U-N-I-S-I-G

ERTMS/ETCS

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

REF : SUBSET-078
ISSUE : 3.5.0
DATE : 07-05-24

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

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 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
2.4.1 2011-03-18	All chapters 4.x	Split different messages into sub-sections of chapter 4.x; Update for SUBSET-039, 3.0.0; changed severity RAM related to RAM Issue, according to updated SUBSET-077	Detlef Skutsch

Issue Number Date	Section Number	Modification / Description	Author
2.4.2 2011-05-11	3.x, 4.1.6.3, 4.1.6.6	Update after internal review in UNISIG RAMS WP: Update of references in chapter 3; added internal barriers to 4.1.6.3 and 4.1.6.6; traceability of Life Sign from 5.1.1.3 to 5.1.1.4.	Detlef Skutsch
2.4.3 2011-07-11	3.x, 4.x	Update during RAMS Meeting and based on review comments	Detlef Skutsch
3.0.0 2011-09-30	All changes	Accept all changes that were agreed, formal update	Detlef Skutsch
3.1.0 2012-01-19	3.x (references), 4.1.6.1 & -.3 (train data), 4.1.7 (IDs in the FMEA), 4.x & 5.x (references to S-037)	Correcting reference IDs in 4.1.7, check to be in-line with S-026 3.2.1, S-039 3.0.2, S-037 2.3.6	Detlef Skutsch
3.2.0 2012-02-24		Update during RAMS meeting	Dag Ribbing
3.3.0 2012-03-12		Baseline 3 release version	Dag Ribbing
3.3.1 2014-04-16	Chapters 3 and 4	Update according to SUBSET-039, v3.1.0, for B3 MR1	Detlef Skutsch
3.3.2 2014-05-08		Baseline 3 1st maintenance release version	Dag Ribbing
3.3.3 2014-10-01	3.1.1.6, 3.1.1.7, 3.1.1.8, 3.1.1.9	Editorial modification as per ERA comment	Alfonso Nardo
3.3.4 2016-02-15	3.1.1.4, 3.1.1.5 (editions of input documents)	Proposal for Baseline 3 2nd release	TS
3.3.5 2016-04-19	3.1.1.4 (revoke of change which was introduced in ed. 3.3.4)	Proposal for Baseline 3 2nd release with UNISIG WP RAMS review comments	TS
3.3.6 2016-06-14	3.1.1.6	Update of reference to SUBSET-026 and 077.	Martin Vlcek

Issue Number Date	Section Number	Modification / Description	Author
3.4.0 2016-06-20	No change	Baseline 3 2nd release version	RAMS WP
3.4.1 2022-10-27	§ 3.1.1.4, § 3.1.1.5, chapter 4, 5 and several editorials	Proposal for Baseline 4 based on SUSBET-039 (ed. 3.2.3 – considering CR940, CR988, CR1238, CR1244, CR1335, CR1342, CR1377, CR1397, CR1409); “Level 2/3” replaced with “Level R"; § 3.1.1.4 consideration of modes which are out of scope; § 3.1.1.5 update of input documents; updated FMEA sheets (AD mode); CR1367 (ERA solution proposal 14.10.2022) - consideration of new messages (Ch. 4 FMEA and Ch.5 Traceability)	TS
3.4.2 2023-02-07		Proposal for Baseline 4 based on SUSBET-039 (ed. 3.9.2)	TS
3.4.3 2023-09-28		Proposal for Baseline 4 (planned edition for SUBSET-078 is 3.5.0) based on SUSBET-039 (ed. 4.0.0); additionally, “Level R” renamed back to “Level 2"; FMEA tables checked with regard to the released editions of the input documents used.	TS
3.4.4 2023-10-25		Incorporation of review remarks made during RAMS WP meeting	RAMS WP
3.4.5 2024-04-17		Application of Quality checks proposed by SG.	TS

Issue Number Date	Section Number	Modification / Description	Author
3.5.0 07-05-24	No change	Baseline 4 release version	RAMS WP

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 an RBC to/from an adjacent RBC. Only mandatory ETCS 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 following shall be noted about the scope of this analysis:

- The operational modes SH, UN, SL, SB, SF, IS, National System, RV, PS are not treated in this document, because RBC-RBC handover according to SUBSET-039 is not triggered by these modes.
- 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 forwarded to the relevant ETCS on-board equipment 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.
- Any operational turnaround movement[1] is not considered in this analysis, as it is assumed that this does not occur in the RBC-RBC area (SUBSET-040 §4.2.4.10.4).
- Both the ACC RBC and the HOV RBC are assumed to be of a system version X=3. Any other combinations of X=1, X=2 and X=3 RBCs will have to be analysed in the application specific safety case, outgoing from the rules in SUBSET-039 and SUBSET-129.

[1] E.g. mode switch from FS/OS to SM or vice versa.

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

3.1.1.6 SUBSET-026, SRS Chapter 3 Principles

3.1.1.7 SUBSET-039, FIS for the RBC/RBC Handover

3.1.1.8 SUBSET-037, Chapter 2 Euroradio FIS Safety Layer

3.1.1.9 SUBSET-098, RBC-RBC Safe Communication Interface

3.1.1.10 SUBSET-077, UNISIG Causal Analysis Process.

3.1.1.11 Note: Deviating from the FMEA definition in SUBSET-077, the column ‘Failure Rate’ is removed from the following tables because no quantification was performed.

4. FMEA

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

4.1.1 Pre-Announcement

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre	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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre	Handing Over RBC transmits incorrect identity of train to Accepting RBC	On-board only receives messages with correct ID.	Potential Service Delays		RAM Issue	
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 Limited Supervision Automatic Driving Supervised Manoeuvre	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-037-2, 2.6.2.3.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre	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	
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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 plus TimeStamp) defined in SUBSET-098 Identification of RBC/RBC HOV transaction by NID_ENGINE and NID_BG, as defined in SUBSET-039, 4.3.1.1 Pre-announcement for existing transaction (after first RRI Request) or for either existing transaction for NID_ENGINE or NID_BG is considered as cancellation condition in SUBSET-039, 4.3.1.4, 4.3.1.5, 4.3.1.6

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 SUBSET-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION Identification of RBC/RBC HOV transaction by NID_ENGINE and NID_BG, as defined in SUBSET-039, 4.3.1.1 Pre-announcement for existing transaction (after first RRI Request) or for either existing transaction for NID_ENGINE or NID_BG is considered as cancellation condition in SUBSET-039, 4.3.1.4, 4.3.1.5, 4.3.1.6

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.1.7		**MASQUERADE** **3rd party pre-announcement message transmitted**	3rd party	Any	Related to a falsified but valid border location, same effect as for corruption	Related to a falsified but valid border location, same effect as for corruption	Related to a falsified but valid 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-037-2, 2.6.2.3.2.1 Apply SUBSET-091, section 5.4.

4.1.2 Route Related Information Request

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre	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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre	Accepting RBC receives wrong ETCS on-board ID. This ID might match another OBU that is currently in a handover situation	The ACC RBC 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, 7.2.3.2.1 Identification of RBC/RBC HOV transaction by NID_ENGINE and NID_BG, as defined in SUBSET-039, 4.3.1.1 If not consistent to an existing RBC/RBC HOV transaction, same effect as for deletion.
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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.2.2.3			RBC Failure RBC Communication Failure	Full supervision On Sight Staff Responsible Trip Post Trip Limited Supervision Automatic Driving Supervised Manoeuvre	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, 7.2.3.2.1 Identification of RBC/RBC HOV transaction by NID_ENGINE and NID_BG, as defined in SUBSET-039, 4.3.1.1 If not consistent to an existing RBC/RBC HOV transaction, same effect as for deletion.
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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.2.2.5			RBC Failure RBC Communication Failure	Full supervision On Sight Staff Responsible Trip Post Trip Limited Supervision Automatic Driving Supervised Manoeuvre	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	
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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving Supervised Manoeuvre		In the extreme case will be the same as for 'deleted' message followed by an 'inserted' message (i.e., an 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., an 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	
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 effect	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 effect	

4.1.3 Announcement

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 effect	
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 effect	
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 effect	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 effects	
4.1.3.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication Failure	Any			As for DELAY		No effects	
4.1.3.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any			None		No effects	

4.1.4 Cancellation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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. RBC/RBC HOV transaction is still active in Accepting RBC while cancelled in Handing Over RBC. If a new route is set for the same train through another border location, the reaction of the ACC RBC is manufacturer dependent	Next Pre-Announcement for the same NID_ENGINE or NID_BG is considered as cancellation condition for Accepting RBC (SUBSET-039, 4.3.1.4, 4.3.1.5, 4.3.1.6), while not be used to establish a new transaction (SUBSET-039, 4.3.1.7).		RAM issue	
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, 7.2.3.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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	
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 SUBSET-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 SUBSET-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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

4.1.5 RRI Confirmation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 an 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 (SUBSET-039, 4.5.1.4).	Accepting RBC cannot re-use the resources blocked by the not successful MA shortening		RAM Issue	
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, 7.2.3.2.1 (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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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, 7.2.3.2.1 (For the effect, please refer to DELETION)
4.1.5.3		**DELAY** **Delayed RRI Confirmation transmitted to Accepting RBC**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives an 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 (SUBSET-039, 4.5.1.4).	Accepting RBC cannot re-use the resources blocked by the not successful MA shortening for some time		RAM Issue	
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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 SUBSET-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 Issue	
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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

4.1.6 Train Data

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.6.1	Train Data From Handing Over RBC to Accepting RBC	**DELETION** **Failure to forward changed train data to Accepting RBC**	RBC Failure RBC Communication Failure	Any	Accepting RBC gets no information on changed train data	Accepting RBC not made aware of a change of the train data. The Accepting RBC cannot correct an already given RRI (due to new train data or shortened route). The basis for following RRI information generated by the Accepting RBC might be wrong.	Accepting RBC provides RRI that does not fit to the train data or is not able to shorten its previously given RRI. Exceedance of safe speed / distance by train		Catastrophic	Usage of SUBSET-098 sequence number If setting N>1 a justification is required. Acknowledgement and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
4.1.6.2		**CORRUPTION** **Incorrect Train Data given to Accepting RBC**	RBC Failure RBC Communication Failure	Any	Accepting RBC gets wrong information on changed train data.	The basis for following RRI information generated by the Accepting RBC might be wrong.	Accepting RBC provides RRI that does not fit to the train data. 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, 7.2.3.2.1 (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	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.6.3		**DELAY** **Delayed transmission of changed train data to Accepting RBC**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives information on changed train data later than intended	Accepting RBC made aware of a change of the train data later than intended. The Accepting RBC cannot correct an already given RRI in time (due to new train data or shortened route). The basis for following RRI information generated by the Accepting RBC might be wrong until the change of train data is received.	Accepting RBC provides RRI that does not fit to the train data or is not able to shorten its previously given RRI. Exceedance of safe speed / distance by train		Catastrophic	Acknowledgement and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
4.1.6.4		**REPETITION** **Update of train data is transmitted more than once**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives same information on changed train data multiple times	Accepting RBC has to acknowledge these train data and probably has to send new RRI	The MA might be shortened to the border in the meantime, depending on the Handing Over RBC reaction		RAM Issue	
4.1.6.5		**INSERTION** **Train Data are given to Accepting RBC that are not intended**	RBC Failure RBC Communication Failure	Any	As for CORRUPTION	As for CORRUPTION	As for CORRUPTION		Catastrophic	Barrier additional to the CORRUPTION: usage of SUBSET-098 sequence number

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.6.6		**RESEQUENCE** **Train data transmitted out of sequence**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives train data and another message in a wrong order	If the re-sequenced message triggers an RRI generation, it may be based on outdated train data. As for DELAY	As for DELAY		Catastrophic	Usage of SUBSET-098 sequence number If setting N>1 a justification is required.
4.1.6.7		**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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

4.1.7 Train Running Number

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.7.1	Train Running Number From Handing Over RBC to Accepting RBC	**DELETION** **Failure to inform the Accepting RBC about the train running number**	RBC Failure RBC Communication Failure	Any	Accepting RBC gets no information about (the change of) the train running number	Accepting RBC might assign a wrong train running number to a train that is handed over	Potential operational abnormalities (e.g., wrong train routing). Train running number is not used for safety related decisions.		RAM Issue	
4.1.7.2		**CORRUPTION** **Incorrect train running number given to Accepting RBC**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives a wrong train running number for a running handover	Accepting RBC assigns a wrong train running number to a train	As for DELETION		RAM Issue	
4.1.7.3		**DELAY** **Train running number transmitted to Accepting RBC with a delay**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives a (change of a) train running number with a delay	Accepting RBC is made aware of the train running number with a delay. In the meantime, the handover is progressing and might be finished with a missing or unknown train running number.	As for DELETION		RAM Issue	
4.1.7.4		**REPETITION** **Train running number transmitted more than once**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives a (change of a) train running number multiple times		None		No effect	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.7.5.1		**INSERTION** **(Correct) train running number transmitted when not required**	RBC Failure RBC Communication Failure	Any	As for REPETITION		None		No effect	
4.1.7.5.2		**INSERTION** **(Wrong) train running number transmitted when not required**	RBC Failure RBC Communication Failure	Any	As for CORRUPTION	As for CORRUPTION	As for CORRUPTION		RAM Issue	
4.1.7.6		**RESEQUENCE** **Train running number is transmitted out of sequence**	RBC Failure RBC Communication Failure	Any	Accepting RBC receives an outdated (wrong) train running number for a running handover or a train running number for a not running handover	As for CORRUPTION	As for CORRUPTION		RAM Issue	
4.1.7.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Any	As for CORRUPTION	As for CORRUPTION	As for CORRUPTION		RAM Issue	

4.1.8 Safe consist length information for SM

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.8.1	SCL information for SM From Handing Over RBC to Accepting RBC	**DELETION** **Failure to inform the Accepting RBC about SCL information**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC gets no information about SCL information	Accepting RBC might not be able to assign a SCL information a train that is handed over (pre-announced train in SM mode)	Accepting RBC provides SM RRI that does not fit to the train data. Exceedance of safe speed / distance by train.		Catastrophic	Usage of SUBSET-098 sequence number If setting N>1 a justification is required. Acknowledgement required and repetition.
4.1.8.2		**CORRUPTION** **Incorrect train SCL information given to Accepting RBC**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC receives a wrong SCL information for a running handover	Accepting RBC assigns a wrong SCL information to a train.	Exceedance of safe speed / distance by train (in case SCL too low).		Catastrophic	Usage of the EuroRadio MAC for revelation of corruption Message is discarded as safety reaction defined in SUBSET-037, 7.2.3.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.8.3		**DELAY** **SCL information transmitted to Accepting RBC with a delay**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC receives SCL information with a delay	Accepting RBC made aware of a change of the SCL information later than intended. The Accepting RBC cannot correct an already given SM RRI in time (due to new SCL information or shortened route). The basis for following SM RRI information generated by the Accepting RBC might be wrong until the change SCL is received.	Accepting RBC provides SM RRI that does not fit to the SCL information. Exceedance of safe speed / distance by train		Catastrophic	Acknowledgement required and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
4.1.8.4		**REPETITION** **SCL information transmitted more than once**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC receives SCL information multiple times	Accepting RBC has to acknowledge these SCL information and probably has to send new SM RRI	The MA might be shortened to the border in the meantime, depending on the Handing Over RBC reaction		RAM issue	
4.1.8.5		**INSERTION** **(Wrong) SCL information transmitted when not required**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	As for CORRUPTION	As for CORRUPTION	As for CORRUPTION		Catastrophic	Barrier additional to the CORRUPTION: usage of SUBSET-098 sequence number

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.1.8.6		**RESEQUENCE** **SCL information is transmitted out of sequence**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC receives an outdated (wrong) SCL information for a running handover or a train running number for a not running handover	As for CORRUPTION	As for CORRUPTION		Catastrophic	Barrier additional to the CORRUPTION: usage of SUBSET-098 sequence number
4.1.8.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Supervised Manoeuvre	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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

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

4.2.1 Route Related Information

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 more restrictive MA	Exceedance of safe speed / distance by train		Catastrophic	Usage of SUBSET-098 sequence number If setting N>1 a justification is required. Acknowledgement and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
4.2.1.1.2			RBC Failure RBC Communication Failure	Full supervision On Sight Staff Responsible Trip Post Trip Limited Supervision Automatic Driving	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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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, 7.2.3.2.1
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, 7.2.3.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 RBC/RBC communication supervision in SUBSET-039, 4.4
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 Limited Supervision Automatic Driving	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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 SUBSET-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 Limited Supervision Automatic Driving	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 SUBSET-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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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, 7.2.3.2.1 Apply SUBSET-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	

Note: This message is not foreseen in SM mode, therefore the operation mode SM is not considered in table above.

4.2.2 Request for RRI Confirmation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 SUBSET-098 sequence number If setting N>1 a justification is required. Ack. and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4 HOV does not send an RRI Confirmation. According to SUBSET-039, 4.5.1.4, the Accepting RBC has to consider that the MA is not shortened on-board until a positive confirmation is received.
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 Limited Supervision Automatic Driving	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, 7.2.3.2.1

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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	
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 Limited Supervision Automatic Driving	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 RBC/RBC communication supervision in SUBSET-039, 4.4 HOV does not send an RRI Confirmation in the expected time. According to SUBSET-039, 4.5.1.4, the Accepting RBC 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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	Handing Over RBC receives a more restrictive MA and mode profile multiple times				No Effect	
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 Limited Supervision Automatic Driving	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	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 SUBSET-098 sequence number If setting N>1 a justification is required. For setting N=1, please refer to DELETION
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 Limited Supervision Automatic Driving	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	

Note: The Accepting RBC shall not send route related information containing a shortened MA with request for confirmation for an ETCS on-board equipment pre-announced in SM mode (SUBSET-039 §4.5.2.4.1), therefore the operation mode SM is not considered in table above.

4.2.3 Taking Over Responsibility

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 indicating that the border is passed by the minimum safe rear end of the train, or, from a similar position report with integrity confirmed, and sends a disconnection order to the ETCS on-board			No Effect	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 indicating that the border is passed by the minimum safe rear end of the train, or, from a similar position report with integrity confirmed 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, 7.2.3.2.1
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	
4.2.3.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication Failure	Any	Accepting RBC repeats the transmission of the takeover message	Handing Over RBC will have stopped sending route related information to the ETCS on-board			No Effect	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 Limited Supervision Automatic Driving	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 SUBSET-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 Limited Supervision Automatic Driving		As for delay. Remark: Accepting RBC has taken over the responsibility of the train.	As for delay		No effect	
4.2.3.6.2			RBC Failure RBC Communication Failure	Non leading		As for delay	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	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.2.3.7.1		**MASQUERADE** **3rd party message transmitted**	3rd party	Full supervision On Sight Staff Responsible Trip Post Trip Limited Supervision Automatic Driving	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, 7.2.3.2.1 Apply SUBSET-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	

4.2.4 Cancellation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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 SUBSET-098 sequence number If setting N>1 a justification is required. Acknowledgement and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
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, 7.2.3.2.1
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. RBC/RBC communication supervision in SUBSET-039, 4.4, for long delays

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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	
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 SUBSET-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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

4.2.5 SM Route Related Information

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.2.5.1	SM Route Related Information (initially sent on request, then may be updated also without request)	**DELETION** **Failure to send SM Route Related Information**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Accepting RBC fails to inform Handing Over RBC of more restrictive SM route related information	Handing Over RBC does not inform the ETCS on-board of more restrictive MA	Exceedance of safe speed / distance by train		Catastrophic	Usage of SUBSET-098 sequence number If setting N>1 a justification is required. Acknowledgement required and repetition. RBC/RBC communication supervision in SUBSET-039, 4.4
4.2.5.2		**CORRUPTION** **Incorrect SM Route Related Information provided**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	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, 7.2.3.2.1
4.2.5.3		**DELAY** **Delayed SM Route Related Information message transmitted to Handing Over RBC**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Delay in transmitting more restrictive SM route related information to Handing Over RBC	ETCS on-board does not receive more restrictive SM route related information in time	Exceedance of safe speed / distance by train		Catastrophic	Acknowledgement and repetition RBC/RBC communication supervision in SUBSET-039, 4.4

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
4.2.5.4		**REPETITION** **Message transmitted more than once**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Handing Over RBC receives a valid SM RRI multiple time				No Effect	
4.2.5.5		**INSERTION** **SM Route Related Information message transmitted to handing over RBC when not required**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Handing Over RBC receives an invalid SM 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 SUBSET-098 sequence number
4.2.5.6		**RESEQUENCE** **Message transmitted out of sequence**	RBC Failure RBC Communication Failure	Supervised Manoeuvre	Sequence of messages is altered, SM RRI followed by shortened/ restrictive SM 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	Barrier as for DELETION
4.2.5.7		**MASQUERADE** **3rd party message transmitted**	3rd party	Supervised Manoeuvre	As for INSERTION	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, 7.2.3.2.1 Apply SUBSET-091, section 5.4.

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

4.3.1 Acknowledgement

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
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	Internal Barriers
					Local	Intermediate	Initial End Effect			
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.

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

1) Pre-Announcement: Chapter 4.1.1

2) Route Related Information Request: Chapter 4.1.2

3) Announcement: Chapter 4.1.3

4) Cancellation: Chapter 4.1.4

5) RRI Confirmation: Chapter 4.1.5

6) Train Data: Chapter 4.1.6

7) Train Running Number: Chapter 4.1.7

8) Safe consist length information for SM: Chapter 4.1.8

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

1) Route Related Information: Chapter 4.2.1

2) Request for RRI Confirmation: Chapter 4.2.2

3) Taking Over Responsibility: Chapter 4.2.3

4) Cancellation: Chapter 4.2.4

5) SM Route Related Information: Chapter 4.2.5

5.1.1.4 Information in Both Directions

1) Acknowledgement: Chapter 4.3.1

2) Cancellation: considered separately for each direction – see clauses 5.1.1.2 and 5.1.1.3

3) Life Sign (considered as a barrier)

6. CONCLUSIONS

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

6.1.1.2 The assumptions of this analysis –as stated in clause 3.1.1.4– have to be checked in the application specific safety case.