ITEA2 Project
Call 6 11025
2012 – 2015

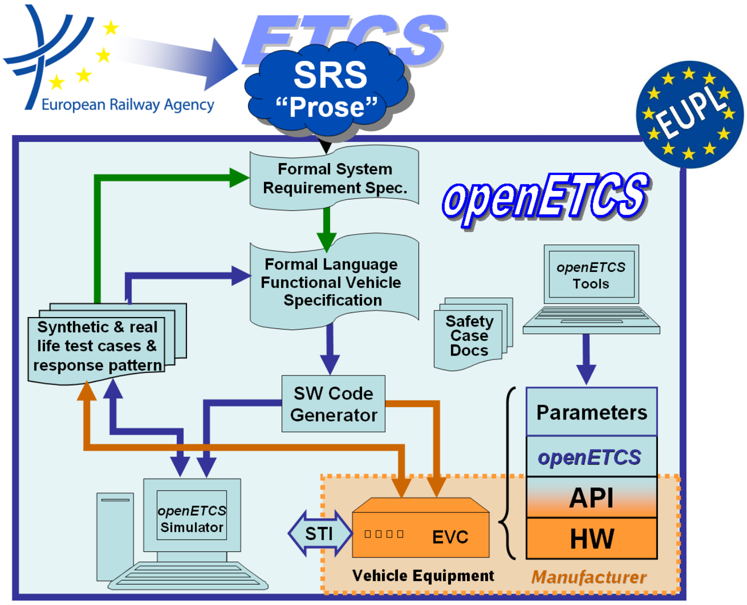
Work-Package 4: “V&V”

# ETCS Specification Findings

## Findings of ETCS specification analyses

Stefan Rieger and Marc Behrens

December 2015



Funded by:

Federal Ministry
of Education
and Research

Région de
Bruxelles-
Capitale

GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing:

This page is intentionally left blank

**Work-Package 4: “V&V”** **OETCS/WP1/D02**
**December 2015**

# ETCS Specification Findings

**Findings of ETCS specification analyses**

Stefan Rieger

TWT GmbH Science & Innovation
Ernsthaldenstraße 17
70565 Stuttgart
Germany

Marc Behrens

Deutsches Zentrum für Luft und Raumfahrt e.V.
Lilienthalplatz 7
38108 Braunschweig
Germany

Description of work

Prepared for openETCS@ITEA2 Project

*This work is licensed under the "openETCS Open License Terms" (oOLT).*

**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.

**Disclaimer: This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing: European Union Public Licence (EUPL v.1.1+) AND Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)**

THE WORK IS PROVIDED UNDER openETCS OPEN LICENSE TERMS (oOLT) WHICH IS A DUAL LICENSE AGREEMENT INCLUDING THE TERMS OF THE EUROPEAN UNION PUBLIC LICENSE (VERSION 1.1 OR ANY LATER VERSION) AND THE TERMS OF THE CREATIVE COMMONS PUBLIC LICENSE ("CCPL"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS OLT LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

http://creativecommons.org/licenses/by-sa/3.0/
http://joinup.ec.europa.eu/software/page/eupl/licence-eupl

# Table of Contents

*This work is licensed under the "openETCS Open License Terms" (oOLT).*

# 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:* The estimated train front end is the measured position of the train whereas the train confidence interval gets added to the estimated train front end and results in safe maximum front end or, if subtracted, in safe minimum front end, see SUBSET-026-3 figure 13c. Issue closed.

## 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. Judging from the conditions it should be read as "If transition condition holds, then change the value of a variable according to the table".

## 2.3 Subset 026 5.4 Procedure Start of Mission

**Issue #3 (5.4.2.2 Train Data):** The specification seems to be inconsistent: The data listed, the control flow also depends on the status of the virtual balise cover.

*Resolution:* The virtual balise cover is handled inside SUBSET-026-3.15.9 and can have the states: valid, removed, non-valid, ordered, deleted, stored. Should the virtual balise cover be handled inside this diagram? Clarification request sent to SUBSET-076 Working Group.

**Issue #4 (5.4.3.2 State S0 - communication session):** Can there be an active communication session other than with the RIU and the RBC?

*This work is licensed under the "openETCS Open License Terms" (oOLT).*

**Issue #5 (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? In other words, what happens if the driver enters an invalid Driver-ID?

*Resolution:* It is true. There are up to three iterations of asking the driver for a correct ID.

**Issue #6 (5.4.3.2 State S1 - Driver-ID Validation):** When does the Driver-ID become invalid or unknown? At End of Mission? The same holds for the *train running number*.

*Resolution:* The Driver-ID is deleted when entering NP, see SUBSET-026-4.10.1.3.

**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. How does setting and removing a virtual balise cover change the status of the virtual balise cover? Our guess is that setting results in a valid virtual balise cover whereas removing changes the status to unknown.

*Resolution:* Clarification request sent to SUBSET-076 Working Group.

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

*Resolution:* "Possibly" describes here the activated menu function to enter/ revalidate the train running number and/ or Virtual Balise Cover setting/ removal.

**Issue #9 (5.4.3.2 State S2 - Missing case: level data is valid):** There seems to be an inconsistency: It is not explicitly mentioned, that the paragraphs 3 & 4 are related to the 'valid' case. 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.

*Resolution:* Following D2 the level data is set to invalid. This case of a valid level data does not exist in S2.

**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).

*Resolution:* It depends on the actual interface of the driver whether we need to distinguish between validation and reentering. From system perspective if the setting is set to unknown or invalid is often only distinguished via a visibility flag. Thus the rationale for invalid is to propose to the train driver the last value and have this value validated.

**Issue #11 (5.4.3.2 State S3 - Selection of Radio Network):** Inconsistency in the specification: It is not mentioned that a valid *radio network ID* must be stored in the on-board unit, but this

This work is licensed under the "openETCS Open License Terms" (oOLT).

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.

*Resolution:* L2 is not supported for this OBU or part of the track if no mobile terminal is registered.

**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?

*Resolution:* Describes in the EIRENE specification. Basically it applies when no Radio Subscriber Number is known and the EIRENE short number is called applying NID_RADIO "FFFF FFFF FFFF FFFF".

**Issue #16 (5.4.3.2 State S3 - missing cases):** How do we proceed if the driver decides not to reenter the radio network ID? Likewise, how do we proceed if no mobile terminal is registered?

**Issue #17 (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 #18 (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)?

**Issue #19 (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.

*This work is licensed under the "openETCS Open License Terms" (oOLT).*

**Issue #20 (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.) Stephan

*Resolution:* According to SUBSET-026-5.4.5.1 after passing D11 the process shall go to S10 after a loss of radio connection, i. e. when an acknowledgement is not received.

**Issue #21 (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 #22 (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"?

*Resolution:* The nominal procedure in contradiction to the "degraded situations" refer to the flow chart as described in Figure 1.

**Issue #23 (5.4.5.2):** Where is the missing information specified?

*Resolution:* The operational situations come from requirements defined by the operator.

**Issue #24 (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 #25 (5.4.5.3 b,c,i):** How does the process continue—as described in state S1?

*Resolution:* Clarification request forwarded to SUBSET-076 working group.

**Issue #26 (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.)

*Resolution:* The OBU enters NL via E10.

### 2.4 Subset 026 5.5 Procedure End of Mission

**Issue #27 (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 #28 (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 #29 (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?

*Resolution:* After the driver acknowledges train trip and the train is at standstill and the ERTMS/ETCS level is 0 or NTC and no valid Train Data is on-board, see SUBSET-026-4.6.3 [68] the mode SH is activated automatically. In case the driver initiates shunting and a "National trip procedure applies" the system switches back to Train Trip.This would mean in order to be

This work is licensed under the "openETCS Open License Terms" (oOLT).

recursive the initial condition of mode FS, LS, OS, SR, PT, SN, UN or SB should be activated. THis case is expected to be taken care of inside the national trip procedure.

**Issue #30 (5.6.2.2 D040 - ongoing mission):** What is an ongoing mission?

*Resolution:* The definition of an on-going mission is implicitly defined between the “Start of Mission“ and the “End of Mission‘, see SUBSET-026-5.4.6.1, SUBSET-026-5.12.2.

**Issue #31 (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)? The same question arises for the situation described in 5.6.4.3.

*Resolution:* In both cases no transition to shunting mode is performed. The first case because of the anster “SH refused“ in the referenced case because of loss of radion connection which mos propapbly should lead in L2/3 to a message of kind “SH impossible due to loss of radion connection“.

**Issue #32 (5.6.4.1.3):** Does this item refer to a transition directly after A220 or to 5.6.4.1.2?

*Resolution:* The hint to “Override“ applies to all cases if no SH authorisation can be receeived and is by this referring to SUBSET-025-5.6.4.1.2.

### 2.6 Subset 026 5.11 Procedure Train Trip

**Issue #33 (5.11.2.2 A025):** Considering the flow chart and D020, I assume the process shall go to D020 rather that A030.

*Resolution:* Corrected in SUBSET-026 v3.4.0.

**Issue #34 (5.11.2.2 D80):** Replace with D080.

*Resolution:* Editorial change request filed via SUBSET-076 working group.

**Issue #35 (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?

*Resolution:* In A115 the OBU reports the mode change and triggers the decision on trackside.

**Issue #36 (5.11.4.1.2 - termination):** How do we proceed after the communication session has been terminated?

*Resolution:* There is a manual solution according to SUBSSET-026-5.11.4.2 and a request report changes to trackside when in L2/L3. In this case the onboard is obliged to build up a radio connection, as defined in position report parameters SUBSET-026-7.4.2.15.

**Issue #37 (5.11.4.2 - override):** How do we proceed after override?

*Resolution:* The handling of the EOA when leaving Override, according to SUBSET-026-5.8.3.1.1, depends on the mode when entering Override.

*This work is licensed under the "openETCS Open License Terms" (oOLT).*

### 2.7 Procedure On Sight and Comparable procedures

**Issue #38 (Delayed messages):** What happens if the acknowledgment of the driver is received after the train is already braking due to overpassing the safe front?

*Resolution:* According to SUBSET-026-5.9.2.4 the brake command shall be released.

### 2.8 Interplay of the procedures

**Issue #39 (How to restart a mission?):** Probably a new Mission can be started after the "End of Mission" procedure. To enter the "Start of Mission" procedure, the mode must be Standby (SB). This is not necessarily the case after finishing End of Mission. Can the Train enter SB-mode after End of Mission and if so, how?

*Resolution:* End of mission can be reached by closing the desk SUBSET-026-5.12.2.3, entering SB, SL or SH. This also depends on the mode coming from SUBSET-026-5.2. While a mission is considered as started when entering FS, LS, SR, OS, NL, UN or SN mode SUBSET-026.5.4.6.1. SB is reached as desceibed in SUBSET-026-4.6.2. Situations in which the train end its mission and starts its mission are expected to be described in the respective operational rule.

**Issue #40 (State after "Train Trip" & "Override"):** Which procedures can be called after having finished the Override/Train Trip procedure?

*Resolution:* After Override expires the normal mode applies. The transitions after Train Trip are described within SUBSET-026-4.6.2.

## References

*This work is licensed under the "openETCS Open License Terms" (oOLT).*