ERTMS/ETCS

Failure Modes and Effects Analysis for DMI-Subsystem in Application Level 2

REF : SUBSET 079-2

ISSUE : 3.14.0

DATE : 2016-06-20

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

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 19-01-01	All	Creation	HB (Editor)
0.1.0 19-01-01	All	Revised version following a RAMS group and ETCS-Supergroup (Mr Bernhard Stamm) review in Zurich 9/10-01-01	HB (Editor)
0.1.1 26-01-01	All	Update following comments from Mr Hans-Georg Kast (ETCS-Supergroup) and Invensys comments	HB (Editor)
0.1.2 07-03-01	All	Update following CSEE comments (Mr S. Chassard)	HB (Editor)
0.1.3 09-07-01	4	completion of barrier-columns	HB (Editor)
0.1.4 06-02-02	4	1.2.6.3.1 in / 1.2.6.3.1 in • Operational Mode changed according to mode table in SRS (4.6).	HB (Editor)
2.0.0. 26-02-02	Section 3	References & raise 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
2.3.0 Feb - 2010	All	Update to SRS Baseline 2.3.0 d	IS

2.3.1 Sep -2010	All	Changes to be aligned to Subset079-1 v.2.3.3 Updated exclusive level 2 MMI information 1.2. 6.12 TAF, 1.9.2.10 RBC contact info,	IS
2.3.2 Sep 2010 (Berlin meeting)	Section 4	Rows 1.2.7.8.1 in & 1.2.7.8.2 in modified during the meeting	IS
2.3.3	All	Comments amended from MoM: 2010:5 – Rome 2010-10-25—26	IS
2.3.4.	All	Minor corrections from RAMS-group review	IS
2.3.5	Section 5	Clarification for MMI-3 event according to MoM:2011-03-12	IS
3.0.0	All	Update to B3 (SRS 3.2.0)	JP and RB
3.1.0	Section 4 and Annex A	Update after Brussels meeting	JP and RB
3.1.1	All	Updates during RAMS-meeting	DR
3.2.1	All	Update after Berlin Meeting	JP and RB
3.3.1	All	Update after SG comments	JP and RB
3.6.0	Section 3 and 4.	Update in20#, in#21 and out#21. New paragraph added at section 3.	JP and RB
3.7.0	All	Update to SRS v3.2.1	All
3.8.0		Updated during RAMS-meeting	DR
3.9.0		Baseline 3 release version	DR
3.10.0	Section 4	FMEA update taking into account SRS 3.18.3.2.2	JP
3.11.0		Update to B3 MR1	NH and JM
3.12.0		Administrative changes during RAMS-meeting	DARI

3.13.0	Section 4 Annex A	CR1223: LS removed from out#04, out#05. Added LSSMA as out#53. Modification of MMI-2f	NH, DARI
3.13.1	Section 4	Modifications due to: CR_539, CR_1091 CR_1107 and CR1187 (from B3 R2)	AV
3.13.2	Section 4	Modifications due to: CR_1197 (from B3 R2)	AV
3.13.3	Section 4	Modifications due to: CR_1087 (from B3 R2) and the review of the assumptions	AV
3.13.4	Section 4 and 5.1.2,	Modifications to align the subset 079 with the analysis done in subset 118 for “Level Crossing not protected” text message (#in16, #out 15 and 5.1.2). Modifications to align the analysis with the consolidated version of table 4.7.2 of subset 026 3.5.0	AV
3.13.5	Section 4 and 5.1.2,	Update after UNISIG RAMS group comments; remove “Level Crossing not protected” text message; maintain ref ids in the table.	AV
3.13.6	Section 3	Update version of SUBSET-026 and 077.	AV
3.14.0	No change	Baseline 3 2nd release version	RAMS WP

2. TABLE OF CONTENTS

1. MODIFICATION HISTORY 2
2. TABLE OF CONTENTS 4
3. INTRODUCTION 6
   3.1 Mode transitions with or without acknowledgment 6
4. FMEA 7
5. CONCLUSIONS 97
   5.1.1 Geographical Position 97
   5.1.2 Text Messages 97
   5.1.3 Planning Window Objects 97
6. ANNEX A – LIST OF MMI-X EVENTS IDENTIFIED 98

3. INTRODUCTION

Scope: Failure Modes and Effects Analysis for UNISIG DMI-Subsystem in Application Level 2

Input documents:

SRS, SUBSET-026, issue 3.6.0.

Causal Analysis Process, SUBSET-077, issue 3.0.0.

Only mandatory ETCS functions are considered.

In Chapter 4 failure of some functions are shown to be RAM issues and are not developed further.

3.1 Mode transitions with or without acknowledgment

In order to clarify all the possible transitions with or without acknowledgment, it is added a little summary considering the mode after transition. All the other conditions are assumed to be fulfilled and only driver actions are specified:

- OS / LS (further location): Transition after acknowledgment, if not it remains in the current mode that always will be FS.
- OS / LS (current location): Immediate transition. The driver acknowledges to assume more responsibility. If there is no acknowledgment the brakes are applied after a specified time.
- SH selected by the driver: Immediate transition.
- SH ordered by trackside (further location): Transition after acknowledgment, if not it remains in the current mode.
- SH ordered by trackside (current location): Immediate transition. The driver acknowledges to assume more responsibility. If there is no acknowledgment the brakes are applied after a specified time.
- SR from Override: Immediate transition.
- SR from Start of mission and Train Trip: Transition after acknowledgment, if not it remains in the current mode. See CR1050.
- TRIP: Immediate transition.
- POST TRIP: Transition after acknowledgment.
- UN: Transition after acknowledgment.
- RV: Transition after acknowledgment.
- SN: Transition after acknowledgment.

4. FMEA

Column “Failure Cause”

Driver is noted for the sake of completeness, although driver is considered outside of the ETCS-system in the Unisig SRS.

Column “Failure Mode”:

Assumption for the FMEA-part of the input functions: Data shown to the driver on the DMI are correct.
Failure modes of the output functions (data shown to the driver on the DMI) are treated in the output-part of the DMI:

	Failure Modes		
		DMI	Driver
Input Functions	Corruption	Failure to handle input data within the DMI Failure to transmit correct data to kernel	Wrong driver input
	Deletion	Failure to transmit data or acknowledgement to kernel	No driver input or no driver acknowledgement
	Insertion	Inappropriate acknowledgement not due to driver Untimely data transmission to kernel	Untimely data input Inappropriate driver acknowledgement (driver presses the button without notice)
Output Functions	Corruption	Incorrect data are shown	-
	Deletion	No data = not shown, when it should be	-
	Insertion	Data displayed appear untimely = shown, when not expected	-

Column “Failure Effects”

Possible failure effects of the failure modes of the output functions (general).
It could lead the driver to take wrong decisions, i.e. no decision, when he should decide.
In case of showing wrong train data to driver, he could assume that the shown train data are valid and he could therefore omit data entry of (the same) valid data.

Column “Ref ID”: Input and Output information have been numerated taking into account SRS 4.7.2. When not included in the table, “in_extra” indicator has been used, together with its SRS reference. Some output functions which are a direct result of an input function are analyzed together with the corresponding input function. It has been seen that a failure in the output is another potential source of failure of the input (e.g. driver sees an ack of a button that he has not pressed). The failure mode of the output has then been assumed to be such that it affects also the input, e.g. if a button is not enabled, it is not possible for the driver to activate the corresponding input function.

Column “Event-ID” replaces the former one named as “Failure Rate” (originally in FMEA template). This column will be used to provide the link of all failure effects to MMI-x hazardous events in Subset-091 (ETCS Core Hazard coverage).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#01	Train Data - train category	**Corruption:** wrong input for international train category (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN avai-lable under condi-tion(s)		error in on-board evaluation of SSPs or wrong information is send to the RBC, that could send wrong SSPs to the train	exceedance of safe speed or distance	operational rules for driver product specific safeguarding	catastrophic	MMI-3	
in#01	Train Data - train length	**Corruption:** wrong input for train length (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN avai-lable under condi-tion(s)		wrong supervision of SSPs and TSRs	exceedance of safe speed or distance	operational rules for driver product specific safeguarding	catastrophic	MMI-3	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#01	Train Data - traction/brake parameters	**Corruption:** input for braking parameters higher than real (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		wrong braking curve calculation	exceedance of safe speed or distance	operational rules for driver product specific safeguarding	catastrophic	MMI-3	
in#01	Train Data - maximum train speed	**Corruption:** input for maximum train speed too high (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		wrong ceiling speed calculation (if vehicle ceiling speed lower than track ceiling speed)	exceedance of safe speed or distance	operational rules for driver product specific safeguarding	catastrophic	MMI-3	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#01	Train Data - loading gauge	**Corruption:** wrong input for loading gauge (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		train enters a route although not suitable	collision with side barriers	operational rules for driver Lineside indications and driver´s route knowledge product specific safeguarding	catastrophic	MMI-3	
in#01	Train Data - axle load category	**Corruption:** wrong input for axle load (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		train enters a route although not suitable	derailment	operational rules for driver Lineside indications and driver´s route knowledge product specific safeguarding	catastrophic	MMI-3	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#01	Train Data - train fitted with airtight system	**Corruption:** wrong input for airtight system available onboard (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		Air conditioning intake is not controlled automatically	Passenger could be affected by sudden change of pressure or noxious air coming inside train	Opening/Closing air conditioning intake can be manually controlled onboard product specific safeguarding	critical		
in#02	Selection of language	**Insertion:** inappropriate selection of language	driver or DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT SN, RV available under condition(s)				operational rules for driver	marginal		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#03	Driver ID	**Corruption:** wrong input of driver identity (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, SN available under condition(s)		wrong data to JRU	difficulties in taking legal actions in case of accident	operational rules for driver	RAM issue		
in#04	Train running number	**Corruption:** wrong input of train running number (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, NL, UN, SN available under condition(s)			confusion for dispatcher	operational rules for driver	RAM issue		not used inside ETCS for safety purposes

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#05	ERTMS/ETCS level	**Corruption:** wrong input for ETCS-level (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, NL, UN, SN available under condition(s)	level 2 or 3 input	establishing a communication session to RBC not possible	start of mission not successful	operational rules for driver	marginal		kernel allows the driver to change the level only at standstill (SRS 5.10.2.9)
in#05	ERTMS/ETCS level	**Corruption:** wrong input for ETCS-level (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, NL, UN, SN available under condition(s)	level 1 input	RBC does not notice the train	exceedance of safe speed or distance	operational rules for driver - operational mitigations necessary product specific safeguarding	catastrophic	MMI-3	kernel allows the driver to change the level only at standstill (SRS 5.10.2.9)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#06	Track Adhesion factor	**Corruption:** wrong input for track adhesion factor (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, UN, SN available under condition(s)		wrong braking curve calculation	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-3	
in#08	Radio network id	**Corruption:** wrong input for Radio network id (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, NL, PT, UN, SN available under condition(s)			unable to initiate a communication session	operational rules for driver	marginal		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#08	RBC Contact information -RBC id	**Corruption:** wrong input of RBC identity number (start of mission) (It also applies to Insertion and Deletion) 1) RBC or driver is able to verify the train position (it depends on operational rules) 2) no verification of train position	driver or DMI failure	in SB, FS, LS, SR, OS, NL, PT available under condition(s)		RBC could address a train in an area of a neighbour RBC or handover although a train has not left the former RBC area	1) unable to initiate a communication session 2) exceedance of safe speed or distance	operational rules for driver	1) marginal 2) catastrophic	MMI-3	engineering-rules: RBC accepts only SR mode, RBC sends an MA only after receiving of reference balises (balises known by the RBC); train has to report its position before accepting by RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#08	RBC Contact information -RBC phone number	**Corruption:** wrong input for RBC phone number (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, NL, PT avai-lable under condi-tion(s)			unable to initiate a communication session	operational rules for driver	marginal		the RBC telephone number is not used for safety purposes engineering-rules
in#09	Train integrity confirmation	**Corruption:** wrong input for train integrity confirmation (It also applies to Insertion and Deletion)	driver or DMI failure	in SB, FS, LS, SR, OS, PT avai-lable under condi-tion(s)		wrong integrity information is send to the RBC, that could send a train to an erroneous track	train collision	operational rules for driver External equipment to detect train integrity (axle counters...)	catastrophic	MMI-5	Specific protection designed by each company

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#10	Start	**Insertion:** inappropriate start	driver or DMI failure	in SB, SR, PT available under condition(s)			mode-transition to staff responsible	operational rules for driver product specific safeguarding of data entry procedure	critical		RBC will reject if train is unsuitable
in#11	Override request	**Insertion:** Inappropriate override selection not due to driver	DMI failure	in SB, SH, FS, LS, SR, OS, UN, PT, SN available under condition(s)	mode-transition to SR	driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1c	kernel accepts the ack only when inside the "rectangle" (see conditions in SRS 5.8.2.1)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#11	Override request	**Deletion:** Driver does not select override or DMI fails to transmit override selection to kernel.	driver or DMI failure	in SB, SH, FS, LS, SR, OS, UN, PT, SN available under condition(s)	override selection not transmitted to kernel		override not activated		RAM issue		
in#11	Override request - Enabled override selection	**Insertion:** inappropriate displaying of enabled override selection: shown when not expected	DMI failure	FS, SR, OS, UN, SN	mode transition to SR after driver input	driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-2f	kernel accepts the request only when inside the "rectangle" (see conditions in SRS 5.8.2.1)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
in#11	Override request - Enabled override selection	**Deletion:** inappropriate displaying of enabled override selection: not shown when it should be	DMI failure	FS, SR, OS, UN, SN	override selection not transmitted to kernel		override not activated		RAM issue		
in#12	Shunting request (SRS 5.6)	**Insertion:** shunting initiated by driver at inappropriate location	driver or DMI failure	in SB, FS, LS, SR, OS, UN, PT, SN available under condition(s)	mode transition to SH mode	train performs shunting in an area, where it is not permitted	exceedance of safe speed and distance	operational rules for driver product specific safeguarding of SH entry procedure	catastrophic	MMI-1g	kernel check of standstill and after authorisation by RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#12	Shunting request (SRS 5.6)	**Deletion:** failure to transmit selection to kernel	DMI failure	in SB, FS, LS, SR, OS, UN, PT, SN available under condition(s)	onboard-equipment remains in performing the current mode		no shunting mode possible		RAM issue		
in#13	“Continue Shunting on desk closure” request	**Insertion:** continue shunting on desk closure at inappropriate location	driver or DMI failure	in SH available under condition(s)	PS mode transition is enabled but not triggered	No effect	No effect	operational rules for driver	RAM issue		Passive input signal from TIU protects against unwanted transition to PS mode
in#13	“Continue Shunting on desk closure” request	**Deletion:** failure to transmit selection to kernel	DMI failure	in SB available under condition(s)	PS mode transition not enable		Transition to PS mode not possible	operational rules for driver	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#14	"Exit of shunting" request	**Insertion:** inappropriate exit of shunting request	driver or DMI failure	SH	corresponds to start of mission		mode transition to SB	operational rules for driver	marginal		kernel check of standstill
in#14	"Exit of shunting" request	**Deletion:** failure to transmit request to kernel	DMI failure	SH	onboard-equipment remains in performing the current mode		no exit of shunting possible		RAM issue		
in#15	Non-leading request	**Insertion:** non-leading request at wrong time	driver or DMI failure	in SB,SH, FS,LS, SR,OS available under condition(s)	unwanted release from supervision (selection of non-leading mode)	non-leading mode: no supervision, driver is fully responsible	exceedance of safe speed and distance	operational rules for driver product specific safeguarding of NL entry procedure	catastrophic	MMI-1b	kernel check of standstill non leading input signal from the train interface

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#15	Non-leading request	**Deletion:** failure to transmit request to kernel	DMI failure	in SB,SH, FS,LS, SR,OS available under condition(s)	onboard-equipment remains in performing the current mode		no non-leading mode possible		RAM issue		
in#16	Acknowledgement of fixed text information	**Deletion:** no acknowledgement of fixed text information	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, RV available under condition(s)	according to the use of the text messages in operational context				RAM issue		not to be used inside ETCS for safety purposes (refer to 5.1.2)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#16	Acknowledgement of fixed text information	**Insertion:** unintentional acknowledgement of fixed text information	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, RV available under condition(s)	according to the use of the text messages in operational context				RAM issue		not to be used inside ETCS for safety purposes (refer to 5.1.2)
in#17	Acknowledgement of plain text information	**Deletion:** no acknowledgement of plain text information	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, RV available under condition(s)	according to the use of the text messages in operational context				RAM issue		not to be used inside ETCS for safety purposes

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#17	Acknowledgement of plain text information	**Insertion:** unintentional acknowledgement of plain text information	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, RV avai-lable under condi-tion(s)	according to the use of the text messages in operational context				RAM issue		not to be used inside ETCS for safety purposes
in#18	Acknowledgement of level transition	**Deletion:** no acknowledgement of level transition	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR avai-lable under condi-tion(s)		driver is not prepared to take more responsibility	exceedance of safe speed or distance (collision)	operational rules for driver	catastrophic	MMI-1d	Service brake is applied after 5 seconds (SRS 5.10.4)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#18	Acknowledgement of level transition	**Insertion:** unintentional acknowledgement of level transition	driver or DMI failure	in SB, FS, LS, SR, OS, UN, TR available under condition(s)	driver not aware of level transition	driver is not prepared to take more responsibility	exceedance of safe speed or distance (collision)	operational rules for driver	catastrophic	MMI-1d	kernel accepts the ack only when inside the "rectangle"
in#19	Acknowledgement of Limited Supervision mode	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB, FS, LS, OS, PT, SN available under condition(s)	mode transition to LS mode	driver is not prepared to take more responsibility	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-1a	kernel accepts the ack only when it is inside the "rectangle"

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
in#19	Acknowledgement of Limited Supervision mode	**Deletion:** Driver does not acknowledge	driver failure	in SB, FS, LS, OS, PT, SN available under condition(s)	mode transition to LS mode at BG transition point	driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	kernel check of LS mode acknowledgement Service Brake is applied after driver acknowledgement time
in#19	Acknowledgement of Limited Supervision mode	**Deletion:** Driver acknowledges and DMI fails to transmit ack to kernel	DMI failure	in SB, FS, LS, OS, PT, SN available under condition(s)	misleads the driver	mode is not changed		operational rules for driver	RAM issue		kernel check of LS mode acknowledgement Service Brake is applied after driver acknowledgement time

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
in#20	Acknowledgement of on sight mode (further and current location)	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB, FS, LS, OS PT available under condition(s)	mode transition to OS mode	driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	kernel accepts the ack only when inside the "rectangle"
in#20	Acknowledgement of on sight mode (further and current location)	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in SB, FS, LS, OS PT available under condition(s)		driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	Service Brake is applied after 5 seconds
in#20	Acknowledgement of on sight mode (further and current location)	**Deletion:** inappropriate displaying of ack: not shown, when it should be	DMI failure	in SB, FS, LS, OS, PT available under condition(s)	mode transition to OS independent from driver input	driver is not prepared to take more responsibility	exceedance of safe speed and distance		catastrophic	MMI-2g	kernel check of OS mode acknowledgement (brake if no ack) kernel monitoring of OS mode

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#20	Acknowledgement of on sight mode (further and current location)	**Insertion:** inappropriate displaying of ack: shown, when not expected	DMI failure	in SB, FS, LS, OS, PT available under condition(s)	driver acknowledges mode change, but kernel doesn't change mode due to conditions not fulfilled	driver assumes onboard is in OS mode because he has acknowledged	exceedance of safe speed and distance in case current mode provides less supervision than OS	awareness of driver for the current mode displayed on the DMI	critical		kernel monitoring of current mode
in#21	Acknowledgement of shunting mode	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB, SH, FS, LS, OS, PT available under condition(s)	mode transition to SH	driver is not prepared to shunt	exceedance of safe speed and distance		catastrophic	MMI-1a	kernel accepts the ack only when inside the "rectangle"

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#21	Acknowledgement of shunting mode	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in SB, SH, FS, LS, OS, PT available under condition(s)		driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	Service Brake is applied after 5 seconds
in#21	Acknowledgement of shunting mode	**Deletion:** inappropriate displaying of ack: not shown when it should be	DMI failure	in SB, FS, SH, OS, LS, PT available under condition(s)	mode transition to SH independent from driver input	driver is not prepared to shunt	exceedance of safe speed and distance		catastrophic	MMI-2g	kernel check of SH mode acknowledgement (brake if no ack) Kernel monitoring of SH mode

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#21	Acknowledgement of shunting mode	**Insertion:** inappropriate displaying of ack: shown when not expected	DMI failure	in SB, FS, SH, OS, LS, PT available under condition(s)	driver acknowledges mode change, but kernel doesn't change mode due to conditions not fulfilled	driver assumes onboard is in SH mode because he has acknowledged	exceedance of safe speed and distance in case current mode provides less supervision than SH	awareness of driver for the current mode displayed on the DMI	critical		kernel monitoring of current mode
in#22	Acknowledgement of staff responsible mode	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB, PT available under condition(s) (see CR 1050)	mode transition to SR mode	driver is not prepared to take more responsibility	exceedance of safe speed and distance	awareness of driver for the new mode displayed on the DMI	catastrophic	MMI-1a	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#22	Acknowledgement of staff responsible mode	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in SB, PT available under condition(s) (see CR 1050)		driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	kernel check of SR mode acknowledgement (no mode change without ack)
in#23	Acknowledgement of unfitted mode	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB available under condition(s)	Level/mode transition to Level 0/unfitted	driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	kernel accepts the ack only when it is inside the "rectangle"
in#23	Acknowledgement of unfitted mode	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in SB available under condition(s)	no mode transition performed	ETCS will keep waiting for confirmation of UN mode		operational rules for driver (e.g. re-start of onboard equipment)	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#23	Acknowledgement of unfitted mode	**Deletion:** inappropriate displaying of ack: not shown, when it should be	DMI failure	in SB, FS, SR, UN available under condition(s)	mode transition to UN independent of driver input	driver is not prepared to take more responsibility	exceedance of safe speed and distance		catastrophic	MMI-2g	kernel check of UN mode acknowledgement (brake if no ack) kernel monitoring of UN mode
in#23	Acknowledgement of unfitted mode	**Insertion:** inappropriate displaying of ack: shown, when not expected	DMI failure	in SB, FS, SR, UN available under condition(s)	driver acknowledges mode change, but kernel doesn’t change mode due to conditions not fulfilled	driver assumes onboard is in UN mode because he has acknowledged	exceedance of safe speed and distance in case current mode provides less supervision than UN	awareness of driver for the current mode/level displayed on the DMI	critical		kernel monitoring of current mode/level

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#24	Acknowledgement of reversing mode (SRS 5.13.1.5)	**Insertion:** Inappropriate ack not due to driver	DMI failure	in FS, LS, OS available under condition(s)	mode transition to RV	driver is not prepared to take more responsibility	exceedance of safe speed and distance		catastrophic	MMI-1a	Train must be at standstill and direction controller set to reverse position by the driver Train must be inside a reversing area
in#24	Acknowledgement of reversing mode (SRS 5.13.1.5)	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in FS, LS, OS available under condition(s)		driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	RAM issue Outside ETCS scope, could be catastrophic		RMP will be triggered if driver tries to reverse
in#25	Acknowledgement of SN mode	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB available under condition(s)	mode transition to SN	driver is not prepared to take more responsibility	exceedance of safe speed and distance		catastrophic	MMI-1a	kernel accepts the ack only when it is inside the "rectangle"

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#25	Acknowledgement of SN mode	**Deletion:** Driver does not acknowledge	driver failure	in SB available under condition(s)		driver is not prepared to take more responsibility	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1a	kernel check of SN mode acknowledgement Service Brake is applied
in#25	Acknowledgement of SN mode	**Deletion:** DMI fails to transmit ack to kernel.	DMI failure	in SB available under condition(s)	misleads the driver	mode is not changed		operational rules for driver	RAM issue		kernel check of SN mode acknowledgement Service Brake is applied
in#26	Acknowledgement of train trip	**Insertion:** Inappropriate ack not due to driver	DMI failure	in TR available under condition(s)	mode transition to PT mode	reversing of train by driver in PT mode possible	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1e	kernel check of standstill
in#26	Acknowledgement of train trip	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	Driver or DMI failure	in TR available under condition(s)	Train remains in TR mode	reversing is not possible	not possible to escape out of an emergency	driver may select IS mode to reverse	Outside ETCS core hazard, could be catastrophic		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#26	Acknowledgement of train trip	**Deletion:** inappropriate displaying of ack: not shown, when it should be	DMI failure	in TR available under condition(s)	Train remains in TR mode	reversing is not possible	not possible to escape out of an emergency	driver may select IS mode to reverse	Outside ETCS core hazard, could be catastrophic		
in#26	Acknowledgement of train trip	**Insertion:** inappropriate displaying of ack: shown, when not expected	DMI failure	in TR available under condition(s)	driver acknowledges Train Trip, but kernel doesn't change mode due to conditions not fulfilled	driver assumes onboard is in PT mode because he has acknowledged	no train-movement possible because EB is applied	awareness of driver for the current mode displayed on the DMI	RAM issue		kernel monitoring of current mode

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#27	Acknowledgement of RAP	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SH, FS, LS, SR, OS, UN, PT, RV available under condition(s)	unintended RAP acknowledgment	unintended train brakes released	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1h	Reinitializing of RAP function using new train position
in#27	Acknowledgement of RAP	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	Driver or DMI failure	in SH, FS, LS, SR, OS, UN, PT, RV available under condition(s)	RAP not acknowledged	train brakes remain applied	no train-movement possible	operational rules for driver	RAM issue		kernel check of standstill

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#28	Acknowledgement of RMP	**Insertion**: Inappropriate ack not due to driver	DMI failure	in FS, LS, SR, OS, PT, RV available under condition(s)	unintended RMP acknowledgment	unintended train brakes released	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1h	Reinitializing of RMP function using new train position
in#28	Acknowledgement of RMP	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	Driver or DMI failure	in FS, LS, SR, OS, PT, RV available under condition(s)	RMP not acknowledged	train brakes remain applied	no train-movement possible	operational rules for driver	RAM issue		kernel check of standstill
in#29	Acknowledgement of Standstill supervision	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB available under condition(s)	unintended SS acknowledgment	unintended train brakes release	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1h	Reinitializing of Standstill function using new train position

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#29	Acknowledgement of Standstill supervision	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	Driver or DMI failure	in SB available under condition(s)	SS not acknowledged	train brakes remain applied	no train-movement possible	operational rules for driver	RAM issue		kernel check of standstill
in#30	Acknowledgement of PT distance exceeded	**Insertion:** Inappropriate ack not due to driver	DMI failure	in PT available under condition(s)	unintended PT distance exceedance acknowledgment	unintended train brakes release	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1h	system keeps PT mode and supervised distances shall be identical
in#30	Acknowledgement of PT distance exceeded	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	Driver or DMI failure	in PT available under condition(s)	PT distance exceedance not acknowledged	train brakes remain applied	no train-movement possible	operational rules for driver	RAM issue		kernel check of standstill

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#31	Acknowledgement of Train Data Change from source different from driver	**Deletion:** no acknowledgement of train data changed	driver or DMI failure	in SB, FS, OS, SR, UN, TR, PT, SN, RV available under condi-tion(s)	Train data change not confirmed onboard	train brakes remain applied	no train movement possible	operational rules for driver	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#31	Acknowledgement of Train Data Change from source different from driver	**Insertion:** unintentional acknowledgement of train data change	driver or DMI failure	in SB, FS, OS, SR, UN, TR, PT, SN, RV avai-lable under condi-tion(s)	driver is not aware of train data changed onboard			Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.) Assumption: this failure mode can be ‘RAM Issue’ only if the ‘acknowledgement of train data change from external source’ is not claimed as internal barrier against failure mode of on board input leading to train data change from external source.	RAM issue		

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#32	Acknowledgement for reversing distance exceeded	**Insertion:** Inappropriate ack not due to driver	DMI failure	in RV avai-lable under condi-tion(s)	unintended RV distance exceedance acknowledgment	unintended train brakes release	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-1h	system keeps RV mode and supervised distances shall be identical
in#32	Acknowledgement for reversing distance exceeded	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in RV avai-lable under condi-tion(s)	RV distance exceedance not acknowledged	train brakes remain applied	no train-movement possible	operational rules for driver	RAM issue		kernel check of standstill
in#34	track ahead free	**Insertion:** Inappropriate ack not due to driver	DMI failure	in SB, LS, SR, OS, PT avai-lable under condi-tion(s)	TAF is granted by ETCS onboard	train movement authority may be erroneously updated by RBC	possible collision with objects in track	operational rules for driver product specific safeguarding of TAF procedure Under OS mode, the driver is responsible for checking track occupancy	catastrophic	MMI-1f	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#34	track ahead free	**Deletion:** Driver does not acknowledge or DMI fails to transmit ack to kernel.	driver or DMI failure	in SB, LS, SR, OS, PT available under condition(s)	track ahead free confirmation not sent to RBC		train movement authority will not be extended in advance		RAM issue		
in#35	SR mode speed limit and distance - maximum SR speed	**Corruption:** too high speed input for Staff Responsible	driver or DMI failure	in SR available under condition(s)		wrong supervision of maximum staff responsible speed	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-4	
in#35	SR mode speed limit and distance - SR distance	**Corruption:** wrong input for staff responsible distance	driver or DMI failure	in SR available under condition(s)		train exceeds staff responsible distance	exceedance of safe distance	operational rules for driver	catastrophic	MMI-4	
in#36	Isolation	**Insertion:** Inappropriate ack not due to driver	DMI failure	All	Unwanted transition of ETCS on-board to IS mode	No train protection available	exceedance of safe distance	operational rules for driver External switch is used to enter in Isolation mode	catastrophic	MMI-1a	Isolation status must be shown to the driver

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#36	Isolation	**Deletion:** DMI fails to transmit order to kernel	DMI failure	All	ETCS does not transit to IS mode when required	Driver does not realize about ETCS not isolated	Current ETCS mode supervision still available on-board *Note: ETCS is intended to be isolated, so that other system (or driver) is meant to control the train. ETCS will conflict with train operation*	operational rules for driver External switch is used to enter in Isolation mode	RAM issue		Isolation status must be shown to the driver

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#37	Virtual Balise Cover	**Insertion:** Unintended input for Virtual Balise Cover	driver or DMI failure	in SB available under condition(s)	unintended inhibition of valid BG processing	safety relevant BG is not processed missing information for train supervision	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-6	Trackside may send a new list of Virtual Balise Cover that shall replace the older one kernel allows the driver to change VBC only at SoM
in#37	Virtual Balise Cover	**Deletion:** Failure to transmit input for Virtual Balise Cover	driver or DMI failure	in SB available under condition(s)	intended inhibition of BG is not performed	Not intended BG is processed providing erroneous information for train supervision	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-6	Trackside may send a new list of Virtual Balise Cover that shall replace the older one product specific safeguarding

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in#37	Virtual Balise Cover	**Corruption:** wrong input for Virtual Balise Cover	driver or DMI failure	in SB available under condition(s)	Same as for in#37 insertion and deletion	Same as for in#37 insertion and deletion	Same as for in#37 insertion and deletion	operational rules for driver	catastrophic	MMI-6	Trackside may send a new list of Virtual Balise Cover that shall replace the older one product specific safeguarding
in_extra_01	show permitted speed + target distance request Related to SRS 4.4.8.1.10 (SH), 4.4.11.1.7 (SR), and 4.4.12.1.4 (OS)	**Deletion:** DMI do not show permitted speed+target distance on driver request	DMI failure	SH, SR, OS	Permitted speed/ target distance not shown after driver request	driver does not obtain the information he needs to drive safely	driver cannot start/continue the mission	operational rules for driver driver needs to exceed permitted speed/distance	RAM issue		supervision of train speed/target distance by kernel (SH, SR, OS)

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
in_extra_01	show permitted speed + target distance request Related to SRS 4.4.8.1.10 (SH), 4.4.11.1.7 (SR), and 4.4.12.1.4 (OS)	**Insertion:** permitted speed+target distance shown when not expected	DMI failure	SH, SR, OS	Permitted speed/ target distance spuriously displayed	misleads the driver	no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out#01	ERTMS /ETCS-mode	**Deletion, Corruption:** displaying no or wrong data: FS although actual mode is partial supervision	DMI failure	SH, LS, SR, OS, NL, UN, PT, SN, RV in SB, TR, SF available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2b	supervision of train speed by kernel
out#01	ERTMS /ETCS-mode	**Deletion, Corruption:** displaying no or wrong data: partial supervision although actual mode is FS	DMI failure	FS	misleads the driver	could lead the driver to take inappropriate decisions	driver could try to take action that could result in train delay	driver-acknowledgement for acceptance of responsibility during level-transitions	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out#01	ERTMS/ETCS-mode	**Corruption:** displaying wrong SN mode	DMI failure	SN	misleads the driver	could lead the driver to take inappropriate decisions for the current SN mode	exceedance of safe speed or distance	SN specific	catastrophic	MMI-2b	
out#02	Current ETCS level	**Deletion, Corruption:** displaying no or wrong data	DMI failure	SH, FS, LS, SR, OS, NL, UN, PT, SN, RV in SB, TR available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		critical		as long as displaying operational mode correctly, there is no problem. (kernel supervision)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 03	Train speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	SH, FS, LS,SR, OS, NL, UN, PT, RV in SB, TR, SN available under condition(s)	misleads the driver	driver could exceed speed restrictions	exceedance of safe speed or distance		catastrophic	MMI-2a.1	supervision of train speed by kernel (SH, FS, SR, OS, UN, RV)
out# 04	Permitted speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	FS, RV in SH, SR, OS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2a.2	supervision of train speed by kernel (SH, FS, SR, OS, RV)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out#05	Target speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in FS, SR, OS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2a.2	supervision of train speed by kernel (FS, SR, OS)
out#06	Target distance	**Deletion, Corruption:** displaying no or wrong data	DMI failure	RV, in FS, SR, OS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2a.2	supervision of train speed by kernel (FS, SR, OS, RV)
out#07	Release speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in FS, LS, OS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic (2 different cases: depending on the available overlap)	MMI-2a.2	supervision of train release speed by kernel (FS, OS)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 08	Speed and distance monitoring supervision status	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SH, FS, LS, SR, OS,UN, PT, RV avai-lable under condi-tion(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance	operational rules for driver	catastrophic	MMI-2a.2	supervision of train speed and distance by kernel
out# 09	Trip reason	**Corruption:** inappropriate triggering of trip alarm	DMI failure	PT, in TR avai-lable undadheer condi-tion(s)	misleads the driver				marginal		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 10	Train Data - train category	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance		catastrophic	MMI-2e	supervision of train speed by kernel (FS, SR, OS, UN, RV)
out# 10	Train Data - train length	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance		catastrophic	MMI-2e	supervision of train speed by kernel (FS, SR, OS, UN, RV)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out#10	Train Data - traction/brake parameters	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2e	supervision of train speed by kernel (FS, SR, OS, UN, RV)
out#10	Train Data - Max train speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance	train max speed is normally indicated at train cabins	catastrophic	MMI-2a.2	supervision of train speed by kernel (SH, FS, SR, OS, UN, RV)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 10	Train Data - loading gauge	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	collision with side barriers	Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.)	catastrophic	MMI-2e	Route Suitability may be provided to ETCS onboard
out# 10	Train Data - axle load category	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	derailment	Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.)	catastrophic	MMI-2e	Route Suitability may be provided to ETCS onboard

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 10	Train Data - Traction systems accepted by the engine	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	damage to train	Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.)	critical		Route Suitability may be provided to ETCS onboard
out# 10	Train Data - Train fitted with airtight system	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	Passenger could be affected by sudden change of pressure or noxious air coming inside train	Driver should know if airtight system is available onboard	critical		ETCS onboard controls the air conditioning intakes if system is available

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 10	Train Data - List of National Systems available on-board	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions		Driver should know which National Systems are available on-board	marginal		
out# 10	Train Data - Axle number	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver				RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 11	Driver identity number	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, SH,FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions			marginal		
out# 12	Train running number	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, SH,FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions			marginal		not to be used inside ETCS for safety purposes

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 13	Radio Network id	**Deletion, Corruption:** displaying no or wrong data		in SB, SH, FS, LS, SR, OS, NL, UN,TR PT, SN, RV available under condi-tion(s)	misleads the driver	could lead the driver to take inappropriate decisions			marginal		The Radio Network id is not used for safety purposes.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 13	RBC contact information - identity number	**Deletion, Corruption:** displaying no or wrong data (SB) 1) RBC or driver are able to verify the train position. (depends on operational rules) 2) no verification of train position	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN,TR PT, SN, RV available under condition(s)	misleads the driver	RBC could address a train in an area of a neighbour RBC or handover although a train has not left the former RBC area	1) - 2) exceedance of safe speed or distance		1) marginal 2) catastrophic	MMI-2e	engineering-rules: RBC accepts only SR mode, RBC sends an MA only after receiving of reference balises; train has to report its position before accepting by RBC

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 13	RBC contact information - phone number	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN,TR PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions			marginal		The RBC telephone number is not used for safety purposes
out# 14	Brake indication	**Corruption:** inappropriate displaying of brake command indication	DMI failure	in SB, SH,FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver		no impact on ETCS-operation		marginal		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 15	Fixed text information	**Repetition, Deletion, Insertion, Resequence, Corruption, Delay:** inappropriate displaying of fixed text messages	DMI failure	in SB, FS, LS, SR, OS, NL, UN, TR, PT, RV available under condition(s)	according to the use of the text messages in operational context			driver acknowledgement Safety application rule (SAR): not to be used for safety relevant purposes	RAM issue		not to be used inside ETCS for safety purposes
out# 16	Plain text information	**Repetition, Deletion, Insertion, Resequence, Corruption, Delay:** inappropriate displaying of fixed text messages	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, RV available under condition(s)	according to the use of the text messages in operational context			driver acknowledgement Safety application rule (SAR): not to be used for safety relevant purposes	RAM issue		not to be used inside ETCS for safety purposes

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 17	Reversing allowed (SRS 5.13.1.3)	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in FS, LS, OS available under condition(s)	reversing mode allowance not presented to driver	Driver is not aware that train reversing is possible	Train is at standstill but reversing mode can be entered	Driver should be aware of trackside area where train reversing is allowed Outside ETCS. Emergency procedures for train evacuation	Outside ETCS core hazard, could be catastrophic		
out# 17	Reversing allowed (SRS 5.13.1.3)	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in FS, LS, OS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance	Driver should be aware of trackside area where train reversing is allowed	catastrophic	MMI-2j	RMP avoids reversing against valid MA onboard

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 18	Track conditions-Power control	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	misleads the driver	Wrong power system could be selected by the driver or main switch is not manually activated	damage to train	Train should measure in advance which voltage is available	RAM issue		Power can be automatically controlled onboard (application specific)
out# 18	Track conditions-Pantograph control	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	misleads the driver	Pantograph could be raised at a wrong location	Train or other external system parts could be damaged	Driver should know where pantograph needs to be raised/lowered	RAM issue		Pantograph can be automatically controlled onboard (application specific)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 18	Track conditions-Air tightness control	**Deletion:** inappropriate displaying of air tightness control: not shown, when it should be	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	air tightness area is not shown to the driver	Driver could fail to close the air conditioning intake	Passenger could be affected by sudden change of pressure or noxious air coming inside train	Driver should know where air tightness areas are located	critical		Opening/Closing air conditioning intake can be automatically controlled onboard (application specific)
out# 18	Track conditions-Air tightness control	**Corruption:** inappropriate displaying of air tightness control	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	misleads the driver	Driver could erroneously close the air conditioning intake		Driver should know where air tightness areas are located	marginal		Opening/Closing air conditioning intake can be automatically controlled onboard (application specific)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 18	Track conditions-Radio hole control	**Insertion:** inappropriate displaying of radio hole control	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	misleads the driver (train operating in Level 1)		no impact on ETCS-operation		RAM issue		
out# 18	Track conditions-Brakes control	**Deletion:** inappropriate displaying of brakes control: not shown, when it should be	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	brake type inhibition area is not shown to the driver (e.g. regenerative, eddy current and magnetic shoes brake)	Driver could fail to inhibit the defined brake type	Train or other external system parts could be damaged	Driver should know where brake type restrictions areas are located	critical		Brakes inhibition can be automatically controlled onboard (application specific)

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 18	Track conditions-Brakes control	**Insertion:** inappropriate displaying of brakes control: shown, when not expected	DMI failure	in FS, LS, OS, NL, TR, PT available under condition(s)	misleads the driver	Driver could erroneously inhibit a defined brake type	no impact on ETCS-operation	Driver should know where brake type restrictions areas are located	RAM issue		Brakes inhibition can be automatically controlled onboard (application specific)
out# 19	Track conditions-Sound horn	**Deletion:** inappropriate displaying of sound horn info: not shown, when it should be	DMI failure	in FS, LS, OS available under condition(s)	Sound horn area is not shown to the driver	Driver could fail to request the sound horn	no impact on ETCS-operation	operational rules for the driver	RAM issue		
out# 19	Track conditions-Sound horn	**Insertion:** inappropriate displaying of sound horn info: shown, when not expected	DMI failure	in FS, LS, OS available under condition(s)	misleads the driver	Driver could erroneously request the sound horn	no impact on ETCS-operation	operational rules for the driver	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 19	Track conditions-non stopping areas, tunnel stopping areas	**Deletion:** inappropriate displaying of stopping-control: not shown, when it should be	DMI failure	in FS, LS, OS available under condition(s)	non permitted stopping area is not shown to the driver	Driver could accept a passenger emergency stop in a dangerous area.	Train could stop in a dangerous area.	Driver should know where the dangerous areas are located	critical		
out# 19	Track conditions-non stopping areas, tunnel stopping areas	**Insertion:** inappropriate displaying of non-stopping-control: shown, when not expected	DMI failure	in FS, LS, OS available under condition(s)	misleads the driver	Driver could not accept a passenger emergency stop although outside a dangerous area	Train could not stop after passenger emergency stop request.	Driver should know where the dangerous areas are located	critical		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 20	Geographical train position	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, NL, UN, TR, PT available under condition(s)	according to the use of the geographical position in operational context			Safety application rule (SAR): not to be used for safety relevant purposes, i.e. awaking of the train *The signaller could provide an inappropriate MA based on the wrong GPI reported by the driver*	RAM issue		not to be used inside ETCS for safety purposes
out# 21	Override status	**Deletion:** inappropriate displaying of override status: not shown, when it should be	DMI failure	in SH, SR, UN, SN available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance	operational rules for driver entry procedure to override	catastrophic	MMI-2f	Kernel supervision: Override time, distance and balise passage.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 21	Override status	**Insertion:** inappropriate displaying of override status: shown, when not expected	DMI failure	in SH, SR, UN, SN avai-lable under condi-tion(s)	misleads the driver	could lead the driver to take inappropriate decision to pass a signal	exceedance of safe speed or distance	operational rules for the driver	catastrophic	MMI-2f	Kernel supervision of current mode (Train trip supervision is actually activated on-board)
out# 22	LX status "not protected"	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in FS, LS, OS avai-lable under condi-tion(s)	LX "not protected" information not shown to the driver	Driver could fail to reduce train speed	exceedance of safe speed or distance	operational rules for the driver	catastrophic	MMI-2i	LX "not protected" speed profile is supervised on-onboard
out# 22	LX status "not protected"	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in FS, LS, OS avai-lable under condi-tion(s)	misleads the driver	could lead the driver to reduce train speed	Train speed unnecessarily reduced		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 23	Shunting refused by RBC	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in SB, FS, LS, SR, OS, PT available under condition(s)	transition to Shunting mode not possible	Driver is not aware about the reason for not entering in Shunting	no impact on ETCS-operation		RAM issue		
out# 23	Shunting refused by RBC	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, FS, LS, SR, OS, PT available under condition(s)	Misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 24	Shunting request not answered by RBC	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in SB, FS, LS, SR, OS, PT available under condition(s)	transition to Shunting mode not possible	Driver is not aware about the reason for not entering in Shunting	no impact on ETCS-operation		RAM issue		
out# 24	Shunting request not answered by RBC	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, FS, LS, SR, OS, PT available under condition(s)	Misleads the driver		no impact on ETCS-operation		RAM issue		
out# 25	Intentionally deleted.										
out# 25	Intentionally deleted.)										

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 26	Entry in FS	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in FS available under condition(s)	misleads the driver	driver does not apply manual routines for speed limitation in SR to FS transition (track description not available for whole train length)	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-2d	
out# 26	Entry in FS	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in FS available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 27	Level transition announcement	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in FS, LS, SR, OS, NL, UN, TR, PT, SN available under condition(s)	misleads the driver	driver is not prepared to take more responsibility	exceedance of safe speed and distance	Driver should be aware where level transition is located (e.g. trackside marker)	catastrophic	MMI-2k	ETCS will require acknowledgment within 5 seconds at level transition point if new level is lower or National System
out# 27	Level transition announcement	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in FS, LS, SR, OS, NL, UN, TR, PT, SN available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance	Driver should be aware where level transition is located (e.g. trackside marker)	catastrophic	MMI-2k	kernel monitoring

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 28	Track ahead free request	**Deletion:** inappropriate displaying of ack: not shown, when it should be	DMI failure	in SB, LS, SR, OS, PT avai-lable under condi-tion(s)	no track ahead free is presented to driver		train movement authority will not be extended in advance		RAM issue		
out# 28	Track ahead free request	**Insertion:** inappropriate displaying of ack: shown, when not expected	DMI failure	in SB, LS, SR, OS, PT avai-lable under condi-tion(s)	TAF is granted after driver input	train movement authority may be erroneously updated by RBC	exceedance of safe speed and distance	operational rules for driver product specific safeguarding of TAF procedure	catastrophic	MMI-2h	

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 29	Adhesion factor “slippery rail”	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	driver could try to take action that could result in train delay		catastrophic	MMI-2c	Braking curve calculation by kernel
out# 35	Trackside malfunction	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	Train could be stopped unnecessarily		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 35	Trackside malfunction	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in SB, SH, FS, LS, SR, OS, UN, TR, PT, SN, RV available under condition(s)	Trackside malfunction information not shown to driver	Driver is not aware about a trackside failure	no impact on ETCS-operation		RAM issue		Supervision of trackside malfunction by on-board (e.g. linking reaction)
out# 36	Notification of Train Data change from source different from the driver	**Deletion:** inappropriate displaying of info: not shown, when it should be	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN available under condition(s)	train data change is not informed to the driver	driver is not aware of train data changed onboard	exceedance of safe speed and distance	operational rules for driver Product specific safeguarding	catastrophic	MMI-2e	

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 36	Notification of Train Data change from source different from the driver	**Insertion:** inappropriate displaying of info: shown, when not expected	DMI failure	in SB, FS, LS, SR, OS, UN, TR, PT, SN available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed and distance	operational rules for driver Product specific safeguarding	catastrophic	MMI-2e	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 37	JRU failure	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	Train could be stopped unnecessarily *Note: reaction to a JRU failure could be dependent on the railway administrator (to do nothing or to take the train out of service)*		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 37	JRU failure	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	JRU failure information not shown to the driver	driver is not aware about the JRU failure	no impact on ETCS-operation		RAM issue		
out# 38	Operated System Version	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 38	Operated System Version	**Deletion, corruption:** displaying no or wrong operated system version	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	Operated System Version information not shown to driver	Driver is not aware about a different Operated System Version	no impact on ETCS-operation		RAM issue		
out# 39	Radio Network registration failed	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, FS, LS, SR, OS, NL, PT available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 39	Radio Network registration failed	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in SB, FS, LS, SR, OS, NL, PT available under condition(s)	Session is not opened	Driver is not aware about the reason for not opening session		no impact on ETCS-operation	RAM issue		
out# 40	Safe radio connection indication	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 40	Safe radio connection indication	**Deletion, Corruption:** displaying no or wrong indication	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		critical		as long as displaying operational mode correctly, there is no problem (kernel supervision)
out# 41	Local time	**Deletion:** inappropriate displaying of local time: not shown, when it should be	DMI failure	SH, FS, LS, SR, OS, NL, UN, PT, RV in SB, TR, SN available under condition(s)	local time is not shown to the driver	Driver is not aware about the local time through the DMI	no impact on ETCS operation	Local time provided by other systems located in the dashboard	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 41	Local time	**Corruption:** wrong local time displayed	DMI failure	SH, FS, LS, SR, OS, NL, UN, PT, RV in SB, TR, SN avai-lable under condi-tion(s)	misleads the driver	could lead the driver to take inappropriate actions	train could be delayed *Note: only if local time is used to follow the train schedules*	Local time provided by other systems located in the dashboard	RAM issue		
out# 42	Gradient	**Insertion:** inappropriate displaying of gradient: shown, when not expected	DMI failure	FS, in OS avai-lable under condi-tion(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like MRSP, permitted speed...) See 5.1.3	RAM issue		

Ref ID	**Macro Function Data Item**	**Failure Mode**	**Failure Cause**	**Operational Mode**	**Failure Effects**			**External Protection / Mitigation / Barriers**	**Severity**	**Event-ID**	**Internal Barriers**
					Local	**Intermediate**	**Initial End Effect**				
out# 42	Gradient	**Deletion, corruption:** displaying no or wrong gradient	DMI failure	FS, in OS available under condition(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like MRSP, permitted speed...) See 5.1.3	RAM issue		
out# 43	MRSP	**Insertion:** inappropriate displaying of MRSP: shown, when not expected	DMI failure	FS, in OS available under condition(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like speed profile discontinuity, permitted speed...) See 5.1.3	RAM issue		
out# 43	MRSP	**Deletion, corruption:** displaying no or wrong MRSP	DMI failure	FS, in OS available under condition(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like speed profile discontinuity, permitted speed...) See 5.1.3	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 44	First Indication location	**Insertion:** inappropriate displaying of first indication location: shown, when not expected	DMI failure	in FS, OS avai-lable under condi-tion(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like target profile, distance to target...) See 5.1.3	RAM issue		
out# 44	First Indication location	**Deletion, corruption:** displaying no or wrong first indication location	DMI failure	in FS, OS avai-lable under condi-tion(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like target profile, distance to target...) See 5.1.3	RAM issue		
out# 45	EOA/LOA	**Insertion:** inappropriate displaying of EOA/LOA : shown, when not expected	DMI failure	in FS, OS avai-lable under condi-tion(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like MRSP, distance to target...) See 5.1.3	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 45	EOA/LOA	**Deletion, corruption:** displaying no or wrong EOA/LOA	DMI failure	in FS, OS available under condition(s)	misleads the driver		no impact on ETCS-operation	Additional information displayed on the DMI (like MRSP, distance to target...) See 5.1.3	RAM issue		
out# 46	Brake reason	**Insertion:** inappropriate displaying of brake reason info: shown, when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, UN, PT, SN, RV available under condition(s)	misleads the driver		no impact on ETCS-operation	Message indicating brake applied is not displayed	RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 46	Brake reason	**Deletion, corruption:** displaying no or wrong brake reason info	DMI failure	in SB, SH, FS, LS, SR, OS, UN, PT, SN, RV available under condition(s)	misleads the driver	Driver is not aware about the reason for braking or the reason is not correct	no impact on ETCS-operation	Driver is aware of brake applied (message is displayed on the DMI)	RAM issue		
out# 48	Trackside not compatible	**Insertion:** inappropriate displaying of info: shown when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 48	Trackside not compatible	**Deletion:** inappropriate displaying of info: not shown when it should be	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN, RV available under condition(s)	Trackside not compatible information not shown to driver	Driver is not aware about the reason for not establishing communication or train trip	no impact on ETCS-operation		RAM issue		
out# 49	Train rejected	**Insertion:** inappropriate displaying of info: shown when not expected	DMI failure	in SB available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		
out# 49	Train rejected	**Deletion:** inappropriate displaying of info: not shown when it should be	DMI failure	in SB available under condition(s)	Train rejected information not shown to the driver	Driver is not aware about the reason for no session established	no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 50	Route unsuitability(ies)	**Insertion:** inappropriate displaying of info: shown, when not expected	DMI failure	in, FS, LS, OS available under condition(s)	misleads the driver	could lead the driver to reduce train speed	train speed unnecessarily reduced	Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.)	marginal		Route Suitability may be provided to ETCS onboard
out# 50	Route unsuitability(ies)	**Deletion:** inappropriate displaying of info: not shown, when it should be	DMI failure	in FS, LS, OS available under condition(s)	Route unsuitability message is not shown to the driver	Train could run at a wrong location	Train or other external system parts could be damaged	Traffic planning will not allow a train passing through a non compatible piece of track (e.g. train axle load, loading gauge, etc.)	critical		Route Suitability may be provided to ETCS onboard
out# 51	SBI Speed	**Deletion, Corruption:** displaying no or wrong data	DMI failure	in FS available under condition(s)	misleads the driver	could lead the driver to take inappropriate decisions	exceedance of safe speed or distance		catastrophic	MMI-2a.2	supervision of train speed by ETCS onboard

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 52	Virtual Balise Covers	**Insertion:** inappropriate displaying of info: shown, when not expected	DMI failure	In SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN and RV available under condition(s)	misleads the driver				RAM issue		
out# 52	Virtual Balise Covers	**Deletion:** inappropriate displaying of info: not shown, when it should be	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN and RV available under condition(s)	VBC information not showed to the driver	Driver is not aware about VBC information	no impact on ETCS-operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 53	LSSMA (including LS frame)	**Deletion**: no LSSMA displayed when it should be	DMI failure	In LS available under condition(s)	LSSMA information not shown to the driver		No impact on ETCS operation (background supervision)	Driver is requested to observe line-side signals	RAM issue		
out# 53	LSSMA	**Corruption**: wrong value of LSSMA displayed	DMI failure	In LS available under condition(s)	Misleading the driver		No impact on ETCS operation (background supervision)	Driver is requested to observe line-side signals	RAM issue		
out# 53	LSSMA	**Insertion**: displaying LSSMA when not expected	DMI failure	In any more	Misleading the driver		No impact on ETCS operation		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out# 54	Set Speed Indication	**Deletion**: no Set Speed Indication displayed when it should be	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN and RV available under condition(s)	Set Speed Indication is not shown to the driver	Driver is not aware about Set Speed Indication information	No impact on ETCS operation (The set speed input is used by ERTMS/ETCS onboard only for display on the DMI. The onboard is only requested to log this value inside the JRU)		RAM issue		

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event -ID	Internal Barriers
					Local	Inter-mediate	Initial End Effect				
out#54	Set Speed Indication	**Insertion**: displaying Set Speed Indication when not expected	DMI failure	in SB, SH, FS, LS, SR, OS, NL, UN, TR, PT, SN and RV available under condition(s)	Set Speed Indication is shown to the driver	Misleads the driver	No impact on ETCS operation (The set speed input is used by ERTMS/ETCS onboard only for display on the DMI. The onboard is only requested to log this value inside the JRU)		RAM issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
					Local	Intermediate	Initial End Effect				
out# 55	Entry in OS	**Deletion:** inappropriate displaying of message: not shown, when it should be	DMI failure	in OS available under condition(s)	misleads the driver	driver does not apply manual routines for speed limitation in SR to OS transition (track description not available for whole train length)	exceedance of safe speed and distance	operational rules for driver	catastrophic	MMI-2d	
out# 55	Entry in OS	**Insertion:** inappropriate displaying of message: shown, when not expected	DMI failure	in OS available under condition(s)	misleads the driver		no impact on ETCS-operation		RAM issue		
out# 56	NTC not available	LEVEL NTC only									
out# 57	NTC data needed	LEVEL NTC only									
out# 58	NTC failed	LEVEL NTC only									

5. CONCLUSIONS

No inconsistencies and open points were found during the analysis. The following assumptions have been considered on the use of ETCS information:

5.1.1 Geographical Position

Geographical position information shall not be used for safety purposes; otherwise wrong geo position information on DMI could derive in a catastrophic event.

5.1.2 Text Messages

Text messages ‘track to train’ cannot be used for the delivery of safety critical information unless a specific application safety analysis can justify this, e.g. if other information/communications between the two parties concerned is provided so that the recipient’s understanding of the message can be verified and safety provision are taken if driver does not acknowledge the message.

5.1.3 Planning Window Objects

A failure in one of the planning window objects (Gradient, MRSP, Indication location at MRSP speed and EOA/LOA) is considered to be not relevant for safety purposes. The reason behind is that all the planning window objects are related to each other. Additionally, other displayed items (e.g. target speed and distance to target bar) provide similar information. Thus, a failure in one of the planning window objects can be easily identified.

6. ANNEX A – LIST OF MMI-X EVENTS IDENTIFIED

Event Id.	Hazardous Event Description
MMI-1a	False acknowledgement of mode change to less restrictive mode
MMI-1b	False command to enter NL mode
MMI-1c	False command of Override request
MMI-1d	False acknowledgement of Level Transition
MMI-1e	False acknowledgement of Train Trip
MMI-1f	False acknowledgement of Track Ahead Free
MMI-1g	False request for SH mode
MMI-1h	False acknowledgement of undesired train movement (RAM, RMP,SSS, PT distance, and reversing distance)
MMI-2a.1	False presentation of train speed
MMI-2a.2	False presentation of speed (except train speed) or distance, including supervision status
MMI-2b	False presentation of mode
MMI-2c	False presentation of track adhesion factor
MMI-2d	Failure to present Entry in FS/OS information
MMI-2e	False presentation of train data/additional data
MMI-2f	Failure to display Override status, including false enabling of override selection
MMI-2g	Failure to present acknowledgement message to a less restrictive mode
MMI-2h	False presentation of TAF request
MMI-2i	Failure to present “LX not protected” information
MMI-2j	False presentation of reversing allowed
MMI-2k	False presentation of level transition announcement
MMI-3	Falsification of driver’s train data/additional data input stored onboard
MMI-4	Falsification of SR speed/distance data
MMI-5	Falsification of train integrity confirmation input
MMI-6	Falsification of Virtual Balise Cover