the corresponding timer. A timer without a stop event once started will run until it is expired. Once expired, this timer will stay in the same state until it is reset when the start condition is met again.

REQ 10	A timer has one or more start events
REQ 11	A timer has zero or more stop events
REQ 12	A timer without a stop event once started will run until expired and stay in the "expired" state until reset when the start condition is met again

There are two main types of timers implemented in the trackside, namely, *waiting* timers and *propagation* timers. The waiting timers are to avoid unnecessary changes of VSS status due to the delay in communication of train position, train integrity information, etc. The propagation timers are to avoid unnecessary propagation of the "unknown" state to the VSS sections with no immediate risk of having a train or a part of a train located on them. We describe some of the important timers here. The complete list of the timers is in [7, Section 3.4].

Mute timers A waiting timer called "mute timer" is assigned to each train. Each *mute timer* runs continually and whenever some information is received from the train, the timer is reset. This timer is used to decide if communication between the trackside and the train is lost.

REQ 13	A *mute timer* is assigned to each train
REQ 14	Each mute timer runs continually
REQ 15	A mute timer is reset whenever some information is received from the train

Wait integrity timers A waiting timer called a "wait integrity timer" is assigned to each train. Each *wait integrity timer* runs continually and whenever integrity confirmation is received from the train, and no change of train length has been reported since the previous position report, the timer is reset. This timer is used to decide if the train has lost integrity.

Disconnected propagation timers A "disconnected propagation timer" is assigned to each VSS. The start event for a "disconnected propagation timer" is that the "mute timer" of a train located on the VSS expired. The stop event for this timer is when the connection of the train is reestablished. This timer is used to propagate the "unknown" status of VSS due to train disconnection.

REQ 16	A *wait integrity timer* is assigned to each train
REQ 17	Each wait integrity timer runs continually
REQ 18	A wait integrity timer is reset whenever integrity confirmation is received from the train, and no change of train length has been reported since the previous position report

REQ 19	A *disconnected propagation timer* is assigned to each VSS
REQ 20	The start event of a disconnected propagation timer is when the mute timer of a train located on the VSS expires
REQ 21	The stop event of a disconnected propagation timer is when connection of the train is restored

Ghost train propagation timers A "ghost train propagation timer" is assigned to each TTD. The start event for a "ghost train propagation timer" is either (1) the TTD become "occupied" without any train on it or (2) the TTD become "occupied" without any MA associated with it. There is no stop event for this timer. This timer is used to propagate the "unknown" status of VSS due to ghost trains (see Sect. 3.5).

REQ 22	A *ghost train propagation timer* is assigned to each TTD
REQ 23	The start event of a ghost train propagation timer is when the TTD becomes "occupied" without any train or MA associated with it
REQ 24	There is no stop event for a ghost train propagation timer

3.5 Ghost trains and shadow trains

In some situation, objects might be detected by the TTD but are unknown to the trackside system (this could due to some physical objects occupied the track or some virtual objects due to trackside failure). They are called ghost trains. For example, when a train is split, the rear part will become a ghost train. When a ghost train is following a normally operated Level 3 train (i.e. an integer train), it is called a *shadow train*. To protect the system against ghost trains, the VSS status "unknown" is used and propagated according to the "ghost train propagation timer" (see [7, Section 4.2.2]). To protect the system against a shadow train hazard, the VSS

REQ 25	Ghost trains are objects detected by the TTD but are unknown to the trackside

status "ambiguous" is used (more information is in [7, Section 4.5]).

3.6 Train connectivity

The communication between the trackside and a train is considered to be lost when the mute timer for the train expires. When the train is disconnected from the trackside, the VSS sections within the train's MA up to either the limit of the first free TTD or the first VSS of the MA are set to "unknown" (they are propagated according to the "disconnected propagation timer"). A disconnected train can reconnect, i.e. the trackside receives a position report from the train after its mute timer has expired. In this case, the status of different VSSes is updated depending on whether they are occupied by the train or in the front of the train or in the rear of the train. Also, the updated VSS status will depend on whether or not the train confirms its integrity with no change in its length. In any situation, the unknown VSSes in rear of the train would become "free" if the TTD section is released. More information is in [7, Section 3.8 and 4.2.1]

REQ 26	The communication between the trackside and a train is considered to be lost when the mute timer for the train expires
REQ 27	When the trackside receives a position report from a disconnected train, the communication between the trackside and the train is reestablished

3.7 The state machine for VSS

For a VSS, its state machine is seen in Fig. 3. Depending on the situation, the status of a VSS can be changed between any two of the four states, i.e. "free", "unknown", "ambiguous", "occupied". Extensive details of the transitions can be found in [7, Section 5] and are not repeated here. In particular, for each transition, there are several situations where the VSS status is changed according to the transition.

4 Conclusions

In this paper, we provided an overview of the key principles of Hybrid ERTMS/ETCS Level 3 at a sufficient level of detail to allow the reader to follow the papers in this special section. We set the specific requirements for Level 3 Hybrid in the context of the three levels of ERTMS and presented the key assumptions and requirements that the participants in the case study were asked to address. As outlined in Sect. 1, we provided guidance to the contributors on a common structure

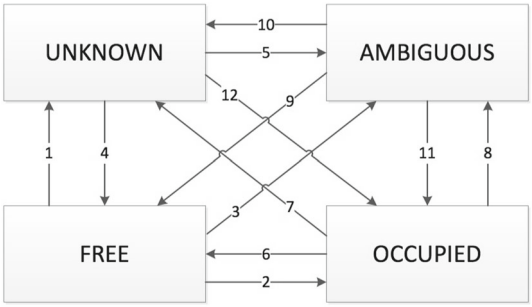

Fig. 3 The state machine of a VSS [7]

for their paper to make it easier for the reader to compare the strengths and weakness of the different contributions. The case study represents a valuable challenge for formal methods, in particular because of the complexities caused by the need for the system to cope with ERTMS-equipped trains and non-equipped trains. We believe the contributions presented in this special section enrich the set of case studies developed with ABZ and related methods, and we hope they help readers to get a better appreciation of the strengths and weaknesses of the various formal methods deployed by the contributors.

Acknowledgements The organisers would like to thank the EEIG ERTMS Users Group (EUG) for sharing an early version of the Hybrid ERTMS/ETCS Level 3 principles [7] when we were preparing the ABZ 2018 case study.

References

1. Abrial, J.-R.: The ABZ-2018 case study with Event-B. Softw. Tools Technol. Transf. (2020). In this issue
2. Arcaini, P., Kofron, J., Jezek, P.: Validation of the Hybrid ERTMS/ETCS Level 3 using SPIN. Softw. Tools Technol. Transf. (2020). In this issue
3. Bartholomeus, M., Luttik, B., Willemse, T., Hansen, D., Leuschel, M., Hendriks, P.: The use of formal methods in specification and demonstration of ERTMS Hybrid Level 3. IRSE News, 260, Nov (2019)
4. Butler, M.J., Raschke, A., Hoang, T.S., Reichl, K. (eds.): Abstract state machines, alloy, B, TLA, VDM, and Z: 6th International Conference, ABZ 2018, Southampton, 5–8 June 2018, Proceedings. vol. 10817 of Lecture Notes in Computer Science. Springer (2018)
5. Cunha, A., Macedo, N.: Validating the Hybrid ERTMS/ETCS Level 3 concept with Electrum. Softw. Tools Technol. Transf. (2020). In this issue
6. Dghaym, D., Dalvandi, M., Poppleton, M., Snook, C.: Formalising the Hybrid ERTMS Level 3 specification in iUML-B and Event-B. Softw. Tools Technol. Transf. (2020). In this issue
7. EEIG ERTMS Users Group, Brussels, Belgium. Hybrid ERTMS/ETCS Level 3: Principles, July 2017. Ref. 16E042 Version 1A
8. EEIG ERTMS Users Group, Brussels, Belgium. Hybrid ERTMS/ETCS Level 3: Principles, July 2018. Ref. 16E042 Version 1C, http://irse.info/kb5q6

9. ERA, UNISIG, EEIG ERTMS Users Group. Glossary of Terms and Abbreviations: ERTMS/ETCS, 3.3.0 edition, May 2016. http://www.era.europa.eu/Document-Register/Documents/SUBSET-023%20v330.pdf
10. Fotso, S.J.T., Frappier, M., Laleau, R., Mammar, A.: Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach. Softw. Tools Technol. Transf. (2020). In this issue
11. Furness, N., van Houten, H., Arenas, L., Bartholomeus, M.: ERTMS Level 3: the game-changer. IRSE News, 232, April (2017)
12. Hansen, D., Leuschel, M., Körner, P., Krings, S., Naulin, T., Nayeri, N., Schneider, D., Skowron, F.: Validation and real-life demonstration of ETCS Hybrid Level 3 Principles using a formal B Model. Softw. Tools Technol. Transf. (2020). In this issue
13. Mammar, A., Frappier, M., Fotso, S.J.T., Laleau, R.: A formal refinement-based analysis of the hybrid ERTMS/ETCS level 3 standard. Softw. Tools Technol. Transf. (2020). In this issue