ERTMS/ETCS
ETCS Hazard Log
REF : SUBSET-113 ISSUE : 1.5.0 DATE : 2022-05-10

Company	Technical Approval	Management approval
ALSTOM		
AZD		
CAF		
HITACHI RAIL STS		
MERMEC		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 – 0.0.12		See HAZLOG_v0.0.13	
0.0.13 2007-12-17	All	Document created from HAZLOG_v0.0.13. Changes marked compared to this document.	Dag Ribbing
0.0.14 2008-01-13	4.7, 4.9, 4.10, 4.11	Clarified text about omitted hazards after comments from RAMS group	Dag Ribbing
0.0.15 2008-02-07	4.18, 4.19, 4.20, 4.21	Updates after agreed changes during RAMS-meeting 2008-02-06/07	Dag Ribbing
0.0.16 2008-04-02		• Updated after review by UNISIG Super Group • Tracing from H0014 to CR 477 added • Minor language corrections	Dag Ribbing
1.0.0 2008-10-14		• Changes agreed during RAMS-meetings plus some minor corrections. Corresponding to HAZLOG_v1.0.0.	Dag Ribbing
1.0.1 2008-12-16		Proposal on how to answer SG comments, agreed in RAMS-meeting and partly in SG-meeting	Dag Ribbing
1.0.6 2008-12-18		Added H0022-H0029 from Hazard Log v1.0.6 Corresponding to HAZLOG_V1.0.6	Dag Ribbing
1.0.7 2009-01-15		Minor update after comments from Thales and Siemens	Dag Ribbing
1.0.8 2009-02-25		• Another example added in the description of H0019	Dag Ribbing

		• Updated after comments from Hans Kast • Updates during joint RAMS-SG meeting 2009-02-17 • A few clarifications agreed in RAMS WP	
1.0.9 2009-04-15		• A few updates after comments from Philippe Prieels • H0029 updated according to proposal from Thales	Dag Ribbing
1.1.0 2009-04-21		• Grammatical corrections after RAMS-meeting 2009-04-21	Dag Ribbing
1.1.1 2009-10-22		• Added H0030 from HAZLOG v1.1.3 • Clarification on H0029 as defined in HAZLOG v1.1.3 • Rows “Found in ETCS baseline” and “Solved in ETCS baseline” added	Dag Ribbing
1.1.2 2009-11-09		• Further clarification on H0029 as defined in HAZLOG v1.1.4 • Added H0031 from HAZLOG v1.1.4	Dag Ribbing
1.1.6 2010-03-21		Updates to match HAZLOG v1.1.6: • H0004 and H0005 slightly modified • H0032-H0036 added.	Dag Ribbing
1.1.8 2010-05-27		Updates to match HAZLOG v1.1.8: • H0019, H0025 and H0036 slightly modified • H0037 added.	Dag Ribbing
1.1.9 2010-07-02		Updates to match HAZLOG v1.1.9:	Dag Ribbing

		• H0019 case 2 modified • Closing notes on H0020 and H0024 added.	
1.1.10 2010-09-14		Updates to match HAZLOG v1.1.10: • H0019, H0030 and H0036 modified	Dag Ribbing
1.1.11 2011-01-25		Updates to match HAZLOG v1.1.11: • H0019 modified • H0038 and H0039 added but no text yet	Dag Ribbing
1.1.12 2011-01-25		Updates to match HAZLOG v1.1.12: • H0016 closed with CR 842 for baseline 3, SRS v3.2.0 • H0020 closed with CR 897 for baseline 3, SRS v3.2.0 • H0031 closed with CR 899 for baseline 3, SRS v3.2.0 • H0037 closed for baseline 3, SRS v3.2.0	Dag Ribbing
1.1.13 2011-03-20		Updates to match HAZLOG v1.1.13: • H0019 completed with another example	Dag Ribbing
1.1.14 2011-05-18		Updates to match HAZLOG v1.1.14: • H0026 closed with CR 659 for baseline 3, SRS v3.0.0 • H0037 clarified acc to proposal from NRBC WP • H0039 and H0039 added	Dag Ribbing

		Text clarified for hazards which are intentionally left empty.	
1.1.15 2011-08-09	4.9	H0009 added.	Dag Ribbing
1.1.17 2011-11-21		Updates to match HAZLOG v1.1.17: • Minor change in H0035 • Solution proposal added in H0038 • H0040 added (so far without solution) • H0041 added • H0042 reserved (so far without content)	Dag Ribbing
1.1.19 2012-03-20		Updates to match HAZLOG v1.1.19: • H0035 closed for B3 because of CR 923 • H0036 closed because of CR 756 being rejected • H0042 added	Dag Ribbing
1.1.20 2012-03-30		Updates to match HAZLOG v1.1.20: • H0040 concluded • H0043 added, currently without complete solution proposal • H0044 added	Dag Ribbing
1.1.21 2012-04-02		• H0040 updated • H0045 added, currently empty	Dag Ribbing
1.1.22 2012-04-19		Updates agreed during RAMS-meeting: - H0018 amended - H0040 and H0043 concluded - H0045 deleted	DARI

		- Fields “found in “ and “solved in” replaced by field “relevant in”	
1.1.23 2012-07-30		Updated during and after RAMS-meeting to consider comments from UNISIG SG	DARI, AJ
1.1.24 2012-08-02		• Editorial improvements • Clarifications in H0018 • Reading notes introduced in chapter 3	DARI
1.1.25 2012-08-14		• Editorial improvements • Clarifications in H0025 • Numbering system improved in App B	DARI
1.1.26 2012-09-13		Updates agreed during RAMS-meeting: • Added reference to CR 650 in H0019 • Updated to consider additional comments from UNISIG SG • Updates in H0022 to cover new considerations	DARI
1.1.27 2012-10-02		• Updated to consider additional comments from UNISIG SG • H0045 added on SG advice • Third example of H0019 deleted, since now covered by H0045 case 2 • Minor editorial alignments	DARI
1.1.28 2012-10-31		• Updated to consider additional comments from UNISIG SG • Minor editorial alignments	DARI
1.1.29 2012-11-14		• Updated to consider additional comments from UNISIG SG	DARI

1.2.0 2012-11-16		Raised in issue for delivery to ERA. No changes in document.	DARI
1.2.1 2013-03/05	§3	Modification of introduction as specified in “20130130 minutes of ERA meeting on Subset113.docx”	AJ + DARI
1.2.2 2013-03-06	§ 3	Minor updates according to comments received from RAMS Group	
1.2.3 2013-09-09	all	Merge of HazLog 1.1.30 into SUBSET-113 1.2.3 to have a single document	DS
1.2.4 2013-10-22		Implementation of ERA comments	AJA
1.2.5 2013-12-12	all	Corrections according to RAMS Group internal review	DS
1.2.6 2013-12-19	All	Corrections due to rework check and enhancement of references	DS
1.2.7	§ 3.3.1.1	Change of “Category 1” definition	AJ
1.2.8 2014-05-28	ALL	Inclusion/modification of Hazards according to SUBSET-128 v100 Minor editorial changes to titles	AN
1.2.9 2014-06-03	ALL	Minor editorial changes for Hazard discussed in SUBSET-128 v1.0.0 coming from RAMS group internal review	AN
1.2.10 2014-06-05	ALL	Consolidation of Hazard taking into account updated SUBSET references and comments coming from implementation of ERA comments (ETCS-H0033, ETCS-H0038, and ETCS-H0037)	AN

1.2.11 2014-06-06	§4.22	Consolidation of ETCS-H0022 according to PhP comments (SG)	AN
1.2.12 2014-09-13	ALL	Deletion of reference to v2.3.0d Implementation of further ERA comments	AN
1.2.13 2014-10-15	§4.62, §4.38	Modification of Relevant in ETCS Baseline matrix according to RAMS WP feedbacks for ETCS-H0062 and added a note to Hazard description in ETCS-H0038	AN
1.2.14 2014-10-16	§4.53-§4.60	Hazards ETCS-H0053 to ETCS-H0060 deleted since not yet fully agreed with ERA	AN
1.2.15 2014-10-17	§4.33, §4.38 and §4.62, §3.4.1.1	Editorial changes and removal of EVC acronym (substituted by On-Board) Update of table 1 according to changes done for v1.2.14. modification of statements for ETCS-H0046 – ETCS-H0060	AN
1.2.16 2014-10-23	§3.1.1.5, §6.9.1.1, §6.10.1.1, §6.11.1.1, §6.12.1.1, §6.13.1.1, §6.14.1.1, §6.16.1.1, §6.17.1.1, §6.18.1.1, §6.19.1.1, §6.20.1.1, §6.21.1.1 and §6.22.1.1	Editorial changes. Sections 6.1 to 6.24 renumbered to 4.40 to 4.63.	SG
1.2.17 2015-xx-xx	§4.37, §4.68, §3.4	Editorial changes to ETCS-H0037 . Correction to table 1 for ETCS-H0035 Introduction of ETCS-H0068	AN
1.2.18	§4.69, §4,70,	Editorial changes. Reintroduction of ETCS-H0053 to ETCS-H0060	AN

		Introduction of ETCS-H0069 to ETCS-H0070. Update of table in 3.4.1.2	
1.2.19 2015-06-15	§4.71	Editorial changes, introduction of new hazards discussed during May 2015 RAMS meeting.	AN
1.2.20 2015-09-04	§4.73, §4.74, §4.75, §4.52, §4.3, §3.4.1.1	Introduction of hazards ETCS-H0073, ETCS-H0074, ETCS-H0075, update of ETCS-H0047, ETCS-H0048, ETCS-H0052, ETCS-H0003	AN
1.2.21 2015-12-01	§4.50, §4.76, §4.77, §4.68	Introduction of Hazard ETCS-H0050, ETCS-H0076, ETCS-H0077, update of ETCS-H0068,	AN
1.2.22 2016-02-03	§4.63, ALL	Update of ETCS-H0063 due to internal remarks Editorial update to align document to CR 1265 ETCS-H0001/0005/0012/0014/0015/0019/0020/0023/0025/0029/0033/0037/0039/0040/0042/0043/0044/0047/0050/0052/0054/0056/0057/0058/0059/0060/0061/0062/0069/0070/0074/0075/0076/0077 (introduction of reference SUBSET-026 v3.5.0 SUBSET-035 v3.2.0 SUBSET-036 v3.1.0 SUBSET-039 v3.2.0 SUBSET-040 v3.4.0 SUBSET-041 v3.2.0 SUBSET-091 v3.5.0). Modification to section “Relevant in ETCS baseline” due to the introduction of Baseline 3 Release 2. Changes done to table 1 due to the introduction of Baseline 3 Release 2. Changes to clause §3.2.1.5 to include the Baseline 3 Release 2	AN

		Changes to §3.4.1.2 due to the introduction of ETCS_H0076	
1.2.23 2016-03-02	ALL	Update during RAMS WP meeting 2016:02.	Martin Vlcek
1.2.24 2016-06-14	3.2.1.2, 3.2.1.5, 4.14, 4.42, 4.72, 4.73, 4.75	Update during RAMS WP meeting 2016:04 - SUBSET versions - CR 1128 reference removed from ETCS-H0072 and matrix updated - Hazards IDs H0078 and H0079 reserved for further use.	Martin Vlcek
1.2.25 2016-10-22	§4.29, §4.42, §4.59, §4.1, §4.5, §4.12, §4.14, §4.19, §4.20, §4.22, §4.23, §4.25, §4.29, §4.39, §4.40, §4.42, §4.43, §4.44, §4.50, §4.53, §4.54, §4.56, §4.57, §4.58, §4.59, §4.60, §4.61, §4.63, §4.68, §4.69, §4.70, §4.71, §4.72, §4.73, §4.74, §4.75, §4.76, Appendix B and C.	Changes done to §4.42 and §4.29 to include SG remarks. Change to “Relevant in ETCS baseline” in §4.59 to correct an editorial error in the matrix. Correction of reference to SUBSET-026 v3.6.0 for ETCS-H0001, ETCS-H0005, ETCS-H0012, ETCS-H0014, ETCS-H0019, ETCS-H0020, ETCS-H0022, ETCS-H0023, ETCS-H0025, ETCS-H0029, ETCS-H0039, ETCS-H0040, ETCS-H0042, ETCS-H0043, ETCS-H0044, ETCS-H0050, ETCS-H0053, ETCS-H0054, ETCS-H0056, ETCS-H0057, ETCS-H0058, ETCS-H0059, ETCS-H0060, ETCS-H0061, ETCS-H0063, ETCS-H0068, ETCS-H0069, ETCS-H0070, ETCS-H0071, ETCS-H0072, ETCS-H0073, ETCS-H0074, ETCS-H0075, ETCS-H0076, Appendix B and Appendix C.	AN

		Correction of reference to DMI ERA 015660 v3.6.0 for ETCS-H0075 Correction of reference to SUBSET-041 v3.2.0 for ETCS-H0061 Modifications to ETCS-H0068 to include correct reference to SUBSET-026 requirements Introduction of ETCS-H0080, ETCS-H0081, ETCS-H0082, and ETCS-H0083,	
1.2.26 2016-10-26	ALL	Update of ETCS-H0061 (based on SG feedbacks), update of ETCS-H0079 to ETCS-H0083. Various editorial updates.	AN
1.2.27 2016-11-03	§4.12, §4.18, §4.22, §4.26, §4.38, §4.61	Fine-tuning for the closure of the 2014 ERA review cycle	LR
1.2.28 2017-01-27	§3.2.1.5, §3.3.1 first bullet, §4, §4.42, §4.45, §4.50, §4.52, §4.63, §4.74, §4.75, §4.76, §4.77, §4.79, §4.80, §4.81, §4.83, §4.84, Annex B	Implementation of remarks #1, #2, #3, #5, #6, #7, #8, #9, #10, #12, #14, #15, #19, #20, #21,#22, #23, #24, #25, #26, #28, #30, #31, #33, #34, #35 and #37 coming from ERA review sheet	AN
1.2.29 2017-03-01	§4.18, §4.50, §4.61, §4.69, §4.71, §4.73, §4.78, §4.81, §4.83, §4.75, table 1 in §3.4.1.1 for ETCS-H0084 and ETCS-H0029, Annex C	Implementation of remarks #4, #7, #9, #14, #16, #17, #24 and #34 of ERA review sheet 9/2/2017 EECT remarks for H0084 and action 27.05 due to EECT meetings.	AN

1.2.30 2017-10-17	§4.12, §4.29, §4.68, §4.73, §4.75, §4.78, §4.79, §4.80, §4.81, §4.82, §4.83, §4.85, §4.86, §4.87, §4.88, §4.89, §4.90, §4.91, §4.92, §4.93 and Appendix C	Inclusion of Hazards ETCS-H0085, ETCS-H0086, ETCS-H0087, ETCS-H0088, ETCS-H0089, ETCS-H0090, ETCS-H0091, ETCS-H0092 and ETCS-H0093 as part of the BCA 2017 process. Changes to hazards: ETCS-H0012, ETCS-H0029, ETCS-H0068, ETCS-H0073, ETCS-H0078, ETCS-H0079, ETCS-H0081, ETCS-H0082, ETCS-H0083 as part of the BCA 2017 process ETCS-H0080 deleted as part of the BCA 2017 process Updates to H0075.	AN
1.2.31 2017-11-29	§4.12, §4.29, §4.73, §4.81, §4.82, §4.87, §4.90	Changes done to further alignment of SUBSET 113 to BCA report 2017 v1.0.0	AN
1.2.32 2017-12-06	§3.1.1.2, §4.77, §3.4.1.1, §4.79,	Inclusion of reference to B2 requirements in H0077, correction in table 1 for H0078, reference to SUBSET 041 version in H0079,. Alignment of RAMS WP	AN
1.2.33	All	Change to document title to “ETCS Hazard Log” Change to mitigations title to “Proposed Mitigation” Change to the footer of the document to align it to the title Removal of H0075 as not being finalized in the EECT meetings	AN
1.3.0 2018-02-05	-	Release version	AN

1.3.1 2019-02-18		TRK acronym removed in hazard 18. Inclusion of Hazards H0094, H0095, H0096, H0097. Entry created for H0098, H0099, H0100, H0101, H0102, H0103, H0104 and H0105. Changes done on H0019. Changes done on H0087. Changes done on table 1	AN
1.3.2 2019-02-21		Inclusion of Hazards ETCS_H0101, ETCS_H0102, ETCS_H0103, ETCS_H0105. H0096 deleted as considered not relvant for any ETCS baseline Changes done on table 1	AN
1.3.3 2020-05-19		Alignment to TO-2020 (Changes to ETCS-H0103 to remove OBU and use ERTMS/ETCS on-board instead, Update of ETCS-H0097, Removal of scenario 1.b in ETCS-H0084, Inclusion of ETCS-H0107 ETCS-H0108	AN
1.3.4 2020-07-27		Inclusion of Hazards ETCS_H0111 ETCS_H0115 Definition of ETCS_H0116 ETCS_H0117 ETCS_H0118 ETCS_H0119 Changes done on table 1 Introduction of §3.1.1.8	AN

1.3.5 2020-08-31		Inclusion of Hazards: ETCS_H0117 ETCS_H0118 Update of table 1	AN
1.3.6 2020-09-25		Inclusion of Hazards: ETCS_H0116 Update of table 1	AN
1.3.7 2020-09-28		Removal of Hazard ETCS_H0095 Corrections to Table 1 ETCS-H0020 corrections to cross references	AN
1.3.8 2020-11-02		Corrections to Table 1 and Section 3.5	AN
1.3.9 2020-12-02		Correction to proposed mitigation in ETCS_H0116 Correction 3.1.1.8 base on SG comment	AN
1.3.10 2021-03-15		Definition of: ETCS_H0120 ETCS_H0121, ETCS_H0122, ETCS_H0123 Update of table 1 Editorial change in ETCS_H0116 Change to hazard description as per comments in ETCS_H0019 Update to Annex B Inclusion of CR1384 picture in ETCS_H0114 “UNISIG Hazard Log” wording changed to “ETCS Hazard Log” in (§3.1.1.1, §3.1.1.5, §3.5.1.1, §3.5.1.2 1st bullet, §3.5.1.2 2nd bullet).	AN

1.3.11 2021-03-26		Removal of picture in ETCS-H0114, Removal of term “by ERA” in the last bullet of clause 3.5.1.2 Removal of the text “The hazard has not been considered as relevant for any ETCS baseline” in the ETCS-H0008, Alignment of bullets in 3.3.1.1, Change to section break in 3.4 Relevant in ETCS baseline matrix restored in ETCS-H0070	AN
1.4.0 2021-03-30		Release version	AN
1.4.1 2021-08-31		Correction to table in 3.4.1.3 for H0110 Inclusion of the following hazards agreed during EECT meetings: - ETCS-H0119 - ETCS-H0121 - ETCS-H0122 - ETCS-H0123 - ETCS-H0124 - ETCS-H0125 Changes to table 1 and 2	AN

1.4.2 2022-04-08		Update of the first page, Inclusion of the following hazards: - ETCS-H0115 - ETCS-H0127 - ETCS-H0128 - ETCS-H0130 - ETCS-H0131 - ETCS-H0132 Changes to table 1 and 2	AN
1.5.0 2022-05-10		Release version	AN

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1 Background and Purpose

3.1.1.1 The ETCS Hazard Log is a list of scenarios possibly leading to hazards when implementing an ETCS system. In this sense, the issues are *causes* in the definition of EN 50129. The hazard log is intended as a complement to the systematic safety analyses of the interfaces performed by UNISIG in SUBSET-088 parts 1 and 2.

3.1.1.2 The causes originate mainly from feedback from application projects reported to the UNISIG RAMS WP. A hazard is included in the hazard log when the following two criteria are fulfilled:

- The hazard is deemed not obvious and might therefore not be identified easily by other application projects
- The corresponding safety risk is deemed high enough to require a mitigation

3.1.1.3 Each application project is responsible to have an exhaustive risk assessment for its scope. The present hazard log is not claimed to be an exhaustive list of causes for hazards, but shall be considered as one input among others to the application project's risk assessment.

3.1.1.4 The recommended mitigations embedded in this document are provided as guidance to trackside implementation projects. Whether or not a particular mitigation is applicable, suitable, or necessary to implement in any particular project, is the responsibility of each individual implementation of ERTMS/ETCS.

3.1.1.5 The present document is a report from the ETCS Hazard Log, intended to export safety relevant issues to application projects that implement one of the baselines listed in the TSI CCS.

3.1.1.6 In order not to impair interoperability of ETCS, no mitigation has been allocated to ERTMS/ETCS On-Board.

3.1.1.7 Note: this document describes technical and operational solutions possibly capable to mitigate the identified hazards. This does not ensure, anyway, that such solutions are always applicable without any condition: the provisions of the TSI CCS preventing that requirements endangering interoperability are exported across the interface track-train must be respected. This applies both to technical and operational issues.

3.1.1.8 Even when not explicitly written in a hazard log entry, each project shall evaluate if the residual risk, if any, is acceptable.

3.2 Reading Notes

3.2.1.1 The template used for each hazard is believed to be self-explanatory.

3.2.1.2 One thing that however deserves to be pointed out is the heading "Relevant in ETCS baseline". It is a table which contains a "Y" (=Yes) if the hazard is deemed relevant for

that particular combination of ERTMS/ETCS On-Board and Trackside system baselines, and an “N” (=No) if not.

3.2.1.3 The same formulation has been used in Table 1: Hazard categorisation and applicability according to trackside baseline. A “Y” should be understood as the hazard being applicable to the referred trackside baseline.

3.2.1.4 Regarding incompatible baselines, the combination of ERTMS/ETCS On-Board baseline 2 and Trackside baseline 3, X=2, is generally marked as “n/a” (=not applicable) because of the reasons stated in §3.4.1.2[1]. However, there are a few exceptions where the hazard occurs in Level 0/NTC and where there is no specific trackside message involved; these are marked as “Y” also for the combination of ERTMS/ETCS On-Board baseline 2 and Trackside baseline 3, X=2.

3.2.1.5 In the tables:

- B2 has to be understood as SUBSET-026 v2.3.0 + SUBSET-108 v1.2.0 and the rest of the documents specified in the set #1 of the Annex A of TSI CCS. In cases where the text in SUBSET-026 v2.3.0 is modified by SUBSET-108 v1.2.0, this is specifically noted in order to provide a full tracing. Older versions (e.g. “2.2.2”) are not covered by this document;
- B3MR1 has to be understood as SUBSET-026 v3.4.0 and the rest of the documents specified in the set #2 of the Annex A of TSI CCS;
- B3R2 has to be understood as SUBSET-026 v3.6.0 and the rest of the documents specified in the set #3 of the Annex A of TSI CCS.

3.2.1.6 In the context of B2, “Level NTC” has to be read “Level STM”.

3.3 Hazard Categories

3.3.1.1 The hazards have been classified into 2 types:

- Category 1: Hazards linked to shortcomings in the ETCS specification. Such a shortcoming is handled via the ERA Change Control Management.
- Category 2: Hazards related to the integration of ETCS in an overall operational signalling system. These hazards can be mitigated by the use of rules (e.g. engineering rules, operational rules).

3.3.1.2 The link between hazard and category is indicated in Table 1: Hazard categorisation and applicability according to trackside baseline.

[1] Note that the X for Trackside version shall be understood as the X of the trackside message involved in the hazardous scenario. This is an important distinction when there is a mix of messages with X=1 and X=2 inside a trackside area.

3.4 Applicability of hazards based on baselines

3.4.1.1 In order for projects to identify easily the hazards associated to the baseline used, an applicability table is integrated hereafter:

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0001	Category 2	Y	Y	Y	Y	Y
ETCS-H0002	Category 2	Y	Y	Y	Y	Y
ETCS-H0003	Category 2	Y	Y	Y	Y	Y
ETCS-H0004	Intentionally left empty.					
ETCS-H0005	Category 2	Y	Y	Y	Y	Y
ETCS-H0006	Intentionally left empty.					
ETCS-H0007	Intentionally left empty.					
ETCS-H0008	Intentionally left empty.					
ETCS-H0009	Intentionally left empty.					
ETCS-H0010	Intentionally left empty.					
ETCS-H0011	Intentionally left empty.					
ETCS-H0012	Category 1	Y	Y	Y	Y	Y
ETCS-H0013	Intentionally left empty.					

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0014	Category 2	Y	Y	Y	Y	Y
ETCS-H0015	Intentionally left empty.					
ETCS-H0016	Category 1	Y	Y	N	Y	N
ETCS-H0017	Intentionally left empty.					
ETCS-H0018	Category 1	Y	N	N	N	N
ETCS-H0019	Category 2	Y	Y	Y	Y	Y
ETCS-H0020	Category 1	Y	Y	N	Y	N
ETCS-H0021	Category 2	Y	Y	Y	Y	Y
ETCS-H0022	Category 2	Y	Y	Y	Y	Y
ETCS-H0023	Category 2	Y	Y	Y	Y	Y
ETCS-H0024	Category 1	Y	Y	N	Y	N
ETCS-H0025	Category 2	Y	Y	Y	Y	Y
ETCS-H0026	Category 1	Y	Y	N	Y	N
ETCS-H0027	Intentionally left empty.					
ETCS-H0028	Category 2	Y	Y	Y	Y	Y
ETCS-H0029	Category 1	Y	Y	Y	Y	Y

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0030	Category 1	Y	Y	N	Y	N
ETCS-H0031	Category 1	Y	Y	N	Y	N
ETCS-H0032	Category 1	Y	Y	N	Y	N
ETCS-H0033	Category 1	Y	Y	N	Y	N
ETCS-H0034	Intentionally left empty.					
ETCS-H0035	Category 1	Y	Y	N	Y	N
ETCS-H0036	Intentionally left empty.					
ETCS-H0037	Category 1	Y	Y	Y	Y	Y
ETCS-H0038	Category 2	Y	Y	Y	Y	Y
ETCS-H0039	Category 2	Y	Y	Y	Y	Y
ETCS-H0040	Category 2	Y	Y	Y	Y	Y
ETCS-H0041	Category 1	Y	Y	N	Y	N
ETCS-H0042	Category 2	N	Y	Y	Y	Y
ETCS-H0043	Category 2	N	Y	Y	Y	Y
ETCS-H0044	Category 2	Y	Y	Y	Y	Y
ETCS-H0045	Category 1	Y	Y	Y	Y	Y

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0046	Intentionally left empty.					
ETCS-H0047	Category 1	Y	Y	Y	Y	Y
ETCS-H0048	Intentionally left empty.					
ETCS-H0049	Intentionally left empty.					
ETCS-H0050	Intentionally left empty.					
ETCS-H0051	Intentionally left empty.					
ETCS-H0052	Intentionally left empty.					
ETCS-H0053	Category 1	Y	Y	N	Y	N
ETCS-H0054	Category 2	Y	Y	Y	Y	Y
ETCS-H0055	Category 1	Y	Y	N	Y	N
ETCS-H0056	Category 1	Y	Y	N	Y	N
ETCS-H0057	Category 1	Y	Y	N	Y	N
ETCS-H0058	Category 1	Y	Y	N	Y	N
ETCS-H0059	Category 1	Y	Y	N	Y	N
ETCS-H0060	Category 1	Y	Y	N	Y	N
ETCS-H0061	Category 2	Y	Y	Y	Y	Y

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0062	Category 1	Y	Y	N	Y	N
ETCS-H0063	Category 2	Y	Y	Y	Y	Y
ETCS-H0064	Intentionally left empty.					
ETCS-H0065	Intentionally left empty.					
ETCS-H0066	Intentionally left empty.					
ETCS-H0067	Intentionally left empty.					
ETCS-H0068	Category 1	Y	Y	Y	Y	Y
ETCS-H0069	Intentionally left empty.					
ETCS-H0070	Category 1	Y	Y	Y	Y	Y
ETCS-H0071	Intentionally left empty.					
ETCS-H0072	Category 1	Y	Y	N	Y	N
ETCS-H0073	Category 1	Y	Y	Y	Y	Y
ETCS-H0074	Category 2	Y	Y	Y	Y	Y
ETCS-H0075	Category 2	Y	Y	Y	Y	Y
ETCS-H0076	Category 2	N	N	Y	N	Y
ETCS-H0077	Category 1	Y	Y	Y	Y	Y

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0078	Category 1	N	Y	Y	Y	Y
ETCS-H0079	Category 1	Y	Y	Y	Y	Y
ETCS-H0080	Intentionally left empty.					
ETCS-H0081	Category 1	Y	Y	Y	Y	Y
ETCS-H0082	Category 1	Y	Y	Y	Y	Y
ETCS-H0083	Category 1	Y	Y	Y	Y	Y
ETCS-H0084	Category 2	Y	Y	Y	Y	Y
ETCS-H0085	Category 1	Y	Y	Y	Y	Y
ETCS-H0086	Category 1	Y	Y	Y	Y	Y
ETCS-H0087	Category 1	Y	Y	Y	Y	Y
ETCS-H0088	Category 1	Y	Y	Y	Y	Y
ETCS-H0089	Category 1	Y	Y	Y	Y	Y
ETCS-H0090	Category 1	Y	Y	Y	Y	Y
ETCS-H0091	Category 1	Y	Y	Y	Y	Y
ETCS-H0092	Category 1	Y	Y	Y	Y	Y

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0093	Category 1	N	Y	Y	Y	Y
ETCS-H0094	Category 1	Y	Y	Y	Y	Y
ETCS-H0095	Under Analysis.					
ETCS-H0096	Intentionally left empty.					
ETCS-H0097	Category 1	Y	Y	Y	Y	Y
ETCS-H0098	Intentionally left empty.					
ETCS-H0099	Under Analysis.					
ETCS-H0100	Intentionally left empty.					
ETCS-H0101	Category 1	Y	Y	Y	Y	Y
ETCS-H0102	Category 1	Y	Y	Y	Y	Y
ETCS-H0103	Category 1	Y	Y	Y	Y	Y
ETCS-H0104	Intentionally left empty.					
ETCS-H0105	Category 1	Y	Y	Y	Y	Y
ETCS-H0106	Category 1	Y	N	N	N	N
ETCS-H0107	Category 2	Y	Y	N	Y	N
ETCS-H0108	Category 1	Y	Y	N	Y	N

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0109	Under Analysis.					
ETCS-H0110	Category 1	Y	Y	Y	Y	Y
ETCS-H0111	Category 1	Y	Y	Y	Y	Y
ETCS-H0112	Category 1	Y	Y	Y	Y	Y
ETCS-H0113	Intentionally left empty.					
ETCS-H0114	Category 1	Y	Y	Y	Y	Y
ETCS-H0115	Category 2	Y	Y	Y	Y	Y
ETCS-H0116	Category 1	Y	Y	Y	Y	Y
ETCS-H0117	Category 1	Y	Y	Y	Y	Y
ETCS-H0118	Category 1	Y	Y	Y	Y	Y
ETCS-H0119	Category 1	Y	Y	Y	Y	Y
ETCS-H0120	Under Analysis					
ETCS-H0121	Category 1	Y	Y	Y	Y	Y
ETCS-H0122	Category 1	Y	Y	Y	Y	Y
ETCS-H0123	Category 1	Y	Y	Y	Y	Y
ETCS-H0124	Category 1	Y	N	N	N	N

Hazard	Category	Trackside Baseline				
		B2	B3MR1		B3R2	
			X=1	X=2	X=1	X=2
ETCS-H0125	Category 1	N	Y	Y	Y	Y
ETCS-H0126	Intentionally left empty, Hazard ID not used.					
ETCS-H0127	Category 1	Y	Y	Y	Y	Y
ETCS-H0128	Category 1	N	Y	Y	Y	Y
ETCS-H0129	Under Analysis					
ETCS-H0130	Under Analysis					
ETCS-H0131	Category 1	Y	Y	Y	Y	Y
ETCS-H0132	Category 1	Y	Y	Y	Y	Y

Table 1: Hazard categorisation and applicability according to trackside baseline

3.4.1.2 An ERTMS/ETCS On-Board system in baseline 2 is not compatible with a Trackside system in baseline 3, X=2. Therefore analysis of such operation is not in the scope of the UNISIG safety analysis. Technically, it is possible for an ERTMS/ETCS On-Board baseline 2 to run on a Trackside baseline 3, X=2, without being tripped, in Level 0 and NTC. This specific situation is treated in ETCS-H0076.

3.4.1.3 The following table provides the traceability between Hazards identified as Category 1 and the related CR that was created to address the Hazardous scenario. When the CR is part of the ERA-OPI-2020/2, a reference is given:

Hazard	CR	ERA-OPI-2020-2
ETCS-H0012	1264	x
ETCS-H0016	842	
ETCS-H0018	782	
ETCS-H0020	897	
ETCS-H0024	854	
ETCS-H0026	659	
ETCS-H0029	887	x
ETCS-H0030	895	
ETCS-H0031	899	
ETCS-H0032	484	
ETCS-H0033	1071	
ETCS-H0035	923	
ETCS-H0037	1168	
ETCS-H0041	896	
ETCS-H0045	919, 650	
ETCS-H0047	1088	
ETCS-H0053	866	
ETCS-H0055	844, 1096	
ETCS-H0056	843	
ETCS-H0057	710	
ETCS-H0058	819	
ETCS-H0059	1030	
ETCS-H0060	1183	
ETCS-H0062	618	
ETCS-H0068	1288	x
ETCS-H0070	933	

Hazard	CR	ERA-OPI-2020-2
ETCS-H0072	548	
ETCS-H0073	1252	x
ETCS-H0077	1229	
ETCS-H0078	1295	x
ETCS-H0079	1296	x
ETCS-H0081	1120	x
ETCS-H0082	1251	x
ETCS-H0083	1259	x
ETCS-H0085	1252	x
ETCS-H0086	940	x
ETCS-H0087	994, 1312, 1334	x
ETCS-H0088	1166	x
ETCS-H0089	1293	x
ETCS-H0090	1300	x
ETCS-H0091	1306	x
ETCS-H0092	1306	x
ETCS-H0093	1306	x
ETCS-H0094	1282	x
ETCS-H0097	1318	x
ETCS-H0101	1313	x
ETCS-H0102	1313	x
ETCS-H0103	1327	x
ETCS-H0105	1325	x
ETCS-H0106	1335	x
ETCS-H0108	342, 638	
ETCS-H0110	1347, 1354	x
ETCS-H0111	1389	
ETCS-H0112	1312	
ETCS-H0114	1348	x
ETCS-H0116	1354	
ETCS-H0117	1358	
ETCS-H0118	1376	
ETCS-H0119	1377	
ETCS-H0121	1384	

Hazard	CR	ERA-OPI-2020-2
ETCS-H0122	1384	
ETCS-H0123	1384	
ETCS-H0124	1395	
ETCS-H0125	1396	
ETCS-H0127	1418	
ETCS-H0128	1372	
ETCS-H0131	1411	
ETCS-H0132	1419	

Table 2: look-up table between all the Category 1 hazards and the related CRs

3.5 Hazard management

3.5.1.1 The ETCS Hazard Log is a living document, based on the information received regarding the hazards discovered during the life cycle of all application projects.

3.5.1.2 The management of the hazards listed in the current document is the following:

- when a new hazard has been identified, the ETCS Hazard Log is updated to integrate it
- this report from the ETCS Hazard Log is regularly updated
- a hazard entry is intentionally left empty when the hazard is not complete or the hazard is not considered as relevant for any ETCS baseline.

4. REPORT FROM HAZARD LOG

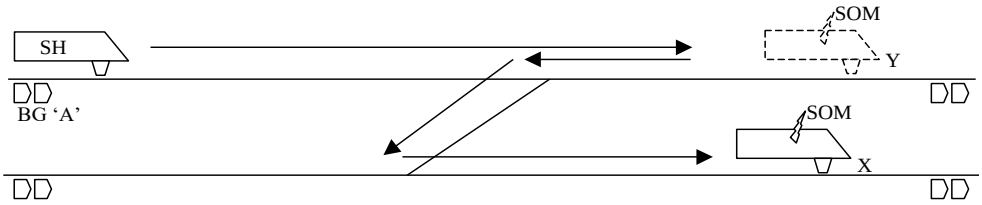
4.1 ETCS-H0001

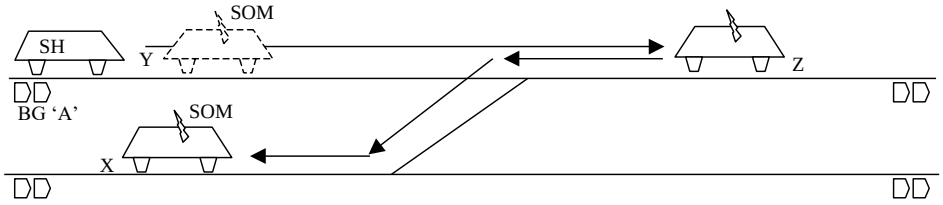
<table>
<tr><td>Hazard ID</td><td>ETCS-H0001</td></tr>
<tr><td>Hazard headline</td><td>Possible overrun of Supervised Location in case the release speed is not calculated On-Board</td></tr>
<tr><td>Hazard description</td><td>ERTMS/ETCS On-Board will allow a train to pass the End of Authority (EoA) in release speed (given by trackside) with a distance equal to the odometer over-reading error before it trips the train, ref SUBSET-026 v2.3.0 section §3.13.8 / SUBSET-026 v3.4.0 section §3.13.10.2.6 / SUBSET-026 v3.6.0 section §3.13.10.2.6 and §7. Moreover, in release speed monitoring, the monitoring of Supervised Location (SvL) is not active.
Therefore, a hazardous situation could arise if:
• The protection of the Supervised Location must be ensured by ETCS, AND
• The driver does not respect the EoA, AND
• There is no balise group with order to trip the train in connection with the EoA, AND
• The trip initiated when the min safe front end (or antenna position in Level 1) passes EoA, is not enough to stop the train before SvL. This could happen if the odometer over-reading error is larger than expected during engineering of EoA and SvL:
  • the ERTMS/ETCS On-Board performs worse than the accuracy requirement for position measured by the ERTMS/ETCS On-Board in SUBSET-041 v2.1.0, v3.1.0 and v3.2.0 section §5.3.1.1, OR
  • there has been no reset of confidence interval due to missing of the relocation balise group close to EoA., OR
  • the ETCS Trackside does not consider a delay between passing EOA and transition to TR mode (applying the emergency brake) as defined for B3 ERTMS/ETCS On-Board or B2 ERTMS/ETCS On-Board implementing CR 977</td></tr>
<tr><td>Proposed mitigation</td><td>The combined probability of these events might be judged as sufficiently low. However, the wayside engineering must do its most in order to avoid this hazard.
The trackside shall calculate the release speed in such a way to enable the train to stop before the SvL. This calculation is based on the assumption that the ERTMS/ETCS On-Board performs according to its accuracy requirements. In order to minimise the probability of the ERTMS/ETCS On-Board performing worse than the accuracy requirements, a relocation balise group could be placed close to the EoA. Moreover, the trackside shall also consider the ERTMS/ETCS On-Board delay of 1 sec (according to SUBSET-041 v3.1.0 or v3.2.0, clause §5.2.1.13) as a delay between passing an EOA/LOA and applying the emergency brake.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.2 ETCS-H0002

<table>
<tr><td>Hazard ID</td><td>ETCS-H0002</td></tr>
<tr><td>Hazard headline</td><td>Loss of a Position report indicating change from FS/OS mode to SR mode</td></tr>
<tr><td>Hazard description</td><td>The loss of a Position Report indicating a mode change from FS/OS to SR may be hazardous. In this situation the RBC will rely on an old position report and furthermore is not aware of the mode change of the ERTMS/ETCS On-Board to the mode SR. If the train then moves in SR, the RBC will try to send an updated MA (because it thinks the ERTMS/ETCS On-Board is in FS/OS mode), without having updated position information. If the RBC doesn’t have any additional position information from e.g. interlocking, it will then generate an MA under wrong conditions and possibly associate the ERTMS/ETCS On-Board with the wrong route (set for another train at the original position of SR train). The MA will be sent to the ERTMS/ETCS On-Board in SR, which is already waiting for a new MA, because the aim from the operational point of view is to leave the SR mode as soon as possible.</td></tr>
<tr><td>Proposed Mitigation</td><td>When generating and sending an MA to the ERTMS/ETCS On-Board, the RBC shall consider the possibility of a mode change from FS/OS to SR by the ERTMS/ETCS On-Board that is not known by the RBC</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

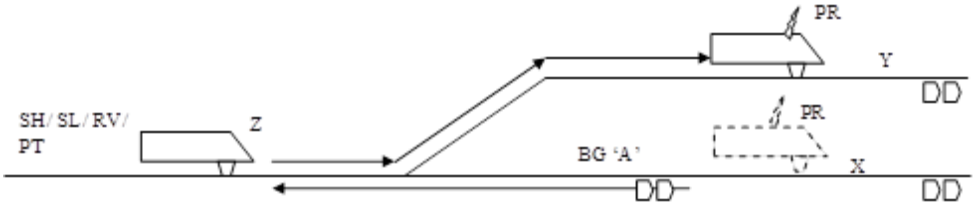
4.3 ETCS-H0003

Hazard ID	ETCS-H0003
Hazard headline	On-Board start of mission position report after movement towards LRBG
Hazard description	Current situation: – A train in SH continues to supervise its location even when running backward. – In the same way, train continues to supervise its location after change of cabin. Such a train may then change of track without crossing over new Balise Group(s) or missing existing one. During Start of Mission (SoM), the ERTMS/ETCS On-Board sends then a valid SoM Position Report that could be ambiguous to the RBC and in worst case relate to an LRBG that may be on another track. As the Position Report is valid, the RBC could consider the train in a wrong place and could deliver a wrong MA. See below examples. ***1) Movement in SH*** Train enters SH mode after passing BG 'A'. ERTMS/ETCS On-Board supervises its location related to BG 'A'. When in SH, train runs backward and changes track (from the "upper" to the "lower" track, see figure). When the train arrives in position 'X', ERTMS/ETCS On-Board performs Start of Mission connecting to the RBC and giving its valid position report with BG 'A' as LRBG. As the position report is valid, RBC could think that the train is in position 'Y'. If a route is set in front of 'Y' position, RBC may send an MA for the "upper" track to the train, which is actually intended for the "lower" track.  ***2) Change of cabin*** Train enters SH mode after passing BG 'A'. ERTMS/ETCS On-Board supervises its location related to BG 'A'. When in SH, train runs up to position 'Z' and then the driver changes cabin (from the right to the left cabin, see figure). Then, two things can happen: - ERTMS/ETCS On-Board enters SH mode (SH → SB → SH or SH→SB + NL→SH or SH→SB + SL→SH) or - ERTMS/ETCS On-Board enters SR mode (SH → SB → SR or SH→SB + NL→SR or SH→SB + SL→SR) The train runs then up to position 'X'. When the train arrives in position 'X', ERTMS/ETCS On-Board performs Start a Mission connecting to the RBC and giving its valid position report with BG 'A' as LRBG. As the position report is valid, RBC could think that the train is in position 'Y'. If a route is set in front of 'Y' position, RBC may send an MA to the train, which is actually intended for the "lower" track.



3) ***Train moving in backward direction***

Due to constraints on the trackside it might be not possible to add or move balise groups already placed on the line. So If there is no balise group before the railway switch or balise groups on different tracks are not placed approximatively at the same distance after the switch, an ambiguity on the train position may arise.



In this scenario given in the above picture the ERTMS/ETCS On-Board moves backward in SH/SL/RV/PT mode and detects only BG A. the train stops at position Z and then moves forward running on the upper part of the line. When the train is in Y, whatever if the train sends a Position Report or a SoM Position Report, the train is reporting its position as if it were in position X

Proposed mitigation

Either:

1. Trackside engineering shall ensure that a valid position reported by a train can be trusted, i.e. is unambiguous, OR
2. RBC shall evaluate position reports in an area with different routes in a way that takes into account the possibility of a position ambiguity.

Solution 1 might be difficult to implement on some infrastructures. Solution 2 is systematic but likely to lead to a loss of performance.

Mitigation allocated to

TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.4 ETCS-H0004

4.4.1.1 Intentionally left empty. No action by application projects is required.

4.5 ETCS-H0005

<table>
<tr><td>Hazard ID</td><td>ETCS-H0005</td></tr>
<tr><td>Hazard headline</td><td>Missing National Values more restrictive than Default Values</td></tr>
<tr><td>Hazard description</td><td>In certain degraded situations defined in SUBSET-026, section §3.18.2.5 for v2.3.0, v3.4.0 and v3.6.0, ERTMS/ETCS On-Board shall use Default Values instead of National Values. If these Default Values are less restrictive than the National Values, an unsafe supervision might result.
Furthermore, note that the safe ceiling speed in Unfitted will be according to the National Values. Therefore, if passing a border in an unfitted area without border balises, the “old” National Values will still apply.</td></tr>
<tr><td>Proposed mitigation</td><td>If an infrastructure uses National Values more restrictive than the Default Values as defined in SUBSET-026, chapter 3, annex A3.2 (v2.3.0, v3.4.0 and v3.6.0), the National Values must be repeated in appropriate balise groups or radio messages. Which balise groups or radio messages this applies to must be analysed in a specific application, however typical examples can be balise groups after stations etc.
Note: When announcing national values in advance (D_VALIDNV), it should be considered that an ERTMS/ETCS On-Board powering off, will lose its announced and not yet applicable national values.
Note: the hazard is further analysed in ETCS-H0057</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.6 ETCS-H0006

4.6.1.1 Intentionally left empty. No action by application projects is required.

4.7 ETCS-H0007

4.7.1.1 Intentionally left empty. No action by application projects is required.

4.8 ETCS-H0008

4.8.1.1 Intentionally left empty. No action by application projects is required.

4.9 ETCS-H0009

4.9.1.1 Intentionally left empty. No action by application projects is required.

4.10 ETCS-H0010

4.10.1.1 Intentionally left empty. No action by application projects is required.

4.11 ETCS-H0011

4.11.1.1 Intentionally left empty. No action by application projects is required.

4.12 ETCS-H0012

Hazard ID	ETCS-H0012
Hazard headline	ERTMS/ETCS On-Board reverts actions related to MA timers while not expected by trackside
Hazard description	The following hazardous scenarios describe how ERTMS/ETCS On-Board can have a valid MA On-board while it is not expected by the trackside (The actions related to the start or stop location of MA timers are reverted without being expected by trackside with the consequence that the proper correlation with timers running in the interlocking is lost): 1. Section timer SUBSET-026 requires to stop the MA section timer when the min safe front end of the train has passed the section time-out stop location (see §3.8.4.2.3 for v2.3.0, v3.4.0 and v3.6.0). It means that once the section time-out stop location is passed, the related section remains "locked" for the train, from ERTMS/ETCS On-Board point of view. If the train then moves backwards, (D_NVROLL) in such a way that it clears the route, the interlocking, depending on its implementation, may revoke the no longer occupied route (possibly delayed by a route release timer). However, the MA in the ERTMS/ETCS On-Board still remains valid. This may result in an unsafe situation. 2. End Section timer According to SUBSET-026 §3.8.4.1.1 (for v2.3.0, v3.4.0, and v3.6.0), the End Section timer shall be started by ERTMS/ETCS On-Board when the train passes with its max safe front end the End Section timer start location given by trackside. If the train stops further than the interlocking timer start location and then moves backwards (D_NVROLL) in such a way that its max safe front end is again located before the End Section timer start location, it is not defined how to manage the End Section timer. Thus, ERTMS/ETCS On-Board can stop or reset this timer and this may result in an unsafe situation (because the MA in the ERTMS/ETCS On-Board remains valid longer than expected). 3. Overlap timer According to SUBSET-026 §3.8.4.4.1 (for v2.3.0, v3.4.0, and v3.6.0), the Overlap timer shall be started by the ERTMS/ETCS On-Board when the train passes the Overlap timer start location given by trackside with its max safe front end. If the train stops further than the interlocking timer start location and then moves backwards (D_NVROLL) in such a way that its max safe front end is again located before the Overlap timer start location, then it is not defined how to manage the Overlap timer. Thus, the ERTMS/ETCS On-Board can stop or reset this timer and this may result in an unsafe situation because the MA in the ERTMS/ETCS On-Board remains valid longer than the overlap is secured by the interlocking Physically the train speed must have been 0 km/h for an indeterminate time between moving forwards and subsequently moving backwards. If the ERTMS/ETCS On-Board recognizes this as an occurrence of standstill there is no hazardous situation because the overlap will be revoked. However, an ERTMS/ETCS On-board may not have determined this standstill when going forward and then almost immediately backwards at very low speed because the exact conditions for determining standstill are supplier specific and may require for example that odometry reports a speed of 0 km/h for a certain duration. In that case the ERTMS/ETCS On-Board may use the overlap when it is no longer secured by the interlocking. Note: it is considered that the case of relocation is not relevant. The reason are the following: Scenario 1: It is assumed that the train reaches with the fist axle the section before it reaches with the minimum safe front end the section timer stop location. For this reason a

	relocation case has no impact: once the train has reached the stop section timer location with the minimum safe front end, it may happen that the minimum safe front end moves again in rear of the stop section timer due to relocation, but it would not be relevant if the ERTMS/ETCS On-Board reverts or not the action related to passing the timer stop location because the section is occupied so guaranteed for this train by the interlocking. Scenarios 2 and 3: It is assumed that the ERTMS/ETCS On-Board starts the timer in the same location where the interlocking starts the corresponding timer or in rear of it. For this reason the relocation has no safety impact: a relocation which happens after the maximum safe front end has passed the ETCS timer start location and after the interlocking has started its timer (first axle of the train is further than interlocking timer start location) cannot lead to a jump of the maximum safe front end in rear of the ETCS timer start location. The reason is that the first axle is in advance of the interlocking timer start location. This means that the real front of the train is further than the ETCS timer start location and therefore the maximum safe front end cannot jump to a location in rear of it.
Proposed mitigation	This has to be solved in trackside project specific analysis. Scenario 1: One possible solution is that when the train has crossed the MA section time-out stop location (D_SECTIONTIMERSTOPLOC), the interlocking considers the section as “locked”, even if after that the train moves backwards and then no more occupies this section. Scenario 2: One possible solution is that the interlocking stops the timer (it will consider it as never expired) as soon as it detects a sequential movement backwards and/or to have the ETCS end section timer start location far enough from the operational stopping point to avoid that it is overpassed when rolling backwards would also decrease a lot the probability of the hazard and/or to have a minimum distance between the ETCS end section timer start location and the interlocking timer start location of the end section: distance from the front of the train to first axle+ D_NVROLL +braking distance for the brake applied due to exceeding D_NVROLL. Scenario 3: One possible solution is that the interlocking stops the timer (it will consider it as never expired) as soon as it detects a sequential movement backwards and/or to have the ETCS overlap timer start location far enough from the operational stopping point to avoid that it is overpassed when rolling backwards would also decrease a lot the probability of the hazard or/and to have a minimum distance between the ETCS overlap start location and the interlocking overlap timer start location: distance from the front of the train to first axle+ D_NVROLL+braking distance for the brake applied due to exceeding D_NVROLL Note: The aim of the last mitigation of scenario 2 and 3 is to ensure that for the first backwards movement the condition that would trigger the reversion of the timer would not be fulfilled. Taking the worst case of a backward movement, this distance corresponds to: distance from the front of the train to first axle+ D_NVROLL +braking distance for the brake applied due to exceeding D_NVROLL.
Mitigation allocated to	TRACKSIDE and EXTERNAL

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.13 ETCS-H0013

4.13.1.1 Intentionally left empty. No action by application projects is required.

4.14 ETCS-H0014

<table>
<tr><td>Hazard ID</td><td>ETCS-H0014</td></tr>
<tr><td>Hazard headline</td><td>Ignoring BTM antenna test alarms because of suspected Big Metal Mass (BMM)</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026:
§3.15.7.1 of SUBSET-026 for v2.3.0, v3.4.0 and v3.6.0: Big metal object in the track, exceeding the limits for big metal masses as defined in SUBSET-036 v3.0.0 and v3.1.0, section 6.5.2 “Metal Masses in the Track” may trigger an alarm reporting a malfunction for the ERTMS/ETCS On-Board balise transmission function.
§3.15.7.2 of SUBSET-026 for v2.3.0, v3.4.0 and v3.6.0: In Levels 0/STM for SUBSET-026 v2.3.0 and 0/NTC for SUBSET-026 v3.4.0 and v3.6.0, the alarms which may be triggered by metal masses shall be ignored for a defined distance (see SUBSET-026 §A3.1 for v2.3.0, v3.4.0 and v3.6.0). If the alarm persists for a longer distance the ERTMS/ETCS On-Board equipment shall trigger a safety reaction.

Furthermore, there is a packet 67 defined in SUBSET-026 (for v2.3.0, v3.4.0 and v3.6.0) chapter §7, that defines areas for which the “integrity check alarms of balise transmission shall be ignored”.

The problem with these functions are, for level0/STM for SUBSET-026 v2.3.0 and 0/NTC for SUBSET-026 v3.4.0 and v3.6.0, when ignoring the balise transmission alarms defined in SUBSET-026 §3.15.7 for v2.3.0, v3.4.0 and v3.6.0, the balise transmission might have degraded safety integrity. Care must be taken by an application so that the applicable safety targets for Level 0/STM for baseline 2, 0/NTC for baselines 3, are still fulfilled.</td></tr>
<tr><td>Proposed mitigation</td><td>Each application must analyse which Eurobalises they have in Level 0/NTC areas and make sure that the safety integrity requirements defined for the corresponding system function in Level 0/STM for baseline 2, 0/NTC for baseline 3 (outside the scope of SUBSET-091) is fulfilled, also considering the possibly degraded safety integrity for the balise detect function when ignoring an antenna test alarm.

For example, the two balise groups announcing a Temporary Speed Restriction could be separated with more than the fixed value “Distance of metal immunity in Levels 0/STM” for baseline 2, “Distance of metal immunity in Levels 0/NTC” for baseline 3 (D_Metal, see SUBSET-026 §A3.1 for v2.3.0, v3.4.0 and v3.6.0) to protect against ignored balise transmission failures. The same goes for level transition announcements balise groups.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.15 ETCS-H0015

4.15.1.1 Intentionally left empty. No action by application projects is required.

4.16 ETCS-H0016

Hazard ID	ETCS-H0016
Hazard headline	Expired MA and Level Transition Order from RBC Becomes Valid (Entry inside Level 2 Area)
Hazard description	Situation: 1. A train with ERTMS/ETCS On-Board is inside a mixed (including Level 2) area running in any other level. Route is set to continue in Level 2 area. The ERTMS/ETCS On-Board has established a communication session to RBC. 2. All preconditions for the announcement of level transition and sending of MA are fulfilled; RBC announces a level transition and sends an MA. 3. The safe connection to ERTMS/ETCS On-Board is interrupted. 4. The protected route is revoked by the interlocking. The RBC is not able to revoke the level transition announcement or granted MA because of the interrupted radio connection. 5. New route, which differs from the previous one, is set in the interlocking. 6. Communication session a. is still maintained b. is terminated c. is terminated and a new communication session is established 7. The location of the announced level transition is reached and the ERTMS/ETCS On-Board switches to Level 2, whereby the expired (=wrong) MA becomes valid. Depending on the time stamp of the last received message from RBC, the following can happen: 1) [case 6a) from above]: If the train passes the level transition position with maintained communication session, the train switches to Level 2 and activates the radio link supervision function. After expiration of T_NVCONTACT, the defined safe reaction M_NVCONTACT is activated. 2) [case 6b) from above]: If the train passes the level transition position without communication session, the train switches to Level 2 and activates the radio link supervision function. After expiration of T_NVCONTACT, the safe reaction M_NVCONTACT is activated. 3) [case 6c) from above]: If: a. a new communication session is established (e.g. triggered by a balise group) before reaching the level transition position announced during the last communication session, but b. no new MA or Level Transition Order is given by the RBC (e.g. some condition for generating MA is not fulfilled), there is a risk for having a wrong MA (received during the first communication session) used by the ERTMS/ETCS On-Board. --> safety issue, potential collision or derailment, in degraded situation, where route revocation and communication interruption come together.

<table>
<tr><td>Proposed mitigation</td><td>Each trackside project must analyse the scenario and implement necessary measures. Such measures could include MA section timers and/or probabilistic evaluation of the scenario.
For baseline 3, the cleaning of the transition buffer specified in CR 842 closes the hazardous situation.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baseline 3, the cleaning of the transition buffer specified in CR 842 closes the hazardous situation.
</td></tr>
</table>

4.17 ETCS-H0017

4.17.1.1 Intentionally left empty. No action by application projects is required.

4.18 ETCS-H0018

Hazard ID	ETCS-H0018
Hazard headline	Lack of specification for the relocation function
Hazard description	In order to safely supervise the train position against trackside locations, it is necessary for the ERTMS/ETCS On-Board that both the train position confidence interval and the distances to such trackside locations refer to the same point. In the baseline 2 specifications, the train position confidence interval is only defined as referring to the LRBG (inducing a reset at each change of LRBG) and it is not specified at all how an ERTMS/ETCS On-Board shall deal with trackside information referred to a balise group that is no longer the current LRBG or that is referred to a balise group marked as unlinked. For the specific case of trackside information retrieved from the transition buffer a relocation mechanism using the linking distances is implicitly suggested by the clauses §4.8.1.6 and §4.8.2.1 d) of SUBSET-026, however the way to achieve it is not specified either. Therefore, any B2 ERTMS/ETCS On-Board behaviour is possible, ranging e.g. from no relocation at all compensated by the handling of as many as necessary train position confidence intervals as trackside information reference locations, to e.g. proprietary relocation functions taking into account somehow the odometry accumulated errors in between reference locations. In the baseline 3 (CR782), the ambiguity is solved by fully specifying the relocation function (see clause §3.6.4.3 of SUBSET-026 v3.4.0 and v.3.6.0) and by giving the trackside the responsibility to take (if necessary) the safe provisions when the linking information cannot be provided in due course (see clause §3.6.4.3.1 of SUBSET-026 v3.4.0 and v3.6.0). In case of trackside information referred to a balise group marked as unlinked (e.g. transmitting TSRs), the ERTMS/ETCS On-Board also manages temporarily only one additional train position confidence interval until a new LRBG is found and the relocation takes place. Since the CR782 is neither marked as “IN” nor as “OUT” in SUBSET-108 v1.2.0, there can be potential hazardous situations when a trackside has been engineered taking into account the proprietary solution from a specific ERTMS/ETCS On-Board supplier rather than the ERTMS/ETCS On-Board behaviour according to CR782, and when later on a train equipped with an ERTMS/ETCS On-Board equipment from another supplier has to operate the concerned line. There are some examples of such hazardous scenarios: 1. Relocation of location based information stored on-board due to encountering a BG marked as unlinked: trackside may not expect that the ERTMS/ETCS On-Board resets confidence interval in between the two subsequent BGs which are known to the trackside and linked. However, the ERTMS/ETCS On-Board can reset it based on encountering an unlinked balise group, as its reaction on detection of an unlinked BG is not specified in Baseline 2. 2. Relocation of location based information received from a BG marked as unlinked: In case the TSR is provided by balises marked as unlinked, the trackside may not expect that the ERTMS/ETCS On-Board will perform a relocation of this TSR when encountering a new BG (marked either as linked or as unlinked). If the ERTMS/ETCS On-Board performs this relocation as specified in CR782 solution, it will be based on the estimated distance between the BG marked as unlinked which has provided the TSR and the new encountered BG. If the Trackside has not foreseen appropriate margins, this can lead to a safety issue. 3. Relocation of location based information from the transition buffer without linking information: If the ERTMS/ETCS On-Board performs this relocation as specified in CR782 solution, it will be based on the estimated distance between the location

<table>
<tr><td></td><td>reference of the location based information and the current location reference (which is different from the location reference of the location based information). If the trackside has not foreseen appropriate margins, this can lead to a safety issue.

For other issues related to relocation, refer also to ETCS-H0061.</td></tr>
<tr><td>Proposed mitigation</td><td>Each Trackside specific application safety analysis shall consider that B2 ERTMS/ETCS On-Board may perform a proprietary relocation or a relocation as per CR 782 solution.

Each trackside specific application shall provide linking in due course. This includes the provision of linking distances to balises marked as linked in rear of the ETCS level transition in case trackside information referring to such balises is stored in the transition buffer. If the location related information is to be used in situations where linking is not provided (e.g. TSR transmitted by balise group marked as unlinked), the trackside shall include provisions when engineering the distance information.

If found not possible to mitigate the hazardous scenarios, each application must evaluate whether the residual risk can be accepted.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N *)</td><td>N *)</td><td>N *)</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N *)</td></tr>
<tr><td>B3R2, X=1</td><td>N *)</td><td>N *)</td><td>N *)</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N *)</td></tr>
</table>
*) For baselines 3, the harmonized solution described in §3.6.4.3, §3.6.4.7, 3.6.4.7.2 and §3.6.4.7.2 as specified in CR782 and SUBSET-026 v3.6.0 close the hazardous situation.
</td></tr>
</table>

4.19 ETCS-H0019

Hazard ID	ETCS-H0019
Hazard headline	Radio message acknowledged by ERTMS/ETCS On-Board but not used
Hazard description	According to the rules in SUBSET-026 the information in a radio message can be rejected by the ERTMS/ETCS On-Board. Even in cases where a radio message is rejected according to these rules, the ERTMS/ETCS On-Board will acknowledge the reception of the message to the RBC, if requested and it is consistent. This may lead to unsafe situations. Examples on such unsafe situations are: • Rejection of MA due to change of Train Data according to SUBSET-026 chapter §4.8.3, for v2.3.0, modified by SUBSET-108 v1.2.0 CR 729 and CR 792, v3.4.0 and v3.6.0. The scenario is that the driver has changed train data which doesn't invalidate the Movement Authority but still require an acknowledgement from the RBC (e.g. train length, train running number). The ERTMS/ETCS On-Board will then reject any new MA until it has received the acknowledgement from the RBC, according to exception [3]. If the RBC sends a shortened MA during this time – the time can be long for instance if the acknowledgement is lost – the ERTMS/ETCS On-Board will acknowledge the reception of the shortened MA (if the RBC has required) but reject the information. The old long MA will be used instead. The reason for the ERTMS/ETCS On-Board not receiving a Train Data acknowledgement (or receiving it late) can be: 1) The shortened MA is sent from RBC before receiving the new Train Data 2) Intentionally deleted 3) The Train Data acknowledgement from RBC is lost or delivered late ETCS-H0105 identifies another reason for the ERTMS/ETCS On-Board of not receiving a Train Data acknowledgement i.e. the loss or the late delivery of the Validated Train Data message to the RBC. • Rejection of assignment of co-ordinate system according to SUBSET-026 chapter §3.4.2 (for v2.3.0 modified by SUBSET-108 v1.2.0 CR 729, v3.4.0 and v3.6.0). The scenario is described in Appendix A. SUBSET-026 chapter §4.8, modified by SUBSET-108 v1.2.0 CR 729 and CR 792, contains several rules for rejection of data, where the cases described above are merely examples.
Proposed mitigation	The trackside shall analyse if the rules in SUBSET-026 (especially chapter §4.8, for v2.3.0, modified by SUBSET-108 v1.2.0 CR 729 and CR 792, v3.4.0 and v3.6.0) will really allow the ERTMS/ETCS On-Board to accept the information when sending more restrictive information and take any needed safety measures if the resulting risk is found unacceptable.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.20 ETCS-H0020

<table>
<tr><td>Hazard ID</td><td>ETCS-H0020</td></tr>
<tr><td>Hazard headline</td><td>Overlap/End Section timer in ERTMS/ETCS On-Board less restrictive than trackside</td></tr>
<tr><td>Hazard description</td><td>See SUBSET-026 v2.3.0 §3.8.4.4, §3.8.4.5 and §3.8.5.1.
Consider the scenario below:
1. RBC sends MA to ERTMS/ETCS On-Board, containing overlap and overlap/end section timer
2. Train with the ERTMS/ETCS On-Board passes On-Board overlap/end section timer start location; timer starts on-board
3. Train with the ERTMS/ETCS On-Board enters the interlocking overlap/end section timer start location (normally entry to end section); timer starts in interlocking
4. RBC repeats MA from step 1 (MA is equal to the first one, or if referred to another LRBG the absolute position of EoA, SvL and overlap/end section timer start location is equal to the first one)
5. ERTMS/ETCS On-Board restarts the overlap/end section timer
6. Since the overlap/end section timer in the interlocking was started (step 3) before the overlap/end section timer in the ERTMS/ETCS On-Board (step 5), it expires first. The signalman can therefore revoke the overlap/end section at a time when the ERTMS/ETCS On-Board still considers it as valid.
Regarding step 5: According to SUBSET-026 v2.3.0 §3.8.5.1 “A new MA shall always replace the one previously received” and as a consequence the ERTMS/ETCS On-Board shall manage accordingly the Section timers (see also SUBSET-026 v2.3.0 §3.8.4.2.1). However it is not specifically required to restart overlap/end section timer (see also SUBSET-026 v2.3.0, §3.8.4.4 and §7.5.1.150).</td></tr>
<tr><td>Proposed mitigation</td><td>The trackside application project shall mitigate or avoid creating this hazard. It has several ways of doing so, for example:
a) by confirming that the situation will not occur in this specific application, or
b) by not repeating MAs containing overlap/end section timers (this might however be impossible from operability / safety needs, and also impossible with semi-continuous infill devices in Level 1) , or
c) by following up the value of the interlocking overlap/end section timer in the RBC, taking into account the delay times for transmission of messages interlocking-RBC-On-Board and transmitting to the train the actual value. Note: Since a baseline 3 ERTMS/ETCS On-Board works differently (see below), it will then consider the timer elapsed when it is still valid, with the resulting operational drawback, if choosing this alternative.
For baselines 3, the new §3.8.4.1.4 (for end section timer) and §3.8.4.4.5 (for overlap timer) of SUBSET-026 v3.4.0 in CR 897 and SUBSET-026 v3.6.0 close the hazardous situation.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td>ERTMS/ETCS On-Board</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
</td></tr>
</table>

	*) For baselines 3, the new §3.8.4.1.4 (for end section timer) and §3.8.4.4.5 (for overlap timer) of SUBSET-026 v3.4.0 in CR 897 and SUBSET-026 v3.6.0 close the hazardous situation.

4.21 ETCS-H0021

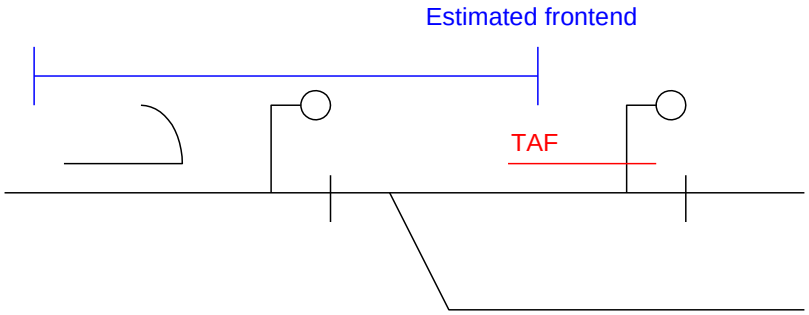
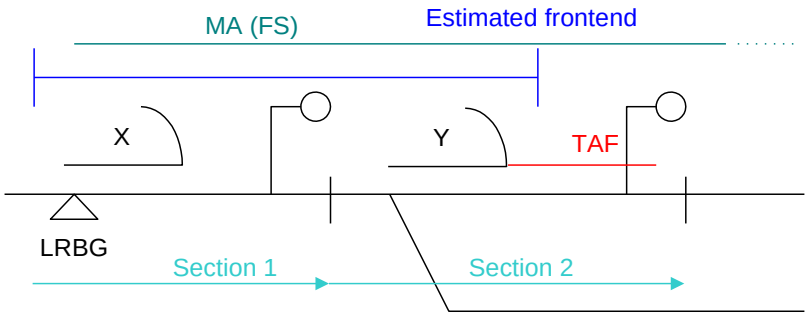
<table>
<tr><td>Hazard ID</td><td>ETCS-H0021</td></tr>
<tr><td>Hazard headline</td><td>Rolling backward past balise group</td></tr>
<tr><td>Hazard description</td><td>If, after having received a L1 MA in FS from a balise group the train moves backwards upstream the BG which gave the MA, the train might end up in rear of the Signal and the BG that gave the MA.
The signal might then be switched to stop (e.g. for operational reason). If the driver then tries to violate the stop signal with ETCS mode still Full Supervision, the BG will be ignored because it is not part of the link chain. Thus, the ERTMS/ETCS On-Board will not trip the train.
The scenario is not hazardous in Level 2.</td></tr>
<tr><td>Proposed mitigation</td><td>The hazardous scenario can be mitigated with the use of MA timer. However, this is not mandatory.
Therefore, if not using MA timers, the scenario must be analysed in a specific application, to find sufficient arguments for safety. This could include evaluation of the scenario probability or operational rules.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.22 ETCS-H0022

Hazard ID	ETCS-H0022
Hazard headline	Supervision Gap In NRBC Handover
Hazard description	There are two independent entities in the ETCS, here the ERTMS/ETCS On-Board and the ACC RBC, that take their own decisions on the moment of crossing the RBC border. The ERTMS/ETCS On-Board decides that it “switches” to the ACC RBC according to SUBSET-026, §3.15.1.3.5, for v2.3.0, v3.4.0 and v3.6.0; no more messages will be accepted from the HOV, i.e. ‘only a disconnection order shall be accepted from the Handing Over RBC’. In some situations (see below), there is a supervision gap, where neither the HOV nor the ACC RBC are able to revoke the MA stored by the ERTMS/ETCS On-Board. In case of a route degraded or revoked, there is no way of giving the related information to the ERTMS/ETCS On-Board. 1. The ERTMS/ETCS On-Board has sent a position report to the Accepting RBC with the train max safe front end having passed the announced border location but: a. the train has not yet passed the BBG with the antenna or b. The train has missed the BBG. Then the ACC does not know the train's location until either a. the BBG or b. the next BG following the BBG is reported by the ERTMS/ETCS On-Board because it has no information about the balise groups in the HOV area. In that case the BG reported as LRBG is not known by the ACC RBC. Therefore ACC RBC is not able to send any location related information to the ERTMS/ETCS On-Board, and HOV RBC is no more able to revoke any MA. 2. Intentionally deleted. 3. The train position report indicating the activation of the ACC’s responsibility is lost (at least the position report to ACC is lost in radio channel). In this case the ERTMS/ETCS On-Board has switched to listen only to the ACC RBC while the ACC RBC is not aware of the responsibility change Please note that there may be no ERTMS/ETCS On-Board reaction for safe radio connection supervision, because the disturbance of the radio communication may be only intermittent. 4. Intentionally deleted
Proposed mitigation	The following figures refer to the situations described in the hazard description: 1. There must be an overlap in the knowledge of balise engineering in the area where RBC transition can take place 2. Intentionally deleted 3. The ACC shall send MA revocations to the HOV (as RRI), and additionally to the ERTMS/ETCS On-Board. This requires the ACC to have an LRBG to relate the new MA to, which could be problematic if all position reports from ERTMS/ETCS On-Board to ACC are lost in radio channel. Alternatives could therefore be that the ACC doesn’t send any messages at all to the ERTMS/ETCS On-Board to invoke the M_NVCONTACT reaction, or issues an Emergency Messages. This could however be too restrictive. Each trackside application has to decide on the most appropriate solution. Note: Redundancy of train position reports when train has passed BBG and when announced RBC transition location is reached with max safe front end; minimizes the gap but does not close it.

<table>
<tr><td></td><td>4. Intentionally deleted.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE, regarding 1 and 3.</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

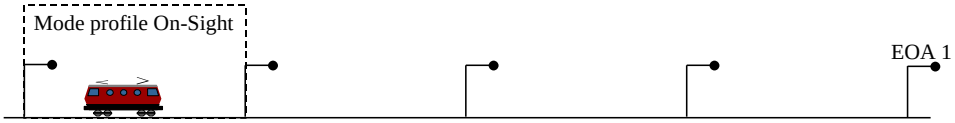
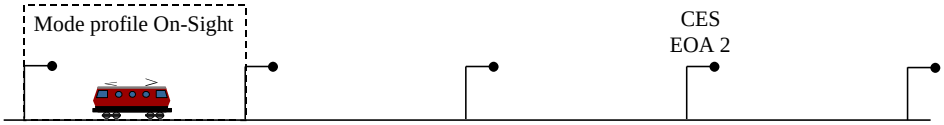
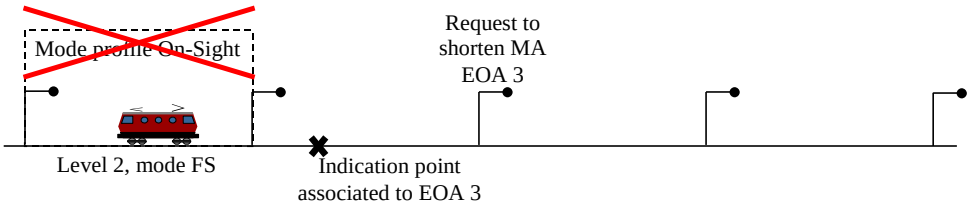
4.23 ETCS-H0023

Hazard ID	ETCS-H0023
Hazard headline	Use of estimated frontend for TAF window in RBC, leading to driver granting the wrong TAF
Hazard description	SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 specify that the estimated frontend shall be used in order to supervise the TAF window by the ERTMS/ETCS On-Board. But using the estimated frontend for the delivery of TAF requests at the Trackside level can lead to hazardous situation. Indeed, in the following situation:  The estimated frontend could be beyond the real train position in such a way that if RBC provides TAF request based on the estimated frontend, the TAF window that the ERTMS/ETCS On-Board will receive is not related to the current section (i.e. the one occupied by the train). This could lead to hazardous situation in the following case:  The driver of the train X grants the TAF, because he sees that the rest of section 1 is free of obstacles. The RBC will associate the received TAF granting to the TAF request it sent (i.e. the TAF request related to section 2) and therefore, will think that this section 2 is occupied by the train X only and that no other train is present on this section, while the train Y is physically occupying this section too. The RBC could therefore send to the train X a FS Movement Authority starting from the LRBG and including the section 2 occupied by the train Y. Note that in case of mixed level area (Level 0/Level 1 + Level 2), the train Y could be in Level 0/Level 1 and therefore, is unknown by the RBC.
Proposed mitigation	A trackside application safety analysis can with regards to a specific track layout consider this hazard as sufficiently improbable. If not, the RBC should check that the min safe front end is within the TAF section, before sending the TAF request, or to export a requirement on operational rule saying that TAF can only be granted if the driver confirms the id of the marker board. Note: If the RBC uses the min safe front end for TAF request, this is not directly a contradiction to SUBSET-026, but will go outside the general statement in section §3.6.4.6 (v2.3.0, v3.4.0 and v3.6.0) that if nothing is specified, estimated position shall be used.
Mitigation allocated to	TRACKSIDE / EXTERNAL

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.24 ETCS-H0024

Hazard ID	ETCS-H0024
Hazard headline	No Mode Profile applied after rejected MA shortening
Hazard description	Following SUBSET-026 v2.3.0 §4.8.3, modified by SUBSET-108 v1.2.0 CR 792, in level 2/3 mode FS/OS, if a Co-operative Shortening of MA is received together with a mode profile, and if a Conditional Emergency Stop is currently in application by the ERTMS/ETCS On-Board (not yet revoked), the "Co-operative shortening of MA" passes the filter on level whereas the mode profile is rejected due to exception [5] where: Exception [5] is: "the movement authority and, if received together with this movement authority, the mode profile shall be rejected if emergency stop(s) have been accepted and are not yet revoked or deleted by the ERTMS/ETCS On-Board (see mode transitions)." The following hazardous scenario may apply: 1) The train is in level 2, mode OS: an MA (to EOA 1) and a mode profile On-Sight are currently supervised by the ERTMS/ETCS On-Board:  2) The RBC sends a Conditional Emergency Stop (to EOA 2) which is accepted and applied by the ERTMS/ETCS On-Board:  3) The RBC sends a Co-operative Shortening of MA (to EOA 3), which also contains the mode profile On-Sight (the same as the one currently supervised by the ERTMS/ETCS On-Board): • According to SUBSET-026 v2.3.0 §4.8.3, modified by SUBSET-108 v1.2.0 CR 729 and CR 792, the Co-operative Shortening of MA is accepted. • According to SUBSET-026 v2.3.0 §4.8.3, modified by SUBSET-108 v1.2.0 CR 729 and CR 792, the mode profile is rejected because a CES is in application (not yet revoked). • According to the indication point location of the shorter MA (refer to SUBSET-026 v2.3.0 §3.8.6.1b), the Co-operative Shortening of MA is granted by the ERTMS/ETCS On-Board and the shorter MA is stored On-Board;  Nevertheless, according to SUBSET-026 v2.3.0 §3.12.4.3, as the associated mode profile has been filtered, the one currently supervised by the ERTMS/ETCS On-Board should be deleted. As a consequence, the train could switch to Full Supervision mode in an On-Sight area.
Proposed mitigation	Until CR 854 is implemented, the solution should be done by the RBC by e.g. not sending Co-operative shortening of MA while there is a CES in application in ERTMS/ETCS On-Board

<table>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §4.8.3 (row “Movement Authority+ (optional) Mode Profile+ (optional) List of Balises for SH area”) of SUBSET-026 by CR 854 and SUBSET-026 v3.6.0 close the hazardous situation.
</td></tr>
</table>

4.25 ETCS-H0025

<table>
<tr><td>Hazard ID</td><td>ETCS-H0025</td></tr>
<tr><td>Hazard headline</td><td>MA shortening extends MA already in ERTMS/ETCS On-Board</td></tr>
<tr><td>Hazard description</td><td>There is no specific requirement in SUBSET-026 v2.3.0 as well as in v3.4.0 and v3.6.0 about the reception of an MA shortening longer than the current EoA (refer to SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.8.6.1b) in the following cases: co-operative shortening of MA or new MA provided without gradient and speed profiles. The ERTMS/ETCS On-Board could therefore accept this new EoA (e.g. corresponds to an MA extension instead of an MA shortening), with more permissive speed and gradient profiles corresponding to the open profiles of the last received MA. This could result in potentially dangerous situation in the following scenario:
1) ERTMS/ETCS On-Board has received an MA with open speed and gradient profile, i.e. the profile is longer than the current EoA.
2) The RBC sends to the ERTMS/ETCS On-Board an extension of the current MA, with more restrictive speed and gradient profile than sent in step 1), but:
a) The ERTMS/ETCS On-Board does not receive it (e.g. radio communication failure) AND, the RBC either does not request the acknowledgement of the MA or may request it but does not take it into account;
OR
b) The ERTMS/ETCS On-Board rejects it (e.g. CES already in application or unacknowledged Train Data).
3) The RBC sends afterwards an MA shortening with an EoA between the ones given in steps 1) and 2).
4) This MA shortening is received by the ERTMS/ETCS On-Board. Since the speed and gradient profiles are generally not sent with a request to shorten MA, the ERTMS/ETCS On-Board will consider the ones given in step 1) as valid together with the MA given in step 3).
The result will be that the ERTMS/ETCS On-Board uses too permissive speed and gradient profiles and could therefore allow the driver to exceed speed limits.
Note: This is not a problem if the speed and gradient profile received in 1) ends at the current EoA, since the longer MA received in 3) does not contain the speed and gradient profile. As a result, the ERTMS/ETCS On-Board will have an MA without profile, and will thereby, according to SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.7.2.3, not accept the new MA.
In baseline 3, CR 854 introduces exception [5] on Co-operative shortening of MA in SUBSET-026 v3.4.0 and v3.6.0 section §4.8.3. This closes case 2b) if the MA is rejected due to the CES already in application. The other situations are however still open.</td></tr>
<tr><td>Proposed mitigation</td><td>The RBC should not use open profiles in combination with co-operative shortening of MA (defined in SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.8.6) or new MA provided without gradient and speed profiles.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

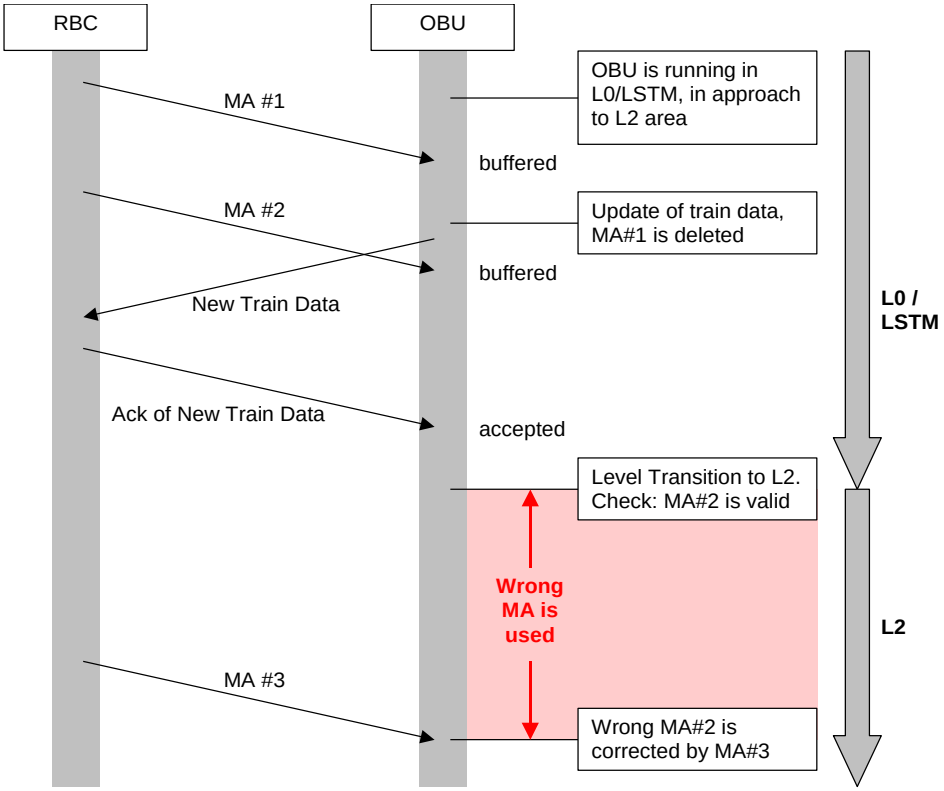
4.26 ETCS-H0026

<table>
<tr><td>Hazard ID</td><td>ETCS-H0026</td></tr>
<tr><td>Hazard headline</td><td>Override in SB possible in levels 0 and NTC</td></tr>
<tr><td>Hazard description</td><td>Following CR 659 (DC of SUBSET-108 v1.2.0), override in SB only possible in level 2/3.
If not implemented in ERTMS/ETCS On-Board, override may be possible in other levels. In particular, SR mode could be entered spuriously in level 0 or NTC. In level NTC, mode SR, the STM may stop supervising the train movements.</td></tr>
<tr><td>Proposed mitigation</td><td>If not implementing CR 659, the override when being in SB mode in Levels 0 and NTC should be forbidden in e.g. driver manual or export the constraint to operational procedures.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td></td><td></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N*)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N*)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §5.8.2.1 of SUBSET-026 by CR 659 and SUBSET-026 v3.6.0 close the hazardous situation.
</td></tr>
</table>

4.27 ETCS-H0027

4.27.1.1 Intentionally left empty. No action by application projects is required.

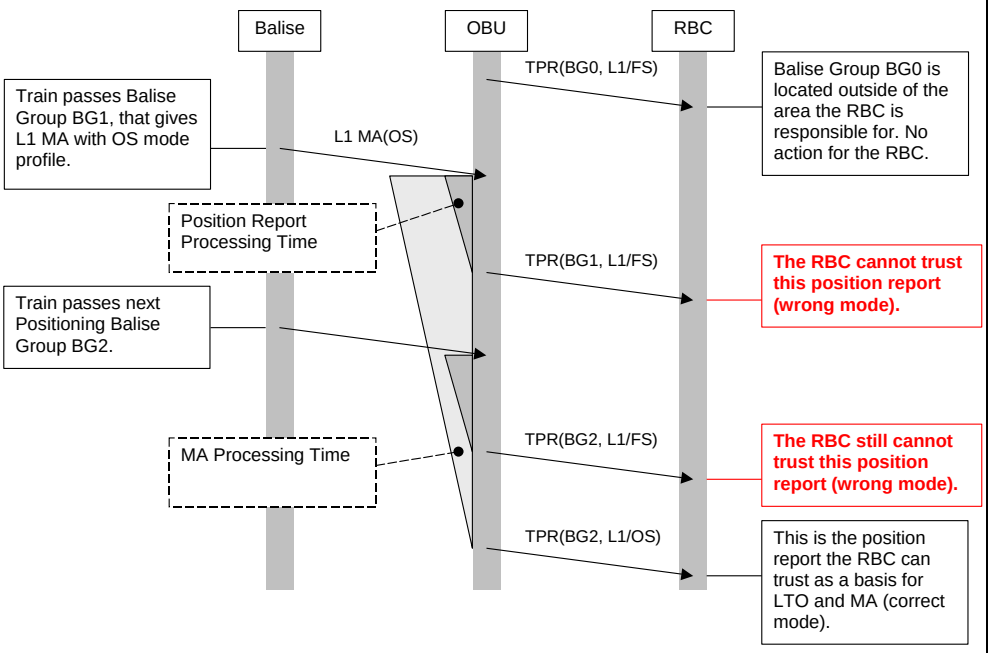
4.28 ETCS-H0028

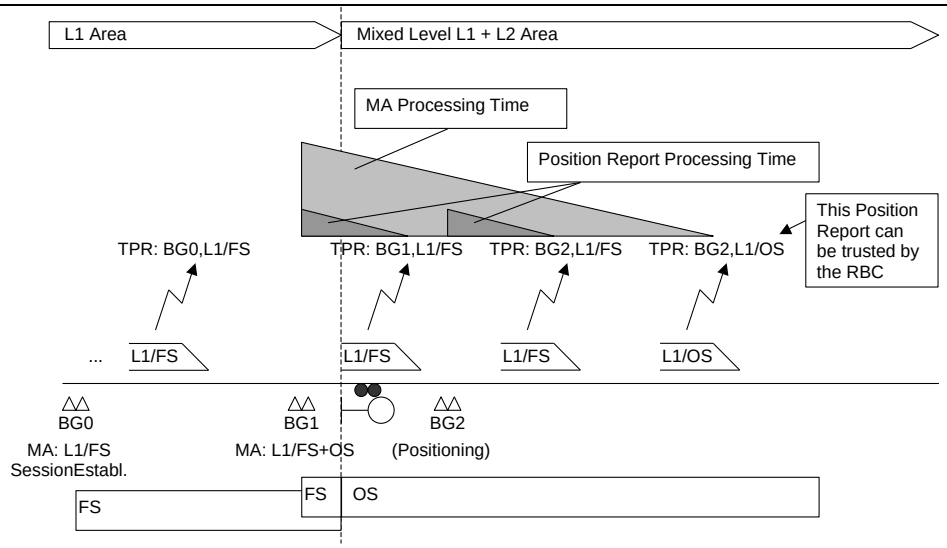
Hazard ID	ETCS-H0028
Hazard headline	Acknowledgement of Train Data validates invalid MA
Hazard description	The Acknowledgement of Train Data, as sent by the RBC, may validate an MA received by the ERTMS/ETCS On-Board that was sent previously by the RBC, under conditions of different train data.  The remaining risk • Train running with the wrong MA (#2) • Corrective MA (#3) may be delayed in delivery to ERTMS/ETCS On-Board, or, due to internal checks, RBC could decide not to send any MA to the train because of the new train data is difficult to quantify in a generic ETCS environment, mainly because the probabilities involved will be very uncertain when quantified in a generic UNISIG level.
Proposed mitigation	As noted in CR 790, the remaining risk can be seen as acceptable providing that the time during which the wrong MA is used, is made sufficiently short (as a proposal for sufficiently short, the accepted value of T_NVCONTACT could be used). The RBC should make sure it is, e.g. to immediately send an updated MA based on the new train data.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.29 ETCS-H0029

Hazard ID	ETCS-H0029
Hazard headline	RBC cannot trust Train Position Report as ERTMS/ETCS On-Board event handling is not predictable
Hazard description	SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.6.5.1.4 defines a number of events when train position reports have to be sent by the ERTMS/ETCS On-Board to the RBC. Furthermore, the RBC can request additional position reports for a combination of the possibilities given in SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.6.5.1.5. In summary, there are a number of situations where position reports have to be sent, with a high probability of overlapping each other. The definition given in SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.6.5.1.8, that the reported mode and level shall be consistent, is not sufficient for the RBC to trust in a train position report when it is received. If the RBC doesn't have route information from the interlocking, it might use signal information instead, which is reflected in the information transmitted in a BG message e.g. at a level 1 to level 2 transition border. In order not to send a stop to the train after it has passed the signal, the RBC needs to know what the route status was prior to passing the signal. In level 2, the RBC itself knows what was sent to the train; therefore there is no problem. However, at a level transition, the RBC must get this information from the adjacent area; the RBC could take it from the ERTMS/ETCS On-Board position report.  The track layout for this scenario looks as below.



Other possible reasons for additional position reports during MA processing may be

a) Driver interactions

b) Internal triggers, based on the position report parameters

With the current definitions of the requirements mentioned above, the RBC cannot trust the Level/Mode reported with the Train Position Report.

This may result in an unsafe situation if the RBC because of availability reasons decides to trust the level-mode combinations in e.g. train position report TPR(BG1, L2/FS) or TPR(BG2, L2/FS) in the figure above. The RBC then sends an FS MA when it should be an OS MA.

There exists a performance requirement of less than 1.5 seconds for update of ERTMS/ETCS On-Board status in SUBSET-041 (see v2.1.0, v3.1.0 and v3.2.0) §5.2.1.3. This can be used for limiting the time at risk.

Proposed mitigation

An application project should take necessary precautions in order to make sure that the RBC does not trust a reported mode without taking into account the maximum ETCS On-board processing time (1.5s) specified in SUBSET-041 (§5.2.1.3 or §5.2.1.4).

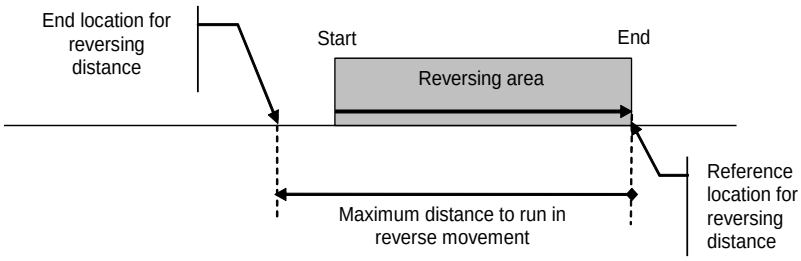
Mitigation allocated to

TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

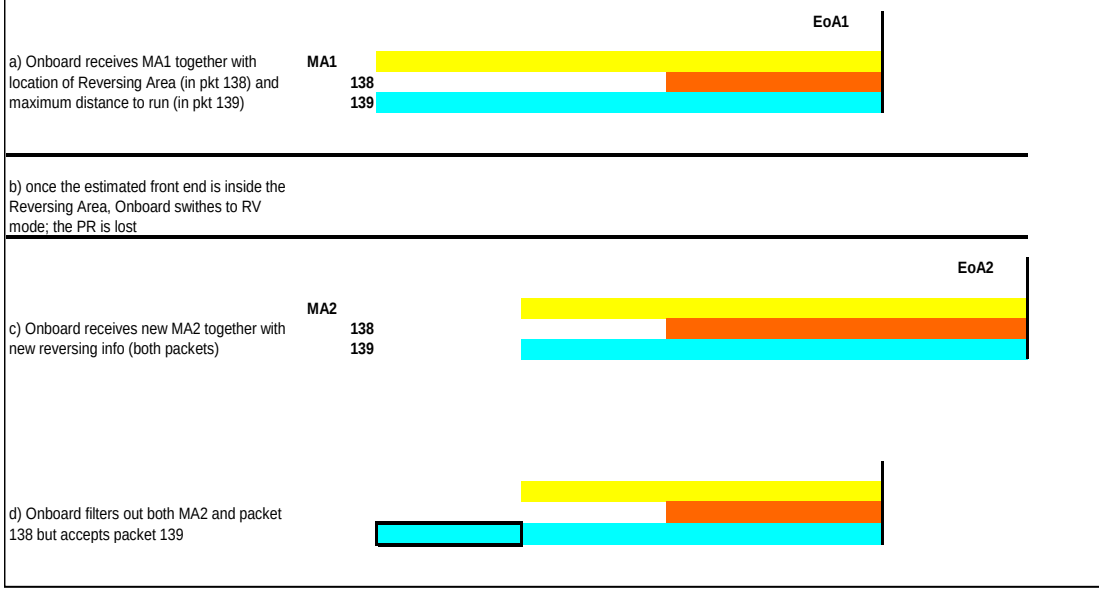
4.30 ETCS-H0030

Hazard ID	ETCS-H0030
Hazard headline	Unwanted change of the permitted distance to run in Reversing mode.
Hazard description	In Reversing mode the trains are allowed to run for a maximum distance, given by trackside: the ERTMS/ETCS On-Board calculates the permitted end location using as a fixed reference location the end of the Reversing Area (also given by trackside):  The RBC can update both the Reversing Area and the maximum distance to run; if the ERTMS/ETCS On-Board is in reversing mode however it rejects any new Reversing Area received. Therefore, should the RBC update both Reversing Area and maximum distance to run, the ERTMS/ETCS On-Board in RV would filter out the new Reversing Area info, which however defines also the starting point of the new maximum distance to run. The ERTMS/ETCS On-Board would then calculate the new end location for the reversing movement starting from a reference location different from the one used by the RBC. The end location in the RBC view would be different from the one in ERTMS/ETCS On-Board view. This can be hazardous as in the following example scenario, where the train is supposed to be with its estimated front end inside the Reversing Area: <SEE FIGURE BELOW TABLE FOR THE CASE OF EXTENSION> a) RBC sends an MA together with Reversing Area information and maximum distance to run (the latter part of the Reversing supervision info) b) The ERTMS/ETCS On-Board switches to RV e.g. for initiating an escape movement, based on the Reversing info received in step a) c) RBC is unaware of the change of mode (e.g. PR lost), it changes (extends/shortens) the MA and sends updated Reversing Area and distance to run. In the RBC view, the end location of the reversing distance is unchanged (the distance to run is longer/shorter but the reference location is also shifted). d) The ERTMS/ETCS On-Board being in RV mode rejects both the new MA and the new Reversing Area information. It accepts the new reversing distance, which however results in a wrong (unduly extended/shortened) maximum distance to run, the end location being calculated backwards from the end of the previous Reversing Area. The end location for the RV movement supervised by the ERTMS/ETCS On-Board is different from the one intended by the RBC: the maximum distance to run becomes unduly extended/shortened.

Proposed mitigation	The mitigations have to be found at project level (specific application), considering the ERTMS/ETCS On-Board behaviour in Reversing (filtering of the Reversing Area). In the example of the described scenario, one possible mitigation would be for the RBC to send in step a) the Reversing information described in step c) (in fact, the Reversing Area does not have to be truncated at the EoA).
Mitigation allocated to	TRACKSIDE
Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	N*)	N
	B3MR1, X=1	Y	N*)	N
	B3MR1, X=2	n/a	N*)	N
	B3R2, X=1	Y	N*)	N
	B3R2, X=2	n/a	N*)	N

*) For baselines 3, the changes introduced to §4.8.4 (row "*Reversing Area Information*") of SUBSET-026 by CR 895 and SUBSET-026 v3.6.0 close the hazardous situation.

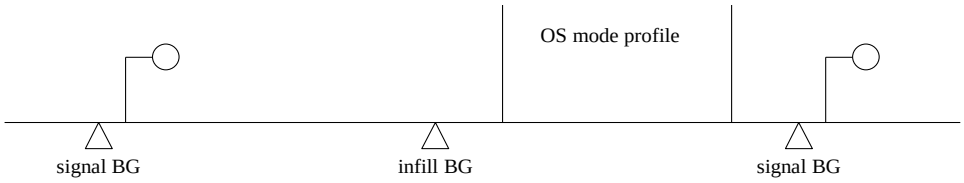


4.31 ETCS-H0031

Hazard ID	ETCS-H0031
Hazard headline	Too many track conditions removed in ERTMS/ETCS On-Board
Hazard description	Background: Track description consists of the following information. 1. Static Speed Profile 2. The gradient profile 3. Optionally Axle load Speed Profile 4. Optionally track conditions: Powerless section (pkt68), Air tightness (pkt68), Stopping not permitted tunnel/bridge/undefined (pkt68), Change of traction power (pkt39), Big metal masses (pkt67), Radio hole (pkt68), Switch off regenerative brake (pkt68), Switch off eddy current brake for service brake (pkt68) and Switch off magnetic shoe brake (pkt68) 5. Optionally route suitability data 6. Optionally areas where reversing is permitted 7. Optionally changed adhesion factor According to SUBSET-026 v2.3.0 §3.7.3.1 “New track description and linking information shall replace (in the ETCS On-Board equipment) previously received track description and linking information…” This is generally no problem, but for the specific track description “track condition” there is a matter of interpretation. For example, trackside could re-send a specific track condition (e.g. Change of traction power), assuming that the ERTMS/ETCS On-Board will keep the other track conditions intact, since §3.7.3.1 only speaks of using the new track description for updating information in ERTMS/ETCS On-Board. However, an ERTMS/ETCS On-Board could in this case remove all other track conditions except the one explicitly given. This might be hazardous if e.g. Stopping not permitted or Powerless section is removed from the ERTMS/ETCS On-Board, without the ETCS trackside intending to do so.
Proposed mitigation	The consequences are not related to the ETCS Core Hazard. Whether the risk of such a hazard is large enough could be analysed for each specific application. If the risk of the above described hazard is not acceptable, the following measure can be imposed: • If trackside wants to update one track condition, it must at the same time resend all the track conditions that it wants the ERTMS/ETCS On-Board to apply (including the ones already entered by the train). Note: Big metal mass cannot be repeated by an RBC (because RBC cannot send BMMs). However, if the ERTMS/ETCS On-Board in error removes a Big metal mass, this has no hazardous consequences. Note: The above rule shall not be interpreted as a recommendation for the ERTMS/ETCS On-Board to remove all types of track conditions just because a certain type of track condition is updated, since this might lead to availability problems if erroneously resetting Big metal mass information. Note: retaining track conditions too long was not thought to be safety critical. There are indeed some RAM-related and track-damage-related scenarios, but none of them critical for meeting the safety target... For baseline 3, CR 899 closes the hazardous situation.
Mitigation allocated to	TRACKSIDE

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §3.7.3 (“Extension, replacement of track description and linking information”) of SUBSET-026 by CR 899 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.32 ETCS-H0032

Hazard ID	ETCS-H0032
Hazard headline	OS mode profile deleted ERTMS/ETCS On-Board after receiving an in-fill MA
Hazard description	Background: According to SUBSET-026 v2.3.0 §3.12.4.3 “On the reception of a new MA without Mode Profile the ERTMS/ETCS On-Board equipment shall delete the current Mode Profile.” Consequently, if a mode profile start location is located in advance of an infill BG, when the train reads this BG in FS mode, the mode profile previously memorised On-Board may be deleted (the infill MA cannot repeat this mode profile) in case the ERTMS/ETCS On-Board is implemented to apply §3.12.4.3 also in rear of the reference location of the in-fill information.  For example, level crossing area could be supervised with on-sight mode profile according to the track layout given in the here above figure. Note that CR 484 (in baseline 3) modifies SUBSET-026 as follow: §3.12.4.3 “On reception of a new MA (with or without Mode Profile) the ERTMS/ETCS On-Board equipment shall delete the currently supervised Mode Profile.” §3.12.4.3.1 “Exception: When receiving a new MA by in-fill, any currently supervised mode profile shall be deleted only beyond the reference location of the in-fill information.” The hazard is thus applicable where ERTMS/ETCS On-Board is implemented according to baseline 2. Note that this hazard is only an issue for Level 1. Note: the problem is also applicable to Euroloop and RIU
Proposed mitigation	The Trackside should not implement an OS mode profile - with a start location between an infill BG and the related main BG (infill location reference) - with a start location between the first location where of infill information can be received by the ERTMS/ETCS On-Board and the related main BG (infill location reference)
Mitigation allocated to	TRACKSIDE

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N*)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N*)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §3.12.4.3.1 (see “§3.12.4 Mode profile”) of SUBSET-026 by CR 484 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.33 ETCS-H0033

<table>
<tr><td>Hazard ID</td><td>ETCS-H0033</td></tr>
<tr><td>Hazard headline</td><td>Packet 18 (Trip) continuously transmitted by STM X before level transition to STM Y area</td></tr>
<tr><td>Hazard description</td><td>In case of transition from level NTC X to level NTC Y, the STM X shall leave DA (Data Available) state and enter CS (Cold Standby) state, see SUBSET-035 section §7.3.2 for v2.1.1 and section §9.2 for v3.1.0 and v3.2.0. However, this procedure is blocked if (and as long as) STM X sends packet 18 (TRIP) to a B2 ERTMS/ETCS On-Board (refer to “conditional CS state transition order” in section §7.3.3 of SUBSET-035 for v2.1.1). The packet 18 informs the ERTMS/ETCS On-Board that a trip procedure is triggered by the national equipment (STM X).

STM X could have a SIL level lower than the one of STM Y. So, emergency brakes command triggered by the STMs could not be with the same safety integrity level.

Basically, after transition STM/STM, a SIL0 STM X could send infinitely a packet 18 to the ERTMS/ETCS On-Board without applying emergency brakes (and there is no time limit for this delay) and thus, could unduly delay the activation of a SIL4 STM Y (still in HS (Hot Standby) state and waiting for the transition order to DA from the ERTMS/ETCS On-Board).

Since ERTMS/ETCS On-Board does not supervise the brakes application in SN mode and STM Y is not in a supervising state (i.e. DA state), hazardous situation would then be the STM Y area not supervised at all.

Note that this hazard is only applicable to a B2 ERTMS/ETCS On-Board since, according to SUBSET-035 sections §10.3.3.3 and §10.3.3.3.1 for v3.1.0 and v3.2.0, the ERTMS/ETCS On-Board applies emergency brake starting from the moment a "conditional CS state transition order" has been sent to a STM to the moment report CS to STM.

Note that this hazard is only an issue for Level NTC.</td></tr>
<tr><td>Proposed mitigation</td><td>When transiting from one national train control system (=X) to another national train control system (=Y), the driver must verify that system Y is active. If system Y is not active[2], the driver must apply national rules for driving without system Y.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to SUBSET-035 by CR 1071 and SUBSET-035 v3.2.0 close the hazardous situation
</td></tr>
</table>

[2] The safe procedure for verifying that STM Y is active must be decided as part of national rules.

4.34 ETCS-H0034

4.34.1.1 Intentionally left empty. No action by application projects is required.

4.35 ETCS-H0035

Hazard ID	ETCS-H0035
Hazard headline	Train enters L1/2/3 area in L0/SH or LNTC/SH without technical restrictions
Hazard description	Even if the rule §4.1.4.1 in SUBSET-040 v2.3.0 (resp. §6.1.1.1.1 both in v3.3.0 and in v3.4.0) does not allow for borders where shunting movements could occur, a train is able to enter an ETCS L1/L2/L3 area in L0/SH mode without any technical restrictions. Moreover, if a B2 ERTMS/ETCS On-Board should implement CR 410 (NA in SUBSET-108 v1.2.0), which allows SH mode also for Level STM, a B2 train is able to enter L1/L2/L3 areas in LSTM/SH mode without technical restriction. In fact, according to SUBSET-026 v2.3.0, §4.8.4, a B2 ERTMS/ETCS On-Board in SH mode shall not manage Level Transition Orders to L1/L2/L3 (i.e. reject them) and according to §4.8.3, in L0 or LSTM the B2 ERTMS/ETCS On-Board shall reject the Danger for Shunting information sent by a balise group. Consequently, a B2 train may enter an ETCS L1/L2/L3 B3 X=1 area in L0/SH or LNTC/SH (if implementing CR 410) and move within this area without protection from ETCS. A B3 ERTMS/ETCS On-Board equipment will accept the Danger for Shunting information sent by a balise group in L0/LNTC if received together with an immediate Level Transition Order to L1/L2/L3. The B3 ERTMS/ETCS On-Board equipment stores immediate Level Transition Orders to execute them when the train leaves the SH mode. But, a B2 trackside may not be aware that it must also send Danger for Shunting information (additional to immediate Level Transition Order) to prevent a B3 train running in L0/LNTC and SH mode from entering L1/L2/L3 areas. With this uncontrolled movement, there is the possibility of - derailment of this train (if the routes are not set for this train) or - collision with another ETCS L1/L2/L3 controlled train.
Proposed mitigation	In a B2 trackside where a border is protected by a balise group with immediate Level Transition Order, to also protect against shunting B3 trains the Danger for Shunting information must be added. In a B3, X=1 trackside a border will be protected by a balise group with Danger for Shunting information also containing an immediate Level Transition Order. This means that trains passing the border in LNTC/SN without an MA will be tripped by the level transition and trains passing the border in L0/SH or LNTC/SH will be tripped by Danger for Shunting information. This mitigation will not work for B2 ERTMS/ETCS On-Boards in LNTC/SH (i.e. implementing CR 410) which are not implementing CR 923. This mitigation will also not work for B2 ERTMS/ETCS On-Boards in L0/SH, see CR 923. B2 and B3 X=1 tracksides shall analyse the remaining risk related to a B2 train not implementing CR 923 moving in SH mode in L0/LNTC entering a L1/L2/L3 area.
Mitigation allocated to	TRACKSIDE

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>

*) For baselines 3, the changes introduced to §4.8.3 (with the introduction of exception [13] for “Danger for Shunting information”) of SUBSET-026 by CR 923 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.36 ETCS-H0036

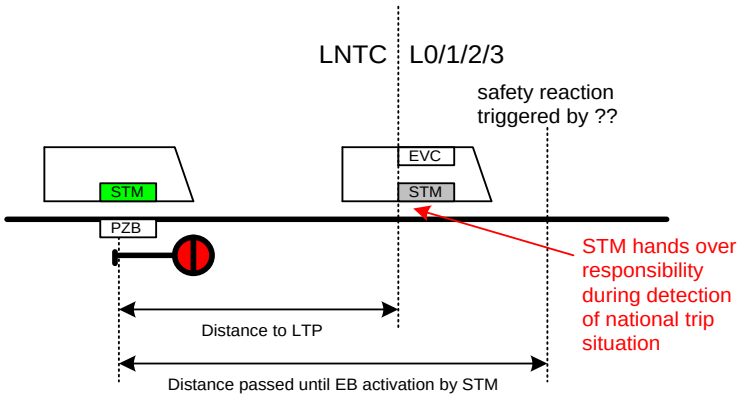
4.36.1.1 Intentionally left empty. No action by application projects is required.

4.37 ETCS-H0037

Hazard ID	ETCS-H0037
Hazard headline	Train Data changed during RBC-RBC Handover
Hazard description	In the SUBSET-039 v.2.3.0 there is only one possibility to send train data; namely in the pre-Announcement message. That means that in case train data has changed (e.g. due to input from external sources) during an ongoing handover transaction, it is not clear how to inform the Accepting RBC about this new train data without cancelling the handover process. The change of some train data by external sources does not necessarily lead to the train coming to standstill (e.g. see right branch of the flowchart in SUBSET-026 v2.3.0 §5.17.3, modified by SUBSET-108 v1.2.0 CR 500, D1=others). Some of these train data could have an impact on the content of an RRI. To understand different possible solutions, the following information is provided: - The driver is not allowed to change Train Data while the train is running; other than the train running number (SUBSET-026 v2.3.0 §3.18.3.5); which is not safety related. - Regarding the Train Data changed by other sources than driver, according to SUBSET-026 v2.3.0 §5.17.3, modified by SUBSET-108 v1.2.0 CR 500, it is only train data “train category, axle load, loading gauge or power supply” that prompts the train to a stand-still. Note that this hazard is only applicable to a B2-B2, B2-B3 and B3-B2 RBC HO since, according to SUBSET-039 v3.1.0 sections §5.12.4, §5.1.2.4.1, §5.1.2.4.2 and §5.1.2.5, a B3 ACC RBC shall consider the HO procedure as cancelled on reception of a pre-announcement with the same (leading) engine or border BG
Proposed mitigation	There are a few alternatives: A) The HOV RBC shall cancel the handover procedure with the ACC RBC and the ERTMS/ETCS On-Board as soon as it detects that the ERTMS/ETCS On-Board sends new Train Data, unless only the Train Running Number changes. This leaves an availability problem; changes by external source in Train Data regarding Train length, Maximum permitted train speed, Train fitted with airtight system and List of STM available On-Board may cause unwanted brake (could be Emergency Brake). B) The HOV RBC shall cancel the handover procedure with the ACC RBC and the ERTMS/ETCS On-Board as soon as it detects that the ERTMS/ETCS On-Board sends new Train Data regarding Train category(ies), Loading gauge, Axle load or Power supply accepted by the train. This will leave a residual hazard; Train Data regarding Train length, Maximum permitted train speed, Train fitted with airtight system or List of STM available to the ERTMS/ETCS On-Board can be changed without notification to the ACC RBC (in baseline 3 also Axle Number). C) The HOV RBC shall never cancel the handover procedure with the ACC RBC and the ERTMS/ETCS On-Board due to changed Train Data. This leaves the hazard that any Train Data in SUBSET-026 §3.18.3.4, modified by SUBSET-108 v1.2.0 CR 500, can be changed without notification to the ACC RBC. D) Send all necessary information to ACC RBC and let it decide whether the new data affects the RRI and take necessary measures. For the short term, you need knowledge of the properties of the actual handover area to decide which of A, B and C is the most appropriate. Where the handover procedure is

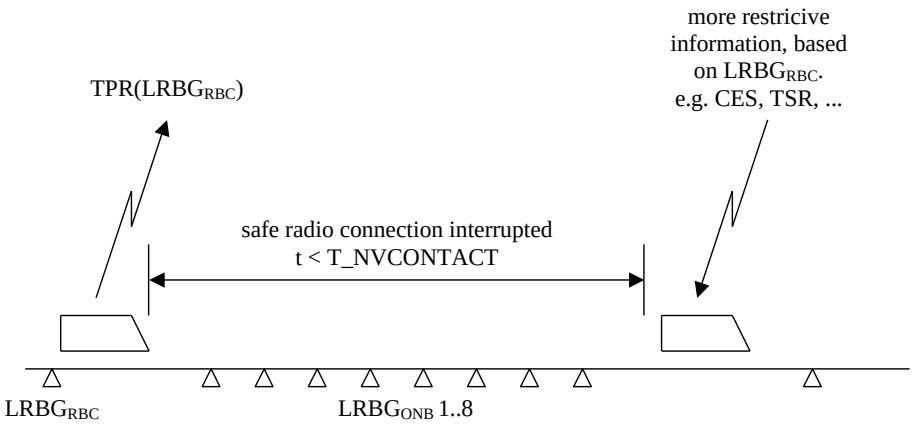
<table>
<tr><td></td><td>cancelled the MA must be shortened by the HOV RBC to a location at or before the border (i.e. inside the HOV area).The decision should be left to the application projects.
In baseline 3, a new message 207 “Train Data” is introduced starting from SUBSET-039 v3.1.0. This is solution D) above and closes the hazardous situation for baseline 3.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2">TRACKSIDE</td><td colspan="5">ACC RBC</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1, X=1</td><td>B3MR1, X=2</td><td>B3R2, X =1</td><td>B3R2, X=2</td></tr>
<tr><td rowspan="5">HOV RBC</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>Y</td><td>N</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>Y</td><td>N</td><td>N</td><td>N</td><td>N</td></tr>
</table>
</td></tr>
</table>

4.38 ETCS-H0038

Hazard ID	ETCS-H0038
Hazard headline	Level transition from LNTC to L0/L1/L2/L3 before National System evaluates emergency brake condition
Hazard description	**Hazard description:** This possible hazard is valid for those level transitions to L0, L1, L2 and L3 that take place in a certain distance beyond a signal that was passed under responsibility and supervision of a National System. *Note: the hazard is applicable if the ERTMS/ETCS On-Board equipment is interfaced to a national system, regardless whether through an STM or by other means; for the sake of simplicity however in the following drawings only the case of STM interface is depicted.* The responsibility of and supervision by the National System ends at the level transition location (LTP). In case the train in level NTC passes a signal showing a stop aspect, which is protected by a national train control system (e.g. PZB (2000Hz magnet) for DB AG), this system is responsible for supervision (see figure, green coloured STM).  In case the distance between Trip relevant locations (e.g. the border signal) and the actual level transition location is too short, the responsibility is handed over to ERTMS/ETCS On-Board during the detection/evaluation of national trip situation. No safety reaction will be applied. In this example, the PZB system evaluates the national trip situation, but does not trigger a safety reaction, due to responsibility handover to ERTMS/ETCS On-Board. No safety reaction (emergency brake) is or will be applied The hazard assumes that a solution for H0062 is implemented in the ERTMS/ETCS On-Board, i.e. the activation of the emergency brake by the national train protection system is reported to the ERTMS/ETCS On-Board and is kept as trip condition
Proposed mitigation	In order to create a safe implementation, trackside engineering therefore has to guarantee a distance between Trip relevant locations (e.g. the border signal) and the actual level transition location. The distance needs not only to be derived from the maximum line speed but must also consider the performance properties of the national system and assumptions of the odometer inaccuracy
Mitigation allocated to	TRACKSIDE
Relevant in ETCS baseline	

			ERTMS/ETCS On-Board		
			B2	B3MR1	B3R2
	Trackside	B2	Y	Y	Y
		B3MR1, X=1	Y	Y	Y
		B3MR1, X=2	n/a	Y	Y
		B3R1, X=2	Y	Y	Y
		B3R2, X=2	n/a	Y	Y

4.39 ETCS-H0039

Hazard ID	ETCS-H0039
Hazard headline	More restrictive RBC data is rejected after re-establishment of safe radio connection
Hazard description	SUBSET-026 (see v2.3.0, v3.4.0 and v3.6.0) §3.6.2.2.2.c requires: c) The ERTMS/ETCS On-Board equipment shall be able to accept information referring to one of at least eight $LRBG_{ONB}$ last reported to the RBC. In case the safe connection is disturbed for some time or an announced radio hole is passed, the number of passed balise groups not reported to the RBC may exceed the maximum number that shall be stored by the ERTMS/ETCS On-Board. This means that the last reported LRBG is not stored in the ERTMS/ETCS On-Board anymore. Note: In SUBSET-026 v2.3.0 it is not specified whether an $LRBG_{ONB}$ not reported to the RBC due to disturbance of safe connection shall be counted as one of the last eight LRBGs or not. In SUBSET-026 v3.4.0 and v3.6.0 (ref §3.5.4.5), a message sent to RBC during radio disturbance is considered as sent. Regardless of baseline, this problem exists.  After re-establishing the safe connection, the RBC tries to send an urgent/more restrictive message (e.g. conditional/unconditional emergency stop, TSR, shortened MA) to the ERTMS/ETCS On-Board and uses the $LRBG_{RBC}$ as a reference, which was reported by the ERTMS/ETCS On-Board equipment (see §3.6.2.2.2.b, which interferes with §3.10.2.1.3 – for v2.3.0 – and with §3.10.2.3 – for v3.4.0 and v3.6.0 – for unconditional emergency stops). But the ERTMS/ETCS On-Board may reject this new message from the RBC, because the used $LRBG_{RBC}$ is not referring to one of at least eight $LRBG_{ONB}$. *Consequences:* The provision of the urgent/more restrictive information is delayed until a new train position report indicating the current $LRBG_{ONB}$ is received (depends on position report parameters or the passing of a new balise group). The radio link supervision will not be effective as safety measure, because consistent messages are received (and may even be acknowledged without acceptance, see ETCS-H0019) by the ERTMS/ETCS On-Board before T_NVCONTACT expires.
Proposed mitigation	The specific application project shall analyse if it is possible to pass eight balise groups during T_NVCONTACT. If there is such a risk, a specific risk analysis has to be carried out.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

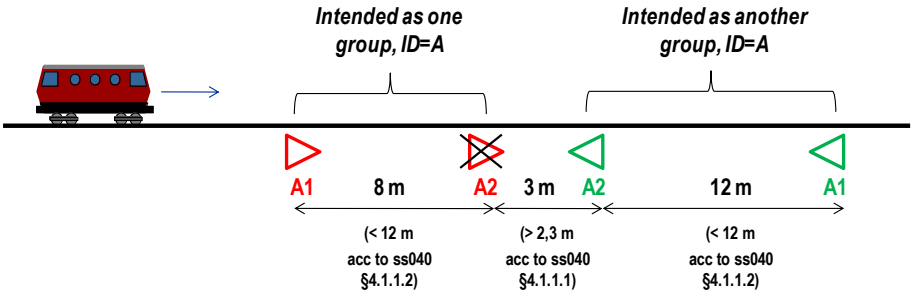
4.40 ETCS-H0040

<table>
<tr><td>Hazard ID</td><td>ETCS-H0040</td></tr>
<tr><td>Hazard headline</td><td>Non-acceptance of National Values in mode SN due to validity direction</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 (see v2.3.0, v3.4.0 and v3.6.0) §3.6.3.1.3 the train takes into account information valid for its orientation, with the exception of SL, PS (only for v3.4.0 and v3.6.0) and SH mode where the crossing direction is used for information from balise groups.
Mode SN may be used for shunting movements controlled by a national system, which might involve backwards movement, possibly over considerable distances. This can lead to the ERTMS/ETCS On-Board unit rejecting new national values because they are transmitted by balise groups for the direction opposite to the train’s orientation, but which happens to be the crossing direction. This is no immediate hazard since ETCS is not responsible for train safety in mode SN. But if later on a level or mode transition occurs (e.g. after manual level selection by driver) an incorrect set of national values will be applied. There is neither reverse movement protection nor roll away protection available in mode SN to prevent backwards movements.
Similar situations may occur in modes UN and NL where long backwards movements are possible because there is no reverse movement protection (UN and NL) and no roll away protection (NL, and in UN only optionally available if information about selected running direction is provided). In UN, a rejection of a change of the national values for Unfitted speed might be immediately hazardous.</td></tr>
<tr><td>Proposed mitigation</td><td>If balise groups transmitting national values are placed in areas where backward movements are be performed in mode SN/NL/UN (e.g. shunting area), then additional BGs for transmission of NV should be placed at the borders of the area to ensure that they are received after the backward movements have ended.
Further, to cover the scenarios where the need of the new national values arises even before the train exits the area, the new NVs could be placed in balise groups valid for both directions.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.41 ETCS-H0041

<table>
<tr><td>Hazard ID</td><td>ETCS-H0041</td></tr>
<tr><td>Hazard headline</td><td>Acknowledgement of Train Data is rejected when received in Reversing mode</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 v2.3.0 chapter §4.8.4, the Acknowledgement of Train Data is rejected by the ERTMS/ETCS On-Board in Reversing mode. This can cause a hazardous scenario: An ERTMS/ETCS On-Board is in Reversing mode, having received and accepted RV information from RBC.
a) The safe radio connection has been lost and the communication session is now considered as terminated. Then
• ERTMS/ETCS On-Board accept pkt 42 (session management) by BG and contacts RBC
• After initiating the session, ERTMS/ETCS On-Board sends Validated Train Data but then rejects the Ack received from RBC
• Further info sent by RBC, like extension of distance to go in RV, is rejected by ERTMS/ETCS On-Board because of SUBSET-026 v2.3.0 chapter 4.8.4, exception [3].
b) The train data are changed from external source (e.g train interface) and are sent to the RBC. This scenario is train-dependent.
In that case, as the acknowledgement of train data is rejected by ERTMS/ETCS On-Board according to SUBSET-026 v2.3.0 table §4.8.4, the RBC cannot update RV information to the ERTMS/ETCS On-Board even if it is connected and in session.
For the communication loss scenario, it is noted that it is relevant for those infrastructure where a train running in reversing mode can encounter packets 42 in BGs. This makes the problem worse compared to infrastructure where these packets are not encountered; because in the latter case at least the situation is clearer to the driver (it is shown that communication with RBC is down). Note that the loss of the session already takes time (5m after loss of radio connection in baseline 2) so there is a time period when nothing can arrive from RBC and driver does not know.
In Baseline 3, CR 896 solves this problem by specifying that the Acknowledgement of Train Data shall be accepted in Reversing mode.</td></tr>
<tr><td>Proposed mitigation</td><td>For scenario a: a possible mitigation is to avoid sending pkt 42 by balises inside an area where reversing is possible
For scenario b: Trackside specific application project should show that the remaining risk is acceptable.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §4.8.4 (see row “Acknowledgement of Train Data” for RV mode) of SUBSET-026 by CR 896 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.42 ETCS-H0042

Hazard ID	ETCS-H0042
Hazard headline	Balise groups with non-unique identities lead to possible hazard
Hazard description	According to SUBSET-026 v3.4.0 and v3.6.0 §3.18.4.4.3 and SUBSET-040 v2.3.0/ v3.3.0/ v3.4.0 §4.2.4.8.1 it is allowed for an unlinked balise group to have the same identity as another unlinked balise group or as a certain BG marked as linked but not announced via linking[3]. However, this could cause some safety related problems which need to be solved in another way than with unique balise group identifiers (NID_C + NID_BG). Here, two examples are pointed out: Example 1 SUBSET-036 v3.0.0 and v3.1.0 requires that balise configuration data, e.g. balise group identity, shall be used to determine which lobes are transmitted by the same balise or by different balises. Quote from SUBSET-036 v3.0.0 and v3.1.0 §6.2.1.6:"The ERTMS/ETCS On-Board Transmission Equipment shall filter the lobes of data transmission based on the physical properties of the Balise signal, and on the Balise configuration data given by the Balise telegram." When adjacent balise groups may have the same identity it is no longer possible to filter transmission lobes based on balise group identities. Also, the ETCS specifications contain no requirements aimed at safely distinguishing telegrams from adjacent balises at short distance from each other by odometer information. Example 2 If two balise groups with the same identity are placed close to each other and one of the closest balises is not read by a passing train, ERTMS/ETCS On-Board may create a "ghost" balise group from one balise in each group. This can lead to hazardous situations: see below:  A new "ghost" group is created from red A1 + green A2 (<12m). The new group could have lost restrictive info from the red group and/or picked up permissive info (valid in nominal direction, which is now to the right) from the green group.

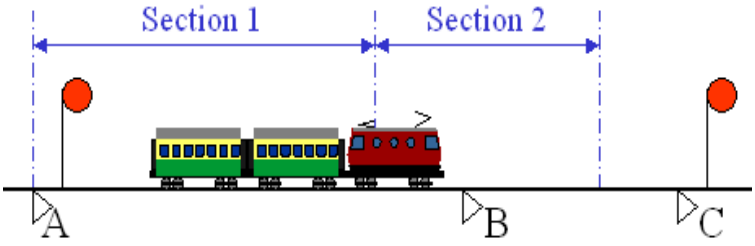
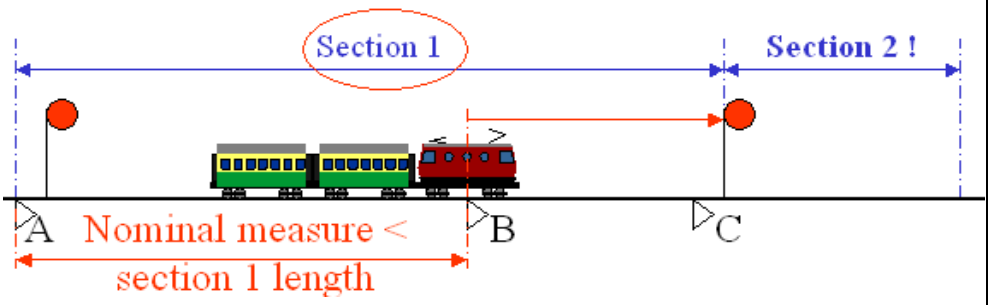
[3] A trackside announcing a BG marked as linked via linking which shares the ETCS ID of a BG marked as unlinked would violate clause 4.2.4.8.1 of SUBSET-040.

<table>
<tr><td></td><td>1) If green A1 still works: restrictive reaction according to SUBSET-026 v3.4.0 and v3.6.0 §3.16.2.5.1 approximately 12m after passing green A1 (delayed compared to engineering intention).
2) If green A1 is also silent: train will continue with the new erroneous information.</td></tr>
<tr><td>Proposed mitigation</td><td>In its hazard analysis, the trackside specific application shall consider the risks arising from balise groups with non-unique identifier. The examples above can be used as a base.
A barrier to risks found could be that between two Balise groups in the same track sharing the same Balise group identity, there shall be at least two Balises with a different Balise group identity.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.43 ETCS-H0043

<table>
<tr><td>Hazard ID</td><td>ETCS-H0043</td></tr>
<tr><td>Hazard headline</td><td>Balises rejected or wrongly considered by the ERTMS/ETCS On-Board when trackside is using VBC function</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 v3.4.0 and v3.6.0 section §3.15.9 (introduced in baseline 3), the Virtual Balise Cover (VBC) function allows the identification of certain balises that shall be ignored by the ERTMS/ETCS On-Board. The identification can be done either:
- by the driver (via the DMI during Start of Mission), or
- by the trackside (via packet 6 in a balise group).
When encountering a balise that is identified in this way, the ERTMS/ETCS On-Board ignores the whole telegram from it, providing that its VBC marker (packet 0 or packet 200) confirms that it can be ignored.
There are two possible hazardous situations resulting from this function:
H1. While the line is still under construction: the ERTMS/ETCS On-Board reads a balise telegram that should not be read, i.e. the inhibition is not on while it should be.
H2. After the line has been put into service: the ERTMS/ETCS On-Board ignores a balise telegram that should be read, i.e. the inhibition is still on while it should have been removed.
The FMEA in Appendix B identifies potential failures which need to be mitigated in order to avoid the two hazardous situations.</td></tr>
<tr><td>Proposed mitigation</td><td>Before implementing the VBC function into the trackside system, the infrastructure owner needs to perform a hazard analysis to define necessary engineering and operational rules; particular attention has to be taken to protect against entering of a B2 ERTMS/ETCS On-Board equipment into a B3 X=1 area. The FMEA in Appendix B can serve as a base.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE + EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.44 ETCS-H0044

Hazard ID	ETCS-H0044
Hazard headline	Repositioning problem in case of multi-sections
Hazard description	In case of repositioning with multi-sections (typically when there is a point) SUBSET-026 v2.3.0 and v3.4.0 §3.8.5.2 explains: “It shall be possible to update the length of the current section by means of repositioning information”. In SUBSET-026 v3.6.0 §3.8.5.2 has been reworded as follows “It shall be possible to update the length of an MA section by means of repositioning information contained in a balise group message”. The problem is linked to the identification of the “current section”. As specified in SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 §3.6.4.6, the ERTMS/ETCS On-Board must use the estimated position of the train to identify the current section. The hazard identified is the following: Before repositioning: the MA is stopped before the red signal  The BG B is considered in section 1, because of measure inaccuracy in the distance estimation, whereas it is physically in section 2, then the MA is extended up to location in advance of the red signal 
Proposed mitigation	The ETCS trackside specific application shall limit the risk by e.g.: • Limiting the odometer uncertainty by placing a linked balise group (with restrictive linking reaction) as close to the physical section boundary as possible (link from A-group to the new one) and by placing the B-group as soon after the physical section boundary as possible. • Increase the tolerance to odometer uncertainty by separating the shift between section 1 and 2 from the B-group as much as possible.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

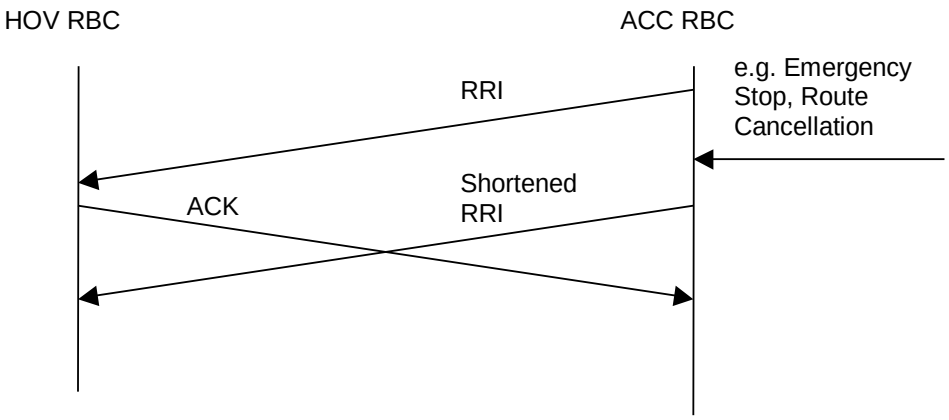
4.45 ETCS-H0045

<table>
<tr><td>Hazard ID</td><td>ETCS-H0045</td></tr>
<tr><td>Hazard headline</td><td>Risks related to “List of balises in SH area” function</td></tr>
<tr><td>Hazard description</td><td>ETCS Trackside has the possibility to limit a shunting area in which a train can move, to a certain number of balise groups allowed for the train to pass over. This information is sent to the ERTMS/ETCS On-Board with Packet 49 “List of balises for SH area”. If the train passes other balises groups, the ERTMS/ETCS On-Board will be tripped.
However, in some specific situations there is a risk that the ERTMS/ETCS On-Board will not use the list of balise groups. Thus the driver can mistakenly exit the shunting area without being stopped by ETCS. Appendix C identifies such situations.</td></tr>
<tr><td>Proposed mitigation</td><td>Before using the function “List of balises for SH area”, the ETCS trackside specific application shall as a minimum demonstrate that the situations in Appendix C will not occur.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE + EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y *)</td><td>Y *)</td><td>Y *)</td></tr>
<tr><td>B3MR1, X=1</td><td>Y *)</td><td>Y *)</td><td>Y *)</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y *)</td><td>Y *)</td></tr>
<tr><td>B3R2, X=1</td><td>Y *)</td><td>Y *)</td><td>Y *)</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y *)</td><td>Y *)</td></tr>
</table>
*) It depends on the case as described in Appendix C.
</td></tr>
</table>

4.46 ETCS-H0046

4.46.1.1 Intentionally left empty. No action by application projects is required.

4.47 ETCS-H0047

Hazard ID	ETCS-H0047
Hazard headline	Faulty definition of Q_RRIMACHANGE and Q_TDCHANGE
Hazard description	The definition of the variables Q_RRIMACHANGE and Q_TDCHANGE is incorrect in Baseline 2. Details can be found in the ERA Database CR 1088, or as follows: SUBSET-039 v2.3.0 §6.6.1.23 defines Q_RRIMACHANGE as “Relation of MA in the current RRI message to the MA in the last acknowledged RRI message.” The following scenario shows a problem with this definition. The ACC RBC sends an RRI to the HOV RBC. Before receiving an ACK for this RRI there is a route cancellation in the area of the ACC RBC and the ACC RBC has to send a shortened RRI to the HOV RBC. According to the definition of Q_RRIMACHANGE above, the ACC RBC shall not send the shortened RRI with Q_RRIMACHANGE = ”shortened”, because the previous RRI was not yet acknowledged. The HOV RBC receives now an RRI which is not identified as “shortened”. This means the HOV RBC cannot detect this situation efficiently by the Q_RRIMACHANGE identifier. For better understanding, please see the figure below.  Conclusion: The definition of Q_RRIMACHANGE has to be changed back to: “Relation of MA in the current RRI message to the MA in the last sent RRI message, if any.” (which is finally done in SUBSET-039 v3.1.0 and v3.2.0 §5.6.1.27 by introduction of CR 1088) Similar considerations are valid for the definition of Q_TDCHANGE.
Proposed mitigation	The proposed mitigation is to have an agreement between ACC RBC and HOV RBC on how to handle the flags Q_RRIMACHANGE and Q_TDCHANGE. Another possible mitigation for any HOV RBC (both B2 and B3), communicating with an ACC B2 RBC, is to compare the RRI messages instead of relying on the flag values. Nevertheless, this way of mitigating the problem somehow thwarts the meaning of the flags Q_RRIMACHANGE and Q_TDCHANGE. Another possible mitigation for any HOV RBC is to implement CR1088.
Mitigation allocated to	TRACKSIDE

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2" rowspan="2">Trackside</td><td colspan="5">ACC</td></tr>
<tr><td>B2</td><td>B3MR1, X=1</td><td>B3MR1, X=2</td><td>B3R2, X=1</td><td>B3R2, X=2</td></tr>
<tr><td rowspan="5">HOV</td><td>B2</td><td>Y</td><td>N *)</td><td>N *)</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N *)</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>Y</td><td>N *)</td><td>N *)</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N *)</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N *)</td><td>N</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §5.6.1.27 of SUBSET 039 by CR 1088 and SUBSET-039 v3.2.0 close the hazardous situation
</td></tr>
</table>

4.48 ETCS-H0048

4.48.1.1 Intentionally left empty. No action by application projects is required.

4.49 ETCS-H0049

4.49.1.1 Intentionally left empty. No action by application projects is required.

4.50 ETCS-H0050

4.50.1.1 Intentionally left empty. No action by application projects is required.

4.51 ETCS-H0051

4.51.1.1 Intentionally left empty. No action by application projects is required.

4.52 ETCS-H0052

4.52.1.1 Intentionally left empty. No action by application projects is required.

4.53 ETCS-H0053

<table>
<tr><td>Hazard ID</td><td>ETCS-H0053</td></tr>
<tr><td>Hazard headline</td><td>Unexpected handling of Conditional Emergency Stop on Entry into L2</td></tr>
<tr><td>Hazard description</td><td>For a Conditional Emergency Stop message stored in the transition buffer, the B2 ERTMS/ETCS On-Board will compare the stop location with the position of the train when this message is extracted from the buffer, while a B3 train will compare it with the position when it was received (see SUBSET-026 both v3.4.0 and v3.6.0 §4.8.5.7). Thus, depending on when the buffer is evaluated, a B2 ERTMS/ETCS On-Board may reject a CES that a B3 ERTMS/ETCS On-Board accepts.</td></tr>
<tr><td>Proposed mitigation</td><td>Trackside could define other measures for MA revocation in an entry situation.
Trackside could design an entry where the entry signal is passed under responsibility of a different train protection system, such as an STM</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §4.8.5.7 of SUBSET-026 by CR 866 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.54 ETCS-H0054

Hazard ID	ETCS-H0054
Hazard headline	Use of Euroloop and Radio Infill for information that if missed could lead to safety consequences
Hazard description	There is a problem with sending safety-critical information via Euroloop or Radio Infill (with safety-critical it is here meant information that is missed could lead to safety consequences). In SUBSET-091, no safety target has been allocated to the deletion of information from Euroloop or Radio Infill. Therefore, the ETCS standard contains no such safety integrity requirement on these components, and thereby the safety performance of this failure mode is supplier specific. This is due to the fact that: • The assumption has been made that deletion of infill information is not hazardous, ref SUBSET-091 §5.3.1.4. • The delivery of the non-infill information from infill devices allowed by SUBSET-040 §4.2.4.4 (both for v3.3.0 and v3.4.0) has not been considered safety critical, with the exception that the use of Packet 44 is undefined in the ETCS specifications and thus not possible to analyse. These two assumptions need to be verified on application level. Specific issue: As a special issue to the first bullet above, a Baseline 3 ERTMS/ETCS On-Board could – under unfavourable circumstances – systematically reject infill information from a Baseline 2 Euroloop or Radio Infill. The problem is related to CR 712 and concerns the fact that SUBSET-040 v3.3.0 and v3.4.0 §4.2.4.4 restricts which packets are allowed to be sent as non-infill information from Euroloop and Radio Infill, while SUBSET-026 v2.3.0 (B2) section §7.4.2 allows “any transmission media” (not excluding Euroloop or Radio Infill) for almost all packets. So if B2 ETCS Trackside interprets SUBSET-026 v2.3.0 so that all packets are allowed to be sent as non-infill information from Euroloop or Radio Infill, while the B3 ERTMS/ETCS On-Board makes a strict interpretation according to SUBSET-040 v3.3.0/v3.4.0, the ERTMS/ETCS On-Board could reject the whole message containing the “not allowed” non-infill packet from the infill device. Most packets are not possible to send as non-infill information from a Euroloop or Radio Infill anyway, because they contain distance information which is not available from these devices. But some packets; 42, 45, 46, 72, 76 and 79, does not contain distance information and could therefore theoretically be sent. It is not believed hazardous to miss these packets in themselves, but as a result of the rejection of the whole message, also other infill information in the packets contained in that message would be rejected, which could have safety consequences if they contain restrictive information. If both ERTMS/ETCS On-Board and Trackside are implemented according to Baseline 3, CR 712 makes sure that the problem is solved because SUBSET-026 (for both v3.4.0 and v3.6.0) section §7.4.2 specifies exactly which transmission media that is allowed for ETCS Trackside to use for each packet (matching the list in SUBSET-040 §4.2.4.4 both for v3.3.0 and v3.4.0).

<table>
<tr><td>Proposed mitigation</td><td>In the safety analysis the ETCS trackside should not rely on the ERTMS/ETCS On-Board use of information transmitted via Euroloop or Radio Infill (i.e. it should not have safety consequences if the information is missed).</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.55 ETCS-H0055

<table>
<tr><td>Hazard ID</td><td>ETCS-H0055</td></tr>
<tr><td>Hazard headline</td><td>Unspecified train movement supervision after PT or RV distance is overpassed</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 v2.3.0, modified by SUBSET-108 v1.2.0 CR 138 and CR 686, §3.14.1.7.1 & §3.15.4.8, if the brake command was triggered due to exceeding the reversing distance related to a reversing area, the brake command shall be released at once if the reversing distance has been extended so that the reversing distance is no longer exceeded, or at standstill after driver acknowledgement. However, a safe reaction of the B2 ERTMS/ETCS On-Board for further backwards movements is not clearly specified.
The hazard situation arises when train is moving backwards after the brake release due to PT or RV distance is overpassed. In Baseline 2, it is not specified that the train shall command again the brake for any further movements in the opposite direction to the train orientation when the permitted distance is overpassed.
Therefore, this situation could lead to derailment or collision since the train could enter a route which is set for other train.
In Baseline 3, CR 844 and CR 1096 solve this problem by specifying that brake command is triggered due to an overpassed reversing distance related to a reversing area or due to any further movement in the direction opposite to the train orientation while the reversing distance is still overpassed</td></tr>
<tr><td>Proposed mitigation</td><td>The ERTMS Application Project shall require Operational Procedures to prevent unsafe consecutive backwards movements.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §3.14.1.7.1 of SUBSET-026 by CR 844 and 1096 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.56 ETCS-H0056

<table>
<tr><td>Hazard ID</td><td>ETCS-H0056</td></tr>
<tr><td>Hazard headline</td><td>Rejection of non revocable TSRs received in a message containing several non revocable TSRs</td></tr>
<tr><td>Hazard description</td><td>Based on SUBSET-026 v2.3.0 §8.4.1.4.2:
‘Exception 2: A message can contain several packets 65 (Temporary Speed Restriction). The identities of the corresponding temporary speed restrictions (variable NID_TSR) transmitted in the same message shall be different.’
A B2 trackside may consider that NID_TSR = 255 is not an ID and that §8.4.1.4.2 does not apply to multiple non revocable TSRs.
A B2 ERTMS/ETCS On-Board may have been implemented so that it rejects multiple non-revocable TSRs (NID_TSR = 255) if they are received in the same message because all non-revocable TSRs in that message have the same ID. The problem is solved in B3, where SUBSET-026 v3.4.0 and v3.6.0 now (via CR 843) specify that the exception is only applicable to revocable TSRs.</td></tr>
<tr><td>Proposed mitigation</td><td>The ETCS Trackside (B2 or B3 X=1) shall not send multiple non-revocable TSRs in the same message but put them in different messages.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §8.4.1.4.2 of SUBSET-026 by CR 843 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.57 ETCS-H0057

<table>
<tr><td>Hazard ID</td><td>ETCS-H0057</td></tr>
<tr><td>Hazard headline</td><td>Possible different approaches of B2 and B3 ERTMS/ETCS On-Boards to NVs received (announced) but not yet applicable while entering NP mode.</td></tr>
<tr><td>Hazard description</td><td>Scenario 1
ETCS B2 ERTMS/ETCS On-Board with implemented CR 710 or B3 ERTMS/ETCS On-Board deletes received (announced) but not yet applicable NVs (see SUBSET-026 v3.4.0 and v3.6.0 section §3.18.2.9). However, this behaviour is not expected by ETCS B2 trackside which is not aware of CR 710. As B2 trackside does not expect this behaviour, it does not send appropriate NVs and thus ERTMS/ETCS On-Board uses default ones. Therefore, a hazardous situation could arise if:
• an ERTMS/ETCS On-Board deletes stored but not yet applicable NVs sent by trackside;
• a trackside does not expect this deletion and does not sent NVs which are appropriate for a given location again;
• an ERTMS/ETCS On-Board uses default NVs that are less restrictive than expected ones.
Scenario 2
B2 ERTMS/ETCS On-Board (without implemented CR 710) could keep received (announced) but not yet applicable NVs while ETCS B2 trackside aware of CR 710 or B3 X=1 trackside expects these NVs to be deleted by the ERTMS/ETCS On-Board. Therefore, a hazardous situation could arise if:
• an ERTMS/ETCS On-Board (after entering NP mode) keeps stored but not yet applicable NVs sent by trackside;
• a trackside expects these NVs to be deleted and thus expects that ERTMS/ETCS On-Board uses default NVs (because of this, trackside does not send other NVs) – e.g. the route, for which NVs were announced, is no longer set;
• an ERTMS/ETCS On-Board uses stored NVs that could be less restrictive than the default ones and applies them for the area in which they are not valid.</td></tr>
<tr><td>Proposed mitigation</td><td>Scenario 1
The problem is related to situations when ERTMS/ETCS On-Board receives NVs intended for specific route but it deletes it by entering NP mode. If there is necessity to use more restrictive NVs for a specific route, NVs should be repeated by trackside when entering the route.
Scenario 2
The B2 trackside or B3 X=1 trackside has always to send valid NVs as soon as possible to ERTMS/ETCS On-Board after it leaves NP mode.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §3.18.2.9 and §3.18.2.10 of SUBSET-026 by CR 710 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.58 ETCS-H0058

<table>
<tr><td>Hazard ID</td><td>ETCS-H0058</td></tr>
<tr><td>Hazard headline</td><td>Balise message rejected in duplicated balise groups</td></tr>
<tr><td>Hazard description</td><td>In Baseline 3 if the balises are duplicated within a balise group and a balise is not read or not decoded correctly but the duplicated balise is, then regardless of whether the balise group is linked or unlinked the message shall not be rejected and no linking reaction (SUBSET-026 for both v3.4.0 and v3.6.0 §3.16.2.4.4.1) shall be applied (as specified in CR 819).

However, Baseline 2 has an ambiguous definition for Balise group message consistency specifications for duplicated Balise Groups. An ERTMS/ETCS On-Board unit (without CR 819 implemented) always rejects BG message if a balise is not found or not decoded in a BG, even if another balise in the group duplicates the missed one, but if a duplicating one is correctly read it will not apply the linking reaction (SUBSET-026 v2.3.0 § 3.16.2.4.4.1). So a hazardous situation can happen when safety related information is sent by duplicated balise groups.

Another effect related to this hazardous situation is the following: the trackside will have used in their safety cases an availability rate for the BG with duplicated balises which is not in line with the system behaviour, i.e. trackside will assume that the BG is unavailable only if both duplicated balises fail, but actually the BG message will not be used if only one of the duplicated balises fails.</td></tr>
<tr><td>Proposed mitigation</td><td>The ETCS trackside should not put information in duplicate balise groups, which if missed, would lead to hazardous consequences.

Related to the BG message availability, the trackside has to analyse availability rate decrease when duplicate balise groups are used.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §3.16.2.4.4.1 of SUBSET-026 by CR 819 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.59 ETCS-H0059

<table>
<tr><td>Hazard ID</td><td>ETCS-H0059</td></tr>
<tr><td>Hazard headline</td><td>Resetting of Adhesion Factor when passing into an STM area</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 v2.3.0 section §4.10, the Adhesion Factor shall be reset from its current (possibly restrictive) value to its non-restrictive default value when entering SN mode. However, reasonably the rail has the same properties on both sides of the level border. Thus, if not handled properly, this could lead to a non-restrictive supervision.
If the reduced Adhesion Factor was set by trackside, it can be assumed that the trackside sets this value also in the STM area, if applicable. However, if the reduced Adhesion Factor was set by the driver, and the driver is not observing this behaviour, this hazardous scenario is possible:
- The ETCS supervision doesn’t consider the slippery track conditions if the train later returns to the ETCS area.
This problem was solved in Baseline 3, with the introduction of CR 1030. SUBSET-026 v3.4.0 and v3.6.0 specify that the Adhesion Factor (from driver) is unchanged when entering SN mode.</td></tr>
<tr><td>Proposed mitigation</td><td>For a Baseline 2 ERTMS/ETCS On-Board, the driver needs to make sure that the reduced Track Adhesion is set again before entering (again) into an L1 or L2/3 area. Particular care must be taken when designing the operational rules since the behaviour is different for Baseline 2 and Baseline 3 ERTMS/ETCS On-Board systems.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N*)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N*)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §4.10 (“Adhesion Factor (from driver) “)of SUBSET-026 by CR 1030 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

4.60 ETCS-H0060

<table>
<tr><td>Hazard ID</td><td>ETCS-H0060</td></tr>
<tr><td>Hazard headline</td><td>Unclear use of telegram header info when a balise telegram or BG message is ignored/rejected</td></tr>
<tr><td>Hazard description</td><td>There are two possible hazardous situations related to the use of some information from the header when the concerned BG is rejected:
1) ERTMS/ETCS On-Board unexpectedly using default National Values, when these are less restrictive than the National Values.
Related to SUBSET-026 (v2.3.0) §3.18.2.5 second bullet: a Baseline 2 ERTMS/ETCS On-Board could use the default National Values when a mismatch has been detected between the country or region identifier read from a BG and the corresponding identifier of the applicable and stored NV although the BG message has been rejected, e.g. according to the SUBSET-026 (v2.3.0) §3.16.2.4.3 (rejection of BG marked as linked not included in the linking). In that situation, default values are used by the ERTMS/ETCS On-Board and this is not expected by ETCS trackside.
2) RBC not sending information because it assumes that the ERTMS/ETCS On-Board has received the information from a BG reported as LRBG.
Related to SUBSET-026 (v2.3.0) §3.6.2.2.2 a): a Baseline 2 ERTMS/ETCS On-Board could use as reference to report its position to the RBC a balise group although the message has been rejected due to M_MCOUNT=254, see SUBSET-026 (v2.3.0) §3.16.2.4.7. The RBC (B2/B3) cannot know that this message has been rejected.</td></tr>
<tr><td>Proposed mitigation</td><td>Related to the first scenario above: This case is covered by ETCS-H0005.
Related to the second scenario above: As project specific mitigation (ETCS Trackside), the RBC should not assume that the ERTMS/ETCS On-Board has received the information from a BG reported as LRBG.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>For both scenarios:
<table>
<tr><td colspan="2"></td><td>ERTMS/ETCS On-Board</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to SUBSET-026 by CR 1183 and SUBSET-026 v3.6.0 close the hazardous situation
If the Baseline 2 ERTMS/ETCS On-Board has an implementation in line with the solution of CR 1183, the above issues are not applicable, either.</td></tr>
</table>

4.61 ETCS-H0061

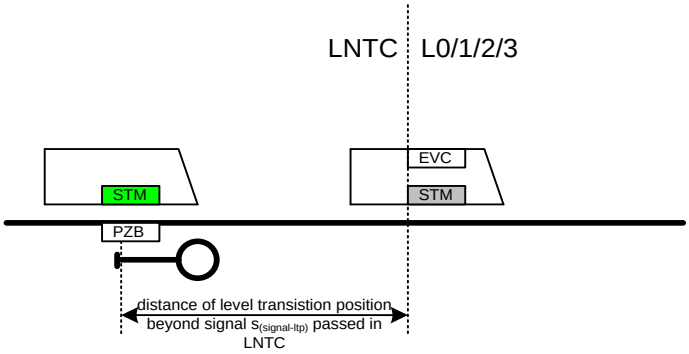
Hazard ID	ETCS-H0061
Hazard headline	Trackside provisions to avert unsafe consequences when the on-board resets the train position confidence interval and relocates trackside information using the estimated travelled distance between current LRBG and a previously encountered BG
Hazard description	A harmonized solution for resetting the train position confidence interval and relocating all location related information in cases where trackside does not provide information about the distance between balise groups was introduced in Baseline 3 by CR 782. This solution is defined in SUBSET-026 (both v3.4.0 and v3.6.0) §3.6.4.3b), §3.6.4.7.1 and §3.6.4.7.2: specifying that when no linking distance is known, only the estimated travelled distance between balise groups shall be taken into account for the reset/relocation. When a BG becomes the new LRBG, the odometry error accumulated since reading the previously encountered BG will not be part of the confidence interval and it will not be considered when relocating the location information based on the former LRBG. In practice, this means that in case the train odometer underestimates the travelled distance, these locations would become farther away from the train than they actually are, while the opposite would happen in case the odometer overestimates the travelled distance. From SUBSET-026 §3.6.4.3.1, it follows that it is the responsibility of the Trackside to be aware of this ERTMS/ETCS On-Board behaviour and – for scenarios where this may result in unsafe situations – take provisions when engineering the distance information. However, there are scenarios where it would be difficult for Trackside to provide the adequate provisions or where the provision would have operational drawbacks. The scope of this hazard log entry is to alert the trackside engineers about the difficulty to take the necessary provisions by giving examples of such scenarios. 1) **Supervision of location based information received from a BG marked as unlinked** It is not possible to provide linking information for a balise group marked as unlinked (for example: a BG installed temporarily on the track). When another balise group becomes the LRBG, the location data (for example: the start and end location of a TSR) that the ERTMS/ETCS On-Board accepted from the BG marked as unlinked will be relocated using the estimated travelled distance and the accumulated odometer errors will not be considered in the confidence interval. In addition, the confidence interval will be recalculated using the location accuracy of the LRBG - not that of the BG that transmitted the TSR (the Q_NVLOCACC from the national values). Since temporary balise groups may be installed with less accuracy than balise groups installed permanently, this may further falsify the relocated position of the location data. Possible consequences: • the actual train front end might be closer to the start of the TSR than the calculated max safe front end; • the actual rear end might still be inside the speed restriction while the ERTMS/ETCS On-Board calculates that the min safe rear end has already left it. 2) **Repositioning** Trackside cannot provide the correct linking distance between the main balise group and the repositioning balise group: linking information announcing a repositioning BG does not provide the actual linking distance to this BG but to the end of the expectation window of the farthest balise group containing repositioning information.

	Thus, when the repositioning balise group encountered by the train becomes the LRBG, SUBSET-026 §3.6.4.3.b applies and the ERTMS/ETCS On-Board performs the relocation using the estimated travelled distance from the BG that provided the linking information (=the main signal BG) to the new LRBG. This may be problematic in supervising the following: • locations beyond the train front end: for example. the location of a speed decrease. If the repositioning BG does not send a speed profile, and the SSP provided by the main signal BG contains a speed decrease, then the on-board when calculating the distance from the max safe front end to this speed decrease will disregard the odometer error accumulated between the main BG and the repositioning BG. The actual train front end might be nearer to the speed decrease location than the calculated max safe front end. • locations to be supervised with the train rear end: for example, the end of a speed restriction covering points in rear of the repositioning BG. Once the repositioning BG is encountered, the on-board in calculating the distance between min safe rear end and the end of the speed restriction will disregard the odometer error accumulated between the main BG and the repositioning BG. The actual rear end might still be inside the speed restriction while the ERTMS/ETCS On-Board calculates that the min safe rear end has already left it. 3) **Transition to Level 1 or 2/3 with information stored in the transition buffer** In case any information retrieved from the transition buffer is using an LRBG which is not part of the linking chain, or in case the current LRBG when the information is retrieved is not part of the linking chain, the actual distance from that former LRBG to the current LRBG cannot be determined from the available linking info. In this case, when relocating any distance information that is based on the former LRBG, the on-board will disregard the odometer error accumulated between that former LRBG and the BG that follows it in the linking chain. The actual train front end might be closer to the relocated locations than the calculated max safe front end. A similar issue would exist with the actual rear end.
Proposed mitigation	In scenarios like those presented in this hazard log entry, each specific application safety analysis shall identify the appropriate measures trackside shall take when engineering the distance information, as hinted in Subset-026 §3.6.4.3.1. In the following, some directions for the measures to be taken are presented. 1) Location based info in BG marked as unlinked The trackside may engineer the distances transmitted adding a margin. The principle would be to reintroduce via this margin the error that the ERTMS/ETCS On-Board odometry accumulates in measuring the distance travelled from the BG that transmits the info to the BG that will become the LRBG, because this accumulated error will not be part of the confidence interval and will not be subtracted from the distance between the previous LRBG and the location info (the start of the TSR in our scenario). There are 2 difficulties in doing that: a) the Trackside cannot know the value of the accumulated errors the ERTMS/ETCS On-Board makes in measuring the travelled distance. The only harmonized requirement on which it could make an estimate is SUBSET-041 §5.3.1.1. However, that requirement states also that “in case of malfunctioning the ERTMS/ETCS On-Board equipment shall evaluate a safe confidence interval”, something trackside cannot do for the ERTMS/ETCS On-Board. b) if trackside to be on the safe side uses a large margin, this would have an operational impact by making all trains – independent of the accumulated

<table>
<tr><td></td><td>odometer error they have – slow down for a much longer stretch of line than required by the TSR.

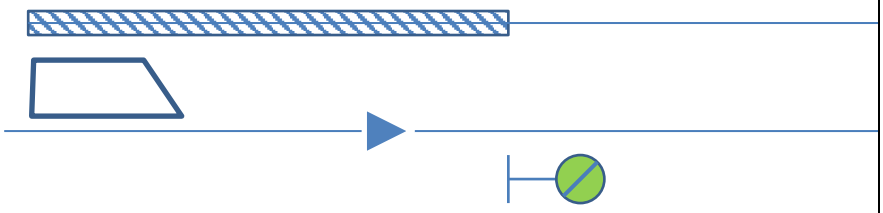
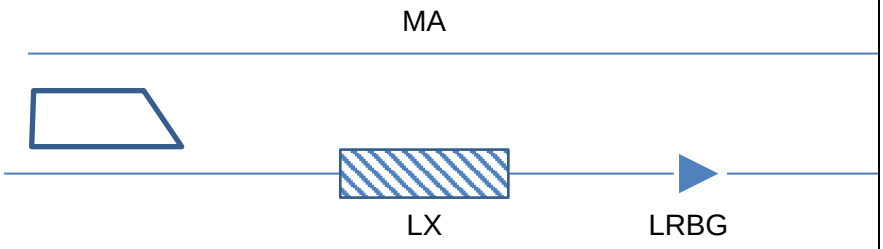
Trackside may also consider to put a margin in the value of Q_LOCACC in the linking packet, to mitigate what is mentioned in the scenario discussion. This would have performance drawbacks and possibly unsafe drawbacks in case of a fixed release speed given by trackside (delayed trip).
2) Repositioning
For the first bullet, include the SSP in the repositioning BG. Note that especially if other info has to be added (ASP, TSR, LX info, etc.) this may imply installing additional balises and there has to be enough space in the track for this. For the second bullet, the same as in scenario 1) applies in artificially enlarging the distance to the location of a speed reduction.
3) Transition to Level 1 or 2/3 with information stored in the transition buffer
Make sure that any BG located between the BG on which the level transition announcement is based and the level transition border is either marked as unlinked or contained in the linking information. However, having it in the linking chain could be inconvenient because the BG in the adjacent area can be related to a national system and therefore ETCS trackside is impacted each time a BG is added or removed in rear of the border.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>(*)</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
(*) See H0018
</td></tr>
</table>

4.62 ETCS-H0062

Hazard ID	ETCS-H0062
Hazard headline	Level transition from LNTC to L0/1/2/3 releases emergency brake
Hazard description	This possible hazard is valid for those level transitions to L0, L1, L2 and L3 that take place in a certain distance beyond a signal that was passed under responsibility and supervision of a National System. *Note: the hazard is applicable if the ERTMS/ETCS On-Board equipment is interfaced to a national system, regardless whether through an STM or by other means; for the sake of simplicity however in the following drawings only the case of STM interface is depicted.* The responsibility of and supervision by the National System ends at the level transition location (LTP). In case the train in level NTC passes a signal showing a stop aspect, which is protected by a national train control system (e.g. PZB (2000Hz magnet) for DB AG), this system is responsible for supervision (see figure, green coloured STM).  If the emergency brake has been triggered in level NTC, the access to the emergency brake command output is revoked by the ERTMS/ETCS On-Board if the train passes the border to a different level. This may lead to a safety critical situation if the conditions to command the emergency brake are still valid, but the ERTMS/ETCS On-Board, now, e.g., in ETCS L1, has no knowledge of the history before the change of level. In this example, the PZB system evaluates the national trip situation, triggers a safety reaction but safety reaction (emergency brake) will be released by ETCS.
Proposed mitigation	This hazard has to be solved in trackside project specific analysis. Another possible solution for L0/L1/L2 trackside could be to analyse and to design the Level transition from LNTC to L0/L1/L2 in a safe way; for instance L0/L1/L2 trackside may take into account the signal aspect of the signal passed under LNTC responsibility.
Mitigation allocated to	TRACKSIDE

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y *)</td><td>N**)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y *)</td><td>N**)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N**)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y *)</td><td>N**)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N**)</td><td>N</td></tr>
</table>
*) If CR 618 is implemented there is no hazard. (CR neither IN nor OUT in SUBSET-108 v1.2.0)
**) For baselines 3, the changes introduced to SUBSET-035 by CR 618 and SUBSET-035 v3.2.0 close the hazardous situation
</td></tr>
</table>

4.63 ETCS-H0063

Hazard ID	ETCS-H0063
Hazard headline	Limits in use of Shifted Location Reference
Hazard description	When the LRBG is in advance of the train's front end, e.g. after a change of driving cab, the RBC can grant a MA to this train using Shifted Location Reference. If – after granting the MA – the operational situation changes, the RBC might be required to react on this change by sending co-operative route revocation (message 9: request to shorten MA) or by updating a restriction using a general message (message 24). In both cases, the use of Shifted Location Reference (D_REF) is not possible. Three examples are given: a) Start of Mission after a change of driving cab, with on-sight mode profile up to the next signal and MA extended beyond this signal:  In case there occurs a restriction inside the MA and the RBC is required to shorten this MA by means of a Request to Shorten MA (message 9) before the train has passed the LRBG, it cannot do this because D_REF is not defined for message 9. Doing this without regarding D_REF, based on the LRBG location, this would remove the OS mode profile from the train's front end up to the LRBG. train would be allowed to run in FS mode where OS mode was required b) Start of Mission in rear of a 'protected' level crossing with MA up to a location beyond the level crossing:  In case the level crossing changes its state to 'not protected' or 'faulty', the RBC is required to update the LX information for the train, by means of LX information or TSR packets, with the same shifted location reference (D_REF). This is not possible because D_REF is not available for a general message (message 24). Sending this new information with an updated MA is also no reliable method, because this new information, added to the original MA, could exceed the limit of 500 bytes in size for a radio message. ➔ New restriction cannot be transmitted to train in a reliable way

<table>
<tr><td></td><td>
c) Start of Mission in rear of a dynamic profile (e.g. track conditions, TSR,…) with MA up to a location beyond the dynamic profile start location:
For B2 ERTMS/ETCS On-Board the only message allowing D_REF field is message 33. In B3 ERTMS/ETCS On-Board the messages allowing the use of D_REF are:
- Message 33
- Message 34
- Message 15.

In fact in all 3 scenarios, according to 3.7.1.1.c (see SUBSET-026 v2.3.0, v3.4.0 and v3.6.0) MA and Mode profile shall not be considered as a Track description. Moreover clause §3.7.3.1 (SUBSET-026 v3.4.0 and v3.6.0) doesn't apply to MA and Mode Profile since mode profile according to 3.7.1.1.c can't be considered a track description. According to SUBSET-026 (see v2.3.0, v3.4.0 and v3.6.0) §3.12.4.3, on a reception of a new MA with or without Mode profile, the currently supervised mode profile shall be deleted and the new one replaces the previous one (see also SUBSET-040, §4.3.2.1.1.c for v2.3.0, v3.3.0 and v3.4.0). According to table §4.8.3 of SUBSET-026 (see v2.3.0, v3.4.0 and v3.6.0), a cooperative shortening of MA sent by RBC is going to go to be accepted because track descriptions cover the MA and the mode profile (filtering condition A [3] [4] [5] of §4.8.3 of SUBSET-026 v3.4.0 and v3.6.0). Finally, according to Item a) of clause §3.8.5.1 (SUBSET-026 v3.4.0 and v3.6.0) new MA shall delete all information given in the previous one. If trackside should use message 9 to give a reduction of MA, the RBC is going to create a danger situation because the ERTMS/ETCS On-Board is going to
- delete the mode profile information from the head of the train (which is in rear of the LRBG) to the LRBG,
- manage the new MA starting from the LRBG and going up to the new SvL
Therefore for B2 the scenario involving the use of CES message shall be taken into account.
</td></tr>
<tr><td>Proposed mitigation</td><td>Each trackside specific application safety analysis shall analyse the scenarios given in this hazard report and take appropriate measures, if necessary.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.64 ETCS-H0064

4.64.1.1 Intentionally left empty. No action by application projects is required.

4.65 ETCS-H0065

4.65.1.1 Intentionally left empty. No action by application projects is required.

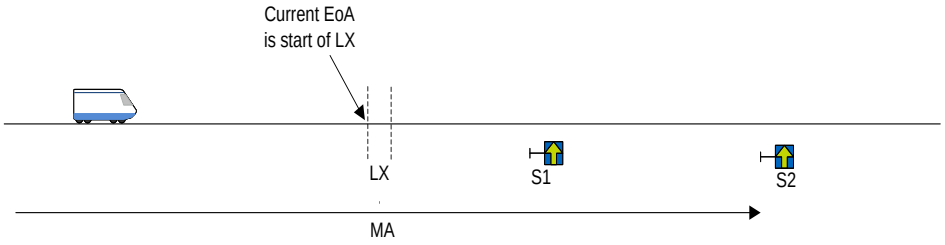
4.66 ETCS-H0066

4.66.1.1 Intentionally left empty. No action by application projects is required.

4.67 ETCS-H0067

4.67.1.1 Intentionally left empty. No action by application projects is required.

4.68 ETCS-H0068

Hazard ID	ETCS-H0068
Hazard headline	Hazardous evaluation of CES beyond a ‘temporary EoA/SvL’
Hazard description	Possible temporary EoA/SvL according SUBSET-026 v2.3.0 and v3.4.0 and v3.6.0: 1. Unprotected LX: §5.16.1.1 of SUBSET-026 v3.4.0 and v3.6.0, 2. Start of SH mode profile: §5.7.3.4 of SUBSET-026 in v2.3.0, modified by SUBSET-108 v1.2.0 CR 601, v3.4.0 and v3.6.0, 3. Start of OS mode profile: §5.9.3.5 of SUBSET-026 in v2.3.0, modified by SUBSET-108 v1.2.0 CR 601, v3.4.0 and v3.6.0, 4. First route unsuitability SUBSET-026 v3.4.0 and v3.6.0, §3.12.2.6 of SUBSET-026 in v2.3.0, modified by SUBSET-108 v1.2.0 CR 664, §3.12.2.4 of SUBSET-026 in v3.4.0 and v3.6.0 5. Start of LS mode profile: §5.19.3.5 of SUBSET-026 v3.4.0 and v3.6.0 In case the ERTMS/ETCS On-Board supervises a temporary EoA/SvL, SUBSET-026 allows different interpretations if the ERTMS/ETCS On-Board should define the new EoA and SvL, if a conditional emergency stop location is given between temporary EoA/SvL and the EoA/SvL given with the MA (refer to SUBSET-026, §3.10.2). It is a matter of interpretation that the ERTMS/ETCS On-Board considers a Conditional Emergency Stop as relevant if the Emergency Stop Location is beyond the temporary EoA/SvL. Scenario (example for unprotected LX only, but the mechanism is similar for the other situations 2 to 5 above): 1. ERTMS/ETCS On-Board receives MA (up to S2) with LX profile. 2. ERTMS/ETCS On-Board considers the start of the unprotected LX as temporary EoA/SvL (S-026 v3.4.0, §5.16.1.1).  3. ERTMS/ETCS On-Board receives a Conditional Emergency Stop (with emergency stop location at S1) from RBC for a location beyond the LX, but in rear of the EoA given by the previous MA. 4. ERTMS/ETCS On-Board accepts the CES, but it does not define a new EoA/SvL because the location is beyond the current (temporary) EoA (if the temporary EoA/SvL is considered as current EoA/SvL; SUBSET-026 v3.4.0 and v3.6.0, §3.10.2.2, 2nd bullet resp. SUBSET-026 v2.3.0 §3.10.2.1.2 2nd bullet). Note: For B3 ERTMS/ETCS On-Board running on a X=2 track, the acknowledgement sent to the RBC is msg 147 with Q_EMERGENCYSTOP = 1 (accepted, but no change in EoA). An ERTMS/ETCS On-Board running on a X=1 track would send a msg 147 with Q_EMERGENCYSTOP = 0 (Conditional Emergency Stop considered)

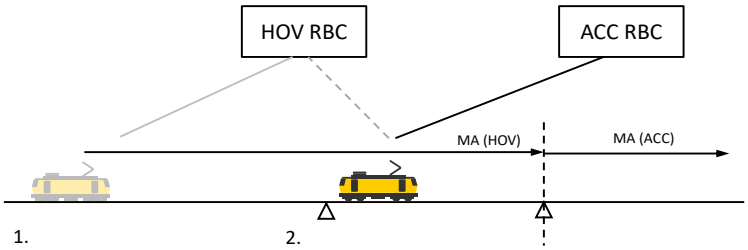
<table>
<tr><td></td><td>5. ERTMS/ETCS On-Board receives information that the LX is protected – the EoA/SvL at the crossing is deleted, and replaced with the EoA/SvL given by the MA (SUBSET-026 v3.4.0 and v3.6.0, §3.12.5.3)
Alternatively, ERTMS/ETCS On-Board has stopped inside the stopping area in rear of the LX. This event removes the temporary EoA/SvL and replaces it with the EoA/SVL given by the MA (SUBSET-026 v3.4.0 and v3.6.0, §5.16.2.1)
The ERTMS/ETCS On-Board may then continue past the LX and beyond the CES location, which will be unsupervised by ETCS.</td></tr>
<tr><td>Proposed mitigation</td><td>The trackside should take appropriate measures to avoid the situation of sending a CES that would be located between the beginning of a mode profile (or start of an unprotected level crossing or first route unsuitability) and the MA EOA (e.g. to send a shorter MA instead of a CES,...).</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.69 ETCS-H0069

4.69.1.1 Intentionally left empty. No action by application projects is required.

4.70 ETCS-H0070

Hazard ID	ETCS-H0070
Hazard headline	Session establishment pkt.42 leads to supervision gap for vehicles with one mobile during NRBC handover
Hazard description	The clause §3.5.3.5.2 for v3.4.0 of SUBSET-026 says: *"If the ERTMS/ETCS On-Board equipment has to establish a communication session with an RBC whilst in session with another RBC, the existing communication session shall be terminated (see §3.5.5.2 for details) and the new one shall be established. Exception: the order to contact an Accepting RBC shall not terminate the communication session with the Handing Over RBC.".* The last sentence of this clause reads as if the exception only concerns the "order to contact an Accepting RBC" as defined in clause §3.5.3.5.3: Clause §3.5.3.5.3 for v3.4.0 of SUBSET-026: *"The order to contact an Accepting RBC shall be part of the RBC transition order and shall include:* *a) The identity of the Accepting RBC.* *b) The telephone number of the Accepting RBC.* *c) Whether this applies also to Sleeping unit.".* If the exception of clause §3.5.3.5.2 for v3.4.0 of SUBSET-026 only applies to the "order to contact an Accepting RBC" as per clause §3.5.3.5.3, for v3.4.0 of SUBSET-026, then it seems that some system aspects have been missed. Let's consider for example the following scenario: A train is running in level 2 in a mixed level area (level 2 + level 1 for instance). The train is approaching and RBC/RBC transition border and can handle only one communication session. The train receives from the handing over RBC an RBC transition order that contains the order to contact the Accepting RBC. The train does not establish the communication session with the Accepting RBC as it can handle only one communication session. The train continues to run and encounters a balise group providing a packet 42 ordering to establish the communication session with the RBC of the area that will be entered. It considers that the clause §3.5.3.5.2 (v3.4.0 of SUBSET-026) applies (the exception does not apply), it terminates the communication session with the handing over RBC and establish the communication session with the Accepting RBC. The train will then consider the Accepting RBC as the supervising RBC as per clause §5.15.3.2.6.1, in v3.4.0 of SUBSET-026, while this RBC may not have taken over the responsibility (see clause §5.15.3.2.6.2 in v3.4.0 of SUBSET-026). After session establishment to ACC RBC the HOV RBC has no possibility to stop the train (e.g. in case of route revocation in the area of HOV RBC).



1.
Handover enganged
(RTA from RBC).

Only one mobile working.
MA into ACC area onboard.

2.
session order:
- establish to approaching (ACC) RBC

With solution of CR 894 (B3, changed exception ch. 3.5.3.5.2) the train will:
- terminate existing comm sess (to HOV RBC)
- establish new comm sess (to ACC RBC)

Train did not yet pass the border.
MA onboard remains valid.

According engaged RBC handover context, the train will only accept information from HOV RBC.

According 3.16.3.4.1.2 the contact-timeout would still relate to „the latest consistent message from the Handing over RBC“ ➔ Contact-Reaction after Timeout.

Proposed mitigation

The trackside application project shall mitigate or avoid creating this hazard. It has several ways of doing so, for example:

- by confirming that the situation will not occur in this specific application, or
- trackside engineering (balise installation).

Mitigation allocated to

TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	N	Y	N *)
	B3MR1, X=1	N	Y	N *)
	B3MR1, X=2	n/a	Y	N *)
	B3R2, X=1	N	Y	N *)
	B3R2, X=2	n/a	Y	N *)

*) For baselines 3, the introduction of §3.15.1.3.7, §3.15.1.3.8, §3.15.1.3.8.1, §3.18.4.3.1 and §3.18.4.3.1.1 in SUBSET-026 v3.6.0 by CR 933 closes the hazardous situation

4.71 ETCS-H0071

4.71.1.1 Intentionally left empty. No action by application projects is required.

4.72 ETCS-H0072

<table>
<tr><td>Hazard ID</td><td>ETCS-H0072</td></tr>
<tr><td>Hazard headline</td><td>Train running in L0/LSTM without validated train data ERTMS/ETCS On-Board due to SH movements in L1 or L2.</td></tr>
<tr><td>Hazard description</td><td>According to §4.4.8.2.1 of SUBSET-026 v2.3.0, an ERTMS/ETCS On-Board equipment can be in Shunting mode in level 0, 1, 2 and 3. Once in SH mode train data, according to §4.10 of SUBSET-026 v2.3.0, are deleted. If a B2 ERTMS/ETCS On-Board, in level 1 or 2, does the transition to TR mode while moving in SH mode (according to [49], [52] and [65] transition table 4.6.2 of SUBSET-026 v2.3.0) train data remains in the “D” state but the ERTMS/ETCS On-Board is now able to manage level transitions (see “Active Functions Table” in §4.5.2 and “Acceptance of received information” in §4.8.3 and §4.8.4 of SUBSET-026 v2.3.0). If after transition to TR mode, the ERTMS/ETCS On-Board receives a level transition order to level 0/STM being in TR mode, the level transition takes place and the ERTMS/ETCS On-Board, once at standstill and after driver acknowledge, would be in UN/SN with no validated Train Data (instead of being back in SH mode).
The train will be then able to move potentially without all necessary protection by the ERTMS/ETCS On-Board.
In B3MR1 and B3R2 this hazardous situation is not applicable because according to transition [62] and [63] transition to UN and SN from TR are possible only if valid train data are stored on ERTMS/ETCS On-Board.</td></tr>
<tr><td>Proposed mitigation</td><td>Each Trackside specific application safety analysis shall take into account that a B2 ERTMS/ETCS On-Board might be able to run without validated train data stored ERTMS/ETCS On-Board, if a level transition border to Level 0/STM is placed close to a shunting area.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td>ERTMS/ETCS On-Board</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N *)</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N *)</td><td>N</td></tr>
</table>
*) For baselines 3, the changes introduced to §4.6.2/§4.6.3 of SUBSET-026 by CR 548 and SUBSET-026 v3.6.0 close the hazardous situation
</td></tr>
</table>

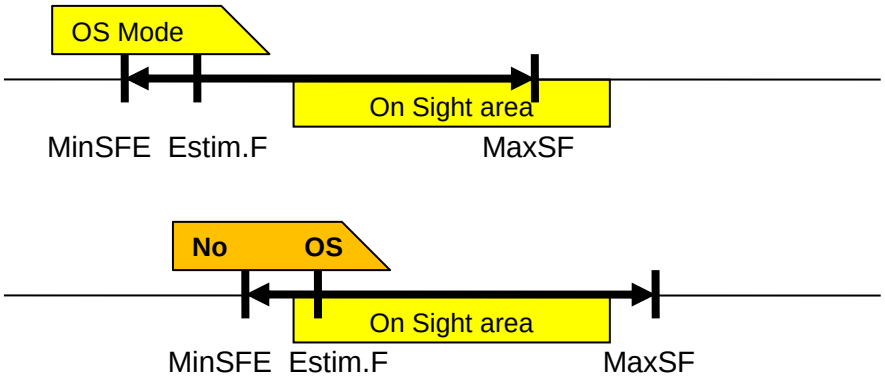
4.73 ETCS-H0073

Hazard ID	ETCS-H0073
Hazard headline	Ambiguity about application of A3.4 in case a B3 ERTMS/ETCS on-board accepts a CES with stop location between EOA and SvL
Hazard description	1.-In case the ERTMS/ETCS On-Board considers that A.3.4.1.2 a) applies for any accepted emergency stop message, independently on whether the EOA/SvL is updated or not, the ERTMS/ETCS On-Board behaviour may fall in a grey area: A.3.4 tells the ERTMS/ETCS On-Board to delete a series of information in advance of the CES location, including the MA, while 3.10.2.2 tells the ERTMS/ETCS On-Board not to touch the SvL. Appendix A3.4 is ambiguous about the conditions leading to the deletion of information stored on board in case the ERTMS/ETCS On-Board receives a CES. In fact, according to A3.4.1.2, the situation acting on the "status" of stored information for CES is the "execution" of a conditional emergency stop (item a of A3.4.1.2 of SUBSET 026 for v2.3.0, v3.4.0 and v3.6.0). In all Baselines, item a) of A3.4.1.2 refers only to section §3.10.2. The term "execution" is however undefined: According to second item of clause §3.10.2.2 of SUBSET-026, v3.6.0, when the CES is received if *"the train has not yet passed with its min safe front end the new stop location, the emergency stop message shall be accepted, however this location shall be used by the onboard to define a new EOA/SvL only if not beyond the current EOA/LOA. Refer to appendix A.3.4 for the exhaustive list of location based information stored on-board, which shall be deleted accordingly."* Note that second item of §3.10.2.2 differs between SUBSET-026 v3.4.0 and v3.6.0 only for some editorial changes (see CR 1283) so it is not reported in this problem description. According to Note [1] of A.3.4.1.3 of SUBSET-026 v340 and v3.6.0, the condition leading to deletion of stored information in case the CES is "executed" is given as: *"[1]: beyond the new SvL or in case of situation a, beyond the stop location of the accepted CES"* According to second item of clause §3.10.2.1.2 of SUBSET-026 v2.3.0, when the CES is received if *"the train has not yet passed with its min safe front end the new stop location, the emergency stop message shall be accepted, however this location shall be used by the onboard to define the new EoA and SvL only if not beyond the current EoA."* According to Note [1] of A.3.4.1.3 of SUBSET-026 v2.3.0, the condition leading to deletion of stored information in case the CES is "executed" is given as: *"[1]: beyond the new stop location"* Note that §3.10.2.1.2 of SUBSET-026 v2.3.0 uses the same terms to describe the stop location defined in the CES So, in all baselines section §3.10.2 and the note [1] of §A.3.4.1.3 do not clarify what is the meaning of "execution" and it is possible that an ERTMS/ETCS On-Board supplier considers that item a) of A.3.4.1.2 applies for any accepted emergency stop message, independently on whether the EOA/SvL is updated or the LoA is changed to an EoA/SvL or not. As result, the ERTMS/ETCS On-Board might accept the CES without changing the EoA/SvL or LoA

	but deleting information stored on-board according to table A.3.4 beyond the CES stop location. 1a-If the CES stop location is beyond the current EOA. The RBC has no knowledge that such information could have been deleted by the ERTMS/ETCS On-Board. As a consequence, once the CES is revoked, the RBC might not send once again trackside information being confident that these pieces of information are still stored on-board. The lack of these pieces of information could be hazardous: for example, the ERTMS/ETCS On-Board has deleted not yet applicable national values and will keep applying the ones stored that will become unsuitable. 1b If the CES stop location is beyond the current LoA: -The train may delete relevant trackside information for building the MRSP beyond the CES stop location, in such a way that the train may not brake to the safe target - Additionally, as the RBC has no knowledge that information has been deleted from CES stop location, it might extend the MA without including again all the trackside information from the CES stop location. Note: The deletion of track description due to the acceptance of a CES stop location is not reported to the RBC (See SRS v.3.4.0 and v.3.6.0, 3.8.2.7.3) 2. In case the ERTMS/ETCS On-Board considers that A.3.4.1.2 a) does not apply for any accepted emergency stop message: 2a In case an emergency stop message whose stop location is beyond the current EoA is accepted, the ERTMS/ETCS On-Board might keep irrelevant trackside information (e.g. not yet applicable NVs, level transition announcement) stored, which will not be replaced/cancelled after the CES is revoked because the Trackside expects the A.3.4 to be applied (i.e. irrelevant trackside information to be deleted). 2b. In case an emergency stop message whose stop location is beyond the current LoA is accepted, the ERTMS/ETCS On-Board might keep irrelevant trackside information (e.g. not yet applicable NVs, level transition announcement) stored, which will not be replaced/cancelled after the CES is revoked because the Trackside expects the A.3.4 to be applied (i.e. irrelevant trackside information to be deleted). 3. In case an emergency stop message whose stop location is between the EOA & SvL is accepted, the ERTMS/ETCS on-board might keep the SvL untouched because it does not consider that A.3.4 a) applies or because it considers that the 1st sentence of SRS clause 3.10.2.2 2nd bullet prevails on A.3.4 exception [1] even if it applies the A.3.4 a), while the Trackside expects the SvL to be moved back to the CES stop location.
Proposed mitigation	The trackside should not send a CES with a stop location beyond the LOA or between the EOA & the SvL from the last sent MA. Note: In case the last sent MA gets lost or not accepted, there is a residual risk, that the stop location of the CES may be located beyond the LOA or between the EOA & the SvL from a previously accepted MA. If CES beyond the SvL from the last sent MA are used, the first MA following the CES revocation should be sent together with track description and all other relevant trackside information covering at least the full length of the MA. Additionally, the trackside should ensure that the ERTMS/ETCS On-Board will not use obsolete information (i.e. information that has been previously received and is no longer valid) which is not part of the track description (e.g. not yet applicable NVs, level transition announcement) by replacing/cancelling it.

<table>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.74 ETCS-H0074

Hazard ID	ETCS-H0074
Hazard headline	Train inside OS/LS/SH area does not activate OS/LS/SH mode
Hazard description	According SUBSET-026 both for v3.4.0 and v3.6.0 the ERTMS/ETCS On-Board does only switch to OS/LS/SH mode in case its **max safe front end** is inside the OS/LS/SH area. While granting a movement authority to a train that includes an OS/LS/SH area, the RBC may expect that the ERTMS/ETCS On-Board switches to OS/LS/SH mode in case the **real front end** is inside the OS/LS/SH area. This can lead to hazardous situations in the case that an MA is sent to the ERTMS/ETCS On-Board including an OS/LS/SH mode profile but the ERTMS/ETCS On-Board does not switch to OS/LS/SH. Example given for On-Sight area: In case the max safe front end is located beyond this OS mode profile, the ERTMS/ETCS On-Board will not switch to OS but to FS mode. Driver is not aware of taking responsibility for OS mission; OS mission profile is not considered for speed supervision. SUBSET-026 for both v3.4.0 and v3.6.0 Analysis: • OS from FS or SR: SUBSET-026 v3.4.0 and v3.6.0, §4.6.3 condition 40 • OS from modes different from SB and PT modes: SUBSET-026 v3.4.0 and v3.6.0, §5.9.2.2 • Flowchart SUBSET-026 v3.4.0 and v3.6.0, §5.9.7 ends at the evaluation of the condition “Beginning of OS area” because neither “Max safe front inside OS area” nor “further location” is fulfilled • OS from SB or PT: SUBSET-026 v3.4.0 and v3.6.0, §5.9.5.1 Trackside cannot guarantee that the OS mode profile will be activated on the ERTMS/ETCS On-Board in case the real front end of the train is located inside the On Sight area:  Note regarding Baseline 2: The UNISIG references used in this hazard report are related to SUBSET-026 v3.4.0 and v3.6.0 but the problem is also relevant for version 2.3.0.
Proposed mitigation	Each trackside specific application shall take into account the possibility that an ERTMS/ETCS On-Board will not perform the immediate mode transition to OS/SH/LS if the

<table>
<tr><td></td><td>mode profile area is inside the confidence interval calculated ERTMS/ETCS On-Board (e.g.: by implementing additional balises, announced in linking in order to reduce the confidence interval, or by having larger mode profile area).</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.75 ETCS-H0075

Hazard ID	ETCS-H0075
Hazard headline	No specific driver indication in case of "RAMS related linking reaction" for an ERTMS/ETCS On-Board
Hazard description	Clauses §3.16.2.7.1.1 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.1 of SUBSET-026 v2.3.0 ensure the safety target for the balise transmission function elaborated in SUBSET-088, version 2.3.0, 3.5.4 and 3.6.0, by applying a safe reaction in case of two consecutive balise groups, announced by means of linking, are missed. According to clause §3.16.2.7.1.1 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.1 of SUBSET-026 v2.3.0 when 2 consecutive linked balise groups announced by linking are not detected the ERTMS/ETCS On-Board shall apply service brake until the train reaches standstill, shorten location based information stored On-board to the current position once at standstill and inform the driver of the specific event. For a B2 ERTMS/ETCS On-Board, it is project specific implementation to select what kind of message the ERTMS/ETCS On-Board has to display on DMI in this situation since no specific requirement is given on the text message that shall be displayed On the contrary for a B3 ERTMS/ETCS On-Board, table 68 of ERA_ERTMS_015560 (both v3.4.0 and v3.6.0) imposes to use a more generic message for all types of balise group reading errors. In this way the possibility for mitigations originally found to cover the hazard detected in SUBSET-088 (version 2.3.0, 3.5.4 and 3.6.0) and originally included in OB03 of SUBSET-091 is reduced. When a B3 ERTMS/ETCS On-Board applies the RAMS related supervision function due to a fault in the balise reception channel, neither the driver nor the signaller is able to determine that the cause of the display of the message is not a trackside problem. When the On-board applies the RAMS related supervision function, the driver shall follow the operational rules as specified in the TSI OPE annex A rule 6.45. The driver shall inform the signaller about the situation. If no new MA is received when the train has come to a standstill, the signaller shall authorize the driver to pass the EOA. To resume a mission in SR mode with a written order from the signaller is not perceived as hazardous.(It is understood that the written order will include all relevant information that could have been missed or will be missed due to a fault in the balise reception channel). If a new MA has been received, the TSI OPE annex A rule 6.45 sub-part (“If the situation is repeated driver and signaller shall apply non-harmonised rules”) applies in case the RAMS related supervision reaction occurs again. The only residual risk is encountering an unlinked BG with TSR information or with a safety relevant fixed text message to be enforced before the RAMS related supervision function occurs again.
Proposed mitigation	In a level 2/3 area or in a level 1 area fitted with RIUs or loops providing infill MAs, TSR information and safety relevant fixed text messages should not be sent by unlinked balise groups. Alternative mitigation on an X=2 RBC: - Following the reception of an M_ERROR = 7, the X=2 RBC should not send a new MA, an RBC transition order, an order to establish a communication session with another RBC or a level transition order to level 0 or NTC to the ERTMS/ETCS On-Board equipment until it is ensured that the On-board is able to read balises e.g. after having received a position report with a new LRBG. AND

	- The trackside should not give an MA to a train that has reported to be in SR mode with an LRBG not set to unknown and located in an adjacent RBC area, until it is ensured that the on-board is able to read balises e.g. by receiving a position report with a new LRBG. Assumption: An SR authorisation is always operationally accompanied by a written order which includes all the relevant information to operate safely. In case this assumption is not fulfilled then the same mitigation as for the MA should be applied to the SR authorisation. Note regarding the two mitigation measures: • The intermittent failure of the balise reception channel which would lead to receive again information from balise (e.g. an MA) after the ERTMS/ETCS On-Board equipment has applied §3.16.2.7.1.1 of SUBSET-026 (both for v3.4.0 and v3.6.0) or §3.16.2.7.1 of SUBSET-026 v2.3.0 is not considered in these mitigations measures. A residual risk exists in case the ERTMS/ETCS On-Board equipment, due to the intermittent failure, would be able to read an MA, an RBC transition order, an order to establish a communication session with another RBC or a level transition order to level 0 or NTC provided by a balise. Notes regarding the alternative mitigation measure for an X=2 RBC: • This mitigation measure relies on the reception by the RBC of the position report containing M_ERROR = 7 and therefore leaves a residual risk in case this message is not received e.g. due to a temporary loss of the safe radio connection. • In case the On-board reaction as per Subset-026 clause 3.16.2.7.1.1 occurs while the On-board is performing an RBC/RBC handover between two X=2 RBCs and the On-board is able to handle only one communication session, the On-board could already have stored the RBC ID/phone number of the Accepting RBC as the current valid RBC ID/phone number when it reaches standstill. The on-board could subsequently establish a communication session with the (former) Accepting RBC e.g. to report a mode change as per clause 3.5.3.4 c) of Subset-026. Since this RBC has not been informed that the On-board has reported M_ERROR = 7, it could give to the On-board an information “precluded” by this mitigation (MA, RBC transition order, order to establish a communication session with another RBC or level transition order to level 0 or NTC). The following case should also be considered: once the train has reached standstill, the desk is closed. When the desk will be reopen, the On-board could call the (former) Accepting RBC. • On a mixed (level 2/3 + level 0) or (level 2/3 + level NTC) area, when the train has reached standstill after the RAMS related supervision reaction, the driver could after having performed the override select level 0 or NTC in the table of supported levels or in the default list of levels. An operational mitigation to this case should be defined.
Mitigation allocated to	EXTERNAL

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y*	Y	Y
	B3MR1, X=1	Y*	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y*	Y	Y
	B3R2, X=2	n/a	Y	Y

* Only if the information displayed by the B2 ERTMS/ETCS On-Board does not explicitly alert the driver that the service brake application is due to a failure of the balise detection function. The DMI specification version 2.3 defines that the “Balise read error” text message will be displayed for such a reaction (see table 50 in this specification) but this specification is only informative.

4.76 ETCS-H0076

<table>
<tr><td>Hazard ID</td><td>ETCS-H0076</td></tr>
<tr><td>Hazard headline</td><td>Train equipped with B2 ERTMS/ETCS On-Board entering a B3 trackside operating with system version X=2</td></tr>
<tr><td>Hazard description</td><td>A train equipped with a B2 ERTMS/ETCS On-Board will not be granted access for an ETCS equipped line operating with system version X=2, if operation in L1/2/3 is required on that line, i.e. if trains running on that line must be equipped with a B3 ERTMS/ETCS On-Board.
However, if the B3 X=2 line has borders to areas in which trains with B2 ERTMS/ETCS On-Boards are allowed to run, an (operational) error in train routing may occur and a route into the B3 X=2 area may be set for a B2 train. So two possible scenarios are detected:
- the border between the B3 X=2 equipped trackside and the other areas are managed through a level transition
- the border between the B3 X=2 equipped trackside and the other areas are managed through an HO.

If the border between the B3 X=2 equipped trackside and the other areas are managed through a level transition, if the border BG of the B3 X=2 area uses system version X=2 this will trip any B2 train approaching in L1/2/3 supervision. But a B2 ERTMS/ETCS On-Board approaching in L0/STM will ignore the BG with system version X=2 including the border Balise Group, therefore not performing a level transition. In case the B3 X=2 line is not equipped for L0/STM operation this could result in serious hazards.
It can be assumed that a B2 train cannot obtain an MA for the B3 X=2 area in the scenario above: if the B3 area is L1, then the BGs transmitting MA’s within the B3 area will use system version X=2. If the B3 area is L2 or L3, the B2 ERTMS/ETCS On-Board cannot establish a session with the B3 X=2 RBC because of incompatible versions.

If both the B3 X=1 area and the B3 X=2 area are equipped with L2 there will be an RBC Handover taking place at the border. The HOV RBC (X=1) will issue an MA for crossing the border to the B2 train, based on information received from the ACC RBC (X=2). Because the B2 ERTMS/ETCS On-Board cannot establish a session with the ACC RBC the ACC RBC has no means to revoke the MA after the train has passed the border. Once the train, has passed the border the ERTMS/ETCS On-Board will continue to accept information from the HOV RBC because it cannot send a position report to the Acc RBC (§3.15.1.3.2 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0), but the HOV RBC will terminate the session according to §3.15.1.2.7 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0. The B2 ERTMS/ETCS On-Board, then, can only run for the duration of T_NVCONTACT. Moreover BG with X=2 are placed after the border BG and they are going to trip a B2 ERTMS/ETCS On-Board and driver will see “Trackside not compatible”. This scenario doesn’t lead to any hazard situation.</td></tr>
<tr><td>Proposed mitigation</td><td>In order to create a safe implementation, a B3 X=2 trackside engineering should take into account of the possibility of a B2 ERTMS/ETCS On-Board, running in L0/LSTM level, to be unduly routed on a B3 X=2 line and find adequate mitigations in order to avoid such trains to run with limited or no supervision at all.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>Y</td><td>N</td><td>N</td></tr>
</table>
</td></tr>
</table>

4.77 ETCS-H0077

<table>
<tr><td>Hazard ID</td><td>ETCS-H0077</td></tr>
<tr><td>Hazard headline</td><td>Outdated Data (e.g. train speed) in Position Report (Packet 0 or 1)</td></tr>
<tr><td>Hazard description</td><td>According to SUBSET-026 v3.4.0 and v2.3.0, §7.4.3.1, the Position Report (Packet 0) contains the following data, in addition to the positioning information provided by Q_SCALE, NID_LRBG, D_LRBG, Q_DIRLRBG, Q_DLRBG, L_DOUBTOVER, L_DOUBTUNDER and, in case of Packet 1 also NID_PRVLRBG:
<table>
<tr><td>Q_LENGTH</td><td>2</td><td></td></tr>
<tr><td>L_TRAININT</td><td>15</td><td>If Q_LENGTH = “Train integrity confirmed by integrity monitoring device” or “Train integrity confirmed by driver”</td></tr>
<tr><td>V_TRAIN</td><td>7</td><td></td></tr>
<tr><td>Q_DIRTRAIN</td><td>2</td><td></td></tr>
<tr><td>M_MODE</td><td>4</td><td></td></tr>
<tr><td>M_LEVEL</td><td>3</td><td></td></tr>
<tr><td>NID_NTC</td><td>8</td><td>If M_LEVEL = NTC</td></tr>
</table>
Clause §5.3.1.3 in SUBSET-041 v2.1.0 and v3.1.0 gives a performance requirement of 1s regarding the location information, but according to SUBSET-041 v2.1.0 and v3.1.0 §5.3.1.1 this requirement only applies to the data that relate to the train front end (i.e. D_LRBG, Q_DIRLRBG, Q_DLRBG, L_DOUBTOVER and L_DOUBTUNDER)
• Q_LENGTH, L_TRAININT:
The train is required to report the real Q_LENGTH and L_TRAININT only in case if the events defined in SUBSET-026 v3.4.0 and v2.3.0, §3.6.5.1.4, i.e. in case the driver confirms the train integrity or in case of a detected loss of train integrity. There is no requirement about the age of the reported train length.
→ in worst case a train can legally report a train length which it once had some time, even hours, before. → Assumed not critical
• V_TRAIN:
The only event that requires the train to update the speed information in the position report is defined in SUBSET-026 v3.4.0 and v2.3.0, §3.6.5.1.4 a) “The train reaches standstill […]” (Note: standstill itself is not harmonized). There is no requirement about the age of the speed information sent with the position report.
→ in worst case a train can legally report a permanent V_TRAIN = 0, independent from its real estimated speed.
• Q_DIRTRAIN:
The running direction of the train is not required to determine the position of the train’s front end. Therefore the performance requirement regarding positioning information (SUBSET-041 v2.1.0 and v3.1.0 §5.3.1.3) is not to be applied. As result, there is no requirement to report a changed running direction to the RBC.
→ A train can legally report an outdated running direction to the RBC.
• M_MODE, M_LEVEL:
for these two variable please refer to ETCS-H0029.

Different readings of SUBSET-041 v2.1.0 and v3.1.0 §5.3.1.3 may lead to hazardous situations (example: based on train speed V_TRAIN).
On the one hand this requirement can be understood as only applying to the “position” of the train. On the other hand this requirement can be understood as also applying to the reported</td></tr>
</table>

<table>
<tr><td></td><td>speed, because it would be impossible for an ERTMS/ETCS On-Board to determine its position within the requested performance but without knowing the speed similarly.
Based on the second reading a trackside may use for example the reported train speed for safety critical functions, e.g. route unlocking, occupation/track free handling or level crossing management. In case an ERTMS/ETCS On-Board reports outdated speed information according to the first reading, the train may be moving faster than reported to trackside while trackside performs safety critical functions based on the (outdated) reported train speed.</td></tr>
<tr><td>Proposed mitigation</td><td>Each trackside specific application safety analysis shall analyse the scenarios given in this hazard report and take appropriate measures, if necessary. Regarding V_TRAIN, Infrastructure manager shall take into account that some ERTMS/ETCS On-Boards could report this information inconsistent with other data in the position report.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL / TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>N</td></tr>
</table>
</td></tr>
</table>

4.78 ETCS-H0078

Hazard ID	ETCS-H0078
Hazard headline	Inhibition of revocable TSRs from balises in L2/3 in SR mode
Hazard description	In SUBSET-026 (both for v3.4.0 and v3.6.0) a possible ambiguity related to the management of the “inhibition of revocable TSRs from balises in L2/3” by RBC has been detected. In SB mode and SR mode the management of “inhibition of Revocable TSRs from balises in L2/3” is not active (see table §4.5.2): the function is only active in FS, LS, OS, TR and PT. But, according to the table §4.8.4 of SUBSET-026 (both for v3.4.0 and v3.6.0) information is accepted in all modes except if the ERTMS/ETCS on-board is in PS/SH/SL/NL/ RV modes. Moreover information is deleted both if the ERTMS/ETCS on-board enters in levels 0/ or STM or if the following modes are reached: NP/SB/SH/PS/SR/SL/NL/UN/SN/RV. Based on the new functionality, Temporary Speed Restrictions coming from balise groups are filtered based on level and modes according to condition A[8]: *(“[8] exception: revocable TSRs shall be rejected if information “inhibition of revocable TSRs from balises in L2/3” is stored on-board.”)* According to exception [8] the event leading to the rejection of packet 65 coming from balises is a packet 64 received and accepted by the ERTMS/ECTS on-board. The ambiguity in SB mode doesn’t lead to any hazardous situation because it is clear from the specification that, if RBC should send packet 64 to the ERTMS/ETCS on-board during Start of Mission procedure, this piece of information shall be deleted at the transition to SR mode (see table in §4.10 of SUBSET-026 both for v3.4.0 and v3.6.0). So, if RBC should send packet 64 to an ERTMS/ETCS On-Board in SR mode, 2 different ERTMS/ETCS on-boards could apply different reactions. One ERTMS/ETCS on-board would consider that the function is not active according to §4.5.2 so TSRs coming from balises will not be filtered. Another ERTMS/ETCS on-board might apply the filtering conditions given in §4.8.3 and rejects TSRs coming from balise groups, considering that (according to exception [8], the packet 64 is stored by the ERTMS/ETCS on-board) a “inhibition of revocable TSRs from balises in L2/3” has been received and accepted. If RBC should rely on the fact that the function is not active in SR mode, there might be a safety issue because an ERTMS/ETCS on-board might be able to supervise a less restrictive speed.
Proposed mitigation	A trackside should always send packet 64 "Inhibition of revocable TSRs from balises in L2/3" in an MA message. This mitigation however does not cover the scenario where the train data changes before the MA is received and so the acknowledgement has not been received yet. In this case, the MA is rejected while the TSR inhibition is accepted. Each trackside specific application safety analysis has to take into account this residual risk.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	N	n/a	n/a
	B3MR1, X=1	N	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	N	Y	Y
	B3R2, X=2	n/a	Y	Y

4.79 ETCS-H0079

Hazard ID	ETCS-H0079
Hazard headline	Wrong assumption in ERTMS/ETCS On-Board calculation of release speed
Hazard description	The ERTMS/ETCS On-Board calculation of release speed should ensure that the brakes are commanded in due time so as to stop a train running at that speed in rear of the supervised location. This can be ensured if the intervention will occur at the same time the min safe front end (or min safe antenna in L1) passes the EoA. However, according to SUBSET-026 v3.6.0, §A.3.5.2, the intervention arising from passing the EoA will not occur at that time if a balise group message is received in the vicinity of the EoA. Intervention will be delayed until the BG message is processed. In SUBSET-026 v3.6.0, §3.11.11.4, 8th bullet a processing delay as defined in SUBSET-041 §5.2.1.1, is taken into account when the ERTMS/ETCS On-Board shall calculate a speed restriction to ensure permitted braking distance. It is not clear, why §5.2.1.13 of SUBSET-041 v2.1.0, v3.1.0 and v3.2.0 is not also referred to. In case the B2 ERTMS/ETCS On-Board implements a proprietary braking curve model, although the SUBSET-026 v2.3.0 clause 3.13.8.1.1 leaves room to an interpretation like e.g. the CR977 solution (followed up by CR1300) consisting in delaying the EB application, SUBSET-026 v2.3.0 clause 3.13.7.2.2 1st bullet does not allow to deduce that this delay to trip in level 1 has to be taken into account for the ERTMS/ETCS On-Board calculation of the release speed. In case the early implementation of braking curves functionality is implemented (current version 5.0 or any earlier one) the SRS chapter 3.13 is replaced as a whole. Neither any delay induced by the SRS 2.3.0 clause 3.13.8.1.1 nor the 1s delay after passing the EOA induced from the CR977 (followed up by CR1300) does exist and consequently the release speed formula is correct.
Proposed mitigation	If the overall risk of a train overpassing the SvL is not acceptable, the trackside should take appropriate measures to compensate the wrong calculation of the ERTMS/ETCS On-Board release speed. One possibility is to move the EOA and SvL upstream from the actual location to protect. Another possibility, for an X=2 trackside, would be to use the permitted braking distance information as follows: • If there is only a DP, i.e. there is no overlap, the permitted braking distance should be equal to the distance between the EOA and the DP; • If there is only an overlap, i.e. there is no DP, the permitted braking distance should be equal to the distance between the EOA and the end of the overlap; • If there is both a DP and an overlap, the permitted braking distance should be the equal to the distance between the EOA and the DP. Note: If the train comes to standstill after the Overlap timer has been started, the overlap will be revoked, so it would be unsafe to use the distance from the EOA to the end of overlap as permitted braking distance. The distance between the EOA and the DP will have to be used instead; but it means that it will not be possible to achieve a higher release speed than the release speed for the DP even while the overlap is still valid. In all cases, the permitted braking distance information should specify that: • The permitted braking distance has to be achieved with the emergency brake; • The start location of the speed restriction to ensure permitted braking distance is the EOA location; • The length of this speed restriction is equal to the permitted braking distance.
Mitigation allocated to	TRACKSIDE and EXTERNAL

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
*) n/a in case the early implementation of braking curves functionality is implemented
</td></tr>
</table>

4.80 ETCS-H0080

4.80.1.1 Intentionally left empty. No action by application projects is required.

4.81 ETCS-H0081

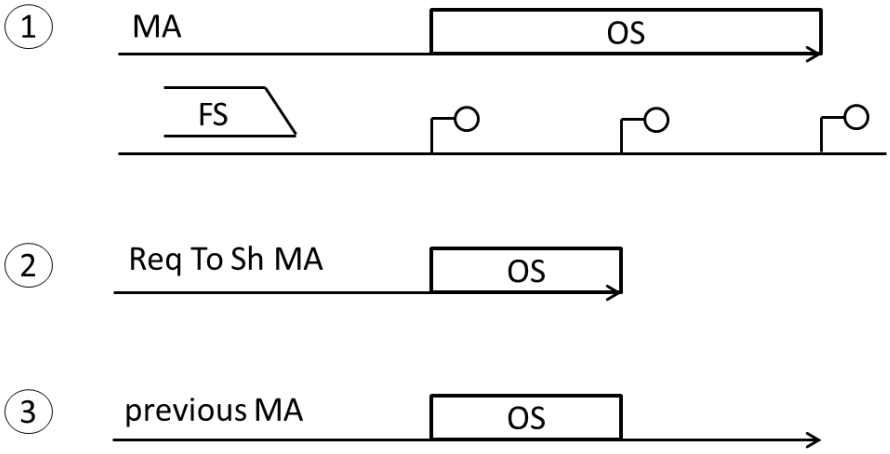
Hazard ID	ETCS-H0081
Hazard headline	Infill information considered before crossing of main BG
Hazard description	There are several problematic situations: 1. According to SRS 4.8.3 "Accepted Information depending on the level and transmission media", some infill information from the list provided in SUBSET-040 clause 4.2.4.5.1 is accepted immediately by the ERTMS/ETCS On-Board while the infill location reference information itself is either rejected (Level 0/NTC) or stored in the transition buffer in case of level 1 announcement (Level 2/3). By definition, the infill location reference provides the reference for all location infill information. Due to the rejection of this reference, the current LRBG (i.e. the infill BG) would be used as location reference of the infill information. This can lead to safety issues (or operational impact) regarding the following infill information: a) packet 41: Level transition order; b) packet 65: TSR; c) packet 67: Track condition big metal masses; d) packet 88: Level Crossing information (Note: this packet does not exist in B2). For instance, since a Big Metal Mass (BMM) area would be wrongly located, i.e. this area would start and end too early compared to the real BMM area, the ERTMS/ETCS On-Board would ignore balise transmission alarms due to a real failure because it erroneously considers that they happen in a BMM area. This could lead to an ERTMS/ETCS On-Board running with a balise receiver in failure without ERTMS/ETCS On-Board reaction and therefore miss balise groups containing restrictive information. 2. According to SRS 4.8.3 "Accepted Information depending on the level and transmission media", some infill information from the list provided in SUBSET-040 clause 4.2.4.5.1 is stored in the buffer while the infill location reference information itself is rejected (Level 0/NTC). Due to the rejection of this reference, the current LRBG (e.g. the infill BG) would be used as location reference of the infill information released from the transition buffer when the level transition will be executed. This can lead to safety issues (or operational impact) regarding the following infill information: a) packet 5: Linking; b) packet 12: Level 1 Movement Authority; c) packet 21: Gradient Profile; d) packet 27: International Static Speed Profile; e) packet 39 or 239: Track Condition Change of traction system; f) packet 40: Track Condition Change of allowed current consumption (Note: this packet does not exist in B2); g) packet 51: Axle Load Speed Profile; h) packet 52: Permitted Braking Distance Information (Note: this packet does not exist in B2); i) packet 65: Temporary Speed Restriction j) packet 68 or 206: Track Condition; k) packet 69: Track Condition Station Platforms (Note: this packet does not exist in B2);

	l) packet 70 or 207: Route Suitability Data; m) packet 71: Adhesion factor; n) packet 80: Mode Profile; o) packet 88: Level Crossing information (Note: this packet does not exist in B2) p) packet 138: Reversing area information; For instance, since an International Static Speed Profile (ISSP) would be wrongly located when released from the transition buffer, i.e. this ISSP would start at the current LRBG (e.g. the infill BG), the ERTMS/ETCS On-Board would apply speed supervision value inappropriate to the current train location. This would typically lead to supervising a too permissive value. 3. The handling of a TSR revocation (packet 66) received as infill information is unclear. According to SRS 4.8.3 "Accepted Information depending on the level and transmission media", this information is accepted immediately (except in level NTC). If applied immediately by the ERTMS/ETCS On-Board, the revocation will apply to a complete TSR which would start before the main BG and end after this BG. By providing this revocation as infill information, the trackside may expect this revocation to take place only from the main BG location. In such a case, revoking the whole TSR would impact the safety. 4. Data to be used by an STM (packet 44 with NID_XUSER = 102) received as infill information could also lead to a safety issue. In case such a packet is received from the airgap and considered as non-infill by a B3 on-board due to the rejection or storage of the infill location reference information, the clause 10.11.1.2 of SUBSET-035 v3.1.0 and v3.2.0 specifies that “The STM Control Function shall add to the transmitted airgap data the odometer reading of the balise group which transmitted the airgap message” and the clause 10.11.1.3 of SUBSET-035 v3.1.0 and v3.2.0 specifies that “The odometer reading shall correspond to the estimated odometer value of the location reference of the balise group”. In case such a packet is received from the airgap by a B2 on-board, the clause 5.2.13.3 of SUBSET-035 v2.1.1 specifies that “If data to be forwarded to an STM are received by the ETCS On-board then the STM Control Function shall add an odometer reading of the LRBG to the transmitted data” and the clause 5.2.13.4 of SUBSET-035 v2.1.1 specifies that “The odometer reading shall correspond to the location of the LRBG using the FFFIS STM odometer function as common reference (nominal odometer value)”. It is therefore uncertain whether the STM will be able to interpret the received information correctly. Depending on the content of the information forwarded to the STM, the safety can be impacted. Note: since it is possible to engineer a packet 44 with NID_XUSER = 102 in B2 or in B3 X=1, the hazard can also occur although the forwarding by the ERTMS/ETCS on-board is considered as a national function due to the absence of National System identity in the packet 44 header.

<table>
<tr><td>Proposed mitigation</td><td>
Common recommendations for all level areas:
– packet 66 should not be implemented after packet 136
– packet 44 should not be implemented after packet 136 if NID_XUSER=102
Additional recommendations for specific levels.
In level 0 areas:
– packets 41, 65 and 67 should not be implemented after packet 136
– packets 88 should not be implemented after packet 136 if level 1 or level 2/3 is announced
– packet 5 should not be implemented after packet 136 if level 1 is announced
– packets 12, 21, 27, 39, 40, 51, 52, 68, 69, 70, 71, 80, 138, 206, 207 and 239 should not be implemented after packet 136 if level 1 is announced (*)
In level NTC areas:
– packets 41 and 67 should not be implemented after packet 136
– packets 65 and 88 should not be implemented after packet 136 if level 1 or level 2/3 is announced
– packet 5 should not be implemented after packet 136 if level 1 is announced
– packets 12, 21, 27, 39, 40, 51, 52, 68, 69, 70, 71, 80, 138,206, 207 and 239 should not be implemented after packet 136 if level 1 is announced (*)
In level 2/3 areas:
– packets 41, 65, 67 and 88 should not be implemented after packet 136
Note: the packet 136 defines the start of the infill information in a balise telegram
(*) A linking reaction for the main balise group (i.e. referred in packet 136) where the level border is can also prevent the issues related to the transitions from level 0 and level NTC to level 1. The information that could be used with wrong location based on LRBG instead of infill location reference is only relevant when the main BG is lost. The linking reaction assures that the MA after the main BG is only valid if the BG is read because, after applying the service brake, at standstill the current MA, track description and linking information shall be shortened to the current position of the train. This alternative mitigation is only valid under the condition that the packet 5 is implemented together with the level transition announcement or in the infill balise group (Justification: it is to ensure that if the balise group containing the packet 5 is missed, the hazard will not occur) and leaves room to the following residual risk: the infill information can be used with a wrong reference location from the first location where the level transition can take place up to the end of the expectation window of the border/main balise group.
</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.82 ETCS-H0082

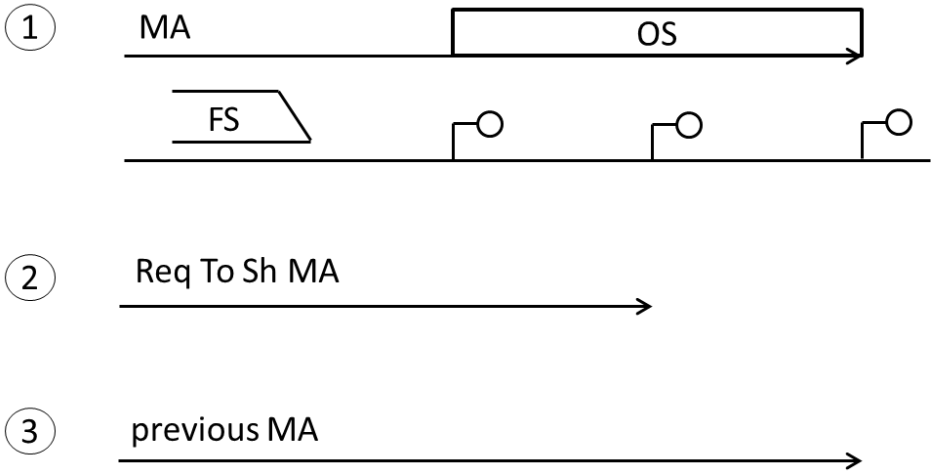
Hazard ID	ETCS-H0082
Hazard headline	Wrong mode profile (OS/LS/SH) and/or list of balises in SH supervised after reception of a Request to Shorten MA.
Hazard description	The RBC sends a request to shorten MA, which includes a proposed shorten MA with an EOA closer to the train than the current EOA/LOA, optionally with OS/LS/SH mode profile and in case of SH mode profile optionally with a list of balises for SH area. 1) According to SUBSET-026 (v2.3.0 and v3.4.0 and v3.6.0), the evaluation of the request to shorten MA in accordance with §3.8.6 is not part of the evaluation criteria defined in §4.8. This means that the check defined in §3.8.6 can only apply in a further step once the request to shorten MA has passed the §4.8 filter. Several hazardous scenarios can arise according to ERTMS/ETCS On-Board interpretation of SUBSET 026 (v2.3.0 and v3.4.0 and v3.6.0), in case the received mode profile (OS or LS or SH) and list of balises in SH are accepted in accordance with the section §4.8 filter, but the request to shorten MA itself may then be rejected in a further step when evaluated in accordance with §3.8.6, replacing the mode profile and/or list of balise for shunting of the original MA with the new accepted OS or LS or SH mode profile. - the train supervises a wrong OS mode profile or - the train supervises a wrong LS mode profile (not applicable for baseline 2) or - the train supervises a wrong SH mode profile and/or - the train supervises a wrong list of balises for SH (not applicable for baseline 2) (See Hazard ETCS-H0045 case 8) Also, a rejected request to shorten MA without any mode profile could lead to an unwanted transition to FS in case the clause 3.12.4.3 is applied by the ERTMS/ETCS On-Board before the clause 3.8.6.1 b) Example 1: 1) ERTMS/ETCS On-Board in L2/FS (or L2/OS) is supervising an MA including an OS mode profile for a further location. 2) ERTMS/ETCS On-Board receives a request to shorten MA, which includes a proposed shortened MA with an EOA closer to the train than the current EOA/LOA, with OS mode profile 3) ERTMS/ETCS On-Board rejects the proposed shortened MA as per SUBSET-026 (v2.3.0 and v3.4.0 and v3.6.0) §3.8.6.1 b, but accepts the OS mode profile. ERTMS/ETCS On-Board replaces the currently supervised mode profile with the mode profile received together with the request to shorten MA, the result would be as depicted in figure below. The resulting MA supervised by the ERTMS/ETCS On-Board does not contain anymore an OS mode profile in advance of the EOA of the rejected proposed shortened MA.



Example 2:

1) ERTMS/ETCS On-Board in L2/FS (or L2/OS) is supervising an MA including an OS mode profile for a further location.
2) ERTMS/ETCS On-Board receives a request to shorten MA, which includes a proposed shortened MA with an EOA closer to the train than the current EOA/LOA, but no OS mode profile.
3) ERTMS/ETCS On-Board rejects the proposed shortened MA as per the SUBSET-026 (v2.3.0 and v3.4.0 and v3.6.0) §3.8.6.1 b, but removes the OS mode profile from the original MA, because no OS mode profile at all was given with the request to shorten MA.

The resulting MA ERTMS/ETCS On-Board does not contain any OS mode profile.

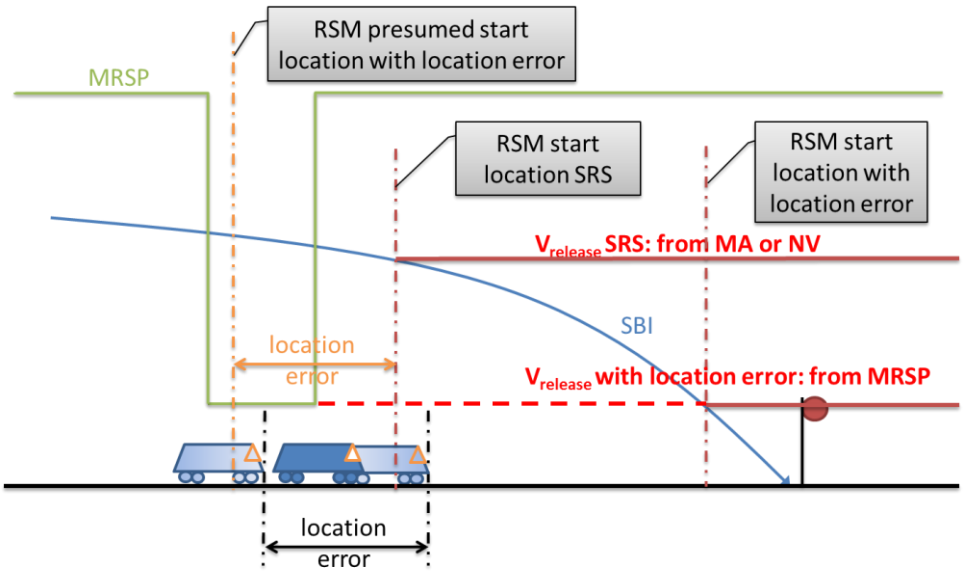


2) (only applicable for baseline 2) It is not clear if §3.12.4.3 applies to the case of Request to shorten MA. The problematic situation arises when the RBC sends to a train with a SH mode profile already stored on- board a Request to shorten MA including the proposed shortened MA with an EOA in rear of the current EOA/LOA but without mode profile. If §3.12.4.3 is not applied while the trackside expects so, the ERTMS/ETCS On-Board may keep a mode profile which has become obsolete. In case the mode profile is SH, it is considered that it can be safety relevant because the status of the trackside may not be ready for shunting movements and shunting protections.

Note: In Baseline 3, according to 3.8.6.2 the annex A3.4 always applies if the request is granted and both the stored MP and list of balises are deleted.

<table>
<tr><td>Proposed mitigation</td><td>Trackside should not send Request to Shorten MA including a mode profile (OS/LS/SH) and when the Trackside has sent an MA with a mode profile, an RBC should not send a Request to Shorten MA till a new MA is sent without mode profile.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.83 ETCS-H0083

Hazard ID	ETCS-H0083
Hazard headline	Accuracy of distances measured on-board not considered when determining Release Speed from MRSP
Hazard description	If an ERTMS/ETCS on-board does not consider the accuracy of distances when determining the release speed then, depending on the odometry error and on the SBI used for the calculation of the start location and on the speed restriction, it may lead to an ERTMS/ETCS on-board not supervising the end of the speed restriction as expected by trackside (i.e. a train could accelerate earlier than expected). SUBSET-026 v3.4.0 and v3.6.0 §3.13.9.4.9 requires to lower Release Speed value if there is a more restrictive MRSP in RSM area. However, the MRSP is sought from presumed RSM start location without considering the accuracy of distances measured on-board. The following hazardous scenarios has been identified: • Case where the SBI limit is derived from Supervised Location EBD (SBI2): It is possible that the “maximum/estimated safe front end” position is in advance of a speed restriction lower than the Release Speed value, whereas the corresponding “min safe front end” is still within this speed restriction. In this case, the supervised speed increases to the Release Speed before the speed restriction area is left • Case where the SBI limit is derived from End of Authority SBD (SBI1): Same problem as for the case above, "max safe front end" has just to be substituted by "estimated front end". The figure below illustrates the situation in which the train front end is still within a speed restriction but is only supervised against the Release Speed which has a higher value than the speed restriction. 
Proposed mitigation	If there exists some speed limitation lower than the release speed in the vicinity of the release speed monitoring area a specific safety analysis must be done. If the risk of a train accelerating too early is not acceptable, the trackside should take appropriate measures in order to avoid the overspeed. Such measures could include: • install relocation balise in the vicinity of a speed restriction lower than the release speed and whose end location is close to the start RSM location • extend the speed restriction

<table>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y *)</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y *)</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y *)</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
*) Only if Baseline 2 Requirements For Implementation Of Braking Curves Functionality are implemented
</td></tr>
</table>

4.84 ETCS-H0084

Hazard ID	ETCS-H0084
Hazard headline	Brake command revocation following to function becoming no longer active due to mode change
Hazard description	In case, due to a change of mode, a function becomes no longer active according to table 4.5.2 (SUBSET-026 v2.3.0, v3.4.0 and v3.6.0), it is not clear what happens to an on-going brake command that had been initiated when the function was active. Due to this unclearness, it may be that when the function becomes inactive the brake command is revoked. This may be hazardous under the scenarios described in the following: **Scenario 1 – Function "linking consistency" and "BG consistency when linking consistency checked**" a. Train is running with ERTMS/ETCS On-Board in FS mode (or OS, or LS) with a stored SH mode profile for a further location. The ERTMS/ETCS On-Board receives information from a BG but is unable to process it. The information in the BG was restrictive, for example a National Values packet containing more restrictive V_NVSHUNT. The brakes are activated because of function "linking consistency" or "BG consistency if linking consistency is checked" and a system status message is displayed. A transition to SH occurs and, since the functions are inactive in this mode, the brakes are released and the message disappears. b. Intentionally deleted. c. Train is running with ERTMS/ETCS On-Board in FS mode (or OS, or LS). The ERTMS/ETCS On-Board receives information from a BG but is unable to process it. The information in the BG was restrictive, for example TSR or National Values packet containing more restrictive V_NVUNFIT. The brakes are activated because of function "linking consistency" or "BG consistency if linking consistency is checked" and a system status message is displayed; in the meanwhile a level transition order is executed to L0 thus leading a mode transition to UN and the functions become inactive so that the brakes are suddenly released and the message disappears. Hazard related to scenario 1. The system status message may have been displayed very briefly and go unnoticed by the driver. Driver only witnessed a short brake application then released. The train missed restrictive info and is unbraked while the driver has no awareness of this situation. **Scenario 2– RAMS related supervision function** An additional problem can arise due to the fact that function 'RAMS related supervision function'(Subset-026 v2.3.0, v3.4.0 and v3.6.0 §3.16.2.7) is missing in 4.5.2 active function table. So it is not clear in the transition to which modes the brakes will be released. <u>2.a Balise reception degradation</u> Clauses §3.16.2.7.1 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.1 of SUBSET-026 v2.3.0 ensure the safety target for the balise transmission function elaborated in SUBSET-088 by applying a safe reaction in case of two consecutive balise groups, announced by means of linking, are missed. According to clause §3.16.2.7.1.1 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.1 of SUBSET-026 v2.3.0 when 2 consecutive linked balise groups announced by linking are not detected the ERTMS/ETCS On-Board shall apply service brake, inform the driver and once at standstill delete track description. <u>2.b Balise cross-talk</u>

<table>
<tr><td></td><td>Clauses §3.16.2.7.2 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.2 of SUBSET-026 v2.3.0 ensure the safety target for the balise transmission function elaborated in SUBSET-088 by applying a safe reaction in case a second balise group is received that satisfies the same criteria as the previously expected and already received repositioning balise group. According to clause §3.16.2.7.2.2 of SUBSET-026 (both for v3.4.0 and v3.6.0) and §3.16.2.7.2 of SUBSET-026 v2.3.0 the ERTMS/ETCS On-Board shall apply service brake, inform the driver and once at standstill delete track description.
If during service brake application RAMS related supervision function (2.a or 2.b) a change of mode occurs and the function becomes no longer active, safety reaction related to failure of balise reception capability may have been issued very briefly and go completely unnoticed by the driver. Driver may only witness a short brake application then released so being unaware of the fault to balise reception channel. In this situation the mitigations found to cover the hazards detected in SUBSET-088 (version 2.3.0, 3.5.4 and 3.6.0) §10.2.2.2 and §10.2.2.3 and originally included in OB3 and OB4 of SUBSET 091 (version 2.3.0, v3.4.0 and v3.6.0) are reduced.

Hazard related to scenario 2. The driver might be not aware of the fault occurred to the balise reception capability and continue to trust on it, as consequence of a change of mode occurred during the safe reaction of RAMS related supervision function.
Scenario 3– Text message not acknowledged
If during a service brake application consequent to a text message not acknowledged a change of mode (to SH or SN) occurs, which leads to the deletion of the text message itself, the brake application could be issued only very shortly and the text message could go completely unnoticed by the driver. This scenario could be hazardous if the text message is safety related.</td></tr>
<tr><td>Proposed mitigation</td><td>Mitigation to scenario 1 (a, c): Lower the probability that the critical information is missed, for example by making safety-relevant information redundant.
Mitigation to scenario 2: At project level (specific application) mitigation have to be found, considering that, as consequence of a change of mode that has happened during RAMS related supervision safe reaction, driver could not be aware that a failure occurred to ERTMS/ETCS On-Board balise reception channel. If found not possible to mitigate the hazardous scenario it must be evaluated whether the residual risk can be accepted.
Mitigation to scenario 3: At project level (specific application) mitigation have to be found, considering that, as consequence of a change of mode a safety related text message not acknowledged could go unnoticed by the driver. If found not possible to mitigate the hazardous scenario it must be evaluated whether the residual risk can be accepted.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.85 ETCS-H0085

Hazard ID	ETCS-H0085
Hazard headline	Ambiguities about Release Speed application in case of CES acceptance
Hazard description	In case the ERTMS/ETCS On-Board supplier considers that A.3.4.1.2 a) applies for any accepted emergency stop message, independently on whether the EOA/SvL is updated or not, the ERTMS/ETCS On-Board behaviour may fall in a grey area: A.3.4 tells the ERTMS/ETCS On-Board to delete a series of information in advance of the CES location, including the MA, while §3.10.2.2 in SUBSET-026 v3.4.0 and v3.6.0 and §3.10.2.1.2 in SUBSET-026 v2.3.0 tell the ERTMS/ETCS On-Board not to touch the SvL. Such a grey area about handling of safety related information like MA or SSP can lead to safety issues. For example, this may cause shifting the SvL to the CES stop location while keeping the release speed provided by Trackside untouched. According to second item of §3.10.2.2 of SUBSET-026, v3.6.0, when the CES is received if "*the train has not yet passed with its min safe front end the new stop location, the emergency stop message shall be accepted, however this location shall be used by the onboard to define a new EOA/SvL only if not beyond the current EOA/LOA. Refer to appendix A.3.4 for the exhaustive list of location based information stored on-board, which shall be deleted accordingly.*" Note that second item of §3.10.2.2 differs between SUBSET-026 v3.4.0 and v3.6.0 only for some editorial changes (see CR 1283) so it is not reported in this problem description. According to second item of §3.10.2.1.2 of SUBSET-026 v2.3.0, when the CES is received if *"the train has not yet passed with its min safe front end the new stop location, the emergency stop message shall be accepted, however this location shall be used by the onboard to define the new EoA and SvL only if not beyond the current EoA."* In SUBSET-026 v2.3.0, no reference is given in §3.10.2.1.2 on how to handle accepted and stored information (including Movement Authority information) if the CES is accepted. In SUBSET-026 v3.4.0 and v3.6.0, even though the reference to table A3.4 is given in §3.10.2.2, it is still not defined how to handle a possible release speed information stored on-board. For instance this release speed could be due to - a movement authority (Danger Point and/or Overlap) or - a section time-out or - the consequence of condition [11] in A.3.4.1.3 of SUBSET-026 v3.4.0 and v3.6.0 (supervision of safe radio connection). (valid only for B3 ERTMS/ETCS On-Board) As a consequence an ERTMS/ETCS On-Board might reduce the EOA to the new stop location, as a result of an accepted CES, but keep the Release Speed information stored on-board and associate it to the new SvL.
Proposed mitigation	If the risk induced by the ERTMS/ETCS On-Board attaching the trackside release speed given in an MA (i.e. not calculated on-board) to a CES stop location is not acceptable, the trackside should either not use a CES to shorten that MA or not use that trackside release speed value with that MA.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.86 ETCS-H0086

<table>
<tr><td>Hazard ID</td><td>ETCS-H0086</td></tr>
<tr><td>Hazard headline</td><td>Minimum Safe Rear End position ambiguities</td></tr>
<tr><td>Hazard description</td><td>In case an ERTMS/ETCS On-Board does not implement CR940, in the following scenario the occupied portion of track could be misinterpreted by trackside:
A train in FS mode (or OS) is split and the driver changes the length of the train, but the message with Validated Train Data is lost. Without CR940, the ERTMS/ETCS On-Board may report a position with the new safe train length and integrity confirmed not matching the length of the train that the RBC knows. The trackside could therefore consider a shorter portion of track as occupied than what is actually the case.
The hazard occurs only if the RBC has not received “train integrity lost” information while doing the splitting, because the train integrity device has not reported it or because this information has not arrived to the RBC.</td></tr>
<tr><td>Proposed mitigation</td><td>Any L3 related safety analysis has to be made entirely on a project specific basis, because L3 is not addressed by Subset-091.
The risk can be reduced with the following mitigation:
Splitting operations in Level 3 should only be performed after ending the current mission.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.87 ETCS-H0087

Hazard ID	ETCS-H0087
Hazard headline	Safety issue due to not displayed trackside text message
Hazard description	Five cases have been identified where a trackside could expect that a text message will be displayed on-board while the on-board does not display this text message. These cases are as follows: **Case 1:** In case a trackside defines that all the events composing the start condition for the display of a text message are not relevant (i.e. the start of the display of this text message is not limited by the location, the mode nor the level; all the start events have the special value), it may happen that the ERTMS/ETCS On-Board does not display this text message and it does not apply a message consistency reaction. This can happen in the following situations: - If the ERTMS/ETCS on-board interprets the specification in such a way that it sees the message consistent and plausible and that the text message does not have to be displayed. - If the ERTMS/ETCS on-board rejects the message according to §3.16.1.1 because it considers that the trackside does not comply with the requirement 3.12.3.1.2, i.e. the text message information does not respect the ETCS language, but it does not apply the message consistency reaction because the conditions included in the message consistency reaction requirements (e.g. §3.16.2.4.4) do not contain this specific case. In case a trackside defines that all the events composing the end condition for the display of text message are not relevant (i.e. the end of the display of this text message is not limited by the location, the time, the mode nor the level; all the end events have the special value), it may happen that the ERTMS/ETCS On-Board does not display this text message either. **Case 2:** Trackside transmits to the ERTMS/ETCS On-Board a text message to be acknowledged by the driver. When this message is received on-board, both start and end display conditions are immediately fulfilled. It may happen that the ERTMS/ETCS On-Board does not display this text message e.g. because of the problem described in CR1312 issue 2. This case could typically be encountered in the following situations: - The text message uses as start/end event a mode which can be left by the ERTMS/ETCS On-Board as a result from a mode profile for current location given in the same trackside message - The text message uses as start/end event a level which can be left by the on-board as a result from an immediate level transition order or from a conditional level transition order given in the same trackside message - The text message uses as start/end event a mode which can be left by the on-board as a result from an immediate level transition order or from a conditional level transition order given in the same trackside message. **Case 3:** SUBSET 026 §3.12.3.4.3 specifies that mode and level can be used as event to define the end condition for the display of a text message. In this clause, the mode end event is written “stop display when leaving mode” and the level end event is written “stop display when leaving level”. A trackside text message which uses such end events may not be displayed in the following case: In case the ERTMS/ETCS On-Board is not in the considered mode/level when the text message starts to be displayed (e.g. because the display start condition is not mode/level

	dependent), the ERTMS/ETCS On-Board may consider that the mode/level related end event is immediately fulfilled. In case the immediate fulfilment of this event would also mean the immediate fulfilment of the display end condition (because this event is the only event defining the end condition or because the end events are combined with a logical "or"), ERTMS/ETCS On-Board may not display the text message to the driver (see SUBSET 026 §3.12.3.4.4). **Case 4:** The clause 3.12.3.4.3.1 in SUBSET-026 v3.4.0/3.6.0 or the clause 3.12.3.6 in SUBSET-026 v2.3.0 does not clearly specify how to combine the display start events when all have to be fulfilled to start the display of the text message because these events may not be fulfilled simultaneously. For instance, a level used as start event could be entered before a mode used as start event or vice-versa. It is not clear if "all of the events" means that: • The display start condition is fulfilled as soon as all the events have been fulfilled at least once (even if some of them have been fulfilled but are no more fulfilled). • The display start condition is fulfilled as soon as all the events are fulfilled simultaneously. For instance, let's consider a text message with the following display start events: • Level • Mode The ERTMS/ETCS On-Board enters first the required mode; at that moment, it is not yet in the required level. Then, when the required level is entered, the mode has changed. In this example, the trackside could consider that the display start condition is fulfilled as soon as the ERTMS/ETCS On-Board enters the required level since the mode related event has already been fulfilled once. On the contrary, the ERTMS/ETCS on-board could consider that the display start condition is not fulfilled because it has to be simultaneously in the required mode and level to display the text message. As a consequence, the ERTMS/ETCS On-Board will not display the text message or display it later than expected by the trackside. **Case 5:** The clause 3.12.3.4.3.1 in SUBSET-026 v3.4.0/3.6.0 or the clause 3.12.3.6 in SUBSET-026 v2.3.0 does not clearly specify how to check a combination of events when all the selected events must be fulfilled to stop a text display, because these events may not be fulfilled simultaneously. For instance, a mode used as end event could be left before a level used as end event, or vice-versa. Thus, it is not clear if "all of the events" means that: • The display end condition is fulfilled as soon as all the end events have been fulfilled at least once (even if some of them have been fulfilled but are no more fulfilled). • The display end condition is fulfilled as soon as all the end events are fulfilled simultaneously. For instance, let's consider a text message with the following end events: • Time • Mode The ERTMS/ETCS On-Board first leaves the required mode, while the time has not expired. Then, before the time expires, the mode changes back to that it left before. This could happen if having two OS mode profiles and a text message to be displayed for a certain time AND until leaving OS mode.

	In this example, the trackside could expect that the display end condition is not fulfilled when the train is in the second OS profile, while the ERTMS/ETCS On-Board ends the text display when the time expires since the mode related end event has already been fulfilled once. Therefore, the text display ends earlier than expected by the trackside. For the five cases above, if the text message is safety relevant, (e.g. a fixed text message informing the driver about a non-protected level crossing), the non-display of the received message can lead to a safety issue. Note: In relation to the example of the non-protected level crossing, the potential non-display due to the causes mentioned above is not covered by the analysis of the MMI events contained in SUBSET 091.
Proposed mitigation	**Case 1:** At least one of the start events should include a value which is not the special value AND at least one of the end events (excluding the acknowledgment) should include a value which is not the special value. **Case 2:** Trackside should not transmit a text message to be acknowledged by the driver which both start and end conditions could be immediately fulfilled when this message is received on-board. In particular: - The trackside should not include in the same message a mode profile and text message(s) with end condition based on a mode that could be left immediately due to the received mode profile. - The trackside should not include in the same message a level transition order and text message(s) with end condition based on a level that could be left immediately due to the received level transition order. - The trackside should not include in the same message a level transition order and text message(s) with end condition based on a mode that could be left immediately due to the received level transition order. **Case 3:** Trackside should not transmit a text message including a mode or level end event and a start condition which could be fulfilled while the ERTMS/ETCS On-Board is not in the corresponding mode or level. **Cases 4&5:** In case the trackside uses more than one event for the start condition or the end condition, it should not request all events to be fulfilled (i.e. it should set Q_TEXTDISPLAY to 0).
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y *)	Y	Y
	B3MR1, X=1	Y **)	Y	Y
	B3MR1, X=2	N/A	Y	Y
	B3R2, X=1	Y **)	Y	Y
	B3R2, X=2	N/A	Y	Y

*) For a B2 On-Board on a B2 Trackside, case 2 is not relevant.

**) For a B2 On-Board on a B3MR1 (X=1) or on a B3R2 (X=1) trackside, case 2 is relevant only if Q_TEXTDISPLAY = 0. For cases 2 and 3, the text message should be displayed by the On-Board but very briefly because the display end condition is evaluated and fulfilled just after the display has started.

4.88 ETCS-H0088

Hazard ID	ETCS-H0088
Hazard headline	Ambiguities in drivers acknowledgement requirements
Hazard description	According to §5.9.2.3 of SUBSET-026, for v2.3.0, v3.4.0 and v3.6.0, the supervision of the driver when a mode transition to OS is executed has to be acknowledged in order to assure the driver is aware of this change of responsibility. Due to this, the supervision of the driver acknowledgement should start at the time the event which triggers the acknowledgement request happens, but, according to §5.9.2.4 of SUBSET-026 for v2.3.0, v3.4.0 and v3.6.0, the start condition of the acknowledgement timer is not clearly defined (note that it is defined for SH mode in §5.7.2.4 of Subset-026 for v2.3.0, v3.4.0 and v3.6.0, where it is clearly stated “after the change to SH mode”). In the same way, §5.19.2.3 of Subset-026 for v3.4.0 and v3.6.0, request the driver acknowledged for LS mode entry, but §5.19.2.4 of Subset-026 for v3.4.0 and v3.6.0 does not define the start event related to this acknowledgement. A misinterpretation of the specification could lead some ERTMS ETCS On–Board to consider the display of acknowledgement request as the start event for the timer, instead of the transition to OS or LS mode. Additionally, it must be taken into account that a mode transition to OS or LS can take place simultaneously with other events to be acknowledged (e.g. a level transition). According to the DMI specification ERA/ERTMS 015960 clause 5.4.1.9, the different objects or trackside text messages to be acknowledged or the system status message “[name of NTC] failed” shall be managed according to a FIFO principle with a delay of 1 s between their display. Therefore, in case the ERTMS/ETCS on-board implementation is made as explained above and taking into account the FIFO principle, it may happen that the request for acknowledgement of the mode change display is delayed due to a previous request for acknowledgement of another message, in such a way that the train is running in OS or LS without appropriate driver supervision for more than 5 seconds, according to Tack §A3.1 of SUBSET-026 for v2.3.0, v3.4.0 and v3.6.0, after the mode transition without brake application. Note: If the display of acknowledgement request is the start event for the timer to brake application, the late application of the service brake could also occur due to a failure of the DMI. Please refer to MMI-2g Subset-091. Note: Referenced CR is CR1166.
Proposed mitigation	For trackside text messages requesting an acknowledgement and for all level transitions for which an acknowledgement is required (i.e. for the level transitions marked as “YES” in the clause 5.10.4.4 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0), the ack request should be engineered in such a way that it is displayed at least 6 seconds before reaching: • the display start location of a trackside text message to be acknowledged, or • the location of a level transition for which an acknowledgement is required, or

<table>
<tr><td></td><td>
the start location of an OS or an LS mode profile.
Note: The first bullet assumes that the display start location of the subsequent trackside text message to be acknowledged can be determined in engineering.
The 6 seconds referred to in the above mitigation includes an assumed 5 seconds driver acknowledgement time for the trackside text messages (similar as the one for level and mode transition acknowledgement) and the 1 second delay between 2 consecutive acknowledgements as specified in clause 5.4.1.9 of ERA_ERTMS_015560 v3.4.0 and v3.6.0.
The following modified TSI OPE appendix A rule 6.53 shall apply:
"In Levels 0, 1, 2, 3, NTC, when the following text message is displayed: “[name of NTC] failed”, the driver shall acknowledge and apply non-harmonised rules."
Note: the mitigation measures provided above leave room to the following residual risks:

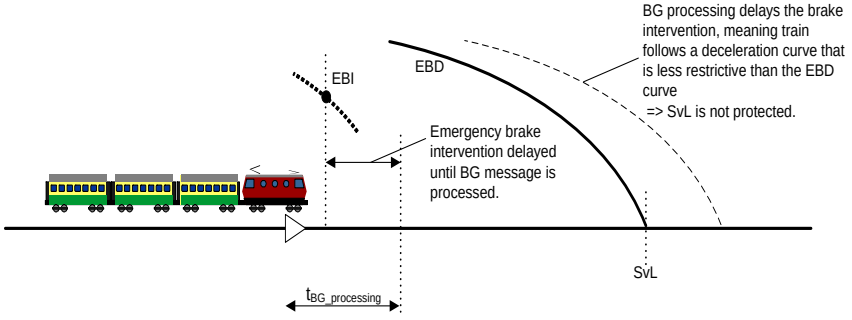
The messages like “[name of NTC] failed” could appear on the DMI in any level at any moment. These messages could delay the display of subsequent acknowledgement request with no other mitigation possible that the expectation that the driver will acknowledge them as soon as possible.
It may happen that the request for acknowledgement of the mode change display is delayed due to a previous request for acknowledgement of another message due to the driver not having acknowledged within 5 seconds.

</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
* In B2 there was no DMI document mandatory so no FIFO mandated by ETCS requirement. However, similar behaviour is expected, see DMI informative document version 2.3 clause 5.4.1.3
</td></tr>
</table>

4.89 ETCS-H0089

<table>
<tr><td>Hazard ID</td><td>ETCS-H0089</td></tr>
<tr><td>Hazard headline</td><td>Expiration of T_NVCONTACT</td></tr>
<tr><td>Hazard description</td><td>An RBC uses CES for passage control. The MA covers at least two interlocking areas. The RBC loses the connection with the second interlocking. RBC reacts as follows:
RBC does intentionally let T_NVCONTACT expire because in case of loss of connection to interlocking the continuation of route protection can be assumed for the time-span of T_NVCONTACT but not for a longer duration (this is a project specific condition). The RBC stops sending MAs and also stops sending life sign messages.
The passage control continues for the area of the first interlocking by RBC sending HP CES.
The RBC assumes that sending HP CES does not impact the expiration of T_NVCONTACT on-board, while the ERTMS/ETCS On-Board resets T_NVCONTACT when HP CES is received. In this case T_NVCONTACT will not expire and ERTMS/ETCS On-Board will not react according to M_NVCONTACT. The train may enter a not protected route.</td></tr>
<tr><td>Proposed mitigation</td><td>RBC should not send HP CES in situations where the RBC wants T_NVCONTACT to expire in the ERTMS/ETCS On-Board.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>Y</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.90 ETCS-H0090

Hazard ID	ETCS-H0090
Hazard headline	Possible supervision gap during ERMS/ETCS On-Board balise message processing
Hazard description	In Subset-026 v3.4.0 clause A.3.5.2, introduced through CR977, the exact meaning of 'the message has been fully processed' is not clear. Also, the same clause states that "the action(s) resulting from its content…shall take precedence on any other action related to a further location…" The clause does not limit the scope of what is meant by the term "any other action", which therefore seems to imply that it really means all location-based actions that may be handled by the ERTMS/ETCS On-Board equipment. If this is really the intention, then it means that every location-based action may be delayed while a BG message is being processed. Failure to take these delays into account may have a detrimental impact on safety and/or performance. It is not clear from the specifications whether it is the responsibility of the ERTMS/ETCS On-Board or the ETCS trackside, to take into account the delays. Clause A.3.5.2: *"Once the ERTMS/ETCS On-Board equipment has received a balise group message (i.e. once it has received the last balise telegram of the balise group), the action(s) resulting from its content shall take into account the train position measured at the time of reception of this last telegram and shall take precedence on any other action related to a further location that is reached before the message has been fully processed."* A general exhaustive analysis of all possible issues arising from the CR 977 delay has not been done. The following scenarios have been identified where delays to performing of actions could have an impact on safety (if neither the ERTMS/ETCS On-Board nor ETCS trackside takes these delays into account): **1. Emergency brake intervention** The EBI supervision limit is a location based entity. Therefore the EBI supervision limit may be passed while the ERTMS/ETCS On-Board equipment is processing a balise group message. As ETCS does not (yet) know the content of the message, and according to A.3.5.2 the evaluation and resulting actions of the message must take precedence over the EBI intervention, the emergency brake reaction must presumably be delayed until the BG message has been fully processed. If this delay is not taken into account in the EBI calculation, then this means that the ERTMS/ETCS On-Board cannot safely protect EBD based targets. See following figure.  So the clause A.3.5.2 brought in by the CR977 leads the ERTMS/ETCS On-Board to unduly delay the emergency brake application in case of BG received in the vicinity of the EBI location. **2. Overlap timer** The overlap timer is started when the train passes the overlap timer start location with the max safe front end. The start of the timer could therefore be delayed if a BG message is

<table>
<tr><td></td><td>being processed when the start location is passed. This is safety relevant, as the ERTMS/ETCS On-Board equipment may start the timer later than the trackside expects (the overlap is maintained on-board longer than it should be).

3. End section timer
The end section timer is started when the train passes the end section timer start location with the max safe front end. The start of the timer could therefore be delayed if a BG message is being processed when the start location is passed. This is safety relevant, as the ERTMS/ETCS On-Board equipment may start the timer later than the trackside expects (the end section is maintained on-board longer than it should be). The consequence could be hazardous situation, due to an untimely behaviour of the interlocking.

Note: Referenced CR is CR1300.</td></tr>
<tr><td>Proposed mitigation</td><td>Scenario1: No realistic trackside mitigation measure found.
Scenario 2&3: There should be a distance of at least 1.3m + 1.5sec (SUBSET-041 v3.2.0, §5.2.1.3) times the line speed between the last encountered balise of a balise group and the timer start location.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N*</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
* The extension of scope (introduced by the CR977) of the delay after passing a location reached before a BG message is fully processed, to other locations than the EOA/LOA cannot be deduced from the B2 SRS clause 3.13.8.1.1
</td></tr>
</table>

4.91 ETCS-H0091

<table>
<tr><td>Hazard ID</td><td>ETCS-H0091</td></tr>
<tr><td>Hazard headline</td><td>Not supervised TSR depending on packet processing order</td></tr>
<tr><td>Hazard description</td><td>The following situation has been detected to be hazardous: A BG containing Packet 66 TSR Revocation and Packet 65 TSR, both using the same NID_TSR.

There are two possible situations in which this scenario could occur:
a) A TSR with a revocable NID_TSR “X” is set on track and it becomes not applicable anymore so the track decides to revoke it. Additionally, a new TSR has been established on track and since identifier X is assumed to be free due to the revocation, then TSR_ID “X” is used for this new TSR.
b) A TSR with a revocable TSR_ID “X” is set on track which is modified (i.e. change of length), so it is revoked and the new definition of the TSR is sent with the same TSR_ID.

No order of processing is defined in the specification if Packet 65 and Packet 66 are received in the same message. Depending on the order of processing for packets 66 and 65 implemented within the ERTMS/ETCS On-Board, the following can occur:
1) The ERTMS/ETCS On-Board first uses Packet 65, then Packet 66. The new TSR will be revoked before it was ever supervised.
2) The ERTMS/ETCS On-Board first uses Packet 66, then Packet 65. The new TSR will be supervised.

If 1) happens, it is a safety issue.</td></tr>
<tr><td>Proposed mitigation</td><td>In any of the cases above, using the same NID_TSR in a message must be avoided.

For situation a), the proper engineering should be to use a different NID_TSR for sending the new TSR, e.g. NID_TSR “Y”. Alternatively, Packet 66 could be transmitted in a first message and Packet 65 in a second message.

For case b), the proper engineering would be to send only Packet 65 for the new definition of TSR with NID_TSR “X” without including a packet 66 for that NID_TSR since, according to Subset 026, clause 3.11.5.9, the new TSR will replace the previous one with the same identifier.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.92 ETCS-H0092

Hazard ID	ETCS-H0092
Hazard headline	Undefined sequence of actions in case of MA shortening accompanied with location based information beyond the new SvL
Hazard description	In case of “MA shortening” accompanied with location based information located further than the SvL of the shortened MA, it is not clearly specified whether: - the deletion of location based information stored on-board due to MA shortening *(according to A.3.4.1.2.b)* applies before or after: - replacing stored location based information with the newly received information (*e.g. new track description and linking information replacing the stored ones according to 3.7.3.1, new level transition for further location replacing the stored one according to 5.10.1.6, new not yet applicable NVs replacing stored ones according to 3.18.2.9 first bullet*). The order of processing information influences the resulting ERTMS/ETCS On-Board behaviour which is therefore not deterministic. “MA shortening” as defined in SUBSET-026 v3.6.0 and v3.4.0 for: - the reception of an MA defining an SvL closer than the one supervised with the former MA (according to 3.8.5.1.3) - the reception of an MA defining an SvL while the ERTMS/ETCS On-Board was supervising an LOA (according to 3.8.5.1.4). And “MA shortening” as defined in SUBSET-026 v2.3.0 modified by SUBSET-108 v1.2.0 when: - an “*MA has been replaced by a shorter one*” (according to 3.7.3.3; Note: this clause was deleted in a later version via CR 963 and stated more precisely in clause 3.8.5.1.3/3.8.5.1.4 – see above). It is not clearly defined, whether the reception of an MA defining an SvL while an LoA is supervised is considered an “MA shortening. **Scenario 1 – ERTMS/ETCS On-Board deletes just received location based information:** On the reception of an MA shortening: - the ERTMS/ETCS On-Board uses the location based information first and replaces the current stored location based information by the new one. - afterwards it uses the new MA and deletes the location based information The trackside expects that the just received location based information is not deleted. When sending an MA extension over the same route, the trackside may not resend this location based information. This could be hazardous for certain location based information if then: - case a: the tracksides sends an MA defining an SvL and does not resend location based information, like not yet applicable NVs etc. *(Note: If the trackside does not resend SSP and gradient information this is not hazardous but may be operationally obstructive, because the new MA will only be accepted if the stored SSP and gradient on-board cover the full length of the new MA, according 3.7.2.3.)* - case b: the trackside sends an MA defining an LoA and does not resend location based information, like SSP, gradient information, not yet applicable NVs etc.

<table>
<tr><td></td><td>(Note: stored SSP and gradient information may impact the braking curve calculation while the train is approaching the LoA.)

Scenario 2 – ERTMS/ETCS On-Board keeps just received location based information:
On the reception of an MA shortening:
- the ERTMS/ETCS On-Board uses the MA first and deletes the stored location based information.
- afterwards it stores the newly received location based information
The trackside expects that the sent location based information is deleted. When afterwards the route changes the trackside may send an MA extension for the new route without revoking/cancelling obsolete location based information.
This could be hazardous because the ERTMS/ETCS On-Board could use the not-deleted location based information on a route for which this location based information is not valid.</td></tr>
<tr><td>Proposed mitigation</td><td>In level 1, any MA should not be sent together with other location based information* further than the SvL of this MA.
In level 2/3, any shortened MA should not be sent together with other location based information* further than the SvL of this MA
Note (in level 2/3): In case the shortened MA gets lost or not accepted, (there is a residual risk that the train considers a further received MA as an MA shortening with location based information further than the SvL of the MA, although this MA is considered an MA extension of the (lost or not accepted) shortened MA by the trackside. If this residual risk cannot be accepted: Trackside shall send all MAs with location based information not further than SvL of the MA
*focusing only on safety, the mitigation could be restricted to safety relevant location based information (e.g. level transition for further location, not yet applicable national values)</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.93 ETCS-H0093

Hazard ID	ETCS-H0093
Hazard headline	Unsafe situations resulting from the sequence of processing between a “System version order” and the other information contained in the same balise group message.

Hazard description	It is not clear in SUBSET-026 if the change of operating system version resulting from a “System version order” (Packet 2) has to be considered before or after the translation/execution of the other packets contained in the same balise group message. This could lead to a safety issue since the ERTMS/ETCS On-Board behaviour may be different depending on whether the operated system version is X=1 or X=2.
	Case 1: In addition to the “System version order” (Packet 2), the message of a balise group may contain a Packet 137 “Stop if in Staff Responsible”.
	The identity of this balise group may also be included in a “List of Balises in SR Authority” (Packet 63) received previously.
	• **Sub-case 1.1:** The ERTMS/ETCS On-Board is operating in SR mode with system version X=2 with no communication session established with the X = 2 RBC having sent the list of balises in SR Authority or considering again the system version orders from balises as per 3.17.2.8 d) or e) when it receives the balise group message with M_VERSION X=1 or X=2. The system version order is to change to X=1 version:
	  ○ in case the ERTMS/ETCS On-Board processes first the system version order, the packet 137 “Stop if in Staff Responsible” is processed while the operated system version is X=1 and the Trip mode is therefore entered (see clauses 6.6.2.2.1 and 6.6.2.2.2 in SUBSET-026 v3.4.0/3.6.0).
	  ○ in case the ERTMS/ETCS On-Board processes first the packet 137 “Stop if in Staff Responsible”, this is processed while the operated system version is still X=2 and the Trip mode is therefore not entered (see transition condition [54] in section 4.6.2 and clause 4.4.11.1.3 d) in SUBSET-026 v3.4.0/3.6.0).
	• **Sub-case 1.2:** The ERTMS/ETCS On-Board is operating in SR mode with system version X=1 with no communication session established with the X = 1 RBC having sent the list of balises in SR Authority or considering again the system version orders from balises as per 3.17.2.8 d) or e) when it receives the balise group message with M_VERSION X=1. The system version order is to change to X=2 version:
	  ○ in case the ERTMS/ETCS On-Board processes first the system version order, the packet 137 “Stop if in Staff Responsible” is processed while the operated system version is X=2 and the Trip mode is therefore not entered (see transition condition [54] in section 4.6.2 and clause 4.4.11.1.3 d) in SUBSET-026 v3.4.0/3.6.0).
	  ○ in case the ERTMS/ETCS On-Board processes first the packet 137 “Stop if in Staff Responsible”, this is processed while the operated system version is still X=1 and the Trip mode is therefore entered (see clauses 6.6.2.2.1 and 6.6.2.2.2 in SUBSET-026 v3.4.0/3.6.0).
	An unsafe situation occurs in case the trackside expects the ERTMS/ETCS On-Board to enter Trip mode and the ERTMS/ETCS On-Board does not enter this mode.
	Case 2: In addition to the “System version order” (Packet 2), the message of a balise group may contain a Packet 3 “National values”.
	The translation of the “National values” (Packet 3) received from an X=1 trackside depends on the operated system version (see section 6.6.3.2 of SUBSET-026 v3.4.0/3.6.0).

	The difference in translation concerns the variable Q_NVLOCACC and V_NVLIMSUPERV (see T [1a] and T [1b]).
	• **Sub-case 2.1:** The ERTMS/ETCS On-Board is operating in system version X=2 when it receives the balise group message with M_VERSION X=1. The system version order is to change to X=1 version:
	  ○ in case the ERTMS/ETCS On-Board translates the National values before processing the system version order, the ERTMS/ETCS On-Board applies the translation [1b] since the operated version is still X=2. As a result, the value of Q_NVLOCACC and the value of V_NVLIMSUPERV are not affected by the content of the packet 3.
	  ○ in case the ERTMS/ETCS On-Board translates the National values after processing the system version order, the ERTMS/ETCS On-Board applies the translation [1a] since the operated version is X=1. As a result, the variables Q_NVLOCACC and V_NVLIMSUPERV are set to their respective default values (12 m and 100 km/h, see A.3.2 in SUBSET-026 v3.4.0/3.6.0).
	• **Sub-case 2.2:** The ERTMS/ETCS On-Board is operating in system version X=1 when it receives the balise group message with M_VERSION X=1. The system version order is to change to X=2 version:
	  ○ in case the ERTMS/ETCS On-Board translates the National values before processing the system version order, the ERTMS/ETCS On-Board applies the translation [1a] since the operated version is still X=1. As a result, the variables Q_NVLOCACC and V_NVLIMSUPERV are set to their respective default values (12 m and 100 km/h, see A.3.2 in SUBSET-026 v3.4.0/3.6.0).
	  ○ in case the ERTMS/ETCS On-Board translates the National values after processing the system version order, the ERTMS/ETCS On-Board applies the translation [1b] since the operated version is X=2. As a result, the value of Q_NVLOCACC and the value of V_NVLIMSUPERV are not affected by the content of the packet 3.
	An unsafe situation may occur in case:
	• as a result of the translation, the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an underestimation of the actual inaccuracy of the balise groups on the track. This can lead to an underestimated train position confidence interval. It has however to be noted that:
	  ○ the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode.
	  ○ the problematic part of the underestimation is limited to 12 m since by definition, a trackside already accepts the risk (or take appropriate measures) related to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode.
	• as a result of the translation, the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an overestimation of the actual inaccuracy of the balise groups on the track. Such an overestimation induces an overestimation of the train position confidence interval which can lead to a late entry in Trip mode related to passing an EOA/LOA. It has however to be noted that:
	  ○ the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode.
	  ○ the problematic part of the overestimation is limited to 51 m (maximum possible value of 63 m minus default value of 12 m) since by definition, a trackside already accepts the risk (or take appropriate measures) related

<table>
<tr><td></td><td>to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode.
• as a result of the translation, the ERTMS/ETCS On-Board uses on the next X=2 area a value of V_LIMSUPERV which is higher than the one expected to be supervised on this area. It has however to be noted that the unsafe situation occurs only in case no X=2 National Values (i.e. no packet 3 with an X=2 structure) are transmitted at the entry of this X=2 area and the LS mode profiles provided in this X=2 area request to use the national value of the LS mode speed limit (V_MAMODE=127).</td></tr>
<tr><td>Proposed Mitigation</td><td>Case 1: A balise group that provides “Stop if in Staff Responsible” information (Packet 137) and which identity is included in a “List of Balises in SR Authority” information (Packet 63) should not contain a “System version order” (Packet 2).
Case 2: A balise group that provides a “System version order” (Packet 2) and “National values” (Packet 3) at the border between an area operated with system version X=2 and an area operated with system version X=1 should always have M_VERSION X=2.
In case this mitigation is applied on a line where B2 trains can operate (these trains operate in Level 0 or STM in the X=2 area), the trackside engineering should consider that:
• in case the B2 train is intended to operate in Level 1, 2 or 3 in the X=1 area, the X=2 balise group has to be read before leaving Level 0/STM to avoid a transition to Trip mode (see clause 3.17.3.5 in SUBSET-026 v2.3.0).
• the content of the X=2 balise group placed at the border between the X=2 and the X=1 area will not be considered by a B2 ERTMS/ETCS On-Board and therefore the national values provided by this balise group will not be applied such an ERTMS/ETCS On-Board. To avoid possible unsafe consequences of this:
○ the National Values to be used in the X=1 area should be provided to the B2 ERTMS/ETCS On-Board either in rear of the border (e.g. by an X=1 balise group located in the X=2 area and which specifies that the national values it provides apply from the start location of the X=1 area) or in advance of this one (e.g. by an X=1 balise group located in the X=1 area). Providing the national values in advance of the border could lead to the reconsideration of providing these values in the border balise group since B3 trains will also read these National Values and will translate them considering an operated system in line with the area where they apply, i.e. X=1.
○ the National Values to be used in the X=2 area should be provided to the B2 ERTMS/ETCS On-Board either in rear of the border (e.g. by an X=1 balise group located in the X=1 area and which specifies that the national values it provides apply from the start location of the X=2 area) or in advance of this one (e.g. by an X=1 balise group located in the X=2 area).</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.94 ETCS-H0094

Hazard ID	ETCS-H0094
Hazard headline	Unsafe situations resulting from an undue change of operated system version due to reception of a loop message by cross-talk
Hazard description	The translation of the “National values” (Packet 3) received from an X=1 trackside depends on the operated system version (see section 6.6.3.2 of SUBSET-026 v3.4.0/3.6.0). The difference in translation concerns the variable Q_NVLOCACC and V_NVLIMSUPERV (see T [1a] and T [1b]). Hazards can occur for the following scenarios: **Scenario 1:** A B3 train runs in SR mode with an operated system version X=2 on a line supervised by an X=2 RBC. The train has received from this RBC a “list of balises in SR”. The communication session between the ERTMS/ETCS On-Board and the RBC is then terminated and the train passes a balise group included in the “list of balises in SR” and providing a “System version order” (Packet 2) which forces the train to change to operated system version X=1. The ERTMS/ETCS On-Board subsequently receives by cross-talk the message of a loop with M_VERSION=2.The ERTMS/ETCS On-Board changes the operated system version to X=2. The ERTMS/ETCS On-Board then receives a balise group which is included in the “list of balises in SR” and which message contains “stop if in SR” information. The ERTMS/ETCS On-Board does not trip the train because it is operating in system version X=2 (see transition condition [54] in section 4.6.2 and clause 4.4.11.1.3 d) in SUBSET-026 v3.4.0/3.6.0) while the trackside was expecting a trip to take place as per X=1 ERTMS/ETCS On-Board behaviour (see clauses 6.6.2.2.1 and 6.6.2.2.2 in SUBSET-026 v3.4.0/3.6.0). **Scenario 2:** A B3 train runs with an operated system version X=2 on an X=2 line with Q_NVLOCACC and V_NVLIMSUPERV different from their respective default values. The train passes a BG providing a “System version order” (Packet 2) with M_VERSION = 1.Y, or goes through a stretch of Level 2 line equipped with an RBC X=1, which forces the On-board equipment to change to operated system version X=1. The values of Q_NVLOCACC and V_NVLIMSUPERV are not changed. The ERTMS/ETCS On-Board receives by cross-talk the message of a loop with M_VERSION=2.The ERTMS/ETCS On-Board changes the operated system version to X=2. Afterwards the ERTMS/ETCS On-Board receives the message from an X=1 BG containing “National values” (Packet 3). Trackside expects that the ERTMS/ETCS On-Board will “reset” the Q_NVLOCACC and V_NVLIMSUPERV variables to their respective default values (12 m and 100 km/h, see A.3.2 in SUBSET-026 v3.4.0/3.6.0). Since the ERTMS/ETCS On-Board is operating in system version X=2, this does not happen because translation [1b] is applied and this translation does not affect the stored values of Q_NVLOCACC and V_NVLIMSUPERV.

Regarding the Q_NVLOCACC variable:

- In case Q_NVLOCACC is larger than the default value (12 m), the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an overestimation of the actual inaccuracy of the balise groups on the track. Such an overestimation induces an overestimation of the train position confidence interval which can lead to a late entry in Trip mode related to passing an EOA/LOA. It has however to be noted that:
  - the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode.
  - the problematic part of the overestimation is limited to 51 m (maximum possible value of 63 m minus default value of 12 m) since by definition, a trackside already accepts the risk (or take appropriate measures) related to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode.
- In case Q_NVLOCACC is smaller than the default value (12 m), the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an underestimation of the actual inaccuracy of the balise groups on the track. This can lead to an underestimated train position confidence interval which may induce an incorrect supervision of speed restrictions e.g. when transmitted by BG marked as unlinked for which the installation rules allow a location inaccuracy of 12m. It can also lead to the rejection of balise groups due to the reception of the reference balise of these groups outside the expectation window. It has however to be noted that:
  - the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode.
  - the problematic part of the underestimation is limited to 12 m since by definition, a trackside already accepts the risk (or take appropriate measures) related to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode.
  - The loss of safety relevant information due to rejection of balise groups can be mitigated by defining a reaction “Apply service brake” or “Train trip” for the balise groups which contain safety related information.

By applying T [1b] instead of T [1a], the ERTMS/ETCS On-Board may use on the next X=2 area a value of V_LIMSUPERV which is higher than the one expected to be supervised on this area. It has however to be noted that an unsafe situation occurs only in case no X=2 National Values (i.e. no packet 3 with an X=2 structure) are transmitted at the entry of this X=2 area and the LS mode profiles provided in this X=2 area request to use the national value of the LS mode speed limit (V_MAMODE=127).

Scenario 3:

A B3 train runs with an operated system version X=2 on an X=2 line with Q_NVLOCACC and V_NVLIMSUPERV different from their respective default values.

The train receives via cross-talk an X=1 loop message with a NID_C different from NID_C used in the area where the train is currently running.

	Due to the mismatch between the NID_C of this message and the NID_C of the currently applicable national values, the ERTMS/ETCS On-Board considers the system version number X transmitted by this loop as the operated one (see 3.17.2.6 in SUBSET-026 v3.4.0/3.6.0). Afterwards, without having encountered X=2 balises/loops since the X=1 loop message has been received, the ERTMS/ETCS On-Board receives the message from an X=1 BG containing “National values” (Packet 3). Trackside expects that the ERTMS/ETCS On-Board will keep the value of the Q_NVLOCACC and V_NVLIMSUPERV variables untouched. Since the ERTMS/ETCS On-Board is operating in system version X=1, this does not happen because translation [1a] is applied and this translation “resets” the Q_NVLOCACC and V_NVLIMSUPERV variables to their respective default values (12 m and 100 km/h, see A.3.2 in SUBSET-026 v3.4.0/3.6.0). Regarding the Q_NVLOCACC variable: • In case Q_NVLOCACC default value (12 m) is larger than the Q_NVLOCACC value relevant for the considered area, the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an overestimation of the actual inaccuracy of the balise groups on the track. Such an overestimation induces an overestimation of the train position confidence interval which can lead to a late entry in Trip mode related to passing an EOA/LOA. It has however to be noted that: ○ the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode. ○ the problematic part of the overestimation is limited to 12 m since by definition, a trackside already accepts the risk (or take appropriate measures) related to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode. • In case Q_NVLOCACC default value (12 m) is smaller than the Q_NVLOCACC value relevant for the considered area, the ERTMS/ETCS On-Board uses a location accuracy for the balise groups which is an underestimation of the actual inaccuracy of the balise groups on the track. This can lead to an underestimated train position confidence interval which may induce an incorrect supervision of speed restrictions e.g. when transmitted by BG marked as linked for which the installation rules allow a location inaccuracy of 63m. It can also lead to the rejection of balise groups due to the reception of the reference balise of these groups outside the expectation window. It has however to be noted that: ○ the issue only exists when no linking information is available for the balise group the train position is referred to or when the linking information is available for this balise group but not used, e.g. due to the train being in SR mode. ○ the problematic part of the underestimation is limited to 51 m (maximum possible value of 63 m minus default value of 12 m) since by definition, a trackside already accepts the risk (or take appropriate measures) related to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode. ○ The loss of safety relevant information due to rejection of balise groups can be mitigated by defining a reaction “Apply service brake” or “Train trip” for the balise groups which contain safety related information. By applying T [1a] instead of T [1b], the ERTMS/ETCS On-Board may use on the next X=2 area a value of V_LIMSUPERV which is higher than the one expected to be supervised on this area. It has however to be noted that an unsafe situation occurs only in case no X=2 National Values (i.e. no packet 3 with an X=2 structure) are transmitted at the entry of this

<table>
<tr><td></td><td>X=2 area and the LS mode profiles provided in this X=2 area request to use the national value of the LS mode speed limit (V_MAMODE=127).</td></tr>
<tr><td>Proposed Mitigation</td><td>For scenario 1:
On X=1 operated lines where trains operating in SR can receive messages from X=2 loops by cross-talk, trackside should not use a combination of “list of SR balises” and “Stop if in SR” information, i.e. the trackside should not provide “Stop if in SR” information in a balise group included in a “list of balises in SR”.

For scenario 2:
On X=1 operated lines where trains can receive messages from X=2 loops by cross-talk, the country/region identity number (NID_C) of a balise group that provides “National values” information (Packet 3) should not be contained in the list of country/region identity numbers (NID_C) for which the national values of any adjacent X=2 line are applicable. Notes:
1. the principle of this mitigation is that the ERTMS/ETCS On-Board will switch to the default values of Q_NVLOCACC and V_NVLIMSUPERV when it will detect the mismatch between the country/region identity number read from the balise group and the country/region identity numbers for which the stored values of Q_NVLOCACC and V_NVLIMSUPERV are applicable.
2. Care should be taken that in case the issues related to Q_NVLOCACC described above would not be relevant for operation on the X=1 line adjoining the X=2 line, they could be relevant for operation on another X=1 line that the train will enter later on.

For scenario 3:
In an X=2 area where X=1 loop messages with a NID_C different from NID_C used in this area can be received via cross talk, trackside should never provide NV in X=1 balise groups.
Note: This mitigation does not bring the train back to operate system version X=2. This can be achieved by using only X=2 balise groups.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>Y (scenarios 1 and 2 only)</td><td>Y (scenarios 1 and 2 only)</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y (scenarios 2 and 3 only)</td><td>Y (scenarios 2 and 3 only)</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>Y (scenarios 1 and 2 only)</td><td>Y (scenarios 1 and 2 only)</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y (scenarios 2 and 3 only)</td><td>Y (scenarios 2 and 3 only)</td></tr>
</table>
</td></tr>
</table>

4.95 ETCS-H0095

4.95.1.1 Intentionally left empty. Hazard entry under analysis.

4.96 ETCS-H0096

4.96.1.1 Intentionally left empty. No action by application projects is required

4.97 ETCS-H0097

Hazard ID	ETCS-H0097
Hazard headline	Ambiguity in determination of location accuracy of a balise group the train position is referred to
Hazard description	It is not clear in SUBSET-026 (3.6.4.3.1 v2.3.0, and 3.6.4.2.3 v3.4.0 and v3.6.0) how the ERTMS/ETCS On-board should behave when there is a change in the location accuracy value of a balise group the train position is referred to. The following events may lead to a possible hazardous situation: • A change of national values is ordered by trackside • The linking information is deleted e.g. due to a mode change which requires deletion of linking information • The linking information is no more used while the accuracy of LRBG was determined based on the linking information • The first balise group announced by the linking information included in a message 15 or 33 (MA with shifted location reference) is the LRBG whose location accuracy was previously determined based on the corresponding National/Default value. For example the following scenarios could happen: • New set of national values. When processing a new set that applies before the LRBG changes, and the new location accuracy is smaller (higher accuracy), the ERTMS/ETCS On-board could apply to the LRBG a value of the location accuracy that does not relate to the area in which the LRBG was located. • End of mission. When closing a desk of a train in FS, for which the location accuracy is known from previously received linking information, it is not clear whether the ERTMS/ETCS On-board should maintain this location accuracy or it should use the national/default value. • Passing last balise group included in linking. A train in FS (or OS) has linking information on board. When passing the last BG included in the linking, the train determines the trackside location accuracy using the linking information. It is not clear whether the location accuracy of the LRBG which was determined based on this linking information will be maintained or not once the linking info is no more used. • A train is running in SR mode with a location accuracy determined based on other means than linking information. The on-board then receives an MA by radio providing linking information including LRBG. It is not clear whether the on-board will update the location accuracy of the LRBG based on the received linking information • A SoM is performed after a change of train orientation and the current LRBG (in advance of the train front) was previously passed in SL mode while no linking information was available. The first MA received on-board is given through the message 33 (MA with shifted location reference) and the first BG announced by the linking information is the LRBG. It is not clear whether the location accuracy of the LRBG that was determined based on e.g. the corresponding National/Default Value will be maintained or will be superseded by the location accuracy from the linking information. An inappropriate value of location accuracy of a balise group the train position is referred to supervised by the ERTMS/ETCS On-board may have one of these consequences: • An underestimation of the train position confidence interval, leading to incorrect supervision of speed restrictions, rejection of BG with safety relevant information. It has however to be noted that the loss of safety relevant information due to rejection of balise groups can be mitigated by defining a reaction “Apply service brake” or “Train trip” for the balise groups which contain safety related information when linking information is available and supervised for these balise groups • .An overestimation of the train position confidence interval, leading to late entry in Trip mode passing an EOA/LOA.

<table>
<tr><td>Proposed mitigation</td><td>Each specific application safety analysis should identify the appropriate measures trackside shall take when engineering the distance information in scenarios like those presented in this hazard log entry. Even if this mitigation is valid for B2, B3MR1 and B3R2, the detail about trackside responsibility related to engineering the distance information is explicitly mentioned only in Subset-026 §3.6.4.3.1 v3.4.0 and v3.6.0, for B3MR1 and B3R2.
Alternative mitigation (except for a change of national values ordered by trackside): For every BG in linking information, the trackside should use a value of BG location accuracy, which is equal to 12 m (for B2) or to the National Value (for B3MR1 and B3R2) and BG should be installed accordingly on the track.
Alternative mitigation for a change of national values ordered by trackside: the trackside should use D_VALIDNV = "now" or 0 in packets 3 sent from balise groups marked as linked.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td></td><td></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.98 ETCS-H0098

4.98.1.1 Intentionally left empty. No action by application projects is required.

4.99 ETCS-H0099

4.99.1.1 Intentionally left empty. Hazard entry under analysis.

4.100 ETCS-H0100

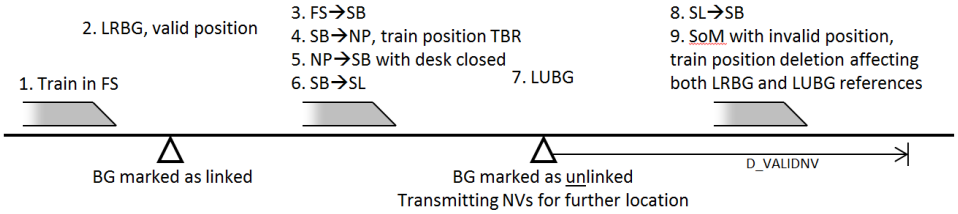
4.100.1.1 Intentionally left empty. No action by application projects is required.

4.101 ETCS-H0101[4]

<table>
<tr><td>Hazard ID</td><td>ETCS-H0101</td></tr>
<tr><td>Hazard headline</td><td>Unexpected rejection of directional information received from unlinked BG(s) due to unclear management of train position status on passing BG(s) marked as unlinked</td></tr>
<tr><td>Hazard description</td><td>SUBSET 026 does not specify clearly when the train position leaves the status “Unknown” outside an SoM procedure and this may result in loss of potentially safety related information. Only SUBSET-026 (v3.4.0 and v3.6.0) §3.6.2.2.2.1 and §3.6.2.2.2.2 specify the transitions from train position status “Unknown”..
The scenario analysed is the following one:
After an SoM, the status of the train position is Unknown.
Then, the first BG the train passes over is marked as unlinked. This BG contains unidirectional location based information valid for the train orientation.
According to SUBSET-026 §3.6.4.7.1 (v3.4.0, v3.6.0), location based information is supervised using the unlinked BG as reference, but it is unclear how §3.6.3.1.3.1 (rejection of data received valid for one direction only, when train position is unknown) should be interpreted because it is not specified what would be the train position status in that circumstance. The ERTMS/ETCS On-Board could consider that the train position status is still “unknown” when encountering the balise group marked as unlinked and due to SUBSET-026 §3.6.3.1.3.1, reject the information valid for one direction only that this BG contains. This would impact safety in case this information is safety related (e.g. a TSR). Note: the wording "train position" does not appear in §3.6.3.1.3.1 of SUBSET-026 (2.3.0). In SUBSET-026 (2.3.0), §3.6.3.1.3.1 uses the notion of "train orientation" which is by definition always known. Therefore §3.6.3.1.3.1 can never be applied.</td></tr>
<tr><td>Proposed mitigation</td><td>No generic mitigation measure could be found. An application specific analysis is necessary.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

[4] Note: This hazard reflects the opinion of ERA and EUG. For the UNISIG opinion please refer to the corresponding BCA report.

4.102 ETCS-H0102[5]

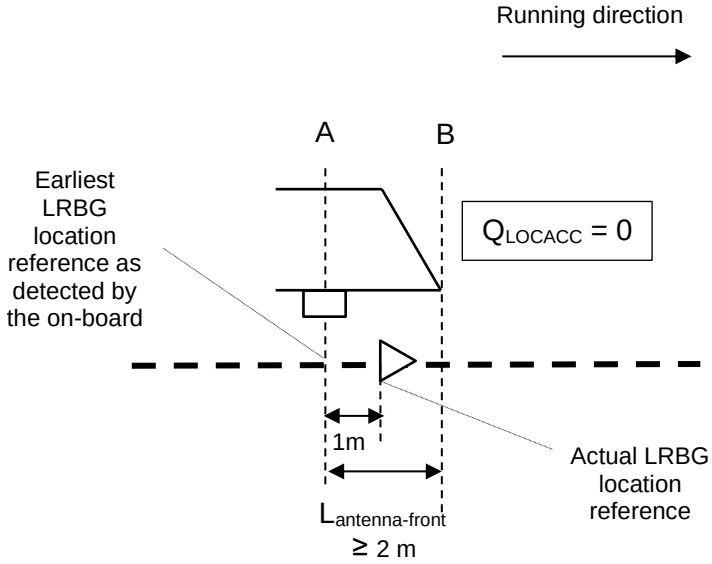
Hazard ID	ETCS-H0102
Hazard headline	Restrictive national values which have been received from balise group marked as unlinked and which are applicable for a further location can no more be supervised after SoM
Hazard description	There is the following hazardous scenario: The train is running with an unknown train position or in SL with an invalid train position.  The train encounters a balise group marked as unlinked which provides national values for application at a further distance i.e. the D_VALIDNV variable in the packet 3 provided by this balise group is different from zero (it is e.g equal to 1000 m). Before reaching the location where the received national values will become applicable, the ERTMS/ETCS on-board enters the SB mode due to the desk closing or in SL due to the disappearance of the “go sleeping” signal with the train being at standstill. The entry in SB mode does not delete nor invalidate the not yet applicable national values: they are kept unchanged as per §4.10 in Subset-026 v2.3.0, v3.4.0 and v3.6.0 . The desk is then opened and a new SoM procedure starts. If the on-board does not consider that this SoM procedure is performed with a valid position (because the train position has not been validated when encountering the balise group marked as unlinked which provided the national values), a deletion of the train position may take place during the SoM procedure or at the end of it: • following E10, E12, E30, E31, E32, • following 5.4.5.3 a), 5.4.5.3. f) or 5.4.5.3. g), • in step A24 or A39. In case the on-board would apply the deletion of the stored position data due to one of the cases listed above also to the train position vs the balise group marked as unlinked which provided the national values (see above), the on-board will no more be able to detect that the train has reached the location where these national values becomes applicable. The train could therefore run without using the appropriate national values. This can have a safety impact.
Proposed Mitigation	In case the trackside provides national values which are applicable for a further location, it should provide at this “further location” a BG repeating the national values and requesting their immediate application, i.e. with D_VALIDNV = 0 or “now”.
Mitigation allocated to	TRACKSIDE

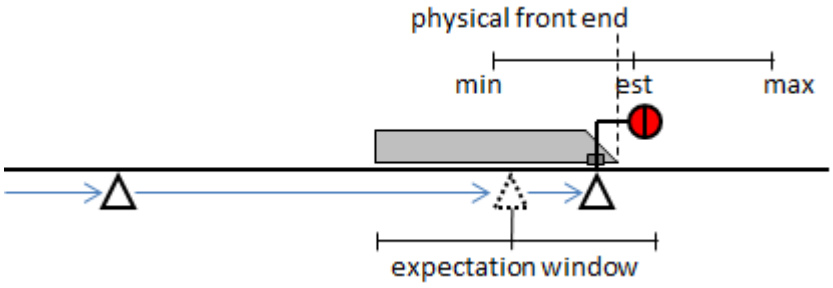
[5] Note: This hazard reflects the opinion of ERA and EUG. For the UNISIG opinion please refer to the corresponding BCA report.

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.103 ETCS-H0103

Hazard ID	ETCS-H0103
Hazard headline	Delay on the entry in Trip mode in Release Speed monitoring
Hazard description	SUBSET-026 § 3.6.4.2 says that the confidence interval shall take into account: a) On-board over-reading amount and under-reading amount (odometer accuracy plus the error in detection of the balise group location reference) b) The location accuracy of the LRBG The point a) might be misread into thinking that when the on-board has just finished processing a BG message, at that moment the train will be “for sure” located within certain “hard limits”. Making reference to the figure below (and for simplicity disregarding the location accuracy of the BG, which is anyway a trackside parameter that the IM can control) trackside engineers (/infrastructure managers) might have done the following reasoning:  1) The LRBG location reference as detected by the on-board can be at most 1 m in rear of the actual location reference of the balise group (location A), as per SUBSET-036 §4.2.10.2 2) Since the distance between Eurobalise antenna and train front is >= 2m (SUBSET-040), the ETCS/ERTMS On-board equipment will consider that it is “physically certain” that the front end is at, or beyond, location B and so it will set the min safe front end not in rear of location B 3) If the EoA is in rear of location B, the train is surely tripped, independently of any odometry inaccuracy defined in Subset-041. So by putting the EoA in rear of location B, the infrastructure manager is sure that by the time the ETCS/ERTMS on-board equipment has processed the balise group message it is sure that the train is tripped. However, the above logic chain does not rely on any explicit on-board requirement implying such hard limit for the determination of the min safe front end. On the contrary: a) Even in case the measured distance would be zero, the over-reading/under-reading amounts (and therefore the “setting of the min safe front end”) mentioned in SUBSET-026 § 3.6.4.2 a) are not limited to the error made in detecting the reference location of the BG. They always include a contribution due to the processing time and odometer accuracy which are used by the BTM to determine

	the LRBG reference location (see SUBSET-036 § 4.2.10.1) and in order to take into account this contribution the 5 m limit is stipulated in the SUBSET-041. b) In addition to a), in case of odometry malfunctioning the over-reading/under-reading amounts in case of zero measured distance can even go beyond the 5m limit that SUBSET-041 defines. In other words, there is no provision in the current specifications that would force the on-board to “discount” such part of the over-reading amount to set the min safe front end at a value that would take into account the "physics" of the train just after a BG has been passed. As a result, the trip that the trackside engineers “was sure to have” at that moment may not happen. The trip may be delayed respect what the trackside engineer thought. Therefore, a hazardous situation could arise if: • The protection of the Supervised Location is not ensured by ETCS in release speed monitoring (release speed fixed value set by trackside), AND • The driver does not respect the EoA (red signal), AND • There is no balise group with order to trip the train in connection with the EoA, AND • The release speed value engineered by the trackside with regards to the risk of passing the Supervised Location (see SUBSET-026 clause 3.13.9.4.5) is not low enough due to the explanation given above.
Proposed mitigation	1.) When performing risk analysis for release speed calculated by trackside the scenario above should be considered. 2.) The trackside could include in the provided linking the opposite direction of the BG As long as the ERTMS/ETCS On-board did not read the BG, the ERTMS/ETCS On-board expects the BG with the “wrong” direction. As soon as the On-board reads the BG, the ERTMS/ETCS On-board will trip according §3.16.2.3.2. In case of an MA prolongation, the trackside provides a new Linking with the correct direction of the BG. Then the train can pass the BG at EoA without tripping. The BG must consist of at least two balises that are not duplicated. This BG must not contain any safety relevant information e.g. National Values. 3.) The trackside could include in the provided Linking a “virtual” BG located close in rear of the BG. The expectation window of the “virtual” BG systematically covers the BG (i.e. using an appropriate value of D_LINK and of Q_LOCACC for the virtual balise). The “virtual” BG has a linking reaction TRIP.  As long as the ERTMS/ETCS On-board did not read the BG, the ERTMS/ETCS On-board still expects the “virtual” BG first and then the BG. As soon as the ERTMS/ETCS On-board reads the BG the ERTMS/ETCS On-board knows that the “virtual” BG was missed and applies the linking reaction of the “virtual” BG as per 3.16.2.3.1c).

<table>
<tr><td></td><td>In case of an MA prolongation, the trackside provides a new Linking without this “virtual” BG. Then the train can pass the BG without tripping.

4). Do not use release speed (use fixed release speed at “0”)

Note for the mitigations 2) and 3): When the train passes the EOA and is tripped, the system status message "balise read error" will be displayed to the driver and the error will be reported to the RBC.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.104 ETCS-H0104

4.104.1.1 Intentionally left empty. No action by application projects is required.

4.105 ETCS-H0105

<table>
<tr><td>Hazard ID</td><td>ETCS-H0105</td></tr>
<tr><td>Hazard headline</td><td>Rejection of safety relevant information due to pending acknowledgement of validated train data</td></tr>
<tr><td>Hazard description</td><td>SUBSET-026 § 3.18.3.4.2 (v3.4.0, v3.6.0) states:
“In case Train Data has been sent to the RBC, and the safe connection is lost before the acknowledgement is received, the Train Data shall be sent again once the safe connection has been re-established within the on-going communication session”.
This means that the on-board repeats the sending of the train data, but only in case there was a loss of safe connection.
However, it is possible that the train data message sent by the ETCS On-Board is not delivered to the RBC even if the safe connection was not lost. The Euroradio protocol may not ensure with the required level of safety that a validated train data message sent by the on-board will be delivered to the RBC application layer. The protocol cannot ensure either that the delivery will not be delayed due to some repetition mechanisms which are included in the protocol.
The delayed (or failed) delivery of the train data message to the RBC may be hazardous due to application by the ETCS On-Board of exception [3] of SUBSET-026 § 4.8.3 as soon as the validated train data are sent to the RBC and as long as the corresponding acknowledgement of train data is not received by the On-board. This exception will filter out more restrictive information received by the On-Board like a shorter MA.
As an example, the following scenario would be hazardous:
- While running with an MA, Train Data are changed by external sources without leading to a brake intervention, AND
- The Train Data message is delayed (or lost) because of radio problems not so severe to cause the release of the safe connection radio connection, AND
- A more restrictive RBC message is sent, AND
- The more restrictive RBC message is able to reach the on-board (even though the radio connection is not healthy) and is rejected due to the absence of RBC acknowledgement of the Train data message.
If the time passed between the first sending of the restrictive message and the repetition of the same message due to the reception of the train data packet is higher than T_NVCONTACT, the safety target may no longer be achieved.</td></tr>
<tr><td>Proposed mitigation</td><td>No realistic trackside mitigation found. It must be evaluated in the projects whether the residual risk can be accepted.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.106 ETCS-H0106

Hazard ID	ETCS-H0106
Hazard headline	A train fitted with a B3 on-board is running faster than allowed due to a replacement of the “Cant Deficiency SSP” by the “Other specific category” not expected by B2 trackside
Hazard description	In B3 there was a major “fix / enhancement” with respect to B2, about the usage of train categories: a B3 on-board is capable of a more refined usage of the speed profiles vs the train categories it belongs to, but it has also to be able to run on B2 (or B3 X=1) Trackside and this is why Ch6 defines how on-board shall translate the X=1 “NC_DIFF” value it receives into the triad of X=2 values for “Q_DIFF/NC_CDDIFF/NC_DIFF”. The translation defined in Ch.6 is however such that it is possible, with the same train data and on the same piece of track, that a B3 on-board follows a different SSP than a B2 on-board. If a B2 trackside engineers, on the same piece of track, SSPs for: 1. A “cant deficiency” train category. Example, for a “80 mm CD” train (in 230d this was called “International Train Category 2”): SSP for NC_DIFF = 1. 2. A “non-cant deficiency” train category. Example, for “Passenger Train” (in 230d this was called “International Train Category 12”): SSP for NC_DIFF = 11. The result for an on-board fitted in a train belonging to both categories (in our example an “80 mm CD” train of type “Passenger”) is that, upon reception of such SSPs: 1. A 230d on-board would select the most conservative between the 2 speed profiles. 2. A B3 on-board would use the 2nd speed profile (the one for “passenger train”). If the speed profile that trackside engineers for the “passenger train” is faster than the one for the “80 mm CD train”, a train equipped with a B3 on-board can run faster than the same type of train equipped with a B2 on-board. This may result in a safety issue: the train may be allowed to run faster than the B2 trackside intended. Important note: the above scenario is also relevant in case SSPs are sent from a B2 ACC RBC to a B2, B3MR1 or B3R2 HOV RBC, which in turn forwards them to the B3 on-board.
Proposed Mitigation	Trackside to design or re-design the SSPs considering the B3 on-board behaviour resulting from translation [3] of SUBSET-026 v3.4.0 and 3.6.0 §6.6.2 and the warning of SUBSET-026 v3.4.0 and 3.6.0 §6.5.1.2.9.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	n/a	Y	Y
	B3MR1, X=1	N*	N**	N**
	B3MR1, X=2	n/a	n/a	n/a
	B3R2, X=1	N*	N**	N**
	B3R2, X=2	n/a	n/a	n/a

TRACKSIDE		ACC RBC				
		B2	B3MR1, X=1	B3MR1, X=2	B3R2, X =1	B3R2, X=2
HOV RBC	B2	Y	N***	N****	N***	N****
	B3MR1, X=1	Y	N***	N****	N***	N****
	B3MR1, X=2	Y	N***	N	N***	N
	B3R2, X=1	Y	N***	N****	N***	N****
	B3R2, X=2	Y	N***	N	N***	N

*the on board does not make a substitution

** see SUBSET-026 v3.4.0 and 3.6.0 §6.5.1.2.9

*** assuming that the SUBSET-026 v3.4.0 and 3.6.0 §6.5.1.2.9 also applies for the data transmitted through the RBC-RBC interface

**** see SUBSET-039 v3.1.0 and 3.2.0 §6.2.4.3.1.1

4.107 ETCS-H0107

<table>
<tr><td>Hazard ID</td><td>ETCS-H0107</td></tr>
<tr><td>Hazard headline</td><td>A train is running faster than allowed due to not considering the basic SSP</td></tr>
<tr><td>Hazard description</td><td>
The B2 on-board mechanism for selecting the SSP from the ones sent by Trackside is such that if train belongs to at least one international train category the on-board will select the most restrictive speed defined for each segment of the track by the specific SSP categories matching (“exact match”) the train categories it belongs to.

So, if trackside sends specific SSP(s) of which at least one is for an international train category that matches one to which the train belongs to, this train would ignore the basic SSP.

For trains fitted with a B3 on-board running on a trackside operated with the system version X=1, the translation of the packet 27 stipulates that in case any other other specific SSP included in the packet 27 matches one to which the train belongs to, it will also lead the on-board to ignore/replace the basic SSP.

This means that if the basic SSP is engineered to be the most conservative speed profile, this train will not follow the most conservative speed profile.

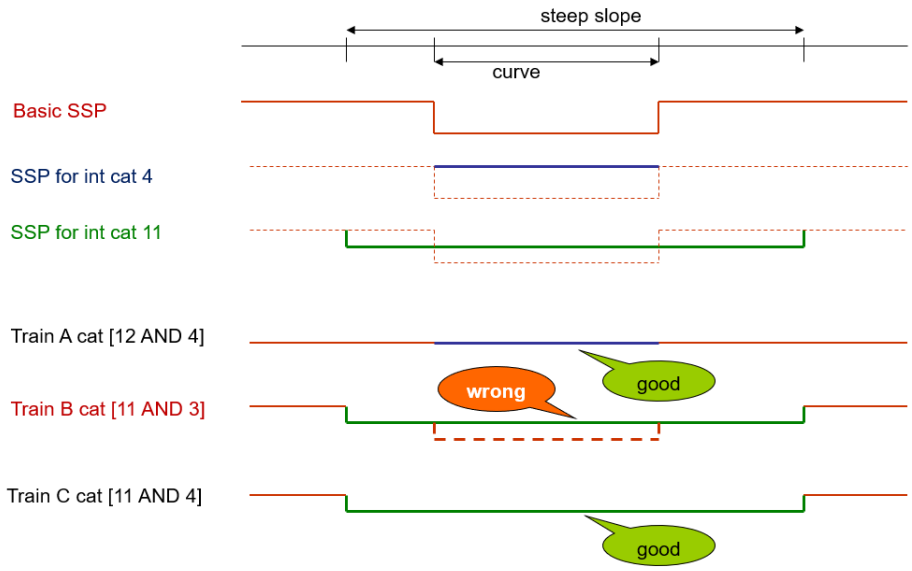
Let’s consider a line section that includes a steep slope, and a curve inside that.

For the curve, trackside sends a “conservative” basic SSP calculated for train with “bad” performance in curves (80 mm admissible cant deficiency), and a faster SSP calculated for trains with “good” performance in curves (130 mm CD).

For the steep slope, trackside sends a speed restriction intended for freight trains braked in G position.

Three types of train run on the line:
<table>
<tr><td></td><td>Brake position</td><td>Admissible cant deficiency</td><td>Resulting international train categories in 230d</td></tr>
<tr><td>Train A</td><td>Passenger in P</td><td>130 mm</td><td>12 and 4</td></tr>
<tr><td>Train B</td><td>Freight in G</td><td>100 mm</td><td>11 and 3</td></tr>
<tr><td>Train C</td><td>Freight in G</td><td>130 mm</td><td>11 and 4</td></tr>
</table>

The result:
</td></tr>
</table>



The OBU of train B ignores the basic SSP, because trackside has sent SSP matching one of the train categories train belongs to. By doing this, in the curve the train can run at a speed that is too high for its suspensions design. The basic SSP (computed for 80 mm CD) would have been on the safe side for this train, but the OBU ignores it, resulting in a hazard.

Proposed Mitigation

Trackside engineering that intends to use specific SSPs shall be aware that a B2 OBU or a B3 OBU running on a B3 X=1 trackside will ignore the basic SSP in case it receives at least one specific SSP (for B2) or one other specific SSP (for B3 X=1 trackside) matching one of the international train categories the train belongs to, with possible hazardous consequences (overspeeding).

In the example used for the hazard description, which illustrates what should not be engineered according to the clause §3.11.3.2.3.1 of SUBSET-026 v2.3.0 modified by SUBSET-108 v1.2.0 and to the clause §6.5.1.2.9 of SUBSET-026 v3.4.0 and v3.6.0, trackside would have avoided the safety issue if it had sent also a specific SSP applicable to international train category 3.

Mitigation allocated to

TRACKSIDE or EXTERNAL

Relevant in ETCS baseline

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	N	N
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	N	N

4.108 ETCS-H0108

<table>
<tr><td>Hazard ID</td><td>ETCS-H0108</td></tr>
<tr><td>Hazard headline</td><td>A B2 train is running faster than allowed due to not taking into account the trackside “Cant deficiency” SSP applicable to a “Cant deficiency” category lower than its own category</td></tr>
<tr><td>Hazard description</td><td>
In B2 the mechanism for selecting the SSP from the ones sent by Trackside is such that an on-board would consider specific SSPs only if related to internat ional train category(ies) exactly matching the ones that the train belongs to.

In the case of the 230d international train categories related to “maximum admissible cant deficiency”, this “exact matching” means that if a train has a certain maximum cant deficiency, it will ignore an SSP related to a value of CD lower than its own – even if from a physical point of view it would be able to use it safely.

The above train if it does not receive an SSP for a cant deficiency exactly matching its own, it would use the basic SSP.

But it is nowhere specified that the basic SSP must be the most conservative one and so it is possible to have a safety issue by following a too permissive speed profile.

Example

Let’s consider a line section that includes a curve, for which the trackside sends SSPs tailored for a limited number of different cant deficiency categories:
<table>
<tr><td></td><td></td><td>NC_DIFF</td><td>V_DIFF</td></tr>
<tr><td>international train category 3</td><td>Cant Deficiency 100 mm</td><td>2</td><td>80 km/h</td></tr>
<tr><td>international train category 5</td><td>Cant Deficiency 150 mm</td><td>4</td><td>120 km/h</td></tr>
<tr><td>international train category 6</td><td>Cant Deficiency 165 mm</td><td>5</td><td>140 km/h</td></tr>
</table>
Trackside also sends the mandatory basic SSP. In this example, trackside computed it for a train of 140 mm CD:
<table>
<tr><td></td><td></td><td>V_STATIC</td></tr>
<tr><td>Basic SSP</td><td>Calculated for 140 mm of CD *</td><td>110 km/h</td></tr>
</table>
[*the chosen value does not correspond to a train category, but the example is valid also choosing an existing train category that the trackside chooses not to use]

Let’s assume a train having 130 mm of admissible cant deficiency arrives, and the maximum speed its suspensions allow in that curve is 100 km/h:
<table>
<tr><td></td><td>Admissible cant deficiency</td><td>Max speed in that curve</td><td>International train category in 230d</td></tr>
<tr><td>Train</td><td>130 mm</td><td>100 km/h</td><td>international train category 4</td></tr>
</table>
This train does not receive an SSP exactly matching its CD, and so according to the B2 mechanism (see §3.11.3.2.2 of SUBSET-026 2.3.0 modified by SUBSET-108 v1.2.0) selects the basic SSP of 110 km/h – which is too fast for its suspensions. This is hazardous.

Note: in Baseline 3 the mechanism of selecting SSP was changed, and train would have selected the “best safe approximation” CD SSP, in our example by selecting the specific SSP
</td></tr>
</table>

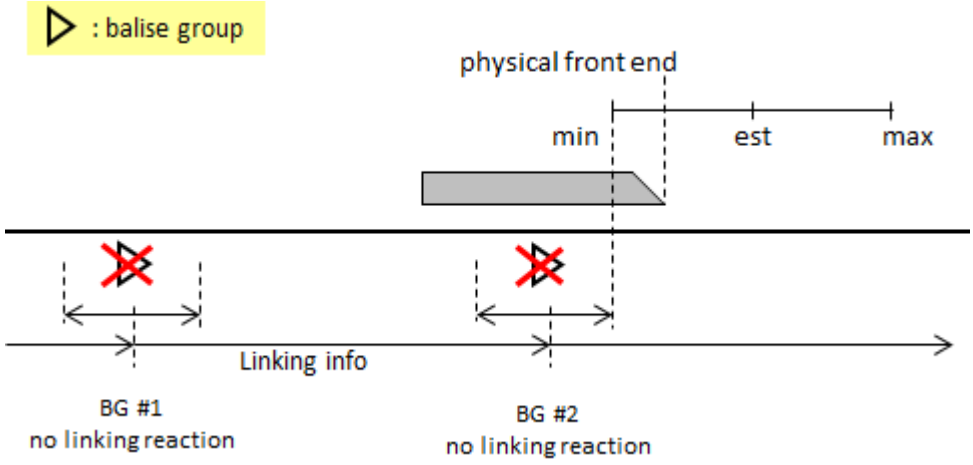
<table>
<tr><td></td><td>for CD 100 mm. The train would be obliged to run slower than what its suspensions are capable of, but on the safe side.</td></tr>
<tr><td>Proposed Mitigation</td><td>Trackside engineering that intends to use specific SSPs shall be aware that if the basic SSP is not conservative, this may have possible hazardous consequences (over speeding), because a B2 OBU will use the basic SSP in case there are no exact matching between at least one of the international train categories the train belongs to and the specific SSPs used by trackside.

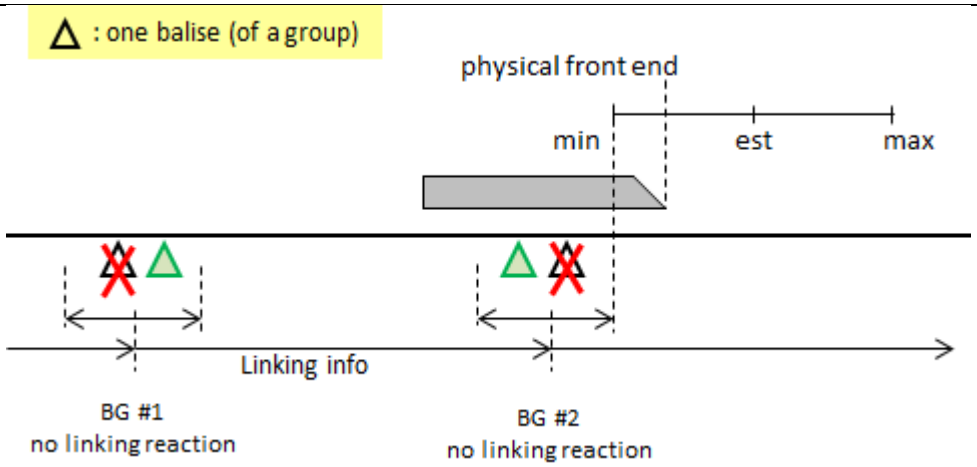
In the example used for the hazard description, trackside would have avoided the safety issue if it had sent also a specific SSP applicable to international train category 4, or if the basic SSP was engineered for the “lowest performant in curve” train.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE or EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N</td><td>N</td></tr>
</table>
</td></tr>
</table>

4.109 ETCS-H0109

4.109.1.1 Intentionally left empty. Hazard entry under analysis.

4.110 ETCS-H0110

Hazard ID	ETCS-H0110
Hazard headline	Unclear specification of "balise detection degradation" function
Hazard description	SUBSET-026 §3.16.2.7.1.1 (for v2.3.0, v3.4.0, and v3.6.0) reads: ***3.16.2.7 RAMS related supervision functions*** *3.16.2.7.1 Mitigation of balise reception degradation* *3.16.2.7.1.1 If 2 consecutive linked balise groups announced by linking are not detected and the end of the expectation window of the second balise group has been passed, the ERTMS/ETCS on-board shall command the service brake and the driver shall be informed. At standstill, the location based information stored on-board shall be shortened to the current position. Refer to appendix A.3.4 for the exhaustive list of information, which shall be shortened.* … uses the word "*detect*" in relation to "*balise groups*". This may lead to a trackside expecting a specific reaction, which could not be performed by the on-board as described below. **Possible trackside expectation:** Two consecutive balise groups BG #1 and BG #2 contain safety related information but no Linking Reaction is used for these two BGs. Both BGs consist of two non-duplicated balises. If the information cannot be transmitted via one of the balise groups, the other balise group serves as a fall-back. For the case that the information cannot be transmitted via any of the two balise groups, the trackside may expect that the service brake is applied when "the end of the expectation window of the second balise group has been passed" as per SRS clause 3.16.2.7.1.1.  **Possible on-board behaviour:** For the case that in both BGs one balise out of the group is malfunctioning while the other one works properly, the information will not be taken into account at all (neither via BG #1 nor via BG #2) due to the SRS clause 3.16.2.4.1.

	 Since the ERTMS/ETCS on-board detects one balise out of each balise group the on-board concludes that SRS clause 3.16.2.7.1.1 ("If 2 consecutive linked balise groups announced by linking are not detected …") does not apply. It shall be noted that the “missing” of the balise in the second group may become systematic in case of “interleaving”, that is if: • the “missed” balise of BG#2 is located between the two balises of the BG#1, or • the “missed” balise of BG#2 is located between the balises of a further announced BG. In the above cases the “missing” would occur but not because of a failure of the balise or of the reader function: the telegram is received, but the onboard would consider it “missed” because of the ambiguities described by CR1354. **Consequence:** The ERTMS/ETCS on-board will not apply the service brake although the safety related information was missed (rejected) from both BGs.
Proposed mitigation	The trackside should not rely on the function "Mitigation of balise reception degradation" when two consecutive BGs contain redundant safety related information but are announced by linking with neither a service brake reaction nor a trip reaction. Alternatively, the trackside should use appropriate linking reaction, e.g. in level 1 define a “Service brake” linking reaction for the second announced BG and update linking information when the first announced one is properly received, to ensure that the on-board will command the application of the service brake when the information from two successive announced BGs is missed. The trackside should not interleave balises from different balises groups.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.111 ETCS-H0111

Hazard ID	ETCS-H0111
Hazard headline	Potential safety issues due to non-compliance with the performance requirement for the accuracy of the distance measured on board
Hazard description	SUBSET-041 v.3.2.0 §5.3.1.1 defines a performance requirement for distances measured on-board (± (5m + 5%) of the travelled distance). In addition the following note is included in the requirement: *Also in case of malfunctioning the on-board equipment shall evaluate a safe confidence interval.* SUBSET-091 provides the following base event ODO-4: *The confidence interval for distance measurement does not include the real position of the train* It has not been analysed systematically if respecting ODO-4 also ensures overall system safety. The increasing of confidence interval (CI) may postpone or reduce the effect of the safety protection. There are several possible hazardous situations resulting from non-compliance with the performance requirement. This is related to: • Minimum safe front end (minSFE) • Maximum safe front end (maxSFE) • Estimated front end (estFE) The Appendix D identifies potential failures which need to be mitigated in order to avoid the hazardous situations and it also gives example of mitigations. **Conclusion:** 1. For scenarios with enlarged CI combined with route revocation/route cancellation a remaining risk exists (see scenario estFE_1, maxSFE_3). 2. For scenarios with enlarged CI combined with more than one mode profile sections a remaining risk exists (see scenario maxSFE_2). 3. For scenarios where ETCS does not have the full technical responsibility for protection (modes SR, SH) the protection applicable in case of driver failure may be delayed or not working at all. Remaining risk exists (see scenario minSFE_3, minSFE_4, maxSFE_1). 4. Scenario minSFE_1 is covered by hazard ETCS-H0001. 5. Scenario minSFE_2 is covered by safety analysis – see SUBSET-091. An ERTMS/ETCS On-board which violates the performance requirement permanently is not covered by this analysis. Note: The probability of growing CI depends on train characteristics (slip / slide) and degraded situations.
Proposed mitigation	For the scenarios as summarized in the conclusion #1 and #2 the ERTMS Trackside specific application project / infrastructure manager should show that the remaining risk is acceptable. Appendix D contains examples of mitigations for the scenarios there described.
Mitigation allocated to	EXTERNAL

Relevant in ETCS baseline					
			ERTMS/ETCS On-Board		
			B2	B3MR1	B3R2
	Trackside	B2	Y	Y	Y
		B3MR1, X=1	Y	Y	Y
		B3MR1, X=2	Y	Y	Y
		B3R2, X=1	Y	Y	Y
		B3R2, X=2	Y	Y	Y

4.112 ETCS-H0112

Hazard ID	ETCS-H0112
Hazard headline	Unexpected ERTMS/ETCS On-Board mode/level resulting from trackside order containing immediate level transition together with MA and mode profile
Hazard description	An ETCS on-board equipment may end up in an unexpected for trackside combination of level and mode when receiving other information together with an immediate level transition order, as explained in the following scenarios. The following hazardous scenarios have been identified: **Scenario 1 – ERTMS/ ETCS On-board in L1 or L2 with L0/LNTC LTO and SH mode:** Scenario 1a: An ERTMS/ETCS On-board in Level 1 mode FS/LS/OS passes over a BG containing: • an immediate order to switch to Level 0 (or NTC), and • an MA with a shunting mode profile for current location. Scenario 1b: An ERTMS/ETCS On-board in Level 2 mode FS/LS/OS receives a radio message containing: • an immediate order to switch to Level 0 (or NTC), and • an MA with a shunting mode profile for current location. The expectation of the trackside is that the ERTMS/ETCS On-board switches to Level 0 (in the case of order to L0) and mode SH. However, depending on the sequence in which an on-board will actually process the information contained in the BG (this being caused by different interpretation of SUBSET-026 § 4.8.1.3.1 and by the absence of other clauses that impose an execution sequence of the information), the ERTMS/ ETCS On-board could end up in any of the following Level/Mode combinations (in the case of order from L1 to L0): 1. L0/SH, or 2. L0/UN, or 3. L1/SH delaying the execution of the level transition until either the SH or PS mode is left, or 4. L1/SH without any level transition stored Note: The above is applicable by analogy with transition order to LNTC but noting that LNTC SH is only possible in B3. Potential hazardous scenario could be if the train does not enter SH mode in such a way that the permitted speed is higher than expected (see case 2 above). For the cases 3 and 4 above, the driver could be misled and apply operational rules for L1 instead of L0/LNTC. The potentially hazardous impact of applying operational rules for L1 instead of L0/LNTC should be evaluated by specific ERTMS/ETCS application project. **Scenario 2 – ERTMS/ ETCS On-board in L2 with L1 LTO and SH mode:** An ERTMS/ETCS On-board in Level 2 mode FS passes over a BG containing: • an immediate order to switch to Level 1, and

<table>
<tr><td></td><td>

- an (L1) MA with a shunting mode profile for current location.

The trackside expectation is that the ERTMS/ETCS On-board switches to Level 1 and mode SH.

However, depending on the interpretation of SUBSET-026 § 4.8.1.3.1, the ERTMS/ETCS On-board could end up in any of the following level/mode combinations:

1. L1/SH, or
2. L2/SH delaying the execution of the level transition until either the SH or PS mode is left, or
3. L2/SH without any level transition stored

For the cases 2 and 3 above, the driver could be misled and apply operational rules for L2 instead of L1. The potentially hazardous impact of applying operational rules for L2 instead of L1 should be evaluated by specific ERTMS/ETCS application project.
</td></tr>
<tr><td>Proposed mitigation</td><td>

The trackside should not combine in the same message an SH mode profile together with an immediate LTO (or a conditional LTO) causing:

- a transition from level 1 or 2 to level 0/NTC (scenario 1)
- a transition from level 2 to level 1 (scenario 2)

For scenario 2 only: alternatively, the remaining risk of applying operational rules from different level should be evaluated by ERTMS/ETCS specific application project.
</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>

<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>

</td></tr>
</table>

4.113 ETCS-H0113

4.113.1.1 Intentionally left empty. No action by application projects is required.

4.114 ETCS-H0114

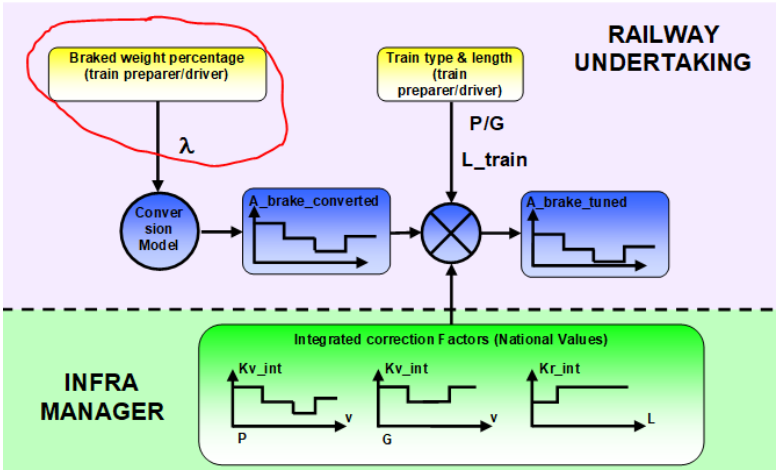
<table>
<tr><td>Hazard ID</td><td>ETCS-H0114</td></tr>
<tr><td>Hazard headline</td><td>Missing train interface (TI) command because of inappropriate speed and distance supervision status</td></tr>
<tr><td>Hazard description</td><td>When the train is in target speed monitoring (TSM), the maximum safe front end is in rear of the indication location, and the train speed is above the current most restrictive speed profile (MRSP), the appropriate supervision statuses (i.e. overspeed status, warning status, intervention status) are not entered and the resulting TI commands (if any) are not triggered.

One example of how to arrive to such a situation is the following:

1. The train is in ceiling speed monitoring (CSM) approaching a target.
2. The max safe front end passes the indication supervision limit for the target, train changes to target speed monitoring (TSM: indication status).
3. A new LRBG is detected leading to the reset of the train position confidence interval and to the relocation of the target. As a result, the max safe front end is no longer beyond the indication supervision limit for the target.
4. The train overpasses the MRSP but all changes of status and corresponding TI commands related to the ceiling limits are not triggered, because (d_I (Vest) < d_max safefront) is not fulfilled (see clause §3.13.10.4 - table 8 or table 9, triggering conditions # t6, t9, t12 and t15 of SUBSET-026 v3.6.0).

It should be noted that the time/distance window, during/within which the relevant supervision statuses will not be triggered as highlighted in step 3, depends on the train speed and on the size of the confidence interval when the step 2 occurs.</td></tr>
<tr><td>Proposed mitigation</td><td>No realistic mitigation found.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y*</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N</td><td>Y</td></tr>
</table>
Hazard exists in B3R2 due to introduction of CR1249 in the ETCS specifications.
*) Only if Baseline 2 Requirements For Implementation Of Braking Curves Functionality as per version 4.0 or higher of document ERA_ERTMS_040022 “Baseline 2 requirements for implementation of braking curves functionality” are implemented</td></tr>
</table>

4.115 ETCS-H0115

Hazard ID	ETCS-H0115
Hazard headline	Unsafe speed and distance supervision due to the input in the ERTMS/ETCS On-Board of a braked weight percentage value obtained according to an “old” version of UIC leaflet 544-1.
Hazard description	For the so called “lambda trains”, the SRS define a “conversion model” that uses as input the braked weight percentage (usually referred to by the Greek letter “λ” - lambda) value of a vehicle or train composition and converts it into an emergency brake deceleration profile which is used by the on-board as element for the supervision of speed and distance.  According to SUBSET-026 v3.6.0 note §3.13.2.2.5.2, the conversion model needs values of λ obtained from characterising a vehicle as per the 6th edition of the UIC leaflet 544-1. In the v3.4.0 of the SUBSET-026, there is no mention of which version of the leaflet shall be used. In the frame of the CCM discussion of rejected CR1361, the UIC brake experts further clarified that the lambda values would be correct for use with the conversion model provided that the vehicle is characterised according to the 4th, 5th, or 6th edition of the leaflet. But if the vehicle is characterised according to an older version of the leaflet, the output of the “conversion model” would be incorrect. This is because the value of lambda obtained as per the 3rd edition is generally higher than the one established with the 4th edition. In an example presented in the mentioned CCM discussion, a 15-coach train set whose lambda was assessed to be 145 % using the 3rd edition, when re-assessed according to the 4th edition showed a lambda value of 131 %. This means that if a Railway Undertaking had characterised some vehicles (for example, freight wagons) using the version 3 of the leaflet, the related lambda value if used as input for the conversion model (typically by the driver at start of mission) would lead to an unsafe speed and distance supervision by the ERTMS/ETCS on-board.
Proposed mitigation	The Railway Undertaking shall ensure that if a vehicle is intended to be used in composition with a train equipped with an ERTMS/ETCS on-board, it shall be assessed according to the UIC leaflet 544-1 edition 4 or 5 or 6. This means that if for example a vehicle had been characterised with version 3 of leaflet, it shall be re-characterised to get the “correct” lambda value.
Mitigation allocated to	EXTERNAL

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N*</td><td>Y</td><td>N**</td></tr>
<tr><td>B3MR1, X=1</td><td>N*</td><td>Y</td><td>N**</td></tr>
<tr><td>B3MR1, X=2</td><td>N*</td><td>Y</td><td>N**</td></tr>
<tr><td>B3R2, X=1</td><td>N*</td><td>Y</td><td>N**</td></tr>
<tr><td>B3R2, X=2</td><td>N*</td><td>Y</td><td>N**</td></tr>
</table>
* for the “early implementation” of braking curves according to ERA_ERTMS_040022
** because the v360 of the SRS mentions the sixth edition of the UIC leaflet
</td></tr>
</table>

4.116 ETCS-H0116

Hazard ID	ETCS-H0116
Hazard headline	Linking consistency reaction not applied as expected from trackside.
Hazard description	In the rules related to linking function the condition when ERTMS/ETCS on-board equipment shall stop expecting a balise group in the linking could be unclear due to the misleading term "the expected balise group is found". The clause 3.4.4.4.6 in SUBSET-026 (both v3.4.0 and v3.6.0), and especially its bullet a), intends to specify when to stop expecting a balise group and to expect the next one. The formulation “the balise group is found inside its expectation window” could be considered as fuzzy, in the sense that it could be understood as “the location reference balise of the balise group is found and is inside the expectation window” or as “the whole balise group has been found with its location reference inside the expectation window”. On the other hand, this clause 3.4.4.4.6, being covered by the clause A.3.3.1 and A.3.3.2 ,could be interpreted that when the term “balise group” is used in such a clause, it means a balise group whose content has passed all the filters, i.e. at least when all the balises from the group have been found (inside the expectation window). Likewise, the application of the clause 3.16.2.4.1 (check of BG message consistency if linking information is used) could depend on how the OBU interprets the term "balise group found in the expected location". Regarding 3.4.4.2.1.1, it is unclear if the status “linking is used” can change before all the balises of the last announced BG are read. These ambiguities could lead OBU to apply reaction to linking consistency check differently from how trackside expects it (see following scenarios). Scenario 01 The last announced BG is crossed in nominal direction and the confidence interval is small, the OBU exits the expectation window (i.e. when the min safe antenna position has reached the last possible location of the balise group location reference) before the last balise(s) of a BG is (are) still to be encountered. In this case OBU might behave setting the condition “linking information is used” to false (see 3.4.4.2.1.1), so that the 3.16.2.3.1 is not applicable anymore. Since OBU is still waiting for another balise to complete the BG’s message, OBU would apply the balise group message consistency check in the scope of the clause 3.16.2.4.4 (no linking information is used), instead of 3.16.2.4.1 (linking information is used) thus degrading the reaction to data check inconsistency from ‘Train Trip’ to ‘service brake application’ up to standstill. Scenario 02 The last announced BG is crossed in nominal direction and, while expecting it, OBU finds the location reference inside the expectation window and, due to the ambiguity in 3.4.4.4.6 a), immediately stop supervising the expectation window and set the condition “linking information is used” to false (see 3.4.4.2.1.1), so the 3.16.2.3.1 is not applicable anymore. But since the OBU is still waiting for another balise to complete the BG’s message, OBU would apply the balise group message consistency check in the scope of the clause 3.16.2.4.4 (no linking information is used), instead of 3.16.2.4.1 (linking information is used) thus degrading the reaction to data check inconsistency from ‘Train Trip’ to service brake application up to standstill. Note: OBU behaviour in scenario 01 is identical to scenario 02 but here the reason for OBU wrong application of 3.16.2.4.4 instead of 3.16.2.4.1 is a possible interpretation of 3.4.4.4.6.a).

<table>
<tr><td></td><td>
Scenario 03
A balise group announced and crossed by OBU in reverse direction contains safety related information and the balise N_PIG = 0 is out of service. The OBU, due to its interpretation of the term “the balise group is found in the expected location”, could consider that the clause 3.16.2.4.1 does not apply because the balise N_PIG = 0 has not been received within the expectation window. As a result it does not react immediately after having travelled the maximum allowed distance between balises (12m) from the balise with N_PIG = 1, and could continue to wait for the location reference balise N_PIG = 0 if the end of the expectation window has not been reached yet.
In this situation, by virtue of the clause 3.16.2.3.1 b), the OBU reacts only when the min_SFE of the train reaches the end of the expectation window and, under a reasonable large confidence interval, OBU reaction could occur at distance much greater than 12m. Hazardous situation could arise if trackside design expects a safety reaction 12m after the last but one balise in the group.

Scenario 04
A balise group is announced with repositioning and a BG is found with one balise of the Group, containing the repositioning information, being out of order. According 3.4.4.4.2.1 only a BG containing repositioning information valid for the train orientation would fit to the definition of 3.16.2.4.3 “…included in the linking information”. On-board will consider the found BG as not included in the linking information and according 3.16.2.4.3 would not apply a linking reaction (still waiting for a repositioning BG). However the balise being out of order contained the repositioning information and the corresponding expected linking reaction according 3.16.2.4.1 a) is not applied.
</td></tr>
<tr><td>Proposed mitigation</td><td>
Scenario 01+02: The last announced BG should not have link reaction ‘Train Trip’, i.e. if you have such a BG then you must always announce a further BG (which does not have link reaction ‘Train Trip’, or else is located beyond the SvL so it will not expected to be encountered anyway). Note: this mitigation would not eliminate completely the hazard in case an MA is shortened on-board to a location in rear or the last BG for example due to timer expiry.
Scenario 03: In case where BGs require a safety reaction after 12m, trackside could install an additional announced BG having its reference balise within the 12m (3.16.2.3.1c would apply).
Scenario 04: Trackside should avoid engineering of information where missing/ignoring of the BG could lead to hazardous consequences. Duplication of the balise containing repositioning information is also a mitigation, provided that the BG is made up of at least 3 balises.
</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.117 ETCS-H0117

<table>
<tr><td>Hazard ID</td><td>ETCS-H0117</td></tr>
<tr><td>Hazard headline</td><td>Protected point overpassed due to Override end condition not applied when expected</td></tr>
<tr><td>Hazard description</td><td>SUBSET-026 v.3.6.0 §5.8.4.1c) identifies the following condition to end the Override procedure:
The former EOA/LOA has been passed with the min safe antenna position (calculated by subtracting distance between active EUROBALISE antenna and the front end of the train from the min safe front end position)
In addition, SUBSET-026 v.3.6.0 §3.6.1.3 defines train confidence interval always related to an LRBG and therefore in case the train position is unknown it is unclear how the on-board shall determine the confidence interval.
A hazardous situation has been identified in case the following scenario happens:
• A start of mission is performed in L2 or L3 and there is no LRBG stored on-board.
• Driver activates Override procedure.
• With the train in SB mode, its former EOA would be the current position of the train front (SUBSET-026 v3.6.0 §5.8.3.1.1).
• Since it is unspecified how the on-board shall determine the confidence interval, the end of override via condition §5.8.4.1c) can happen at a later place/moment than expected by trackside.
In case there is a protective measure engineered by trackside to Trip the train when it is not in Override procedure (e.g. BG giving “Stop if in SR mode”, or use of a finite SR distance), it would not be applied due to the train unexpectedly remaining with Override active.
Note: in the case of a finite SR distance, the hazard would arise from delaying the transition to trip [42]. This is more relevant for a B2 on-board, because in B3 there is an EBD curve at the end of the SR distance supervised with the max safe front end whereas in B2 this was not defined. In addition, in the case of a finite SR distance the hazard can occur only if other conditions like 5.8.4.1a or b are not fulfilled before the SR distance is reached.</td></tr>
<tr><td>Proposed mitigation</td><td>ERTMS/ETCS specific application shall evaluate if the remaining risk is tolerable.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE + EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td></td><td></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td>Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.118 ETCS-H0118

Hazard ID	ETCS-H0118
Hazard headline	List of available levels after transition announcement
Hazard description	This hazard concerns the table of priority of trackside supported levels (table of trackside supported levels) stored on-board which controls the levels that the driver is able to select. Once a driver has passed a level transition announcement, in the event that the train stops before the level transition border and the driver changes cab (perhaps because the driver realises, he is not authorised to enter a L2 area), or also without changing cab but continuing in the same direction, which table of priority of trackside supported levels is available to the driver? After receiving a level transition announcement, the SUBSET-026 is not clear on the status of the old table of priority of trackside supported levels: - Are there two tables of priority of trackside supported levels stored on-board once passing the transition announcement? - Is the new list applied as the current table of priority of trackside supported levels, before reaching the level transition order? - When is the old table discarded by the ERTMS/ETCS On-board? The clauses 3.18.4.2.5, 5.10.2.2 & 5.10.2.8 may be read so that the table of priority of trackside supported levels received with the announcement is stored and therefore becomes available and applicable as soon as the announcement is received. For that reason there is the possibility that the driver selects a level which is not coherent with the trackside installation at the location where the driver selects the level. So, the inability of the driver to select a level compatible with the trackside due to the fact that system has applied a future table of priority of trackside supported levels is a safety hazard. Note: not related to this specification ambiguity, a similar hazardous situation can occur in case of starting from no power without CMD (or with a CMD that detected movement) because in this case the driver can select any level of the “default list”.
Proposed mitigation	In the vicinity of level transition borders (between the announcement and the border), it should be operationally avoided that the driver is asked to change manually the level or the manual level changes should be performed only in co-operation with signaller, because the signaller should know which train protection system is applicable/active for current train location. If not possible, the manual change of level should occur elsewhere or the trackside should send conditional transition orders in order to confirm the levels supported in the area where the manual level change takes place. If no specific mitigation is found then each trackside application must evaluate whether the risk related to a train that can be moved selecting a level not allowed by trackside as consequence of above described scenario, can be accepted.
Mitigation allocated to	TRACKSIDE

Relevant in ETCS baseline	

		ERTMS/ETCS On-Board		
		B2	B3MR1	B3R2
Trackside	B2	Y	Y	Y
	B3MR1, X=1	Y	Y	Y
	B3MR1, X=2	n/a	Y	Y
	B3R2, X=1	Y	Y	Y
	B3R2, X=2	n/a	Y	Y

4.119 ETCS-H0119

Hazard ID	ETCS-H0119
Hazard headline	Handling of an RBC transition order for a different RBC during an on-going RBC/RBC handover
Hazard description	When a handover from RBC1 to RBC2 is ongoing and the onboard receives a transition order indicating a new RBC (RBC3) as accepting, it is unclear from SUBSET-026 which RBC becomes the handing over one. It can be interpreted to be RBC2 or RBC1, depending whether clause 5.15.1.5 is applied on its own or in conjunction with clause 3.5.3.5.2. This uncertainty on which RBC is the handing over may result in hazardous situations. Let us consider the following scenario: 1. The train is supervised by RBC1 and the route is set into the RBC2 area. 2. RBC1 sends an RBC Transition Order to the ERTMS/ETCS On-board indicating RBC2 as ACC RBC. 3. The ERTMS/ETCS On-board establishes a communication session with RBC2 and then approaches the border to RBC2. 4. The ERTMS/ETCS On-board reports its position to RBC1 and RBC2 with the max safe front end beyond the border[6] and considers RBC2 to be the supervising RBC (§3.15.1.3.5 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0). 5. The route for the train already extends into the RBC3 area, but the rear of the train has not yet left the RBC1 area. 6. While the ERTMS/ETCS On-board is still communicating with RBC1 (HOV RBC), it receives a new RBC transition order, from BG or RBC2, which indicates RBC3 as ACC RBC. 7. According to §3.15.1.3.1 a) of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0, the ERTMS/ETCS On-board establishes a communication session with the ACC RBC (RBC3) and according to §3.5.3.5.2, the ERTMS/ETCS On-board shall not terminate a communication session with the HOV RBC (RBC1). 8. The interpretation of the bullet above could lead to the ERTMS/ETCS On-board establishing a communication session with RBC3 and terminating the communication session with RBC1 (HOV RBC) or RBC2. 9. While the route is set into the RBC3 area and the MA is up to the border RBC2/RBC3, it could occur that the ERTMS/ETCS On-board terminates the communication session with RBC2 (ACC RBC). As a result the onboard is in session with RBC1 and RBC3, and it is unclear which becomes the supervising RBC (normally it should be RBC2).Subsequently, a route revocation/cancellation in the area of RBC2 occurs. • Route revocation cannot be handled by RBC2 and will be potential hazardous. • The train may not be stopped by T_NVCONTACT reaction in case RBC3 sends messages to the on-board. This because it is unclear which RBC the on-board shall consider as the supervising one. In case the on-board considers it to be RBC3, then according to

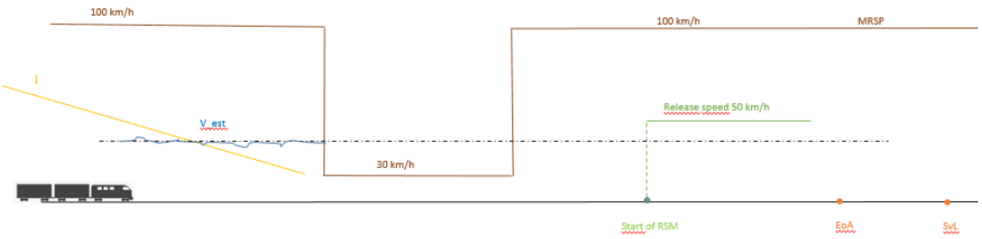
[6] It is assumed that the train has passed the border

<table>
<tr><td></td><td>§3.16.3.4.1.2 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0, a message from RBC3 would reset the T_NVCONTACT supervision.</td></tr>
<tr><td>Proposed mitigation</td><td>Each ERTMS/ETCS specific trackside application must evaluate whether the risk related to a scenario above, can be accepted. The following measures reduce the likelihood of the ERTMS/ETCS On-board receiving an RTO for a further RBC/RBC-border while not having completed the previous RBC/RBC-handover:
The next RBC/RBC-handover announcement should have a distance to the previous RBC/RBC-border corresponding to at least a radio round trip time plus additional times (BG reading time, OBU processing time, RBC processing time, and the time possibly taken by 3 attempts before considering the session with RBC1 terminated) for a train with the maximum train length allowed on the line plus an assumption on the maximum confidence interval
HOV RBC should order the termination of communication session when a position report was received with an LRBG located at or beyond the border (this ensures that the physical front end has passed the border). This however is safe only when the HOV RBC stops handling emergency situations for a train of which the real front end has already left the RBC area.
HOV RBC should order the termination of communication session when the ACC RBC informs the HOV RBC that it has taken over responsibility.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.120 ETCS-H0120

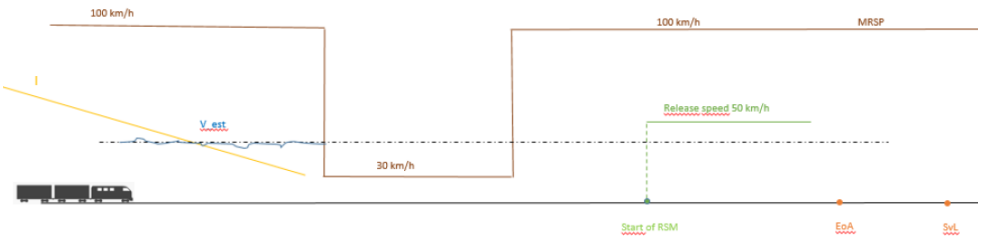
4.120.1.1 Intentionally left empty. Hazard entry under analysis.

4.121 ETCS-H0121

Hazard ID	ETCS-H0121
Hazard headline	Not correct supervision of targets with a speed value lower than the release speed
Hazard description	The term “release speed is supervised” can be understood in different ways in the context of the clause 3.13.10.6.1. One possible interpretation is that this term refers to a situation where the closest indication location corresponds to a supervised target EoA/SvL. Another possible interpretation is that it corresponds to a situation where a release speed “exists”. This last interpretation is problematic because it could lead to not supervising the targets with a speed value lower than the release speed and located between the max safe front end of the train and the start of the RSM area, when the train speed is lower than the release speed, because the conditions for entering in TSM for those targets will not be fulfilled (see SUBSET-026-3, table 16). Please take note that according to this table, and in the case of “a release speed is supervised”, the condition 1 only applies if “the train speed is above or equal to the release speed". The following figure illustrates one example of the conditions that will lead to the hazard 
Proposed mitigation	If it is needed to implement a trackside speed restriction that affects the MRSP (e.g. due to SSP or TSRs) with a speed value lower than the release speed, the value of the release speed should be reduced to the value of the speed restriction Note: This mitigation cannot work if the release speed calculated on board is used, because the trackside cannot know a priori the value of the release speed that the on-board will calculate. It could maybe make an estimation of the maximum value, but even in that case, it would not be easy to provoke the reduction of the value, the only way to mitigate the hazard in this case would be to not allow the speed restrictions lower than this estimated maximum value. The same can be said in case of PBD speed restriction. Other possible mitigations: In case the trackside speed restriction corresponds to a TSR, the TSR should be prolonged up to the EoA location. In this case the value of the release speed will be decreased automatically to the value of the TSR without the need to change the data preparation related to the release speed. This mitigation can be used for the fixed release speed or release speed calculated on board and it is useful when the TSR is not far from the EoA In Level 2/3, the trackside should provide the value of the release speed once the restriction has been passed by the train. This mitigation can be used for the fixed release speed or release speed calculated on board.
Mitigation allocated to	TRACKSIDE+EXTERNAL

<table>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>N*</td><td>N</td><td>Y</td></tr>
</table>
*Y in case the on-board applies the early implementation of braking curves functionality (version 4.0 or later versions)
</td></tr>
</table>

4.122 ETCS-H0122

Hazard ID	ETCS-H0122
Hazard headline	Confusing displayed information related to the targets that have a speed lower than release speed when driving under low adhesion conditions
Hazard description	The term “release speed is supervised” can be understood in different ways in the context of the clause 3.13.10.3.8.1 of SUBSET-026 v3.6.0 One possible interpretation is that this term refers to a situation where the closest indication location corresponds to a supervised target EoA/SvL. Another possible interpretation is that it corresponds to a situation where a release speed “exists”. This last interpretation is problematic because it could lead to the following hazardous scenarios: 1.-The train is running under low adhesion conditions and the driver uses the target information to anticipate the braking if needed. The national value A_MAXREDADH requests the target information as supplementary information on the DMI. SUBSET-026 clause 3.13.10.3.9 requests to display the target information of the MRDT that shall be selected amongst the supervised targets whose remaining distance to its indication supervision limit is the shortest. The same clause gives reference to the requirements 3.13.10.3.8 and 3.13.10.3.8.1. These two requirements, if implemented according to the problematic interpretation mentioned above, would lead for the case where V_est < V_release to locate the first indication location at the “start of the RSM” and to display the target information related to the “start of the RSM” and not related to the closest target This might be safety relevant if the **target information** (target distance/target speed) is used by the driver to drive under low adhesion conditions. 2.-The train is running under low adhesion conditions and the driver uses the Time to Indication (TTI) information to anticipate the braking if needed. The national value A_MAXREDADH requests the time to indication as supplementary information on the DMI. SUBSET-026 clause 3.13.10.3.10 requests to display the time needed to travel at the estimated speed the distance up to the closest indication location. The same clause gives reference to the requirements 3.13.10.3.8 and 3.13.10.3.8.1. These two requirements, if implemented according to the problematic interpretation mentioned above, would lead for the case where V_est < V_release to locate the first indication location at the “start of the RSM” and to display the TTI information related the “start of the RSM” and not related to the closest target This might be safety relevant if the **TTI information** used by the driver to drive under low adhesion conditions. The following figure illustrates one example of the conditions that will lead to the hazard 

<table>
<tr><td>Proposed mitigation</td><td>If it is needed to implement a trackside speed restriction that affects the MRSP (e.g. due to SSP or TSRs) with a speed value lower than the release speed, the value of the release speed should be reduced to the value of the speed restriction

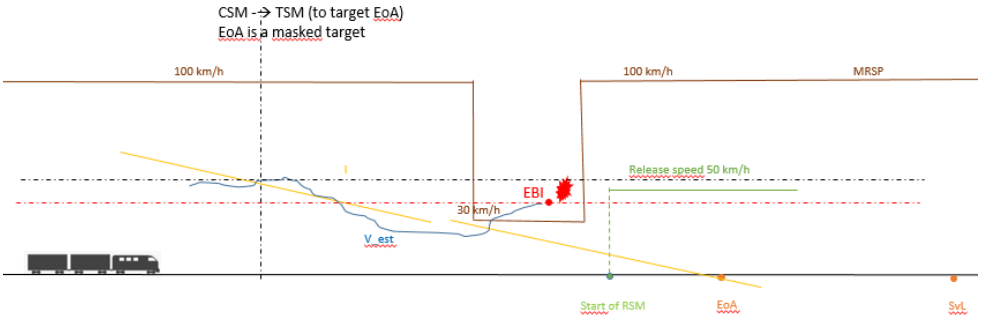
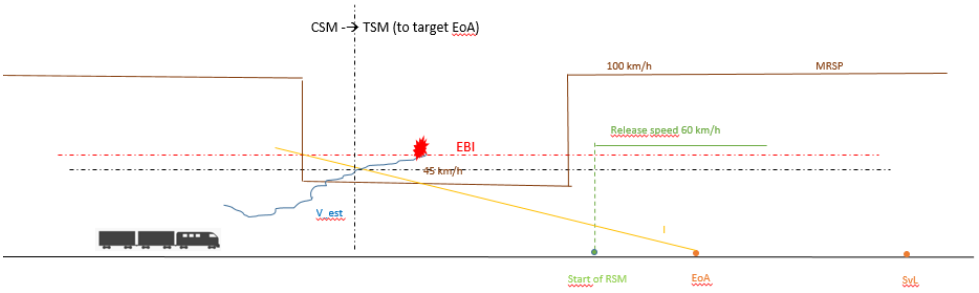
Note: This mitigation cannot work if the release speed calculated on board is used, because the trackside cannot know a priori the value of the release speed that the on-board will calculate. It could maybe make an estimation of the maximum value, but even in that case, it would not be easy to provoke the reduction of the value; the only way to mitigate the hazard in this case would be to not allow the speed restrictions lower than this estimated maximum value. The same can be said in case of PBD speed restriction.

Other possible mitigations:

In case the trackside speed restriction corresponds to a TSR, the TSR should be prolonged up to the EoA location. In this case the value of the release speed will be decreased automatically to the value of the TSR without the need to change the data preparation related to the release speed. This mitigation can be used for the fixed release speed or release speed calculated on board and it is useful when the TSR is not far from the EoA

In Level 2/3, the trackside should provide the value of the release speed once the restriction has been passed by the train. This mitigation can be used for the fixed release speed or release speed calculated on board.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE+EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N*</td><td>N</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>N*</td><td>N</td><td>Y</td></tr>
</table>
*Y in case the on-board applies the early implementation of braking curves functionality (version 4.0 or later versions)
</td></tr>
</table>

4.123 ETCS-H0123

Hazard ID	ETCS-H0123
Hazard headline	A brake application is released too soon in TSM when V_MRSP< release speed.
Hazard description	According to SUBSET-026, v3.4.0 and v3.6.0, if the train speed overpasses V_MRSP while being in TSM and a change of status/command is applied (table 9, t6, t9, t12 or t15), the status/command is automatically revoked when the train reaches a speed equal or lower than the release speed (SUBSET-026 table 11, r1). If the value of V_MRSP is lower than the value of the release speed, this would imply to release the status/command sooner than expected, and in some cases even immediately, something that could lead in specific situations to a safety issue, e.g. for the case of a EB command immediately revoked due to having a release speed value higher than the one corresponding to the EBI limit The following figures illustrate different ways on how to arrive to that scenario:  Figure 1: the train enters TSM and the EOA is selected as MRDT at a speed higher than the release speed and after overpasses V_MRSP up to the triggering command limit  Figure 2: The train accelerates in CSM over V_MRSP, enters in TSM at a speed lower than the release speed and reaches the triggering command limit

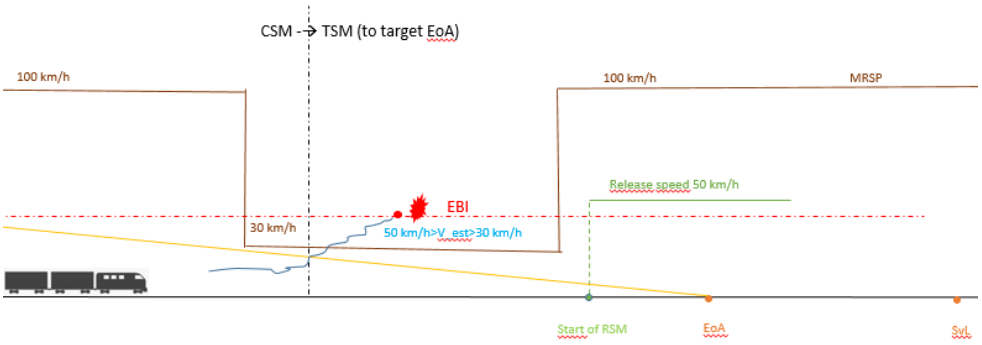


Figure 3: the train enters in TSM at a speed lower than the release speed and increases the speed over V_MRSP up to the triggering command limit.

Proposed mitigation

If it is needed to implement a trackside speed restriction that affects the MRSP (e.g. due to SSP or TSRs) with a speed value lower than the release speed, the value of the release speed should be reduced to the value of the speed restriction

Note: This mitigation cannot work if the release speed calculated on board is used, because the trackside cannot know a priori the value of the release speed that the on-board will calculate. It could maybe make an estimation of the maximum value, but even in that case, it would not be easy to provoke the reduction of the value, the only way to mitigate the hazard in this case would be to not allow the speed restrictions lower than this estimated maximum value. The same can be said in case of PBD speed restriction.

Other possible mitigations:

In case the trackside speed restriction corresponds to a TSR, the TSR should be prolonged up to the EoA location. In this case the value of the release speed will be decreased automatically to the value of the TSR without the need to change the data preparation related to the release speed. This mitigation can be used for the fixed release speed or release speed calculated on board and it is useful when the TSR is not far from the EoA

In Level 2/3, the trackside should provide the value of the release speed once the restriction has been passed by the train. This mitigation can be used for the fixed release speed or release speed calculated on board.

Mitigation allocated to

TRACKSIDE+EXTERNAL

Relevant in ETCS baseline

		ERTMS/ETCS On-board		
		B2	B3MR1	B3R2
Trackside	B2	N*	Y	Y
	B3MR1, X=1	N*	Y	Y
	B3MR1, X=2	N*	Y	Y
	B3R2, X=1	N*	Y	Y
	B3R2, X=2	N*	Y	Y

*Y in case the on-board applies the early implementation of braking curves functionality (current version 5.0 or any earlier one)

4.124 ETCS-H0124

<table>
<tr><td>Hazard ID</td><td>ETCS-H0124</td></tr>
<tr><td>Hazard headline</td><td>Rejection of safety related information by B3 on-board on reception of Packet 76 (fixed text message) from a B2 trackside.</td></tr>
<tr><td>Hazard description</td><td>It is not clear in SUBSET-026v3.4.0 and 3.6.0 how the on board will react when receiving a Packet 76 from an X=1 trackside.
-The ERTMS/ETCS On-Board could reject the whole message. In this case the ERTMS/ETCS On-Board would detect an invalid value in the message (see sections 6.5.1.5.2 and section 6.5.1.5.16 and 7.3.3.4) before translating the message (section 6.6.3.2.3) in such a way that it would conclude that there is a message consistency error, rejecting therefore the whole message without applying any reaction if the message is sent by the RBC. OR
-The ERTMS/ETCS On-Board could reject the Packet 76 without brake application. In this case the ERTMS/ETCS On-Board would translate the message (section 6.6.3.2.3) therefore not detecting an invalid value in the message (sections 6.5.1.5.2 and section 6.5.1.5.16 and 7.3.3.4)

This may lead to a safety issue:
- in case the whole RBC message is rejected while it includes safety related information
- in case only the Packet 76 is rejected but contains safety relevant information, because the text message would not be displayed to the driver and the ERTMS/ETCS On-Board would not apply a safe reaction related to this rejection.

Note: X=1 trackside in the scope of this hazard needs to be understood as B2 trackside only because in B3 the sending of Packet 76 by an X=1 trackside is forbidden by the specifications.</td></tr>
<tr><td>Proposed mitigation</td><td>Packet 76 should not be used in B2 trackside</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE+EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>N</td><td>N</td></tr>
</table>
</td></tr>
</table>

4.125 ETCS-H0125

<table>
<tr><td>Hazard ID</td><td>ETCS-H0125</td></tr>
<tr><td>Hazard headline</td><td>Unclear specification of VBC validity period</td></tr>
<tr><td>Hazard description</td><td>The resolution of T_VBC is defined as 1 day (SUBSET-026 v3.4.0 and v3.6.0 §7.5.1.154.1). It is not absolutely clear whether this means a 24-hour interval (starting at the moment the message is received) or a calendar day (ending at midnight the nth day or (n+1)th day).

The Virtual Balise Cover stored on-board could expire sooner or later than trackside expects; so both hazardous situations of ETCS-H0043 can occur (although for a different cause than the ones described in the hazard) i.e.:
• H1 “While the line is still under construction: the ERTMS/ETCS On-Board reads a balise telegram that should not be read, i.e. the inhibition is not on while it should be” and
• H2 “After the line has been put into service: the ERTMS/ETCS On-Board ignores a balise telegram that should be read, i.e. the inhibition is still on while it should have been removed.”

These 2 Hazards are covered by H0043 but due to these possible interpretations for T_VBC, the definition of T_VBC might be too short or the time period for application of the procedure to remove VBCO after line is put in service may also be too short.

Case 1: Related to H1, if a train removes VBCO at end of the nth day, it could remove VBCO too early : at midnight and not next day at same hour VBCO has been received as expected by trackside. Train might then not be protected.

Case 2: Related to H2, in case of application of procedure to remove VBCO stops exactly (24h * T_VBC) after line has been put in service, some trains could remain running with VBCO active until (n+1)th day midnight and not (24h * T_VBC) after line has been put in service as expected by trackside. Train might then not be protected.</td></tr>
<tr><td>Proposed mitigation</td><td>The VBCO should be removed on-board by balise order (where possible) and by operational procedure (e.g. when powering up the train inside a line which is no more under construction).

For case 1, T_VBC, calculated considering the constraint identified in H0043, should be extended by one day to cover on-boards that could remove VBCO at midnight the nth day.

For case 2, The procedure to remove manually VBCO on-board by the driver after a line has been put in service shall be applicable for a minimum of T_VBC (the one resulting from the previous mitigation) +1 day to cover on-boards that could only remove VBCO at midnight the (n+1)th day.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE+EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>n/a</td><td>N</td><td>N</td></tr>
<tr><td>B3MR1, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.126 ETCS-H0126

4.126.1.1 Intentionally left empty. Hazard ID not used.

4.127 ETCS-H0127

Hazard ID	ETCS-H0127
Hazard headline	Unclear management of MA section timers
Hazard description	SRS has a contradiction related to the application location of MA section timers when they are in the transition buffer. Sections 3.8.4.2.1, 3.8.4.2.2 and 3.8.4.2.3 in Subset-026 are in conflict with application of A.3.3 and filters in Table 17. Furthermore clauses 3.8.4.2.1, 3.8.4.2.2 and 3.8.4.2.3 do not clarify what has to be the on-board behaviour in case of reception of an MA including time limited sections and for which a section timer stop location is in rear of the min safe front end either when the information is received or when it is released from the transition buffer in case of a level transition or an RBC/RBC handover. For the end section timer start location, clauses 3.8.4.1.3 and 3.8.4.1.4 specify the on-board behaviour in a somewhat similar situation and for the overlap timer start location, the on-board behaviour is specified in clauses 3.8.4.4.4 and 3.8.4.4.5. Regarding the section timer there is (are) no “equivalent” clause(s). Example of scenarios: Scenario 1: • A train is running in Level 1 inside a mixed L1/L2 area. • A communication session with the RBC exists and a transition to L2 is announced. • Train is running with L1 LS MA that does not contain section timer • If the RBC is ready to take over responsibility it could send an immediate LTO and L2 MA to the train which contains the assumed section timers and section timer stop location. • The LRBG of this MA is located in rear of the current train location. This MA contains time-limited sections located in rear of the train and with the corresponding section timer stop locations also located in rear of the min safe front end of the train as well. • When received on-board, this MA goes to the transition buffer (see 4.8.1.3.1) and it is evaluated when the buffer is released. • Considering SRS clauses A.3.3.1 and A.3.3.2, while the MA is in the transition buffer the clauses 3.8.4.2.1, 3.8.4.2.2 and 3.8.4.2.3 cannot be applied. However, these clauses will start to be applied when the MA is released from the transition buffer but even if the ERTMS/ETCS on-board could apply 3.8.4.2.1, there is an ambiguity about the application of clause 3.8.4.2.3. In this case, the ERTMS/ETCS on-board does not know when the min safe front end has passed the section timer stop location. Scenario 2: • A train is running in Level 1 or 2 SR. • An MA is received by the ERTMS/ETCS on-board and the LRBG of this MA is located in rear of the train. This MA contains time-limited sections located in rear of the min safe front end and with the corresponding section timer stop locations also located in rear of the min safe front end. • In this case, the ERTMS/ETCS on-board does not know when the min safe front end has passed the section timer stop location. Scenario 3: • A train is running in Level 1 or 2 FS. • A MA repetition/extension is received by the ERTMS/ETCS on-board. This MA repetition/extension contains time-limited sections located in rear of the min safe

<table>
<tr><td></td><td>front end and with the corresponding section timer stop locations also located in rear of the min safe front end.
• In this case, the ERTMS/ETCS on-board does not know when the min safe front end has passed the section timer stop location.

The ERTMS/ETCS on-board could consider that the section timer has expired (i.e. apply 3.8.4.2.2) and possibly go to TR. However, the behaviour which the ERTMS/ETCS on-board has to adopt is not specified by any clause. There could be ERTMS/ETCS on-board implementations which consider that once the section timer stop location has been passed, those sections are assumed granted and should no more be released without a shortening of MA.

These situations could be problematic in case ERTMS/ETCS trackside expects that the ERTMS/ETCS on-board will consider the timers as expired (due to the lack of knowledge whether the timer stop location was passed in due time or not). The hazardous situation occurs if the ERTMS/ETCS trackside releases the sections after the related timer has expired.

This hazard is also applicable in case of RBC/RBC handover transitions and transitions between ETCS Levels 1, 2.</td></tr>
<tr><td>Proposed mitigation</td><td>Specifically for scenario 1:

The ERTMS/ETCS trackside should not send time-limited MAs in rear of a transition location with the timer stop location in rear of the train. Or it should consider in its engineering rules that the ERTMS/ETCS on-board may start the timer only when the train changes the level.

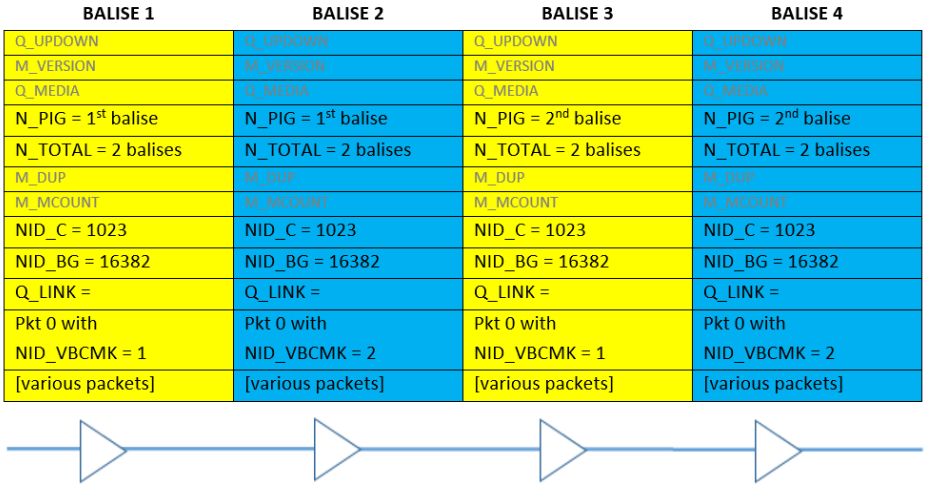
Specifically for scenario 2, 3:

The ERTMS/ETCS trackside should not immediately release the sections after the related timer expiration but shall check it with ERTMS/ETCS on-board through e.g. a conditional emergency stop message.

For Level 1 other possible mitigation following the concept of SUBSET-040, clause 4.1.1.4, is that the last encountered balise of the BG giving a time-limited MA should be at minimum distance of 1.3 m plus the distance the train may run during the time Tn, calculated from the formulas in SUBSET-036, clause 4.2.9, in rear of MA’s timer stop location. Note: for train speeds lower than 80 km/h, the time Tn always equals to 100 ms.

Note: ETCS-H0016, ETCS-H0021 include the use of section timers as mitigation. Then if such mitigation is applied, these above proposed mitigations shall also be considered.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>n/a</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.128 ETCS-H0128

Hazard ID	ETCS-H0128
Hazard headline	Balise telegram unduly dismissed by the on-board because of a virtually covered neighbouring balise
Hazard description	The hazard refers to situation where ERTMS/ETCS Trackside “interleaves” in the same BG balises intended to be virtually covered and balises not intended to be virtually covered. The resulting installation presents in the same balise group neighbouring balises whose telegram headers are identical but their appended Packet 0 includes different NID_VBCMK. Figure with possible example situation:  The ERTMS/ETCS Trackside expects that the telegrams from balises 2 and 4 are ignored due to the masking by VBC (because they are for example in commissioning phase or not in service) and that the safety-related telegrams from balises 1 and 3 are sent to and accepted by the ERTMS/ETCS On-board. Hazardous scenario: The ERTMS/ETCS On-board moving on the line has a VBC stored, not yet expired, with identity matching the VBC of balises 2 and 4 (NID_C = 1023, NID_VBCMK = 2). Sequence: • Train runs over the four balises. • The BTM cannot distinguish if the header of balise 1 and 2 are from just one balise or from two different balises; the same happens with balises 3 and 4. • Because of that, the BTM function is not able to discriminate balises 1 and 2 and consider them as the same balise with side-lobes. The same happens for balises 3 and 4. • Consequently, the BTM may decide to forward to the Kernel only the telegrams of balises 2 and 4. • The ERTMS/ETCS On-board then discards those telegrams because it considers them coming from balises that were “virtually covered” by VBC. Intermediate result: • The (“in commissioning phase”) balises 2 and 4 are totally ignored. • The (safety-related) information of balises 1 and 3 is “lost”. Possible subcases: a) Q_LINK = 0 b) Q_LINK = 1 and linking active on-board; trackside requested “no liking reaction”.

BALISE 1	BALISE 2	BALISE 3	BALISE 4
Q_UPDOWN	Q_UPDOWN	Q_UPDOWN	Q_UPDOWN
M_VERSION	M_VERSION	M_VERSION	M_VERSION
Q_MEDIA	Q_MEDIA	Q_MEDIA	Q_MEDIA
N_PIG = 1st balise	N_PIG = 1st balise	N_PIG = 2nd balise	N_PIG = 2nd balise
N_TOTAL = 2 balises	N_TOTAL = 2 balises	N_TOTAL = 2 balises	N_TOTAL = 2 balises
M_DUP	M_DUP	M_DUP	M_DUP
M_MCOUNT	M_MCOUNT	M_MCOUNT	M_MCOUNT
NID_C = 1023	NID_C = 1023	NID_C = 1023	NID_C = 1023
NID_BG = 16382	NID_BG = 16382	NID_BG = 16382	NID_BG = 16382
Q_LINK =	Q_LINK =	Q_LINK =	Q_LINK =
Pkt 0 with NID_VBCMK = 1	Pkt 0 with NID_VBCMK = 2	Pkt 0 with NID_VBCMK = 1	Pkt 0 with NID_VBCMK = 2
[various packets]	[various packets]	[various packets]	[various packets]

<table>
<tr><td></td><td>c) Q_LINK = 1 and linking active on-board; trackside requested “reaction brake/trip”.
Final result:
a) Information is lost without brake intervention.
b) Information is lost without brake intervention.
c) Information is lost but with brake intervention.

The results a) and b) are hazardous, since there is loss of safety related information without a restrictive reaction.</td></tr>
<tr><td>Proposed mitigation</td><td>The ERTMS/ETCS Trackside shall install side by side balises at a distance greater than 5 meters if they have identical telegram header. This constraint is to be sure that no lobe overlapping can occur and therefore avoid an undue filtering of a telegram .</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td></td><td></td><td colspan="3">ERTMS/ETCS On-board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td>Trackside</td><td>B2</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td></td><td>B3MR1, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3MR1, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3R2, X=1</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td></td><td>B3R2, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

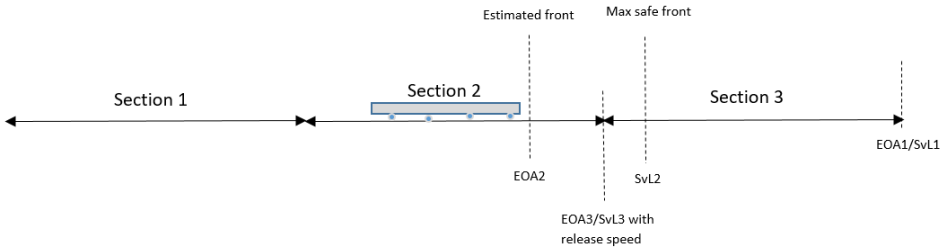
4.129 ETCS-H0129

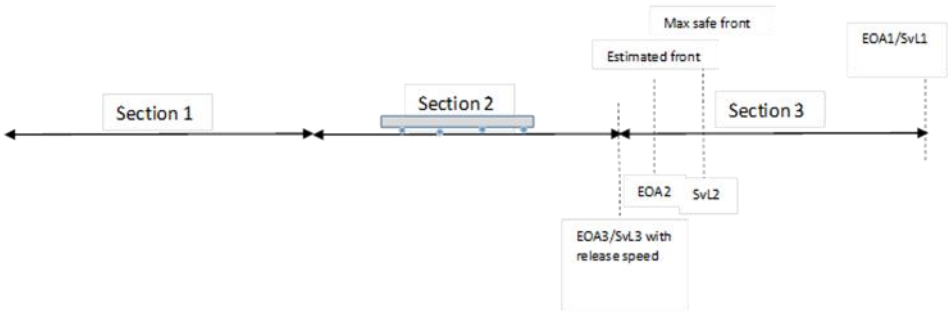
4.129.1.1 Intentionally left empty. Hazard entry under analysis.

4.130 ETCS-H0130

4.130.1.1 Intentionally left empty. Hazard entry under analysis.

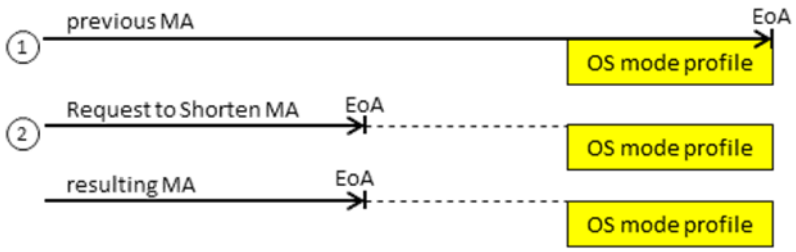
4.131 ETCS-H0131

Hazard ID	ETCS-H0131
Hazard headline	Undue MA extension when a section timer expires
Hazard description	The following potentially hazardous scenarios were identified: Scenario 1:  MA with 3 sections and with the EOA1/SvL1 located at the end of the last section. Then an event occurs which triggers condition according to SUBSET-026, A.3.4.1.3, condition [11] (except clause e) of A.3.4.1.2). Therefore, the EOA1/SvL1 are shortened to the estimated front end/maximum safe front end respectively, EOA2/SvL2 with no release speed. Since the SvL2 is at max safe front end of the train, the train will not be able to move. Still the max safe front end is inside Section 3 not all of the section 3 will be deleted after the shortening of the EOA1/SvL1. When the timer related to Section 3 expires the SUBSET-026 3.8.4.2.2 paragraph is triggered. Therefore, the EOA2/SvL2 move to the start of the section 3 (EOA3/SvL3). This implies that the EOA moves to a location in advance of the previous EOA and that a release speed related to the new EOA/SvL is created (NV/Default). This could be interpreted as not consistent with the meaning of the word “withdrawn” (which would only apply if the move is towards the front of the train) in the SUBSET-026 3.8.4.2.2 a) paragraph but if an ERTMS/ETCS On-Board would nonetheless extend the MA with a release speed this may be hazardous, if trackside expects that without further information the train cannot move forward at all. Scenario 2: MA with 3 sections and with the EOA1/SvL1 located at the end of the last section. An event occurs which triggers A.3.4.1.3 condition [11]. The ERTMS/ETCS On-board equipment shall consider the current estimated front end and max safe front end positions of the train, as the EOA and SvL respectively, with no release speed. Therefore, the EOA1/SvL1 are shortened to the estimated front end/maximum safe front end respectively -> EOA2/SvL2 with no release speed. The timer related to section 3 expires and the requirement in 3.8.4.2.2 is triggered. The EOA2/SvL2 move to the start of the section 3 (EOA3/SvL3).

<table>
<tr><td></td><td>


In this case the EOA and SvL are both “withdrawn” upon expiry of the section timer, the same hazardous situation applies: the train is allowed to proceed with the national value for the release speed, when the trackside would expect that the train should not be able to move forward at all after the application of condition [11].
</td></tr>
<tr><td>Proposed mitigation</td><td>It must be evaluated in the projects whether the residual risk can be accepted.
Possible mitigation for ETCS Level 2 is to set the release speed to “0” in the National values by the ERTMS/ETCS Trackside.
Possible mitigation for ETCS Level 1 is to not use the section timers when RS from NV could be problematic.</td></tr>
<tr><td>Mitigation allocated to</td><td>TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>N/A</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.132 ETCS-H0132

Hazard ID	ETCS-H0132
Hazard headline	Potential safety issues due to the use of the temporary EOA/SvL beyond EOA
Hazard description	If the start of a mode profile, route suitability or not protected LX is located further that SvL derived from MA it may happen that the ERTMS/ETCS On-board supervise the SvL which is located further that the SvL derived from the MA. Scenario 1 (LOA): An ERTMS/ETCS On-board receives an MA with an OS mode profile for further location, and the beginning of the mode profile is beyond the LOA of the MA. The result of the above mentioned §5.9.3.5 is that the ERTMS/ETCS On-board shall consider a temporary EOA at the beginning of the mode profile and a temporary SvL at the LOA of the MA. Since the start of the mode profile is beyond the LOA, it means that the EOA is beyond the SvL but such configuration (SvL in rear of the EOA) is not foreseen in the specifications and the ERTMS/ETCS On-board may fall in a grey area. Scenario 2 (EOA): An ERTMS/ETCS-On-board receives an MA with an OS mode profile for further location, and the beginning of the mode profile is beyond the EOA of the MA: 1. ERTMS/ETCS On-board has MA on-board with OS mode profile that starts before and ends at the EoA. 2. RBC sends Request to Shorten MA to ERTMS/ETCS On-board with requested stop location in rear of the start of OS mode profile. As an alternative mitigation for the example 1 of ETCS-H0082 the RBC sends together with the Request to Shorten MA a OS mode profile that equals the mode profile currently stored on-board. 3. ERTMS/ETCS On-board accepts the Request to Shorten MA and OS mode profile.  SUBSET-026 v.3.6.0[7] §5.9.3.5 defines a requirement *"...Until the ERTMS/ETCS on-board equipment has switched to OS mode, the beginning of the On Sight area shall be temporarily considered as the EOA (instead of the EOA/LOA derived from the MA) and the SvL (with no release speed) shall be determined according to the mode profile either:*

[7] Including all previous B2 and B3 related versions

<table>
<tr><td></td><td>
a. as the SvL derived from the MA. In case the MA defines an LOA, the SvL shall be derived as if no LOA had been given.
OR
b. as the beginning of the On Sight area…”

Note: Comparable requirements available for SH mode profile (see SUBSET-026 v.3.6.0[7] §5.7.3.4), for route suitability data (see SUBSET-026 v.3.6.0[7] §3.13.2.4), for not protected LX (see SUBSET-026 v.3.6.0[8] §5.16.1.1) and for LS mode profile (see SUBSET-026 v.3.6.0[8] §5.19.3.5).

These requirements may postpone or reduce the effect of the safety protection, especially when ERTMS/ETCS On-board receives an MA with an

OS/SH/LS mode profile,
route suitability
or
not protected LX

for further location, and their beginning is beyond the EOA/LOA/SvL.
</td></tr>
<tr><td>Proposed mitigation</td><td>ERTMS/ETCS Trackside specific application project / infrastructure manager should show that the remaining risk is acceptable.</td></tr>
<tr><td>Mitigation allocated to</td><td>EXTERNAL + TRACKSIDE</td></tr>
<tr><td>Relevant in ETCS baseline</td><td>
<table>
<tr><td colspan="2"></td><td colspan="3">ERTMS/ETCS On-Board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5">Trackside</td><td>B2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3MR1, X=2</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=1</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>B3R2, X=2</td><td>Y</td><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>

[8] Including all previous B3 related versions

APPENDICES TO SUBSET-113

Appendix A ETCS-H0019 clarification: Rejection of coordinate system

A.1.1.1.1 SUBSET-026 (both v2.3.0 and v3.4.0) states:

> 3.4.2.3.3.8 A co-ordinate system assignment received from trackside shall be rejected by the ERTMS/ETCS On-Board equipment if the referred LRBG is memorised (see 3.6.2.2.2c) to have been reported more than once and with different “previous LRBGs”.
>
> 3.4.2.3.3.8.1 Note: If a single balise group is memorised, according to 3.6.2.2.2c, more than once, and with different “previous LRBGs”, the assignment of the co-ordinate system is ambiguous.

A.1.1.1.2 This could lead to the following scenario:

(a) Train in level 2 mode SR.

(b) The train sends a position report packet 1 with LRBG = BG 2 and PRV_LRBG = BG 1. No assignment of co-ordinate is received from the RBC.

(c) After BG 3, the train is stopped and the active cabin is changed.

(d) The train sends a position report packet 1 with LRBG = BG 2 and PRV_LRBG = BG 3. Then, if an assignment of co-ordinate is received, it will be acknowledged but rejected in a further step by the ERTMS/ETCS On-Board equipment due to SUBSET-026 §3.4.2.3.3.8 (both v2.3.0, modified by SUBSET-108 v1.2.0 CR 729, and v3.4.0).

A.1.1.1.3 This scenario could lead to the following hazard:

> The RBC is not informed that the assignment of co-ordinate has been rejected by the ERTMS/ETCS On-Board equipment. It could then send oriented information (q_dir <> "BOTH") with LRBG = BG 2 which will be rejected by the ERTMS/ETCS On-Board equipment because the orientation of BG 2 is still undetermined. This has an impact on the availability (MA, TAF request ...) and safety (TSR, track conditions).

A.1.1.1.4 Note that the hazard cannot occur in FS/OS mode, since assignment of co-ordinate is rejected in these modes.

Appendix B ETCS-H0043 clarification: VBC FMEA

B.1 Introduction

B.1.1.1.1 The purpose of this FMEA is to derive proposed Engineering Rules (ENG RULE) and Operational Rules (OP RULE) in relation to the Virtual Balise Marker function defined in section §3.15.9 of SUBSET-026 v3.4.0 and v3.6.0 (introduced in baseline 3). It is assumed that the infrastructure owner derives and implements these rules.

B.1.1.1.2 It is furthermore assumed that the infrastructure owner defines correct Virtual Balise Cover orders and supplies the driver with these orders in a process that guarantees the correctness and timeliness of the order.

B.1.1.1.3 Normally, the FMEAs in UNISIG only concern the information at the interoperable interfaces of ETCS. In order to fulfil the above purpose, however, this FMEA also analyses some ERTMS/ETCS On-Board internal failure modes and some operational situations. The analysis is then still performed for the information flowing on the interfaces; however this shall then be understood as the handling of this information inside ERTMS/ETCS On-Board all the way into the execution of the function using it.

B.1.1.1.4 DMI failures modes are included, using SUBSET-079 as input. Driver failures are however not analysed here.

B.1.1.1.5 This FMEA analyses the two information packets “VBC marker” and “VBC order”. They are given the ERTMS/ETCS On-Board in different ways:

- The VBC marker analysed in chapter B.2.1 can only be given from a balise, as Packet 0 from trackside with version X=2 and Packet 200 from trackside with version X=1, Y=1.
- The VBC order analysed in chapter B.2.2 can either be given from a balise, as Packet 6, or from the driver as DMI input.

B.1.1.1.6 The analysis in cases B.2.2.2.3.x uses the failure cause “The T_VBC is set to a value which doesn’t exceed the maximum time of train operation inside the LUC”. Therefore, it is here assumed that T_VBC is rather set too long instead of too short and that the driver will systematically have to manually check all applicable VBCs once at SoM[9] inside this area. The assumption is further elaborated and defined in the FMEA, see OP RULE 1 and OP RULE 2.

B.1.1.1.7 Compatibility with baseline 2: a B2 ERTMS/ETCS On-Board equipment will be stopped due to system version check if entering a LUC B3 X=2 area; in a B3 X=1 LUC area a B2 ERTMS/ETCS On-Board equipment will not be protected by version check and will not

[9] It is further assumed that commissioning of the LUC is not done with trains operating in traffic inside it.

consider VBC information included in balise groups. So external protections are necessary to avoid a B2 ERTMS/ETCS On-Board equipment entering such area.

B.2 FMEA

B.2.1 Virtual Balise Cover Marker

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			Proposed External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
B.2.1.1.1	NID_VBCMK	**DELETION**	Engineering error in non-commissioned balises (e.g. VBC marker forgotten)	Any but NP	The ERTMS/ETCS On-Board will not ignore the balise telegram in the LUC	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	-
B.2.1.1.2			Any failure of the non-trusted transmission system	Any but NP	As above	As above	As above	-	Catastrophic	The Eurobalise code protects against losing a packet inside a balise telegram. If the whole telegram is lost, there is no hazard.

B.2.1.2.1	**CORRUPTION**	Engineering error in non-commissioned balises (e.g. wrong NID_VBCMK programmed)	Any but NP	In case the balise telegram should have been ignored: The ERTMS/ETCS On-Board will not ignore the balise telegram	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	
B.2.1.2.2				In case the balise should not have been ignored: The ERTMS/ETCS On-Board will ignore the balise telegram if there is a VBC order pointing to the new "wrong" NID_VBCMK	H2: Balise information (potentially restrictive) intended for traffic will be ignored	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	It is not certain that there is a VBC order pointing to the new "wrong" id. Ignoring all balise telegrams in a group can lead to a linking reaction.
B.2.1.2.3		Any failure of the non-trusted transmission system	Any but NP	As above (both cases)	As above (both cases)	As above (both cases)	As above (both cases)	Catastrophic	The Eurobalise code protects against corruption

B.2.1.3.1		**INSERTION**	Any failure of the non-trusted transmission system, i.e. cross-talk	Any but NP	If a VBC marker is cross-talked, the ERTMS/ETCS On-Board will ignore the balise telegram according to rules in SUBSET-026 v3.4.0	None	None		'	

B.2.2 Virtual Balise Cover Order

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
B.2.2.1.1	Q_VBCO, NID_VBCMK, NID_C, T_VBC	**DELETION**	Any failure of the non-trusted transmission system	Any but NP	Intended setting of VBC order is not performed (in case Q_VBCO=1 was intended)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 2: A balise group giving a VBC order shall consist of at least two balises	Catastrophic	
B.2.2.1.2					Intended removal of VBC is not performed (in case Q_VBCO=0 was intended)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	As above
B.2.2.1.3			ERTMS/ETCS On-Board internal failure	Any but NP	As above	As above	As above		Catastrophic	Product specific safeguarding to SIL4[10]

[10] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
B.2.2.1.4			ERTMS/ETCS On-Board memory buffer full	Any but NP	As above	As above	As above		Catastrophic	The number of memorised VBCs On-Board is defined in SUBSET-040 v3.3.0 and v3.4.0 §4.3.2.1.1w (and must thereby be respected by trackside). For transitions between countries/regions, the previous VBCs are deleted when a balise group with a new country/region identifier (NID_C) is received, see SUBSET-026 v3.4.0 and v3.6.0 §3.15.9.5d.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
B.2.2.1.5			The VBC order never reaches the ERTMS/ETCS On-Board because the train has been moved into a LUC in a mode where balises are not read (NP, IS and SF)	Any but NP	As above	As above	As above	OP RULE 1: Driver needs to “re-enter and validate” or “remove” VBCs at each SoM inside a LUC to be sure the onboard uses the correct set of VBCs	Catastrophic	-

B.2.2.2.1	**CORRUPTION**	Any failure of the non-trusted transmission system	Any but NP	Intended setting of VBC order is not performed (in case Q_VBCO=1 was intended)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	None needed	Catastrophic	The Eurobalise code protects against corruption in the transmission channel
B.2.2.2.2				Intended removal of VBC order is not performed (in case Q_VBCO=0 was intended)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	As above
B.2.2.2.3		ERTMS/ETCS On-Board internal failure	Any but NP	As above (both cases)	As above (both cases)	As above (both cases)		Catastrophic	Product specific safeguarding to SIL4[11]. Specifically for corruption of T_VBC, special considerations are needed, and the case is analysed separately below, see B.2.2.2.3.x.

[11] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

B.2.2.2.3.1	T_VBC	**CORRUPTION**	Train is **outside** LUC 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC.". 2. ERTMS/ETCS On-Board internal failure (e.g. clock) 3. External failure (e.g. UTC)	All	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 3: Balise group giving VBC order shall be placed at all entries to a LUC and need to correctly reflect the status of the LUC at all times, both setting valid VBCs and removing non-valid[12] VBCs and to define adequate T_VBC (long enough)	Catastrophic	
B.2.2.2.3.2					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	

[12] The remove VBC order should be enforced until the need for using the same VBC code again arises.

B.2.2.2.3.3			Train is **inside** LUC with ERTMS/ETCS On-Board **powered off** 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC." 2. ERTMS/ETCS On-Board internal failure (e.g. clock) 3. External failure (e.g. UTC)	NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	OP RULE 1 Driver needs to "re-enter and validate" or "remove" VBCs at each SoM inside a LUC to be sure the onboard uses the correct set of VBCs	Catastrophic	

B.2.2.2.3.4					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	OP RULE 2: For every vehicle, driver needs to remove the VBC orders at the first SoM inside a LUC after the commis-sioning of the LUC [13]	Catastrophic	

[13] To cover the case of erroneously too long T_VBC, the manual removal needs to be done once per vehicle after the commissioning:. thus it is not enough to enforce this procedure only up to commissioning date + T_VBC days

B.2.2.2.3.5			Train is **parked inside** LUC with ERTMS/ETCS On-Board **powered on** [14] 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC." 2. ERTMS/ETCS On-Board internal failure (e.g. clock) 3. External failure (e.g. UTC)	Any but NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	As ENG RULE 3 above. In addition: the balise groups need to be placed also where trains are normally parked with ERTMS/ETCS On-Board powered. If this is not possible, OP RULE 1 and 2 can be applied also in other situations than SoM [15].	Catastrophic	

[14] Since the ERTMS/ETCS On-Board is powered on the whole time, the Start of Mission procedure is not executed and therefore barrier OP RULE 1 is not effective.

[15] If this barrier is pursued, situations to be considered shall include using a vehicle that has been parked with ERTMS/ETCS On-Board in SL mode, since it could be hazardous to receive e.g. erroneous National Values and Level Transition Orders, which will be used later when the vehicle becomes the leading vehicle.

B.2.2.2.3.6					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignore	As above	As above	Catastrophic

B.2.2.2.3.7			Train is running **inside** LUC with ERTMS/ETCS On-Board **powered on** 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC." 2. ERTMS/ETCS On-Board internal failure (e.g. clock) 3. External failure (e.g. UTC)	Any but NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	The time at risk is small. see further B2.3.1.3.	Catastrophic	
B.2.2.2.3.8					Timer expires and VBC order removed later than intended.	Not an applicable scenario. A LUC is not commissioned when there is traffic inside it.	n.a.	n.a.	None	n.a.

B.2.2.3.1		**INSERTION**	Any failure of the non-trusted transmission system; i.e. cross-talk	Any but NP	If a correct VBC order is cross-talked, the ERTMS/ETCS On-Board will use it and - set the VBC (in case Q_VBCO=1) or - remove the VBC (in case Q_VBCO=0)	None, since the VBC order is correct	None		'	
B.2.2.3.2			ERTMS/ETCS On-Board internal failure	Intended setting of VBC order is not performed (in case 'set VBC' is inserted)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	None needed	Catastrophic		Product specific safeguarding to SIL4[16].
B.2.2.3.3				Intended removal of VBC order is not performed (in case 'remove VBC' is inserted)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic		As above

[16] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

B.2.3 Notes

B.2.3.1.1 Notes of ENG RULE 1: The rule says that the setting of a VBC marker needs to follow a safe process. This could be perceived as redundant to the general rule in SUBSET-091 called EXT_SR01 that requires the preparation of the ETCS Trackside Data to be of a quality that is appropriate to the required safety level. However, in a construction area the data (e.g. balise telegrams) is not commissioned and can therefore not be expected to have gone through all safety processes. Even so, safety reliance is placed on balise telegrams in the construction area; therefore ENG RULE 1 is necessary.

B.2.3.1.2 Notes on OP RULE 1 and 2:

- The use of the VBC function requires the driver to validate that ERTMS/ETCS On-Board has the correct set of VBCs in many operational situations, at least connected to the technical procedure Start of Mission inside a LUC. In some of these situations it is clear that the validation is not merely a double check of a list that should already be valid, but that the driver will be expected to actually correct the set of VBCs (if not using VBC orders from balises at all, the driver will need to enter the VBC codes even more frequently). The effect of a failure to do so correctly might have catastrophic consequences. Therefore, the operational procedure which shall guarantee that the driver can take this responsibility must be elaborated with great care, taking into account the aspects of human failures given the ergonomics of the VBC set and remove function specified in ERA_ERTMS_015560 “ERTMS/ETCS, ETCS Driver Machine Interface”.
- It needs to be made sure that the timer is restarted when the driver checks the VBC. Therefore, OP RULE 1 must contain the instruction to go through the set and validation procedure for each VBC that is required for operation in the LUC.

B.2.3.1.3 Notes on ERTMS/ETCS On-Board timer function:

- The timer related to the VBC function shall be active also when ERTMS/ETCS On-Board is powered off. This implies that ERTMS/ETCS On-Board must make itself reliant upon external sources of time, most likely with unknown safety properties. The timer at power off shall therefore not be considered as a safety function, but must be mitigated with external barriers; see further cases B.2.2.2.3.x.
- For the case of erroneously releasing a VBC timer while running inside a LUC, there are no operational mitigations. The driver will not be given any warning on the DMI if a VBC timer expires, but the ERTMS/ETCS On-Board will simply start processing the balise telegrams that should have been ignored in the LUC. However, it is believed that the time at risk for such an event will be limited since the train will at some point in time go outside the LUC. Therefore, any accuracy and safety requirements imposed by this scenario will highly likely be bounded by accuracy and safety requirements imposed by other scenarios involving the ERTMS/ETCS On-Board clock with ERTMS/ETCS On-Board powered, e.g. MA timer.

Appendix C ETCS-H0045 clarification: Risks related to “List of balises in SH” function

C.1 Overview

C.1.1.1.1 This appendix analyses the potential risk of entering mainlines in Shunting mode because the limits of the shunting area sent by trackside with Packet 49 “List of balises for SH area” will not be used by the ERTMS/ETCS On-Board.

C.1.1.1.2 The risk comes from the fact that the ERTMS/ETCS On-Board will not use the list of BGs, whereas the trackside expected it to. This analysis has identified eight cases in which the ERTMS/ETCS On-Board will not use the list of balises: the cases are listed in Table 3 and analysed in detail in the subsequent sections.

Case	Description	Applicability
Case 1	The packet 49 is received out of an MA containing an SH mode profile or out of an “SH Authorised” message	ERTMS/ETCS On-Board implementing CR 919 on a B2 trackside not implementing that CR.
Case 2	The packet 49 is received in “SH Authorised” message when the ERTMS/ETCS On-Board is in mode SB without valid train data stored ERTMS/ETCS On-Board (typical case: SoM procedure in level 2)	ERTMS/ETCS On-Board (B2) implementing CR 650 and not implementing CR 919.
Case 3	The SH mode is entered in the execution of “Shunting initiated by driver” procedure	ERTMS/ETCS On-Board behaving as per new step A050 (introduced by CR 919) of the “Shunting initiated by driver” procedure, on a B2 trackside that has not considered this behaviour.
Case 4	A “list of balises for SH area” is accepted by the ERTMS/ETCS On-Board while the related MA and mode profile are rejected	ERTMS/ETCS On-Board (B2) not implementing CR 919.
Case 5	A “list of balises for SH area” transmitted “alone” by the trackside is accepted by the ERTMS/ETCS On-Board	ERTMS/ETCS On-Board (B2) not implementing CR 919 on B2 trackside also not implementing that CR.
Case 6	The ERTMS/ETCS On-Board has considered a wider field of application of the SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 clause §3.12.4.4 than the trackside	B2 trackside not implementing CR 919.
Case 7	Intentionally deleted.	Intentionally deleted.

Case 8	The request to Shorten MA message can contain a Mode Profile (v2.3.0 and v3.4.0 and v3.6.0) and a List of Balises for Shunting. In the SUBSET-026 (v3.4.0 and v3.6.0) it is not clear that the mode profile and list of balises cannot be considered “accepted” until the evaluation of the cooperative shortening is complete (see also ETCS-H0082)..	ERTMS/ETCS On-Board (B3MR1 and B3R2) implementing the acceptance of List of SH balise received in a request to shorten MA according to C.3.8.1.6 description.

Table 3: cases and applicability for the risk

C.1.1.1.3 Regarding the applicability conditions, it shall be noted that:

- The CR 919 is not in the SUBSET-108 v1.2.0.
- The CR 650 is in the SUBSET-108 v1.2.0 but not classified (“DC”).
- A B3 ERTMS/ETCS On-Board will always implement the CR 919 and CR 650; a B3 trackside will always implement the CR 919 (the CR 650 is about the ERTMS/ETCS On-Board).
- A B2 ERTMS/ETCS On-Board may already be consistent with the CR 919 solution.

C.2 Assumption

C.2.1.1.1 It is assumed that a trackside that has implemented the CR 919 has considered the Chapter 6 of SUBSET-026 v3.4.0 and v3.6.0, table 6.5.1.6.5 which revokes for X=1 trackside the airgap modifications brought by the CR, and that an ERTMS/ETCS On-Board that has implemented the CR 919 has considered the clause §6.6.3.1.1 of SUBSET-026 v3.4.0 and v3.6.0 for the data consistency check of the received airgap information.

C.3 Analysis

C.3.1 Case 1

C.3.1.1.1 It is possible for a B2 trackside that has not implemented the CR 919 to send a “list of balises for SH area” (airgap packet 49) in an MA without sending a mode profile for the SH mode in the same MA. The “list of balises for SH area” aims at protecting the borders of the Shunting area by tripping the train (i.e. the ERTMS/ETCS On-Board equipment enters the TR mode) in case the train encounters a balise group which is not part of the list. It is even possible for a trackside that has not implemented the CR 919 to transmit by balise group a “list of balises for SH area” without MA. Example: the ETCS trackside provides first the MA with SH mode profile and then in a subsequent balise group message, before the ERTMS/ETCS On-Board enters in SH mode, the list of balises for SH area.

C.3.1.1.2 An ERTMS/ETCS On-Board equipment that has implemented the CR 919 does not expect the reception of a “list of balises for SH area” out of an MA containing a packet 80

(Mode Profile) with the variable M_MAMODE = “Shunting” nor out of a “SH authorised” message.

C.3.1.1.3 The safety issue may appear in case the ERTMS/ETCS On-Board equipment rejects the received list of balises for SH area. The ERTMS/ETCS On-Board equipment enters in SH mode and the list of balises for the related SH area is not supervised.

C.3.1.1.4 If the protection against the train passing the borders of the Shunting area does in part or completely rely on the list of balises, a train not supervising this list may leave the Shunting area while being in SH mode, i.e. enter a main line with an insufficient ETCS supervision.

C.3.2 Case 2

C.3.2.1.1 An ERTMS/ETCS On-Board equipment that has implemented the CR 650 without implementing CR 919 will accept a “list of balises for SH area” (airgap packet 49) received in mode SB only if valid train data is stored ERTMS/ETCS On-Board. This acceptation condition does not apply to the “SH authorised” message (airgap message 28). This means that in case the ERTMS/ETCS On-Board equipment receives in mode SB without valid train data being stored ERTMS/ETCS On-Board a “SH authorised” message containing a “list of balises for SH area”, the ERTMS/ETCS On-Board equipment will accept the “SH authorised” message but reject the “list of balises for SH area”. The ERTMS/ETCS On-Board equipment enters the SH mode according to the received “SH authorised” message and the list of balises for the related SH area is not supervised.

C.3.2.1.2 The typical scenario is a Start of Mission in Level 2 in a Shunting area: the driver selects Shunting during the Start of Mission procedure, without having entered train data, and the RBC responds with a “SH authorised” message including packet 49.

C.3.2.1.3 If the protection against the train passing the borders of the Shunting area does in part or completely rely on the list of balises, a train not supervising this list may leave the Shunting area while being in SH mode, i.e. enter a main line with an insufficient ETCS supervision.

C.3.2.1.4 Note that CR 919 (part of baseline 3) closes the potentially hazardous situation.

C.3.3 Case 3

C.3.3.1.1 An ERTMS/ETCS On-Board equipment that has implemented the CR 919 has implemented the new step A050 of the “Shunting initiated by driver” procedure (see section 5.6 of SUBSET-026 v3.4.0 and v3.6.0). This new step A050 specifies that “*At the mode change to SH, any previous list of balise groups for SH area shall be deleted or replaced by a new list of balise groups for SH area*”. If the trackside has not foreseen such a behaviour by the ERTMS/ETCS On-Board (typically a B2 trackside), hazardous situations can occur.

C.3.3.1.2 Example: the ETCS trackside cannot technically provide the SH mode profile. The SH mode is entered on driver selection (procedure “Shunting initiated by driver”). As the SH area is delimited, the ETCS trackside can however provide the list of balises for SH area.

As a list of balises for SH area is not accepted by an ERTMS/ETCS On-Board in SH mode, the trackside provides this list in rear (i.e. upstream) of the operational location where the driver will initiate the Shunting. This list is therefore received by the ERTMS/ETCS On-Board before performing the transition to SH mode and according to the new step A050 of the “Shunting initiated by driver” procedure, this list will be deleted when entering the SH mode. Here also the train will be in SH mode without supervising the list of balises related to SH area.

C.3.3.1.3 The same result appears even if ETCS trackside was able to provide the SH mode profile but the driver manually selects shunting before the train enters the SH area of the mode profile.

C.3.3.1.4 Note that the deletion of the list in step A050, brought by CR 919, is “on top” of the table “what happens when a mode is entered” that shows “unchanged” for the switching to SH.

C.3.4 Case 4

C.3.4.1.1 An ERTMS/ETCS On-Board equipment that has not implemented the CR 919 (B2 On-Board) will accept or reject the information MA, list of balises in SH, mode profile and SH authorized, according to Table 4 (excerpt of SUBSET-026 v2.3.0, modified by SUBSET-108 v1.2.0, chapter §4.8.3; A=Accepted; R=Rejected).

Information	From RBC	Onboard operating level				
		0	STM	1	2	3
Movement Authority	No	R [1]	R [1]	A [4]	R [1]	R [1]
	Yes	R [2]	R [2]	R [2]	A [3] [4] [5]	A [3] [4] [5]
List of balises for SH area	No	R [1]	R [1]	A	R [1]	R [1]
	Yes	R [2]	R [2]	R [2]	A [3]	A [3]
Mode Profile	No	R [1]	R [1]	A [4]	R [1]	R [1]
	Yes	R [2]	R [2]	R [2]	A [3] [4] [5]	A [3] [4] [5]
SH authorised	No					
	Yes	R	R	R	A [3]	A [3]

[4] exception: the movement authority and, if received together with this movement authority, the mode profile shall be rejected if the SSP and gradient already available on-board or given together with the MA do not cover the full length of the MA.

[5] exception: the movement authority and, if received together with this movement authority, the mode profile shall be rejected if emergency stop(s) have been accepted and are not yet revoked or deleted onboard (see mode transitions).

Table 4 – acceptance of information by B2 ERTMS/ETCS On-Board

C.3.4.1.2 From Table 4 it can be observed that in level 2 and 3, the exceptions [4] and [5] apply to “Movement Authority” and “Mode profile” but not to “List of balises for SH area” - also received from RBC - and not to “SH authorised”.

C.3.4.1.3 From a Movement Authority with both a SH mode profile and a “List of balises for SH area” that would be received by the ERTMS/ETCS On-Board equipment while the exception [4] or [5] is active, only the “List of balises for SH area” will be accepted by the ERTMS/ETCS On-Board (both the MA and the mode profile will be rejected).

C.3.4.1.4 From Table 4 it can also be observed that in level 1, the exception [4] applies to “Movement Authority” and “Mode profile” but not to “List of balises for SH area”.

C.3.4.1.5 From a Movement Authority with both a SH mode profile and a “List of balises for SH area” that would be received by the ERTMS/ETCS On-Board equipment while the exception [4] is active, only the “List of balises for SH area” will be accepted by the ERTMS/ETCS On-Board (both the MA and the mode profile will be rejected).

C.3.4.1.6 Regarding the handling of the accepted list, SUBSET-026 v2.3.0 does not cover this case where the “list of balises for SH area” is accepted alone. Indeed, the clause 3.12.4.4. of SUBSET-026 v2.3.0 says “*In case the mode profile information for shunting is overwritten by a new shunting profile, before the ERTMS/ETCS On-Board equipment switches to SH mode, a previous list of identifiers of balise groups shall be deleted or replaced by a new list of balise groups*”. Stricto sensu, this clause 3.12.4.4 only applies to the case where the mode profile information for shunting is overwritten by a new shunting profile, i.e. does not cover this case of the “list of balises for SH area” accepted alone.

C.3.4.1.7 Note that there is a “hint” in SUBSET-040 v2.3.0 that a new list always replaces an existing one (§4.3.2.1.1. b), but no requirement in SUBSET-026 v2.3.0 to do so.

C.3.4.1.8 Projects shall therefore check that the acceptation of this “list of balises for SH area” will not create any hazardous situation, i.e. that the ERTMS/ETCS On-Board will not end up in SH mode without list of balises for SH area (the correct list for that area).

C.3.4.1.9 Two cases shall be considered for this check:

1) The “list of balises for SH area” is accepted by the ERTMS/ETCS On-Board when another “list of balises for SH area” is already stored ERTMS/ETCS On-Board.

2) A new “list of balises for SH area” is received when the “list of balises for SH area” that has been accepted alone is still stored ERTMS/ETCS On-Board.

C.3.5 Case 5

C.3.5.1.1 It is possible for a B2 trackside that has not implemented the CR 919 to send a “list of balises for SH area” (airgap packet 49) in an MA without sending a mode profile for the SH mode in the same MA. It is even possible for a trackside that has not implemented the CR 919 to transmit by balise group a “list of balises for SH area” without MA. If the ERTMS/ETCS On-Board has not implemented the CR 919 either, it will accept this “list of balises for SH area” received alone (i.e. received without mode profile for SH).

C.3.5.1.2 As in case 4, the projects shall check that the acceptation of this “list of balises for SH area” will not create any hazardous situation.

C.3.6 Case 6

C.3.6.1.1 The clause 3.12.4.4 of SUBSET-026 v2.3.0, v3.4.0 and v3.6.0 says “*In case the mode profile information for shunting is overwritten by a new shunting profile, before the ERTMS/ETCS On-Board equipment switches to SH mode, a previous list of identifiers*

of balise groups shall be deleted or replaced by a new list of balise groups". Stricto sensu, this clause 3.12.4.4 only applies to the case where the mode profile information for shunting is overwritten by a new shunting profile.

C.3.6.1.2 It shall be checked by the project that the ERTMS/ETCS On-Board implementation has not considered a field of application of this clause wider than the strict case of overwriting of Shunting mode profile when the trackside expects a strict reading of the clause.

C.3.6.1.3 Example: a B2 trackside that has not implemented the CR 919 may provide the information for a Shunting area in two subsequent balise groups:

1) The first balise group provides the "list of balises for SH area".

2) The second balise group provides the MA and SH mode profile.

C.3.6.1.4 The ERTMS/ETCS On-Board first receives the "list of balises for SH area" and stores it. At the reception of the MA and SH mode profile, the ERTMS/ETCS On-Board considers that the clause 3.12.4.4 applies and deletes the stored "list of balises for SH area" while the trackside was expecting the ERTMS/ETCS On-Board to keep this list.

C.3.7 Case 7

C.3.7.1.1 Intentionally deleted.

C.3.7.1.2 Intentionally deleted.

C.3.7.1.3 Intentionally deleted.

C.3.8 Case 8

C.3.8.1.1 The request to Shorten MA message can contain a Mode Profile (see ETCS-H0082) and a List of Balises for Shunting.

C.3.8.1.2 According to SUBSET-026 (v2.3.0 and v3.4.0 and v3.6.0), the evaluation of the cooperative shortening in accordance with SUBSET-026 §3.8.6 is not part of the evaluation criteria defined in SUBSET-026 §4.8.

C.3.8.1.3 This means that the check defined in §3.8.6 can only apply in a further step once the cooperative shortening has passed the §4.8.

C.3.8.1.4 This leads to the following problem: the 4.8 filtering is applied simultaneously (and collectively) to the information in the received message, and the cooperative shortening and the list of balise groups are 'Accepted'.

C.3.8.1.5 The cooperative shortening is however subject to the further check defined in SUBSET-026 §3.8.6 but such additional check is not required for the List of BGs.

C.3.8.1.6 The following interpretation of SRS is possible:

C.3.8.1.6.1 The list of balises for Shunting is considered accepted as soon as passing the filter according to SUBSET-026 §4.8.

C.3.8.1.7 Due to C.3.8.1.6.1 the following hazardous scenarios could occur (see also ETCS-H0082):

C.3.8.1.7.1 C.3.8.1.7.2 The list of balises for Shunting is not the correct one to be supervised in SH mode when the ERTMS/ETCS On-Board rejects the cooperative shortening request in a further step since the previous list has been replaced as for C.3.8.1.6.1.

C.3.8.1.8 Trackside should not send request to shorten MA including a SH mode profile.

Appendix D ETCS-H0111 clarification: Examples of hazardous scenarios and mitigations

D.1.1.1.1 Examples with min safe front end (minSFE)

minSFE 1) Trip reaction on passing EOA with min SFE (or min antenna position in Level 1) is not applied when expected by the trackside (SUBSET-026 §4.6.3 condition [12], [16] and §3.13.10.2.6, §3.13.10.2.7)

Hazardous situation: Train approaches EOA with associated release speed. After switching to release speed monitoring, the SvL is no more supervised. If the train passes the EOA, the train will not be tripped when expected by the trackside.
Mitigation: See hazard ETCS-H0001; see also CR1327 for further baselines.

minSFE 2) Application of linking reaction when min SFE leaves expectation window of announced but missed balise group is not performed when expected by the trackside (SUBSET-026 §3.16.2.3.1)

Hazardous situation: A balise group contains safety related information and the linking reaction for that balise group (via linking information) is supposed to lead to a brake reaction if the balise group is missed, but in such case the brake reaction may not be performed when expected by the trackside if no new BG is encountered.

Hazard occurs if the complete balise group was missed or if ERTMS/ETCS On-board reacted only at the end of the expectation window (this could happen even if only one of the balises in the group was missed.[17]) (see Subset-091 ETCS_TR04 “Failure of a balise group being detectable” and ETCS_TR07 “Number of balises in each group”)

Mitigation: Safety related content should be engineered in balise group(s) with more than one balise in the group.

minSFE 3) Trip reaction in SR without Override active on overpassing former EOA with min SFE is not applied when expected by the trackside (SUBSET-026 §4.6.2 [43])

Hazardous situation: A train moves in SR (e.g. driver activates override, but override timer expires) and passes the former EOA with min safe antenna position. The trip reaction may not be performed when expected by the trackside.

Note: Driver is responsible in SR; this protection function will be applied only if the driver tries to pass the signal when override is not active anymore.

Mitigation: Balise group should be engineered including the packet “Stop if in SR”.

Driver shall ask signaller before overpassing a new protected location.

[17] Refer to CR1354 for explanation.

minSFE 4) Trip reaction in SR does not apply while Override is still active, because of large CI, i.e. while Override was not yet finished on passing former EOA/LOA with min safe antenna position (SUBSET-026 §5.8.4.1 c):

Basis for hazardous situation: Train switches from FS/OS to SR. Then the Override procedure should end when the train overpasses the former EOA/LOA with the min safe antenna position. The Override procedure may not be ended when expected even if it is limited by time and distance parameters.
This might be hazardous in the following cases:

- No trip reaction on passing balise group that is not in the list of expected balises related to SR mode (SUBSET-026 §4.6.2 [36]).
  Hazardous situation: The train moves in SR and supervises a list of expected balises related to SR mode. While the Override procedure is still unduly active (see above), the train passes a balise that is not included in the list of expected balises related to SR mode. The trip reaction will not be performed at all (even if the Override procedure ends afterwards).

- Only valid for B2: No trip reaction on overpassing SR distance with estimated front end 4.6.2 [42].
  Hazardous situation: The train moves in SR and the SR distance (national value) is not infinite. While the Override procedure is still active unduly (see above), the train passes the SR distance. The trip reaction may be performed too late or may not be performed at all.

- No trip reaction on reception of information "Stop if in SR mode" (without list of BGs for SR or passed BG not included in list of BGs for SR, SUBSET-026 §4.6.2 [54]).
  Hazardous situation: The train moves in SR and does not supervise a list of expected balises related to SR mode. While the Override procedure is still unduly active (see above), the train passes a balise giving the information "stop if in Staff Responsible". The trip reaction will not be performed at all.
  Hazardous situation: The train moves in SR and supervises a list of expected balises related to SR mode. While the Override procedure is still active unduly (see above), the train passes a balise giving the information "stop if in Staff Responsible" but that balise is not included in the list of expected balises. The trip reaction will not be performed at all.

Note: Driver is responsible in SR. This protection function will fail if the driver tries to pass a location (for example signal, marker board,…) which he should not pass without asking again permission to proceed.

Mitigations:

The max distance in override should not allow to pass two protection locations.

The timer in override should be as short as operationally possible.

Driver shall ask signaller before overpassing a new protected location (the operational permission to enter the next section shall be given by the signaller in each case even if override function is still active).

D.2.1.1.1 Examples with max safe front end (maxSFE)

maxSFE_1) Unexpected early switching to SH mode.

ERTMS/ETCS On-board receives an MA extending beyond several signals with a Shunting Mode Profile at the end, e.g. because the last signal at the end of MA protects a shunting route into a shunting yard.

In case the Max SFE reaches the begin of SH mode profile the ERTMS/ETCS On-board will switch from FS to SH mode via transition [51] in SUBSET-026 §4.6.3:

[51] (A Mode Profile defining the entry of a Shunting area is used on-board) AND (The max safe front end of the train is inside the Shunting area)

This happens when the physical front end of the train is too far in rear of the SH area, the driver will be requested to acknowledge the SH mode within an area where the train is not supposed to be in SH mode (otherwise the service brake will be applied).

Hazardous situation: the train may operate in SH mode in an area where it was not supposed to operate in SH mode. In case of early switch to SH mode the driver could be misled (e.g. in area where SH is operationally not allowed). In case of additional event of route revocation/route cancellation, e.g. by flank protection violation of route in rear of SH area the consequences of potential hazardous situation depends on operational rules, e.g. if the driver (of SH mission) is allowed to pass (main) signal showing a stop aspect (in rear of SH area). Note: In case the (main) signals in rear of SH area are marker boards only, the driver is not aware about the “stop” aspect.

Note: Driver and signaller/shunter are responsible in SH mode.

Mitigation: The trackside should not send SH mode profiles for further location but only SH mode profiles for current location.

Alternative mitigation where/when possible: The trackside should send an MA including an SH mode profile for further location only when the train is detected as being within a defined distance, e.g. based on train position report with new LRBG, in rear of the beginning of the SH mode profile area.

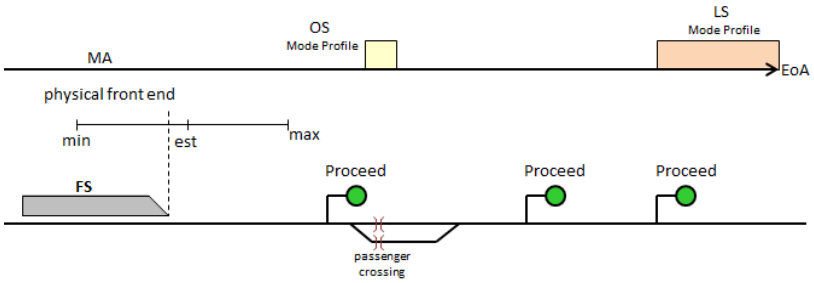
When a driver realises that the on-board mode is SH and he is in rear of marker board or signal without dedicated information to pass the signal in SH, operational rules should exist to force the driver to contact the adequate staff (signaller, shunter, ...).

maxSFE_2) Unexpected switch to LS without performing OS

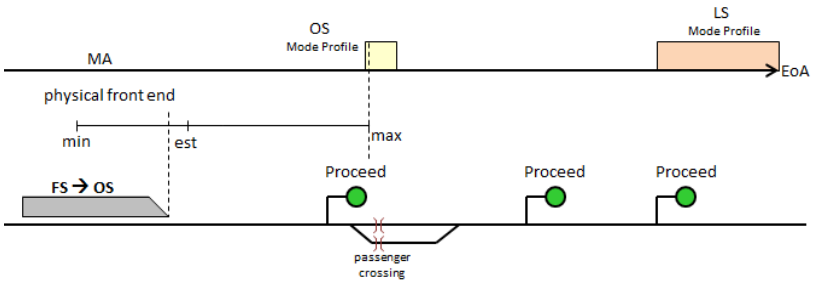
Step 1 - ERTMS/ETCS On-board receives an MA extending beyond several signals with:

- an OS Mode Profile, e.g. in order to pass a passenger crossing in a station and
  (The OS Mode Profile indicates that the SvL is derived from the MA, i.e. Q_MAMODE=0.)
- an LS Mode Profile at the end.
  (The LS Mode Profile indicates that the SvL is derived from the MA, i.e. Q_MAMODE=0.)

… while the train is located with its front ends well in front of the OS mode profile:



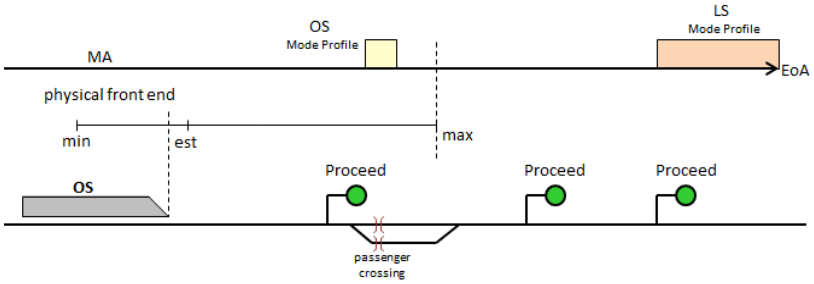
Step 2 - Now the Max SFE may grow and reach the OS section (while the min SFE and est FE remain where they are or move very slow):



According to transition [40] the on-board will immediately switch to OS:

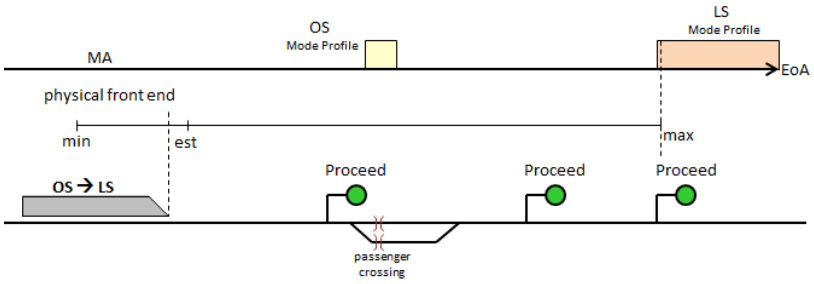
[40] (A Mode Profile defining an On Sight area is on-board) AND (The max safe front end of the train is inside the On Sight area)

Step 3 - Then the Max SFE may grow further and leave the OS section (while the min SFE and est FE remain in rear of the mode profile area):



The on-board remains in OS.

Step 4 - Then the Max SFE may grow even further and reach the LS section (while the min SFE and est FE remain in rear of the mode profile area):



According to transition [74] the on-board will immediately switch to LS:

[74] (A Mode Profile defining a Limited Supervision area is on-board) AND (The max safe front end of the train is inside the Limited Supervision area) AND (The estimated front end of the train is not inside an OS acknowledgement area)

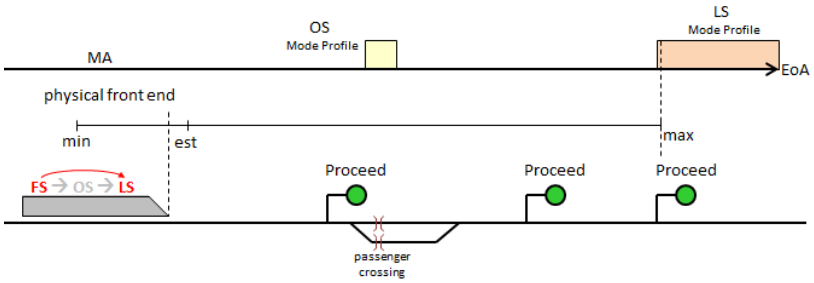
(Let's assume that the Est FE of the train is not inside the OS acknowledgement window)

Consequence: The train may physically be in an OS section with the on-board being in LS mode.

Note: the intermediate steps 2 and 3 may not happen, there might be a sequence step 1 -> step 4. This means there can be a direct switch from FS to LS; it is possible that the transition to OS is skipped altogether. In particular, the driver would not see any request for ack to OS

This may happen when the on-board first considers the Max SFE well in front of the OS section and at the next time the on-board detects that the Max SFE has reached the LS section. In this situation transition [72] may be applied:

[72] (A Mode Profile defining a Limited Supervision area is on-board) AND (The max safe front end of the train is inside the Limited Supervision area)



Note: in the above case it may happen that the train would not proceed, because keeping the beginning of the OS area as temporary EOA, but whether the on-board shall keep it or remove it seems not defined in the SRS.

Mitigations:

- The driver could realise that something is wrong, for example on-board switches to Limited Supervision and asks the driver for acknowledgment. The driver however might know that he does not have the sufficient information to drive in LS - for example he had not seen the signage that would allow him to drive LS, he was not paying attention because coming from a mode of full cab signalling (FS) - and to assume the related responsibility. An operational rule should be imposed, for example that in such cases the driver shall not acknowledge the switch to LS and that after the on-board reaction (brake to standstill) calls the signaller.

- Trackside shall analyse if sending of two mode profile sections, for different modes or same modes with different mode related speeds, in the same MA leads to this hazardous situation or not.

maxSFE 3) Unexpected early transfer of supervision during RBC/RBC handover

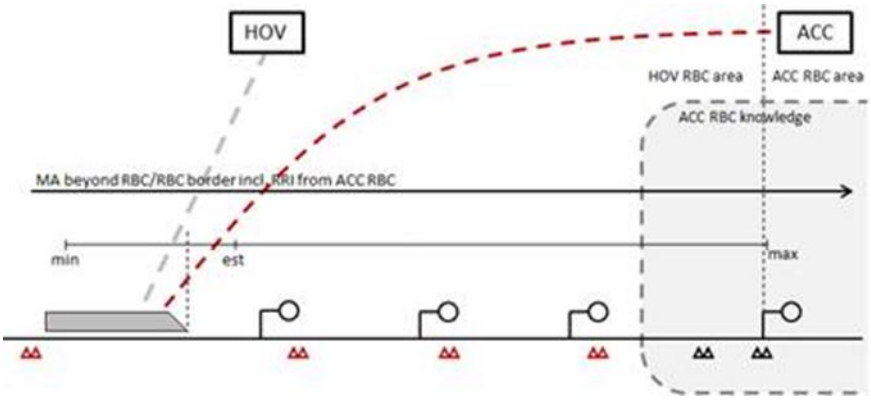
ERTMS/ETCS On-board receives an MA extending beyond several signals and beyond an RBC/RBC border (incl. RRI from ACC RBC).

ERTMS/ETCS On-board receives an RBC Transition Order.

(Let's assume that the ERTMS/ETCS On-board handles two communication sessions, one to HOV and one to ACC RBC.)

As soon as the Max SFE reaches the announced RBC Transition Location, the supervision will be transferred from the HOV to the ACC RBC according to SUBSET-026 §3.15.1.3.5:

3.15.1.3.5 As soon as the on-board sends a position report directly to the Accepting RBC with its maximum safe front end having passed the border, it shall use information received from the Accepting RBC and only a disconnection order shall be accepted from the Handing Over RBC.



It is common practice that the knowledge of the ACC RBC may extend for some range in approach of the border, but typically the ACC RBC is ignoring Position Reports with LRBGs not known to the ACC RBC.

Hazardous situation: any emergency situation within the HOV RBC area can no more be transmitted from HOV RBC to the ERTMS/ETCS On-board, because the ERTMS/ETCS On-board will no more accept any message from the HOV RBC.

Because the LRBG in the position report is not known by the ACC RBC, the ACC RBC cannot send location based information to the train.

Mitigation: See hazard ETCS-H0022.

Moreover Trackside could add additional balise groups to reset the confidence interval (CI) in rear the RBC border, e.g. starting from the LRBG of the RBC transition announcement to the RBC-RBC border BG. This reduces the probability of the potential hazardous situation.

In case of route revocation/route cancellation, e.g. flank protection violation, within the HOV RBC area remaining risk exists.

D.3.1.1.1 Examples with Estimated front end (estFE)

Examples with Estimated front end (estFE):

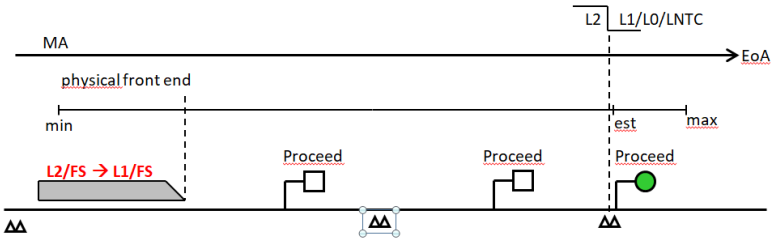
estFE_1) Unexpected early switching of level

ERTMS/ETCS On-board receives an MA extending beyond several signals and beyond a L2 to L0/L1/LNTC border.

ERTMS/ETCS On-board receives a Level transition Order to L0, L1 or LNTC.

As soon as the Estimated FE reaches the announced Level Transition Location, the transition to L0/L1/LNTC will be performed according to SUBSET-026 §5.10.1.5:

5.10.1.5 If the message from the border balise group is not received, the level transition shall still be executed when the estimated front end passes the location given in the announcement.



ERTMS/ETCS On-board will not accept further information from the RBC according to §5.10.1.8 (even Unconditional ES would be rejected):

5.10.1.8 When the onboard has performed the level transition, further data (mainly movement authority and track description data) received from the transmission media of the level being left shall be rejected.

Hazardous situation: in this situation, any emergency situation within the RBC area can no more be transmitted to ERTMS/ETCS On-board, because the ERTMS/ETCS On-board will no more accept any message from the RBC while the train is still in the level 2 area.

Mitigation:

Trackside could add additional balise groups to reset the confidence interval (CI) in rear of the level transition, e.g. starting from the earliest LRBG of the level transition announcement to the level transition border BG. This reduces the probability of the potential hazardous situation.

In case of route revocation/route cancellation within the RBC area a remaining risk exists. For mitigation an assumption of upper limit of CI is necessary.