The original publication is available at
http://doi.org/10.1007/978-3-319-91271-4_17
In ABZ2018: Proceedings of the 6th International ABZ Conference ASM,
Alloy, B, TLA, VDM, Z, 2018 © Springer 2018

The Hybrid ERTMS/ETCS Level 3 Case Study

Thai Son Hoang[1], Michael Butler[1], and Klaus Reichl[2]

[1] ECS, University of Southampton, U.K.
{t.s.hoang,mjb}@ecs.soton.ac.uk
[2] Thales Austria GmbH
klaus.reichl@thalesgroup.com

Abstract. This document presents a description of the European Rail Traffic Management System (ERTMS) case study. ERTMS is a system of standards for management and interoperation of signalling for railways by the European Union (EU). The case study focuses on the *ERTMS Level 3 Hybrid* principle, which accommodates different types of trains including ERTMS trains equiped with the Train Integrity Monitoring System (TIMS), ERTMS trains without TIMS, and non-ERTMS trains.

Keywords: ERTMS; ETCS; Level 3 Hybrid;

1 Introduction

The case study concerns the European Rail Traffic Management System (ERTMS)[3], the system of standards for management and interoperation of signalling for railways by the European Union (EU)[4]. The aim of ERTMS is to replace the different national train control and command systems in Europe with a seamless European railway system. The advantages of ERTMS include increased capacity, higher reliability rates, improved safety, and open supply market.

There are three signaling levels for ERTMS[5].

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[6] 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.

[3] http://ertms.net.
[4] http://https://en.wikipedia.org/wiki/European_Rail_Traffic_Management_System.
[5] https://ec.europa.eu/transport/modes/rail/ertms/what-is-ertms/levels_and_modes_en.
[6] Train integrity means the train is complete and has not been accidentally split.

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 [3].

Abbreviations. Fig. 1 shows the list of abbreviations used in this document. A more complete glossary of terms and abbreviations referenced here can be found in [2].

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

Requirements Taxonomy. In this document, we use ASM to indicate an *assumption* and REQ to indicate a *requirement* of the system. The list of requirements in this document is intended to provide a high level view of the system and does not cover all system details. We refer the reader to [1] for the detailed principles of the system under consideration.

Structure. The rest of this document is as follows. Section 2 gives an overview of the system. Section 3 presents a more detailed description of various aspects of the system under consideration. We briefly review the state machine for the Virtual Sub-Section (VSS), the key idea for the ERTMS Level 3 Hybrid principle, in Section 4. Section 5 gives a short conclusion on our expectation for the case study.

2 System Overview

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 VSSes. The scope of the case study is the management of the VSSes (more detailed specification is in [1]). 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.

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 can be 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".

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.

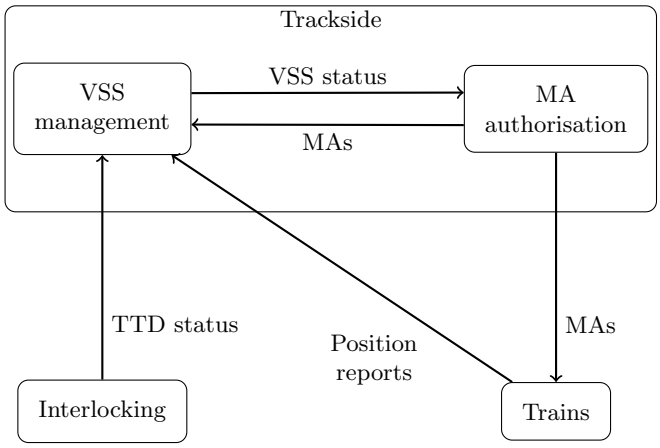

Fig. 2. System Overview

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 6	A VSS can have one of the following statuses: "free", "occupied", "ambiguous", or "unknown"

REQ 7	A VSS is *free* when there are no trains or no part of a train located on the VSS.

REQ 8	A VSS is *occupied* if there is exactly one train or a part of a train located on the VSS.

REQ 9	A VSS is *ambiguous* if there is a train occupying the VSS but its status is not known.

REQ 10	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 11	The system should accomodate three types of trains: TIMS-equipped ERTMS, ERTMS not fitted with TIMS, and non-ERTMS.

REQ 12	A TIMS-fitted ERTMS train occupies the relevant VSSes that it is located on.

REQ 13	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 14	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 15	For non-ERTMS trains, their EoAs are defined in terms of TTD sections.

ASM 16	For ERTMS trains, their EoAs are defined in terms of the VSSes.

ASM 17	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 18	A timer has one or more start events.

REQ 19	A timer has zero or more stop events.

REQ 20	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 [1, 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 21	A *mute timer* is assigned to each train.

REQ 22	Each mute timer runs continually.

REQ 23	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.

REQ 24	A *wait integrity timer* is assigned to each train.

REQ 25	Each wait integrity timer runs continually.

REQ 26	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.

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 27	A *disconnected propagation timer* is assigned to each VSS.

REQ 28	The start event of a disconnected propagation timer is when the mute timer of a train located on the VSS expires.

REQ 29	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 Section 3.5).

REQ 30	A *ghost train propagation timer* is assigned to each TTD.

REQ 31	The start event of a ghost train propagation timer is when the TTD becomes "occupied" without any train or MA associated with it.

REQ 32	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*.

REQ 33	Ghost trains are objects detected by the TTD but are unknown to the trackside.

REQ 34	A ghost train following an integer train 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 [1, Section 4.2.2]). To protect the system against a shadow train hazard, the VSS status "ambiguous" is used (more information is in [1, 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 are 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 [1, Section 3.8 and 4.2.1]

REQ 35	The communication between the trackside and a train is considered to be lost when the mute timer for the train expires.

REQ 36	When the trackside receives a position report from a disconnected train, the communication between the trackside and the train is reestablished

4 The State Machine for VSS

For a VSS, its state machine can be 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

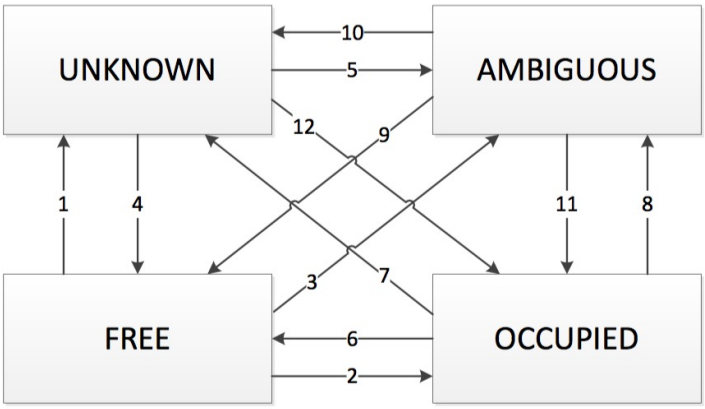

Fig. 3. The State Machine of a VSS [1]

be found in [1, 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.

5 Conclusion

We have given an overview of the ERTMS Level 3 Hybrid principles. We are looking for solutions that address the various challenges of the case study, and also provide insights into the case study and/or the formal methods used. For the case study, we expect the solutions will illustrate what can be guaranteed by the system (e.g., in terms of collision-free), and/or explanation about various hazard-mitigating mechanisms of the system. Regarding formal methods, we expect to see a justification of the "need" and the "value" of the methods and/or tools in addressing a complex industrial challenge.

Acknowledgements

The organisers would like to thank the EEIG ERTMS Users Group (EUG) for the Principles on "Hybrid ERTMS/ETCS Level 3" document [1] released on 14/07/2017.

References

1. EEIG ERTMS Users Group, Brussels, Belgium. *Hybrid ERTMS/ETCS Level 3: Principles*, July 2017. Ref. 16E042 Version 1A.
2. 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.
3. Nicola Furness, Henri van Houten, Laura Arenas, and Maarten Bartholomeus. ERTMS Level 3: the game-changer. *IRSE News View 232*, 232, April 2017.