UNISIG

ERTMS/ETCS

Hazard Items for Baselines Compatibility Assessment

REF : SUBSET-128
ISSUE : 1.0.0
DATE : 22-05-14

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
AZD		
BOMBARDIER		
CAF		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 21-05-14	All	Creation	LR
0.0.2 22-05-14	Various	As per review in SG meeting 22/5/14	LR
1.0.0 22-05-14	-	For delivery	LR

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1 Background and purpose

3.1.1.1 This document is intended as auxiliary information for the “Baseline Compatibility Assessment Final Report” (ref. EUG_UNISIG_BCA): the reader is directed to that report in order to understand the context.

3.1.1.2 This document contains the items of Subset-113 “Report from UNISIG Hazard Log” that are referred by the BCA final report; the items consist in Hazard Log sheets to which that report makes reference in presenting the results of the baselines compatibility assessment.

3.1.1.3 At the time of the delivery of this document, which is contextual to the delivery of the BCA final report, the Subset-113 is undergoing a review process, therefore the hazards sheets contained in the present document may differ from the ones that will be presented in the version of the Subset that will be referenced by the TSI CCS Application Guideline which is foreseen to be issued later in 2014. However, the identities of the hazards will remain unchanged.

3.2 Overview table of correspondence

3.2.1.1 The following table presents the correspondence between the recommendations for the CR entries that in the “BCA Final Report” refer to Subset-113 and the Hazard IDs of such entries:

#	CR ID in BCA report	Hz ID in Subset-113	Link to this document
1	410/923	ETCS-H0035	§ 4.9
2	484	ETCS-H0032	§ 4.8
3	618	ETCS-H0038	§ 4.10
4	650/919	ETCS-H0045	§ 4.13
5	710	ETCS-H0057	§ 4.18
6	712	ETCS-H0054	§ 4.15
7	782	ETCS-H0018	§ 4.3
8	819	ETCS-H0058	§ 4.19
9	842	ETCS-H0016	§ 4.2
10	843	ETCS-H0056	§ 4.17
11	844	ETCS-H0055	§ 4.16
12	854	ETCS-H0024	§ 4.5
13	866	ETCS-H0053	§ 4.14
14	895	ETCS-H0030	§ 4.6

#	CR ID in BCA report	Hz ID in Subset-113	Link to this document
15	896	ETCS-H0041	§ 4.11
16	897	ETCS-H0020	§ 4.4
17	899	ETCS-H0031	§ 4.7
18	961	ETCS-H0042	§ 4.12
19	977	ETCS-H0001	§ 4.1
20	1030	ETCS-H0059	§ 4.20
21	1183	ETCS-H0060	§ 4.21

4. HAZARDS REFERRED IN THE BCA FINAL REPORT

4.1 ETCS-H0001 (CR977)

<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>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 v2.3.0d section 3.13.8 / Subset-026 v3.4.0 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 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 ETCS On-board performs worse than the accuracy requirement for position measured on-board in Subset-041 v2.1.0 and v3.1.0 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 On-board or B2 On-board implementing CR 977.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>The combined probability of these events is 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 on-board performs according to its accuracy requirements. In order to minimise the probability of the 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 On-board delay of 1 sec (according to Subset-041 v3.1.0, 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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.2 ETCS-H0016 (CR842)

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 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 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 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 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 ETCS On-board. --> safety issue, potential collision or derailment, in degraded situation, where route revocation and communication interruption come together.

<table>
<tr><td>Mitigation proposed by RAMS-group</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 CR842 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>On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR842)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR842)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR842)</td></tr>
</table>
</td></tr>
</table>

4.3 ETCS-H0018 (CR782)

Hazard ID	ETCS-H0018
Hazard headline	Implementation of CR782
Hazard description	CR782 introduces a harmonized solution for resetting the odometric confidence interval and relocating all location related information in cases where trackside does not provide information about the distance between balise groups. This solution is defined in Subset-026 v3.4.0 §3.6.4.3b), §3.6.4.7.1 and §3.6.4.7.2.The CR specifies that when no linking distance is known, only the estimated travelled distance between balise groups shall be taken into account for the reset/relocation. This means that any odometric inaccuracies which may have accumulated since reading the previous LRBG are eliminated from the confidence interval. Normally, when using linking, this is safe since the estimated travelled distance is replaced by the actual distance at the relocation, but here in the unlinked case this is not possible. This will lead to an unsafe distance between the position of the max/min safe front end and the position - resulting from a relocation executed according to Subset-026 v3.4.0 §3.6.4.3 - of a location to be supervised. Examples of situations where this could be unsafe is: 1) **Information received from a balise group marked as unlinked** It is not possible to provide linking information for a balise group marked as unlinked. Location related information received from a balise group marked as unlinked cannot be supervised safely if a change of LRBG occurs after the start of supervision, or if another balise group marked as unlinked is encountered. When encountering a new LRBG the locations of any information (e.g. TSR) received from a 'balise group marked as unlinked' might be additionally falsified because the location accuracy of the balise group marked as unlinked (which is Q_NVLOCACC from the national values) will be replaced in the confidence interval by the location accuracy of the new LRBG. Temporary balise groups may be installed with less accuracy than balise groups installed permanently. 2) **Maximum SR distance** In mode SR, linking information is not used (even if it is available, it is only stored On-board for later use in modes FS, OS or LS). The SR distance will not be supervised with the accumulated odometric errors since the start of the supervision, but only with the odometric errors since the last change of LRBG. The end of the SR distance cannot be supervised safely if a change of LRBG occurs after the start of supervision. 3) **Repositioning** It is impossible for trackside to provide the correct linking distance between main balise group and repositioning balise group. Linking information which announces a repositioning BG does not provide the actual linking distance for this BG but only the end of the expectation window. Thus Subset-026 v3.4.0 §3.6.4.3.b) applies when the repositioning balise group becomes the LRBG. Assuming that the repositioning balise group provides linking information, all location related information provided by the repositioning balise group are safely given, but not for information which was given before. This applies: • to locations beyond the train front end, e.g. when the repositioning balise group does not send a speed profile, and the SSP which was provided by the main balise group contains a speed decrease, then the distance to the speed decrease will not be supervised safely because any odometric inaccuracy

	occurring between the main balise group and the repositioning balise group is no longer taken into account; • to locations which have to be supervised with the train rear end, e.g. when a speed restriction on the points, before the location of the repositioning balise group, is supervised with train rear end, then this will not be supervised because odometric errors accumulated between main balise group and repositioning balise group are eliminated from the confidence interval. 4) **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 (i.e. the actual distance from that former LRBG to the current LRBG cannot be determined from the available linking info), then any odometric errors occurring between that former LRBG and the start of the linking chain will be eliminated from the confidence interval and location related information based on that former LRBG cannot be supervised safely. 5) **Encountering unannounced balise groups after the end of the linking chain** Trackside might not include all balise groups in the linking info, e.g. Eurobalises used exclusively to transmit information for national systems may be omitted. Once the last balise group announced in the linking info has been passed, the On-board will regard this as driving without linking info, and will use any balise group marked as linked as LRBG. Any odometric error occurring between the last announced balise group and the new unannounced LRBG will be eliminated from the confidence interval. Because of these potentially hazardous cases, the CR specifies in Subset-026 v3.4.0 §3.6.4.3.1 that wherever deemed necessary, appropriate measures have to be applied, when engineering the distance information. However, in the following cases such engineering will be problematic: • In Baseline 2, CR782 is not mandatory. Therefore, ETCS Trackside engineering has no requirement to implement the necessary measures. Reliance is placed upon each project finding this issue in their hazard analysis. • Some situations above are believed very difficult to mitigate safely by engineering of distance information, even when having discovered the problem: ○ Situations 1, 3, 4 and 5 could be mitigated if ETCS Trackside assumes that the ETCS On-board always respects the requirement on accuracy of distances measured On-board (given in Subset-041 §5.3.1.1, for both v2.1.0 and v3.1.0). This is a performance requirement and thus not guaranteed with any specific safety integrity. ○ Situation 2 is not possible to mitigate, since the ETCS Trackside doesn't know exactly where the supervision of the SR distance starts. It is however possible that such a violation can be considered acceptable since SR distance is anyway only supervised with the estimated position.
Mitigation proposed by RAMS-group	Each specific application safety analysis shall identify if the use of odometric margins as specified in CR782 may require additional safety provisions to be handled by the ETCS System Design / infrastructure owner. Note: In ETCS baseline 3, CR782 was implemented in Subset-026 and the mitigation proposed here was also defined in Subset-026 v3.4.0 §3.6.4.3.1. If found not possible to mitigate the hazardous scenarios, each application must evaluate whether the residual risk can be accepted.

<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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y *)</td><td>Y</td></tr>
<tr><td>B3, X=1</td><td>Y *)</td><td>Y</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>Y</td></tr>
</table>
*) The hazard is applicable only if CR782 is implemented in the ETCS On-board system.
</td></tr>
</table>

4.4 ETCS-H0020 (CR897)

<table>
<tr><td>Hazard ID</td><td>ETCS-H0020</td></tr>
<tr><td>Hazard headline</td><td>Overlap/End Section timer in ETCS On-board less restrictive than trackside</td></tr>
<tr><td>Hazard description</td><td>See Subset-026 v2.3.0d §3.8.4.4, §3.8.4.5 and §3.8.5.1.

Consider the scenario below:

1. RBC sends MA to ETCS On-board, containing overlap and overlap/end section timer
2. Train with the ETCS On-board passes On-board overlap/end section timer start location; timer starts On-board
3. Train with the 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. ETCS On-board restarts the overlap/end section timer
6. Since the overlap/end section timer in the interlocking was started (step Error! Reference source not found.) before the overlap/end section timer in the ETCS On-board (step Error! Reference source not found.), it expires first. The signalman can therefore revoke the overlap/end section at a time when the ETCS On-board still considers it as valid.

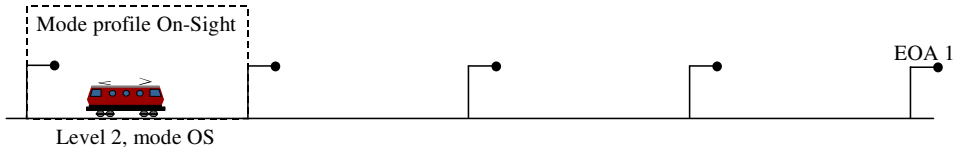
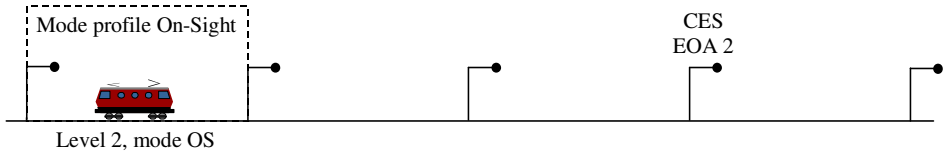
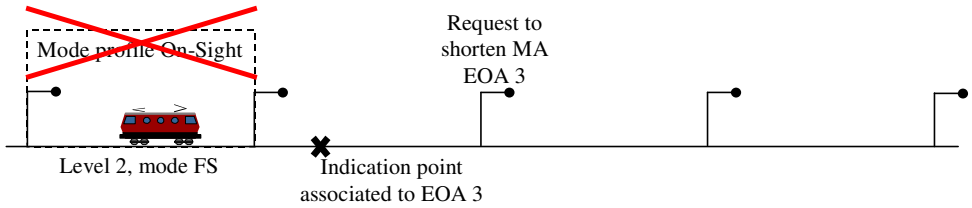
Regarding step Error! Reference source not found.: According to Subset-026 v2.3.0d §3.8.5.1 “A new MA shall always replace the one previously received” and as a consequence the ETCS On-board shall manage accordingly the Section timers (see also Subset-026 v2.3.0d §3.8.4.2.1). However it is not specifically required to restart overlap/end section timer (see also Subset-026 v2.3.0d, §3.8.4.4 and §7.5.1.150).</td></tr>
<tr><td>Mitigation proposed by RAMS-group</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 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 baseline 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 CR897 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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="2">Trackside</td><td>B2</td><td>Y</td><td>N (CR897)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR897)</td></tr>
</table>
</td></tr>
</table>

		B3, X=2	n/a	N (CR897)	

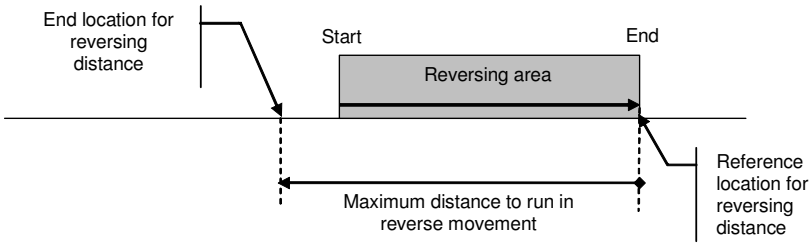
4.5 ETCS-H0024 (CR854)

Hazard ID	ETCS-H0024
Hazard headline	No Mode Profile applied after rejected MA shortening
Hazard description	Following Subset-026 v2.3.0d §4.8.3, 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 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 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 on-board:  2) The RBC sends a Conditional Emergency Stop (to EOA 2) which is accepted and applied 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 on-board): • According to Subset-026 v2.3.0d §4.8.3, the Co-operative Shortening of MA is accepted. • According to Subset-026 v2.3.0d §4.8.3, 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 v2.3.0d §3.8.6.1b), the Co-operative Shortening of MA is granted by the ETCS On-board and the shorter MA is stored on-board;  Nevertheless, according to Subset-026 v2.3.0d §3.12.4.3, as the associated mode profile has been filtered, the one currently supervised on-board should be deleted. As a consequence, the train could switch to Full Supervision mode in an On-Sight area.
Mitigation proposed by RAMS-group	Until CR854 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 ETCS On-board

Mitigation allocated to	TRACKSIDE
Relevant in ETCS baseline	

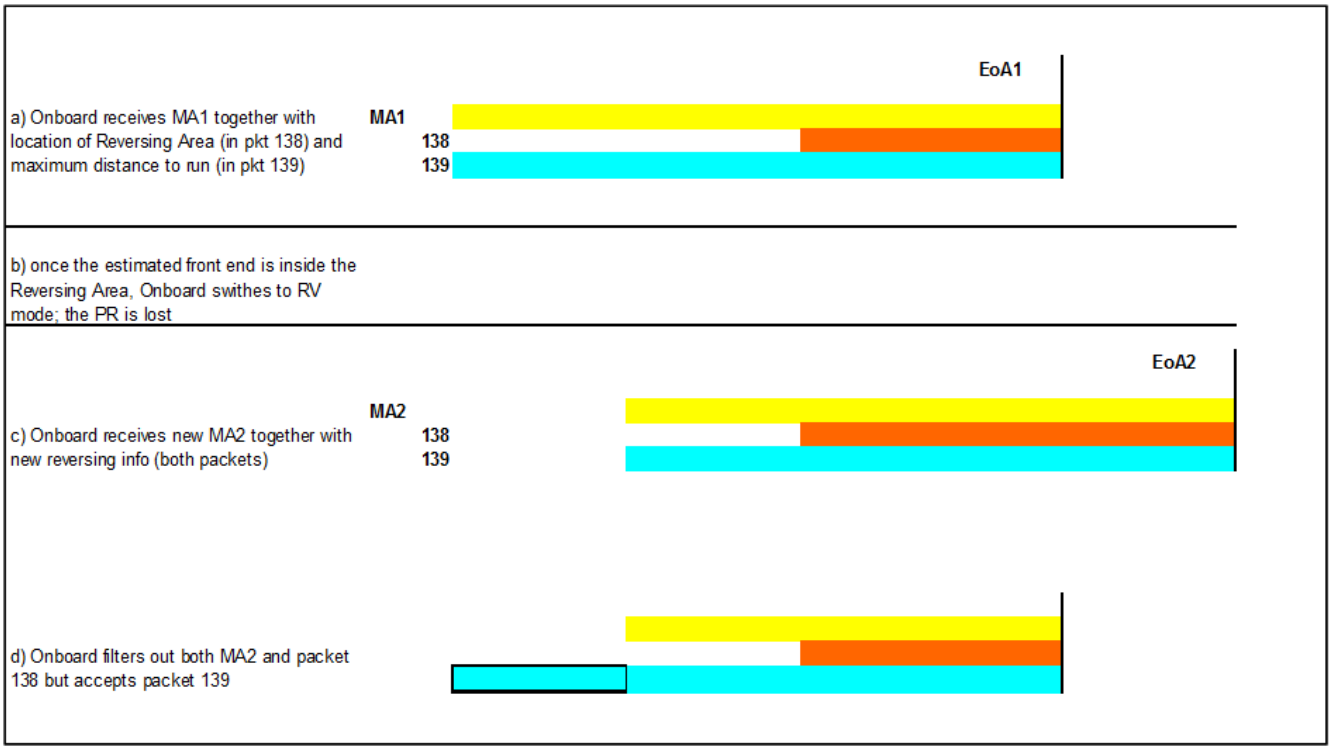
		On-board	
		B2	B3
Trackside	B2	Y	N (CR854)
	B3, X=1	Y	N (CR854)
	B3, X=2	n/a	N (CR854)

4.6 ETCS-H0030 (CR895)

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 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 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 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 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 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 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 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 On-board is different from the one intended by the RBC: the maximum distance to run becomes unduly extended/shortened.

Mitigation proposed by RAMS-group	The mitigations have to be found at project level (specific application), considering the 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	

		On-board	
		B2	B3
Trackside	B2	Y	N (CR895)
	B3, X=1	Y	N (CR895)
	B3, X=2	n/a	N (CR895)



4.7 ETCS-H0031 (CR899)

Hazard ID	ETCS-H0031
Hazard headline	Too many track conditions removed in 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 v2.3.0d §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 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 ETCS On-board. However, an 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 ETCS On-board, without the ETCS trackside intending to do so.
Mitigation proposed by RAMS-group	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 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 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 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, CR899 closes the hazardous situation.
Mitigation allocated to	TRACKSIDE

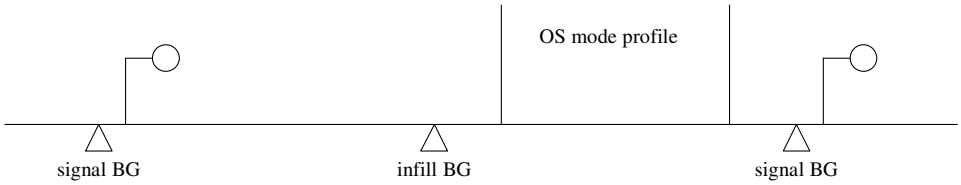
Relevant in ETCS baseline				
			On-board	
			B2	B3
	Trackside	B2	Y	Y
		B3, X=1	Y	N (CR899)
		B3, X=2	n/a	N (CR899)

4.8 ETCS-H0032 (CR484)

<table>
<tr><td>Hazard ID</td><td>ETCS-H0032</td></tr>
<tr><td>Hazard headline</td><td>OS mode profile deleted On-board after receiving an in-fill MA</td></tr>
<tr><td>Hazard description</td><td>Background:

According to Subset-026 v2.3.0d §3.12.4.3 “On the reception of a new MA without Mode Profile the 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 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 CR484 (in baseline 3) modifies Subset-026 as follow:

§3.12.4.3 “On reception of a new MA (with or without Mode Profile) the 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 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</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>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 on-board and the related main BG (infill location reference)</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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR484)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR484)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR484)</td></tr>
</table>
</td></tr>
</table>

4.9 ETCS-H0035 (CR410/923)

<table>
<tr><td>Hazard ID</td><td>ETCS-H0035</td></tr>
<tr><td>Hazard headline</td><td>Train enters L1/2/3 area in L0/SH or LNTC/SH without technical restrictions</td></tr>
<tr><td>Hazard description</td><td>Even if the rule 4.1.4.1 in Subset-040 v2.3.0 (resp. 6.1.1.1.1 in v3.3.0) 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 on-board should implement CR410 (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 v2.3.0d, §4.8.4, a B2 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 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 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 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.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>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.

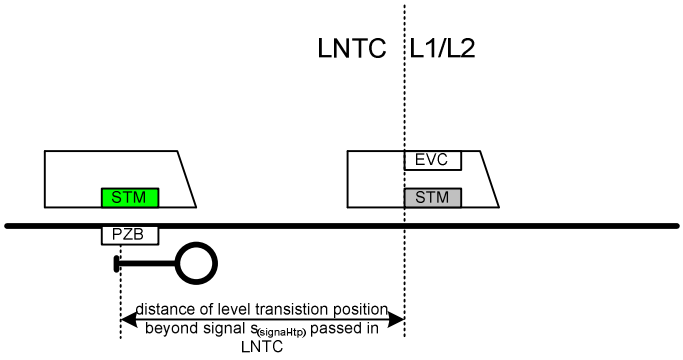
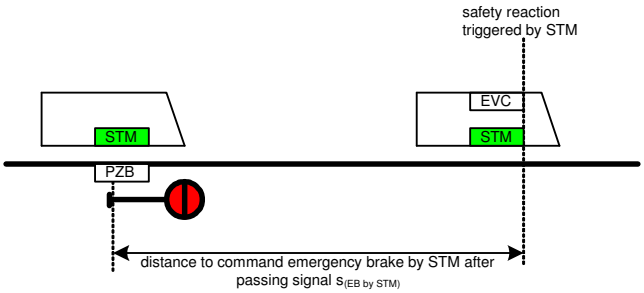
This means that trains passing the border in LNTC/SN without an MA will be tripped by the level transition and trains passing the border in L0/SH or LNTC/SH will be tripped by Danger for Shunting information.

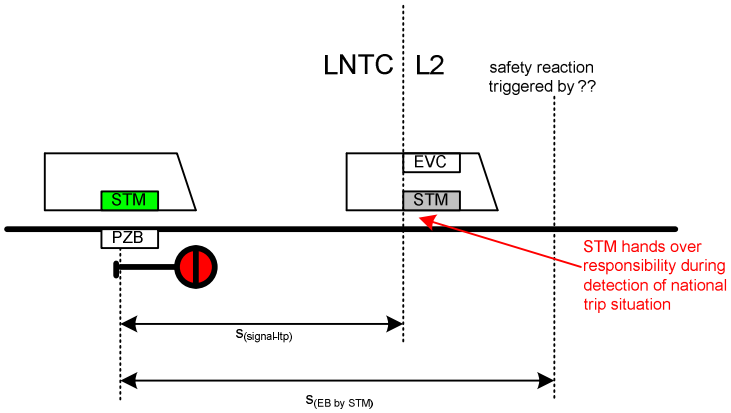
This mitigation will not work for B2 on-boards in LNTC/SH (i.e. implementing CR410) which are not implementing CR 923.

This mitigation will also not work for B2 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.</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>Onboard</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR 923)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR 923)</td></tr>
</table>
</td></tr>
</table>

4.10 ETCS-H0038 (CR618)

Hazard ID	ETCS-H0038
Hazard headline	Level transition from LNTC to L1 or L2 disables emergency brake triggered by STM
Hazard description	**Hazard description:** This possible hazard is valid for those level transitions to L1 or L2 that take place in a certain distance beyond a signal that was passed under responsibility and supervision by a STM. The responsibility of and supervision by the STM ends at the level transition location (LTP) (see figure, grey coloured STM).  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), the STM is responsible for supervision (see figure, green coloured STM). Here, the STM triggers a safety reaction.  Note: Level transition location not considered in figure above. This safety reaction could be disabled in case the level transition is performed during the evaluation of national trip situation by the STM. In this case, no safety reaction is triggered by STM — see following figure.



Justification:

In case of transition from Level NTC to Level 1 or Level 2, the STM shall leave the Data Available (DA) state and enter the Cold Standby (CS) state, see Subset-035 (both v2.1.1 and v3.1.0), section 7.3.2. However, this procedure is blocked if (and as long as) STM sends packet 18 (TRIP) to the EVC (refer to "conditional CS state transition order" in section 7.3.3 of Subset-035 v2.1.1 and v3.1.0). The specification allows for the case that Cold Standby (CS) is entered before the evaluation of the national trip situation is completed.

The interface between EVC and STM is defined in Subset-058:

- The packet 18 informs the EVC that a trip procedure is triggered by the national equipment (STM). The indication report of the adequate packet 18 (TRIP) to the EVC is depending on STM performance itself.
- The packet 14 orders the STM to a specified state (in case a level transition to L2 the state CS will be ordered by EVC).
- The packet 15 informs the EVC about the current STM state.

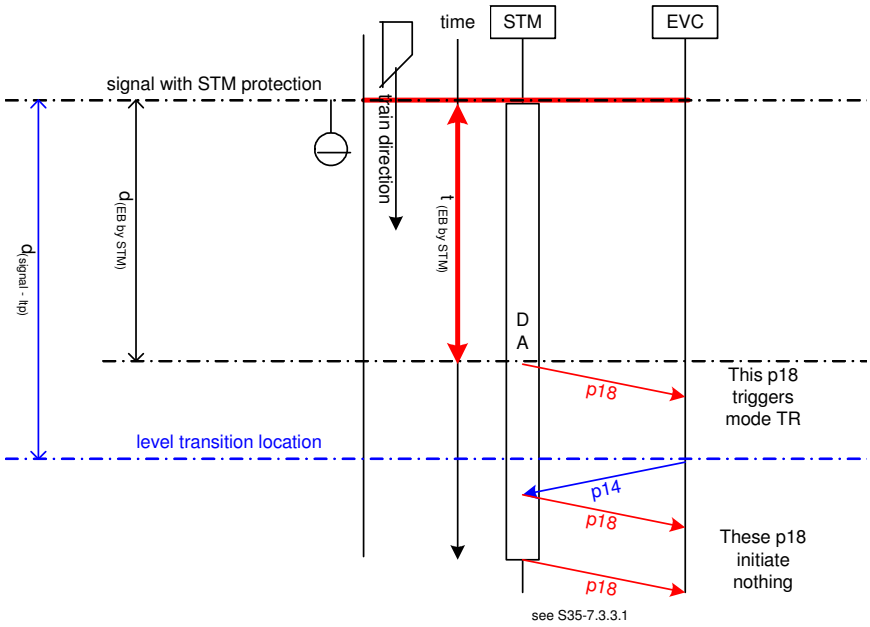
Examples:

Pre-conditions and assumptions for following examples:

1) STM performance (delay time for evaluation, reporting TRIP packet, command EB):
   $t_{(EB\ by\ STM)}$ = 5s -as assumption-
2) Maximum allowed track speed: 160km/h (44,5m/s)
3) Maximum distance between passing the STM controlled signal and indication national trip situation (packet 18 and activating emergency brake) to EVC:
   $d_{(EB\ by\ STM)}$ = 222,5m (= 5s * 44,5m/s)

Example 1:

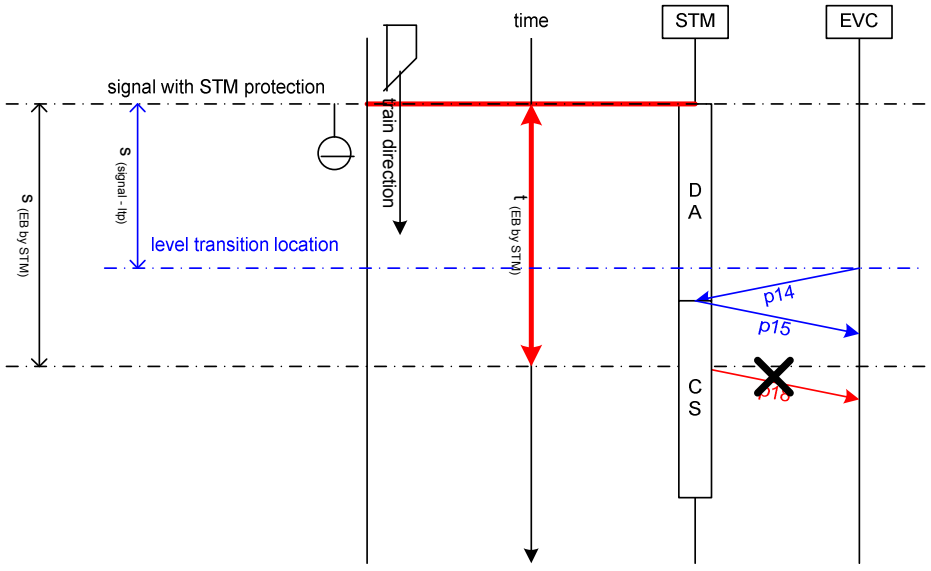
Level transition location (beyond STM protected signal): 250m



The depicted situation above is covered by CR618.

Example 2:

Level transition location (beyond STM protected signal): 200m



P1

8 cannot be sent anymore by the STM as the STM is no more in DA state (Subset-059 §7.2.10).

The depicted situation above is covered by this hazard description and still present after implementation of CR618.

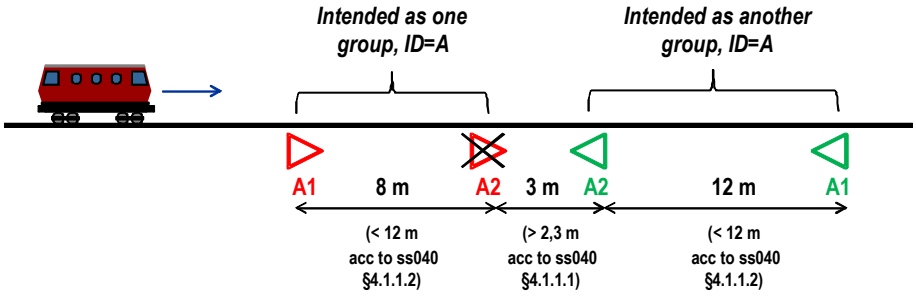
References:

<table>
<tr><td></td><td>UNISIG CR618 (STM has performed it’s safety reaction and safety reaction is not disabled by EVC (e.g. L2/TR))</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>Each trackside application project is responsible to solve this hazard if applicable, by ensuring that the ETCS system won't send an MA if the National system is in a trip condition, or if the MA has been sent the ETCS system needs to ensure that the train is stopped, e.g.:
For level transition from LNTC to L1: define the L1 border in a way that the information for both the STM and the ETCS L1 are given at the signal location.
For level transition from LNTC to L2 (or alternative entries into L1): Based on the national requirements for STM performance or on a product specific analysis, a definition of a safe minimum distance between STM protected signal and level transition location (beyond the signal) could be derived. Note that in case of national system based on continuous transmission, the train could be tripped also after passing the protecting signal.</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="2">On-board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR618)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR618)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR618)</td></tr>
</table>
</td></tr>
</table>

4.11 ETCS-H0041 (CR896)

<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 v2.3.0d chapter 4.8.4, the Acknowledgement of Train Data is rejected by the ETCS On-board in Reversing mode. This can cause a hazardous scenario: An 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
• On-board accept pkt 42 (session management) by BG and contacts RBC
• After initiating the session, 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 On-board because of Subset-026 v2.3.0d 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 On-board according to Subset-026 v2.3.0d table 4.8.4, the RBC cannot update RV information to 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, CR896 solves this problem by specifying that the Acknowledgement of Train Data shall be accepted in Reversing mode.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>Trackside specific application project must be able to demonstrate that the hazard is not relevant.</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>On-board</td><td></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR896)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR896)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR896)</td></tr>
</table>
</td></tr>
</table>

4.12 ETCS-H0042 (CR961)

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 §3.18.4.4.3 it is allowed for an unlinked balise group to have the same identity as another unlinked balise group or as a certain linked balise group. However, this could cause some safety related problems which need to be solved in another way than with unique balise group identifies. Here, two examples are pointed out: Example 1 Subset-036 v3.0.0 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 §6.2.1.6:"The 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, On-board ETCS 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. 1) If green A1 still works: restrictive reaction according to Subset-026 v3.4.0 §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.
Mitigation proposed by RAMS-group	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.

<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>On-board</td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>N</td><td>N</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.13 ETCS-H0045 (CR650/919)

Hazard ID	ETCS-H0045
Hazard headline	Risks related to “List of balises in SH area” function
Hazard description	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 ETCS On-board with Packet 49 “List of balises for SH area”. If the train passes other balises groups, the ETCS On-board will be tripped. However, in some specific situations there is a risk that the 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. Chapter 5 identifies seven such situations.
Mitigation proposed by RAMS-group	Before using the function “List of balises for SH area”, the ETCS trackside specific application shall as a minimum demonstrate that the situations in Chapter 5 will not occur.
Mitigation allocated to	TRACKSIDE + EXTERNAL
Relevant in ETCS baseline	See Chapter 5

4.14 ETCS-H0053 (CR866)

<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 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-026v3.4.0 §4.8.5.7). Thus, depending on when the buffer is evaluated, a B2 on-board may reject a CES that a B3 on-board accepts..</td></tr>
<tr><td>Mitigation proposed by RAMS-group</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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR866)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR866)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR866)</td></tr>
</table>
</td></tr>
</table>

4.15 ETCS-H0054 (CR712)

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 Subest-040 v3.2.0 §4.2.2.2 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 ETCS On-board could – under unfavourable circumstances – systematically reject infill information from a Baseline 2 Euroloop or Radio Infill. The problem is related to CR712 and concerns the fact that Subset-040 v3.2.0 (B3) §4.2.4.4 restricts which packets are allowed to be sent as non-infill information from Euroloop and Radio Infill, while Subset-026 v2.3.0d (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 v2.3.0d so that all packets are allowed to be sent as non-infill information from Euroloop or Radio Infill, while the B3 ETCS On-board makes a strict interpretation according to Subset-040 v3.4.0, the 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 ETCS On-board and Trackside are implemented according to Baseline 3, CR712 makes sure that the problem is solved because Subset-026 v3.4.0 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 v3.3.0 §4.2.4.4).
Mitigation proposed by RAMS-group	In the safety analysis the ETCS trackside should not rely on the ETCS on-board use of information transmitted via Euroloop or Radio Infill (i.e. it should not have safety

<table>
<tr><td></td><td>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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>Y</td></tr>
</table>
</td></tr>
</table>

4.16 ETCS-H0055 (CR844)

<table>
<tr><td>Hazard ID</td><td colspan="4">ETCS-H0055</td></tr>
<tr><td>Hazard headline</td><td colspan="4">Unspecified train movement supervision after PT or RV distance is overpassed</td></tr>
<tr><td>Hazard description</td><td colspan="4">According to subset-026 v2.3.0d, §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 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, CR844 solves 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>Mitigation allocated to</td><td colspan="4">EXTERNAL</td></tr>
<tr><td>Relevant in ETCS baseline</td><td colspan="4"><table>
<tr><td colspan="2"></td><td>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR844)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR844)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR844)</td></tr>
</table></td></tr>
</table>

4.17 ETCS-H0056 (CR843)

<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 v2.3.0d §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 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 now (via CR843) specifies that the exception is only applicable to revocable TSRs.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>The ETCS Trackside 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></td><td></td><td colspan="2">On-board</td></tr>
<tr><td></td><td></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR843)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR843)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR843)</td></tr>
</table>
</td></tr>
</table>

4.18 ETCS-H0057 (CR710)

<table>
<tr><td>Hazard ID</td><td>ETCS-H0057</td></tr>
<tr><td>Hazard headline</td><td>Possible different approaches of B2 and B3 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 on-board with implemented CR710 or B3 on-board deletes received (announced) but not yet applicable NVs (see Subset-026 v3.3.3 section 3.18.2.9). However, this behavior is not expected by ETCS B2 trackside which is not aware of CR710. As B2 trackside does not expect this behavior, it does not send appropriate NVs and thus on-board uses default ones. Therefore, a hazardous situation could arise if:

• an 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 on-board uses default NVs that are less restrictive than expected ones.

Scenario 2

ETCS B2 on-board (without implemented CR710) could keep received (announced) but not yet applicable NVs while ETCS B2 trackside aware of CR710 or B3 X=1 trackside expects these NVs to be deleted by the on-board. Therefore, a hazardous situation could arise if:

• an 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 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 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>Mitigation proposed by RAMS-group</td><td>Scenario 1

The problem is related to situations when 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 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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>Y</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR710)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR710)</td></tr>
</table>
</td></tr>
</table>

4.19 ETCS-H0058 (CR819)

<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 v3.4.0 §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 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 v2.3.0d § 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 behavior, 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>Mitigation proposed by RAMS-group</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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2</td><td>Y</td><td>N (CR819)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR819)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR819)</td></tr>
</table>
</td></tr>
</table>

4.20 ETCS-H0059 (CR1030)

<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 v2.3.0d 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 CR1030. Subset-026 v3.4.0 specifies that the Adhesion Factor (from driver) is unchanged when entering SN mode.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</td><td>For a Baseline 2 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 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></td><td></td><td>On-board</td><td></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3</td></tr>
<tr><td>Trackside</td><td>B2</td><td>N</td><td>N (CR1030)</td></tr>
<tr><td></td><td>B3, X=1</td><td>Y</td><td>N (CR1030)</td></tr>
<tr><td></td><td>B3, X=2</td><td>n/a</td><td>N (CR1030)</td></tr>
</table>
</td></tr>
</table>

4.21 ETCS-H0060 (CR1183)

<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) On-board unexpectedly using default National Values, when these are less restrictive than the National Values.
Related to Subset-026 (both v2.3.0d and v3.4.0) §3.18.2.5 second bullet: a Baseline 2 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 (both v2.3.0d and v3.4.0) §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 ETCS On-board and this is not expected by ETCS trackside.
2) RBC not sending information because it assumes that the On-board has received the information from a BG reported as LRBG.
Related to Subset-026 (both v2.3.0d and v3.4.0) §3.6.2.2.2 a): a Baseline 2 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 (both v2.3.0d and v3.4.0) §3.16.2.4.7. The RBC (B2/B3) cannot know that this message has been rejected.</td></tr>
<tr><td>Mitigation proposed by RAMS-group</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 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>On-board</td><td></td></tr>
<tr><td colspan="2"></td><td>B2 (2.3.0d)</td><td>B3</td></tr>
<tr><td rowspan="3">Trackside</td><td>B2 (2.3.0d)</td><td>Y</td><td>N (CR1183)</td></tr>
<tr><td>B3, X=1</td><td>Y</td><td>N (CR1183)</td></tr>
<tr><td>B3, X=2</td><td>n/a</td><td>N (CR1183)</td></tr>
</table>
If the Baseline 2 ETCS On-board has an implementation in line with the solution of CR1183, the above issues are not applicable, either.</td></tr>
</table>

5. H0045 CLARIFICATION: RISKS RELATED TO "LIST OF BALISES IN SH" FUNCTION

5.1.1 Overview

5.1.1.1 This Chapter 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 ETCS On-board.

5.1.1.2 The risk comes from the fact that the ETCS On-board will not use the list of BGs, whereas the trackside expected it to. This analysis has identified seven cases in which the ETCS On-board will not use the list of balises: the cases are listed in Table 1 and analyzed 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	On-board implementing CR919 on a B2 trackside not implementing that CR
Case 2	The packet 49 is received in "SH Authorised" message when the ETCS On-board is in mode SB without valid train data stored ETCS On-board (typical case: SoM procedure in level 2)	On-board (B2) implementing CR650 and not implementing CR919
Case 3	The SH mode is entered in the execution of "Shunting initiated by driver" procedure	On-board behaving as per new step A050 (introduced by CR919) 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 ETCS On-board while the related MA and mode profile are rejected	On-board (B2) not implementing CR919
Case 5	A "list of balises for SH area" transmitted "alone" by the trackside is accepted by the ETCS On-board	On-board (B2) not implementing CR919 on B2 trackside also not implementing that CR
Case 6	The ETCS On-board has considered a wider field of application of the Subset-026 v2.3.0d and v3.4.0 clause 3.12.4.4 than the trackside	B2 trackside not implementing CR919
Case 7	An in-fill MA with an SH mode profile and a "list of balises for SH area" has been received	No restrictions related to baselines or CRs implemented

Table 1: cases and applicability for the risk

5.1.1.3 Regarding the applicability conditions, it shall be noted that:

- The CR919 is not in the Subset-108 v1.2.0.

- The CR650 is in the Subset-108 v1.2.0 but not classified ("DC").
- A B3 ETCS On-board will always implement the CR919 and CR650; a B3 trackside will always implement the CR919 (the CR650 is about the ETCS On-board).
- A B2 ETCS On-board may already be consistent with the CR919 solution.

5.2 Assumption

5.2.1.1 It is assumed that a trackside that has implemented the CR919 has considered the Chapter 6 of Subset-026 v3.4.0, table 6.5.1.6.5 which revokes for X=1 trackside the airgap modifications brought by the CR, and that an ETCS On-board that has implemented the CR919 has considered the clause 6.6.3.1.1 of Subset-026 v3.4.0 for the data consistency check of the received airgap information.

5.3 Analysis

5.3.1 Case 1

5.3.1.1 It is possible for a B2 trackside that has not implemented the CR919 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 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 CR919 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 ETCS On-board enters in SH mode, the list of balises for SH area.

5.3.1.2 An ETCS On-board equipment that has implemented the CR919 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.

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

5.3.1.4 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.

5.3.2 Case 2

5.3.2.1 An ETCS On-board equipment that has implemented the CR650 without implementing CR919 will accept a "list of balises for SH area" (airgap packet 49) received in mode SB only if valid train data is stored ETCS On-board. This acceptation condition does not apply to the "SH authorised" message (airgap message 28). This means that in case the ETCS On-board equipment receives in mode SB without valid train data being stored ETCS On-board an "SH authorised" message containing a "list of balises for SH area", the ETCS On-board equipment will accept the "SH authorised" message but reject the "list of balises for SH area". The 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.

5.3.2.2 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.

5.3.2.3 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.

5.3.2.4 Note that CR919 (part of baseline 3) closes the potentially hazardous situation.

5.3.3 Case 3

5.3.3.1 An ETCS On-board equipment that has implemented the CR919 has implemented the new step A050 of the "Shunting initiated by driver" procedure (see section 5.6 of Subset-026 v3.4.0). 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 ETCS On-board (typically a B2 trackside), hazardous situations can occur.

5.3.3.2 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 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 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.

5.3.3.3 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.

5.3.3.4 Note that the deletion of the list in step A050, brought by CR919, is "on top" of the table "what happens when a mode is entered" that shows "unchanged" for the switching to SH.

5.3.4 Case 4

5.3.4.1 An ETCS On-board equipment that has not implemented the CR919 (B2 On-board) will accept or reject the information MA, list of balises in SH, mode profile and SH authorized, according to Table 2 (excerpt of Subset-026 v2.3.0d 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 2 – acceptance of information by B2 On-board

5.3.4.2 From Table 2 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”.

5.3.4.3 From a Movement Authority with both a SH mode profile and a “List of balises for SH area” that would be received by the 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 ETCS On-board (both the MA and the mode profile will be rejected).

5.3.4.4 From Table 2 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”.

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

5.3.4.6 Regarding the handling of the accepted list, Subset-026 v2.3.0d 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 v2.3.0d says “In case the mode profile information for shunting is overwritten by a new shunting profile, before the 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.

5.3.4.7 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 v2.3.0d to do so.

5.3.4.8 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 ETCS On-board will not end up in SH mode without list of balises for SH area (the correct list for that area).

5.3.4.9 Two cases shall be considered for this check:

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

5.3.5 Case 5

5.3.5.1 It is possible for a B2 trackside that has not implemented the CR919 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 CR919 to transmit by balise group a “list of balises for SH area” without MA. If the ETCS On-board has not implemented the CR919 either, it will accept this “list of balises for SH area” received alone (i.e. received without mode profile for SH).

5.3.5.2 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.

5.3.6 Case 6

5.3.6.1 The clause 3.12.4.4 of Subset-026 v2.3.0d and v3.4.0 says *“In case the mode profile information for shunting is overwritten by a new shunting profile, before the 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.

5.3.6.2 It shall be checked by the project that the 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.

5.3.6.3 Example: a B2 trackside that has not implemented the CR919 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.

5.3.6.4 The 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 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 ETCS On-board to keep this list.

5.3.7 Case 7

5.3.7.1 The clause 3.12.4.4 of Subset-026 v2.3.0d and v3.4.0 says "*In case the mode profile information for shunting is overwritten by a new shunting profile, before the 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*".

5.3.7.2 In case the mode profile for shunting is partly overwritten by a new shunting mode profile (case of new mode profile received by infill and which therefore replaces the previous mode profile only from main balise group location), the application of the clause 3.12.4.4 may lead to the deletion of the complete list of balise groups related to the previous mode profile.

5.3.7.3 The "list of balises for SH area" part between the infill balise group and the main balise group will therefore not be supervised.