OETCS/WP1/D02

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

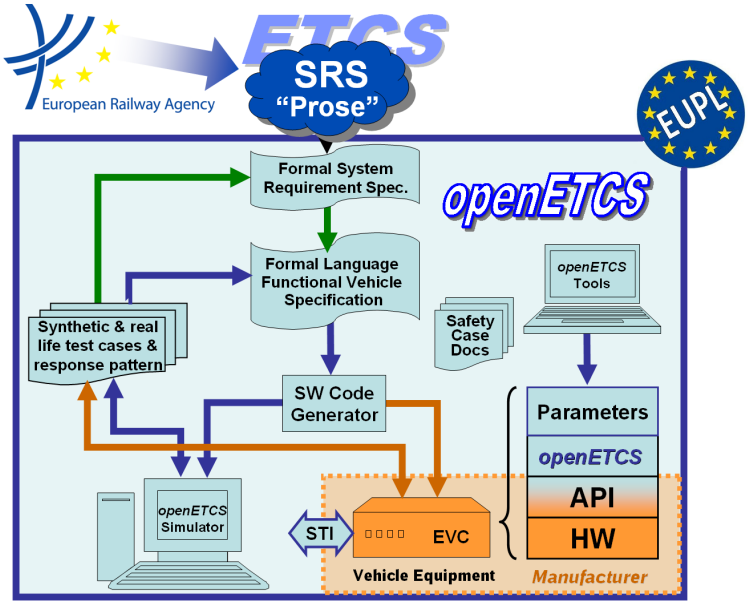
Work-Package 4: “V&V”

ETCS Specification Findings

Findings of ETCS specification analyses

Stefan Rieger

January 2014



Funded by:

Federal Ministry of Education and Research
Région de Bruxelles-Capitale
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

This page is intentionally left blank

Work-Package 4: “V&V”

OETCS/WP1/D02
January 2014

ETCS Specification Findings

Findings of ETCS specification analyses

Stefan Rieger

TWT GmbH Science & Innovation
Ernsthaldenstraße 17
70565 Stuttgart
Germany

Description of work

Prepared for openETCS@ITEA2 Project

Abstract: This document lists analysis results of the ETCS specification and accompagnying standards that indicate problems such as unclearities, inconsistencies, ambiguities, incompleteness or errors. For now it is part of TWT's model verification user story but the goal is to extend its scope.

Table of Contents

1 Purpose of this Document

This document lists findings in the ETCS specification and accompagnying standards indicating problems such as inconsistencies, ambiguities, incompleteness or errors that arise during analysis or modelling. The goals are the following:

- Clarify and correct problems to help in system modelling
- Indicate issues in the standard for future improvement
- ...

This document is to be considered as “living document” that is continuously extended during the runtime of the project. Solutions to issues or workarounds shall be added when available.

2 List of Issues

2.1 Subset 026 3.6 Location Principles, Train Position and Train Orientation

Issue #1 (3.6.1.3 Train Position): What is the difference between the *estimated train front end position* and the *train confidence interval*? Both values are contained in the *train position information*. It seems that the *train confidence interval* is a more conservative approximation. If this is the case, how exactly is the *estimated train front end position* defined?

Resolution: Write resolution here...

2.2 Subset 026 5.x

Issue #2 (Semantics of the tables specifying the update of on-board variables): Do I read each row of such a table as “If transition condition holds and a variable a the value as shown in the table, then change the value of that variable according to the table” (i.e., the variable does not necessarily have the value as shown in the table) or “If transition condition holds, then change the value of a variable according to the table” (i.e., each variable has the value as shown in the table).

Resolution: The semantics is unclear and the values should be checked.

2.3 Subset 026 5.4 Procedure Start of Mission

Issue #3 (5.4.2.2 Train Data): It is not clear what the train data consists of.

Issue #4 (5.4.3.2 State S0 - Driver starts a mission): We assume that this also refers to a signal sent by the driver to the on-board unit (e.g., by pushing a button).

Issue #5 (5.4.3.2 State S0 - communication session): Can there be active communication session other than with the RIU and the RBC?

Issue #6 (5.4.3.2 State S1 - Driver-ID Validation): The specification states that the driver revalidates the Driver-ID. So it can be assumed that the system relies on correct validation by the driver. Is this true? When does the Driver-ID become invalid or unknown? At End of Mission? The same holds for the *train running number*.

Issue #7 (5.4.3.2 State S1 - Virtual Balise Cover): Virtual balise cover is not properly specified. The same holds for the process of setting/removing virtual balise cover.

Issue #8 (5.4.3.2 State S1 - Transition E1): Last paragraph, S1: How do I understand “possibly further to Train running number ...”?

Issue #9 (5.4.3.2 State S2 - Missing case: level data is valid): This case is possible, see D2 but it is not mentioned how to proceed. We assume that also in this case para 3 and 4 in S2 are applied.

Issue #10 (5.4.3.2 State S2 - Enter/Re-validate Level): The specification distinguishes the following three cases:

1. Entering level (if state *unknown*)
2. Re-validate level (if state *invalid*)
3. Re-enter level (if state *invalid*)

The purpose of this distinction is not clear as entering the level suffices (the current setting is invalid or unknown and thus irrelevant).

Issue #11 (5.4.3.2 State S3 - Selection of Radio Network): It is not mentioned that a valid *radio network ID* must be stored in the on-board unit, but this seems to be necessary because the driver may not select a new radio network. The type of the radio network IDs is not mentioned.

Issue #12 (5.4.3.2 State S3 - Mobile terminal): What happens if no Mobile terminal is registered to a Radio Network (or can we assume that at least one mobile terminal is always registered); see 2nd para in S3.

Issue #13 (5.4.3.2 State S3 - RBC-ID): What is the difference between the *RBC-ID* that may be invalid and the *last stored RBC-ID*? Why can the latter not be invalid?

Issue #14 (5.4.3.2 State S3): In item 2 in S3, the driver sets a radio network ID and RBC-ID to unknown but in item 3, it is assumed that the RBC-ID is invalid. So is it possible to skip the first two items? In addition, after applying item 3 (i.e., using the last stored RBC-ID number) is the RBC-ID set to valid?

Issue #15 (5.4.3.2 State S3 - EIRENE Short Number): The option to use the EIRENE short number is unclear: I assume the RBC is triggered to send an RBC-ID (i.e., the respective variable is set to valid). However, what happens if something goes wrong? We read in 3.18.4.3.4.1: “... does not direct to a RBC with the stored RBC ID, the connection will be terminated”. So how does the flow continue and which state do we enter in this case?

Issue #16 (5.4.3.2 State D7 - Mobile Terminal registered): The definition of a mobile terminal is missing. How many mobile terminals are there? Is this equivalent to radio network registration (see state S3)? The latter is assumed for the initial models.

Issue #17 (5.4.3.2 State D33): Does the RBC send a signal showing whether it can validate the position report (see para 1 and 3 in D33)? Should not there be a timeout as the position may become invalid after some time?

Issue #18 (5.4.3.2 State S10): The point in time when item 4 takes place is unclear for E12 (i.e., item 1): I assume the driver selects SH (i.e., the mode is changed), then item 4 is applied (invalid position is set to unknown), then the level check (see item 1) is performed, and based on this check procedure shunting is called or the process goes back to S10.

Moreover, how do I read the last sentence in item 1: Does the RBC reject the request for shunting if the level is 2 or 3 or can the RBC always reject the request for shunting but there will be a special treatment in case the level is 2 or 3?

The same question arises at 5.4.5.3.g.

Issue #19 (5.4.3.2 State S11 - RBC acknowledgment): Can we always expect an acknowledgment? (Sometimes it is specified that the RBC is, after some timeout, triggered again.)

Issue #20 (5.4.3.3, last row on p.17): I assume that if the driver chooses to re-enter the level (see 5.4.5.3.e), then the values are set according to the table, and after he entered the level, at least the status of the ETCS level should be set to valid.

Issue #21 (5.4.5.1): What is meant by “above D11” in a flowchart where flow also goes from left to right, and what is meant by “the nominal procedure applies”?

Issue #22 (5.4.5.2): Where is the missing information specified?

Issue #23 (5.4.5.3 a): Does “if the position is still invalid” (line 3) refer to a condition that is checked after the procedure Override has been executed?

Issue #24 (5.4.5.3 b,c,i): How does the process continue—as described in state S1?

Issue #25 (5.4.5.3 f): How does the procedure continue; that is, to which state do we go? (Assumption: The mission is considered as started, see 5.4.6.1.)

2.4 Subset 026 5.5 Procedure End of Mission

Issue #26 (5.5.3.1.3 - report to RBC): Is End of Mission reported to RBC in every level or only in ETCS level 2 and 3. If yes, what happens in the situation described in 5.5.4.1.1?

Issue #27 (5.5.4.1.2): By 5.5.3.1.2 and 5.5.3.1.3, this should hold for every ETCS level and not only for 2 and 3.

2.5 Subset 026 5.6 Procedure Shunting Initiated by Driver

Issue #28 (5.6.2.2 A030 - calling Trip procedure): We call the train trip procedure which itself calls Shunting. How do we ensure that this recursion eventually stops?

Issue #29 (5.6.2.2 D040 - ongoing mission): What is an ongoing mission?

Issue #30 (5.6.4.1.2 – termination): What happens after the driver has been informed; that is, do we continue as we would do in case the session was not terminated (i.e., as in A220)?

Issue #31 (5.6.4.1.3): Does this item refer to a transition directly after A220 or 5.6.4.1.2?

2.6 Subset 026 5.11 Procedure Train Trip

Issue #32 (5.11.2.2 A025): Considering the flow chart and D020, I assume the process shall go to D020 rather that A030.

Issue #33 (5.11.2.2 D80): Replace with D080.

Issue #34 (5.11.2.2 S130): After having acknowledged mode change to PT (see S120), the RBC is assumed to revoke all pending emergency stops. Is the RBC triggered by the on-board unit to do so (e.g., after D130) or does S120 serve as the trigger?

Issue #35 (5.11.4.1.2 - termination): How do we proceed after the communication session has been terminated?

Issue #36 (5.11.4.2 - override): How do we proceed after override?