

## ERTMS/ETCS

### ETCS Application Level 2 - Safety Analysis

#### Part 1 - Functional Fault Tree

REF : SUBSET-088-2 Part 1

ISSUE : 3.7.0

DATE : 2019-12-16

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



# 1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1. 14-05-01	All	Document Creation	WLH
0.0.2 25-05-01	4	Key to the fault tree symbols added	WLH
0.1.0 14-06-01	3.1.1.2 & 5.2.1.2	Inclusion of Ansaldo comments. Release for general Unisig review	WLH
0.1.1. 25-06-01	Section 8 Appendix B	Initial comments added Fault tree raised to issue 005.	WLH
0.1.2.	All 06-08-01	Document restructured into 4 parts. This part becoming part 1	WLH
0.1.3	Appendix B	Restructure of Fault Tree plus modifications following functional analysis and UNISIG comments	GM
0.1.4	Appendix B	Restructure of Fault Tree	GM
0.1.5	All	Incorporation of minor comments following UNISIG RAMS meeting	GM
0.1.6.	Section 3	Clarified in accordance with comments from the Super Group	WLH
0.2.0. 01-10-01	Sections 3, 5 & 6	Minor amendments and raised in issue for release to Esrog	WLH
0.2.1. 30-11-01	Appendix B	regarding revised Part 2	Ado
0.2.2. 10-12-01	Appendix B	regarding revised Part 2	Ado
0.3.0 16-01-02	All	revised regarding review comments function list added	Ado

2.0.0. 26-02-02	Minor amendments to section 3	Raised in issue for release to the EEIG	WLH
2.0.1. 26-10-02	Document Title 3.1.1.1. 3.1.1.2. 7.1.1.2.	Report Number deleted Clarified Reference the change request deleted Definition of the core hazard amended	WLH
2.0.2. 04-12-02	3.1.1.6, 3.1.1.7, Function table amended	Amended in line with review comments from Ansaldo and Siemens	WLH
2.1.0. 31-01-03		Raised in issue for release to the Users Group.	WLH
2.2.2. 21-03-03		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	WLH
2.2.3 25-03-04		Modifications on Fault Tree due to new events added during consolidation process	IS
2.2.4 15-10-04		App B. General. TRANS-events definitions updated according to Part 3 App B. Added Gate 160, explanatory OR-gate between RS and Kernel-34 event Kernel-23 removed from Gate 120	IS
2.2.5 06-07-05		Reference to SRS updated.	DARI
2.2.10 08-07-05		Raised in issue for release to the Users Group. Version	DARI

		number to be consistent with SUBSET-091.	
2.2.11 20-09-07		<ul style="list-style-type: none"> <li>Updated version of reference SUBSET-026 to match baseline 2.3.0</li> <li>Formal changes, corrections of grammar and spelling</li> </ul>	KN
2.3.0 02-04-08		Administrative updates for baseline 2.3.0	DARI
2.3.1 18-12-09	10.1.3	Corrections to match Subset-026, 2.3.0d	DARI
2.3.2 15-03-11	Appendix B, 10.1.2	Update with new/changed MMI-x events according to final version of Subset-079 (updated to 2.3.0)	KN
	10.1	Adaptation to Subset.026, 3.2.0 New modes LS, PS included Speed restriction concerning permitted braking distance added Onboard function table corrected to match Subset.026, 3.2.0, column SE deleted	KN
2.3.3	10.1.2	Adaptation to Subset.026, 3.2.0, Active function table 4.5.2	
2.3.4 17-06-2011	Appendix B	Update according to Subset-079: MMI-4A and MMI-4B removed	
2.3.5	Appendix B	Update according to Subset-079: MMI-2j and MMI-4 added, MMI-2i removed	KN
3.0.0		Update according to Subset-079: MMI- 2j, MMI- 2k and MMI-5 added, MMI-	KN

		2a split into MMI-2a.1 and MMI-2a.2	
3.0.1	Appendix B	update according to Subset-079: Event description changed, MMI-1g added,	KN
3.1.0		CR1106 considered. Administrative changes for release to ERA.	DR
3.2.0		<ul style="list-style-type: none"> <li>Adaptation to Subset.026, 3.2.1, Active function table 4.5.2</li> <li>Use ETCS Core Hazard as standardized term</li> <li>MMI-6 added</li> </ul>	KN
3.3.0		Update after internal RAMS WP review	KN
3.4.0		Updated during RAMS-meeting	DR
3.5.0		Baseline 3 release version	DR
3.5.1		Appendix B: update for B3 MR1	KN
3.5.3		Formal updates during RAMS-meeting	DARI
3.5.4	10.1.2	Add new function "LSSMA display to the driver"	KN
3.5.5	10.1.2	Adaptation to SUBSET-026, 3.2.1, Active function table 4.5.2	KN
3.5.6	Appendix B 3.1.1.1, 10.1.2	update for BL3 R2 Formal corrections	KN
3.5.7	Appendix B	Embedded files for FT added	KN
3.6.0 2016-06-20	No change	Baseline 3 2 <sup>nd</sup> release version	RAMS WP
3.6.1	Appendix B	Formal Corrections (remove not openable object, remove overlay page 16)	KN



3.6.2	Appendix B	Formal Corrections	KN
3.7.0	No change	Release version	RAMS WP



## 2. TABLE OF CONTENTS

1. MODIFICATION HISTORY .....	2
2. TABLE OF CONTENTS.....	7
3. INTRODUCTION.....	8
4. KEY TO THE FAULT TREE SYMBOLS .....	9
4.2 Gate Symbols .....	9
4.3 Primary Event Symbols.....	9
4.4 Gate / Event Description Symbol.....	9
5. CONCEPTUAL FAULT TREE .....	10
5.1 Purpose .....	10
5.2 Structure .....	10
5.3 Fault Tree Diagram .....	10
6. DETAILED, GENERIC LEVEL 2 FAULT TREE.....	11
6.1 Concept .....	11
7. PRELIMINARY SAFETY RELATED COMMENTS.....	12
7.1 General Comments.....	12
8. APPENDIX A.....	1
8.1 Conceptual Fault Tree.....	1
9. APPENDIX B - DETAILED SYSTEM LEVEL FAULT TREE.....	1
10. APPENDIX C.....	1
10.1 Modes and Class 1 Functions in Level 2 .....	1
10.1.1 Introduction .....	1
10.1.2 Active Functions Onboard Function Table.....	1
10.1.3 Trackside Function Table.....	13



### 3. INTRODUCTION

- 3.1.1.1 This document contains the functional fault tree for ETCS application level 2 based on the failure modes of the ETCS macro functions. These macro functions are derived from Unisig SRS version 3.6.0 (Please refer to Appendix C). This fault tree does not imply or mandate a specific system implementation and neither is it related to specific system mode.
- 3.1.1.2 The function table of Appendix C contains references to related Fault Tree gates.
- 3.1.1.3 The objective of producing the generic functional fault tree is to provide a system wide view of functional interactions so that the migration of base events that have been identified as being potentially catastrophic can be analysed. The base events were identified by the FMEA analyses of the mandatory interfaces.
- 3.1.1.4 The detailed analysis against specific modes is undertaken in Part 2 of this suite of documents.
- 3.1.1.5 The analysis is undertaken separately in Part 2 because of the difficulty in accounting for the degree of failure necessary to result in the occurrence of the ETCS Core Hazard in the confines of a diagrammatic representation. The analysis identifies the criticality of base events and ETCS functions.
- 3.1.1.6 The system fault trees form the starting point for the documented analysis in part 2 for the different grades of protection available to an ETCS fitted train, the relevant operational modes being, Full Supervision (FS), On Sight (OS), Limited Supervision (LS), Staff Responsible (SR), Reversing (RV) and Shunting (SH).
- 3.1.1.7 The functional fault tree puts the macro function failure modes into a hierarchy leading up to the ETCS Core Hazard

Exceedance of the safe speed or distance as advised to ETCS.

Note: The hierarchy is generic and not mandatory for a product design. It is developed to provide a static view of functional interaction.

- 3.1.1.8 The functional fault tree provides full traceability to the set of system macro functions as defined in the SRS, whether or not the failure leads to a catastrophic event.
- 3.1.1.9 The general hierarchy for the system fault tree is given in appendix A.
- 3.1.1.10 Appendix B gives the detailed system fault tree from the perspective of a single system.

## 4. KEY TO THE FAULT TREE SYMBOLS

4.1.1.1 The fault tree tool adopted for the analysis work is Isograph Fault Tree+ Version 9.0 where the following symbols are used in the fault tree modelling:

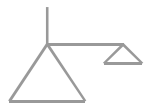
### 4.2 Gate Symbols



OR Gate: Gate event occurs if any one of the input events occurs.



AND Gate: Gate event occurs if all of the input events occur.

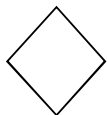


TRANSFER Gate The output is used as part of a lower level tree on page n:

### 4.3 Primary Event Symbols

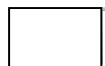


Basic Event: Event using a Primary Event Failure Model.



Undeveloped Event: Event that is yet to be developed.

### 4.4 Gate / Event Description Symbol



Description Symbol: Text describing the logical result of the gate or event



## **5. CONCEPTUAL FAULT TREE**

### **5.1 Purpose**

5.1.1.1 The Conceptual Fault Tree is intended to provide an overview of the principle behind the construction of the detailed fault tree. The hierarchy is developed from a purely functional standpoint linking to the top level ETCS Core Hazard as identified in document Part 0.

5.1.1.2 The functional development of the fault tree stems from the definition of the Unisig ETCS within an operational railway environment. This definition is given in Part 0 as

To provide the driver with information to drive the train safely and to enforce respect of this information to the extent advised to ETCS.

### **5.2 Structure**

5.2.1.1 From the system definition, the system splits naturally into two parts

- a) The provision of information to the driver that keeps him informed of limits, in terms of speed and distance that he must observe in order to maintain safety
- b) The enforcement function that protects the train from breaching a safe speed and distance envelope by intervening with a request for a pre-emptive brake application.

5.2.1.2 Both the provision of information and enforcement functions are dependent upon knowing the safety parameters in terms of allowed movements and permissible speeds and then relating this to the capability of the train. This information is then used to supervise the passage of the train by continuously comparing actual performance against that required such that a decision about intervention can be made.

5.2.1.3 The speed profile for a route is represented by the Most Restrictive Speed Profile. This in turn is modified by the Movement Authority authorisations to create the Dynamic Speed Profile. The Dynamic Speed Profile is the embodiment of the safety parameters as it contains both the speed and distance limits.

5.2.1.4 This simplified operational view based on the major functionality of ETCS is used to create the conceptual fault tree.

Note: Being based on the major functions the event names do not match those of the macro functions used in appendix B

### **5.3 Fault Tree Diagram**

5.3.1.1 The conceptual fault tree is given Appendix A



## **6. DETAILED, GENERIC LEVEL 2 FAULT TREE**

### **6.1 Concept**

- 6.1.1.1 This fault tree is a detailed development based on the principles of the conceptual tree given in appendix A.
- 6.1.1.2 The tree provides a complete deployment of the functions as given in the Function List but not necessarily in the same groupings.
- 6.1.1.3 The Tree provides a complete picture of the functional hierarchy of the Unisig system when being operated in application level 2.
- 6.1.1.4 This fault tree is given in Appendix B. This fault tree is developed on Fault Tree Plus version 11.2.



## **7. PRELIMINARY SAFETY RELATED COMMENTS**

### **7.1 General Comments.**

7.1.1.1 Even at this initial stage, comments on the safety aspects of the system design can be made following examination of the functional fault tree. Many of the issues noted will in practice be affected by the magnitude (too large or too small) of the error and the direction (high or low) of the error. This analysis, along with the effect of different modes of operation, is the subject of Part 2 of this suite of documents.

7.1.1.2 The role of the ETCS system has been defined in Part 0 as being:

To provide the driver with information to enable him to drive his train safely and to enforce respect of this information to the extent advised to ETCS.

Associated with this role is the ETCS Core Hazard, also defined in Part 0:

Exceedance of the safe speed or distance as advised to ETCS

7.1.1.3 Working down the fault tree from the top hazard (ETCS Core Hazard) it is clear that due to the need to keep the display to the driver and the supervision parameters co-incident, there will be major common mode issues within the system. This is borne out by the functional fault tree.

7.1.1.4 From a safety perspective this need for co-incidence means, if the information provided to the train carried system is incorrect in terms of a safe speed and distance, then the driver will be shown the wrong targets. If he drives to these incorrect targets he will be allowed to do so without being protected from making an unsafe move by the ETCS supervision and intervention functions.

7.1.1.5 There are benefits however, which act to reduce the integrity requirements on the display to the driver. This is because, assuming the supervision function is correctly functioning, the driver is protected against a failure of the display.

7.1.1.6 The most important common mode issue external to ETCS is the function of Data Entry whereby the length and capability of the train are provided to the ETCS. This information affects the calculation of the Most Restrictive Speed Profile (MSRP) and separately, the braking algorithm calculation.

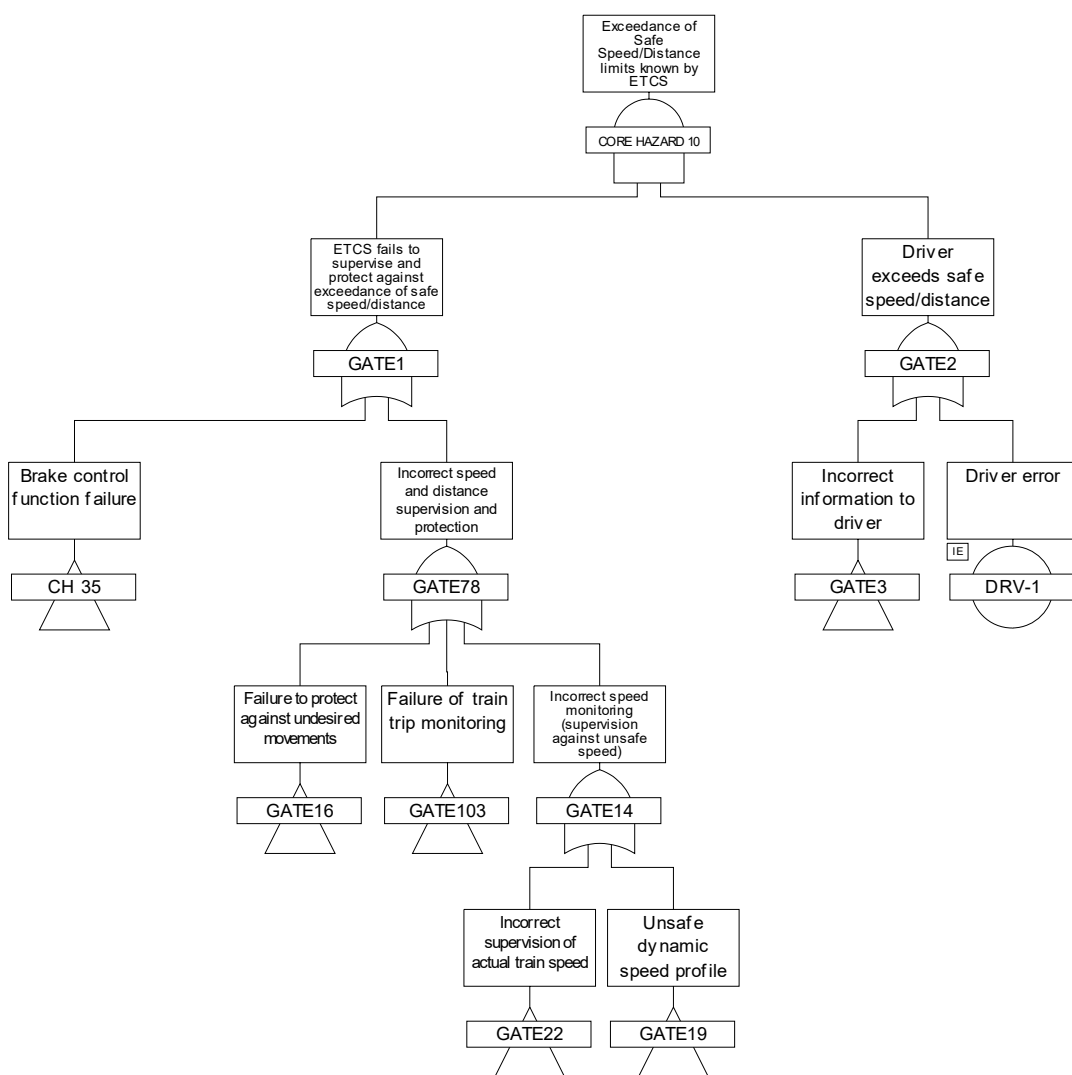
7.1.1.7 There is nothing that ETCS can do if a driver confidently enters and acknowledges erroneous data. Thus rigorous checks outside ETCS will be essential, particularly if data is modified during a journey or under emergency conditions where an independent check may be difficult to initiate.



- 7.1.1.8 Internal to ETCS there are several common mode issues which may affect the internal assignment of integrity levels. In this respect the primary base event would be that of speed and position which will impact on the Dynamic Speed Profile calculation.
- 7.1.1.9 Another source of common mode error would be incorrect track topography and/or incorrect placing of balises. Again this error would affect both the supervision and the display functions.

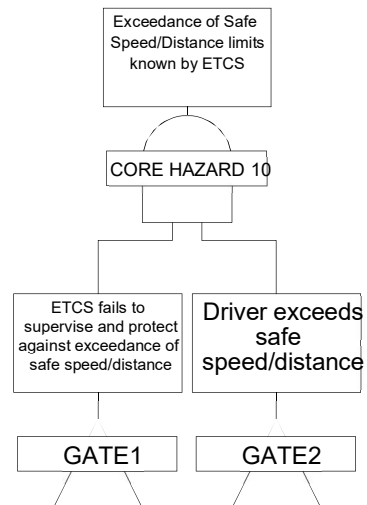
## 8. APPENDIX A

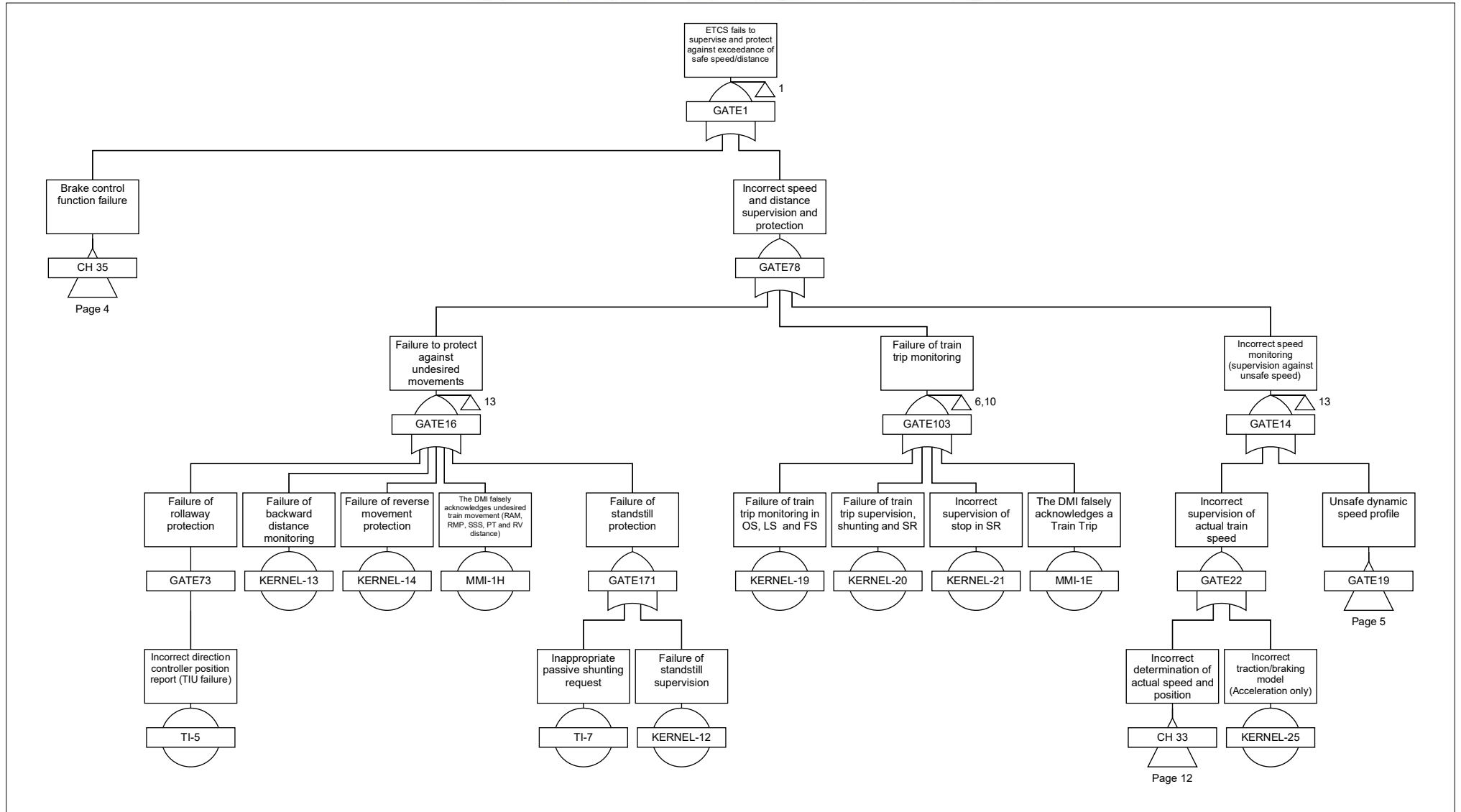
### 8.1 Conceptual Fault Tree

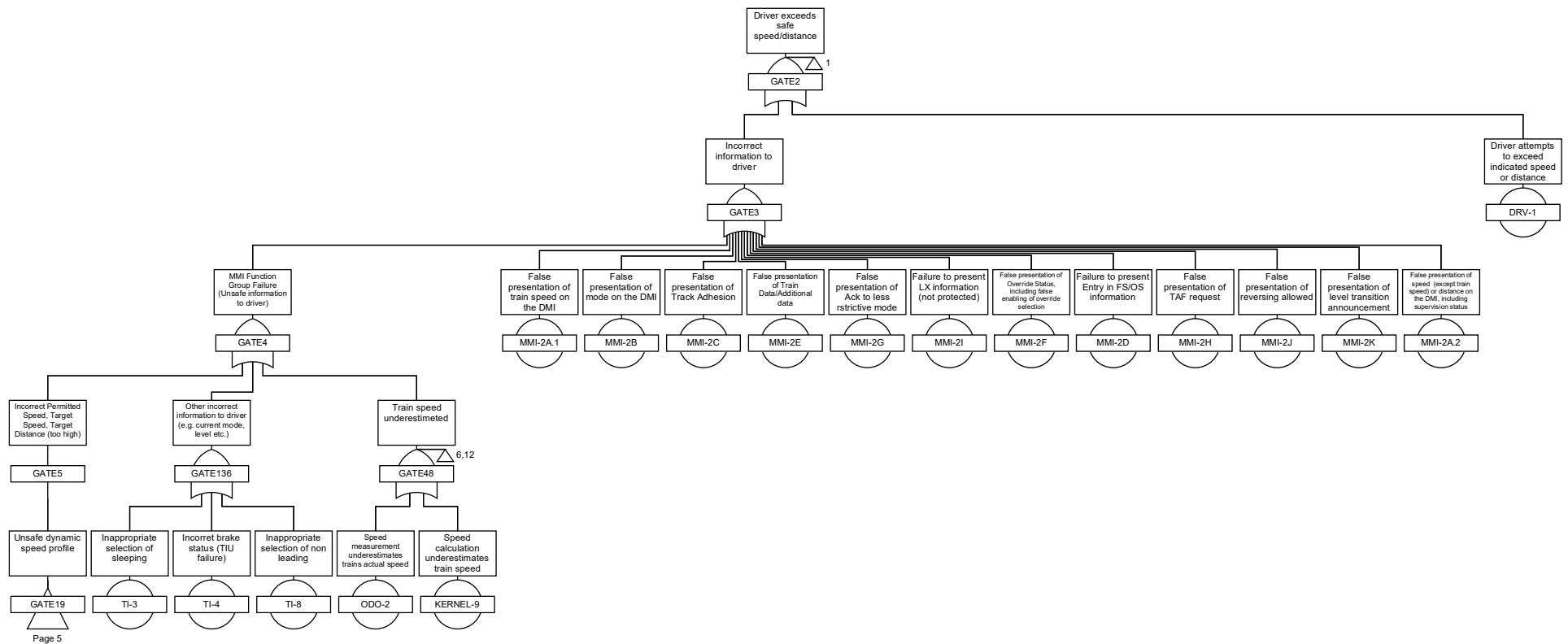


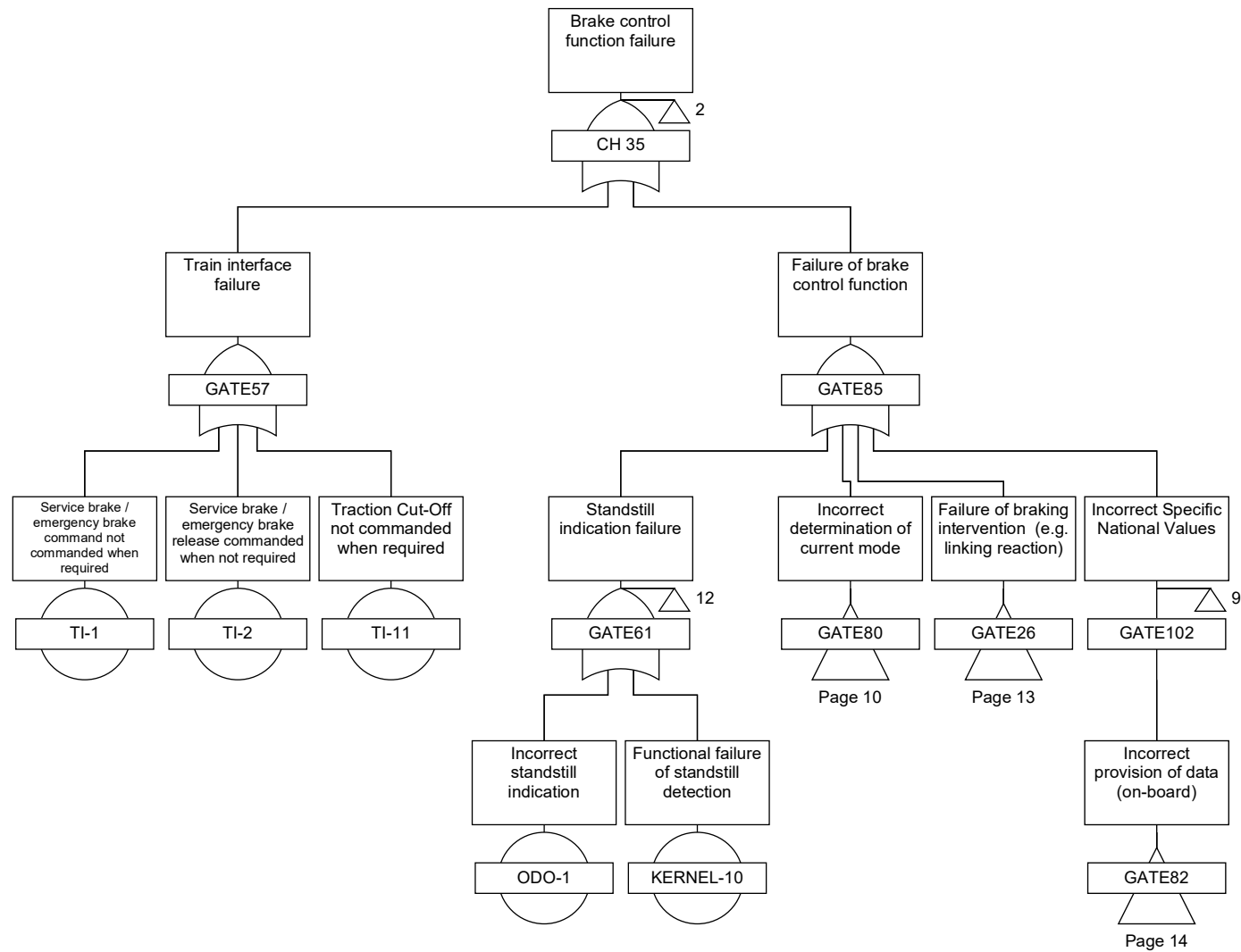


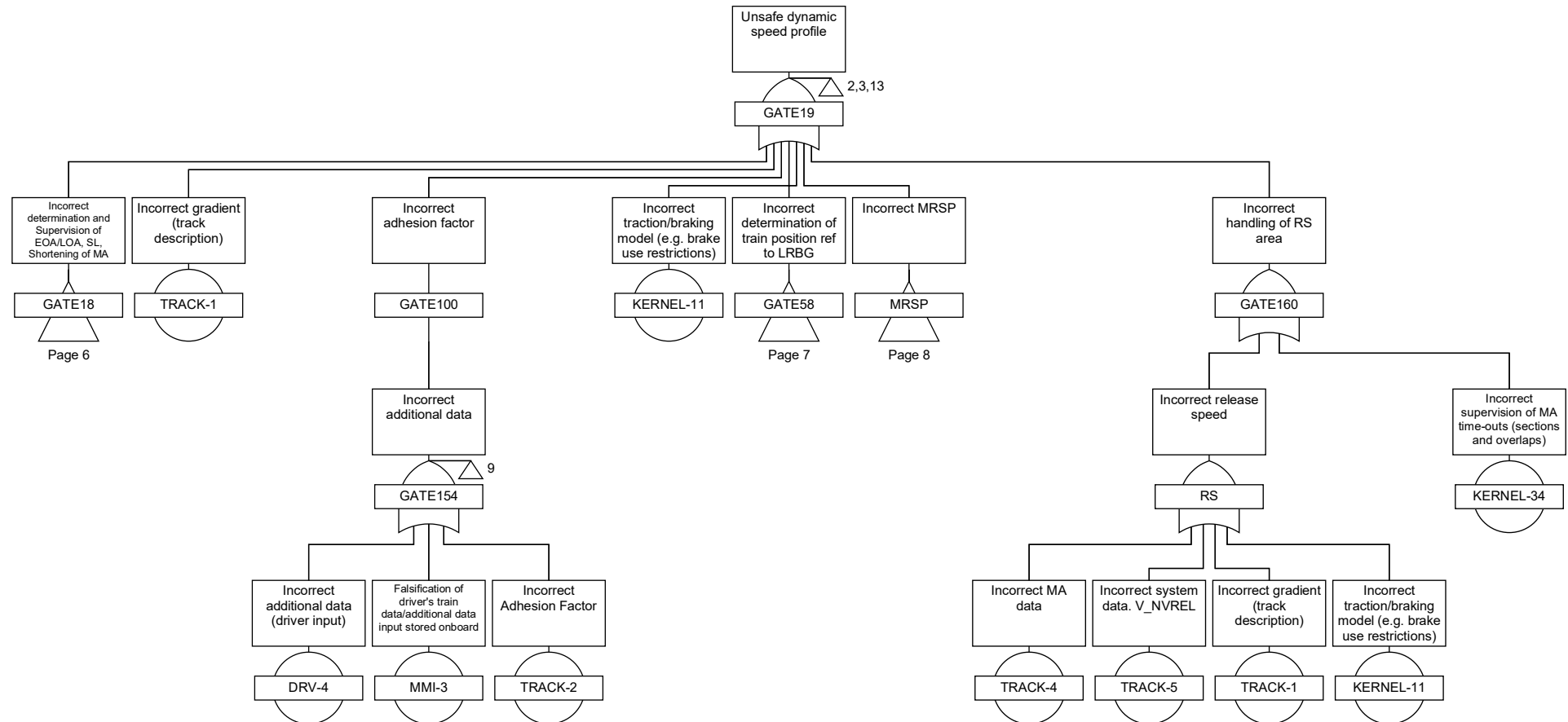
## 9. APPENDIX B - DETAILED SYSTEM LEVEL FAULT TREE

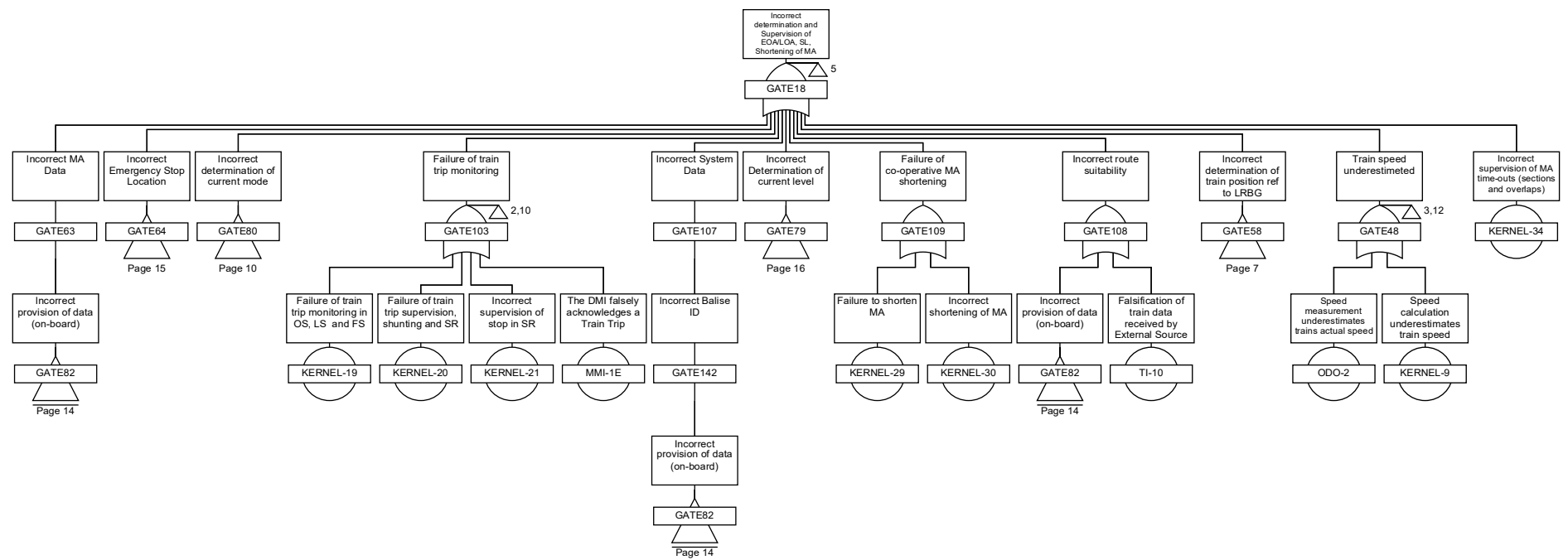


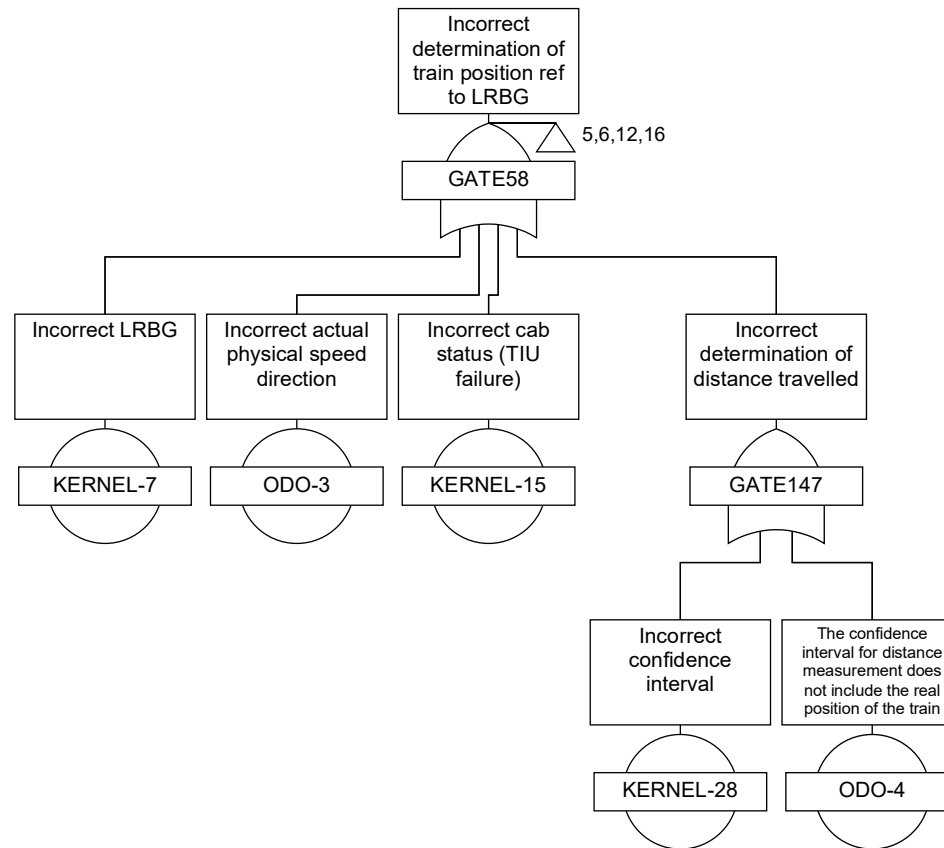


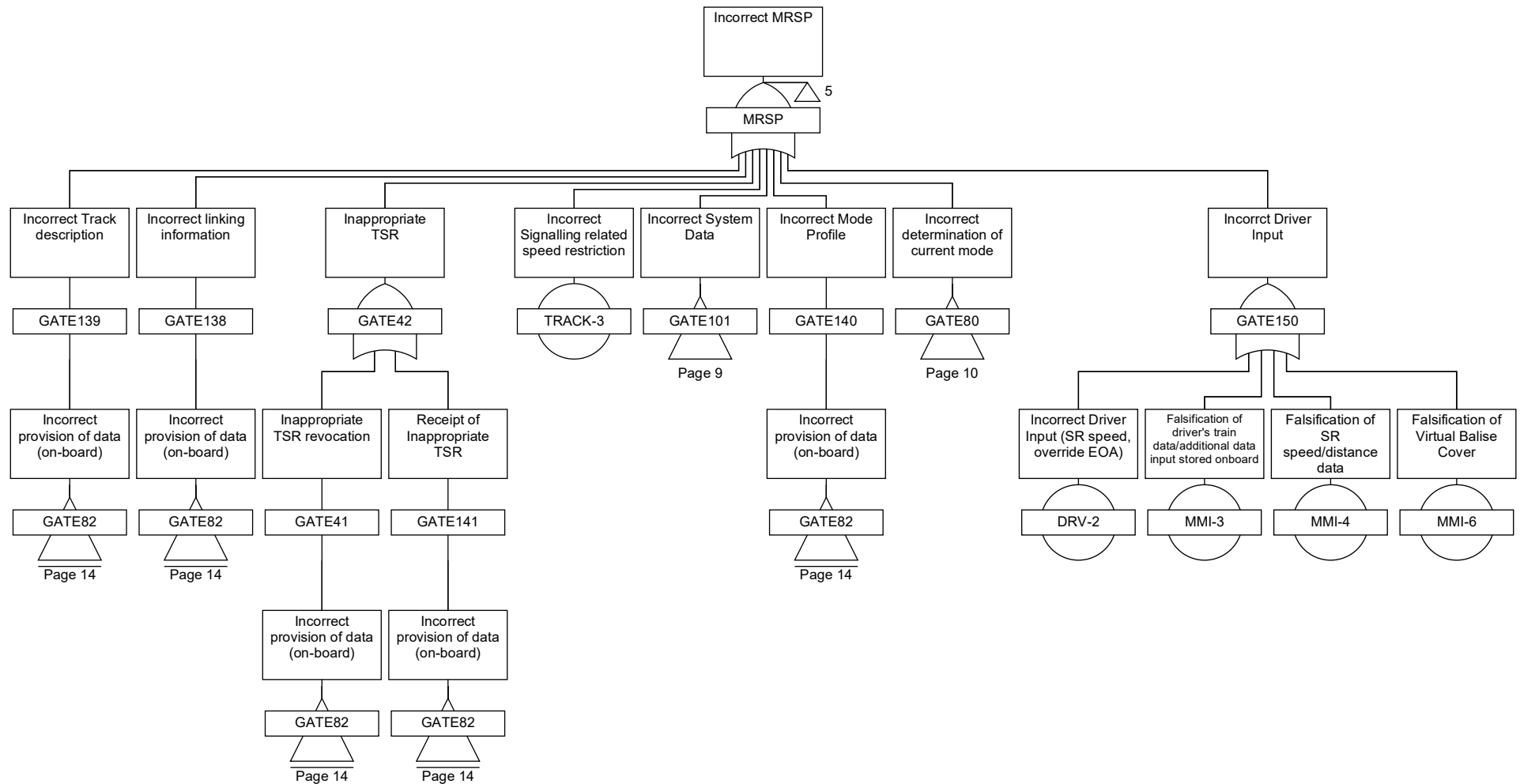


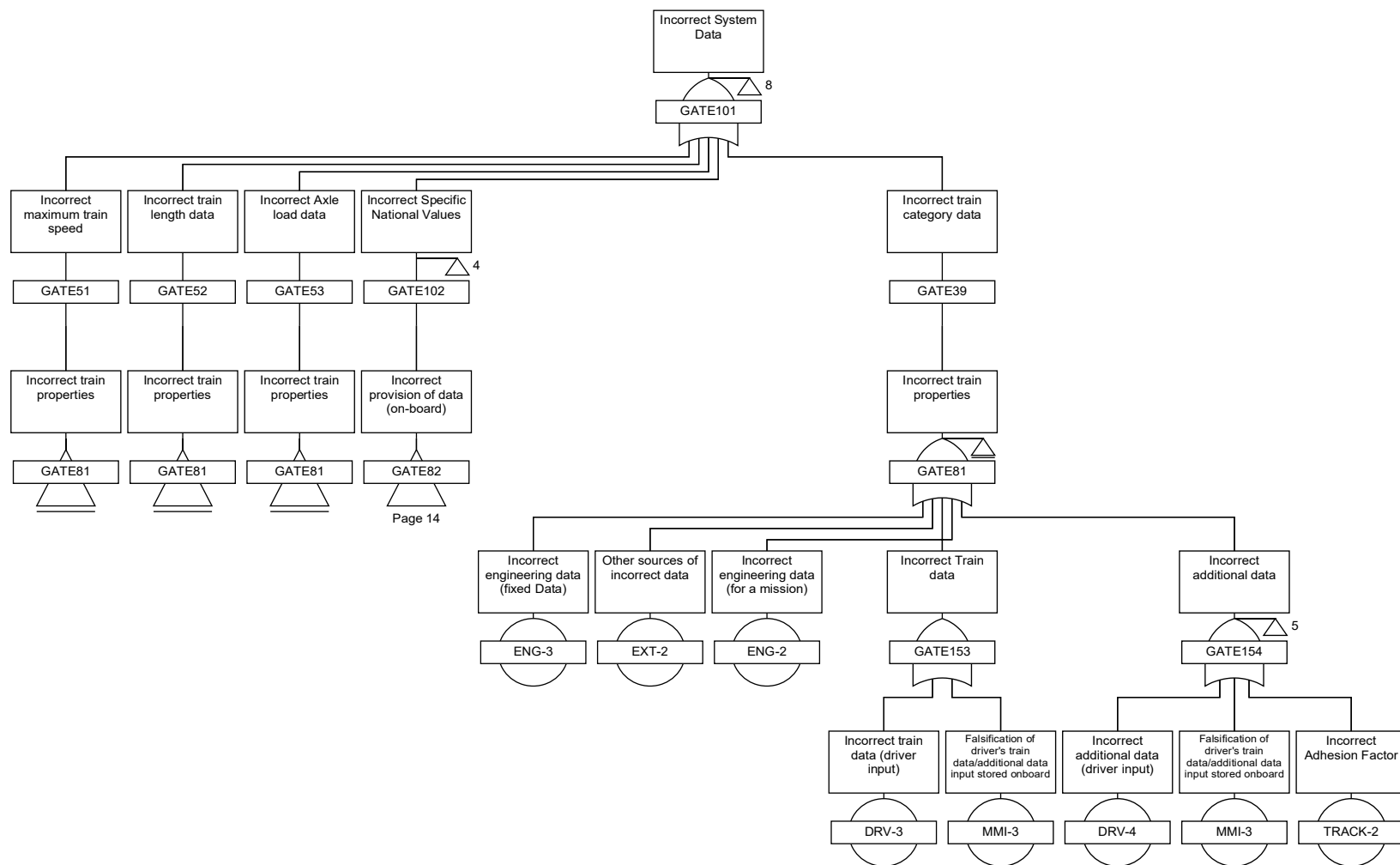


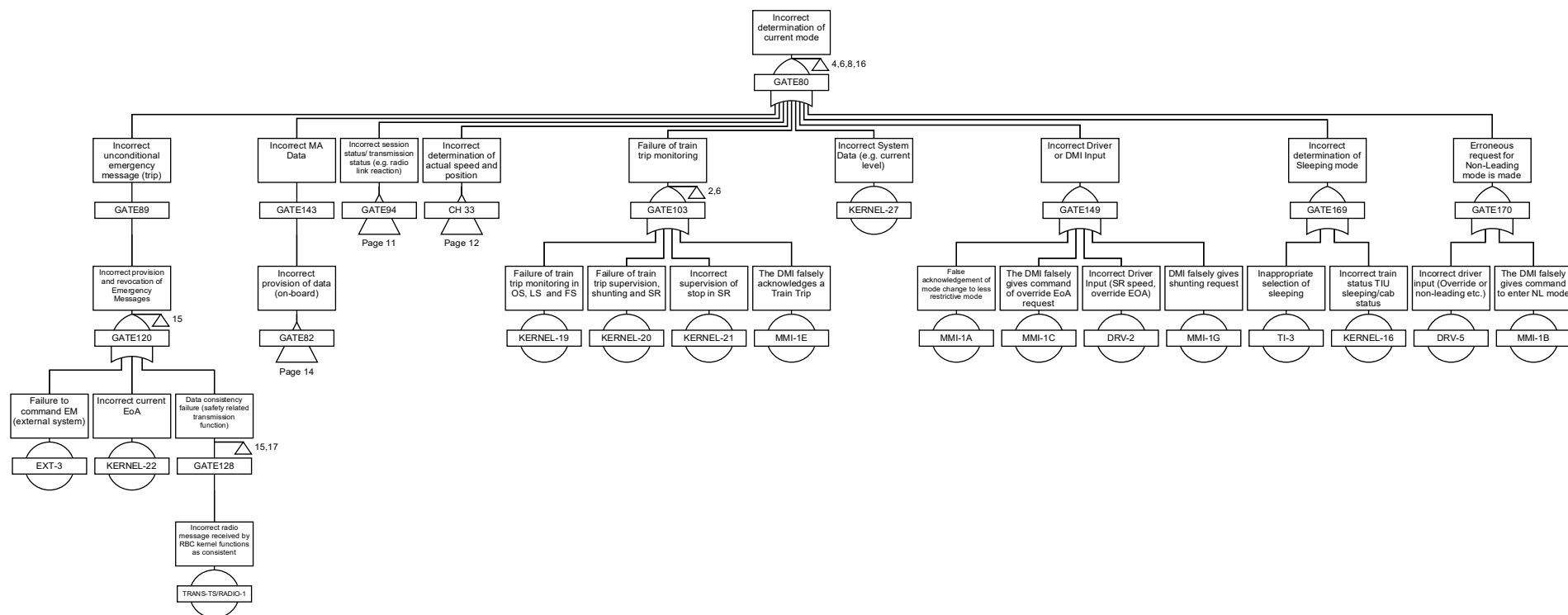


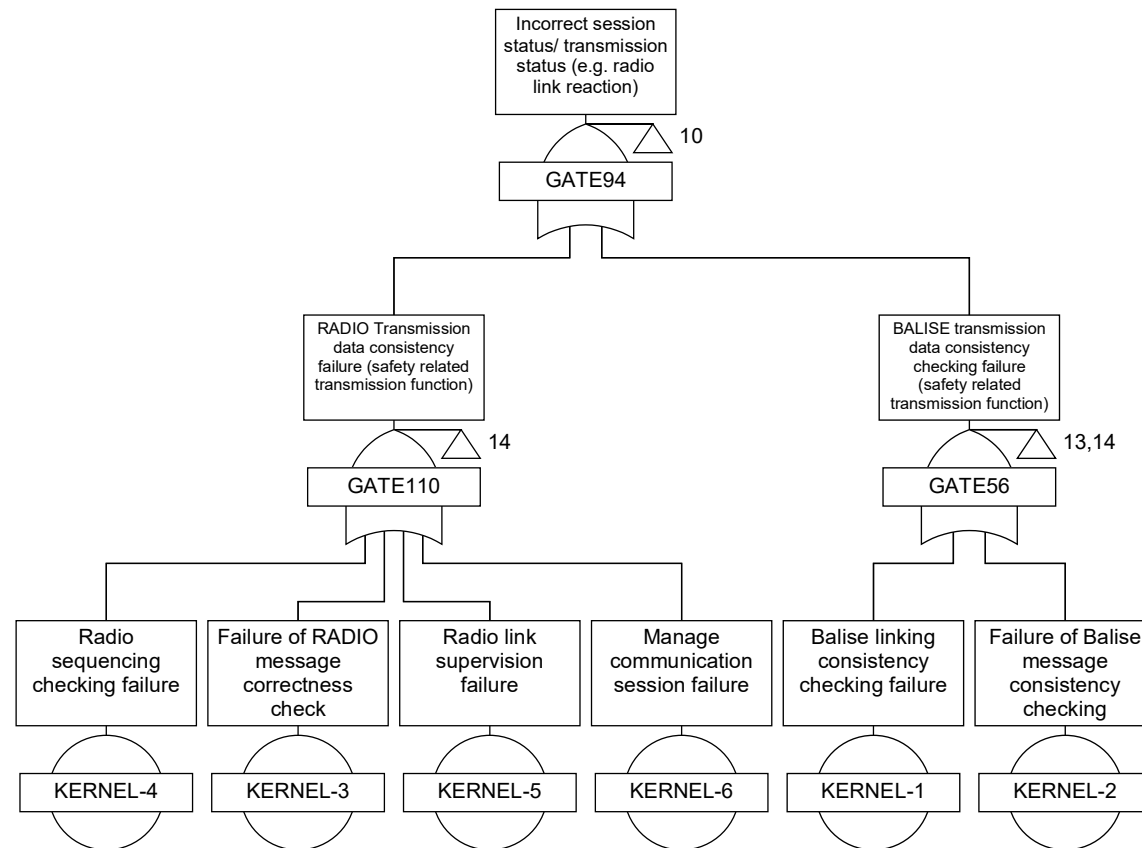


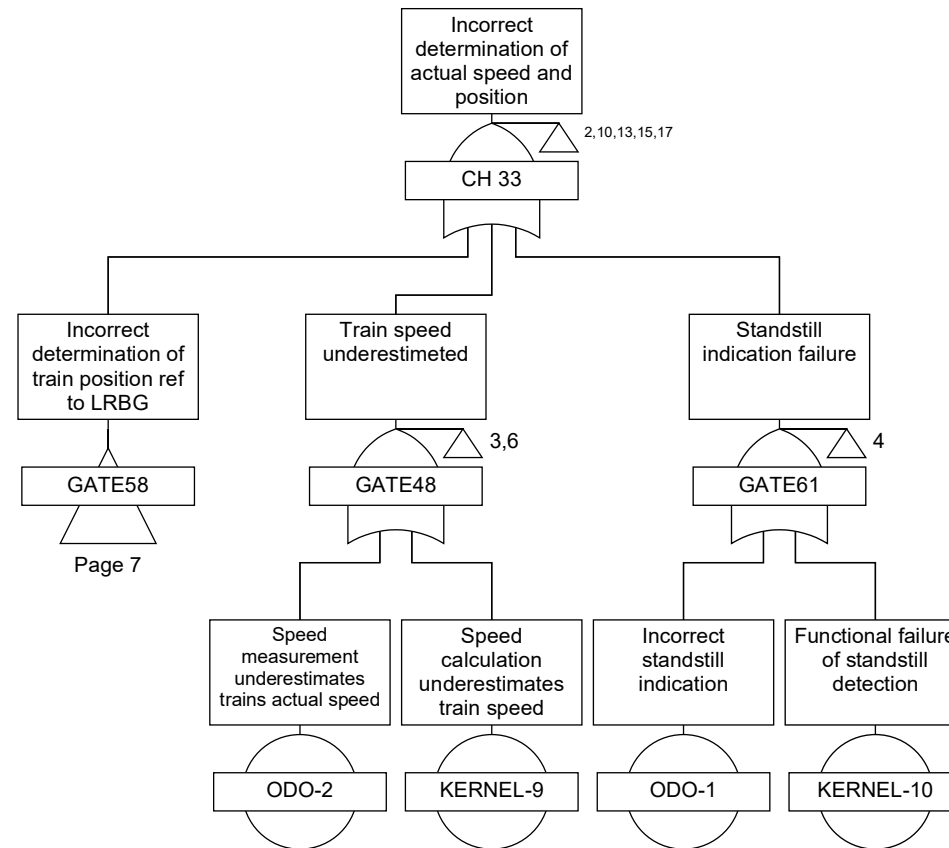


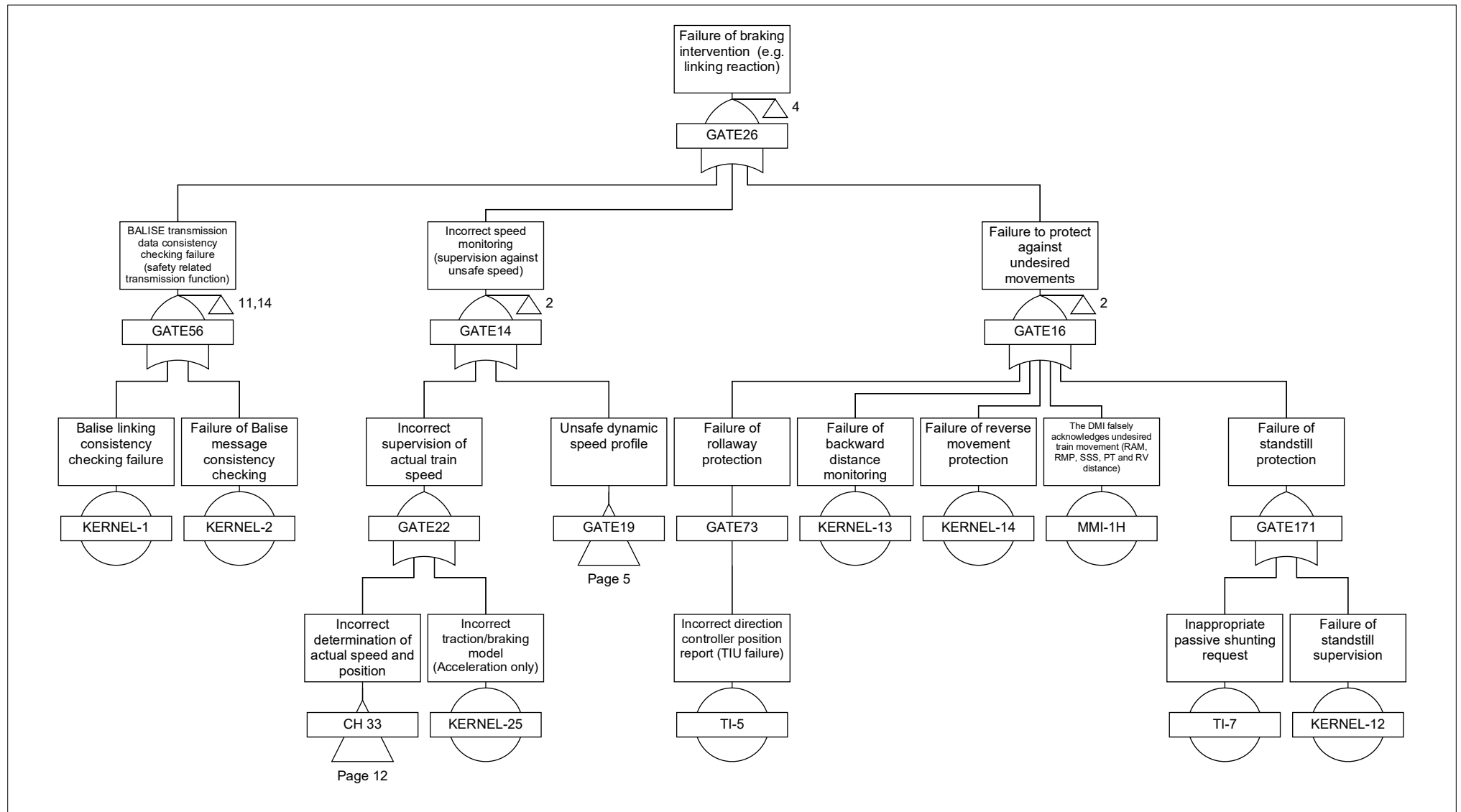




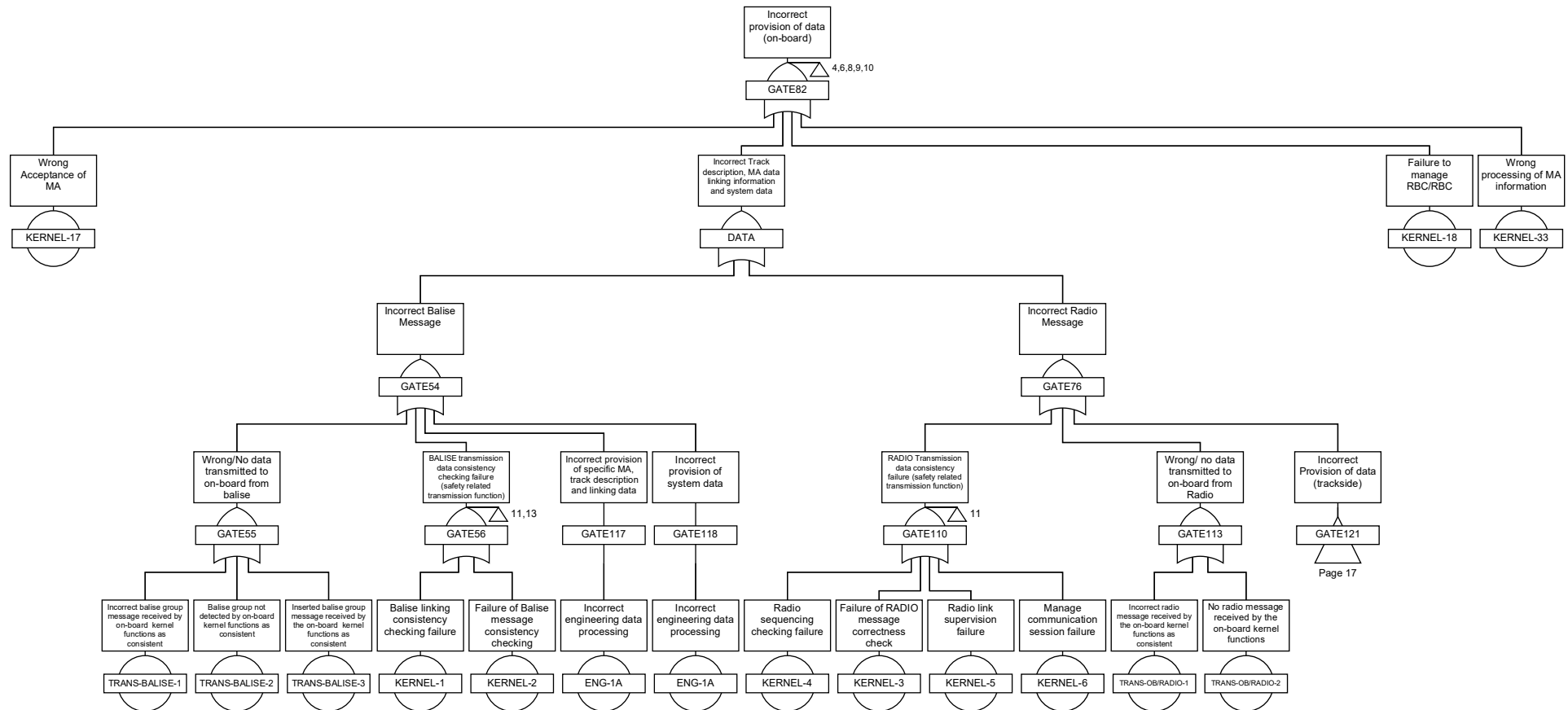


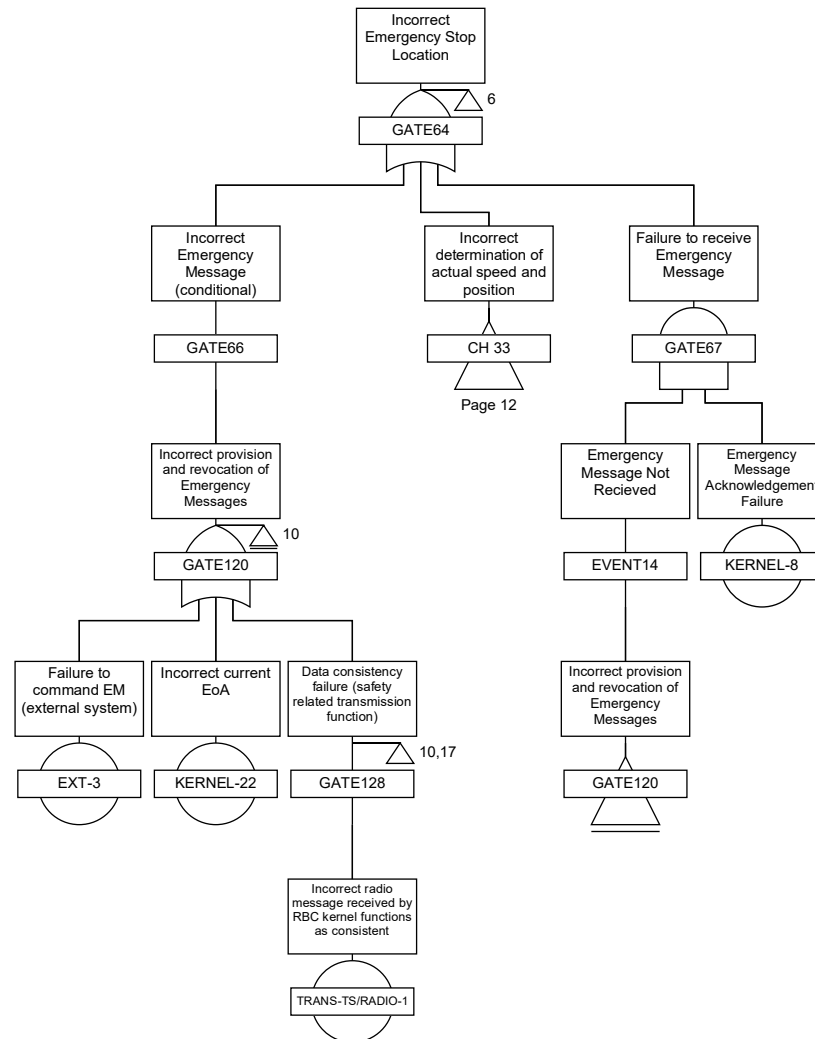


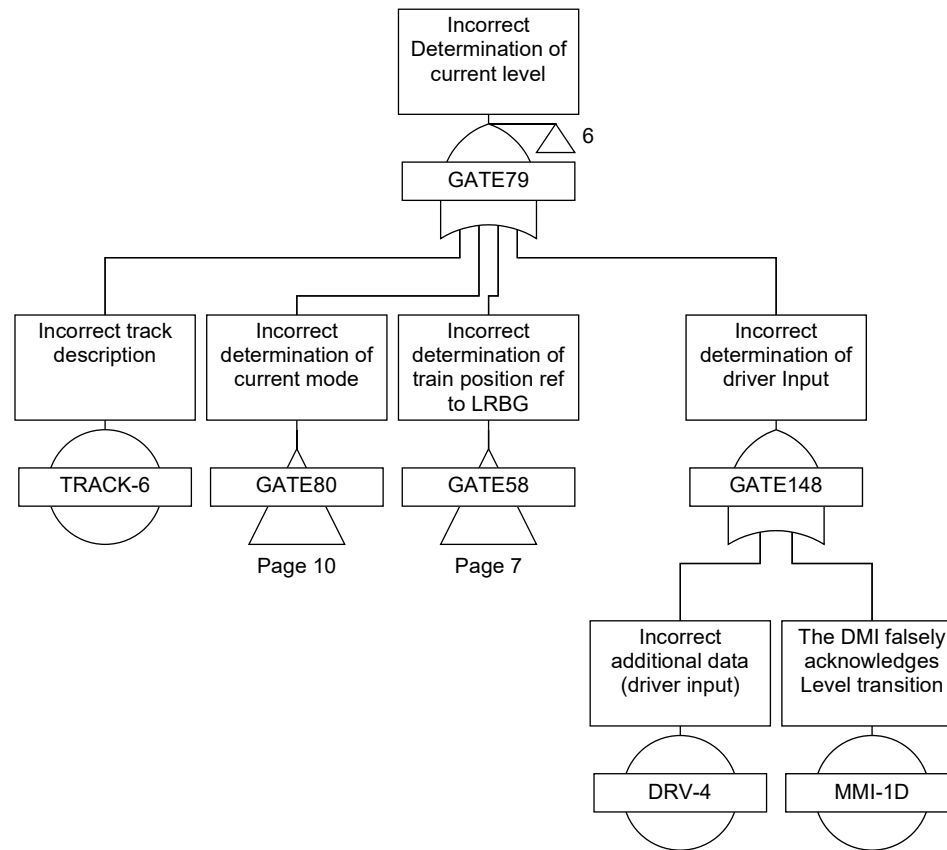


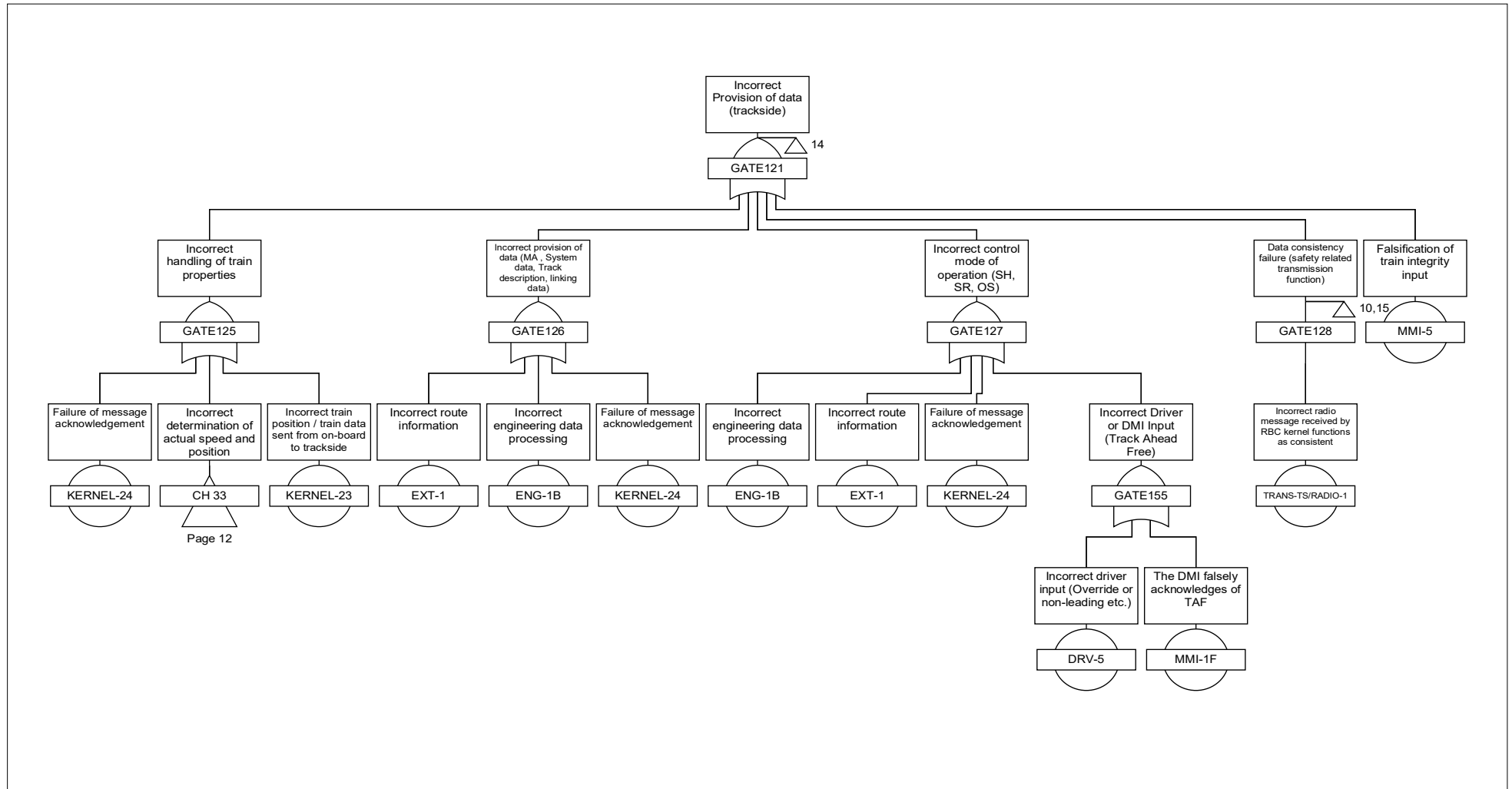


© This document has been developed and released by UNISIG









## 10. APPENDIX C

### 10.1 Modes and on-board Functions in Level 2

#### 10.1.1 Introduction

10.1.1.1 The following function table is derived from the SRS Chapter 4.5 'Modes and on-board Functions'. The following table, which specifies in which modes the on-board functions are active or not, was developed to enable the creation of the fault tree. The functions are described in detail in the SRS with the appropriate reference being given in the fourth column of the table under "Related SRS paragraph". In addition, references to the gates in the fault tree are provided.

10.1.1.2 The resulting hierarchy is generic and not mandatory for the design of a product. It is developed to provide a static view of functional interaction.

10.1.1.3 Note: Modes are not the only thing that can influence an onboard function. This is why this table is not enough in itself to understand all the ERTMS/ETCS onboard behaviour. It must be understood as a complement to all other SRS chapters (especially SRS chapters 4.7, 4.8, 4.9 and 4.10).

10.1.1.4 Note: for DMI depending on modes, refer to SRS chapter 4.7.

#### 10.1.2 Active Functions Onboard Function Table

10.1.2.1 X = functions shall be active

Empty case = function shall be inactive

O = Optional (function is not required for interoperability, but is not forbidden)

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
<b>1</b>	<b>Check data consistency</b>																			
<b>1.1</b>	<b>Balise Message Consistency</b>	Gate 54																		
1.1.1	Check balise linking consistency	Gate 54 56	3.16.2.3 3.4.4					X	X		X									

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
1.1.2	Check Balise Group Message Consistency (if linking consistency is checked)	Gate 54 56	3.16.2.4.1 3.16.2.4.3					X	X		X									
1.1.3	Check Balise Group Message Consistency (if no linking consistency is checked) (because no linking information is available and/or because the function "check linking consistency" is not active)	Gate 54 56	3.16.2.4.4		X	X	X	X	X	X	X	X	X	X	X	X			X	X
1.1.4	Check Unlinked Balise Group Message Consistency	Gate 54 56	3.16.2.5		X	X	X	X	X	X	X	X	X	X	X	X			X	X
1.1.5	System Version Management	Gate 54 56	3.17		X	X	X	X	X	X	X	X	X	X	X	X			X	X
<b>1.2</b>	<b>Radio Message Consistency</b>	Gate 76																		
1.2.1	Check correctness of radio messages	Gate 76 110	3.16.3.1		X	X	X	X	X	X	X	X	X	X	X	X			X	X
1.2.2	Check radio sequence	Gate 76 110	3.16.3.3		X	X	X	X	X	X	X	X	X	X	X	X			X	X
1.2.3	Check safe radio connection	Gate 76 110	3.16.3.4					X	X		X									
1.2.4	Manage Communication Session	Gate 76 110	3.5		X	X	X	X	X	X	X	X	X	X	X	X			X	X

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N	S	P	S	F	L	S	O	S	N	U	T	P	S	I	S	R
				P	B	S	H	S	S	R	S	L	L	N	R	T	F	S	N	V
<b>2</b>	<b>Determine Train Speed and Position:</b>	CH 33																		
2.1	Determine train position referenced to LRBG	Gate 58	3.6.1 3.6.4		X	X	X	X	X	X	X	X	X	X	X	X			X	X
2.2	Determine train speed, train standstill	Gates 48 61	None		X	X	X	X	X	X	X	X	X	X	X	X		O	X	X
2.3	Determine current onboard-LRBG	Event "Kernel - 7"	3.4.4, 3.6.1.4, 3.6.2.2.2		X		X	X	X	X	X	X	X	X	X	X			X	X
<b>3</b>	<b>Handle Train Properties</b>	Gate 81							X											
3.1	Manage change of Train Data from external sources	Gate 81 153	3.18.3, 5.17, 5.4.3		X			X	X	X	X			X	X	X			X	
3.2	Report Validated Train Data	Gate 81	3.18.3.4		X															
3.3	Report Train Position	Gate "CH33"	3.6.5.																	
3.3.1	Report train position when train reaches standstill	Gate 58 & 48	3.6.5.1.4 a)					X	X	X	X							O		X
3.3.2	Report train position when mode changes to ...	Gate 58 & 48	3.6.5.1.4 b)		X		X	X	X	X	X	X	X	X	X	X	X	O	X	X
3.3.3	Report train position when train integrity confirmed by driver	Gate 58 & 48	3.6.5.1.4 c)		X			X		X	X					X				
3.3.4	Report train position when loss of train integrity is detected	Gate 58 & 48	3.6.5.1.4 d)		X			X	X	X	X				X	X				X
3.3.5	Report train position when train front/rear passes an RBC/RBC border	Gate 58 & 48	3.6.5.1.4 e)					X	X	X	X				X					
3.3.6	Report train position when train rear passes a level transition border (from level 2/3 to 0, NTC, 1)	Gate 58 & 48	3.6.5.1.4 f)					X	X	X	X			X	X					X

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N	S	P	S	F	L	S	O	S	N	U	T	P	S	I	S	R
				P	B	S	H	S	S	R	S	L	L	N	R	T	F	S	N	V
3.3.7	Report train position when change of level due to trackside order	Gate 58 & 48	3.6.5.1.4 g)					X	X	X	X		X		X					
3.3.8	Report train position when change of level due to driver request	Gate 58 & 48	3.6.5.1.4 g)		X			X	X	X	X		X							
3.3.9	Report train position after establishment of a session with RBC	Gate 58 & 48	3.6.5.1.4 h)		X		X	X	X	X	X	X	X	X	X	X			X	X
3.3.10	Report train position when a data consistency error is detected	Gate 58 & 48	3.6.5.1.4 i)		X			X	X	X	X	X	X	X	X	X			X	X
3.3.11	Report train position as requested by RBC...	Gate 58 & 48	3.6.5.1.5 3.6.5.1.4 i)		X			X	X	X	X		X	X	X	X			X	X
3.3.12	... or Report train position at every passage of an LRBG compliant balise group	Gate 58 & 48	3.6.5.1.4 j)					X	X	X	X		X	X	X	X			X	X
3.4	Provide Date and Time	no impact to safety	3.18.5		X	X	X	X	X	X	X	X	X	X	X	X			X	X
<b>4</b>	<b>Determine Mode and Level</b>	-																		
4.1	Determine ERTMS/ETCS Mode	Gate 80	3.12.4, 4.6	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.1.1	Inhibit Trip (Override function)	Gates 143 149	5.8				X			X				X					X	
4.2	Determine ERTMS/ETCS level	Gate 79	5.10		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X
<b>5</b>	<b>Manage Emergencies</b>	-																		
5.1	Manage Conditional Emergency Stop	Gate 64	3.10					X	X		X					X				
5.2	Manage Unconditional Emergency Stop	Gate 89	3.10		X			X	X	X	X					X				

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N	S	P	S	F	L	S	O	S	N	U	T	P	S	I	S	R
				P	B	S	H	S	S	R	S	L	L	N	R	T	F	S	N	V
<b>6</b>	<b>Provide Data</b>																			
<b>6.1</b>	<b>Handle Data</b>	Gate 82																		
6.1.1	Accept MA	Event "Kernel-17"	3.7.2 3.8.5 4.8.4		X			X	X	X	X			X		X			X	
6.1.2	Delete Track Description, Linking Information and MA data	Gates "DATA" 139 138 63	3.7.3.3 4.9 4.10	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.1.3	Delete Revoked TSR	Gate 41	3.11.5.5		X			X	X	X	X			X	X	X				
<b>6.2</b>	<b>Provide Fixed Values, and Default/National Values</b>	Gate 118	3.18.1 3.18.2		X	X	X	X	X	X	X	X	X	X	X	X			X	X
<b>7</b>	<b>Supervise and Protect</b>	-																		
<b>7.1</b>	<b>Determine EOA/LOA SL Shortening of MA</b>																			
7.1.1	Determine EOA/LOA, SL	Gates 18, 160	3.8.4 3.8.5					X	X		X									
7.1.2	Co-operative Shortening of MA	Gate 109	3.8.6					X	X		X									
7.1.3	Supervise "danger for shunting" information and list of expected balises for shunting	Event "Kernel-20"	4.4.8.1.1 b) and c)				X													
7.1.4	Supervise "Stop if in SR" information and list of expected balises for Staff Responsible	Event "Kernel-21"	4.4.11.1.3 c) and d)							X										



	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
7.1.5	Supervise passing EOA/LOA	Gate 18  Event "Kernel- 34"	3.13.8					X		X <sub>1</sub>	X									

<sup>1</sup> In SR mode the end of the SR Authorization is supervised.

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
<b>7.2</b>	<b>Monitor Speed</b>	Gate 14																		
7.2.1	Request MA Cyclically respect to approach of perturbation location (T_MAR) or MA timer elapsing (T_TIMEOUTRQST)	no impact to safety	3.8.2.3 a) and b)					X	X		X									
7.2.2	Request MA Cyclically when "Start" is selected	no impact to safety	3.8.2.7 4.4.11 5.4, 5.11		X					X						X				
7.2.3	Determine Most Restrictive Speed Profile	Gate "MRSP"																		
7.2.3.1	Calculate SSP	Gate "MRSP"	3.11.3					X	X		X									
7.2.3.2	Calculate ASP	Gate "MRSP"	3.11.4					X	X		X									
7.2.3.3	Calculate TSR	Gate "MRSP"	3.11.5					X	X	X	X			X						
7.2.3.4	Calculate Signalling related speed restriction when evaluated as a speed limit	Gate "MRSP"	3.11.6					X	X		X									
7.2.3.5	Calculate (or enter) Mode related speed restriction	Gate "MRSP"	3.11.7				X		X	X	X			X						X
7.2.3.6	Calculate (or enter) Train related speed restriction	Gate "MRSP"	3.11.8					X	X	X	X			X						X
7.2.3.7	STM max speed	Gate "MRSP"	3.11.2.2 g)					X	X	X	X			X					X	
7.2.3.8	STM system speed	Gate "MRSP"	3.11.2.2 h)					X	X	X	X			X						
7.2.3.9	LX speed	Gate "MRSP"	3.12.5.6					X	X		X									
7.2.3.10	Speed restriction to ensure a given permitted braking distance	GATE "MRSP"	3.11.11					X	X		X									



	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
7.2.3.11	Override related speed restriction	GATE “MRSP”	5.8.3.6				X			X				X						

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
7.2.4	<b>Supervise Train Speed</b>																			
7.2.4.1	Monitor Speed and Distance based on MRSP (Dynamic Speed Profiles), MA, release speed, gradient, mode profile, non protected LX start location, and route unsuitability location	Gate 14	3.13 5.9.3.5 5.7.3.4 3.12.2.8 3.12.5.4					X	X		X									
7.2.4.2	Monitor Speed and Distance based on MRSP	Gate 14	4.4.10.1											X						
7.2.4.3	Monitor Speed and Distance based on MRSP (Dynamic Speed Profiles), allowed distance to run in SR mode	Gate 14	4.4.11							X										
7.2.4.4	Monitoring Ceiling Speed (no braking curve) based on MRSP	Gate 14	4.4.8.1.1 a) 4.4.18.1.3 a)				X												X	X
7.2.5	Request MA on track description deletion	Gate 14	3.8.2.7.3					X	X		X									
<b>7.3</b>	<b>Protect against undesirable Train Movements</b>	Gate 16																		
7.3.1	Protect against Backwards Distance movement	Event "Kernel-13"	4.4.14, 4.4.18													X				X
7.3.2	Protect against Roll Away	Gate 73	3.14.2				X	X	X	X	X			X		X				X
7.3.3	Protect against Reverse Movement	Event "Kernel-14"	3.14.3					X	X	X	X					X				X
7.3.4	Supervise Standstill	Event "Kernel-12"	3.14.4 4.4.7.1.5		X															

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N	S	P	S	F	L	S	O	S	N	U	T	P	S	I	S	R
				P	B	S	H	S	S	R	S	L	L	N	R	T	F	S	N	V
7.3.5	Supervise signalling related speed restriction when evaluated as a trip order	Gate "MRSP"	3.11.6.4					X	X	X	X									
<b>7.4</b>	<b>Control Brakes</b>	Gate 85	3.13 3.14.1	X	X		X	X	X	X	X			X	X	X	X			X
7.4.1	Command Emergency Brake	Gate 85	4	X											X		X			
<b>7.5</b>	<b>Protection functions</b>																			
7.5.1	Manage Track Conditions excluding Sound Horn, Non Stopping Areas, Tunnel Stopping Areas and Big Metal Masses	no impact to exceed safe speed and distance	3.12.1					X	X		X		X		X	X				
7.5.1.1	Manage Track Condition Big Metal Masses	no impact to exceed safe speed and distance	3.12.1		X	X	X	X	X	X	X	X	X	X	X	X	O			X
7.5.1.2	Manage Track Conditions Sound Horn, Non Stopping Areas, Tunnel Stopping Areas	no impact to exceed safe speed and distance	3.12.1					X	X		X									
7.5.2	Manage Route Suitability	Gate 108	3.12.2					X	X		X									
7.5.3	Manage Text Display to the driver	Gate 4	3.12.3		X			X	X	X	X		X	X	X	X				X
<b>8</b>	<b>Other functions</b>								X											
8.1	Determine Geographical Position	Gate 4	3.6.6		X			X	X	X	X		X	X	X	X				

	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
8.2	Manage RBC/RBC Handover	(Gate 82)	3.15.1, 5.15					X	X	X	X	X	X		X					
8.3	Manage Track Ahead Free Request	-	3.15.5		X				X	X	X					X				
8.4	Provide Juridical Data	no impact to exceed safe speed and distance	3.20		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8.6	Continue Shunting on desk closure (Enabling transition to Passive Shunting mode)	no impact to exceed safe speed and distance	5.12.4				X													
8.7	Manage "Stop Shunting on desk opening" information	Gate 80	4.4.20.1.8 4.4.20.1.9			X														
8.8	Inhibition of revocable TSRs from balises (only level 2/3)	MRSP	3.11.5.12 3.11.5.13 3.11.5.14 3.11.5.15					X	X		X				X	X				
8.9	Cold Movement Detection	-	3.15.8	O																
8.10	Advance display of route related information	no impact to exceed safe speed and distance	3.15.10					O												
8.11	Virtual Balise Cover	MRSP	3.15.9		X	X	X	X	X	X	X	X	X	X	X	X	X	O	O	X



	ONBOARD-FUNCTIONS	Related Fault Tree Gates	Related SRS paragraph	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
8.12	Manage LSSMA display to the driver	no impact to exceed safe speed and distance	4.4.19.1						X											

### 10.1.3 Trackside Function Table

10.1.3.1 The following table specifies the trackside functions. The functions described in the SRS and the reference is given in the fourth column of the table denoted “Related SRS paragraph”.

	TRACKSIDE-FUNCTIONS	Related Fault Tree Gates	RELATED SRS paragraph
<b>1</b>	<b>Define Balise configuration and linking</b>	Gate 54	
1.1	<p>Define Balise group</p> <p><i>It is the trackside responsibility to take care that the number of balises in a group and that their identification within the group is correct.</i></p> <p><i>Variables in the balise message may be affected by basic message errors during transmission (mitigations: safety code)</i></p>	Gate 54	3.4.1
1.2	<p>Define Balise co-ordinate system</p> <p><i>It is the trackside responsibility to take care that orientation information and the installation of a balise group is correct.</i></p> <p><i>Variables in the balise message may be affected by basic message errors during transmission (mitigations: safety code, groups of more than one balise)</i></p>	Gate 54	3.4.2
1.3	<p>Define Linking</p> <p><i>It is the trackside responsibility to take care that linking information is correct.</i></p> <p><i>Variables in the message may be affected by basic message errors during transmission (mitigations: safety code)</i></p>	Gate 54 and 126	3.4.4
<b>2</b>	<b>Manage radio communication</b>	Gate 128	
2.1	<p>Establish a communication session</p> <p><i>It is the trackside responsibility to order an on-board to initiate the establishment of a communication session.</i></p> <p><i>It is also the trackside responsibility to send the correct system version.</i></p>	not detailed further	3.5.3
2.2	<p>Maintain a communication session</p> <p><i>The trackside shall not attempt to re-establish a connection accidentally lost.</i></p>	not detailed further	3.5.4

	TRACKSIDE-FUNCTIONS	Related Fault Tree Gates	RELATED SRS paragraph
2.3	<p>Terminate a communication session</p> <p><i>It is the trackside responsibility to order an on-board to terminate a communication session.</i></p>	not detailed further	3.5.5
<b>3</b>	<b>Transmit location specific data</b>		
3.1	<p>Transmit location specific data from balise</p> <p><i>It is the trackside responsibility to send location and profile data correctly referred to balise location and to install appropriately the balise groups.</i></p> <p><i>Variables in the balise message may be affected by basic message errors during transmission (mitigations: safety code, groups of more than one balise,...)</i></p>	Gate 117	3.6.2.1
3.2	<p>Transmit location specific data from RBC</p> <p><i>It is the trackside responsibility to send location and profile data correctly referred to LRBG location and to install appropriately the balise groups.</i></p> <p><i>Also internal functionality of RBC is relevant (e.g., selection of the appropriate message in a data base, on-line assembly of radio messages, etc.)</i></p> <p><i>Variables in the message may be affected by basic message errors during transmission (mitigations: safety code, ...)</i></p>	Gate 126	3.6.2.2
<b>4</b>	<b>Determine Train position</b>	Gate 125	
4.1	<p>Validate direction of transmitted information</p> <p><i>It is the trackside responsibility to identify correctly the direction of validity of information sent to the on-board.</i></p> <p><i>Variables in the message may be affected by basic message errors during transmission (mitigations: safety code,...)</i></p>	Gate 125	3.6.3
4.2	<p>Estimate of train location based on position report</p> <p><i>It is the trackside responsibility to use position reports received from the train, to select the correct information to send (e.g., a wrong MA could be sent to a train).</i></p> <p><i>Errors in this function may depend on internal RBC operations or on error in data configuration (trackside design).</i></p>	Gate 125	3.6.5

	TRACKSIDE-FUNCTIONS	Related Fault Tree Gates	RELATED SRS paragraph
<b>5</b>	<b>Check Completeness of data</b>	-	
5.1	<p>Check completeness of data</p> <p><i>It is the trackside responsibility to send MA only when all necessary information are received by the on-board and to send additional information when needed (e.g., emergency messages).</i></p> <p><i>Errors in this function may depend on trackside design errors (especially in level 1) internal operation of RBC or on errors at the interface with other trackside equipment (e.g., alarm detectors).</i></p> <p><i>(mitigations: on-board does not accept MA if SSP, gradient, etc. are not available for its length).</i></p> <p><i>Messages may be affected by basic message errors during transmission (mitigations: safety code, ack procedures,...)</i></p>	Gate 126	3.7.2
5.2	<p>Repeat data</p> <p>The RBC is responsible to send again track description and linking data, if informed that they have been deleted on-board.</p> <p><i>Radio messages may be affected by basic message errors during transmission (mitigations: safety code, ack procedures)</i></p>	Gate 126	3.7.3
<b>6</b>	<b>Manage Movement Authorities</b>	Gate 126	
6.1	<p>Structure MA</p> <p>It is the responsibility of trackside to send MA complying with ERTMS language and corresponding to trackside state.</p> <p><i>Messages may be affected by basic message errors during transmission (mitigations: safety code, ...)</i></p>	Gate 125 and 126	3.8.1, 3.8.3
6.2	<p>Manage MA</p> <p>Correctness of the engineering process in providing balise data and positioning balises correctly.</p>	Event "ENG-1A"	
6.3	<p>Co-operate in MA shortening</p> <p><i>It is the responsibility of the RBC to ask the concerned train, before allowing the release of a route.</i></p> <p><i>Messages may be affected by basic message errors during transmission, as corruption leading to request a false new EOA, to ask the wrong train, to false acceptance by the train, etc. (mitigations: safety code, time stamping,...)</i></p>	Gate 126	3.8.6

<b>7</b>	<b>Manage Emergency messages</b>	Gate 120	
7.1	<p>Structure emergency messages</p> <p><i>It is the responsibility of the RBC to send emergency messages complying with ERTMS language.</i></p> <p><i>Messages can also be affected by basic message errors during transmission as, corruption.</i></p>	Gate 120	3.10
7.2	<p>Send Emergency stop</p> <p><i>It is the responsibility of the RBC to send correct emergency messages when needed, according to input from trackside detectors, train position, etc.</i></p> <p><i>Messages can also be affected by basic message errors during transmission (e.g., deletion, repetition).</i></p> <p><i>(mitigations: safety code, ack procedures, time stamping,...)</i></p>	Gate 120	3.10.2
7.3	<p>Revoke emergency message</p> <p><i>It is the responsibility of the RBC to send correct emergency messages when needed, according to input from trackside detectors, train position, etc.</i></p> <p><i>Messages can also be affected by basic message errors during transmission (e.g., deletion, repetition).</i></p> <p><i>(mitigations: safety code, ack procedures, time stamping,...)</i></p>	Gate 120	3.10.3
<b>8</b>	<b>Manage Track description data</b>	Gate 126	
8.1	<p>Structure message</p> <p><i>It is the responsibility of trackside to send messages complying with ERTMS language.</i></p> <p><i>Messages may also be affected by basic message errors during transmission (mitigations: safety code, ...)</i></p>	Gate 125 and 126	3.11, 3.12
8.2	<p>Manage Temporary speed restrictions</p> <p><i>It is the responsibility of trackside to send correct messages when needed to the appropriate train.</i></p> <p><i>Messages may also be affected by basic message errors during transmission, as deletion, repetition, insertion.</i></p> <p><i>(mitigations: safety code, ack procedures...)</i></p>	Gate 126 or 117	3.11.5

8.3	<p>Send Text messages</p> <p>It is the responsibility of trackside to send correct messages when needed to the appropriate train.</p> <p><i>Messages may also be affected by basic message errors during transmission, as deletion, repetition, insertion. (mitigations: safety code, ack procedures...)</i></p>	<p>Gate 126  or  117</p>	3.12.3
9	<p><b>Manage RBC/RBC Handover</b></p> <p>Handing over RBC sends messages to the train.</p> <p>Input: information received from the accepting RBC, train location.</p> <p>Output: MA message to the train.</p> <p><i>Accepting RBC must inform the handing over RBC.</i></p> <p><i>Input: request from handing over RBC, information from trackside (state of routes)</i></p> <p><i>Output: state of the routes to the handing over RBC.</i></p> <p><i>The handing over RBC shall terminate the supervision of the train.</i></p> <p><i>Input: train location</i></p> <p><i>Output: termination of supervision.</i></p> <p><i>The accepting RBC shall start to send information to the train.</i></p> <p><i>Input: train location</i></p> <p><i>Output: initiation of train supervision.</i></p> <p><i>All messages may be affected by basic message errors during transmission.</i></p>		3.15.1
10	<p><b>Handle trains with NL engines</b></p> <p><i>The trackside may be informed on the location of NL engines, possibly used if they initiate a mission.</i></p>		3.15.2
11	<p><b>Splitting/joining</b></p>		3.15.3
12	<p><b>Manage Reversing</b></p> <p><i>It is trackside responsibility to send reversing area information.</i></p> <p><i>Message may be affected by basic message errors during transmission (mitigations: safety code, ack procedures, ...)</i></p>	<p>Gate 126</p>	3.15.4

<b>13</b>	<b>Request Track status (Track ahead free request)</b> It is the responsibility of the trackside to ask for information and use information received from the on-board to send MAs. <i>Input: information from trackside, train position.</i> <i>Output: decision to send MA message.</i>  <i>Messages may be affected by basic message errors during transmission (mitigations: safety code, ack procedures, ...)</i>		<b>3.15.5</b>
<b>14</b>	<b>Manage Data consistency</b>		
14.1	Prepare of balise and Loop messages Correctness of the engineering process in providing balise data and positioning balises correctly.	Event “ENG-1A”	3.16.2
14.2	Prepare of radio messages It is responsibility of trackside to prepare radio messages complying with ERTMS language. <i>Messages may also be affected by basic message errors during transmission. (mitigations. Safety code, time stamping, ...)</i>	Gate 128	3.16.3
14.3	Check received radio messages <i>It is the responsibility of trackside to reject a corrupted message and to avoid errors due to delayed, resequenced, masqueraded, etc. messages.</i>	Gate 121	3.16.3
<b>15</b>	<b>Manage System Version</b> Correctness of data from the engineering process.	Event “ENG-1B”	<b>3.17</b>
<b>16</b>	<b>Manage System data</b>	Gate 126	
16.1	Manage National values <i>It is the responsibility of trackside to send correct national values when necessary.</i> <i>Messages may also be affected by basic message errors during transmission. (mitigations: safety code, ...)</i>	Gate 126 or 118	3.18.2
16.2	Manage Train data It is the trackside responsibility to use train data received from on-board to select appropriate information for the train (e.g., SSP). <i>Messages may also be affected by basic message errors during transmission. (mitigations: safety code, ...)</i>	Gate 125	3.18.3

16.3	<p>Manage Additional data</p> <p>It is the trackside responsibility to use additional data received from on-board, e.g., to inform a supervision system outside ERTMS.</p> <p><i>Messages may also be affected by basic message errors during transmission. (mitigations: safety code,...)</i></p>	Gate 126	3.18.4
------	--	-------------	--------