UNISIG

ERTMS/ETCS – Class 1

Failure Modes and Effects Analysis for the Interface to/from an Adjacent RBC - in Application Level 2

REF : SUBSET 078
ISSUE : 2.4.0
DATE : 2009-04-07

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
BOMBARDIER		
INVENSYS		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 12-12-00	All		JGM
0.0.2 19-01-01	All	Inclusion of additional Failure Modes and Comments following RAMS Group review.	JGM
0.0.3 09-02-01	All	Inclusion of comments following UNISIG review	JGM
0.0.4 27-03-01	All	Addition of On-Board to RBC Handover functionality	JGM
0.1.0 20-4-01	All	Inclusion of comments following UNISIG review	JGM
2.0.0. 26-02-02		Raised in issue for release to the EEIG	WLH
2.2.2. 21-03-03		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	WLH
2.2.3	All	Review according to new version of SUBSET-039, for discussion in the UNISIG RAMS group	Angelo Chiappini
2.2.4	all	Review after Alcatel comments	Angelo Chiappini
2.2.5	All	Rework according to introduction of SUBSET-098, discussion in the UNISIG RAMS Group	Detlef Skutsch

Issue Number Date	Section Number	Modification / Description	Author
2.2.6	2.1.1.6, 2.1.4.6, 2.1.5.1.1, 2.1.5.6.1, 6.1.1.3	Remove requirement on repetition of Cancellation according to discussion in the UNISIG RAMS Group. Cleanup of Deletion/ Re-sequence handling	Detlef Skutsch
2.2.7	All	Update according to review comments and new edition of Subset-039	Detlef Skutsch
2.2.8 2007-12-13	2.1.7, 2.1.8, 5.1.1	Inserted ACC to HOV Cancellation message, agreed during UNISIG RAMS WG meeting	Detlef Skutsch
2.3.0 2008-10-14		Administrative updates for baseline 2.3.0d agreed during RAMS-meeting	DARI
2.3.1 2009-02-19	3.1.1.8, 4, 5.1.1.2, 5.1.1.3, 6.	Added Request for RRI Confirmation and RRI Conformation messages, for consistence with Subset-039, v2.2.9. Split of chapter 4 and re-numbering FMEA table lines	Detlef Skutsch
2.4.0 2009-04-07		Version 2.4.0 created for official release after UNISIG SC approval. Subset-039 changed to version 2.3.0.	DARI

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1.1.1 The purpose of the analysis is to systematically evaluate and document the potential impact of a failure of each of the mandatory Interface of a RBC to/from an adjacent RBC. Only mandatory Class 1 functions are considered. Each defined functional failure is assessed for its effects on the ETCS system and on train operation assuming that there are no other failures. The effect of each failure on train operation is assigned a severity category based upon the impact of such a failure on the safety of a passenger on the train. Failures that do not affect the safety of a passenger on the train are classed as RAM issues and are not considered any further in this document.

3.1.1.2 The analysis for the Interfaces to/from an Adjacent RBC has been carried out in Application Level 2.

3.1.1.3 The operation mode indicated in the table, refers to the current operational mode of the ETCS on-board, at the moment the analysed message should be exchanged between the RBCs: this is not necessarily the operational mode reported by the on-board and advised by the HOV to the ACC RBC, because in the meantime the operational mode could have changed.

3.1.1.4 The operation mode SL is not treated in this document, because the sleeping unit is remote controlled by the leading unit.

3.1.1.5 Note: In any case, the ACC RBC will send RRI messages according to its own rules and on the basis of the state of trackside in its area and, possibly, of the reported operational mode of the ETCS on-board. Similarly, the RRI messages will be used by the HOV RBC according to its own rules. Such rules are not in the scope of this analysis and are mainly national. For this reason, the analysis performed in this FMEA has to be refined in the application specific safety case.

3.1.1.6 The input documents used as a basis for this study are:

3.1.1.7 UNISIG: Subset –026-3, SRS Chapter 3 Principles, Issue 2.3.0

3.1.1.8 UNISIG: Subset –039, FIS for the RBC/RBC Handover, Issue 2.3.0

3.1.1.9 UNISIG: Subset –037, Euroradio FIS, Issue 2.3.0

3.1.1.10 UNISIG: Subset –098, RBC-RBC Safe Communication Interface, Issue 1.0.0

3.1.1.11 UNISIG: Subset –077, UNISIG Causal Analysis Process, Issue 2.2.2.

4. FMEA

4.1 FMEA RBC-RBC Interface: Handing Over RBC to Accepting RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.1.1.1	Pre-Announcement (The Handing Over RBC informs the Accepting RBC that a given ETCS on-board will enter its area)	**DELETION** **Failure to 'Pre-Announce'**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC fails to inform Accepting RBC of approaching ETCS on-board	RRI not sent to Handing Over RBC	Train allowed to proceed with Override EoA into the Area of the Accepting RBC		RAM Issue		
4.1.1.1.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC fails to inform Accepting RBC of approaching ETCS on-board	RBC not able to send information to the NL unit (e.g., track conditions)	Potential operational abnormalities (e.g., pantograph operations)		RAM Issue		
4.1.1.2.1		**CORRUPTION** **Incorrect 'Pre-Announcement' transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC transmits incorrect identity of train to Accepting RBC	On-board only receives messages with correct ID.	Potential Service Delays		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.1.2.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC transmits incorrect identity of train to Accepting RBC	On-board only receives messages with correct ID.	Potential operational abnormalities (e.g., pantograph operations)		RAM Issue		
4.1.1.2.3			RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC transmits an incorrect border location to the Accepting RBC, such that the Accepting RBC accepts it as a valid border location. Note: if the RBC can understand that the location is not valid, there are no dangerous effects.	Incorrect information Transmitted to ETCS on-board	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1
4.1.1.2.4			RBC Failure RBC Communication failure	Non leading	Handing Over RBC transmits an incorrect border location to the Accepting RBC	Incorrect information sent to the NL unit (e.g. track conditions)	Potential operational abnormalities (e.g. pantograph operations)		RAM issue		
4.1.1.3.1		**DELAY** **Delayed 'Pre-Announcement' message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Delayed start of Handover Procedure; in extreme case same effect as for deletion	In the extreme case will be the same as for 'deleted' message	Train allowed to proceed with Override EoA into the Area of the Accepting RBC		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.1.3.2			RBC Failure RBC Communication failure	Non leading		In the extreme case will be the same as for 'deleted' message	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.1.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any	Handing Over RBC repeats Pre-Announcement message to the Accepting RBC	No effect	No effect		No effect		
4.1.1.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any	Pre-announcement received, that is not appropriate for the accepting RBC. On-Board ID could match with an On-Board that will later be pre-announced, with a different border location	Possible pre-announcement of a train with a different border location than the one that will pre-announced later on. Same effect as for corruption.	Possible wrong route assignment and following wrong RRI generation by ACC. Exceedance of safe speed / distance by train		Catastrophic		Measure against insertion (Sequence Number, TimeStamp, Euroradio MAC) defined in Subset-098 Consistency check of NID_ENGINE and NID_BG in ACC before generating RRI, as defined in Subset-039, 5.1.1.5

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.1.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any	As for deletion in the first step. Then insertion in the second step, depending on the parameter setting of Subset-098	As for deletion in the first step. Then insertion in the second step, depending on the parameter setting of Subset-098	As for deletion in the first step. Then insertion in the second step, depending on the parameter setting of Subset-098		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION Consistency check of NID_ENGINE and NID_BG in ACC before generating RRI, as defined in Subset-039, 5.1.1.5
4.1.1.7		**MASQUERADE** **3rd party pre-announcement message transmitted**	3rd party	Any	Related to a falsified border location, same effect as for corruption	Related to a falsified border location, same effect as for corruption	Related to a falsified border location, same effect as for corruption		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.2.1.1	Route Related Information Request	**DELETION** **Failure to Request Route Related Information**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC fails to request route related information from Accepting RBC	RRI not sent to Handing Over RBC Train allowed to proceed with Override EoA into the Area of the Accepting RBC			RAM Issue		
4.1.2.1.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC fails to request route related information from Accepting RBC	RRI not sent to Handing Over RBC and track conditions not sent to the slave unit	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.2.2.1		**CORRUPTION** **Incorrect Request for Route Related Information**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Accepting RBC receives wrong ETCS on-board ID. This ID might match another OBU that is currently in a handover situation	The ACC RBC either rejects the RRI Request or sends RRI for another ETCS on-board	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Consistency check of NID_ENGINE and NID_BG in ACC before generating RRI, as defined in Subset-039, 5.1.1.5 If not consistent, same effect as for deletion.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.2.2.2			RBC Failure RBC Communication failure	Non leading	Accepting RBC receives wrong ETCS on-board ID.	The ACC RBC either rejects the RRI Request or sends RRI for another ETCS on-board. ETCS on-board will not receive track condition information	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.2.2.3			RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Accepting RBC receives wrong border balise group ID. This ID might match another BBG that is known by the ACC RBC.	The ACC RBC either rejects the RRI request or sends RRI based on wrong BBG. Incorrect information transmitted to ETCS on-board	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Consistency check of NID_ENGINE and NID_BG in ACC before generating RRI, as defined in Subset-039, 5.1.1.5 If not consistent, same effect as for deletion.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.2.2.4			RBC Failure RBC Communication failure	Non leading	Accepting RBC receives wrong border location	Handing Over RBC transmits an incorrect border location to the Accepting RBC Incorrect information transmitted to ETCS on-board. ETCS on-board will not receive track condition information	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.2.2.5			RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Wrong restrictions in RRIR message	The Accepting RBC will send RRI, possibly not usable by the Handing Over RBC The ETCS on-board could not receive information Note: in case of MA shortening, the accepting shall send shorter MA than already accepted by the on-board, so restrictions will not apply)			RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.2.2.6			RBC Failure RBC Communication failure	Non leading	Wrong restrictions in RRIR message	The accepting RBC will send RRI, possibly not usable by the Handing Over RBC. ETCS on-board will not receive track condition information	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.2.3.1		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip		In the extreme case will be the same as for 'deleted' message followed by an 'inserted' message (i.e., a RRI request for a hand-over procedure no more actual)			RAM issue		
4.1.2.3.2			RBC Failure RBC Communication failure	Non leading		In the extreme case will be the same as for 'deleted' message followed by an 'inserted' message (i.e., a RRI request for a hand-over procedure no more actual)	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.1.2.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any	Handing Over RBC repeats message to the Accepting RBC	No Effect, Although may result in performance problems.			RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.2.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any		Inadvertent requests for Route Related Information will have no adverse effects			No effects		
4.1.2.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any		As for DELAY			RAM Issue		
4.1.2.7		**MASQUERADE** **3rd party pre-announcement message transmitted**	3rd party	Any		As for INSERTION			No effects		
4.1.3.1	Announcement (The handing over RBC informs the Accepting RBC that the maximum safe front end of train has passed the location corresponding to the border) It is noted that this message is not used by the accepting RBC	**DELETION** **Failure to Announce**	RBC Failure RBC Communication failure	Any	Handing Over RBC fails to inform Accepting RBC that the maximum safe front end of the train has passed the location corresponding to the border	On-board equipment informs Accepting RBC that the maximum safe front end of the train has passed the location corresponding to the border	None		No effects		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.3.2		**CORRUPTION** **Incorrect 'Announcement' transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any	Accepting RBC receives incorrect Announcement (Incorrect ETCS on-board ID)	On-board equipment transmission of position report takes precedence over RBC transmitted information	None		No effects		
4.1.3.3		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any		In the extreme case will be the same as for 'deleted' message followed by an 'inserted' message (i.e., late announcement of a train already entered).	None		No effects		
4.1.3.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any			None		No effects		
4.1.3.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any			None		No effect		
4.1.3.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any			As for DELAY		No effects		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.3.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any			None		No effects		
4.1.4.1	Cancellation (of Handover) From Handing Over RBC to Accepting RBC	**DELETION** **Failure to Cancel Handover**	RBC Failure RBC Communication failure	Any	Handing Over RBC fails to Cancel Handover	Accepting RBC not made aware of Cancellation of Handover. If a new route is set for the same train through another border location, the reaction of the ACC RBC is manufacturer dependent	RRI could be set for the wrong entry		Catastrophic		No new handover possible with the same NID_ENGINE or same NID_BG, as defined in Subset-039, 5.1.1.5.
4.1.4.2		**CORRUPTION** **Incorrect Cancellation of Handover**	RBC Failure RBC Communication failure	Any	Accepting RBC receives a wrong cancellation message	Accepting RBC terminates the communication session with the wrong on-board equipment. Accepting RBC is not able to revoke RRI anymore	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1
4.1.4.3		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any		The cancellation is performed later than intended. Resources in the ACC are blocked for the delay time.			RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.4.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any			None		No effect		
4.1.4.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any		Accepting RBC terminates the Handover and is not able to revoke RRI anymore	As for CORRUPTION		Catastrophic		Barrier additional to the CORRUPTION: usage of S-098 sequence number
4.1.4.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any	As for DELETION	As for DELETION	As for DELETION		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION Additional barriers as for deletion.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.4.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any			As for INSERTION		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.
4.1.5.1	RRI Confirmation From Handing Over RBC to Accepting RBC	**DELETION** **Failure to give positive or negative RRI Confirmation**	RBC Failure RBC Communication failure	Any	Accepting RBC gets no confirmation on handling a RRI shortening	Accepting RBC not made aware of the result of RRI shortening. As result, the accepting RBC has to consider that that the MA is not successfully shortened on-board, as long as it has not received a positive confirmation (S-039, 6.2.4.2 -- assumed to apply also for missing confirmation).	Accepting RBC cannot re-use the resources blocked by the not successful MA shortening		RAM related		Note: No life sign supervision in this communication

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.5.2.1		**CORRUPTION** **Incorrect RRI Confirmation given to Accepting RBC (negative confirmation turns into positive one)**	RBC Failure RBC Communication failure	Any	Accepting RBC receives an erroneously positive RRI Confirmation message	Accepting RBC could falsely believe that RRI was shortened successfully, and allow usage of the revoked routes for another train	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 (For the effect, please refer to DELETION)
4.1.5.2.2		**CORRUPTION** **Incorrect RRI Confirmation given to Accepting RBC (for wrong RRI shortening)**	RBC Failure RBC Communication failure	Any	Accepting RBC receives a positive RRI Confirmation message for a wrong RRI revocation	Accepting RBC could falsely believe that RRI was shortened successfully, and allow usage of the revoked routes for another train	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 (For the effect, please refer to DELETION)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.5.3		**DELAY** **Delayed RRI Confirmation transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any	Accepting RBC receives a RRI Confirmation message delayed	Accepting RBC is made aware of the result of RRI shortening with a delay. In the meantime, the accepting RBC has to consider that that the MA is not successfully shortened on-board, as long as it has not received a positive confirmation (S-039, 6.2.4.2 -- assumed to apply also for missing confirmation).	Accepting RBC cannot re-use the resources blocked by the not successful MA shortening for some time		RAM related		
4.1.5.4		**REPETITION** **RRI Confirmation transmitted more than once**	RBC Failure RBC Communication failure	Any	Accepting RBC receives same RRI Confirmation multiple times		None		No effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.1.5.5		**INSERTION** **RRI Confirmation when not required**	RBC Failure RBC Communication failure	Any	Accepting RBC falsely receives a positive RRI Confirmation message	If there was a related RRI Confirmation Request sent before, the accepting RBC could falsely believe that RRI was shortened successfully, and allow usage of the revoked routes for another train.	Exceedance of safe speed / distance by train		Catastrophic		Barrier additional to the CORRUPTION: usage of S-098 sequence number
4.1.5.6		**RESEQUENCE** **RRI Confirmation transmitted out of sequence**	RBC Failure RBC Communication failure	Any	As for DELAY	As for DELAY	As for DELAY		RAM related		
4.1.5.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any	As for INSERTION	As for INSERTION	As for INSERTION		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.

4.2 FMEA RBC-RBC Interface: Accepting RBC to Handing Over RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.1.1.1	Route Related Information (initially sent on request, then may be updated also without request)	**DELETION** **Failure to send Route Related Information**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Accepting RBC fails to inform Handing Over RBC of more restrictive route related information	Handing Over RBC does not inform the ETCS on-board of shortened MA	Exceedance of safe speed / distance by train		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. Acknowledgement and repetition. Life Sign supervision in S-039, 6.3.3
4.2.1.1.2			RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Accepting RBC fails to inform Handing Over RBC of extended route related information	Handing over RBC does not extend the MA for the ETCS on-board	Potential Service delays		RAM Issue		
4.2.1.1.3			RBC Failure RBC Communication failure	Non leading	Accepting RBC does not inform Handing Over RBC of track conditions	Handing Over RBC does not inform non leading units of changed track conditions	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.1.2.1		**CORRUPTION** **Incorrect Route Related Information provided**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives incorrect route information (e.g. for wrong train)	Handing Over RBC gives wrong MA to train	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1
4.2.1.2.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives incorrect route information (e.g. for wrong train)	Handing Over RBC gives wrong track conditions to the train	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.1.2.3			RBC Failure RBC Communication failure	Any	Handing Over RBC receives RRI exceeding its capacity	Handing Over RBC is not able to send MA extensions ETCS on-board does not receive information that might be more restrictive (e.g. speed profile, gradients)	Exceedance of safe speed by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption in communication Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.1.3.1		**DELAY** **Delayed Route Related Information message transmitted to Handing Over RBC**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Delay in transmitting more restrictive route related information to Handing Over RBC	ETCS on-board does not receive more restrictive route related information in time	Exceedance of safe speed / distance by train		Catastrophic		Acknowledgement and repetition Life Sign supervision in S-039, 6.3.3
4.2.1.3.2			RBC Failure RBC Communication failure	Non leading	Delay in transmitting more restrictive route related information to handing over RBC	ETCS on-board does not receive more restrictive route related information in time	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.1.4.1		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives a valid RRI multiple times				No Effect		
4.2.1.4.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives a valid RRI multiple times				No Effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.1.5.1		**INSERTION** **Route Related Information message transmitted to handing over RBC when not required**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives an invalid RRI	Potential for inappropriate extension of MA, if the content of the message is not correct (i.e., it does not correspond to the current state of the system)	Exceedance of safe speed / distance by train		Catastrophic		Barrier additional to the CORRUPTION: usage of S-098 sequence number
4.2.1.5.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives an invalid RRI	Potential for inappropriate track condition information, if the content of the message is not correct (i.e., it does not correspond to the current state of the system)	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.1.6.1		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Sequence of messages is altered, RRI followed by shortened RRI is received in opposite order	An older message could be received and overwrite valid information with information no more valid	Exceedance of safe speed/distance by the train		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.1.6.2			RBC Failure RBC Communication failure	Non leading	Sequence of messages is altered	An older message could be received and overwrite valid information with information no more valid	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.1.7.1		**MASQUERADE** **3rd party message transmitted**	3rd party	Full supervision On Sight Staff Responsible Trip Post Trip	As for Insertion		Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade in communication Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.
4.2.1.7.2			3rd party	Non leading	As for insertion		Potential operational abnormalities (e.g., pantograph operations)		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.2.1	Request for RRI Confirmation (Used for shortening MAs)	**DELETION** **Failure to send Request for RRI Confirmation**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Accepting RBC fails to inform Handing Over RBC of more restrictive route related information	Handing Over RBC does not inform the ETCS on-board of shortened MA	Exceedance of safe speed / distance by train		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. Ack. and repetition. Life Sign supervision in S-039, 6.3.3 HOV does not send a RRI Confirmation. According to S-039, 6.2.4.2, the ACC has to consider that the MA is not shortened on-board (assumed to apply also for missing confirmation).
4.2.2.2.1		**CORRUPTION** **Incorrect Request for RRI Confirmation provided**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives incorrect MA and mode profile (e.g. for wrong train)	Handing Over RBC gives wrong MA and mode profile to train	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1
4.2.2.2.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives incorrect MA and mode profile (e.g. for wrong train)	Handing Over RBC gives wrong MA and mode profile to the train	None, because NL units do nothing with the MA and mode profile		No Effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.2.3.1		**DELAY** **Delayed Request for RRI Confirmation message transmitted to Handing Over RBC**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Delay in transmitting more restrictive MA and mode profile to Handing Over RBC	ETCS on-board does not receive more restrictive MA and mode profile in time	Exceedance of safe speed / distance by train		Catastrophic		Acknowledgement and repetition Life Sign supervision in S-039, 6.3.3 HOV does not send a RRI Confirmation in the expected time. According to S-039, 6.2.4.2, the ACC has to consider that the MA is not shortened on-board (until a positive confirmation is received)
4.2.2.3.2			RBC Failure RBC Communication failure	Non leading	Delay in transmitting more restrictive MA and mode profile to handing over RBC	ETCS on-board does not receive more restrictive MA and mode profile in time	None, because NL units do nothing with the MA and mode profile		No Effect		
4.2.2.4.1		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives a more restrictive MA and mode profile multiple times				No Effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.2.4.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives a more restrictive MA and mode profile multiple times				No Effect		
4.2.2.5.1		**INSERTION** **Request for RRI Confirmation message transmitted to handing over RBC when not required**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Handing Over RBC receives a more restrictive MA and more profile than necessary	MA is shortened or more restrictive than necessary			RAM issue		
4.2.2.5.2			RBC Failure RBC Communication failure	Non leading	Handing Over RBC receives a more restrictive MA and more profile than necessary	ETCS on-board receives a more restrictive MA and more profile than necessary	None, because NL units do nothing with the MA and mode profile		No effect		
4.2.2.6.1		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip	Sequence of messages is altered, RRI followed by Request for RRI Confirmation is received in opposite order	An older message could be received and overwrite valid information with information no more valid	Exceedance of safe speed/distance by the train		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.2.6.2			RBC Failure RBC Communication failure	Non leading	Sequence of messages is altered	An older message could be received and overwrite valid information with information no more valid	None, because NL units do nothing with the MA and mode profile		No effect		
4.2.2.7.1		**MASQUERADE** **3rd party message transmitted**	3rd party	Full supervision On Sight Staff Responsible Trip Post Trip	As for Insertion	As for Insertion	MA is shortened or more restrictive than necessary		RAM Issue		
4.2.2.7.2			3rd party	Non leading	As for Insertion	As for Insertion	None, because NL units do nothing with the MA and mode profile		No effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.3.1	Taking Over Responsibility (Accepting RBC informs Handing Over RBC that it has taken Over)	**DELETION** **Failure to send take over information**	RBC Failure RBC Communication failure	Any	Accepting RBC fails to inform Handing Over RBC that it has taken over responsibility for the train	Handing Over RBC maintains message transmission to ETCS on-board Handing Over RBC receives a position report from ETCS on-board that the min safe rear end has crossed the border, and sends a disconnection order to the ETCS on-board			No Effect		
4.2.3.2		**CORRUPTION** **Incorrect Take Over information transmitted to handing over RBC**	RBC Failure RBC Communication failure	Any	Handing Over RBC commands a non intended ETCS on-board (wrong ETCS on-board ID) to terminate the communication, while maintaining the communication to the intended ETCS on-board.	Non intended ETCS on-board is not connected to an RBC anymore. Handing Over RBC receives a position report from intended ETCS on-board that the min safe rear end has crossed the border, and sends a disconnection order to this ETCS on-board	No MA revocations can be transmitted to the non intended on-board		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption in communication. Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1
4.2.3.3		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any		Handing Over RBC keeps the connection to the ETCS On-Board longer than required			No effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.3.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any	Accepting RBC repeats the transmission of the take over message	Handing Over RBC will have stopped sending route related information to the ETCS on-board			No Effect		
4.2.3.5.1		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure - Third Party Insertion	Full supervision On Sight Staff Responsible Trip Post Trip	Inadvertent Take Over message received by Handing Over RBC	Handing Over RBC stops sending route related information to ETCS on-board No more route revocations can be sent to the ETCS on-board	Exceedance of safe speed / distance by train		Catastrophic		Barrier additional to the CORRUPTION: usage of S-098 sequence number
4.2.3.5.2			RBC Failure RBC Communication failure - Third Party Insertion	Non leading	Inadvertent Take Over message received by Handing Over RBC	Handing Over RBC stops sending route related information to ETCS on-board	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.3.6.1		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Full supervision On Sight Staff Responsible Trip Post Trip		As for delay. Remark: Accepting RBC has taken over the responsibility of the train.	As for delay		No effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.3.6.2			RBC Failure RBC Communication failure	Non leading		As for delay	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		
4.2.3.7.1		**MASQUERADE** **3rd party message transmitted**	3rd party	Full supervision On Sight Staff Responsible Trip Post Trip	As for insertion	As for insertion	As for insertion		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade in communication. Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.
4.2.3.7.2			3rd party	Non leading		As for insertion	Potential operational abnormalities (e.g., pantograph operations)		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.4.1	Cancellation (of Handover) From Accepting RBC to Handing Over RBC	**DELETION** **Failure to Cancel Handover**	RBC Failure RBC Communication failure	Any	Accepting RBC fails to Cancel Handover	Handing Over RBC not made aware of Cancellation of Handover, but Accepting RBC assumes Handover as being cancelled. Later route revocations are not sent by ACC by means of a shortened RRI because there is no handover from ACC point of view.	Exceedance of safe speed / distance by train		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. Acknowledgement and repetition. Life Sign supervision in S-039, 6.3.3
4.2.4.2		**CORRUPTION** **Incorrect Cancellation of Handover**	RBC Failure RBC Communication failure	Any	Handing Over RBC receives a wrong cancellation message	Handing Over RBC terminates the Handover process for the wrong on-board equipment. Accepting RBC is not able to revoke RRI anymore	Exceedance of safe speed / distance by train		Catastrophic		Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.4.3		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any	The cancellation is performed later than intended.	In the meantime, the train passes the RBC border while the Accepting RBC intends to have the train stopped in rear of the border. Same effect as for delay of shortened RRI.	Exceedance of safe speed / distance by train		Catastrophic		Acknowledgement and repetition. Life Sign supervision in S-039, 6.3.3, for long delays
4.2.4.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any			None		No effect		
4.2.4.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any	Handing Over RBC terminates a handover that was not intended by the Accepting RBC	Handing Over RBC shortens the MA to the RBC-RBC border, train will not pass the border	No further handover possible at the border location or for the affected on-board, as the related resources are blocked in the Accepting RBC		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.2.4.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any	As for DELAY	As for DELAY	As for DELAY		Catastrophic		Usage of S-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION Additional barriers as for deletion.
4.2.4.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any	As for DELETION	As for DELETION	As for DELETION		Catastrophic		Usage of the EuroRadio MAC for revelation of masquerade Message is discarded as safety reaction defined in Subset-037, 7.2.2.2.1 Apply S-091, section 5.4.

4.3 FMEA RBC-RBC Interface: Accepting RBC to/from Handing Over RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.3.1.1	Acknowledgement (for any message)	**DELETION** **Failure to send acknowledgment**	RBC Failure RBC Communication failure	Any		The sender will repeat the message, with updated information			No effect		
4.3.1.2		**CORRUPTION** **Incorrect acknowledgment transmitted to handing over RBC**	RBC Failure RBC Communication failure	Any		Incorrect message could be misunderstood as an acknowledgment and stop the repetitions in sending of a message			Note 1		
4.3.1.3		**DELAY** **Delayed message transmitted to Accepting RBC**	RBC Failure RBC Communication failure	Any		In the extreme case will be the same as for 'deleted' message followed by an 'inserted' message (i.e, acknowledgement of an old message, that, under very pessimistic assumptions, might be misunderstood as the acknowledgement of an actual message)			Note 1		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Failure Rate	Internal Barriers
					Local	Intermediate	End				
4.3.1.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication failure	Any			None		No effect		
4.3.1.5		**INSERTION** **Message transmitted when not required**	RBC Failure RBC Communication failure	Any		If the inserted acknowledgement refers to an "unknown" message, it will have no effect. If the inserted message refers to a "known" message, it will stop its repetition. In this case, if the previous messages have not been received, it may cause the deletion of information.			Note 1		
4.3.1.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication failure	Any		As for DELAY			Note 1		
4.3.1.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any		As for INSERTION			Note 1		

Note 1: The effects are the same as for the deletion of the message, whose sending is stopped: See in the table the effects of deletion for the different types of messages.

5. TRACEABILITY

5.1.1.1 This section lists the mandatory functions analysed from the FIS for the RBC/RBC Handover, UNISIG: Subset –039 and the On-board to RBC functions from the SRS Chapter 3, Principles, UNISIG: Subset –026-3.

5.1.1.2 Information from the “Handing Over” RBC to the “Accepting” RBC

1) Pre-Announcement

2) Route Related Information Request

3) Announcement

4) Cancellation

5) RRI Confirmation

5.1.1.3 Information from the “Accepting” RBC to the “Handing Over” RBC

1) Route Related Information

2) Request for RRI Confirmation

3) Taking Over Responsibility

4) Cancellation

5) Life Sign (considered as a barrier)

5.1.1.4 Information in Both Directions

1) Acknowledgement

6. CONCLUSIONS

6.1.1.1 No inconsistencies and open points were found during the analysis.