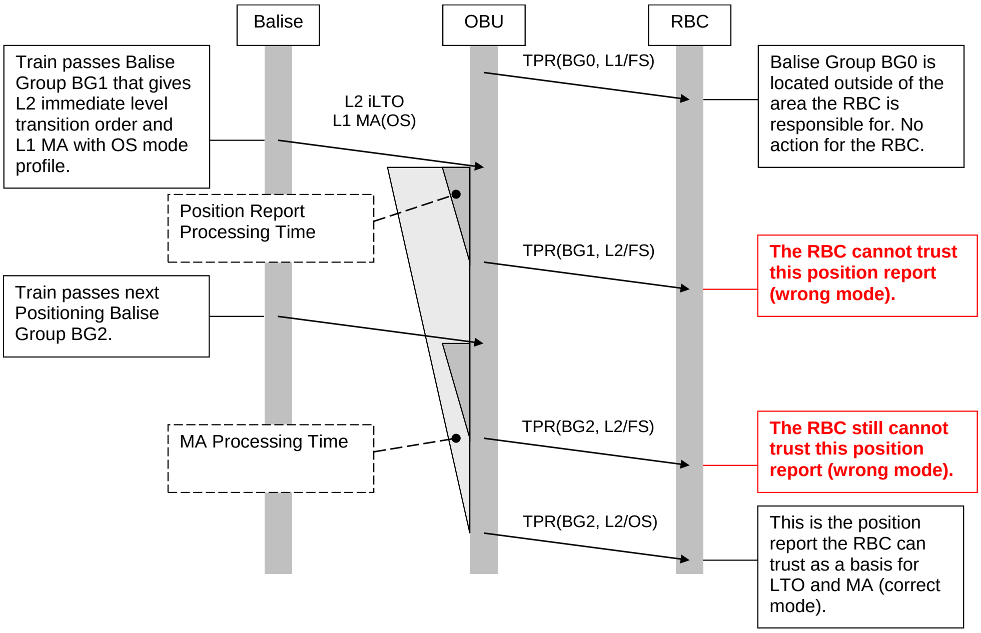
ETCS-H0012

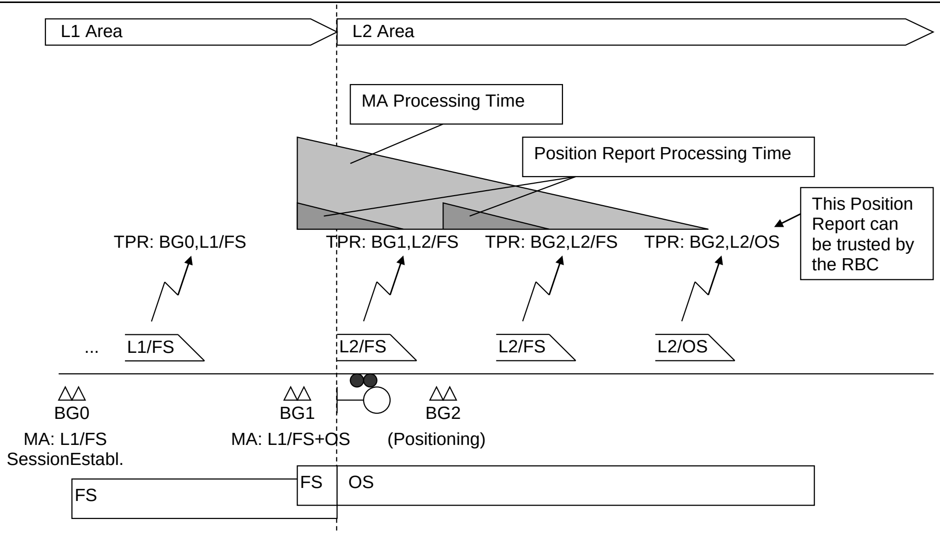
Hazard ID	ETCS-H0012
Hazard headline	ERTMS/ETCS on-board reverts actions related to MA timers while not expected by trackside
Hazard description	The following hazardous scenarios describe how ERTMS/ETCS on-board can have a valid MA on-board while it is not expected by the trackside (The actions related 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.
Mitigation	This has to be solved in trackside project specific analysis. <u>Scenario 1:</u> 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. <u>Scenario 2</u> 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. <u>Scenario 3</u> 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

<table>
<tr>
<td><b>Relevant in ETCS baseline</b></td>
<td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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.  Balise OBU RBC Train passes Balise Group BG1 that gives L2 immediate level transition order and L1 MA with OS mode profile. TPR(BG0, L1/FS) Balise Group BG0 is located outside of the area the RBC is responsible for. No action for the RBC. L2 iLTO L1 MA(OS) Position Report Processing Time TPR(BG1, L2/FS) The RBC cannot trust this position report (wrong mode). Train passes next Positioning Balise Group BG2. MA Processing Time TPR(BG2, L2/FS) The RBC still cannot trust this position report (wrong mode). TPR(BG2, L2/OS) This is the position report the RBC can trust as a basis for LTO and MA (correct mode). The track layout for this scenario looks as below.

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


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

a) Driver interactions

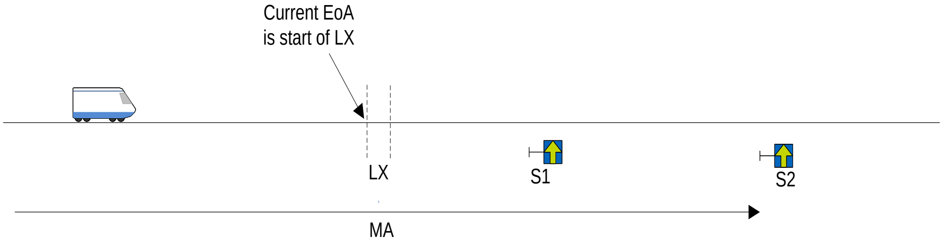
b) Internal triggers, based on the position report parameters

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.
</td>
</tr>
<tr>
<td><b>Mitigation</b></td>
<td>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).</td>
</tr>
<tr>
<td><b>Mitigation allocated to</b></td>
<td>TRACKSIDE</td>
</tr>
<tr>
<td><b>Relevant in ETCS baseline</b></td>
<td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td><b>Trackside</b></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>

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) 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)

<table>
<tr><td></td><td>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><b>Mitigation</b></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><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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 OBU 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 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.
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.
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

ETCS-H0078

<table>
<tr><td><b>Hazard ID</b></td><td>ETCS-H0078</td></tr>
<tr><td><b>Hazard headline</b></td><td>Inhibition of revocable TSRs from balises in L2/3 in SR mode</td></tr>
<tr><td><b>Hazard description</b></td><td>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]:
<i>(“[8] exception: revocable TSRs shall be rejected if information “inhibition of revocable TSRs from balises in L2/3” is stored on-board.”)</i>
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.</td></tr>
<tr><td><b>Mitigation</b></td><td>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.</td></tr>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td><b>Trackside</b></td><td>B2</td><td>N</td><td>n/a</td><td>n/a</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>

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 SUBSET-041 §5.2.1.13 is not also referred to. In case the B2 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 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.
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 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><b>Relevant in ETCS baseline</b></td>
<td>
<table>
<tr><th></th><th></th><th colspan="3">ERTMS/ETCS on-board</th></tr>
<tr><th></th><th></th><th>B2</th><th>B3MR1</th><th>B3R2</th></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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.

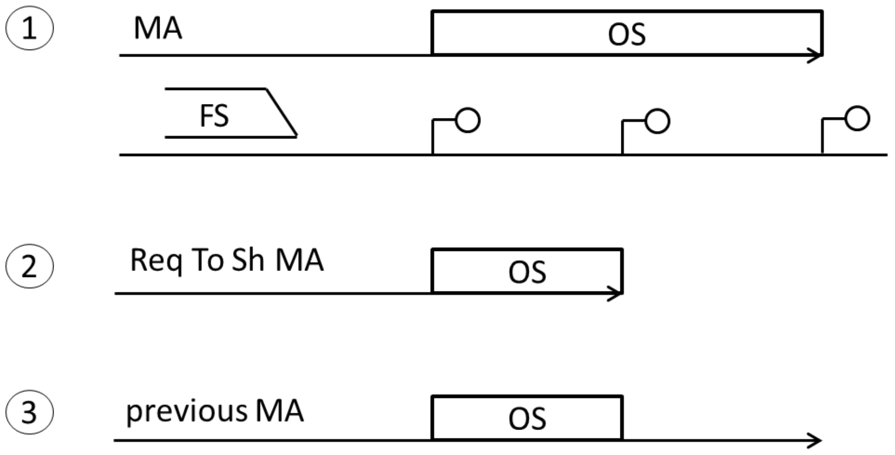
4. Data to be used by an STM (packet 44 with NID_XUSER = 102) received as infill information could also lead to a safety issue. In case such a packet is received from the airgap and considered as non-infill by a B3 on-board due to the rejection or storage of the infill location reference information, 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.
Mitigation	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.

<table>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td colspan="2"></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td colspan="2"></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

ETCS-H0082

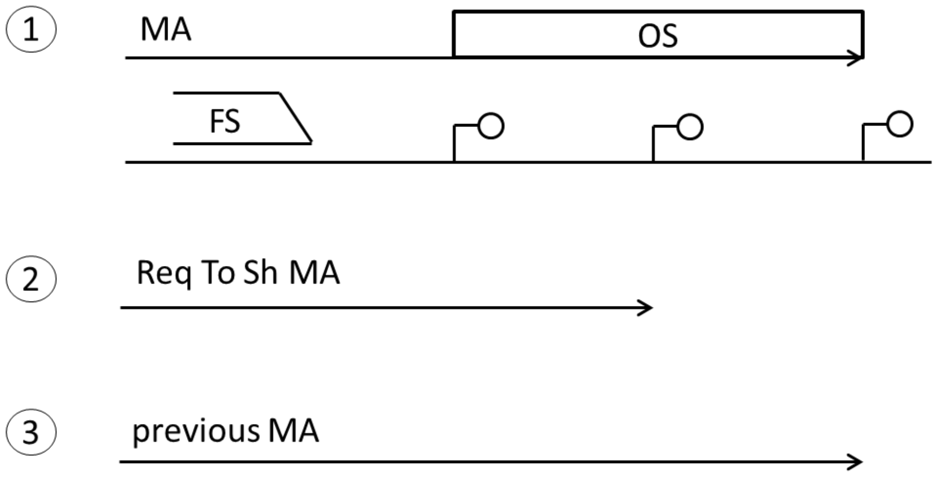
Hazard ID	ETCS-H0082
Hazard headline	Wrong mode profile (OS/LS/SH) and/or list of balises in SH supervised after reception of a Request to Shorten MA.
Hazard description	The RBC sends a request to shorten MA, which includes a proposed shorten MA with an EOA closer to the train than the current EOA/LOA, 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.

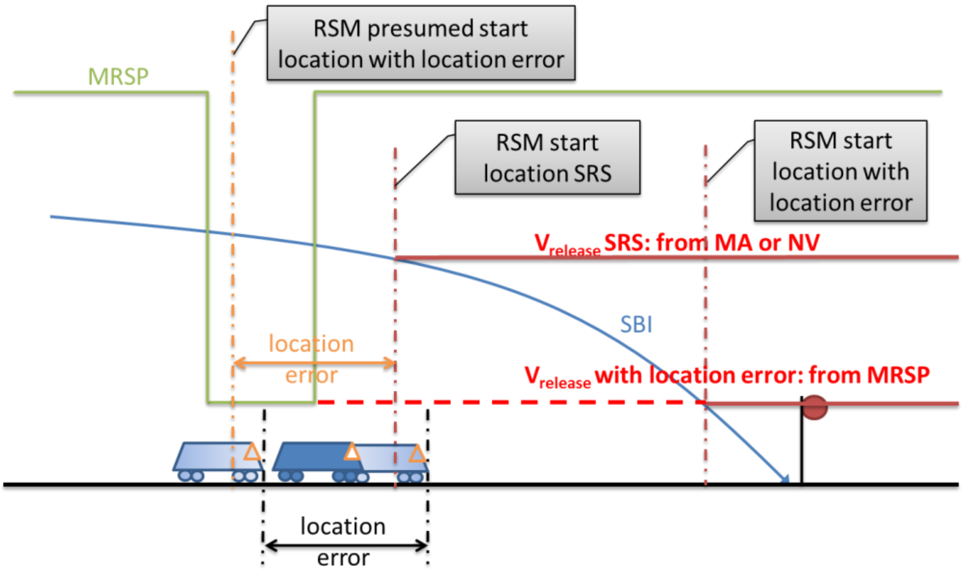
The resulting MA ERTMS/ETCS on-board does not contain any OS mode profile.



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.

<table>
<tr><td></td><td>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.</td></tr>
<tr><td><b>Mitigation</b></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><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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.  RSM presumed start location with location error MRSP RSM start location SRS RSM start location with location error $V_{release}$ SRS: from MA or NV SBI location error $V_{release}$ with location error: from MRSP location error
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.

<table>
<tr><td></td><td>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</td></tr>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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.
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

<table>
<tr>
<td><strong>Relevant in ETCS baseline</strong></td>
<td>
<table>
<tr><th></th><th></th><th colspan="3">ERTMS/ETCS on-board</th></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td><strong>Trackside</strong></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>

ETCS-H0086

<table>
<tr><td><b>Hazard ID</b></td><td>ETCS-H0086</td></tr>
<tr><td><b>Hazard headline</b></td><td>Minimum Safe Rear End position ambiguities</td></tr>
<tr><td><b>Hazard description</b></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.
1. 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><b>Mitigation</b></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><b>Mitigation allocated to</b></td><td>EXTERNAL</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

ETCS-H0087

<table>
<tr><td><b>Hazard ID</b></td><td>ETCS-H0087</td></tr>
<tr><td><b>Hazard headline</b></td><td>Safety issue due to not displayed trackside text message</td></tr>
<tr><td><b>Hazard description</b></td><td>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.

If this 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.</td></tr>
<tr><td><b>Mitigation</b></td><td>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.</td></tr>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

ETCS-H0088

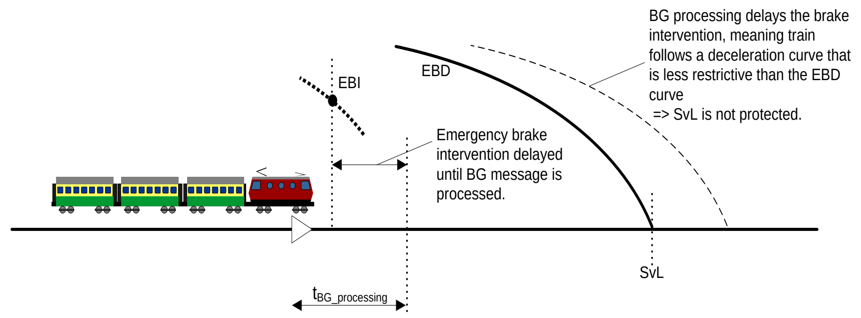
Hazard ID	ETCS-H0088
Hazard headline	Ambiguities in drivers acknowledgement requirements
Hazard description	According to §5.9.2.3 of SUBSET-026, for v2.3.0, v3.4.0 and v3.6.0, the supervision of the driver when a mode transition to OS is executed has to be acknowledged in order to assure the driver is 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.
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),

<table>
<tr><td></td><td>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
• 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><b>Mitigation allocated to</b></td><td>TRACKSIDE and EXTERNAL</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

ETCS-H0089

<table>
<tr><td><b>Hazard ID</b></td><td>ETCS-H0089</td></tr>
<tr><td><b>Hazard headline</b></td><td>Expiration of T_NVCONTACT</td></tr>
<tr><td><b>Hazard description</b></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:<ul><li>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.</li><li>The passage control continues for the area of the first interlocking by RBC sending HP CES.</li></ul>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 OBU will not react according to M_NVCONTACT. The train may enter a not protected route.</td></tr>
<tr><td><b>Mitigation</b></td><td>RBC should not send HP CES in situations where the RBC wants T_NVCONTACT to expire in the OBU.</td></tr>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

ETCS-H0090

Hazard ID	ETCS-H0090
Hazard headline	Possible supervision gap during ERMS/ETCS on-board balise message processing
Hazard description	In Subset-026v3.4.0 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.  BG processing delays the brake intervention, meaning train follows a deceleration curve that is less restrictive than the EBD curve => SvL is not protected. Emergency brake intervention delayed until BG message is processed. 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**

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

ETCS-H0091

<table>
<tr><td><b>Hazard ID</b></td><td>ETCS-H0091</td></tr>
<tr><td><b>Hazard headline</b></td><td>Not supervised TSR depending on packet processing order</td></tr>
<tr><td><b>Hazard description</b></td><td>The following situation has been detected to be hazardous: A BG containing P66 TSR Revocation and P65 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 P65 and P66 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 OBU first uses P65, then P66. The new TSR will be revoked before it was ever supervised.
2) The OBU first uses P66, then P65. The new TSR will be supervised.
If 1) happens, it is a safety issue.</td></tr>
<tr><td><b>Mitigation</b></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, P66 could be transmitted in a first message and P65 in a second message.
For case b), the proper engineering would be to send only P65 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><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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 – 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 – 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><b>Mitigation</b></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><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td>
<table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>

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: o 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). o 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: o 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). o 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 to the use of the default value instead of the actual accuracy, e.g. when the train is in SR mode.

<table>
<tr><td></td><td><ul><li>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).</li></ul></td></tr>
<tr><td><b>Mitigation</b></td><td><p><b>Case 1:</b> 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).</p>
<p><b>Case 2:</b> 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.</p>
<p>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:</p>
<ul><li>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).</li>
<li>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 On-Board and therefore the national values provided by this balise group will not be applied such an On-Board. To avoid possible unsafe consequences of this:
<ul><li>the National Values to be used in the X=1 area should be provided to the B2 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.</li>
<li>the National Values to be used in the X=2 area should be provided to the B2 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).</li></ul></li></ul></td></tr>
<tr><td><b>Mitigation allocated to</b></td><td>TRACKSIDE</td></tr>
<tr><td><b>Relevant in ETCS baseline</b></td><td><table>
<tr><td></td><td></td><td colspan="3"><b>ERTMS/ETCS on-board</b></td></tr>
<tr><td></td><td></td><td>B2</td><td>B3MR1</td><td>B3R2</td></tr>
<tr><td rowspan="5"><b>Trackside</b></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>