

1 Verification Report for Architecture and Design
2 of Train Positioning
3 Version 0.1

4 Marc Behrens (DLR), Bernd Gonska (DLR),
Jens Gerlach (Fraunhofer), Bernd Hekele (DB),
Jan Welte (TU-BS)

5 Oct 29, 2014

6 **Abstract**

7 This verification report presents the verification results for the archi-
8 tecture, interfaces and design artifacts for the component "Train Position-
9 ing" in the overall openETCS Kernel architecture.

10 **1 Roles**

- 11 • Fausto Cochetti - Design (PM)
- 12 • Jens Gerlach - Verification of SW/Implementation
- 13 • Uwe Steinke - Design/Implementation
- 14 • Jan Welvaarts - Design
- 15 • Vincent Nuhaan - Simulation/Design
- 16 • Bernd Gonska - Verification
- 17 • Marc Behrens - Verification
- 18 • Jan Welte - Verification
- 19 • Bernd Hekele - Verification

20 **2 Verification Object**

21 **2.1 Identity of Verification Object**

22 The component `Train Positioning` provides the central functionality to de-
23 termine the train position based on detected balises and their measured and
24 announced distances.

25 The component is defined in the **openETCS System Architecture and Design**
 26 **Specification** [3] as F.2.2 Calculate Train Position. Here it is defined that the
 27 function shall cover the requirements defined in the SRS [2] Chapter 3.6.

28 Concepts for **Train Positioning** have been defined in two parallel work
 29 streams, which developed independently two documents and simulations to
 30 clarify their approach. To achieve one implementation in context of the over-
 31 all openETCS architecture both concepts have to be integrated. Respectively,
 32 this verification report is concerned with the following two groups of docu-
 33 ments, which are handled as one verification object. All artifacts for verifi-
 34 cation and verification activities are documented in the github issue <https://github.com/openETCS/validation/issues/227>.
 35

36 **Train Positioning concept 1**

37

reviewed document	Train Position and Locations (concept document)
	Train Position and Location Tester (Lab View Simulation)
github location	https://github.com/openETCS/SRS-Analysis/commit/edc8a3238e59ad4d2a2440f39e4c791cf6bbf7bd
comitted	10. July 2014
designer	Jan Welvaarts (concept)
	Vincent Nuhaan (simulation)
covered specification	SUBSET-026(SRS) chapter 3.6 version 3.3.0

38

39 **Train Positioning concept 2**

40

reviewed document	openETCS Determine Train Location Procedure (concept document)
github location	https://github.com/openETCS/SRS-Analysis/commit/153e793955b38c986dad3bfd8d3fbfe8d5ced77e
comitted	21. January 2014
reviewed document	CalculateTrainPosition (SCADE report)
github location	https://github.com/openETCS/modeling/commit/5cea2abbbf67da49b324aa8307129b5c47aba2188#diff-9fd0c16adf976a82850cd9184a13f0f5
comitted	1. September 2014
reviewed document	openETCS CalculateTrainPosition implementation Test Scenario 3_linked_2_unlinkedBG (Test Scenarios)
github location	https://github.com/openETCS/modeling/commit/3934d76f1fcba7cb28da7e8131f201182cc7d220
comitted	22. October 2014
designer	Uwe Steinke (concept, SCADE implementation, Test Scenarios)
covered specification	SUBSET-26(SRS) chapter 3.6 version 3.3.0

This verification reports only address the documents in the committed versions named above.

The verification mainly concentrated on the concept papers and took the simulation and the SCADE model only in consideration to specify the approach presented in the concept documents.

2.2 Configuration related Components

The functionality **Train Positioning** has been defined with respect to the SUBSET-026 System Requirements Specification (SRS) [2] chapter 3.6 version 3.3.0 on the legal basis of the Technical Specification for Interoperability Control Command Signalling (TSI-CCS) [4] and amended by [5].

The component limits have to be defined by the **openETCS System Architecture and Design Specification**, which has to present the interfaces either with respect to data from balise (and radio) messages defined in the SUBSET-026

55 chapters 7 and 8 or as in consistence with inputs and outputs of related func-
56 tions.

57 As the **openETCS System Architecture and Design Specification** have
58 not been available at the beginning of the verification and not all functions
59 interacting with **Train Positioning** are covered completely, the verification
60 results have to accept assumptions made by the designers. Additionally, no
61 further requirements for the interfaces have been assessed.

62 **3 Software Architecture, Interface and Design** 63 **Verification**

64 This section presents all verification results concerning the verification object
65 **Train Positioning**.

66 The following subsection present all different verification aspects in accor-
67 dance with EN 50128 7.3.4.42 [1].

68 **3.1 Internal Consistency**

69 *by Jan Welte and Marc Behrens*

70 Contant:

- 71 • relations
- 72 • historical development
- 73 • claim of same approach
- 74 • of naming between documents consistence

75 Are the internal functional allocation and all related input and output con-
76 sistent?

77 **3.2 Adequacy to fulfill Software Requirements**

78 *by Bernd Gonska*

79 **3.2.1 Description of the developed train positioning system**

80 The train positioning system clearly deviates from the SRS on purpose. This is
81 justified by the intended operational performance.

82 It basically implements the following concepts:

- 83 • All distances are given as the triple of safe distances (minimum,nominal,maximal)
- 84 • The estimated position, (also named nominal position) is calculated to be
85 the middle of the maximum safe position and the minimum safe position.

- 86 • Each Balise Group (BG) has a an own accuracy and position, relative to
87 the Last Relevant Balise Group (LRBG) and the LRBG accuracy. Loca-
88 tions do not change their reference BG.
- 89 • Linking distances and accuracies are used to improve the accuracy when
90 ever possible.
- 91 • Accuracy of a distance is calculated taking the worst possible case into
92 account. For example: The accuracy of the distance between two ends of
93 a linking chain includes the first and the last BG accuracy. The distance
94 between two BG without linking is the odometry measured distance. The
95 accuracy is the odometry accuracy during that distance. This inaccuracy
96 is not reseted later.
- 97 • The confidence interval of an announced location never increases when
98 a new BG is accepted. Always use the most accurate information. The
99 odometry error estimation is trustworthy enough to optimize linking ac-
100 curacy and distances.

101 3.2.2 Deviations

102 Within this paragraph the deviations to the specification is described by first
103 mentioning the number of the Subset-026 paragraph [2] and then stating how
104 the design deviates:

105 **3.6.4.1 REMARK:** There are several confidence intervals: They depend on
106 the announced location.

107 **3.6.4.2:** In addition, the odometry inaccuracy of older track areas and older
108 linking accuracy can be taken into account to widen a the confidence in-
109 terval for safety reasons. The location accuracy of the LRBG is shortened
110 on if the detected Balise group position is extreme. An old confidence in-
111 terval can be taken instead of a larger new one.// 3.6.4.2.2: An odometer
112 inaccuracy may not be reset at the new LRBG.

113 **3.6.4.3:** Even if the linking chain is not complete, linked parts replace odometry
114 distances if they provide higher accuracy.

115 In the "sandwich problem" where two linked BGs enclose an unlinked
116 BG (linked BG1 → unlinked BG2 → linked BG3) the distance and the
117 accuracy between BG2 and BG3 can be calculated involving the linking
118 accuracy of BG1 and BG3 and the linking distance between BG1 and BG3.

119 The estimated distance may differ from the linking distance and from the
120 odometry measured distance. The estimated distance is set to the middle
121 of the maximum and minimum safe distance.

122 **3.6.4.3.1:** The train takes responsibility, it does not reset inaccuracies if this
123 could lead to unsafe behavior.

124 **Figure 13 a,b,c:** There is more than one confidence interval.
 125 The confidence interval is calculated differently.
 126 The estimated distance can be different since it is the middle of the max-
 127 imum and minimum safe distance.
 128 Linking distance is not used if it leads to a less accurate distances.

129 **3.6.4.4:** The estimated distance is the middle of the maximum and the min-
 130 imum safe position with respect to the possible LRBG position. It may
 131 differ from the measured traveled distance.

132 **3.6.4.4.1:** analogue for the rear end position.

133 **3.6.4.7.1:** The unlinked BG confidence interval is not reset at the next LRBG.

134 **3.6.4.7.2** The unlinked BG confidence interval is not reset at the next unlinked
 135 BG. In some cases the estimated traveled distance between two unlinked
 136 BG is calculated by using other rules.

137 **3.2.3 Readability and Traceability**

138 by Marc Behrens

139 Content

- 140 • traceability of requirements
- 141 • unique references

142 Are all related system and software requirements uniquely referenced and
 143 is the relationship to other documents clearly defined? Are all parts of the
 144 architecture and inputs and outputs referenced to the related requirements.
 145 Are the elements referred to in the same way in all documents?

146 ** 10' item: look for findings inside the two verification reports ** 10' struc-
 147 ture: two chapters, one for each report ** 20' 3 documents: readability: statis-
 148 tics: wordlength + syllable over sentence length ** 20' look in 2.x: traceability
 149 to openetcs req ** 10' only 3.6 available traceability to SRS requirements ***
 150 high level ** traceability to TSI requirements *** 20' are there more req in TSI
 151 to positioning? *** 10' what is missing *** 15' design reasoning: what is needed
 152 for performance reasons *** 5' what is the least cycle time *** 5' are realtime
 153 requirements defined on architecture level? ** 10' traceability to higher level
 154 artifacts *** 10' high level requirements were defined during workshop as RO
 155 US who will be response ** 10' application of glossary *** 5' subset-023 *** 5'
 156 openETCS glossary *** 5' make jan's document openETCS licensed + upload

157 **3.2.4 Consideration of hardware and software constraints**

158 Hardware design is out of scope of the openETCS project. No hardware as-
 159 sumptions have been formulated so far.
 160 Software constraints encompass:

- 161 1. Constraints by the software design method. The design should rely on
- 162 • modelling
- 163 • a modular approach
- 164 • defensive programming
- 165 2. Restrictions implied by the coding standards. The coding standard should
- 166 include
- 167 • a coding style guide
- 168 • restrict the use of pointers, dynamic objects, recursion and global
- 169 variables
- 170 3. Constraints on timing, performance, or memory of individual modules.
- 171 4. Any constraints implied by the interfacing system (e.g. decoder and en-
- 172 coder functions).
- 173 5. Constraints of the operating system.

174 4 Conclusions

175 Concluding the meeting the following points were agreed on as action item list:

176 4.1 Implementation and Design

177 Differences within the simulation and implementation has been detected and
178 the two approaches have to be merged (Jan: Specify, Uwe: Implement)

- 179 1. synchronize on using the inaccuracies of the BG passed or just of the last
- 180 BG and the 1st BG (Uwe and Jan Welvaarts)
- 181 2. backwards calculation of inaccuracies need to be synchronized (Uwe, Jan)
- 182 3. agree on the output data (Uwe, Jan Welvaarts, Vincent)
- 183 4. synchronize data structure for balise storage and storage of other trackside
- 184 related information
- 185 5. agree on the input data (Uwe, Jan Welvaarts, Vincent)
- 186 6. integer arithmetic only on the model (design decision of WP3)
- 187 7. resolution of train position in cm (design decision of WP3)
- 188 8. Inaccuracy of the Odometer is agreed to be taken into account (Uwe)
- 189 9. Center Detection accuracy is agreed to be taken into account (Uwe)
- 190 10. define national values to be used (Jan Welvaarts)

- 191 11. national values can also change at some point on track (Uwe)
- 192 12. a as common reference for saving the data the start-up position of the
193 OBU is taken
- 194 13. rules have to be implemented correctly
- 195 14. Q_LOCACC will be made dependant on the national values and on the
196 linking information (Uwe, Vincent)
- 197 15. Implement distance calculation to track objects, other than balises (Uwe)

198 4.2 Scenarios

199 Concerning the scenario simulation the following was decided:

- 200 1. Two scenarios to contain all possible situations are to be sketched (Jan)
- 201 2. Calculate distance related values with the LabView Simulation to be com-
202 pared with the SCADE execution (Vincent)

203 4.3 Report

204 Concerning the follow up of the verification report the following points were
205 decided:

- 206 1. Verification report is to be written (Marc, Jan Welte, Jens Gerlach, Bernd
207 Gonska)
- 208 2. once the design is merged and implemented the verification will rework
209 the results based on the merged version (Marc)
- 210 3. traceability to the SRS will be delivered (Jan, Marc)
- 211 4. justification on the deviations need to be documented (Jan, Uwe)

212 References

- 213 [1] Comité Européen de Normalisation Electrotechnique. Railway applications
214 - Communication, signalling and processing systems - Software for railway
215 control and protection systems, EN 50128. *EUROPEAN STANDARD*, 6
216 2011.
- 217 [2] ERA, UNISIG, and EEIG ERTMS USERS GROUP. ERTMS/ ETCS
218 System Requirements Specification, SUBSET-026. *European Rail-
219 way Agency Document Register*, 3 2012. [http://www.era.europa.eu/
220 Document-Register/Documents/Set-2-Index004-SUBSET-026%20v330.
221 zip](http://www.era.europa.eu/Document-Register/Documents/Set-2-Index004-SUBSET-026%20v330.zip).

- 222 [3] Bernd Hekele, Paymann Farhangi, Peter Mahlmann, Uwe
223 Steinke, Christian Stahl, and David Mentré. openetcs sys-
224 tem architecture and design specification. *openETCS mod-*
225 *eling repository*, 10 2014. [https://github.com/openETCS/](https://github.com/openETCS/modeling/blob/18cd45f54932b46dde7fea404f21aa5b27bcc516/openETCS%20ArchitectureAndDesign/FirstIteration/openETCSArchitectureAndDesignSpecification.pdf?raw=true)
226 [modeling/blob/18cd45f54932b46dde7fea404f21aa5b27bcc516/](https://github.com/openETCS/modeling/blob/18cd45f54932b46dde7fea404f21aa5b27bcc516/openETCS%20ArchitectureAndDesign/FirstIteration/openETCSArchitectureAndDesignSpecification.pdf?raw=true)
227 [openETCS%20ArchitectureAndDesign/FirstIteration/](https://github.com/openETCS/modeling/blob/18cd45f54932b46dde7fea404f21aa5b27bcc516/openETCS%20ArchitectureAndDesign/FirstIteration/openETCSArchitectureAndDesignSpecification.pdf?raw=true)
228 [openETCSArchitectureAndDesignSpecification.pdf?raw=true](https://github.com/openETCS/modeling/blob/18cd45f54932b46dde7fea404f21aa5b27bcc516/openETCSArchitectureAndDesignSpecification.pdf?raw=true).
- 229 [4] European Union. Commission Decision of 25 January 2012 on the technical
230 specification for interoperability relating to the control-command and sig-
231 nalling subsystems of the trans-European rail system. *Official Journal of*
232 *the European Union*, pages L51/1–L51/65, 2012.
- 233 [5] European Union. Commission Decision of 6 November 2012 amending Deci-
234 sion 2012/88/EU on the technical specifications for interoperability relating
235 to the control-command and signalling subsystems of the trans-European
236 rail system. *Official Journal of the European Union*, pages L311/3–L311/13,
237 2012.