Formalizing and Analyzing System Requirements of Automatic Train Operation over ETCS Using Event-B

Robert Eschbach(✉)

ITK Engineering GmbH, Im Speyerer Tal 6, 76761 Ruelzheim, Germany
robert.eschbach@itk-engineering.de
https://www.itk-engineering.de/en/

Abstract. The European Railway Traffic Management System (ERTMS) aims at the replacement of incompatible national railway traffic management systems in Europe. A part of ERTMS is the European Train Control System (ETCS). ETCS is an automatic train protection system and can collaborate with an automatic train operation system (ATO). ATO can control and monitor the braking, traction and door system of a train. This collaboration is called ATO over ETCS. In this paper we describe the experiences gained in the formalization and the formal analysis of system requirements related to the modes of the ATO onboard unit and its interfaces to train, ATO trackside unit, and ETCS onboard unit. A primary goal to achieve was the stepwise and systematic construction of an Event-B specification tightly coupled with the requirements based on a bidirectional traceability concept. Another goal was the formal verification of important safety properties related to the mode transitions and transition conditions of the ATO onboard unit.

Keywords: ATO over ETCS · Formalization · Traceability · Formal verification · Event-B

1 ATO over ETCS

The European Railway Traffic Management System (ERTMS) aims at the replacement of incompatible national railway traffic management systems in Europe. A central part of ERTMS is ETCS. In this paper we will focus on the collaboration of ETCS with ATO called ATO over ETCS (AoE). The system requirements for ATO over ETCS (AoE) have been specified within the Shift2Rail research project X2RAIL-1. Further information can be obtained from https://projects.shift2rail.org (accessed Feb 11, 2021). The system requirements are specified in SUBSET-125[1]. As can be seen in the reference architecture of

[1] Technical specifications for ETCS are published in the Control Command and Signalling Technical Specification for Interoperability hosted by the European Rail Agency. These specifications are grouped into several uniquely numbered subsets.

A. Raschke and D. Méry (Eds.): ABZ 2021, LNCS 12709, pp. 137–142, 2021.
https://doi.org/10.1007/978-3-030-77543-8_13

AoE depicted in Fig. 1 the ATO is divided in ATO onboard unit (ATO-OB) and ATO trackside unit (ATO-TS). The following ATO-OB interface specifications have been analyzed: ATO-TS (SUBSET-125), ETCS onboard unit (ETCS-OB) (SUBSET-130, SUBSET-143) and Train (SUBSET-139). A main part of the system requirements is related to ATO-OB operation modes and mode transitions (see Fig. 2).

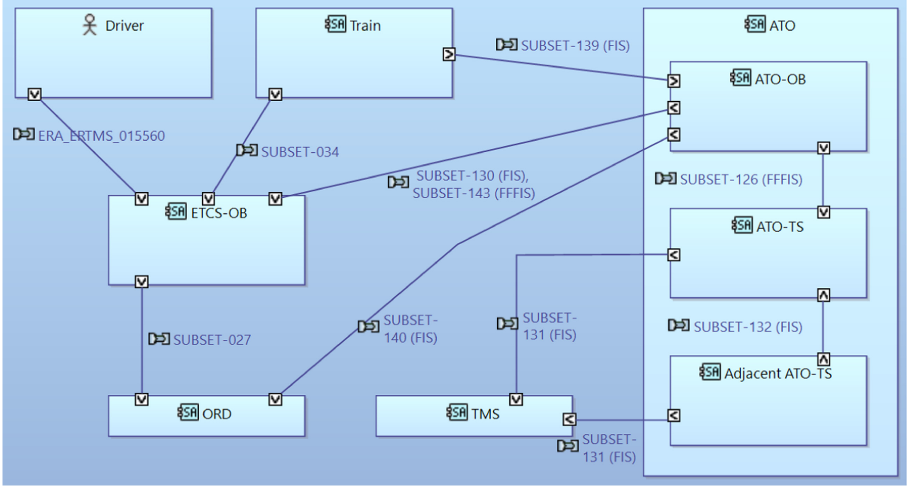


Fig. 1. AoE reference architecture

Related Work. Formal methods have been applied to ETCS in several research and industrial projects. For example, in [9] the authors designed a controller for a cooperation protocol of control parameters. They identified constraints in order to ensure collision freedom. In [7] a concrete implementation of the ETCS Hybrid Level 3 concept is presented. The authors introduce so called virtual block functions which computes the occupation states of virtual subsections. In [3] the authors describe the experiences gained in modelling a satellite-based ERTMS L3 moving block signalling system with Simulink and Uppaal and analysing the Uppaal model with the statistical model checker Uppaal SMC. In [5] the authors present a proof of concept of Virtual coupling. They introduce a specific operating mode for ETCS and define a coupling control algorithm that addresses time-varying delays affecting the communication links. In [1] the authors model the principles of ERTMS Hybrid Level 3 in the mCRL2 process algebra. They perform an analysis with the mCRL2 toolset which can be used for modelling, validation and verification of concurrent systems and protocols. The identified issues have been communicated to the EEIG ERTMS Users Group and have led to several improvements of the affected specifications. In [4] the authors present a detailed report on the convergence of FM related studies carried out in the

Shift2Rail projects X2Rail-2 and ASTRail. In both projects a systematic survey of the state of the art of formal methods application in railway industry and related best practices was carried out. In [2] the authors present the results of a questionnaire which was part of the analysis phase of ASTRail research project. One of the most important results is that classical B and Event-B with the respective tools Atelier-B, ProB and Rodin were used most often in projects.

The formalization approach described in this paper consists of the following six steps (1) identify components, (2) derive function tables for relevant requirements, (3) derive a variable table with read/write permissions for the identified components, (4) derive Event-B specification, (5) validation, and (6) verification.

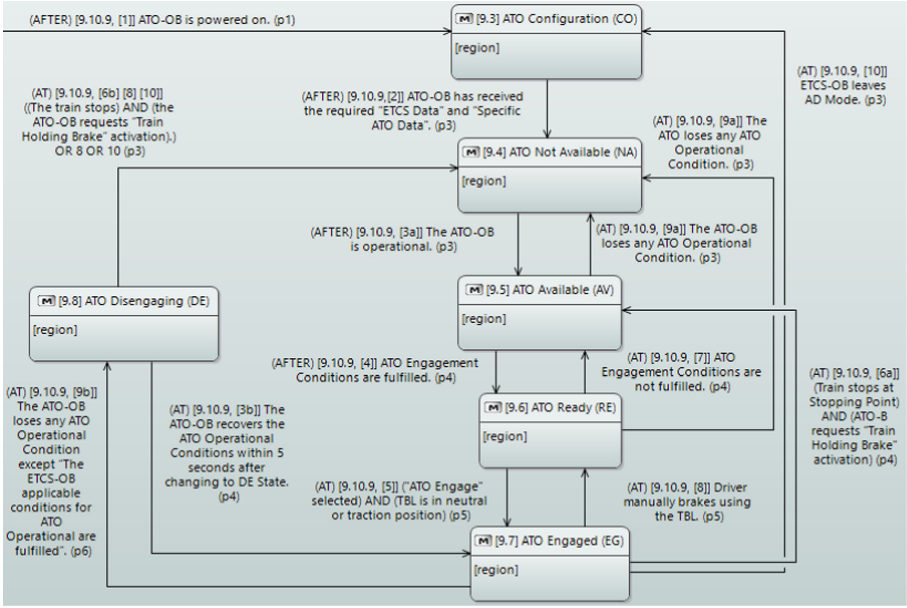
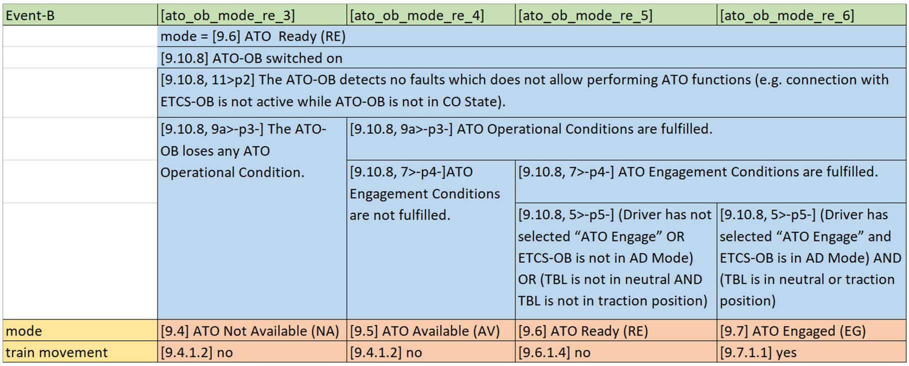

(AFTER) [9.10.9, [1]] ATO-OB is powered on. (p1)
[9.3] ATO Configuration (CO)
[region]
(AT) [9.10.9, [10]] ETCS-OB leaves AD Mode. (p3)
(AT) [9.10.9, [6b] [8] [10]] ((The train stops) AND (the ATO-OB requests "Train Holding Brake" activation).) OR 8 OR 10 (p3)
(AFTER) [9.10.9,[2]] ATO-OB has received the required "ETCS Data" and "Specific ATO Data". (p3)
(AT) [9.10.9, [9a]] The ATO loses any ATO Operational Condition. (p3)
[9.4] ATO Not Available (NA)
[region]
(AFTER) [9.10.9, [3a]] The ATO-OB is operational. (p3)
(AT) [9.10.9, [9a]] The ATO-OB loses any ATO Operational Condition. (p3)
[9.8] ATO Disengaging (DE)
[region]
[9.5] ATO Available (AV)
[region]
(AFTER) [9.10.9, [4]] ATO Engagement Conditions are fulfilled. (p4)
(AT) [9.10.9, [7]] ATO Engagement Conditions are not fulfilled. (p4)
(AT) [9.10.9, [6a]] (Train stops at Stopping Point) AND (ATO-B requests "Train Holding Brake" activation) (p4)
(AT) [9.10.9, [9b]] The ATO-OB loses any ATO Operational Condition except "The ETCS-OB applicable conditions for ATO Operational are fulfilled". (p6)
(AT) [9.10.9, [3b]] The ATO-OB recovers the ATO Operational Conditions within 5 seconds after changing to DE State. (p4)
[9.6] ATO Ready (RE)
[region]
(AT) [9.10.9, [5]] ("ATO Engage" selected) AND (TBL is in neutral or traction position) (p5)
(AT) [9.10.9, [8]] Driver manually brakes using the TBL. (p5)
[9.7] ATO Engaged (EG)
[region]

Fig. 2. AoE mode transitions (excerpt)

Step 1: Identify Components. The first step in the formal analysis consists of the systematic identification of components and boundaries specified in SUBSET-125. The ATO-OB is the main component whereas in the environment of ATO-OB the following components were identified: ATO-TS, ETCS-OB, Driver and Train.

Step 2: Derive Function Tables. The formalization started with the stepwise extraction of conditions and actions related to modes like *ATO Engaged* of the ATO-OB and its related mode transitions and transition conditions. For each mode all conditions and actions were combined in a so-called function table as proposed by Dave Parnas (for example [8]). Function tables and Event-B were successfully applied in [6]. Traceability information was added to conditions and actions that allows for relating requirements with elements of the function tables. Furthermore, a coverage analysis was made in order to ensure that all relevant requirements have been covered by the analysis. In Fig. 3 an excerpt of function table for ATO-OB mode ATO Ready (RE) is depicted.



<table>
<tr><td>Event-B</td><td>[ato_ob_mode_re_3]</td><td>[ato_ob_mode_re_4]</td><td>[ato_ob_mode_re_5]</td><td>[ato_ob_mode_re_6]</td></tr>
<tr><td></td><td colspan="4">mode = [9.6] ATO Ready (RE)</td></tr>
<tr><td></td><td colspan="4">[9.10.8] ATO-OB switched on</td></tr>
<tr><td></td><td colspan="4">[9.10.8, 11>p2] The ATO-OB detects no faults which does not allow performing ATO functions (e.g. connection with ETCS-OB is not active while ATO-OB is not in CO State).</td></tr>
<tr><td></td><td rowspan="3">[9.10.8, 9a>-p3-] The ATO-OB loses any ATO Operational Condition.</td><td colspan="3">[9.10.8, 9a>-p3-] ATO Operational Conditions are fulfilled.</td></tr>
<tr><td></td><td rowspan="2">[9.10.8, 7>-p4-]ATO Engagement Conditions are not fulfilled.</td><td colspan="2">[9.10.8, 7>-p4-] ATO Engagement Conditions are fulfilled.</td></tr>
<tr><td></td><td>[9.10.8, 5>-p5-] (Driver has not selected “ATO Engage” OR ETCS-OB is not in AD Mode) OR (TBL is not in neutral AND TBL is not in traction position)</td><td>[9.10.8, 5>-p5-] (Driver has selected “ATO Engage” and ETCS-OB is in AD Mode) AND (TBL is in neutral or traction position)</td></tr>
<tr><td>mode</td><td>[9.4] ATO Not Available (NA)</td><td>[9.5] ATO Available (AV)</td><td>[9.6] ATO Ready (RE)</td><td>[9.7] ATO Engaged (EG)</td></tr>
<tr><td>train movement</td><td>[9.4.1.2] no</td><td>[9.4.1.2] no</td><td>[9.6.1.4] no</td><td>[9.7.1.1] yes</td></tr>
</table>

Fig. 3. AoE function table for ATO-OB mode ready (excerpt)

Each function table consists of a hierarchical structured condition block, a value block and a variable block. Each column describes an event that consist of the conjunction of all conditions which are part of the column and an action which assigns in parallel all column values to the variables. Each column has been later formalized to an event of the corresponding Event-B specification. The trace to this event is specified in the first row of the function table. In this way a bidirectional traceability between function table and events of the Event-B specification is established.

Step 3: Derive Variable Table. The next analysis step consists of identifying variables in the conditions and actions so that conditions and actions can be reformulated formally. The requirements were analyzed such that types (like bool or enumeration types) can be assigned to the variables. This involves the analysis of relevant interface specifications, especially the interface between ATO-OB and ETCS-OB and the interface between ATO-OB and train, respectively. Based on this analysis, for each variable and for each component read/write permissions were assigned. In addition, traceability information related to both the interface and system requirements and events of the Event-B specification was added. For example, variable *ato_ob_etcs_ob_in_ad_mode* with type *bool* is defined. The justification for this decision is given by the trace `[130, 7.3.2.2] [9.10.8, 10>-p3-]` pointing to section 7.3.2.2 of SUBSET-130 and to transition 10 (with priority 3) in section 9.1.8 of SUBSET-125. SUBSET-130 defines a signal with name *Q_ADMODE* which can take the values 0 or 1. The ETCS-OB will send this signal cyclically to the ATO-OB (indicating whether it is in AD mode or not). The component ATO-OB has read permission, the environment component ETCS-OB has write permission. All other environment components have neither read nor write permissions.

Step 4: Derive Event-B Specification. The derived Event-B Specification has 25 variables, 30 invariants and 41 events. In Fig. 4 event `ato_ob_mode_re_6` (excerpt) is shown which has been derived from column `[ato_ob_mode_re_6]` of the function table depicted in Fig. 3.

```
ato_ob_mode_re_6
any
   ato_ob
where
   ato_ob ∈ ATO_OB
   ato_ob_mode(ato_ob) = RE
   ato_ob_operational_conditions(ato_ob) = TRUE
   ato_ob_engagement_conditions(ato_ob) = TRUE
   ato_ob_etcs_ob_in_ad_mode(ato_ob) = TRUE
   ...
then
   ato_ob_mode(ato_ob) = EG
   ...
end
```

Fig. 4. Event ato_ob_mode_re_6

Step 5: Validation. In SUBSET-125 several scenarios of AoE are specified. These scenarios are classified as descriptions (they are not requirements). For example, section 9.10.2 describes the nominal scenario in which the ATO will be engaged by the driver for each so-called journey segment. We have used ProB for simulating step-by-step these scenarios in order to validate the model.

Step 6: Verification. The formal verification was mainly done by theorem proving with the tool Rodin and the Atelier B prover, the SMT solvers and ProB plugins. Furthermore, refinement steps were used to impose further constraints on the environment. For example, since AoE realizes so-called Grade of Automation level 2, a very important safety property is that ATO will never be engaged when the driver never selects ATO Engage. In a refinement step the behavior of the driver was constrained such that he can never select ATO Engage. It was proven that an ATO-OB in this refined Event-B specification is never in mode *ATO Engaged (EG)* or *ATO Disengaging (DE)* (the only modes in which ATO is engaged).

Conclusion. In this paper the experiences gained in the formalisation and analysis of AoE was presented. The formal analysis of the mode transition requirements revealed 23 ambiguities and missing requirements. The formal analysis will be continued in the future. According to the determined refinement strategy the focus will be on the important functional layers ATO Active Functions Table and ETCS mode transition requests (SUBSET-125, 9.11, 9.12), respectively. With these refinement steps the functional layer ATO Operational States (SUBSET-125, 9) will be completely addressed.

Acknowledgments. I thank the anonymous reviewers for their valuable suggestions to improve the paper.

References

1. Bartholomeus, M., Luttik, B., Willemse, T.: Modelling and analysing ERTMS hybrid level 3 with the mCRL2 toolset. In: Howar, F., Barnat, J. (eds.) FMICS 2018. LNCS, vol. 11119, pp. 98–114. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00244-2_7
2. Basile, D., et al.: On the industrial uptake of formal methods in the railway domain. In: Furia, C.A., Winter, K. (eds.) IFM 2018. LNCS, vol. 11023, pp. 20–29. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98938-9_2
3. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Modelling and analysing ERTMS L3 moving block railway signalling with simulink and Uppaal SMC. In: Larsen, K.G., Willemse, T. (eds.) FMICS 2019. LNCS, vol. 11687, pp. 1–21. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27008-7_1
4. ter Beek, M.H., et al.: Adopting formal methods in an industrial setting: the railways case. In: ter Beek, M.H., McIver, A., Oliveira, J.N. (eds.) FM 2019. LNCS, vol. 11800, pp. 762–772. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30942-8_46
5. Di Meo, C., Di Vaio, M., Flammini, F., Nardone, R., Santini, S., Vittorini, V.: ERTMS/ETCS virtual coupling: proof of concept and numerical analysis. IEEE Trans. Intell. Transp. Syst. **21**(6), 2545–2556 (2020)
6. Eschbach, R.: Industrial application of Event-B to a wayside train monitoring system: formal conceptual data analysis. In: ter Beek, M.H., McIver, A., Oliveira, J.N. (eds.) FM 2019. LNCS, vol. 11800, pp. 738–745. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30942-8_43
7. Hansen, D., et al.: Using a formal B model at runtime in a demonstration of the ETCS hybrid level 3 concept with real trains. In: Butler, M., Raschke, A., Hoang, T.S., Reichl, K. (eds.) ABZ 2018. LNCS, vol. 10817, pp. 292–306. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91271-4_20
8. Parnas, D.L.: Inspection of safety-critical software using program-function tables. In: Linkage and Developing Countries, Information Processing 1994, Proceedings of the IFIP 13th World Computer Congress, Hamburg, Germany, 28 August–2 September 1994, vol. 3, pp. 270–277. IFIP Transactions (1994)
9. Platzer, A., Quesel, J.-D.: European train control system: a case study in formal verification. In: Breitman, K., Cavalcanti, A. (eds.) ICFEM 2009. LNCS, vol. 5885, pp. 246–265. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10373-5_13