IRSE
Institution of Railway Signal Engineers

The use of formal methods in specification and demonstration of ERTMS Hybrid Level 3

Prepared on behalf of the International Technical Committee
by Maarten Bartholomeus, Bas Luttik, Tim Willemse,
Dominik Hansen, Michael Leuschel and Paul Hendriks

Software has become an essential component in signalling systems. Writing clear, precise and accurate specifications is of course important for these systems. Can formal methods help in this process? An interesting case is the recent development of the Hybrid Level 3 for ERTMS/ETCS. This paper addresses the specification and demonstration of ERTMS Hybrid Level 3.

Hybrid Level 3 and formal methods

During development of Hybrid Level 3 it was realised that a pure functional specification did not provide enough insight into possible degraded scenarios and their impact on current operational processes. The list of generated scenarios kept growing and growing. A more precise method to specify the system behaviour on a functional level was required. For this purpose, a specification with state diagrams was developed describing the possible states of the track sections and transitions, see [1]. This allowed the railway specialists to evaluate the operational impact and the system specialist to check if a system could be made according to these specifications.

The number of operational scenarios implicitly described by the state diagram is very large. Hence, there is a high risk that unsafe operational scenarios are missed in a review of the principles by railway experts. Using formal methods, computer tools can be used to exhaustively analyse all operational scenarios for a given track layout.

Formal methods are already well established to avoid errors in the software coding phase, but this does not guarantee that software safety requirements themselves are correct. The formal methods can also be used to prove that the software specification and its implementation satisfy the expected system properties.

The Hybrid Level 3 specification [1] was selected as a case study for the formal methods conference ABZ [2]. One of these cases was an implementation in a real-life test environment and was one of the successful demonstrators of Hybrid Level 3 in the UK on the ERTMS National Integration Facility (ENIF) test track in 2017 [3]. The Hybrid Level 3 specification was also analysed in cooperation with the University of Eindhoven [4]. This paper will reflect on these studies and the benefits of using formal methods in this project.

ETCS Hybrid Level 3 offers an interesting alternative approach to realising the benefits of new technology on existing lines. This extract from Maarten's video [5] of testing at the UK's ENIF facility shows that it is very real.

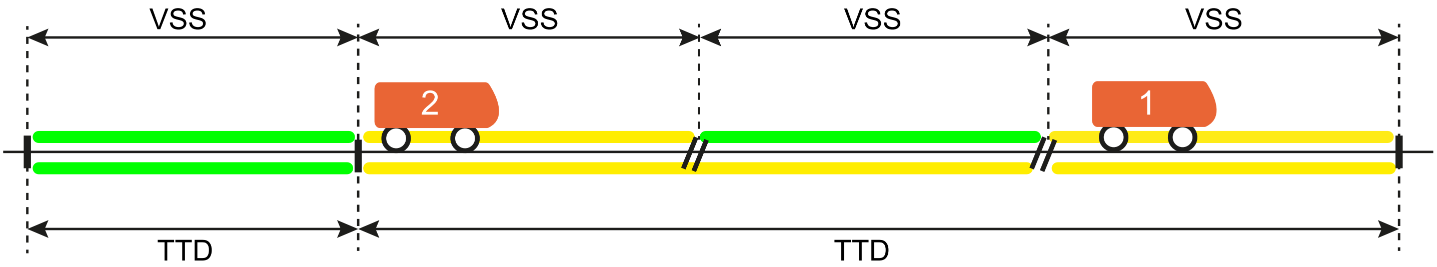


Figure 1 – The principle of ETCS Hybrid Level 3 is to divide trackside train detection sections into several virtual sub sections, increasing capacity.

Hybrid Level 3

Hybrid Level 3 is a development that allows ERTMS trains to follow each other based on the train positions reported by the on-board systems providing an optimal performance without the 'pure' Level 3 drawbacks: a 'pure' Level 3 system requires that all trains are fitted with a Train Integrity Monitoring System (TIMS) and that the RBC (Radio Block Centre) knows at all times the position and integrity status of each train or vehicle that is physically present in the area under its control. The problem is that in practice these conditions cannot always be fulfilled considering the wide range of vehicles and scenarios, for instance switched-off trains, parked wagons, communication failures, when performing shunting operations or after a restart of the system. Procedures to overcome this lack of train information would cause a significant operational disruption.

The Hybrid Level 3 concept combines on-board train position information, on-board train integrity confirmation and trackside train detection, and supports trains with and without on-board integrity proving. It mitigates operational risks in degraded scenarios and allows for fast and robust system recovery.

Thus, it provides a migration path for trains operating on the line while increasing capacity and providing robust operation.

Hybrid Level 3 principles

For Hybrid Level 3, trackside train detection sections (TTD) can be divided into several virtual sub sections (VSS), see Figure 1. As the VSS are software-defined, they can be configured to a size providing a performance comparable to the 'moving block' concept. The status occupied or free of the VSS section is based on both on-board derived train position information and trackside train detection information. A VSS section is reported free if the underlying trackside train detection is reported free or if all conditions are met to safely clear this VSS based on information reported by a train. A VSS section is reported occupied if a train reports itself inside this section (based on reported front-end position and train length).

Because the timing and spatial accuracy of the trackside train detection and ERTMS train position vary considerably, two additional internal VSS statuses are introduced: "ambiguous" and "unknown". These two additional statuses can be represented as occupied to avoid new requirements and/or operational procedures. The trackside train detection occupancy information is used only as an input for the VSS status. This feature allows the Hybrid Level 3 solution to interface with existing systems.

The different VSS state transitions are defined based on reported train information and trackside information; this is explained in more detail in the Hybrid Level 3 Principles [1]. For instance, the transition from "occupied" to "free" takes place if a train with confirmed integrity reports that it has left this VSS. Another example is the transition from "occupied" to "ambiguous". This happens when a train loses its integrity or does not report integrity. VSS sections left by a train without proven integrity in an ambiguous VSS section will become "unknown" until the underlying trackside train detection reports free. The transitions between VSS statuses are described meticulously in [1]. See for instance transition #1A below:

#1A : (TTD is occupied) AND (no FS MA is issued
or no train is located on this TTD)

This specification detail allowed the Hybrid Level 3 specification to be analysed and tested with formal methods.

Using a Formal B model in a demonstration of ETCS Hybrid Level 3

In 2017, Thales contributed to a field demonstration of the Hybrid Level 3 concept by providing the Trackside System supporting the new Hybrid Level 3 specification. The Thales approach was to develop an add-on for the RBC, called Virtual Block Function (VBF), which computes the occupation states of the VSSs according to the Hybrid Level 3 specification. From the perspective of the RBC, the VBF behaves as an Interlocking (IXL) that transmits all signal aspects for the virtual signals – introduced for each VSS – to the RBC. This architecture provides the benefit that the RBC can be used without modification to its core functionalities (see figure 2).

Two main tasks were identified for the development of the new VBF component:

1. Providing evidence that the Hybrid Level 3 specification is consistent and complete to handle possible hazards and to allow the desired operational behaviour.
2. Building software that conforms to the Hybrid Level 3 specification and can be used in a field demonstration by supporting the existing interfaces to the other components of the system (RBC, IXL).

The high level of detail within the Hybrid Level 3 specification, which describes the expected behaviour in every situation, eases the development of conforming software but increases the challenge of providing evidence that the specification itself is correct and complete.

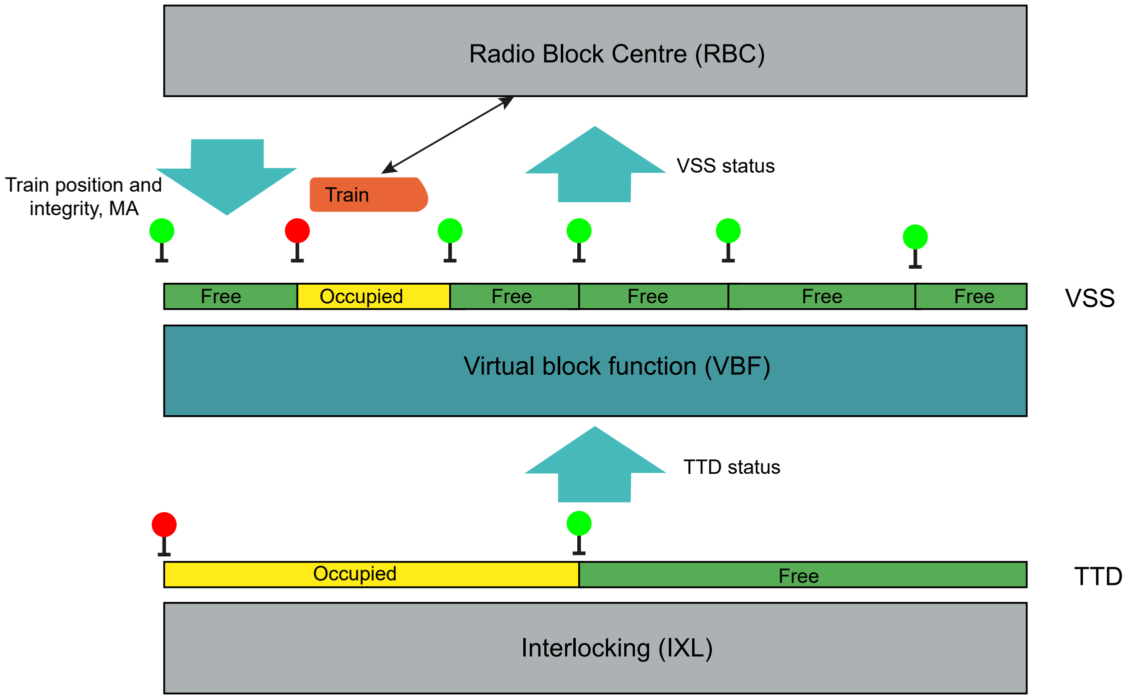


Figure 2 – The role of the Virtual Block Function (VBF).

For this Thales developed a formal B model of the Hybrid Level 3 specification in cooperation with the University of Düsseldorf.

The formal model allowed an analysis of the specification before a single line of interface code was written. The ProB model checker and animator allows the interactive replay of all operational scenarios contained in the Hybrid Level 3 specification as well as the derivation of new scenarios.

A non-deterministic environment model provides all possible input events for the state machine, which could be interactively selected by a user or automatically selected by the model checker to search for violations of generic invariants (e.g. a train should never be located on a free VSS). The developed graphical visualisation (similar to the picture in Figure 1) even allows a domain expert without a formal methods background to inspect the behaviour of the Hybrid Level 3 specification and perform their own 'experiment scenario analysis'. Moreover, scenarios can be stored and used as regression tests in case of modification to the state machine. Indeed, this was very useful as several issues were found in the Hybrid Level 3 specification and it was necessary to adjust either the state machine or the scenarios. In resolving such issues, the model combined with the visualisation served as an unambiguous, interactive specification to communicate the problem within the team.

To accomplish the second task of developing a demonstrator the formal model was used in real time (executed by ProB) for the field demonstrations. This was possible as the model covers the entire Hybrid Level 3 specification with all necessary details so that it can be combined with the manually produced interfaces. The visualisation, which was also used during the offline analysis, was reused during the field demonstrations to check the correct functioning of the trackside system in real time. Moreover, the observed real-life events (e.g. train position reports of real trains) were captured by ProB and could be replayed (step by step) by a domain expert in the ProB animator at a later stage (instead of inspecting large log files).

Thanks to this innovative approach, the field demonstrations were successfully completed within a tight time schedule in the UK [5] and Germany [6] .

Modelling and analysing ERTMS Hybrid Level 3 with the mCRL2 toolset

Eindhoven University of Technology develops the formal specification language mCRL2 and an associated toolset. The toolset comes with a simulator and with a model checker. With the simulator, operational scenarios can be executed. The model checker can be instructed to exhaustively search for operational scenarios that violate a property, which is also formally specified. If such an operational scenario is found, then it can be visualised.

The Hybrid Level 3 principles defined by the VSS state diagram, together with the table that specifies the conditions for transitioning between statuses, turned out to be precise enough to admit a fairly direct translation into mCRL2. Formal methods researchers without extensive railway expertise could, in fact, do an initial translation without consulting a railway expert.

For a meaningful formal safety analysis, it is necessary to also specify to some extent the context into which a Hybrid Level 3 system is embedded. To this end, the mCRL2 model includes an abstract description of the operation of a trackside system and the behaviour of trains.

The trackside system implements the Hybrid Level 3 principles, computing new VSS statuses on the basis of events (e.g., a train reports its position, the train detection system reports a change in occupancy of a particular section). Although in a real implementation one would have to determine in which order VSS statuses are updated in response to an event, this is not necessary in formal specification languages, such as mCRL2, that include a facility to specify non-deterministic behaviour. Non-determinism can be used to avoid committing to one particular implementation of the update mechanism, and thus the formal analysis done with mCRL2 is not limited to one particular implementation. The trackside system issues movement authorities to trains based on information regarding the statuses of the VSSs.

The specification of the behaviour of trains also makes use of non-determinism to generate all possible movements of trains through a network. Trains can receive movement authorities from the trackside, can move from one VSS to the next, and report their position to the trackside. Furthermore, they are also indirectly detected by the trackside through the train detection system.

The mCRL2 model can thus be thought of as an abstract description of all trackside systems implementing the Hybrid Level 3 principles. To actually simulate operational scenarios, or perform an exhaustive search for unsafe operational scenarios, it is necessary to add a track layout, specifying how many trains and track sections are controlled by the trackside system and how the track sections are subdivided into VSSs. For simulation purposes, track layouts of the size considered by the inventors of the Hybrid Level 3 principles (three sections, each subdivided into three VSSs, with three trains) are unproblematic. For a complete exhaustive analysis, currently only smaller track layouts have been considered. Nevertheless, analysis of smaller track layouts has already revealed issues in earlier versions of the Hybrid Level 3 principles.

Conclusion

The use of formal methods proved to be very useful to analyse and validate the Hybrid Level 3 specification. Whilst the two tool sets that were used have very similar capabilities, the approaches had a slightly different focus. The goal of the developed B model was to obtain a reference implementation which conforms to Hybrid Level 3 specification with all necessary details to be used in the field demonstration. In contrast, the mCRL2 approach focused more on analysing the correctness of the principles independent of the implementation strategy.

We summarise the benefits of using these formal methods:

Eliminating ambiguities in the natural language phrasings. Formal languages provide an unambiguous mathematical notation with well-defined semantics. Thus, the formalisation alone led to improvements of the principles, by eliminating ambiguities.

Visualisation and tooling. To execute scenarios and analyse the behaviour of the model these tools provide useful visualisations of issues and inconsistencies in the model and allow a simple demonstration of the identified scenarios. Visualisations help to get a common view within a heterogeneous team where members had different backgrounds.

Model checking. As the number of operational scenarios implicitly described by the VSS state machine is enormous, review of a number of example scenarios by experts would not be sufficient to reach the complete coverage of the state machine. By model checking it is possible to exhaustively search through all operational scenarios associated with a known track layout in order to determine whether there are violations of a particular safety property. Using this method, a safety invariant such as “no train shall have a normal authorisation over a section occupied by another train” was verified for various track layouts. In the early stages of development, the application of this approach typically quickly produces interesting operational scenarios that require further consideration and yields fast feedback on proposed changes. In later stages, it significantly increases confidence in the correctness of the principles.

Fast feedback on changes in specification. It was very valuable that the model checking allowed fast feedback on changes in the specification and regression testing. The tools can quickly produce examples of interesting operational scenarios.

Bridging the gap to the software level. By converting the formal model into an executable prototype, it was possible to perform field demonstrations with real trains. This shows that formal methods can be used for the creation of rapid prototypes to test not only at the component level but also on the system level. There are also appropriate tools available to generate low level code – which can be used within SIL4 capable product development – from a formal model.

The ITC and the authors thank ProRail, Thales, and the involved universities that contributed to this article.

References

[1] Principles Hybrid ERTMS/ETCS Level 3, Ref 16E042, Version 1C, EEIG User Group. **irse.info/kb5q6**.

[2] Case study Hybrid Level 3 with formal methods, International ABZ Conference ASM, 2018.

[3] Using a Formal B Model at Runtime in a Demonstration of the ETCS Hybrid Level 3 Concept with Real Trains, University Düsseldorf, Thales, Published in ABZ 2018.

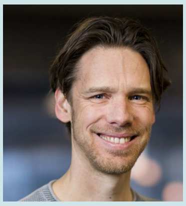
[4] Modelling and Analysing ERTMS Hybrid Level 3 with the mCRL2 toolset, Maarten Bartholomeus, Bas Luttik and Tim Willemse, Formal Methods for Industrial Critical Systems, FMICS 2018.

[5] ATO/ERTMS Level 3 test at the ETCS National Integration facility. Video by Maarten Bartholomeus, July 2018. **irse.info/g492d**.

[6] Demonstration der ETCS Level 3 Technologie im Living Lab der DB Netz, Video by DB, September 2018. **irse.info/ugzy8**, with English subtitles **irse.info/ce4it**.

About the authors ...

Maarten Bartholomeus is ERTMS signalling expert, Prorail BV, Netherlands.



Bas Luttik is assistant professor, Department of Mathematics and Computer Science, Eindhoven University of Technology, Netherlands.

Tim Willemse is associate professor, Department of Mathematics and Computer Science, Eindhoven University of Technology, Netherlands.

Dominik Hansen is system architect, Thales Transportation, Germany.

Michael Leuschel is professor, Department of Computer Science, University of Düsseldorf, Germany.

Paul Hendriks is manager signalling, ProRail BV, Netherlands.