ERTMS/ETCS
Functional Safety Analysis of ETCS DMI for ETCS Auxiliary Hazard
REF : SUBSET-118 ISSUE : 1.6.0 DATE : 2021-09-15

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

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.1.0 2011-11-10	All	Conversion to UNISIG template of: LR Rail report "Functional Safety Analysis of ETCS DMI, Final Safety Analysis Report, for European Railway Agency, December 2009", <62612rnpb090724>, v04.	Dag Ribbing
0.1.1 2011-11-23	All	- General updates to adapt document to baseline 3, version 3.2.0 according to performed impact analysis. - Minor formulation changes, since it is now a UNISIG document.	Dag Ribbing
0.1.2 2011-12-06		Updated after comments from UNISIG companies	Dag Ribbing
0.2.0 2011-12-06		Assigned document number Subset-118	Dag Ribbing
0.2.1 2012-01-27		- Updates due to further comments from UNISIG companies - Updates to adapt document to baseline 3, version 3.2.1 according to updated impact analysis. - Event Trees updated according to the updates in Appendix B	Dag Ribbing
0.3.0 2012-03-14		- Checked against baseline 3, version 3.3.0 according to updated impact analysis (no resulting updates).	Dag Ribbing

		- Various references updated with new version numbers. - Correction of analysis for MMI-6 in hazard H5.	
0.3.1 2012-05-04		- First quantification done in Event Trees - Document generally adapted to quantification - Various textual improvements - INAPP (GPI) consequences updated - Base event DRV INDICATION split in several events - Base event FALSE MODE changed to DRV CHANGE MODE in analysis of MMI-1A - Base event DRV CHANGE MODE added in analysis of MMI-1B - Base event MODE SUPERVISED added in analysis of MMI-2a.1 and MMI-2b - Base event TSR added in analysis of secondary tree DERAIL Document issues to UNISIG, EEIG and ERA for review.	Dag Ribbing
0.3.2 2012-06-21		- Comments from UNISIG companies incorporated - Comments from EEIG and ERA incorporated according to agreement in meeting 2012-06-01	Dag Ribbing
0.3.3 2012-09-21		Additional comments from ERA incorporated	Dag Ribbing

0.3.4 2012-11-23		- Updates agreed in meeting with ERA and EEIG 2012-10-11 - DRV INDICATION WARNING merged with DRV INDICATION - NOT IN SB exchanged for NOT IN SB AT STANDSTILL in DMI-04E L2 - Detailed Results added in Appendix I - Minor editorial clarifications	Dag Ribbing
1.0 2012-12-04		-Transferred to Bombardier template. - Assigned document number EEEA 120007. No other changes.	Dag Ribbing
1.1 2012-12-19		- Updates agreed in meeting with ERA and EEIG 2012-12-06. - Consequence S1 removed. Event trees UBA, OVERSPEED SHT 2 and OVERSPEED (JNC) therefore slightly remodelled.	Dag Ribbing
1.2 2013-01-14		- Verifier comments implemented according to review form EEEA 120009. - Added 'exclusion of GPI' in clause 1.2.1.3. - Note added to Ref 9. - Ref 10 deleted.	Dag Ribbing
1.2.1 2014-02-04		- Transferred to UNISIG template. Updates agreed in meetings within UNISIG RAMS group	Jesús A. Pérez

		on 11/09/2013, 05/11/2013 and 20/11/2013	
1.2.2 2014-02-18	All	General update according to new Event Tree file generated during review. Comments from UNISIG RAMS group meetings added.	Jesús A. Pérez
1.2.3 2014-04-07	All	Update taking into account comments from Siemens, Bombardier and CAF.	Jesús A. Pérez
1.2.4 2014-04-10	All	Editorial comments from Bombardier and CAF.	Jesús A. Pérez
1.2.5 2014-04-16		Editorial comments during RAMS-meeting	Dag Ribbing
1.2.6 2014-05-08	All	Editorial comments agreed by UNISIG RAMS group.	Jesús A. Pérez
1.2.7 2015-06-01	6.8.1.2 7.1.1.2	Updated due to SUBSET 118 – SUBSET 091 Issue document v0.0.3	Martin Vlček
1.2.8 2016-03-03	 6.8.1.2 7.1.1.2	Update due to ERA-OPI-2014-8 Table 4 : DMI-04h → SIL 0 Table 8 : fully updated	Roland Legrain
1.3.0 2016-03-03	No change	Baseline 3 1st maintenance release version as recommended by ERA Technical Opinion ERA/OPI/2014-8	RAMS WP
1.3.1 2016-03-06	All (refer to revision marks) 3.3 3.4 G.2	Update following last discussions on B3R2 and small inconsistency/errors in the document. Update assumption A8; add A15 Update references versions Update constraint 2, add constraint 14	Roland Legrain

1.3.2 2016-04-24	Table 3; 6.5.7.5; 6.5.7.6; Table 4; Table 8; Appendix B; Appendix D; Appendix E; Appendix H	Update according to CR1249	Roland Legrain
1.3.3 2016-06-14	3.3.1.1, 3.4, D.2	Assumption A15 clarification, Update of references, update of MMI-2C event tree.	Martin Vlcek
1.4.0 2016-06-20	No change	Baseline 3 2nd release version	RAMS WP
1.4.1 2019-12-19	3.4	Update reference subset 088 version	ERA
1.5.0 2019-12-20	No change	CCS TSI Application Guide v6 release	ERA
1.5.1 2021-04-13	3.4 5.4.1.1 Table 1 G.2 item 2	Correction of version for [Ref 4] and [Ref 6] Remove of reference to old [Ref 9] S2 : remove of reference S3 : replace [Ref 9] with [Ref 8] Improvement of constraint	RAMS WP
1.5.2 2021-04-13	Cover page	Update with new template	RAMS WP
1.6.0 2021-09-15	No change	Baseline 3 2nd release updated version	RAMS WP

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1 Purpose

3.1.1.1 The goal of this study is to:

Identify hazards associated with the DMI functions that are at the same level as, and independent of, the ETCS Core Hazard ($ETCS_{CH}$), and, taking into account the consequences of the hazards and barriers to their occurrence, to provide quantification of Tolerable Hazard Rate (THR) requirements for these DMI hazards.

3.1.1.2 This report presents a summary of the work undertaken; setting out the methodology applied and results of the analysis.

3.2 Scope

3.2.1.1 The following items are explicitly included/excluded for the study overall:

3.2.1.2 Included:

- ETCS Levels 0, 1 and 2, and permitted transitions including exit to NTC.
- ETCS modes according to level specified above, and transitions between them as defined in the ETCS System Requirements Specification in SUBSET-026 [Ref 1].
- The DMI as the interface between the ETCS On-Board and the Driver.

3.2.1.3 Excluded:

- ETCS Level NTC. This means that input/output defined in SUBSET-026 to be handled in SN mode is excluded from this study, as well as information coming from the STM.
- Errors by railway staff other than users of the DMI e.g. Signaller whilst in degraded operation.
- Ergonomic design and justification of the DMI display.
- Application Data input / configuration of the DMI.
- Errors in operational rules.
- Errors in non-ETCS railway systems.
- National Train Control systems allowing interaction with legacy signalling systems.
- Quantification of the GPI function is excluded because the function is not to be used for safety purposes, see further safety requirement SReq07.

3.2.1.4 The DMI is treated as an interface, with consideration limited to the display of information to the Driver and the entry of data for the ETCS On-Board, as defined in the ETCS DMI document [Ref 6] and SUBSET-026 [Ref 1], as the analysis must be technology

independent to permit any supplier's interoperable ETCS On-Board constituent to be used. A corollary is that even though there is a specification for the ETCS Driver Machine Interface, the ergonomic suitability of the DMI itself is outside the scope of this study.

3.2.1.5 The scope of consideration of consequence severity is limited to passengers. Separate consequence severities are not set for freight trains because the passenger train consequences are deemed to be bounding for freight trains.

3.2.1.6 Fixed text messages are included in this study, since their content is harmonized in the TSI CCS and can therefore be analysed. However, plain text messages are defined freely by the applications themselves and can therefore not be included here. As a consequence, plain 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 (e.g. a written order), so that the recipient's understanding of the message can be verified. This clarification of the scope for the study arose following the identification of hazardous effects that could lead directly to severe consequences. This constraint imposed upon the study results in the need for applications to provide some form of additional support or communication in the use of safety critical plain text messages, and in turn imposes a safety requirement on the application of the DMI functions or ETCS On-Board system. It is defined as Exported Constraint 2.

3.2.1.7 There is no harmonized specification within the scope of the TSI CCS for the communication between the DMI and the ETCS On-Board. This implies the following:

A. The behaviour of the ETCS On-Board in receipt of erroneous data from the driver via DMI cannot be determined. It is likely that corrupted or invalid messages will simply be rejected by the ETCS On-Board, but this cannot be assumed, nor can the response of the ETCS On-Board to the receipt of 'invalid' data. Accordingly, this study can only assess the situation where the DMI provides erroneous data that is still a valid data/message to the ETCS On-Board. The impact of the DMI issuing invalid erroneous data to the ETCS On-Board will need to be addressed by the product suppliers.

B. The role of the DMI equipment in the driver´s input/outputs to the ETCS On-Board is not harmonized. It is likely that for many safety critical functions, a supplier would choose to involve the ETCS On-Board equipment in validation procedures. Examples of such functions are train data entry, train integrity confirmation, track ahead free, override, virtual balise cover etc. Since these ETCS On-Board internal procedures are not harmonized within the scope of the TSI CCS, this analysis imposes requirements on the resulting driver´s input/outputs, i.e. after the procedure is finalized and the validated data is stored in the ETCS On-Board.

3.2.1.8 Recovery from situations where a failure in the DMI has caused ETCS brake intervention depends upon Operational Rules and specific circumstances at the location. Sufficiency of the rules and procedures regarding recovery from such situations is therefore not modelled.

3.3 Assumptions

3.3.1.1 The following assumptions have been made with regard to, or in the course of performing, the functional safety analysis.

A1 The ETCS On-Board system will be compliant with the relevant and current ETCS specifications, notably SUBSET-026 [Ref 1].

A2 Any system interfacing the ETCS On-Board system is assumed to be working correctly. Any function of the ETCS On-Board system except the ones studied here for inputs and outputs are considered to be working correctly.

A3 Intentionally deleted

A4 Erroneous indication of IS mode to a driver will result in the adoption of the Operational Rules for IS mode.

A5 intentionally deleted

A6 intentionally deleted

A7 There is no harmonized requirement within the scope of the TSI CCS to display Service or Emergency brake applications via the DMI unless initiated by the ETCS. However, train braking systems are known to indicate that braking is actually being applied. This assumption is used in the base event CONTROLLED BRAKING, described in Appendix E.

A8 A display to the driver that is obviously incorrect / invalid through the inclusion of garbled text or non valid items (e.g. characters, icons, etc.) will be recognised by the driver and the unit taken out of service at the earliest opportunity. Accordingly, only erroneous but valid data and messages are addressed here.

A9 The impact of invalid erroneous data exchange via the DMI will be addressed by the product suppliers as this is not a harmonized requirement within the scope of the TSI CCS (see clause 3.2.1.7 A above).

A10 Intentionally deleted.

A11 When required to use GPI and none is displayed via the DMI when requested to do so, the driver has a choice of what to do. If the driver reports that no information is available, it is assumed that Operational Rules will ensure safe recovery from the situation.

A12 Intentionally deleted.

A13 Incorrect estimated train speed displayed via the DMI is assumed to have an equal likelihood of being erroneously higher or lower.

A14 Intentionally deleted.

A15 Barriers identified in Appendix B are considered to be applied e.g. text messages linked to safety (for example level crossing not protected) shall be protected by confirmation with a safe reaction (brake application) if not confirmed.

3.4 References

[Ref 1] ERTMS/ETCS, System Requirement Specification, SUBSET-026, issue 3.6.0.

[Ref 2] ERTMS/ETCS, UNISIG Causal Analysis Process, SUBSET-077, issue 3.0.0; UNISIG.

[Ref 3] ERTMS/ETCS, DMI Failure Modes and Effects Analysis (two documents), SUBSET-079, issue 3.14.0; UNISIG.

[Ref 4] ERTMS/ETCS, Safety Analysis (five documents), SUBSET-088, issue 3.7.0; UNISIG.

[Ref 5] ERTMS/ETCS, Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, SUBSET-091; UNISIG.

[Ref 6] ETCS Driver Machine Interface, ERA_ERTMS_015560, issue 3.6.0.

[Ref 7] ERTMS/ETCS Train Interface FIS, SUBSET-034, issue 3.2.0.

[Ref 8] Commission regulation on the adoption of a common safety method on risk evaluation and assessment, EC/402/2013 amended by EC/1136/2015.

3.5 Abbreviations and Glossary

Abbreviation	Definition
ACK	Acknowledge or Acknowledgement
ATP	Automatic Train Protection
CCF	Common Cause Failure
CMF	Common Mode Failure
DMI	Driver Machine Interface
EoA	End of Authority
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ET	Event Tree
ETA	Event Tree Analysis
ETCS	European Train Control System
$ETCH_{CH}$	ETCS Core Hazard

Abbreviation	Definition
FIS	Functional Interface Specification
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GPI	Geographical Position Information
GSM-R	Global System for Mobile Communications - Railways
HAZID	Hazard Identification meeting/activity
HAZOP	Hazard and Operability study
HS	Hazardous Situation
IE	Immediate Effect
INAPP	Inappropriate Authority (for train movement provided)
JRU	Juridical Recording Unit
L0	ETCS Level zero
L1	ETCS Level one
L2	ETCS Level two
LOSS	Loss, or reduced, level of ETCS supervision and protection.
LR Rail	Lloyd's Register Rail Limited (UK or BV)
LSP	Loss of Standstill Protection
LX	Level Crossing
LXI	Level Crossing Incident
MA	Movement Authority
MMI	Man Machine Interface (earlier term for 'DMI')
NTC	National Train Control
N/A	Not Applicable
OUTWITH	Operation outside the control of the signaller and signalling system
OVS	Overspeed
RAC	Risk Acceptance Criteria
RAM	Reliability, Availability and Maintainability
RAP	Roll Away Protection
RBC	Radio Block Centre
SIL	Safety Integrity Level
SPAD	Signal Passed At Danger
SReq	Safety Requirement

Abbreviation	Definition
SRS	System Requirement Specification (SUBSET-026 [Ref 1])
SvL	Supervised Location
THR	Tolerable Hazard Rate
TSR	Temporary Speed Restriction
UBA	Unexpected Brake Application
VBC	Virtual Balise Cover

3.5.1.1 “Erroneous but valid” is used within this report to indicate where an item of data or text is correct with respect to the ETCS specification at the boundary of the ETCS On-Board input/output from/to the driver, but is not the correct value or text that it should be. For example, a displayed train speed of 200 km/h when the actual train speed was 220 km/h would be erroneous but valid. The validity primarily concerns the message containing the data / text as being uncorrupted and whole (complete), and text being correct and complete, it does not extend to whether the message is permitted at that specific time and Level / Mode combination.

3.5.1.2 An ”Erroneous but valid” item of data may therefore still be rejected by the ETCS On-Board, depending upon the nature of the data item and the in-built protection within the ETCS specification, e.g. the acceptance time window for acknowledgements, or product (e.g. setting bounds for valid data values). Similarly, the display to the driver may be valid in that it is a standard display icon or message, but not permitted in the current configuration, through which the driver may identify the fault.

3.5.1.3 “limiting THR”: The limiting THR is that hazard / scenario that places the most onerous requirement on the DMI. For hazard rates (frequencies), the limiting value will be the lowest one as this is the more difficult to provide.

4. SYSTEM UNDER INSPECTION

4.1 Context & Hazard Definition

4.1.1.1 The role of ETCS as it is defined by the ETCS Reference Architecture in the railway environment has been defined [SUBSET-091 [Ref 5] clause 4.2.1.6] as:

> ***To provide the Driver with information to allow him to drive the train safely and to enforce respect of this information, to the extent advised to ETCS***

4.1.1.2 The ETCS Core Hazard for the reference architecture is defined [SUBSET-091 [Ref 5] clause 4.2.1.8] as:

> ***Exceedance of the safe speed or distance as advised to ETCS***

4.1.1.3 In addition, the ETCS Auxiliary hazard is defined in the same clause as:

> ***ETCS interacts erroneously with the driver so that safe train operation NOT supervised by ETCS, is jeopardized***

4.1.1.4 For the purpose of this analysis (3.1.1.1), the ETCS Auxiliary Hazard is used, because it is on the same level as, and independent of, the ETCS Core Hazard, and deals exclusively with the ETCS On-Board input/output on the DMI. The ETCS Auxiliary Hazard is further broken down to the lower-level hazards H1-H5 which are systematically derived and defined in the following chapters.

4.1.1.5 The Reference Architecture is presented schematically in Figure 1 below, along with a delineation of the boundary for this assessment. The figure also maps the DMI hazards H1-H5 (see further Section 6.2) onto the Reference Architecture.

Limit of DMI Safety Analysis:

Note: Interaction with the Driver falls within the study, but their actions are assumed to be correct, and only failures *caused* by the DMI itself are considered.

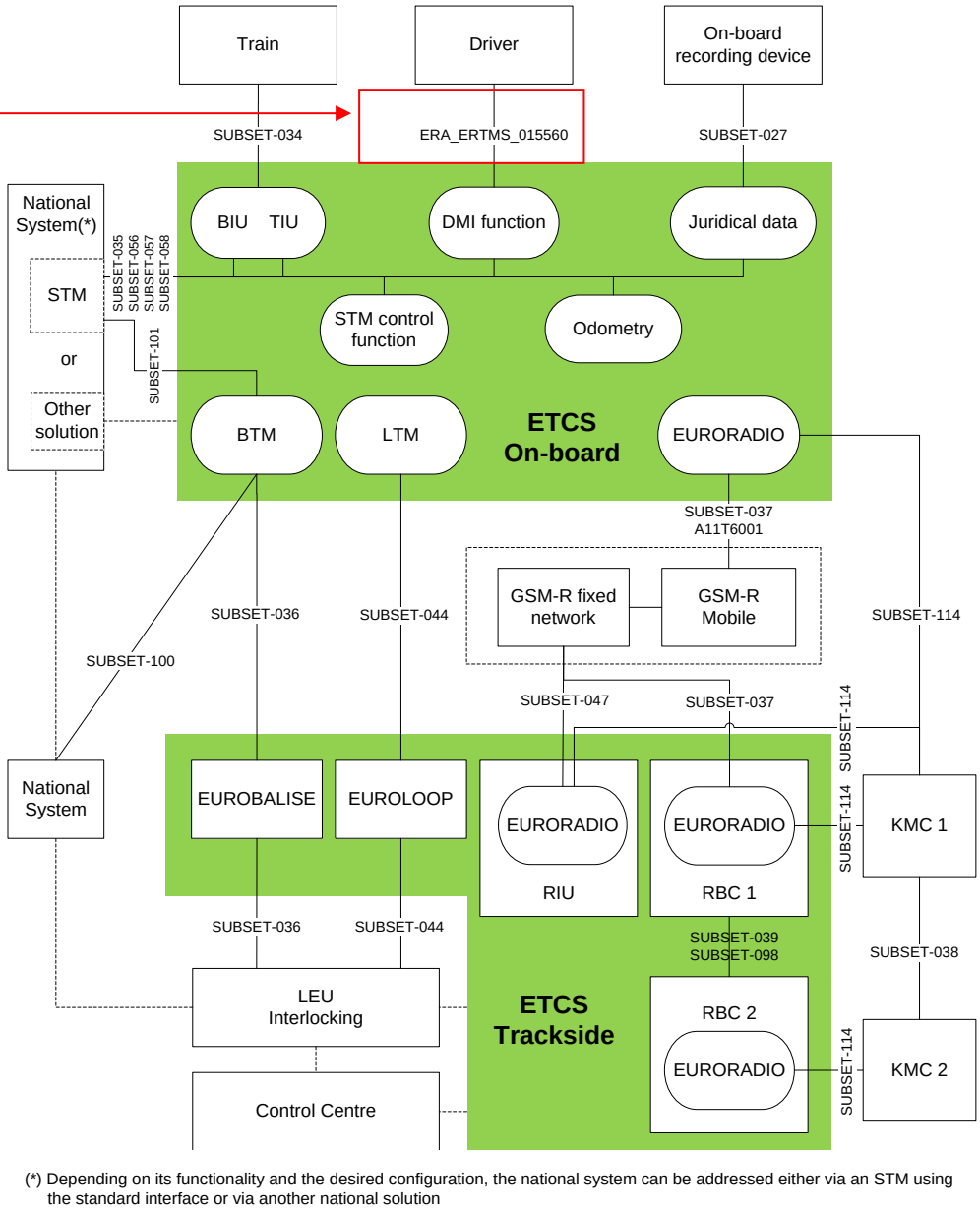


Figure 1 – ERTMS/ETCS system Reference Architecture

4.1.1.6 The DMI top hazards can be divided into inputs to the ETCS On-Board and outputs to the Driver. Figure 2 shows the DMI top hazards allocation:

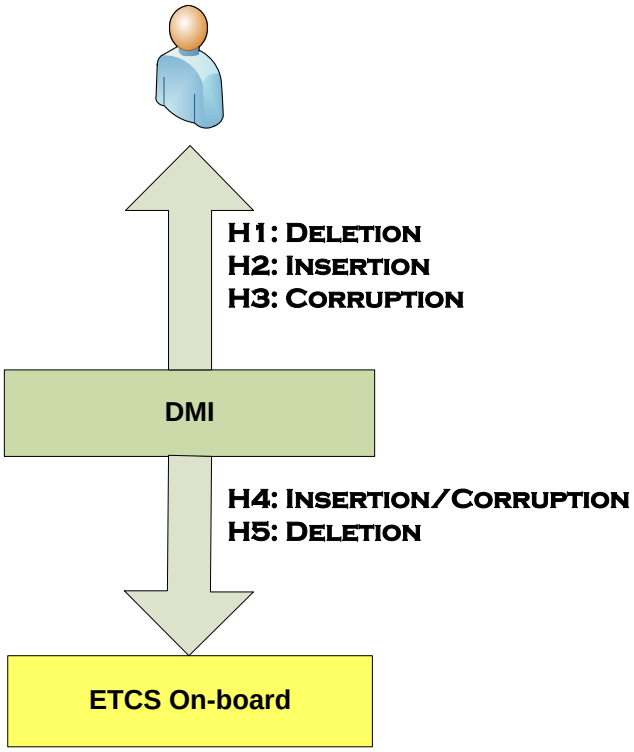


Figure 2 – DMI Top Hazards allocation

4.1.1.7 Apportionment of the THR for the ETCS Core Hazard to the hazard rates of the UNISIG grouping of constituents is undertaken in SUBSET-088 Part 3 [Ref 4].

4.1.1.8 The existing safety analysis of ETCS reported in SUBSET-088 [Ref 4] and -091 [Ref 5] identified subsidiary 'hazardous situations' (HS) associated with the DMI (prefixed with the identity 'MMI-'). Whilst these hazardous situations undoubtedly contribute to the $ETCS_{CH}$, due to the specific definition of the $ETCS_{CH}$, this study has identified that under certain operating Modes their failure can also result in a 'non Core hazard' event, namely one of the 'DMI Hazards' identified as part of this study.

4.2 Operating Modes Assessed

4.2.1.1 All modes according to SUBSET-026 [Ref 1] Chapter 4.7.2 are studied in the current study except for SN mode.

4.2.1.2 Transitions from SL mode were generally addressed under the mode then adopted. When a sleeping engine is awoken following a safety critical fault, the transition to SF and application of the brakes is delayed until the On-Board leaves SL mode, leading to a transition SL → SB → SF according to SUBSET-026 [Ref 1] 4.4.6.1.6. The indication to be displayed to the driver in this situation is therefore the transient status of SB followed by adoption of the SF status indications.

4.3 DMI Functions Assessed

4.3.1.1 The assessment was limited to ETCS functionality in terms of information provided to, or by, the driver, and the required Driver behaviour related to these. SUBSET-026 [Ref 1] defines the ETCS functionality and responsibilities of the system and Driver.

4.3.1.2 The DMI functionality is defined in SUBSET-026 [Ref 1] Chapter 4.7, in terms of the inputs and outputs with the Driver. Internal ETCS On-Board Information exchanged is not explicitly defined, though this can be implicitly identified from the overall ETCS On-Board functioning.

4.3.1.3 The THRs for the DMI hazards are defined on a functional basis. However, the 'functions' defined in SUBSET-026 [Ref 1] Chapter 4.7 are not at the 'same level' as the $ETCS_{CH}$, and therefore a definition of DMI functions at the same level as the $ETCS_{CH}$ is required.

4.3.1.4 At the most basic level the DMI conveys an "Input / Output" between ETCS On-Board and the Driver, providing a mechanism to receive and send information. The DMI is the interface between the Driver and the ETCS On-Board. The core DMI functions are therefore related to this information exchange.

4.3.1.5 The DMI functions reduce to:

- **F1 – Convey information from the ETCS On-Board via the DMI (audio and visual) to the Driver**
- **F2 – Convey information from the Driver via the DMI to the ETCS On-Board**

4.3.1.6 The basis for this is set out in Appendix A as part of the top-level, top-down functional failure analysis, and is summarized in the figure below:

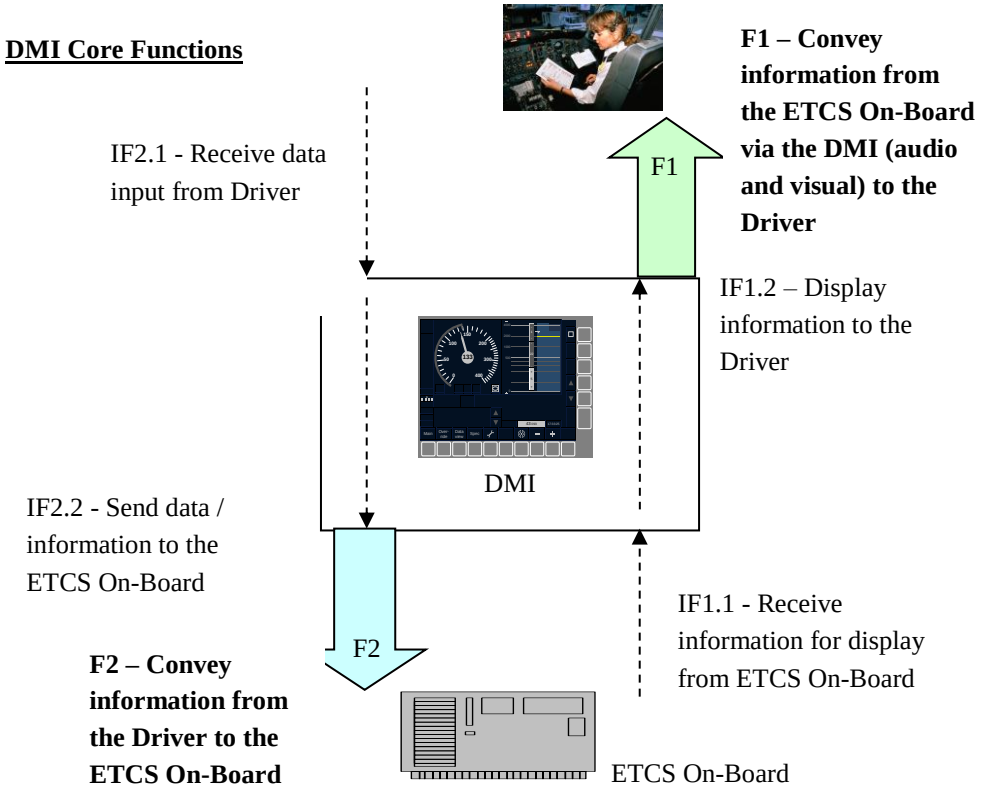


Figure 3 – ETCS DMI 'Core' Functions

4.3.1.7 The reason that failures associated with receiving and transferring data are not separate 'Core DMI' functions (i.e. IF1.1 and IF2.1) is that these do not exist independently, and in practice are causal events of the 'Top Level' DMI functions F1 and F2. These linkages are illustrated in the schematic with the dotted lines, where it is illustrated that IF2.1 and IF2.2 are causal events of F2 while IF1.1 and IF1.2 are causal events of F1.

4.3.1.8 Thus failure to correctly accept or transfer information received from the Driver, can only manifest itself as failure of the DMI to either display the required output to the Driver, or transmit the requisite information to the ETCS On-Board.

5. METHODOLOGY

5.1 Approach

5.1.1.1 The only practicable method of deriving THRs (as opposed to assuming a value and iterating to consider its acceptability) is to work back from the end risk by developing "Consequence – Loss" models back to initial error that is supposed to receive the THR. Such models are then open to review and modification regarding the quantitative values to be applied once the logic of the model is accepted.

5.1.1.2 "Consequence – Loss" models are most effectively described through Event Tree Analysis (ETA), especially when there is a range of possible outcomes/consequences.

5.1.1.3 This study therefore focuses on developing the ETAs to connect the Hazardous Situations via barriers for each scenario to the end Consequence.

5.2 Work Flow

5.2.1.1 As a foundation for further work, the present report was first produced by LR Rail for baseline 2, version 2.3.0d. The overall approach used is summarised in the schematic below, even if minor variations were done during the course of the work. The "Final Report" denoted as D4 in Figure 4 below refers then to the final report from LR Rail.

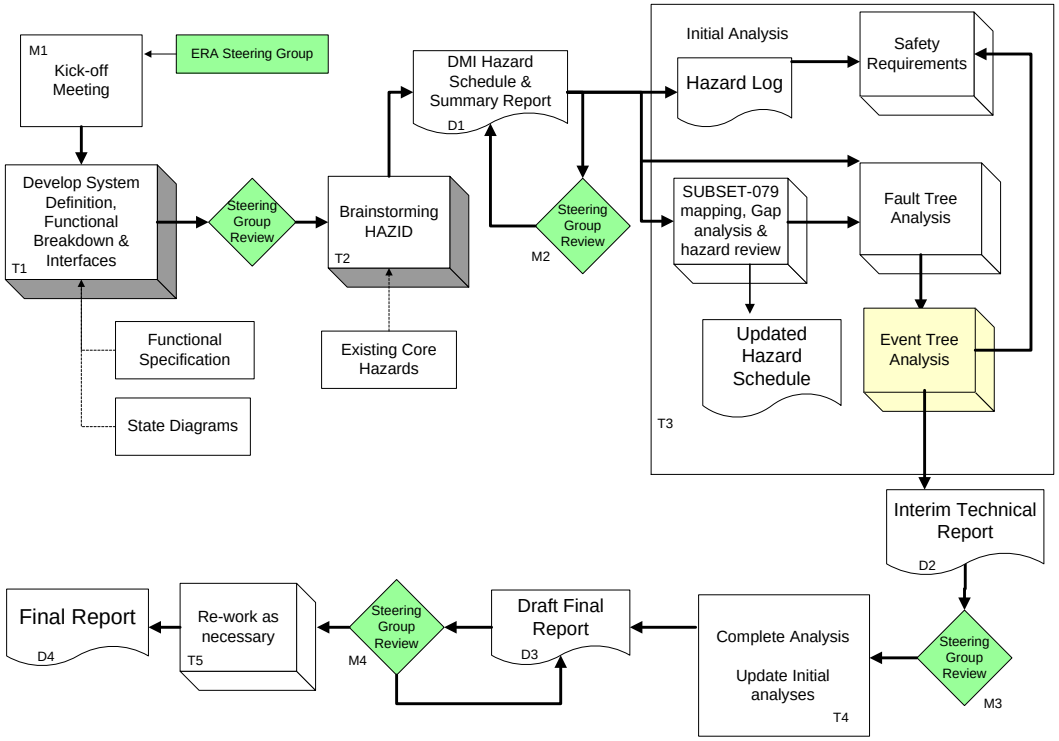


Figure 4 – Study Methodology

5.2.1.2 An update of LR Rail's report was then made by Bombardier to comply with baseline 3. The methodology was to first assess the impact on the LR Rail's report from the Change Requests inside this ETCS version. The updates concluded necessary were then incorporated in the present report. No other changes to the scope and assumptions were made. After UNISIG RAMS group review, several changes were agreed. UNISIG has performed the document updating which mainly affect to the cut sets and correct several mistakes. Main conclusions remain unchanged.

5.2.1.3 Subsequent to the update for baseline 3, quantifications of the event trees were carried out, as described in the following chapters.

5.3 System Boundary, Hazards and THRs

5.3.1.1 As noted above, hazards only reside at the boundary of a system or product. For this study, the boundary is that of the Driver´s inputs/outputs to/from the ETCS On-Board system. Part of this boundary is also part of the external ETCS On-Board system boundary.

5.3.1.2 Given the coincident boundary and the nature of the $ETCS_{CH}$, some of the failures of the driver´s inputs/outputs will result in the $ETCS_{CH}$ (and are therefore not within the scope of this study), whilst conversely, failures in the ETCS On-Board system may lead to the identified DMI hazards H1-H5.

5.3.1.3 This is illustrated in Figure 5 below, where ETCS On-Board functions have a potential of being associated with both the ETCS Core Hazard and the DMI hazards.

5.3.1.4 THRs are assigned at a functional level but may be composed of a series of contributions from different system functions, of which the DMI is but one element (e.g. an output displays the current speed to the driver, but the data to be displayed comes from the ETCS On-Board).

5.3.1.5 For the existing consideration of the $ETCS_{CH}$ within the scope of the CCS TSI, no apportionment has been made between the overall THR and the functions of the ETCS On-Board which may cause it. Separate THRs for the different elements which compose the ETCS On-Board (e.g. ODO, BTM etc.) have not been developed with regard to the ETCS Core Hazard, but are encompassed within the overall $ETCS_{CH}$ THR.

5.3.1.6 Intentionally deleted.

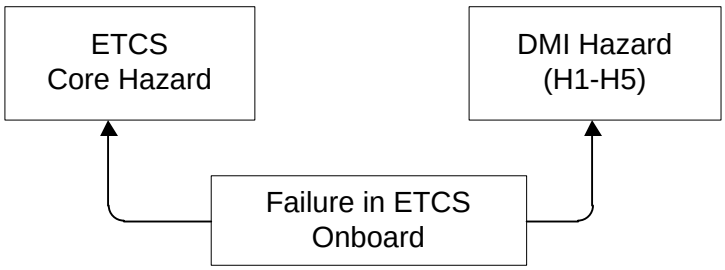


Figure 5 – Functions and Hazards. ETCS On-Board functions have a potential of being associated with both the ETCS Core Hazard and DMI Hazard.

5.3.1.7 Intentionally deleted.

5.3.1.8 Intentionally deleted.

5.3.1.9 As noted above, there may be a number of hazards that can arise associated with a single function, and a number of 'hazardous situations' that give rise to each Hazard. The $ETCS_{CH}$ relates to the single (principal) ETCS Core function, for which the DMI-related Hazardous Situations[1] where identified and modelled along with contributions

[1] Hazardous Situations are not true causal events, being more akin to failure modes, though they are the limit used in the SUBSET-088 FTA analysis, as true causal events cannot be identified because the technology and internal workings of the ETCS On-Board system is not mandated for interoperability.

from other ETCS On-Board system in SUBSET-088 [Ref 4]. These $ETCS_{CH}$ DMI Hazardous Situations are presented in Appendix E.

5.3.1.10 The DMI related Hazardous Situations associated with the $ETCS_{CH}$ are identified with a prefix “MMI-“. It is possible that the same failure mode could result in a non-Core Hazard effect in a particular ETCS Level and Mode combination. To cater for such situations the “MMI” failure identities are retained in this analysis to differentiate them from failures that only result in non-Core hazards which are prefixed “DMI”. Appendix F provides a list of the “MMI“-events and an explanation how the event is covered in this DMI study in case the event id is not directly used here.

5.3.1.11 As an example, MMI-2a.1 in SUBSET-088 [Ref 4] is “False presentation of train speed”. If the speed or distance limit is not advised to ETCS then it is not part of the $ETCS_{CH}$. Thus, any limit that the Driver is responsible for achieving, based on their understanding of train speed (mostly Level 0 limits, but some Level 1 / Level 2, e.g. stopping short of another rail vehicle in OS mode or stopping in a platform), would be non-Core. MMI-2a.1 can therefore result in an ETCS Core Hazard and also a non-Core hazard.

5.3.1.12 Hazardous Events associated with the $ETCS_{CH}$ cover MMI-1 to MMI-6, along with a further division in a, b, c sub-elements. The ‘additional’ DMI hazards derived in this study use the Hazard identity as a first identifier, followed by an a, b, c delineation similar to that used for the MMI failures. Thus, the DMI Hazardous Situation name is immediately identifiable to the hazard which it falls within; e.g. DMI-03a is the first Hazardous Situation associated with Hazard H3.

5.3.1.13 The linkage between Functions, Hazards and Hazardous Situations can also be seen as a pyramidal structure, in the sense that the Hazardous Situations at the bottom of the pyramid are generalised into a smaller set of Hazards, which in its turn is generalized into the failure of the very few top-level Functions.

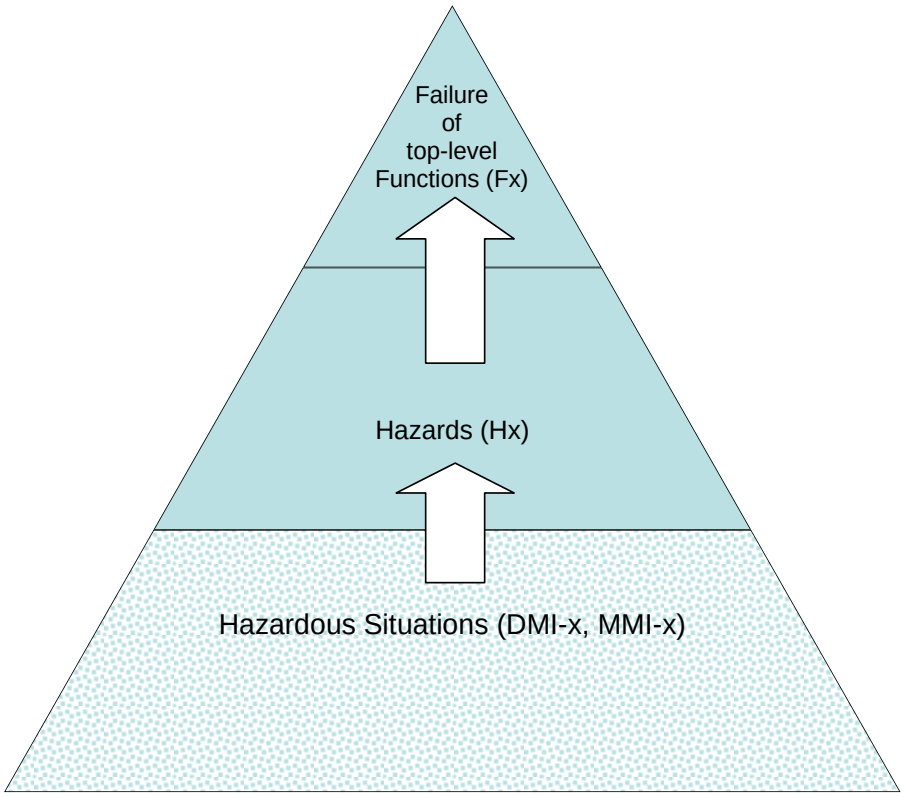


Figure 6 – Pyramidal Relationship of Functions, Hazards and Causes

5.3.1.14 Whilst there is a range of Hazardous Situations identified under each Hazard, the generic nature of the Hazards is such that the Hazardous Situations are specific variations of the generic failure mode connected to a Hazard. For example, the Hazard can be that the output to the driver is corrupted, while the corresponding Hazardous Situations can be that the speed indication is corrupted, the mode indication is corrupted, etc.

5.3.1.15 The Hazardous Situation must develop further in many instances in order for harm to occur, and the intermediate states between initial failure and harm may be the same for a number of different Hazardous Situations. The intermediate states are referred to in this analysis as the “Immediate Effect” of the Hazardous Situation. For example, the displaying of an incorrect train speed on the DMI does not itself cause immediate harm, but could result in the train running at a higher speed than intended (referred to herein

as ‘Overspeed’ [OVS]), which could cause harm. The Overspeed is an Immediate Effect[2] that can arise from other Hazardous Situations.

5.3.1.16 The Event Tree models contain the quantification of the top-level functional THRs. The Hazard Schedule and ETA models in Appendix B and Appendix D respectively illustrate the Immediate Effects along with the barriers/shaping factors that can prevent the Immediate Effect occurring, and mitigation and controls that can limit the potential harm.

[2] Accepted that Overspeed may not be “immediate” but the term is used as an impact / state that potentially leads to harm.

5.4 Hazard Consequence and Likelihood

5.4.1.1 Risk acceptance criteria (RAC) for different consequences (single/multiple injury/fatality) have been set in the currently applicable Common Safety Methods for Risk Assessment, [Ref 8]. See Table 1 below. These RAC are used here by assigning each Event Tree to one of the consequences below and then applying the corresponding RAC as acceptance criteria for this analysis. To simplify the Event Trees each of these categories has been given an ID in the range S2 to S4 as indicated in Table 1 below.

5.4.1.2 Failure modes that result in end effects that are not safety related, i.e. those that do not put the passenger at risk, present no hazard, but could degrade the Reliability, Availability or Maintainability (RAM) of the Driver´s inputs/outputs, resulting in delays and service impact. Degraded reliability and availability may lead to operation of the train in a degraded mode, with increased driver's responsibility, which can indirectly impact the safety. This indirect impact is not considered in this study.

ID	Severity Level	Consequence to Passenger	Risk Acceptance Criteria (/h)	Reference for RAC
S2	Marginal	One or more light injuries	10^{-5}	
S3	Critical	Single fatality and/or single serious injury	10^{-7}	[Ref 8]
S4	Catastrophic	Fatalities and/or serious injuries[3]	10^{-9}	[Ref 8]

Table 1 – Risk Acceptance Criteria (RAC)

[3] The consequence “major damages to the environment” has not been explicitly considered here.

5.5 Quantification of Hazardous Events

5.5.1.1 In the event trees, each scenario is started off with a DMI Hazardous Situation (DMI-xx/MMI-xx).

5.5.1.2 Initially the analysis assumed a frequency of one failure per hour for all DMI Hazardous Situation (DMI-xx/MMI-xx). Having determined the highest risk outcome for a frequency of one per hour, the limiting THR was derived by adjusting the frequency until an acceptable (tolerable) worst-case individual risk is achieved. In practical terms, this is simply the ratio between the risk derived with a frequency of one, and the corresponding RAC.

5.5.1.3 For example, if the worst-case risk of a certain outcome of a DMI hazard at a frequency of one per hour was 1E-06 per hour, and the corresponding RAC set at 1E-09 per hour, then the limiting THR would become 1E-03 per hour. This procedure was carried out for each of the hazards in the event tree, one by one.

5.5.1.4 All Hazardous Situations have been modelled in the ETA, and all trees have been quantified. However, the risks have not been summed, since such an approach would derive a highly pessimistic THR. The reason is that many different scenarios in which Hazardous Situations develop into its Consequences are really only different formulations of the same scenario, and shall therefore not be represented by independent probabilities. Therefore, as initial approach, a limiting THR is here derived by selecting the highest risk sequence.

5.5.1.5 In practical analysis terms, this means that it is made sure that all individual Cut-Sets[4] are below the RAC for the corresponding Consequence, but the sum of all Cut-Sets for a Consequence is allowed to exceed the RAC.

5.5.1.6 However, since there exist also scenarios which are indeed truly independent and should therefore be represented by independent probabilities, this method introduces a non-conservative error. This error is treated by an uncertainty factor in 6.9.3.1.

[4] The concept of Cut-Sets is not explained further here, but can be studied in the FaultTree+ manual or general literature on numerical safety analysis.

5.6 Quantification of Failures in Driver Actions

5.6.1.1 It is not believed possible to determine the probabilities of failures in driver actions with any high accuracy. However, it is still necessary to have some general rules in order to achieve the correct priority between the different scenarios. Therefore Table 2 was developed. The assignments of probabilities in the different scenarios have been extensively reviewed during the course of this work.

Category	Probability of action failure	Driver action
A	p=1.0E-03	The driver performs an action in a non-complex situation which is covered by training and procedures.
B	p=0.01	The driver recognises that ETCS is behaving in a way that is clearly contrary to their expectations. To fall into this category, the contradiction must be obvious. OR The driver manages to operate the train safely, although a certain degree of ETCS support which is normally present, has failed. To fall into this category, the reliance on the failed ETCS support must be fairly low.
C	p=0.1	The driver recognises that ETCS is behaving in a way that is contrary to their expectations. The contradiction is not obvious as in category B, but still clear to a driver who is paying normal attention. OR The driver manages to operate the train safely, although a certain degree of ETCS support which is normally present, has failed. To fall into this category, the reliance on the failed ETCS support is higher than in category B.
D	p=0.2 – 0.9	The driver performs an action in a more or less complex / pressing situation which is not covered by training or procedures.

Table 2 – Probability of Failure in Driver Action

6. SAFETY ANALYSES AND RESULTS

6.1 Hazard Identification

6.1.1.1 A number of hazard identification activities have been undertaken, both previously and reported in ETCS 'SUBSET' reports, and as part of this DMI study. The studies include an FMEA of the Driver´s inputs and outputs via DMI for ETCS Level 1 and Level 2 operation reported in SUBSET-079 [Ref 3], and a 'HAZID' workshop looking similarly at operation in ETCS Level 0 as part of this study. This HAZID study isn't specifically referenced, but the relevant conclusions are instead incorporated in the present document.

6.1.1.2 From these studies a DMI Hazard Schedule was derived. A number of assurance activities were also undertaken to confirm the content of the hazard schedule, and to ensure its completeness. The hazard identification and assurance activities are summarised in Figure 7 and discussed in the following text:

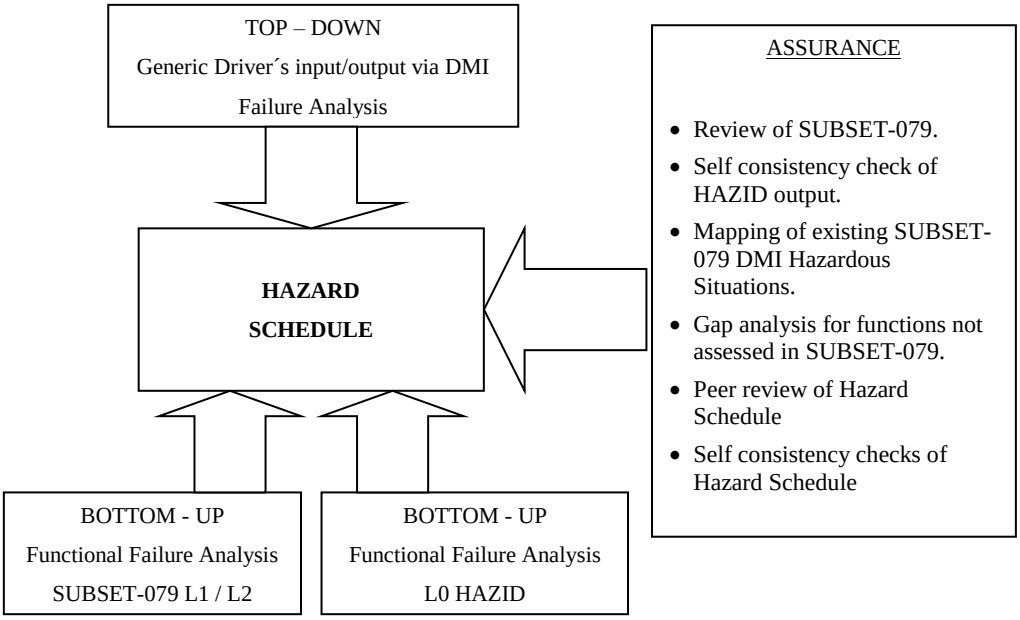


Figure 7 – Hazard Identification and Assurance

6.1.1.3 The initial Hazard Schedule was peer reviewed, looking in particular for self-consistency such that "complementary" hazardous situations were identified. For example, if there is a Hazardous Situation associated with failure to display information to a driver, is there an equivalent Hazardous Situation where there is a failure in transmitting the associated reply from the Driver to the ETCS On-Board? The content of the Hazard Schedule was also reviewed during the development of the Event Trees and in further internal reviews and workshops within this study.

6.1.1.4 A similar self-consistency review was undertaken for the HAZID.

6.1.1.5 The Hazard Schedule assurance activities included an analysis of the HAZID study to identify potential areas where the HAZID table did explicitly cover a DMI activity or keyword (e.g. Absent, Incorrect). This review was undertaken by a competent person who did not attend the HAZID to provide independence.

6.1.1.6 In many cases it was found that the HAZID had considered the various situations, even if these were not explicitly identifiable during the safety analysis, while in a small number of situations some additional occurrences were made explicit; e.g. no new Hazards were found but a second, complementary Hazardous Situation was formalised.

6.1.1.7 The Hazard Schedule is considered robust and complete as far as the top-level DMI hazard identification (Hazards H1 to H5 – see Section 6.2 below) is concerned.

6.2 Hazard Schedule

6.2.1.1 The Functions, hazards, associated Hazardous Situations and their IEs are summarised in the 'Hazard Schedule', reported in full in Appendix B, along with explanations of the impacts and associated notes and comments for context.

6.2.1.2 The Hazard Schedule is too extensive to summarise fully in the main body of the report. Table 3 below provides a full summary of the top level (generic) DMI hazards and associated Hazardous Situations. An Event Tree has been developed for each Hazardous Situation showing the Barriers / Shaping Factors associated with the development to an Immediate Effect.

6.2.1.3 In the hazard schedule, the Top-Level DMI Hazards use the term "DMI". As anywhere throughout this document, this shall be understood as the "Interface between the ETCS On-Board and the driver", as on this black-box level, no notion of any DMI equipment exists.

6.2.1.4 When "potentially direct catastrophic" is noted in the Immediate Effect column, it means that there is no transfer to an IE in a secondary event tree, but the catastrophic consequence S4 is assigned directly in the primary fault tree.

Func-tion	Top-Level DMI Hazard	Hazardous Situation	Potential Impact (IE) (see Appendix B for scenario development)
F1	**H1** Information NOT displayed when it should have been	**DMI-01a** Failure to provide Warning indication	**UBA**: Unexpected Brake Application
		DMI-01b Valid ETCS On-Board output via DMI obscured by erroneous output (audio or visual)	**OVS:** Overspeed **UBA**

Func-tion	Top-Level DMI Hazard	Hazardous Situation		Potential Impact (IE) (see Appendix B for scenario development)
		DMI-01c	Failure to display request for acknowledgement	**UBA**
		DMI-01d	Failure to display Geographical Position data	As DMI-03a in H3.
		MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	**DISTRACTION** (of driver) – shaping factor on other failures and simply one of numerous factors which could distract a driver whilst driving. **LOSS:** Loss of or reduced supervision and protection
		DMI-01f	Failure to display ACK for RV request	Potentially directly catastrophic if the need for RV mode was in an Emergency situation.
		DMI-01g	Failure to display Air Tightness Control	Potentially directly Marginal or Catastrophic, depending on scenario
		MMI-2i	Failure to present “LX not protected” information	**LOSS**
		DMI-01h	Failure to present Display Distance to Target information	Variant of **OVS.**
		DMI-01i	Failure to present Time To Indication information	Variant of **OVS.**
	H2	**DMI-02a**	False presentation of Warning	**DISTRACTION** Bounded by **UBA**

Func-tion	Top-Level DMI Hazard	Hazardous Situation		Potential Impact (IE) (see Appendix B for scenario development)
	Information displayed when it SHOULD NOT have been. *This includes "Spurious output distracts train Driver" and 'stale' data being retained.*	**DMI-02b**	False presentation of IS mode (shown as IS mode when not)	**DISTRACTION** Bounded by **UBA**
		DMI-02c	False presentation of brake indication	**DISTRACTION** Bounded by **UBA**
		MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	**UBA**
		DMI-02e	Spurious notification of Train Data change (which normally is from source different from the driver)	**DISTRACTION**
		MMI-2c	False presentation of track adhesion factor (shown as applied when not)	Variant of **OVS**.
		DMI-02g	False presentation of "LX not protected"	**DISTRACTION** Bounded by **UBA**
	H3 Erroneous but valid information displayed	**DMI-03a**	Incorrect Geographical Position data displayed	**OVS**: (Overspeed in specific circumstance at a speed restriction) and, Inappropriate Authority **(INAPP)** given to driver.
		MMI-2a.1	False presentation of train speed	**OVS**
		MMI-2b	False presentation of mode	**LOSS** **DISTRACTION**

Func-tion	Top-Level DMI Hazard	Hazardous Situation		Potential Impact (IE) (see Appendix B for scenario development)
		DMI-03c	Wrong acknowledgement request displayed	Cause of other Hazardous Situations identified separately (e.g. DMI-04d, MMI-1a) so not modelled in its own ET.
		DMI-03d	Wrong Trip Reason displayed	**OVS**
		DMI-03e	Wrong fixed text message displayed	Potentially directly catastrophic
		DMI-03f	"Tunnel stopping area" displayed at the wrong geographical place	Potentially directly catastrophic if the need for evacuation was in an Emergency situation.
		DMI-03g	Wrong Display Distance to Target information	Variant of **OVS.**
		DMI-03h	Wrong Time To Indication information	Variant of **OVS.**
F2	**H4** Erroneous but valid input to the ETCS On-Board via DMI	**DMI-04a**	False command to exit shunting	Bounded by **UBA** **DISTRACTION**
		DMI-04c	False START command	**LSP**: Unexpected loss of standstill protection
		DMI-04d	False UN acknowledgement	**LSP** – as DMI-04c (only applicable in Level 0)
		MMI-1g	False request for SH Mode	**LSP** **UBA** **LOSS** **OUTWITH**: Operation outside the control of the signaller and signalling system

Func-tion	Top-Level DMI Hazard	Hazardous Situation		Potential Impact (IE) (see Appendix B for scenario development)
		DMI-04f	Spurious or wrong language requested distracting the train Driver	**DISTRACTION** Not a specific risk in itself, but a performance shaping factor of the other scenarios already covered.
		DMI-04g	Spurious request to change to another ETCS Level	**DISTRACTION** **LOSS**
		DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	**DISTRACTION** **UBA** Potentially directly catastrophic if train on a gradient and ACK occurs repeatedly.
		DMI-04j	False Isolation command	**LOSS**
		MMI-1a	False acknowledgement of mode change to less restrictive mode	**LOSS**
		MMI-1b	False Command to enter NL mode	**LOSS** **OUTWITH**
		MMI-1d	False acknowledgement of Level Transition	**LOSS**
		MMI-6	Falsification[5] of Virtual Balise Cover (failure modes insertion or corruption)	**LOSS**

[5] This refers to the failure that an erroneous VBC is stored in the ETCS On-Board. As noted in clause 3.2.1.7, there is currently no harmonized specification within the scope of the TSI CCS for the process and role of the DMI in confirming VBC input, and accordingly it is not possible to define the failure on a more detailed level. However, MMI-6 can be further developed in a product specific fault tree to obtain a less demanding tolerable hazard rate for an individual DMI failure.

Func-tion	Top-Level DMI Hazard	Hazardous Situation		Potential Impact (IE) (see Appendix B for scenario development)
	H5 Deleted input to the ETCS On-Board via DMI	**DMI-05a**	Deleted Level transition acknowledgement	Bounded by **UBA**
		DMI-05b	Deleted acknowledgement	**UBA**
		DMI-05c	Deleted request for GPI	As DMI-01d
		DMI-05d	Deleted change of language request	As DMI-04f
		DMI-05e	Deleted driver request to apply Track Adhesion Factor	Similar to MMI-2c.
		DMI-05f	Deleted Reversing mode acknowledgement	**DISTRACTION** Potentially directly catastrophic if the need for RV mode was in an Emergency situation.
		DMI-05g	Deleted “PT distance exceeded” acknow-ledgement	Not a specific risk in itself, train remains at standstill with brakes applied.
		DMI-05i	Deleted “reversing distance exceeded” acknowledgement	Not a specific risk in itself, train remains at standstill with brakes applied.
		DMI-05j	Deleted Isolation command	As DMI-01f
		DMI-05l	Deleted Train Trip acknowledgement	Not a specific risk in itself, train remains at standstill with brakes applied.
		MMI-6	Falsification of Virtual Balise Cover (failure mode deletion)	**LOSS** (Similar to MMI-6 failure mode corruption)

Table 3 – Summary of Hazard Schedule

6.2.1.5 The spuriously request of removing ‘Track Adhesion Factor’ was considered in the analysis, but is considered to be a cause of the $ETCS_{CH}$ analysed in SUBSET-091 [Ref 5], and not a new hazard (as the failure erroneously changes the supervision and protection “advised to the ETCS” internally with within the ETCS On-Board system).

6.2.1.6 Conceptually, there could be three hazards under F2, as the equivalent failure modes to the three hazards under F1. However, unlike a Driver, the ETCS On-Board makes no distinction between ‘spurious’ or ‘incorrect’ information provided to it – it is just information. As the ETCS On-Board simply acts upon the information it receives, these two failure modes are combined for simplicity as Hazard H4.

6.2.1.7 The more detailed Hazard Schedule in Appendix B also details if the Hazardous Situation leads directly to the Immediate Effect or if further barriers or probability shaping functions exist to prevent the harmful situation arising. The Hazard Schedule in Appendix B also summarises barriers and mitigations to reduce the possible consequences of the harmful situations.

6.2.1.8 The hazard identification activities have been primarily based upon the assessment of single DMI failures followed by their development into harm causing events. Generally, no specific account has been taken of multiple DMI failures. In the majority of cases it is likely that any further failure in DMI would be independent of the first failure as the nature of the two differ e.g. one is a false command whilst the other a false display. In addition, for a second or dependent DMI failure to be of concern, it would also need to be credible, or exactly mask the nature of the first failure, both unlikely from hardware failure modes[6].

6.2.1.9 Regarding the potential for multiple combined DMI failures, one scenario of potential concern would be where ETCS On-Board receives a false (spurious) request, and then the confirmation request issued by the ETCS On-Board is spuriously acknowledged. However, as the issuing of false requests and false acknowledgement are already addressed as separate events, the combination of false request AND false acknowledgment will generally be bounded by the modelling of each individual failure.

6.2.1.10 The review identified only one situation where a further failure of the DMI may subvert the protection[7]. This arises in DMI-04c, falsely requesting Start command to the ETCS On-Board, where the subsequent acknowledgment (which is a pre-requisite for DMI-04c to develop into a hazardous scenario) could also arise from a second DMI failure. Event AUTO ACK has been updated to reflect this.

6.2.1.11 The linkage of the top level functions and hazards are illustrated graphically in the Fault Trees in Appendix C.

[6] Software failures could be potentially more onerous but are not normally quantified. Software integrity will need to be commensurate with any SIL assigned to the DMI.

[7] False request and acknowledgment of NL mode would be an issue, but the false request is a Core hazard covered through MMI-1b.

6.3 Functional Safety Analysis

6.3.1.1 The scope of this study is defined assuming the correct functioning of any interfacing functions, and therefore the impact of the hazardous situation and the external response to it is known. Accordingly, in developing the Hazard Schedule and undertaking safety analysis of the DMI, any response of the of the ETCS On-Board, and any other train system, to a fault arising within the Driver´s input/outputs via DMI, is assumed to occur according to specification. For example, if there is a failure to send the Level Transition Acknowledgement to the ETCS On-Board within the stated time frame (5 seconds after ETCS On-Board transmits the request to the driver), then the ETCS On-Board will intervene.

6.3.1.2 This approach differs from that underpinning the FMEA reported in SUBSET-079 [Ref 3] where no credit was taken for any internal or external mitigation when assigning the potential consequences of a DMI failure (although also internal and external mitigations are listed in SUBSET-079).

6.3.1.3 Event Tree Analysis (ETA) has been undertaken to examine and model the consequences and accident development. Two types of Event Trees (ETs) are present in the ETA model:

- ‘Primary’ ETs reflect initiating events and cannot be transferred to from other ETs. Each Hazardous Situation is reflected by one of the Primary ETs. As initiating event for each Primary ET, the corresponding DMI Hazardous Situation (DMI-xx/MMI-xx) is used.
- ‘Secondary’ ETs model the development of the Immediate Effects, addressing the potential mitigation and controls that act to prevent or reduce harmful consequences. Secondary ETs receive transfers from one or more Primary ET.

6.3.1.4 Note that every entry in Table 3 above does not have a dedicated / unique Event Tree model, since some identical effect failures could be combined in one model.

6.3.1.5 Of the seven Immediate Effects summarised in Table 3, all were modelled as Secondary Event Trees with the exception of DISTRACTION. Distraction of a driver can occur due to many other reasons, including equipment failures within the train cab, external activities at the trackside and stimuli of the driver (e.g. fatigue, hunger). It is also not practicable to model herein the myriad of different situations in which a distraction could occur and the response of the driver in each context.

6.3.1.6 Thus, DISTRACTION has not been a part of the quantification of the Event Trees.

6.3.1.7 The Event Trees are presented in Appendix D. The ETA uses ‘Events’ to describe the alternative developments of the accident scenarios and to condition these by the effectiveness of the barrier or likelihood of the condition occurring. A description of each event and the rationale behind the activities or moderating action are set out in Appendix E.

6.3.1.8 The development of the Event Tree is undertaken considering what may then occur during the subsequent train service. As such, it is route based and takes into account the sort of situations which could occur. Not all situations may occur in every constituent country, but those included are considered reasonably credible, since the DMI THRs should cater for the most onerous situations that could occur.

6.3.1.9 The Event Trees have been constructed to show the logic of the potential accident sequence. Some of the events in the Event Tree relate to a driver recognising the DMI fault from the nature of the information displayed, or lack of it, or from the route information or direct observation (e.g. train has not stopped at the required platform marker). As the events relate to a driver's response, this takes a finite time, which will vary due to the nature of the specific failure and the particular circumstances.

6.3.1.10 In such instances, the Immediate Effect or potential for harm technically exists on the 'Success' leg of the event tree for this response period, and applies whether the event was modelled as part of the Primary Event Tree (Hazardous Situation) or Secondary Event Tree (Immediate Effect).

6.3.1.11 Due to the variety of different transfers to each Immediate Effect [event tree], this modelling has been included in the Primary Event Trees as it better shows the logic of the failure scenario, and makes the Immediate Effect 'Secondary' Event Tree generic, as the likelihood of the driver revealing the fault may be not be the same for all hazardous Situations. In many instances, the response from the driver being considered is within a relatively short time frame from the fault occurring. A more explicit consideration of the timeframe is done in some cases, but has not been found generally useful, since the probabilities for driver actions are anyway not that exact of a science.

6.3.1.12 Definitive modelling of all possible outcomes and variants is not practical for the DMI hazards. Whilst the high level impact is relatively easy to discern, the downstream effect of this is myriad, being dependent on numerous possible factors such as:

- Specifics of the route (line speed, gauge, station stops and lineside features),
- Timing of the failure,
- Current state of the railway (e.g. what temporary speed restrictions are in place, any existing asset failures in the area),
- National application rules,
- Driver experience and driving style,

6.3.1.13 Accordingly, the 'Consequence – Loss' models in the Event Trees have been limited to a basic simple approach, believed to bound the variety of possible situations.

6.4 DMI Hazard Safety Requirements

6.4.1.1 Safety Requirements have been developed as part of completing the Hazard Schedule and creating the incident Event Trees. The DMI top-level hazards and supporting safety requirements are summarised in Appendix G.1, which also acts as a hazard log.

6.5 Discussion

6.5.1 General

6.5.1.1 The complex nature of interaction between a driver, their inputs/outputs with the ETCS On-Board via DMI and variety of situations potentially encountered during railway operation is such that there will often be vigorous debate and different views regarding the likelihood of actions and events. Already at a stage when the Event Trees were not quantified, the failure modes and their development to accident consequences were reviewed objectively, considering only their validity as potential occurrences (even if these are possible but highly unlikely). Once the logic of the analysis was accepted, the subsequent discussion concerning the event data quantification was able to start from an accepted understanding of failures in the Driver´s inputs/outputs to ETCS On-Board via DMI and their impact.

6.5.1.2 The models therefore provide a consistent framework as a generic representation of both the failures in the Driver´s inputs/outputs to ETCS On-Board via DMI and the impact on the operational railway of various generic hazardous impacts (the Immediate Effects).

6.5.1.3 There are no failures in the Driver´s inputs/outputs to ETCS On-Board via DMI that lead directly to critical and catastrophic consequences without there being present some form of ‘barrier’ or mitigation, even if these only reflect determining the likelihood of circumstances within which the DMI failure leads to a hazard.

6.5.1.4 A summary of the principal findings or considerations for each Immediate Effect arising from non-Core Hazard failures are discussed in turn below. The discussion, and report as a whole, needs to be read in conjunction with the more detailed descriptions and rationale presented in Appendices B to D.

6.5.2 Event Trees without intermediate ‘Immediate Effect’ states

6.5.2.1 Some Event Trees do not transfer to an intermediate ‘Immediate Effect’ state – DMI-01f, DMI-01g, DMI-03f, DMI-04h, DMI-05f, and DMI-05j.

6.5.2.2 DMI-04h principally reflects an unlikely situation where a repeated DMI failure could defeat the ETCS standstill, rollaway or reverse movement protection. In addition to requiring multiple (or Common Cause / Common Mode – see clause 6.5.9.6) failures of the DMI functions, unless a driver were incapacitated in some manner or not present on the train, it is highly unlikely that the train would move sufficient distance for an accident to occur.

6.5.2.3 DMI-01f, DMI-01g, and DMI-05f are potentially very onerous in that little time may be available for a Driver to realise that a DMI failure has occurred and to respond to prevent harm occurring. In the case of DMI-01f and DMI-05f, RV mode is intended for use in emergency situations, and thus a driver may not be able to respond in time if the ACK request from the ETCS On-Board is not displayed or the ACK response not sent to the ETCS On-Board and ETCS intervenes. The hazardous frequency of the consequence of this event could therefore simply be the probability of this specific DMI failure occurring in conjunction with need for RV in an Emergency situation, with no mitigation or barrier available. DMI-05j represent a similar situation where reversing is needed for an emergency situation.

6.5.2.4 Intentionally deleted.

6.5.2.5 DMI-01g arises if the DMI output reminding a driver that the Air Tightness Control is not displayed. Mitigation / protection is only provided if the driver applies it anyway due to lineside signalling / route information, or the specific location(s) where this occurs only requires the control for passenger comfort and not safety. Situations where this hazard may lead to catastrophic consequences are explained in Appendix B.

6.5.3 INAPP – Inappropriate authority (given by Signaller)

6.5.3.1 INAPP is associated with a Signaller providing a driver with an inappropriate (potentially unsafe) authority to move in a degraded working situation where the train's position has been incorrectly determined on the basis of GPI. Incorrect positioning could be either because the GPI provided by the ETCS On-Board via the DMI is incorrect, or is absent and the driver attempts to estimate their position and does so incorrectly. In getting into the INAPP situation, the Primary ET modelling takes into account the likelihood of being in degraded working where interlocking control was not effective (e.g. where train detection had been lost).

6.5.3.2 The proposed ET model reflects the situations envisaged regarding the train being given authority to proceed towards a level crossing in degraded or abnormal working, an object on the line, or in conflict with another train movement.

6.5.3.3 The object on the line could be engineering on-track equipment if permission for work to proceed was instructed on the basis of the Signaller believing the train has passed that location. Track workers could also be at risk but this has not been modelled due to passenger risk being the defined assessment criteria.

6.5.4 LOSS – Loss of or reduced supervision and protection

6.5.4.1 Once a driver's train is in a mode with no or reduced ETCS supervision and protection and they are unaware of this, there are no formal safety barriers to prevent harm occurring. ETCS protection has been defeated by the failure and subsequent developments. Only a driving style that does not exceed any safety limits (see base event DRV STYLE in Appendix E) provides mitigation for all transfers to LOSS. Where Level change occurs along with the Mode change, lineside signalling / route information and,

if originally in L2, possibly the loss of MA information may also alert the driver to the reduced supervision & protection, though no credit for these has been taken.

6.5.4.2 There are a number of transfers to LOSS, some of which are more onerous than others, something which could be studied further in the quantified Event Tree.

6.5.4.3 The MMI-1g and MMI-1b failures are discussed further under OUTWITH below, as both Immediate Effects arise concurrently. MMI-2b failures (False presentation of Mode) can arise in any ETCS Level (L0, L1 and L2) and is only detectable by the driver recognising that displayed indications are inconsistent with the Mode displayed. N.B. This report only addresses the part of MMI-2b that is not covered by the ETCS Core Hazard, where the driver may be led to believe they are in a Mode with a higher level of supervision and protection than that which the ETCS is advised of. For example, where a Mode change to one with a reduced level of supervision and protection has correctly occurred, but a still different Mode is displayed to the driver which whilst reduced in the level of supervision and protection from that originally, is higher than that being managed by the ETCS On-Board.

6.5.4.4 As Warning and Intervention will not arise in the current Mode, the worst-case situation would be where a driver's style relied upon information or Warnings to prompt a response or action. Defensive driving styles would be least likely to place the train in a situation where ETCS protection was required but not available.

6.5.5 LSP – Loss of Standstill protection

6.5.5.1 LSP occurs in three Hazardous Situations that result in leaving Stand By mode and entering another Mode where Standstill protection is not provided. A hazard is posed should a train move[8] whilst passengers were embarking or disembarking from the train, and passengers are caught and injured between the train and the platform.

6.5.5.2 The principal protection against such unpowered movement is that drivers would be expected not to rely on Standstill protection to hold a train stationary and would maintain a brake application (see SReq09 in Appendix G). In addition, the train may be fitted with open door interlocks which independently maintain a brake application. The train must be on a gradient, and passengers may be able to compensate for the unexpected train movement.

6.5.6 OUTWITH – Operation outside interlocking or signaller's control

6.5.6.1 OUTWITH arises from two Hazardous Situations, "MMI-1g: False request for SH Mode" and "MMI-1b: False Command to enter NL mode", and occurs with a coincident LOSS situation as the change also removes or reduces the level of ETCS supervision and protection.

[8] Roll away protection should still be available.

6.5.6.2 With MMI-1g, (false request for SH mode) the OUTWITH Immediate Effect only applies in a specific situation where the train is stationary in Level 2 FS or OS Mode at the time of the failure (Level 0 and Level 1 scenarios lead to other Immediate Effects such as LSP, LOSS and UBA). Other initial modes may be possible but with reduced consequences commensurate with the reduced interlocking/Signaller control for those modes. Entering the OUTWITH situation may still not always occur depending upon how the trackside application design is developed. The analysis is carried out without assuming any additional protection by the trackside system or operational rules, such as verifying that the On-Board system is really allowed to enter SH mode. Such function or rules would decrease the safety requirements for MMI-1g.

6.5.6.3 For MMI-1b, if the conditions that permit NL mode to be adopted are in place at the time of the false request, due to the specific purpose of NL mode no further protection is available beyond the driver recognising the change of Mode and the condition that makes the NL input signal state as “non leading permitted”.

6.5.7 OVS - Overspeed

6.5.7.1 Overspeed is a situation that can arise following a variety of sequences involving failures in the Driver´s input/outputs via DMI.

6.5.7.2 One of the simplest causes of Overspeed is the presentation of an incorrect train speed to a driver in a Level and Mode where there is limited or no ETCS supervision and protection. This applies particularly in Level 0 when the actual train speed displayed is important as the ETCS supervision and protection is limited (e.g. vehicle maximum speed and national ceiling speeds).

6.5.7.3 Existing core hazard Event MMI-2a.1 can therefore also lead to hazards not covered by the Core Hazard (“non-core”). This is principally in Level 0, but also certain Level 1 and Level 2 situations, see further MMI-2a.1 in Appendix B. However, the risk posed is dependent upon the magnitude of the error, the time over which it is present, and the likelihood of encountering a situation where the additional speed is a problem. This presents a spectrum of scenarios ranging between:

- A gross error that is very easily recognised by the driver but presents potentially more onerous consequences over a short period, and
- A smaller speed error, that is more difficult to recognise by the driver (thereby presenting a hazard for a longer period but being less likely to result in the safe speed or distance being exceeded sufficient to cause serious consequences).

6.5.7.4 DMI-01b: Valid ETCS On-Board output via DMI obscured by erroneous output (audio or visual) is similar to MMI-2a.1. This is considered to be less onerous than MMI-2a.1, as the driver would be aware that the DMI indications are defective, compared to MMI-2a.1 where a driver would assume the indicated speed to be correct unless there are indications to the contrary.

6.5.7.5 Other causes of Overspeed involve a variety of failures associated directly or indirectly with the Track Adhesion factor functionality/status (MMI-2c, DMI-05e, DMI-1h, DMI-1i, DMI-3g, DMI-3h).

6.5.7.6 The six situations involving the Track Adhesion factor functionality/status are potentially onerous in that the Movement Authority (MA) is likely to be exceeded, either in terms of the permitted speed or the EoA. However, the extent of any overrun may be lower compared to other Overspeed situations because braking should take place, and the safety margins in the On-Board and trackside ETCS application design may ameliorate some of the poor adhesion encountered (though this will be of minimal benefit where the adhesion levels is significantly low).

6.5.7.7 The potential consequences when in an Overspeed situation are numerous, with the resultant risk posed depending upon a range of factors and circumstances. In addition to the magnitude of the Overspeed, the risks depend upon the route and operational factors associated with each of the identified outcomes described in Appendix A and modelled in the ETA (e.g. whether Buffer Stops are approached, whether the train is required to stop at an EoA, features of the route including Level Crossings, etc.).

6.5.8 UBA – Unexpected Brake Application

6.5.8.1 Whilst an Unexpected Brake Application (UBA) could potentially lead to a passenger injury, the likelihood is considered low. However, whilst the level of risk posed may be minimal, the risk only arises due to a failure of the DMI, and should therefore be recognised as such. Whilst UBA can arise as a consequence of numerous Hazardous Situations, in a number of these the Hazardous Situation is a direct consequence with no mitigating barriers or protection.

6.5.8.2 Although modelled here as with negative safety consequence it is clear that the risk posed by UBA is more than offset by the safety benefit provided by the protection functions of ETCS. Indeed, the operational and passenger confidence requirements are such that a reliability of the ETCS On-Board system, which satisfies these, will certainly be sufficient to ensure that UBA is of negligible importance.

6.5.9 Multiple DMI Failures

6.5.9.1 The analysis has not considered Common Cause Failures or Common Mode failures (CCF/CMF) of the DMI.

6.5.9.2 In order to consider the CCF/CMF of the DMI, it is required information on the specific hardware (and potentially software) designs, as the technologies used and the functional allocation to hardware elements (and software modules) determine the impact of specific failures on other functions. These cannot therefore be addressed generically in the models of this study.

6.5.9.3 It may be expected that, where subsequent action or mitigation in later events utilises a different driver´s input/output via DMI, then the scope for CCF/CMF may be low (e.g. the initial DMI fault relates to a command action such as an acknowledgement, and the later

events are concerned with display functions). Thus, the model currently assumes that if the DMI has spuriously requested a Mode change, or spuriously acknowledged a Mode change proposed, then it will correctly display to the Driver the information sent to it by the ETCS On-Board when the change is made by the ETCS On-Board itself.

6.5.9.4 Whilst a CCF/CMF of the DMI could occur, the models do not explicitly model a second, *independent* failure in the DMI within the failure sequence. This is because the likelihood of a second independent DMI failure at that exact time is considered less likely than the mitigating event / driver response that is modelled in the Event Trees. That is, except for CCF/CMF reasons, the failures scenarios that would limit THR derivation are those regarding the subsequent driver response rather further independent failures in the DMI in such a short timescale. To include every possible DMI failure occurring independently after an initial DMI failure would also obscure the logic of the scenario itself.

6.5.9.5 Where subsequent barriers or mitigation in the models call upon a similar driver´s input/output via DMI, then this is highlighted in the event descriptions so that it can be considered in deriving the event probabilities.

6.5.9.6 One possible outcome of a CCF/CMF worthy of note is that forming the basis of DMI-04h. Here, a continuous failure in the DMI causing continuous or repeated ‘automatic’ acknowledgement could result, in practical terms, in standstill, reverse movement or rollaway protection being defeated, albeit as a series of start/stop sequences. The situation would arise where the ‘acknowledgement of release emergency brake’ or ‘acknowledgement of release service brake’ occurred spuriously, the train moved, protection was applied, but then removed by a further spurious acknowledgement.

6.6 Constraints and Exported Requirements

6.6.1.1 Due to the constraints and scope of the study, the results must be viewed within the context of a number of key assumptions or aspects that are to be addressed outside of this study. These are in addition to the Safety Requirements arising from the study which are listed in Appendix G.1. The constraints and exported requirements are listed in Appendix G.2.

6.7 Scenarios not Modelled

6.7.1.1 The following scenarios have not been modelled since the consequences of them are believed to be depending too much on Operational Rules (potentially national) or circumstances:

- The consequences of some specific **level crossing incidents** due to overspeeding have not been modelled. See further analysis of immediate effect “Overspeed”, case c) Level Crossing Incidents in Appendix B and secondary event tree LXI in Appendix D.
- The consequence of a potential **collision with a structure** or a stationary vehicle due to overspeeding (train leans additionally and is out of gauge) has not been

modelled. See further event STRUCTURE in Appendix B and secondary event tree OVERSPEED in Appendix D, failure impact “STRUCTURE GAUGE”.

- The consequence of the train running on an **incompatible infrastructure** due to overspeeding (driver not being able to stop before the incompatibility occurs) has not been modelled. See further event UNSUITABLE in Appendix B and secondary event tree OVERSPEED in Appendix D, failure impact “INCOMPATIBLE”.
- The consequence of the train **collision with an object** due to overspeeding (driver not being able to stop before the object) has not been modelled. See further secondary event tree OVERSPEED in Appendix D, failure impact “OBJECT”.

6.8 Results of Quantification

6.8.1.1 Calculations have been carried out with the tool FaultTree+ V11.0. Resulting event trees are included in Appendix D.

6.8.1.2 Table 4 shows the THR which satisfies the RAC for all Consequences in which each Hazard is involved. From this rate, the corresponding SIL is derived according to EN 50129:2003.

Top-Level DMI Hazard		Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
H1	Information NOT displayed when it should have been	**DMI-01a**	Failure to provide Warning indication	$5.0*10^{-4}$	0
		DMI-01b	Valid ETCS On-Board output via DMI obscured by erroneous output (audio or visual)	$1.0*10^{-3}$	0
		DMI-01c	Failure to display request for acknowledgement	$1.0*10^{-4}$	0
		DMI-01d	Failure to display Geographical Position data	-	-
		MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	$1.0*10^{-4}$	0
		DMI-01f	Failure to display ACK for RV request	$1.0*10^{-3}$	0
		DMI-01g	Failure to display Air Tightness Control	$1.0*10^{-4}$	0

Top-Level DMI Hazard		Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
		MMI-2i	Failure to present “LX not protected” information	-	-
		DMI-01h	Failure to present Display Distance to Target information	$6.7*10^{-5}$	0
		DMI-01i	Failure to present Time To Indication information	$6.7*10^{-5}$	0
H2	Information displayed when it SHOULD NOT have been	**DMI-02a**	False presentation of Warning	$1.0*10^{-4}$	0
		DMI-02b	False presentation of IS mode (shown as IS mode when not)	$1.0*10^{-1}$	0
		DMI-02c	False presentation of brake indication	$5.0*10^{-3}$	0
		MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	$5.0*10^{-3}$	0
		DMI-02e	Spurious notification of Train Data change (which normally is from source different from the driver)	-	-
		DMI-02g	False presentation of “LX not protected”	$1.0*10^{-4}$	0
		MMI-2c	False presentation of track adhesion factor (shown as applied when not)	$6.7*10^{-5}$	0
H3	Erroneous but valid information displayed	**DMI-03a**	Incorrect Geographical Position data displayed	-	-
		DMI-03c	Wrong acknowledgement request displayed	-	-
		DMI-03d	Wrong Trip Reason displayed	-	-
		DMI-03e	Wrong fixed text message displayed	$1.0*10^{-5}$	0

Top-Level DMI Hazard		Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
		DMI-03f	"Tunnel stopping area" displayed at the wrong geographical place	$1.0*10^{-3}$	0
		MMI-2a.1	False presentation of train speed	$3.7*10^{-6}$	1
		MMI-2b	False presentation of mode	$5.0*10^{-6}$	1
		DMI-03g	Wrong Display Distance to Target information	$6.7*10^{-5}$	0
		DMI-03h	Wrong Time To Indication information	$6.7*10^{-5}$	0
H4	Erroneous but valid input to the ETCS On-Board via the DMI	**DMI-04a**	False command to exit shunting	$2.0*10^{-2}$	0
		DMI-04c	False START command	$1.0*10^{-1}$	0
		DMI-04d	False UN acknowledgement	-	-
		MMI-1g	False request for SH Mode	$4.0*10^{-4}$	0
		DMI-04f	Spurious or wrong language requested distracting the train Driver	-	-
		DMI-04g	Spurious request to change to another ETCS Level	$2.0*10^{-4}$	0
		DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	$1.0*10^{-5}$	0
		DMI-04j	False Isolation command	$1.0*10^{-6}$	1
		MMI-1a	False acknowledgement of mode change to less restrictive mode	$2.0*10^{-5}$	0
		MMI-1b	False Command to enter NL mode	$1.0*10^{-1}$	0
		MMI-1d	False acknowledgement of Level Transition	$2.0*10^{-4}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour)	SIL
	MMI-6	Falsification of Virtual Balise Cover (failure mode corruption)	$2.0*10^{-6}$	1
	MMI-6	Falsification of Virtual Balise Cover (failure mode insertion)	$1.5*10^{-5}$	0
H5 Deleted input to the ETCS On-Board via DMI	**DMI-05a**	Deleted Level transition acknowledgement	$5.0*10^{-5}$	0
	DMI-05b	Deleted acknowledgement	$5.0*10^{-5}$	0
	DMI-05c	Deleted request for GPI	-	-
	DMI-05d	Deleted change of language request	-	-
	DMI-05e	Deleted driver request to apply Track Adhesion Factor	$1.0*10^{-4}$	0
	DMI-05f	Deleted Reversing mode acknowledgement	$1.0*10^{-3}$	0
	DMI-05g	Deleted “PT distance exceeded” acknowledgement	-	-
	DMI-05i	Deleted “reversing distance exceeded” acknowledgement	-	-
	DMI-05j	Deleted Isolation command	-	-
	DMI-05l	Deleted Train Trip acknowledgement	-	-
	MMI-6	Falsification of Virtual Balise Cover (failure mode deletion)	-	-

6.8.2 Table 4 – Derived Tolerable Hazard Rates

6.8.2.1 Cut-Sets can be found in Appendix H.

6.8.2.2 As discussed in section 5.5, the DMI Hazardous Situations (DMI-xx/MMI-xx) are used as initiating events in the event tree analysis. The result of these studies is summarized on **Table 8**.

6.9 Sensitivity Analysis

6.9.1 General

6.9.1.1 Obviously, the reliability of the results reported in Chapter 6.8 is highly dependent on the quality of the input to the calculations. The main input sources are:

- Event Tree modelling
- Risk Acceptance Criteria
- Probabilities of barriers and mitigations

6.9.1.2 The Event Tree modelling has been extensively reviewed by several parties of the railway sector, as noted in clause 6.5.1, and is believed to be of a high quality.

6.9.1.3 The RAC given in Section 5.4 is really not in the scope of this report to determine, but is an input to it. However, the RAC has been determined by ERA on the basis of work on the Common Safety Methods and should therefore be regarded as reliable.

6.9.1.4 The probabilities of barriers and mitigations are estimates largely based on engineering judgement. As such, to gain credibility, it must be reviewed by people with different roles and competencies. Section 6.9.2 has provided the reviewers with information on which of the barriers and mitigations that are of the most importance to the results, and subsequently that the review should focus on. The group of reviewers have included people with extensive experience in operational rules. In addition, a work has been undertaken by the ERTMS User's Group specifically to review the assignment of probabilities to driver actions. The results of this study have been incorporated into the present analysis by updating the probabilities according to agreement with the ERTMS User's Group and ERA.

6.9.1.5 In addition to the calculation input, there are also some important analysis method assumptions which need to be further discussed. This is done in Section 6.9.3.

6.9.2 Importance Ranking of Barriers and Mitigations

6.9.2.1 The below tables present an importance ranking for each consequence. Both methods available in FaultTree+, Fussell-Vesely and Birnbaum, are presented. The first method gives an event's relative importance to the total frequency of the consequence, while the second method gives a measure of how sensitive the total frequency of the consequence is to variations in an event's probability. Here, only the events with the highest importance ranking for each consequence are presented; this is defined as events which are among the 20 most important measured with either of the two methods.

6.9.2.2 S4 is the consequence with by far the largest amount of Cut-Sets close to the RAC, and therefore this should be considered as the most important one.

6.9.2.3 Not surprisingly, the figures show that the driver actions and mission profile parameters are completely dominating the importance.

6.9.2.4 Despite of the large impact of some input parameter and their inherent uncertainty, it is not recommended to add any safety margin to the results in Section 6.8 because of this, but rather to consider the input parameters consolidated after review.

Event	Fussell-Vesely Importance	Birnbaum Importance
SEV HS UBA-MIN	8.03E-01	3.71E-04
STANDSTILL	1.10E-01	2.03E-04
DRV CHANGE MODE	1.10E-01	1.01E-04
DRV AIR TIGHT	1.08E-01	1.00E-04
OUT OF SERVICE	1.08E-01	5.00E-05
ACK DISPLAY OK	1.08E-01	2.00E-05
CONTROLLED BRAKING	1.08E-01	9.99E-04
DRV INDICATION OVERRIDE	1.08E-01	9.99E-04
NO STAFF	1.08E-01	2.00E-05
DRV OVERSPEED	1.08E-01	9.99E-05
ACK MISS NOT UBA	1.08E-01	2.00E-05
SEV LS UBA-MIN	8.83E-02	4.08E-05
DRV INDICATION	6.50E-02	2.00E-05
DRV STYLE	6.50E-02	5.99E-04
FALSE MODE	6.50E-02	5.99E-05
DRV WARNING	6.50E-02	2.00E-05
GRADIENT	1.95E-03	1.80E-06
ROUGH RIDE	4.34E-05	4.00E-07
DRV BS	3.91E-05	3.60E-08
PROB-BS	3.91E-05	3.60E-08
CAREFUL	2.06E-05	1.90E-06
DRV INDICATION SLIPPERY	2.06E-05	1.90E-06

Table 5 – Importance ranking for events contributing the most to consequence S2 “one or more light injuries”

Event	Fussell-Vesely Importance	Birnbaum Importance
TRAIN SPEED HIGH	8.49E-01	4.12E-06
SEV LS UBA-MAJ	8.49E-01	4.12E-05
GRADIENT	1.19E-01	5.76E-07
DRV STATION BRAKE	1.17E-01	5.67E-05
DOOR INTERLOCK	1.17E-01	5.67E-05
PASSADJUST	1.17E-01	5.67E-08
NOT IN SB	1.16E-01	1.13E-06
LEVEL 1 OR LEVEL 2 OP	1.16E-01	1.12E-07
OUT OF SERVICE	1.12E-01	2.70E-07
IN L0	1.11E-01	5.99E-08
DRV CHANGE MODE	1.05E-01	5.08E-07
STANDSTILL	1.05E-01	1.02E-06
NO STAFF	1.03E-01	1.00E-07
ACK DISPLAY OK	1.03E-01	1.00E-07
CONTROLLED BRAKING	1.03E-01	5.00E-06
DRV INDICATION OVERRIDE	1.03E-01	5.00E-06
DRV OVERSPEED	1.03E-01	5.00E-07
ACK MISS NOT UBA	1.03E-01	1.00E-07
DRV INDICATION	7.03E-02	1.14E-07
DRV WARNING	6.19E-02	1.00E-07
DRV INDICATION SLIPPERY	8.39E-03	4.07E-06
CAREFUL	8.39E-03	4.07E-06
DRV STYLE	6.19E-02	3.00E-06
FALSE MODE	6.19E-02	3.00E-07
INTERUPTION	5.16E-04	2.50E-07
DRV JUNCTION	4.05E-03	1.96E-07

AUTO ACK	4.00E-04	1.94E-07

Table 6 – Importance ranking for events contributing the most to consequence S3 “single fatality and/or single serious injury”

Event	Fussell-Vesely Importance	Birnbaum Importance
DRV STYLE	3.79E-01	9.71E-07
TRAIN UP	2.37E-01	1.21E-08
MODE SUPERVISED	1.75E-01	2.24E-08
DRV SIGNAL	1.60E-01	4.10E-07
TSR SPEEDING MINOR	1.55E-01	3.96E-08
TSR	1.55E-01	1.98E-08
DRV CHANGE MODE	1.51E-01	3.87E-08
STANDSTILL	1.12E-01	5.75E-08
IN L0	1.06E-01	3.03E-09
DRV STYLE LAF	1.01E-01	2.59E-08
GOOD ADHESION	1.01E-01	5.19E-08
DRV INDICATION	1.01E-01	8.64E-09
SPEED DISPLAY	1.01E-01	5.16E-09
DRV INDICATION SLIPPERY	1.01E-01	2.58E-06
CAREFUL	1.01E-01	2.58E-06
OUT OF SERVICE	1.01E-01	1.29E-08
HIGH-LOW DISPLAY	1.01E-01	5.15E-09
DRV SPEED RECOG	1.01E-01	8.59E-09
SPEED OK	1.01E-01	2.86E-09
LINE CLEAR	7.81E-02	4.00E-09
DRV RV ALT	7.88E-02	4.00E-09
RV EMG	7.88E-02	1.00E-03
FIRE	5.85E-02	7.50E-04
EXTERNAL ACCIDENT	7.80E-03	1.00E-04
NL INPUT SIGNAL	1.95E-03	5.00E-06

LX NORMAL	3.74E-02	9.60E-07
DRV JUNCTION	7.65E-02	1.96E-07
DRV ANNOUNCED	7.41E-02	1.90E-07
DRV REPEAT PROT	3.90E-02	1.00E-07
DRV INDICATION NO OVERRIDE	3.90E-02	1.00E-07
ETCS ON-BOARD REJECTS	3.90E-02	2.00E-08

Table 7 – Importance ranking for events contributing the most to consequence S4 "fatalities and/or serious injuries"

6.9.3 Main Analysis Method Assumptions

6.9.3.1 Several analysis methods assumptions have been made in the course of this analysis. The one with the largest impact is:

The **co-incidence** of DMI Hazardous Situations and Consequence scenarios is neglected. As stated in clause 5.5.1.4, it has been assumed that each Cut-Set can be studied individually, and not the sum of them.

The impact of this assumption is quite large, and proportional to the number of scenarios modelled. The Consequence S4 has the largest number of Cut-Sets close to the RAC, and – after Cut-Set reduction – the sum of the Cut-Sets frequencies would be approximately 10 times larger than the largest Cut-Set frequency. This value has been obtained after performing the analysis taking into account the main hazards as initiating events. The reason to use main hazards is that functions are studied and not individual items to display/input. This would mean that the required safety integrity of the DMI would be shifted towards the more demanding side one decade.

As already stated, the approach of summing all the Cut-Sets is quite unrealistic. However, a deeper study of the Cut-Sets shows that some scenarios are really independent. It is practically impossible to calculate how large portion of the sum of the Cut-Sets that originate from independent Cut-Sets, but it is believed that approximately half is a conservative estimation. Considering the factor 10 above, it is therefore recommended to use an uncertainty factor of 5 to the results derived (in addition to what is stated for case a) above).

Note: An alternative approach would be to first sum all Cut-Sets and then make the results a factor of 2 less restrictive. This would however be highly impractical, since it would mean that the complete analysis results would change as soon as a new event tree was introduced, even if it was not bounding, or as soon as the quantification of a barrier would change, even if it was not part of a bounding scenario.

6.9.3.2 In summary, it is believed appropriate to reduce the THRs from Section 6.8 with a factor of 5, i.e. making them a factor of 5 more demanding.

7. CONCLUSIONS

7.1.1.1 This study has;

- Identified hazards associated with the DMI functions that are at the same level as, and independent of, the ETCS Core Hazard.
- Quantified Tolerable Hazard Rate requirements for these DMI hazards, taking into account the consequences of the hazards and barriers to their occurrence.

7.1.1.2 The result is the below set of Tolerable Hazard Rates for the DMI hazards, which can be used as part of the safety requirements for the DMI function in the ETCS On-Board system. Additionally, it has been included a column where the corresponding SIL is derived according to EN 50126-2 Table 3 (currently Issue 04 Draft 02 is used):

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour) with uncertainty factor	SIL
H1 Information NOT displayed when it should have been	**DMI-01a**	Failure to provide Warning indication	$1.0*10^{-4}$	0
	DMI-01b	Valid ETCS On-Board output via DMI obscured by erroneous output (audio or visual)	$2.0*10^{-4}$	0
	DMI-01c	Failure to display request for acknowledgement	$2.0*10^{-5}$	0
	DMI-01d	Failure to display Geographical Position data	-	-
	MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	$2.0*10^{-5}$	0
	DMI-01f	Failure to display ACK for RV request	$2.0*10^{-4}$	0
	DMI-01g	Failure to display Air Tightness Control	$2.0*10^{-5}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour) with uncertainty factor	SIL
	MMI-2i	Failure to present “LX not protected” information	-	-
	DMI-01h	Failure to present Display Distance to Target information	$1.3*10^{-5}$	0
	DMI-01i	Failure to present Time To Indication information	$1.3*10^{-5}$	0
H2 Information displayed on the DMI when it SHOULD NOT have been	**DMI-02a**	False presentation of Warning	$2.0*10^{-5}$	0
	DMI-02b	False presentation of IS mode (shown as IS mode when not)	$2.0*10^{-2}$	0
	DMI-02c	False presentation of brake indication	$1.0*10^{-3}$	0
	MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	$1.0*10^{-3}$	0
	DMI-02e	Spurious notification of Train Data change (which normally is from source different from the driver)	-	-
	DMI-02g	False presentation of “LX not protected”	$2.0*10^{-5}$	0
	MMI-2c	False presentation of track adhesion factor (shown as applied when not)	$1.3*10^{-5}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour) with uncertainty factor	SIL
H3 Erroneous but valid information displayed	**DMI-03a**	Incorrect Geographical Position data displayed	-	-
	DMI-03c	Wrong acknowledgement request displayed	-	-
	DMI-03d	Wrong Trip Reason displayed	-	-
	DMI-03e	Wrong fixed text message displayed	$2.0*10^{-6}$	1
	DMI-03f	"Tunnel stopping area" displayed at the wrong geographical place	$2.0*10^{-4}$	0
	MMI-2a.1	False presentation of train speed	$7.4*10^{-7}$	2
	MMI-2b	False presentation of mode	$1.0*10^{-6}$	1
	DMI-03g	Wrong Display Distance to Target information	$1.3*10^{-5}$	0
	DMI-03h	Wrong Time To Indication information	$1.3*10^{-5}$	0
H4 Erroneous but valid input to the ETCS On-Board via the DMI	**DMI-04a**	False command to exit shunting	$4.0*10^{-3}$	0
	DMI-04c	False START command	$2.0*10^{-2}$	0
	DMI-04d	False UN acknowledgement	-	-
	MMI-1g	False request for SH Mode	$8.0*10^{-5}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour) with uncertainty factor	SIL
	DMI-04f	Spurious or wrong language requested distracting the train Driver	-	-
	DMI-04g	Spurious request to change to another ETCS Level	$4.0*10^{-5}$	0
	DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	$2.0*10^{-6}$	1
	DMI-04j	False Isolation command	$2.0*10^{-7}$	2
	MMI-1a	False acknowledgement of mode change to less restrictive mode	$4.0*10^{-6}$	1
	MMI-1b	False Command to enter NL mode	$2.0*10^{-2}$	0
	MMI-1d	False acknowledgement of Level Transition	$4.0*10^{-5}$	0
	MMI-6	Falsification of Virtual Balise Cover (failure mode corruption)	$4.0*10^{-7}$	2
	MMI-6	Falsification of Virtual Balise Cover (failure mode insertion)	$3.0*10^{-6}$	1
H5 Deleted input to the ETCS On-Board via DMI	**DMI-05a**	Deleted Level transition acknowledgement	$1.0*10^{-5}$	0
	DMI-05b	Deleted acknowledgement	$1.0*10^{-5}$	0

Top-Level DMI Hazard	Hazardous Situation		THR for Hazardous Situation (per hour) with uncertainty factor	SIL
	DMI-05c	Deleted request for GPI	-	-
	DMI-05d	Deleted change of language request	-	-
	DMI-05e	Deleted driver request to apply Track Adhesion Factor	$2.0*10^{-5}$	0
	DMI-05f	Deleted Reversing mode acknowledgement	$2.0*10^{-4}$	0
	DMI-05g	Deleted “PT distance exceeded” acknowledgement	-	-
	DMI-05i	Deleted “reversing distance exceeded” acknowledgement	-	-
	DMI-05j	Deleted Isolation command	-	-
	DMI-05l	Deleted Train Trip acknowledgement	-	-
	MMI-06	Falsification of Virtual Balise Cover (failure mode deletion)	-	-

Table 8 – Main Results

7.1.1.3 The above results have taken into consideration the THRs from Section 6.8 with the recommended uncertainty factor from Section 6.9.

7.1.1.4 The following must be noted:

a) Because this study doesn’t consider the ETCS Core Hazard, the above requirements are not the only ones needed to fully specify the safety integrity requirements of the DMI. The complete set of requirements is given by this study together with requirement ETCS_OB01 in SUBSET-091 [Ref 5].

b) In the present analysis, all possible barriers to the studied DMI hazardous event developing into an accident have been scrutinized and taken into consideration when found appropriate. Therefore, when showing attainment to the above THRs, no further credit can be taken for such barriers, e.g. operational circumstances or driver mitigations, but the rates must be fulfilled by the Driver´s input/outputs to ETCS On-Board via DMI. There is an exception with MMI-2A.1, where it is noted that some company specific solutions could be used as a barrier. See Appendix E.

7.1.1.5 This analysis is valid under the assumptions stated in Section 3.3 and with the safety requirements and exported constraints listed in Appendix G.

7.1.1.6 This study only applies to SUBSET-026 [Ref 1].

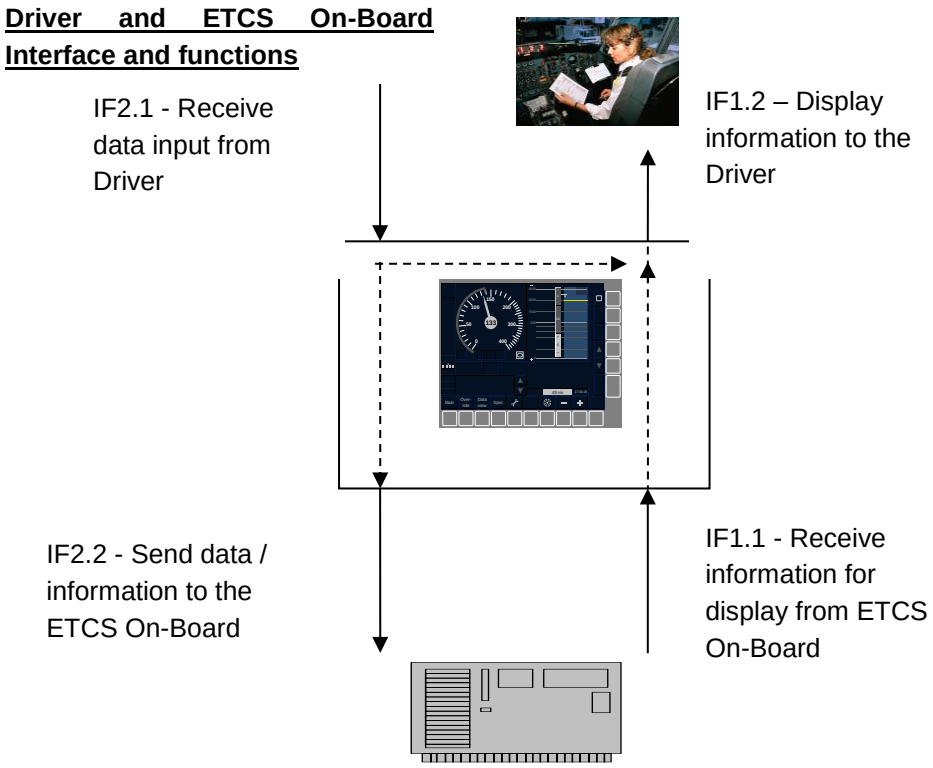
APPENDICES

Appendix A ETCS DMI Functional Failure Analysis (FFA)

A.1 Driver and ETCS On-Board Interface and functions

A.1.1.1 At the most basic level the DMI conveys an “Input / Output”, providing a mechanism to receive and send information.

A.1.1.2 The DMI is the interface between the Driver and the ETCS On-Board. The core DMI functions assessed here are therefore related to this information exchange: “Receive and Display information via the DMI” (IF1) and “Output to and receive information from the ETCS On-Board” (IF2), perhaps strictly with a caveat of doing these actions correctly. The two functions can be broken down further relating to the information source/destination (Driver and ETCS On-Board) using IF1.1, IF1.2, IF2.1, IF2.2:



A.1.1.3 Function IF1.1, ‘Receive information for display from ETCS On-Board’ is a DMI function, however, whatever failure modes the DMI may have when managing this information, these can only be additional causal events to equivalent failure modes that already exist within the ETCS On-Board, since anything that the DMI can do regarding failing to pass on the information or corrupting the information could also occur within the ETCS On-Board system. Thus, as far as the true ‘functional’ failure is concerned, failure to display information could occur due to the information not being generated by the rest of the ETCS On-Board system or by failures within the DMI itself.

A.1.1.4 This causes a complication for this study which is limited to deriving a THR for the DMI only, yet there are further failure modes associated with the same functional failure that arise from ETCS On-Board functions. The situation is further complicated in that failures of the DMI that result in the $ETCS_{CH}$ are also excluded from the scope of the study, being already addressed in existing analysis (e.g. SUBSET-079 [Ref 3] and -088 [Ref 4]).

A.1.1.5 The DMI functional failures may be simplified a little in that failures associated with function IF2.1 do not exist independently, since they are in practice all causal events of functional failure IF1.2. Similarly, failures associated with IF1.1 (data input from ETCS On-Board) will be causal events of functional failures associated with IF1.2 again, and also IF2.2. These linkages are illustrated with the dotted lines within the DMI function.

A.1.1.6 Thus, the DMI functions reduce to:

- F1 – Convey information from the ETCS On-Board via the DMI (audio and visual) to the Driver, and
- F2 – Convey information from the Driver to the ETCS On-Board.

DMI Core Functions

F1 – Convey information from the ETCS On-Board via the DMI (audio and visual) to the Driver

IF2.1 - Receive data input from Driver

F1

IF1.2 – Display information to the Driver

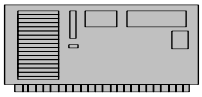
DMI

IF2.2 - Send data / information to the ETCS On-Board

IF1.1 - Receive information for display from ETCS On-Board

F2

F2 – Convey information from the Driver to the ETCS On-Board



ETCS On-Board

A.2 Functional Failure Analysis

A.2.1.1 The two basic DMI functions result in five functional failures specified below:

ID	Function	Failure Mode	Hazardous Event / Functional Failure	Comment
1	Convey information from the ETCS On-Board via the DMI (audio and visual) to the driver	ABSENT	Information NOT displayed to the driver when it should have been.	Hazard H1
		INSERTION	Information displayed to the driver when it SHOULD NOT have been.	Includes any spurious display. Principally concerned with directly misleading the driver. Failure mode could also distract a driver whilst determining the output to be false, although considered less onerous as a driver could be distracted by many stimuli or issues other than a failure in the DMI. Hazard H2.
		INCORRECT	Erroneous but valid information displayed to the driver.	Covers incorrect, corruption, erroneous value or retention of 'stale' data. Hazard H3.
		TIMING	As above.	Impact results in information being either absent or inserted (i.e., not displayed when needed or displayed when it should not be).

ID	Function	Failure Mode	Hazardous Event / Functional Failure	Comment
2	Convey information from the driver via the DMI to the ETCS On-Board	ABSENT	Absence of output via the DMI to the driver when required.	Hazard H5
		INSERTION	Information sent via the DMI to the ETCS On-Board when not required.	Hazard H4. DMI provides information to the ETCS On-Board spuriously.
		INCORRECT	Erroneous but valid output via the DMI to the ETCS On-Board.	Hazard H4. DMI provides data to the ETCS On-Board which is erroneous.
		TIMING	As above.	Impact results in information being either absent or inserted (i.e., not displayed when needed or displayed when it should not be).

A.2.1.2 Note 1: In strict terms, Hazard H4 could be split into two, the equivalent of H2 and H3 under Function F1, regarding providing spurious or incorrect information. However, unlike a Driver, the ETCS On-Board makes no distinction between spurious or incorrect information, as the ETCS On-Board simply acts upon the information it receives, and hence the two are combined for simplicity.

A.2.1.3 Note 2: Incorrect information may be in one of three states which impacts on the immediate impact / consequences of the failure:

- “valid but incorrect” meaning that it is a formally correct item of data / information but incorrect to the current state / activities; e.g. the text of the information is coherent and correct but not required at that time or the speed displayed has the right number of valid characters but is the wrong value. May also be referred to as Erroneous (see clause 3.5.1.1).
- “valid and correct” also referred to as spurious e.g. the spuriously ‘correct’ acknowledgement to a request from the ETCS On-Board, but without receiving the input to do so from the Driver.
- “erroneous and incorrect” meaning that the information is corrupted or includes non-valid characters or content in some manner, and thus not valid.

Appendix B DMI Hazard Schedule

Blue highlighted cells indicate hazardous situations that were presented in previous issues as Non-Core, but were subsequently concluded only being part of the Core Hazard. They are retained as part of an auditable trail, and to present information to future readers regarding their consideration in the analysis.

The hazard schedule references which HAZID identity that is concerned with a certain hazardous situation, although the HAZID report is not explicitly referenced. However, the information is retained for the sake of easing future updates of this document.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
H1 - Information NOT displayed when it should have been	1.	**DMI-01a**: Failure to provide Warning indication	If driver does not respect the permitted speed plus a margin, DMI failure leads directly to the Unexpected Brake Application (**UBA**).	**UBA**: Unexpected Brake Application	None, but the likelihood of any significant injury occurring is considered minimal based upon experience of railway operations to date.	L0 - HAZID 12.1, 12.2, 12.3. As ETCS is working correctly, Intervention occurs unexpectedly. L1 & L2 Intervention would similar occur unexpectedly. Affected Modes are all where supervision occurs, the more onerous ones being those with travel at higher speeds.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	2.	**DMI-01b**: Valid ETCS On-Board output via DMI obscured by erroneous output (audio or visual)	1. Against Overspeed (**OVS**): a) Driver may be able to remove the erroneous display. b) Driver takes a cautionary approach in the absence of speed indication. c) Driver takes train out of service at earliest opportunity (as DMI display clearly faulty).	Driver may not perform the required operation. Considering what information required by a driver that does lead to a core hazard, the following could, in the limit, potentially occur: 1. **OVS** - Overspeed – due to speed information being obscured.	1. OVS: Bounded by / same barriers as for OVS under hazardous situation MMI-2a.1.	L0 – HAZID 6.6 identified during data entry. The generic potential applies in principle to the DMI screen display (e.g. degradation) and any spurious presentation of information to the driver that could block other DMI screen data. May also prevent access to a valid function that is blocked e.g. an acknowledgement button cannot be accessed by a spurious other DMI action.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						OVS is considered to be less onerous than an incorrect speed being indicated as the driver would have no speed indication and therefore need to estimate the speed, and with a 'head-up' driving style where the speedometer is only periodically sampled, the driver would be expected to have knowledge of the prior speed, as opposed to an consistently incorrect speed indication.
			2: Against **UBA**:	2. **UBA**	2. UBA: As DMI-01a	

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			None as failure to observe or get access to relevant request to an acknowledgement would lead directly to the UBA event. Obscuration of an audible **or** visual Warning could still be protected by the presence of the corresponding visual or audible component of the Warning (where both are provided).	The above are the specific events that could occur, however, the failure mode could be a causal event of other hazardous situations already addressed below e.g. for 'Absent indication' by obscuring Mode or Level indications, failure to see response to a driver requested action. These are therefore covered directly under the specific hazardous situation.		

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	3.	**DMI-01c**: Failure to display request for acknowledge-ment	No barriers – if request is not acknowledged the timeout will occur. CR1166 says it is undefined when the timer shall start. Thus, it has been considered in this analysis that the timer starts counting when the ETCS On-Board outputs the ACK, so that a deleted ACK will cause a timer elapse.	**UBA** – e.g. if Request for Level Transition Ack not displayed. This includes any level transition or mode change that is supervised by the ETCS.	None	Confirmed effect is not $ETCS_{CH}$ as there exists a valid MA, and the issue is that a DMI failure has meant that intervention occurs whilst ETCS is correctly adhering to the speed and distance requirement. DMI-01c applies to ACKs where failure to ACK results in a brake application by the ETCS On-Board (there are ACKs which do not result of UBA, e.g. Trip mode ACK, test message ACK…). ACK of RV has different consequences and is covered DMI-01f.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	4.	**DMI-01d**: Failure to display Geographical Position data	Additional barrier applies compared to INCORRECT data failure mode (see H3, DMI-03a) in that the driver must choose to derive / estimate data in place of the 'missing' correct data, and must do this incorrectly (the latter is however partly credited in DMI-03a via DRV POSITION).	For "Incorrect Geographical Position data" – see H3	see DMI-03a	HAZID 11.1, 11.3. Principal impact is RAM in that driver will not have the relevant data, which may delay resolution of the problem that required use of GPI. Whilst less likely, a potentially hazardous situation arises if the driver attempts to compensate and provide information based on route knowledge that is incorrect. **Safety Requirement SReq07**: The trackside application (engineering in combination with operational rules) should not put any safety reliance on the Geographic Position Information. Some examples on scenarios to avoid are presented in Appendix G.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						DMI-01d scenario is bounded by DMI-03a, which introduces barriers to reduce the frequency of data being incorrect.
	5.	**MMI-2f:** Failure to display Override status (failure mode deletion), including false enabling of override selection	Driver requests Override to be applied when actually not required (see comment column for examples).	HAZID 15.4: LOSS of protection – tripping does not occur when required.	HAZID 15.4: LOSS 1. Must encounter location where tripping is required for safety. 2. Override only for a predefined period (time or distance according to set National Values), e.g. a maximum of 255 seconds duration. 3. The unsafe situation only occurs when driver misses the closed signal that has been inhibited due to the Override request, or if it is already passed, fails to obey operational procedures.	For HAZID 15.4, the harm situation is analogous to Core Hazard failure MMI-1c, in that tripping is not active when it is expected to be so. The non-core situation that leads to this, is that a genuine request to the ETCS On-Board is made for Override, and with Override erroneously not being displayed by the DMI, the driver continues as if tripping is still active. As non-core, the most likely scenarios are:

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						a) where a driver **mistakenly** requested Override, but on checking the display, believed that it was not acted upon (lack of indication prevents to discover it). b) driver unaware that request for Override has been made (e.g. operated accidently by driver or external object contacting the selection control) and the lack of DMI indication prevents the error being revealed. In these two instances as the location is not one where Override of an EoA had been planned /anticipated, it is potentially more likely that a hazard requiring ETCS supervision and protection that is no longer available could arise.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	6.	**DMI-01f:** Failure to display ACK for RV request	1. The reason for needing to reverse is for emergency purposes to avoid a conflict or incident. Note: SRS 5.13.1.1 states that RV is only intended for rapid mitigation of an emergency situation, and hence the need for it to be available immediately is likely to be high.	If the need to adopt RV Mode is for emergency (mitigation) purposes, then catastrophic failure is assumed if no reaction to avoid an accident is taken in a range of few minutes.	Potentially none. In some scenarios there may be insufficient time to change to NL or SH mode, or to isolate ETCS, and resume the reversing movement. The probability of this specific DMI failure occurring in conjunction with need for RV in an Emergency situation would be the only mitigation in such circumstances.	For Level 1 and 2, as the proposal from the ETCS On-Board for this RV ACK only arises after the driver has deliberately started to reverse the train, they will be expecting the ACK proposal, and would then ACK it in almost all cases. A spurious ACK by the DMI would have little impact. A spurious ACK when the train was not already reversing would also have no impact as the ETCS On-Board would reject. Accordingly, spurious ACK of RV request does not lead to a hazard.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			2. Driver able to adopt alternative Mode or isolate ETCS and reverse in time.			Failure to display (Output) the ACK message, or to send the ACK to ETCS On-Board (covered under DMI-05f) is an issue as reverse movement protection will be applied if the ACK is not received, which will be onerous because the reason for the RV mode functionality is to manage emergency situations.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						SRS 3.14.1.5 requires release of the Reverse Movement Protection (RMP) brake application at standstill with Driver acknowledgement (potential for common cause failure of DMI). Also, the type of brake application with RMP is not defined for interoperability (SRS 3.14.3.3 > 3.14.1.1). If the trainborne application design uses the emergency brake then there may be additional delay in resumption of movement due to a conventional train EB timer.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	7.	**DMI-01g:** Failure to display Air Tightness Control	1. Driver aware of need for Air Tightness Controls at specific locations (through lineside signalling, written instructions…). 2. Air Tightness control at specific location is only required for passenger comfort.	None - if the need to apply Air Tightness control is just for passenger comfort rather than for the protection of safety (e.g. due to atmospheric conditions or air pressure considerations).	None other than possibility that none of the passengers are susceptible.	Potentially directly Marginal (due to pressure chock or particles in tunnel) or Catastrophic (due to inhalation of toxic fumes in areas of external accidents, e.g. chemical power plants, fire in a tunnel). It shall be noted that the Catastrophic consequences can only occur in case of an external accident, e.g. in a chemical power plant.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			3. Air Tightness command is given by ETCS On-Board to the train. However, there is no harmonized requirement in the scope of the TSIs for such a train function. Therefore it cannot be credited here.			

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	8.	**MMI-2i:** Failure to present “LX not protected” information	1. This information is only needed when the level crossing is implemented without protections or there is a failure in a level crossing system so that the crossing is not protected 2. If the information is a text message: driver confirmation of text message	In case driver is not warned about the fact that the level crossing is not protected, it could lead to **LOSS**	1. There might be no road vehicle to collide with even if running through the unprotected LX at too high speed. 2. The driver could discover the faulty level crossing even if not warned by the ETCS On-Board, and might still be able to stop the train before colliding with the road vehicle. In modes in which an LX is not supervised, the ceiling speed is normally low.	This hazardous situation refers to both information: • the DMI symbol “LX status «not protected»” available in FS, OS and LS modes • the text message “Level crossing not protected” Because of the strength of the barriers, especially nr 2 and 3, ETA modelling is not warranted.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			3. Only in FS, OS and LS modes: In case the level crossing is not protected, the ETCS On-Board also supervises it, in addition to warning the driver.			
	9.	**DMI-01h :** Failure to present Display Distance to Target information	When DDT is used in an area, the driver should know it. He is Expecting that DDT is always displayed if a target exist. He is then able to know that a display error exist and will adapt its driving style (DRV INDICATION)	In case of low adhesion, driver is not aware that a target exists (he thinks he is still in normal ceiling speed monitoring without target).	Based on “Low Adhesion” Indication or external weather conditions, driver could run slower to anticipate (DRV STYLE LAF). This could nevertheless be against performance requirements where driver would be in the higher speed as possible.	This information is only useful in case of low adhesion (GOOD ADHESION). Note : An infrastructure manager could not use the technical “Low adhesion” information. In this situation, this information needs to be sent to the driver by another way.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				If the driver waits for DDT information to anticipate braking, “be lower than speed at target” cannot be guaranteed as braking curves are not adapted. ➔ Overspeed	Speed and distance to target are displayed when indication curve is crossed. Indication time could be sufficient to cover reduction braking capacity in some circumstances Target speed and distance are also available on planning area (DRV INDICATION)	Anyway, it will be the responsibility of the driver to start braking at the right time. Without DDT info, driver cannot anticipate braking and target speed cannot be guaranteed. → Overspeed Event tree related to this DMI-01H is exactly the same as those for MMI-2C (use of same reduction factor DRV INDICATION, GOOD ADHESION and DRV STYLE LAF)

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	10.	**DMI-01i :** Failure to present Time To Indication information	When TTI is used in an area, the driver should know it. He is waiting that TTI is always displayed when approaching indication to a target. He is then able to know that a display error exist and will adapt its driving style (DRV INDICATION)	In case of low adhesion, driver is not aware that the remaining time before indication to target is lower than a predefined time (he thinks he is still in normal ceiling speed monitoring without announced target). If the driver waits for TTI information to anticipate braking, "be lower than speed at target" cannot be guaranteed as braking curves are not adapted. ➔ Overspeed	Based on "Low Adhesion" Indication or external weather conditions, driver could run slower to anticipate (DRV STYLE LAF). This could nevertheless be against performance requirements where driver would be in the higher speed as possible. Speed and distance to target are displayed when indication curve is crossed. Indication time could be sufficient to cover reduction braking capacity in some circumstances Target speed and distance are also available on planning area (DRV INDICATION)	This information is only useful in case of low adhesion (GOOD ADHESION). Note : An infrastructure manager could not use the technical "Low adhesion" information. In this situation, this information needs to be sent to the driver by another way. Anyway, it will be the responsibility of the driver to start braking at the right time. Without TTI info, driver cannot anticipate braking and target speed cannot be guaranteed. → Overspeed

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Event tree related to this DMI-01I is exactly the same as those for MMI-2C (use of same reduction factor DRV INDICATION, GOOD ADHESION and DRV STYLE LAF)
	Note: HAZID 12.9, IS Mode indication absent is not a safety issue under Hazard H1, as this missing alone is a RAM issue (no other DMI output information is shown to the driver according to SUBSET-026 [Ref 1] 4.7.2). Absence of the IS Mode display removes the indication to a driver that the speed displayed may not be robust. This is covered under H3 as a cause of MMI-2a.1.					
	Note for Hazard H2: Information being displayed when it should not be may arise due to the DMI presenting incorrect information OR the DMI failing to remove information when it is no longer required. Whilst the internal failure mechanisms causing the error may differ, the functional failure at the system boundary is the same.					

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
H2 - Information displayed on the DMI when it SHOULD NOT have been	11.	**DMI-02a**: False presentation of Warning	Driver experience and skill.	Bounded by **UBA** Driver may over-react to situation and apply full service brake. Likely to be less onerous than UBA applied by ETCS intervention as braking rates can be managed by the driver.	No / negligible hazard. Full service brake unlikely to cause significant harm.	HAZID 12.4. This is not a hazardous situation, since the driver will respond by braking and check (Marginal consequence). The hazard will not limit the THR. Related to L0, L1, L2.
This includes "Spurious DMI output distracts train Driver"	12.	**DMI-02b**: False presentation of IS mode (shown as IS mode when not)	1. Driver training and experience.	**DISTRACTION**: IS mode is presented at DMI (according to SRS ch3) with another actual active mode. The driver may be distracted, as a result he misses safety relevant information (at DMI or at track side, for non-core hazard related information) which has a critical consequence.	Consequences and hence potential barriers will vary widely depending upon what specific information is missed. However, the same situation could occur from other distractions to a driver arising from other systems or activities (e.g. talking to train staff or a signaller).	HAZID 12.10. In the HAZID noted as Critical relating to L0, L1 and L2. As ETCS is still active, there is the potential for unexpected Intervention if the independent IS control is not operated by the driver but drives believing IS Mode is active.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			Most likely the driver will recognise that something unexpected has occurred with the DMI display, and so isolate the On-Board ETCS as concerned regarding its integrity, for which consequence is RAM and possible Distraction whilst assessing the situation.	**UBA**: Intervention occurs when driver not expecting it, believing they were in IS mode.		Note: As there has already been an initial DMI mode display error, there could be further DMI errors (or a common failure) which may limit the effectiveness of barriers 2 & 3.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			For UBA, the driver must believe the DMI IS status is correct without checking the independent IS control, and then there are two further barriers: 2. Driver must exceed intervention conditions (see comments) 3. Warning of intervention (see comments)			

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	13.	**DMI-02c**: False presentation of brake indication	Driver experience and skill.	Bounded by **UBA** Driver may over-react to situation and apply full service brake. Likely to be less onerous than UBA applied by ETCS intervention as braking rates can be managed by the driver.	No / negligible hazard. Full service brake unlikely to cause significant harm.	HAZID 14.1. Marginal consequence at worst. The likelihood of overreacting of full service brake by driver is low, and the hazard will not limit the THR. Relates to L0, L1, L2.
	14.	**MMI-2f**: Failure to display Override status (failure mode insertion), including false enabling of override selection	15.3 (UBA) The driver may notice the erroneous presentation and isolate the On-Board ETCS.	15.3 Bounded by **UBA**	**UBA**: None, but the likelihood of any significant injury occurring is considered minimal based upon experience of railway operations to date.	HAZID 15.3 & 15.4. 15.4 is where Overridden is not shown when it is (i.e. tripping is not active). 15.3 is where shown as Overridden when not (i.e. tripping is active). Additional special speed limits apply during Override (SRS 5.8.3.6 b) e.g. V_NVSUPOVTRP SRS 3 A3.2

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				Tripping shown inhibited while it is not. If this happens in the case of a procedure to override the end of authority it is likely the train will be tripped. Override speed limit(s) are nationally set, but their values are likely to be a reduced speed (thus marginal consequence). If it happens in other cases, the consequence is low.		

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	15.	**DMI-02e**: Spurious notification of Train Data change (which normally is from source different from the driver)	Driver experience and skill. Driver takes train out of service.	**DISTRACTION**: Spurious DMI output distracts train Driver. Note: UBA does not occur in this situation (unlike DMI-02b), as the indication is spurious and hence ETCS will not command service brake application to a stand. This difference is one of the features that may allow a driver to determine the notification as spurious.	As DMI-02b	HAZID 6.9. See SRS 5.17. The train would be expected to normally be at standstill for such actions to occur. If a train is moving, it is possible that certain train data (Train category, Axle load, Loading gauge, Power supply) could be changed, however, the ETCS would command service brake application to a stand and request the driver to acknowledge the new data. The presence of neither of these conditions should alert the driver to abnormal operation.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						The HAZID doesn't analyse the case of deletion of the notification. This could be hazardous if e.g. the driver is not notified of an increase in train length and stops the train at the wrong marker to let passengers off. To mitigate this, constraint nr 10 is exported in Appendix G.2; any train data from external sources that are safety critical for the driver to know about, must be validated by the driver. If this is implemented, the train data update procedure is halted if the driver doesn't validate the data, thus blocking further hazardous development.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	16.	**MMI-2c**: False presentation of track adhesion factor ("slippery rail" shown as applied when not)	Driver may notice spurious display. A genuine need to apply Poor Adhesion adjustment needs to occur. Driver should query why DMI shows poor adhesion already applied when requested to apply the control. In L0 or L1 OS and SR, the driver should already be taking account of the poor adhesion conditions from the original DMI display.	Variant of **OVS**. Similar to DMI-04h in that braking may be insufficient leading to overspeeding in a speed restriction or not brought to a stand within the safe distance. Driver does not apply poor adhesion request into the ETCS On-Board when required to do believing it in place already.	As OVS.	HAZID 13.6. An unjust presentation of bad adhesion may cause the driver not to modify into bad adhesion when needed. Non core hazard. Potentially Critical / catastrophic. Note : when DDT(61) or TTI(62) or nothing(63) is used, "False presentation" has no impact as the whole responsibility remains to the driver to have appropriate behaviour. Driver should know that maximum deceleration is not used.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			In L0 a TSR condition needs to be encountered.			In most L0 situations and in L1 OS and SR, the situation is performance limiting. In L0 the ETCS supervision for a TSR may become less effective or ineffective due to the poor adhesion factor not being applied.

						L1/L2 FS is also affected by this situation. An indication that ETCS had implemented the low adhesion condition when it had not, could lead to a supervised distance limit being exceeded in any Level / Mode. A significant complication in this situation is that in a genuine low adhesion situation there would be an input to the ETCS On-Board to select the low adhesion setting, and that should still work. However, if the input is a Driver selection (rather than trackside), and the Driver observes that it is already selected, the scenario being postulated here, this would not be covered by the $ETCS_{CH}$ as the Driver would not actually make the input to the ETCS On-Board.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	17.	**DMI-02g**: False presentation of “LX not protected”	Driver experience and skill.	Bounded by **UBA.** If the driver is falsely warned that there is an unprotected level crossing ahead, he will most likely reduce speed to be able to stop on sight. This is only a decrease in the availability of the train service. If the driver reacts by applying full brake, the event is likely to be less onerous than UBA applied by ETCS intervention as braking rates can be managed by the driver.	No / negligible hazard. Full service brake unlikely to cause significant harm.	This hazardous situation refers to both information: • the DMI symbol “LX status «not protected»” available in FS, OS and LS modes • the text message “Level crossing not protected” available in SB, FS, SR, LS, OS, NL, UN, TR, PT and RV modes This is not a hazardous situation, since the driver will respond by braking and check (Marginal consequence). The hazard will not limit the THR, but is modelled in the ETA to be consistent with the previously modelled DMI-02a.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
H3 - Erroneous but valid information displayed	18.	**DMI-03a**: Incorrect Geographical Position data displayed	**OVS**: 1. Normal arrangements insufficient such that GPI is used. 2. Speed restriction not applied via ETCS.	A) Where Geographical Position data may be used by a driver in support of a Written Order, an incorrect position could lead to the safe speed or distance being exceeded. The most likely scenario is where a speed restriction is not applied via ETCS, but instructed to a driver by track kilometres (e.g. in L0, or where the restriction does not apply to all trains or where it has not yet been implemented through infrastructure such as for unplanned restrictions).	As OVS	HAZID 11.2, 11.3 applies to L0 UN, but also applies to normal and degraded L1 & L2 operations. Scenarios could also occur on restarting trains after a revocation of MA (Op rule 06E222 6.16). These require the issue of a 'written order' to the driver to authorise recommencement. Could result in a collision between passenger trains and is a Non Core Hazard since it relates to re-instating ETCS control. In the case of Incorrect Geographical Position data being provided to the driver in the first instance, the hazardous situation could be immediate.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				OVS: Overspeed in specific circumstance at a speed restriction.		
			INAPP 1. Normal arrangements insufficient such that GPI is used. (as above) 2. Movement outside interlocking protection (e.g. major power failure, defect in train detection or interlocking operation forces degraded working).	B) Management of abnormal or degraded working between driver and signaller. Incorrect GPI given to a Signaller may lead them to undertake inappropriate authorisation. **Inappropriate Authority (INAPP)**: leading to authority given for something else to occupy the track ahead of the train: 1. **LXI**: User Worked Crossing (UWC) or exceptional load on automatic crossing.	1. LXI – UWC, probability of co-incident crossing use. 2. LXI – Auto, probability of co-incident exceptional crossing usage. 3. Engineering work in progress (if OBJECT). 4. Conflicting train movement required (Collision) 5. Driver may recognise GPI data is incorrect.	SRS 3.6.6: Geographic Position data is presented as a stated distance in relation to “track kilometre” (trackside chainage) i.e. absolute value not relative to any named location. Situations where points could be moved under a train were considered, but whilst technically possible, no practicable scenario involving passenger trains was identified without the need for a co-incident Wrong Side Failure of other elements of the signalling system.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				2. ENGINEERING: Collision with track worker (depending upon National track access arrangements and hence cannot be modelled as dangerous scenarios depend upon non interoperable conditions). 3. Collision between passenger trains or with other rail vehicle (L1 & L2 only). <different to OVS collision as no protecting signals> 4. OBJECT: Collision with object on the line (including engineering trolley). <modelled within INAPP>		**Safety Requirement SReq07**: The trackside application (engineering in combination with operational rules) should not put any safety reliance on the Geographic Position Information. Some examples on scenarios to avoid are presented in Appendix I. Because of this safety requirement, the DMI-03a scenario is not modelled in the event trees, and no safety integrity requirement is derived.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	19.	Incorrect train speed displayed when in IS mode	N/A – see comment	N/A– see comment	N/A– see comment	HAZID 12.9. The Safety Analysis workshop reviewed this further and concluded that the hazard could not occur. Whilst the SRS at 4.5.2 has an option for the ETCS On-Board to determine train speed whilst in IS Mode, 4.7.2 does not list the train speed display as being active or available. The inference of this apparent conflict between 4.5.2 & 4.7.2 is that the information is being generated for the JRU and not for the driver.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	20.	**MMI-2a.1:** False presentation of train speed N.B. an incorrect speed higher than the actual speed is performance affecting only – train travels slower than thought. A hazard only occurs where the displayed speed is lower than the actual speed.	1. Driver perceives the speedometer error and takes the train out of service. 2. The ETCS On-Board system still supervises the safe speed.	Overspeed (**OVS**) An overspeed could lead to issues arising due to the higher speed than expected, and as a consequence, exceedance of expected braking distance. Each of these along with secondary effects are dealt with below: <u>Speed Issues:</u> a) **RIDE**: Rough – Ride [L0 plus elements of L1 & L2 see Notes 3 & 4]. Note: Rough Ride and Derailment could arise from exceeding the permitted vehicle speed or from that limited by the infrastructure (line speed).	RIDE: None.	HAZID 10.2, 10.3, 10.4, 10.5, 10.6 in L0. In L0, to a large extent, ETCS supervision is minimal and the DMI train speed indication is functioning in the same manner as the Speedometer in non-ETCS fitted stock. One difference is that the ETCS DMI has a digital speed display and may exhibit different failure modes. Certain failure modes / impacts are covered under the $ETCS_{CH}$ where MMI-2a.2 relates to the display of supervision limits in the Movement Authority (e.g. permitted speed, target speed or distance). Non $ETCS_{CH}$ failures can occur in certain L1 and L2 modes – see Notes 3 & 4.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Workshop considered possible implications in FS/OS for applications which may require a driver to sight locally monitored level crossings [e.g. flashing white lights] and to confirm that crossing is clear. Also potential for reduced strike in distances for automated crossings. Normal operation of these crossings (train not stopping) is considered to be encompassed within the $ETCS_{CH}$ as the approach speed profile is assumed to be part of the train supervision speed profile [Assumption A1], and thus exceedance of the speed envelope even with an incorrect DMI speed indication is Core Hazard.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						However, in degraded modes where there is known to be a previous failure of some sort, the train may be approaching under a written order in FS/OS/SR, where an erroneous DMI speed indication may increase braking distances. Noted excessive speed could alter hazards to track workers (reduced warning times) and to the travelling public on platforms (increased suction from high speed passing train), however, these do not affect passengers on the train and so outside the scope of the THR being derived.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Note: There are some specific solutions that could be used as a barrier, such as diversification of speed dial and numerical value. These solutions are company specific.
				b) **DERAIL**: Derailment (highly unlikely) [L0 plus elements of L1 & L2 see Note 3].	DERAIL: Driver skill and lineside signalling / route information ensure speed through junction is regulated avoiding derailment.	
				c) **LXI**: Level Crossing incident (strike in reduced for automatic crossings) [L0 plus elements of L1 & L2 see Note 3].	LXI: The effect of the OVS on LX operation is dependent upon the following factors: 1. Crossing in normal or some form of abnormal operation.	In normal operation the only impact is a potential for the designed controls to be invalidated by the increased approach speed.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
					2. Crossing controls not invalidated by additional approach speed. 3. Crossing in Abnormal or Emergency operation. 4. Driver able to still brake sufficiently to avoid collision. 5. Excess speed does not invalidate degraded crossing operation.	Abnormal operation encompasses degraded and emergency operation. Abnormal operation includes the management of unusual situations such as abnormal loads or users on the crossing. An emergency situation reflects where the crossing may have become occupied during the train's approach, but is limited to the situation where a collision would have been avoided without the DMI failure but arises due to it i.e. the extra approach speed means that a collision occurs where it otherwise would not have.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Most of the identified mitigation and control measures can only be assessed within the context of the Operational Rules (potentially national considerations including type of crossing, route setting rules) and operational procedures for crossing usage.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				d) **GAUGE**: Structure gauge infringement (increased kinematic envelope).	GAUGE: Having not identified the excess speed, the only barrier to harm is the likelihood that a train encounters a structure that is within the expanded kinematic envelope.	This can only be assessed at National level in consideration of gauge requirements, characteristics of the routes and the expected magnitude of overspeed. It may be expected that collision with another moving train would not occur since it would be leaning in the same direction at the 'overspeeding' train. However, consideration should also be given to the potential for the kinetic envelope to the breached by a stationary train on an adjacent line since this will not be tilting.
				<u>Distance Issues:</u>		

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				In most cases the driver will be braking for the situation and the effect of the Overspeed is an extension of the stopping distance which may be accommodated in many instances by the defensive driving[9] techniques and the braking **capability** of the train. Collision would be low speed unless lying foul of a high speed line with minimal prior warning for the second train.		

[9] The actual degree of credit that can be taken for this in different scenarios is elaborated in Appendix F.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				a) **BUFFERS**: Collision with buffer stops [L0, plus elements of L1 & L2 see Note 4].	BUFFERS: Driver regulates approach using local markers, naturally compensating for any speedometer error.	
				b) **COLLISION**: Collision with another train[10] [L0 plus elements of L1 & L2 see Note 3] c) **COLLISION:** Collision between passenger trains [L0 plus elements of L1 & L2 see Note 3].	COLLISION: 1: Driver may be able to brake to a stand short of the junction fouling point. 2: Second train may not be approaching or may be stopped short of a collision by other protection systems (e.g. NTC, ATP, TPWS). 3: If collision avoided, the reduced train speed may be sufficient for the train not to derail if the points are run through.	

[10] 'another train' addresses instances such as Engineering Trains in a Possession or a Freight train

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
					4: The train may stay upright after running through the points thereby reducing the impact on passengers.	
				d) **OBJECT**: Collision with object on the line.	OBJECT: 1. Driver may still be able to brake the train to a stand short of the object or obstruction.	If approaching under a written order in FS/OS/SR/LS, any erroneous DMI speed indication is likely to have a minimal impact as the driver is required to be able to bring the train to a stand upon sighting a problem. If there is no prior warning of an object on the line, then a driver would be unlikely to be able to stop short of the object even with a correct displayed speed i.e. the DMI error has a minimal impact.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				e) **DERAIL**: Derailment (over running junction with points set for lower speed turnout, trap points, intentionally missing infrastructure [Engineering Works, Swing Bridge].	As above for speed.	
				f) **PLATFORM**: Incorrect station stop position (Disembarkation injury) [L0, 1 & 2].	PLATFORM: 1: Driver compensates stopping position using local markers. 2: Platform length sufficient that doors still open onto platform. 3: Selective Door Opening available and used to prevent egress where unsafe. Where no SDO the driver and train staff manage the situation using local announcements.	Incorrect station stop position may be managed by Selective Door Operation (if available) or not releasing the doors until the local management of the overrun was in place.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
					4: Passengers recognise that unsafe to disembark and remain on the train.	
				g) **NON STOP**: Non stopping zone infringed.	NON STOP: 1. Overrun of intended stopping point is not within a Non-Stopping Zone.	The full consequences can only be assessed at national level taking into account the nature of the non-stopping zone (what it is protecting) and the Operational Rules for recovery of a train that had entered one.
				h) **LXI**: LX infringement (overrun onto vehicle on the crossing).	As LXI above.	

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				i) **INCOMPATIBLE**: Train is incompatible with the infrastructure (e.g. traction, track gauge, structure gauge).	INCOMPATIBLE: Consequences are considered to be RAM only with regard to traction, track gauge. Infrastructure gauge infringement due to not being able to stop short of the point of conflict between train and infrastructure is the only harm scenario of this Immediate Effect.	**Note**, this does not refer to the ETCS Route Suitability function, which only applies in FS and OS in Level 1 and 2. The concern here is not related to implementation of the Route Suitability ETCS function, but that due to overspeeding in Level 0, or Level 1 or 2 in other than FS / OS, a driver is unable to stop short of the point of conflict between train and infrastructure. Similar reasoning applies to infrastructure gauge infringement.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	21.	**MMI-2b:** False presentation of mode	1. The Mode displayed may conflict with current operation / displayed information presented, Note: For a change to a lower level of supervision and protection, the Driver will have had to accept an ACK of Mode change, but it is critical to establish whether the driver understood this	Loss of Supervision (**LOSS**) Driver believes a limit is being supervised due to the Mode indicated (e.g. FS) via the DMI having a higher degree of supervision than the ETCS On-Board actually applies (e.g. UN, OS, SR, LS). Driver may rely on alert indication that will not be generated.	Driving style based on route information or respect of line-side information means that intervention limits are not breached. **LOSS** in turn may lead to **OVS** if the above limited mitigation is un-successful.	HAZID 7.2 and 7.3. Concerns L0, L1 and L2. Concerns non-core hazard for exceeding the safe speed or distance which is not advised to ETCS, see Note 3). The most onerous scenario would be if a driver had a driving style that relied upon Alerts or Warnings to prompt initiation of braking. Note I: Model LOSS in the same manner as Incorrect Speed Display leading to transfer to OVS.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Note II: A frozen Mode icon might be easily recognised in relation to the rest of the displayed information. A genuine change to a Mode of reduced supervision and protection that is incorrectly displayed as a still lower mode than the original may be harder to identify (e.g. change from FS to SH but OS is displayed). **Design Consideration**: The ACK request message should include specific detail of the proposed change rather than just a “generic” ACK statement that relies upon the rest of the DMI display to determine what the change has been.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Design Consideration: The ability for a driver to be able to review recent commands and messages (rather than just alarms) would permit checking back what had just occurred. For example, if the ACK was provided as a reflex due to the current driver priorities, and there was a need to look back to the specific details subsequently when time was available.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	22.	**DMI-03c:** Wrong acknowledge-ment request displayed	1. Request is not valid for the current Level / Mode or conditions and driver recognises this fact.	If the driver acknowledges the wrong request, the ETCS On-Board will implement the change according to the request it sent via the DMI, which is not the request the driver believes they have accepted. The principal impact of this is to enter a mode that the driver may not be aware of, which is similar to MMI-2b, 'False presentation of mode'.	As for relevant MMI / DMI event that it may cause e.g. MMI-2b, DMI-04d, MMI-1a, MMI-1d and MMI-1f. The ETCS On-Board will send the correct, valid, Mode to the DMI which may alert the driver to the fault as the displayed Mode will differ from that which the driver is expecting.	This Hazardous Situation is principally a method of entering into a different mode / level than the driver expected, so it is a LOSS situation if the new Mode / Level has reduced supervision and protection, or any of the erroneous acknowledgment situations covered under DMI-04d, MMI-1a, MMI-1d and MMI-1f.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						All these events are false acknowledgements. The connection with DMI-03c is thus that it is displayed one reason for acknowledgement while it is sent another acknowledgement to the ETCS. Therefore, this Hazardous Situation does not need to be modelled separately but its likelihood should be accounted for in assessing the above specific situations.
	23.	**DMI-03d:** Wrong Trip Reason displayed	1. The train is at standstill after the trip. 2. The driver may note that trip reason by other means than the DMI output.	Erroneous information to the driver about the reason for Trip could mislead him in recovering from a trip situation in the correct way, potentially leading to Overspeed (**OVS**).		With barrier 3, ETA modelling is not warranted.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			3. After a trip, the driver shall assume that there is a dangerous situation and he shall perform all actions necessary to handle this situation with the help of the signalman who knows which train movements are safe. There should be no need to place any reliance on the DMI output Trip Reason. This is brought forward to the exported constraints.	For example if the train is tripped because it has overpassed the End of Authority with its min safe front end (being potentially very close to the danger point), but the driver is informed that the trip is because of a linking error, he could request from the signalman to proceed with override in SR mode.		

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	24.	**DMI-03e:** Wrong fixed text message displayed	**Text message "Level crossing not protected"**: As for MMI-2i, but here, the confir-mation barrier (nr 2) of MMI-2i cannot be credited, since the driver might confirm this erroneous text message without having understood that the upcoming LX is not protected.	Potentially direct catastrophic	As for MMI-2i	As opposed to MMI-2i, this refers to only the text message, not the DMI symbol that can be shown in FS, OS and LS modes. The corruption of this symbol can be considered as covered by the deletion of it, which means it is covered by MMI-2i.
			Text message "Acknowledge-ment":	Potentially direct catastrophic		This message is intended to confirm that the driver is aware of an unsupervised speed restriction ahead. When the driver receives this message, they shall look

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			1. The driver might understand that the erroneous text message is out of its context and therefore not confirm 2. The driver is already in full control and doesn't need the reminder			out of the cab window and search for the relevant speed restriction. But the driver is anyway responsible for obeying the lineside signalling when there is an unsupervised speed restriction and should have their full attention to it. This text message can add only little safety and doesn't need to be modelled in the analysis, providing that the ETCS On-Board is already in a mode where the driver is responsible for knowing all speed restrictions, such as LS. This is noted as Exported Constraint 11

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	25.	**DMI-03f:** "Tunnel stopping area" displayed at the wrong geographical place	1. The driver realizes this is not the correct safe area and therefore doesn't initiate evacuation 2. Probability for no fire in the tunnel	Potentially directly catastrophic if the need for evacuation was in an Emergency situation		The hazardous scenario is that the driver and train crew evacuates the passengers at a location where there is no emergency facility. The passengers are exposed to fire or toxic fumes.
	26.	**DMI-03g :** Wrong Display Distance to Target information	The driver realizes these values are not correct as not in line with planning area (with assumption of independencies between DDT and planning area information) (DRV INDICATION)	Driver make wrong evaluation and could start to brake too late ➔ OVERSPEED	Based on "Low Adhesion" Indication or external weather conditions, driver could run slower to anticipate (DRV STYLE LAF). This could nevertheless be against performance requirements where driver would be in the higher speed as possible.	This information is only useful in case of low adhesion (GOOD ADHESION). Note : An infrastructure manager could not use the technical "Low adhesion" information. In this situation, this information needs to be sent to the driver by another way.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
					Speed and distance to target are displayed when indication curve is crossed. Indication time could be sufficient to cover reduction braking capacity in some circumstances Target speed and distance are also available on planning area (DRV INDICATION)	Anyway, it will be the responsibility of the driver to start braking at the right time. Without DDT info, driver cannot anticipate braking and target speed cannot be guaranteed. → Overspeed Event tree related to this DMI-03G is exactly the same as those for DMI-01H (both are bounded by the ETCS automatic protection)

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	27.	**DMI-03h :** Wrong Time To Indication information	The driver realizes he approach the indication point in planning area(with assumption of independencies between DDT and planning area information) (DRV INDICATION)	Driver make wrong evaluation and could start to brake too late ➔ OVERSPEED	Based on “Low Adhesion” Indication or external weather conditions, driver could run slower to anticipate (DRV STYLE LAF). This could nevertheless be against performance requirements where driver would be in the higher speed as possible. Speed and distance to target are displayed when indication curve is crossed. Indication time could be sufficient to cover reduction braking capacity in some circumstances Target speed and distance are also available on planning area (DRV INDICATION)	This information is only useful in case of low adhesion (GOOD ADHESION). Note : An infrastructure manager could not use the technical “Low adhesion” information. In this situation, this information needs to be sent to the driver by another way. Anyway, it will be the responsibility of the driver to start braking at the right time. Without TTI info, driver cannot anticipate braking and target speed cannot be guaranteed. → Overspeed

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Event tree related to this DMI-03H is exactly the same as those for DMI-01I (both are bounded by the ETCS automatic protection. A small reduction factor could be added with regard DMI-01I as it is better to have a bad information than no information in this case. This would nevertheless not reduce so much the target)

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
H4 - Erroneous but valid input to the ETCS On-Board via the DMI	28.	**DMI-04a:** False command to exit shunting	Train must be at standstill. The driver may note the change to SB mode and does not accelerate. Train staff must be aboard train.	Bounded by **UBA** The driver is not aware that the mode changed from SH to SB, accelerates and ETCS intervenes with a brake command after a distance which is a national value). Hazard is from additional jerk motion by loosely coupled train, rather marginal, and not for passengers.	Jerk effect is similar to the low speed UBA scenario. This situation may be considered bounded by UBA given that there is a prior conditioning probability here that there are train staff present on the train, whereas there are always passengers at potential risk in the UBA situation.	HAZID 16.6. L0,L1,L2 The HAZID assigned the consequence severity as Critical. Whilst this is possible in a worst-case situation, a minor injury is far more likely.
	29.	**DMI-04c:** False START command	1. Must be in SB mode.	**LSP**: Unexpected loss of standstill protection.	a) Driver should not rely on ETCS mode to keep the train stationary. b) Open door interlock (if fitted) prevents start away from Station.	HAZID 1.2 Does not apply to L2 since the RBC will not give a MA. Could result in a proposal to the driver to accept the corresponding mode (L0 : UN, L1: SR)

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			2. In L0 driver must accept proposed UN mode without awareness of the consequence (reflex acceptance). Similar in L1 for accepting SR mode.	For loss of standstill protection the consequence is critical. Train movements could occur with open doors at platforms if not interlocked. Passenger injury occurs through falling from moving train or being knocked over whilst embarking / disembarking.	Note: Depending on the direction controller, which will likely be in neutral position as the driver is performing a SoM, the Roll Away protection (RAP) will brake the train after a few metres, the exact value being configurable and Nationally set. In this manner, RAP is similar to standstill supervision. Whilst this will stop hazards associated with a train running away, it does not protect against the potential harm addressed here of injury to passengers embarking & disembarking.	The scenarios arise where the train mode is altered by the spurious insertion of certain requests or acknowledgements to the ETCS On-Board which the driver may not be aware of. The action of SB mode to prevent train movement is then defeated, potentially without the driver being aware of this. This situation arises every time a driver presses START. The driver's training to maintain the train stationary should be robust, and therefore it is unlikely that a train would not be held braked in the incidences where the START request was due to a DMI error.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			3. In L2, the RBC could issue an FS MA immediately, and so no barrier of protection. If an FS MA not is initially available, RBC could send OS MA, SH MA or SR authority, each of which would require reflex acknowledgment to initiate LSP.			**Safety Requirement SReq09**: Drivers should not rely upon Standstill Protection as the primary means of holding the train stationary.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	30.	**DMI-04d**: False UN acknowledgement.	Must be in SB and L0. Driver interrupted after pressing START when ETCS On-Board has presented a proposal for UN.	**LSP** – as Level 0 parts of DMI-04c The likelihood of being interrupted immediately after requesting start and the DMI falsely acknowledging UN is very low.	as Level 0 parts of DMI-04c	HAZID 4.1. Only applies in L0. Routine start-up would be to select START immediately followed by accepting UN when proposed by the ETCS On-Board. To be in UN without the driver's knowledge they would need to have been distracted between requesting start and completing the deliberate adoption of UN.
	31.	**MMI-1g**: False request for SH Mode	1. Must be at a standstill when false SH request issued. No additional protection in L0 and L1 scenarios except:	L0: 1.1 If in SB mode, then **LSP** as DMI-04c.	**UBA**: None **LSP**: as DMI-04c **LOSS**: As MMI-2b , with the additional barrier of area might be protected by balises (Stop-if-in-SH, List-of-balises-in-SH) or RBC (if it does not grant the mode transition).	HAZID 16.2 Failure can also result in a loss of supervision (LOSS) as SH mode if in FS or OS at the time of the fault.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			2. Driver may notice the change of mode. 3. In L2, the response of the RBC to the SH request is not harmonized within the scope of the TSI CCS. The response will depend upon product design, application design and Operational Rules. This barrier can therefore not be credited.	1.2 If in UN, **UBA** upon departure (if ceiling speed in SH is lower – National value) or when moving if trackside is protected against erroneous circulation in SH mode L1: 2.1 If in SB mode, then **LSP** as DMI-04c. 2.2 **UBA** upon departure (if ceiling speed in SH is lower than the current permitted speed of the mode he thinks he is in) or when moving if trackside is protected against erroneous circulation in SH mode.	**OUTWITH**: Possible mitigation: 1. The DMI is the prime interface for the driver. If the driver checks the DMI before starting away then the Mode change would be revealed as the expected information would not be present if SH mode had been spuriously adopted.	In Level 2, it is the responsibility of the trackside implementation to ensure that suitable controls and / or Signaller's authority is obtained as part of SH authorisation procedure. Such considerations are outside the scope of this study, and not credited as a barrier.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				LOSS if in FS or OS, (if remains below SH ceiling speed and trackside is not protected against erroneous circulation in SH mode). L2: 3.1 as 2.1 3.2 as 2.2 3.3 **OUTWITH –** operation outside the control of the signaller and signalling system as train in SH mode, no longer communicating with the RBC, with the driver potentially believing they remain in the original mode with a valid MA. See notes in comment field.	2. If L2 area still has line side signals these provide driver with an MA and interlocking control. (N.B. The Interlocking will prevent conflicting moves of other trains against the affected train, but it cannot protect against the affected train adopting movements that may cause it to collide with something else including a train on the line ahead).	

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
				Also **LOSS** as in mode with reduced supervision and protection. Catastrophic consequence.	Once the train is not under the control of the RBC it is not certain that it is within Interlocking control. Thus, a second train could potentially be routed in conflict. Protection against this is dependent on the non-interoperable application / design of the RBC and Interlocking systems.	
	Notes on MMI-1g and related scenarios: a) In L0 and L1 the Driver can have an authority to move with control via lineside signals, although the movement may actually be unprotected by ETCS, e.g. in SH Mode the end of the authorised move may not be supervised in L1, and is not for L0. In L2, this may not apply, depending upon how the application design is developed. However, at least one application is known to be proposing to automatically authorise SH mode when in L2. This would remove a train from RBC control and, if the SH request was due to a DMI error, the train may not be under appropriate procedural control (Operational Rules). b) The DMI spuriously Acknowledging a valid request for Acknowledgement has the same effect as the DMI spuriously requesting SH Mode from a Level where it is accepted automatically. The spurious acknowledgment is part of the core hazard and it is included in SUBSET-079 [Ref 3] as MMI-1a “False acknowledgement of mode change to less restrictive mode.					

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	c) MMI-1g concerns only the request to change to SH mode. However, a related mode is the PS, which can be entered (only from SH) triggered by a similar request: “Continue Shunting on desk closure”. A separate hazardous situation is not created for this request, but it is instead analysed here: • An erroneous Deletion of this request will not lead to any hazardous consequences since the ETCS On-Board will then change to the more restrictive SB mode at desk closure instead of PS mode. • An erroneous Insertion of this request will at desk closure send the ETCS On-Board to PS mode instead of SB mode. The “passive shunting” input signal from TIU protects against unwanted transition to the less restrictive PS mode. In summary, ETA modelling is not warranted.					
	32.	**DMI-04f:** Spurious or wrong language requested distracting the train Driver	1. Driver recognizes the change of language before potential to be misled.	The downstream impact should a driver attempt to use a language for which they are not fully conversant, is not a specific risk in itself, but a performance shaping factor of the other scenarios already covered herein for DMI failures.		HAZID 6.8 This is a H4 category since the DMI selects the language by Insertion.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			2. Driver either competent in the new language or should take ETCS out of service if not able to reselect required language (Operational / RAM impact)	This failure is therefore not limiting in terms of any downstream Immediate Effect, since it is conditioned by the stated Barrier / Shaping Factor.		
	33.	**DMI-04g**: Spurious request to change to another ETCS Level	**All**: Train must be at standstill. 1. **Distraction**: no barriers. 2. **LOSS**: Barriers to preclude the reduced ETCS Level being adopted are:	1. **DISTRACTION**: 2. **LOSS**: Operation in L0 from L1 or L2 will have less protection. A catastrophic consequence is possible.	**DISTRACTION** – shaping factor on other scenarios. **LOSS**:	HAZID 13.2 Most likely scenario is Distraction, which does not lead directly to a hazard. Should the train remain unrevealed in L0 then more onerous consequences would occur. Also applies to transition to Level NTC, but consequences likely to be bounded by those of transition to Level 0.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			a) Application and Operational rules may limit the conditions for adoption (see Comments). b) Driver, observation of Level change. For change to Level 0 the information displayed will also change e.g. no presentation of target speed. c) If moving from L2 to L1, in a L2 area without line side signals (i.e. not an overlay application) the driver will more easily recognise the loss of MA.	Note: Spuriously requesting L1 or L2 from L0 has been considered as not safety related in the HAZID study.		It is possible for a Level change to occur that is not the result of a normal transition from one Level to another by moving from one infrastructure area to another whilst the train is moving. The SRS details how this is done in a number of places e.g. Start of Mission (in section 5.4.4) and fall-back situations (in clause 3.18.4.2.4). This is further clarified in SRS 5.10.2.9 and 5.10.2.10.1. In all instances, Level change can only occur at standstill.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Therefore, the rules for adoption provide protection. Whilst SRS 4.7 indicates the input as “additional data”, which may be possible on the move, this cannot force a level change whilst on the move. The driver does not need to acknowledge the level change as it has been initiated by them. If the ETCS Level increased, this would provide additional protection and thus has not considered further.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	34.	**DMI-04h:** Spurious acknowledgement of release emergency or service brake (after Intervention)	None (to UBA) 1. Driver action to re-apply brake.	**UBA** Potentially Catastrophic hazard if the standstill, reverse movement or rollaway was defeated.		A spurious ACK due to a DMI failure could remove the applied brakes after an ETCS intervention without the driver being aware of this. Should train movement then occur, the standstill, reverse movement or rollaway protection would act providing an Unexpected Brake Application (UBA).

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Of more concern is the potential to, in practical terms, defeat the standstill, reverse movement or rollaway protection if the automatic acknowledgement was a systematic failure that remained present, so that the spurious ACK was repeatedly sent. In such circumstances, the “Intervention - auto ACK - non-permitted train movement – Intervention” cycle would repeat continually, defeating the standstill, reverse movement or rollaway protection, albeit as a series of start/stop sequences.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						It is considered unlikely that a Driver would permit such a situation for long unless incapacitated or absent, and the situation may be affected by other factors relating to the train systems design, operating procedures and Operational Rules.
	35.	**DMI-04j:** False Isolation command	None	**LOSS** Unwanted transition of ETCS On-Board to IS mode (could also be considered as $ETCS_{CH}$, but is analysed here anyway for completeness)	The driver could discover that the ETCS On-Board has transited to IS mode and take safe action. See exported constraint 13.	The DMI shall offer a means to isolate the ETCS On-Board equipment. Although implementation dependent, it is expected that a switch which is separated from the driver's screen is used for this purpose. See exported constraint 13.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	36.	**MMI-1a** False acknowledge-ment {by DMI} of mode change to less restrictive mode	DMI failure must occur within the 'rectangle' (acceptance window).	**LOSS** For L0 this means a mode transition to UN, as well as a level transition - identical to "MMI-1d – False acknowledgement of Level Transition (Safety Related)" Mode change whilst remaining in same level (L2 & L1) – as MMI-2b. This may lead to a catastrophic consequence.	Similar to MMI-1d and MMI-2b. Driver may notice the change in Mode (if the DMI display functions are unaffected by the earlier failure)	There is a HAZID defined for mode transition to UN: 4.1. MMI-1d is identical to HAZID 18.3
	37.	**MMI-1b** False Command to enter NL mode	For mode change to NL to be accepted by the ETCS On-Board: - the train must be at standstill and	**LOSS** & **OUTWITH**: All ETCS protection and supervision is lost (except for ceiling speed). Catastrophic consequence	1. Drivers recognizes the NL mode 2. If accepted by the ETCS On-Board, i NL mode will be shown to the Driver unless prevented by a CCF/CMF with the spurious request.	HAZID 17.2 Applicable in L0, L1 & L2.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			- the non-leading input signal must be received			
	38.	**MMI-1d** – False acknowledge-ment of Level Transition	1. ETCS On-Board accepts acknowledgemen t only when the max safe front end of the train passes a trackside defined location in rear of the level transition border, thus a valid request must have co-incidentally occurred.	**LOSS**: The driver may not be aware that a Level with lower safety protection has become active (from L1 or L2 to L0 only). This may lead to a catastrophic consequence.	1. Level transitions will be at fixed locations, increasing the likelihood that the driver notices the difference using lineside signalling, written instructions... 2. Driver expecting the change, and therefore the driving style may remain appropriate, as the change is routine whether he has accepted it or it has spuriously been acknowledged. 3. Driver notices L0 displayed on the DMI Note: Considered to be minimal impact compared to other LOSS scenarios.	HAZID 18.3 L2 to L1 Transitions do not need acknowledgement (SRS 5.10.4.4). Acknowledgement is only required for entering L0 or leaving/entering NTC. Could also occur at start of mission following occurrence of Hazardous Situation DMI-04g. As this requires additional failures and DMI-04g also leads to LOSS, this additional cause is not modelled explicitly.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
			2. Most likely the transition has been announced to the driver (at DMI and by lineside signage) and the driver has noticed that.			Note: Transitions from L2 or L1 to Level NTC should be bounded by those to Level 0, since Level NTC provides supervision and protection through the National system(s). The case of false acknowledgement of an NTC Level which is not supported by the On-Board is not analysed here, since it implies double failures (ref clause 6.2.1.9); both a corrupted level transition order and a false acknowledgement.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						It is very difficult to quantify the expectation window where the ETCS On-Board is waiting for the level acknowledgement after sending the level change request to the driver. Nevertheless, a conservative approach can be assumed, since the time spent on a level transition area is very small compared to the operation time.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						It is possible, but unlikely, that false acknowledgements could be continually or periodically occurring. Whilst the ETCS On-Board would be expected to reject them as there would usually be no valid Level transition ‘active’, such a scenario would increase the likelihood that a genuine Level transition would be falsely acknowledged.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
						Similar situations could occur for other acknowledgments. It is not standardized how the DMI caters for the presentation of alarms and the monitoring of data logs. It would be good practice to routinely check logs for the presence of false requests or repeated rejection of requests by the ETCS On-Board. Similarly, it is not standardized what indication the driver gets if a spurious acknowledgement or request is rejected by the ETCS On-Board.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	39.	**MMI-6:** Falsification of Virtual Balise Cover (failure mode corruption, see comment)	Only for E1: Trackside may send a new list of Virtual Balise Cover that is appended to the older one. This is however a weak barrier which is not credited, see further NEW VBC in Appendix E.	**LOSS** The wrong balise will be ignored, which means that (E1) A balise that should have been ignored will be read, and (E2) A balise that should have been read will be ignored This could have virtually any effect inside ETCS. As bounding case, LOSS is used.	1. The driver discovers that the wrong VBC is active and takes safe action. It is not expected that the driver has been instructed to perform a check in addition to what is implicitly part of the set+validation procedure. 2. Only for E2: The erroneous VBC doesn't match the VBC of a balise that the train encounters. 3. Only for E2: The loss of balise information could be not hazardous. 4. Only for E1: The balise information contains no hazardous data.	Effect E1 is considered to be the most limiting effect, considering the mitigations and their quantification in Appendix E (mitigation nr 2 is NO VBC MATCH, nr 3 is BALISE MISS NOT HAZ and nr 4 is BALISE DATA NOT HAZ), and is therefore the one modelled in the ETA. The analysis serves as a bounding case also for the failure mode deletion. SUBSET-079 **[Ref 3]** considers this as Core Hazard. However, it is a matter of definitions and included in this study anyway for completeness.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
					5. Not all operation is done with a VBC active. Failures in the components causing VBC corruption is most likely discovered from other reasons even when the VBC function is not used.	
	40.	**MMI-6:** Falsification of Virtual Balise Cover (failure mode insertion, see comment)	ETCS On-Board allows the driver to change VBC only at SoM	**LOSS** This means that (E2) A balise that should have been read will be ignored This could have virtually any effect inside ETCS. As bounding case, LOSS is used.	1. The driver could discover that a VBC is active and takes safe action. However, it is not likely, since he has not tried to activate a VBC and thus he has no reason to check. 2. The erroneous VBC doesn't match the VBC of a balise that the train encounters. 3. The loss of balise information could be not hazardous.	The failure referred to here is a spurious VBC sent to the ETCS On-Board. SUBSET-079 **[Ref 3]** considers this as Core Hazard. However, it has been included in this study in order to keep all the modelling that was performed before including it in the mentioned SUBSET.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	41.	**MMI-1e** False acknowledgement of Train Trip	No barriers.	Occurrence in L1 or L2 is ETCS Core Hazard.	None	HAZID 5 Hazardous Situation removed from assessment as ERA meeting on 25/09/09 confirmed that this is accepted solely as a Core Hazard. No 'non-core' hazards identified.
	42.	**MMI-1f** False acknowledgement of Track Ahead Free	No barriers.	TAF in L0 is not defined. As for MMI-1e above.	None	HAZID 20.1 As MMI-1e above.
	43.	**MMI-1h** False acknowledgement of undesired train movement (RAM, RMP, SSS)	Reinitializing of RAP/RMP/SSS function using new train position	Occurrence in L1 or L2 is ETCS Core Hazard.	None	No 'non-core' hazards identified.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	44.	**MMI-1h** False acknowledgement of undesired train movement (PT distance)	System keeps PT mode and supervised distances shall be identical	Occurrence in L1 or L2 is ETCS Core Hazard.	None	No ‘non-core’ hazards identified.
	45.	**MMI-1h** False acknowledgement of undesired train movement (reversing distance)	System keeps RV mode and supervised distances shall be identical	Occurrence in L1 or L2 is ETCS Core Hazard.	None	No ‘non-core’ hazards identified.
	46.	DMI spuriously requests removal of Track Adhesion Factor (part of **MMI-3** in SUBSET-079 **[Ref 3]**)				This is considered to be Core hazard because the hazardous situation involves the reduced track adhesion (which gives a more restrictive supervision) that is being correctly applied, but then removed because of an ETCS On-Board error.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
H5 - Deleted input to the ETCS On-Board via DMI	47.	**DMI-05a:** Deleted Level transition acknowledgement	None	Bounded by **UBA**: Service brake application occurs directly. Impact similar, but marginally less severe than an Unexpected Brake Application (UBA).	None, but the likelihood of any significant injury occurring is considered minimal based upon experience of railway operations to date.	L0 HAZID 4.2 and 18.3. Also Level NTC transitions. ETCS On-Board accepts the ack only when inside the "rectangle" (5s), thus “Timing” can also cause this Hazardous Situation as well as absent.
	48.	**DMI-05b:** Deleted acknowledge-ment	None	**UBA:** If request is not acknowledged within the timeout ETCS will intervene.	As DMI-01c.	Equivalent hazardous situation to DMI-01c (failure to display request to driver).
	49.	**DMI-05c:** Deleted request for GPI.	As DMI-01d	As DMI-01d	As DMI-01d	This is the corollary of DMI-01d, where the same effect as the DMI not displaying information arises due to the request not being sent to the ETCS On-Board, which in turn leads to the DMI not being provided with said information to display.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	50.	**DMI-05d:** Deleted change of language request.	As DMI-04f	As DMI-04f	As DMI-04f	This is the corollary of DMI-04f, where the same effect as the DMI providing an incorrect display can arise due to a spurious request being sent to the ETCS On-Board to change the language. As most information is displayed graphically or numerically, a change of language will only have a limited effect, most likely RAM / operational delay. However, text based information could result in a hazard arising if not correctly understood.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	51.	**DMI-05e:** Deleted driver request to apply Track Adhesion Factor.	Driver confirms that Track Adhesion Factor request has been applied by the ETCS On-Board	Driver is aware that no additional protection is taken by ETCS On-Board (no icon) and need to adapt its behaviour. If not, driver could start to brake too late (DRV INDICATION SLIPPERY) ➔ OVERSPEED	Similar to MMI-2c.	If icon ”Low adhesion” is not displayed, driver should request again and adapt his behaviour
	52.	**DMI-05f:** Deleted Reversing mode acknowledgement.	Similar to DMI-01f	Similar to DMI-01f	Similar to DMI-01f	Similar to DMI-01f. Change to RV mode would not be implemented by the ETCS On-Board, reverse movement protection would be applied. Adoption of another mode (e.g. NL or isolation of ETCS) may not be possible in time to permit movement in an emergency situation (see DMI-01f for further details).

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	53.	**DMI-05g:** Deleted “PT distance exceeded” acknowledgement	Brakes remain applied not allowing any further movement (Operational / RAM impact)	Vehicle cannot proceed in any direction.	None.	The train brakes will remain applied and further reverse movement will be blocked. Final situation is identical to the case where acknowledge is sent and brakes are released: when ERTMS/ETCS equipment detects further movement in the direction opposite to train orientation, service brake is commanded.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	54.	**DMI-05i:** Deleted “reversing distance exceeded” acknowledgement	Brakes remain applied not allowing any further movement (Operational / RAM impact)	Vehicle cannot proceed in any direction.	None.	The train brakes will remain applied and further reversing will be blocked. Final situation is identical to the case where acknowledge is sent and brakes are released: when ERTMS/ETCS equipment detects further movement in the direction opposite to train orientation, service brake is commanded.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment
	55.	**DMI-05j:** Deleted Isolation command	1. The reason for needing to reverse is for emergency purposes to avoid a conflict or incident. 2. Driver able to adopt alternative method for reversing in time e.g. RV or SH mode (anyway the IS command is just a backup in this situation).	If the need to reverse is for emergency (mitigation) purposes, then catastrophic failure is assumed.	None	The probability of the emergency need for IS mode is judged to be extremely low. ETA modelling not warranted.
	56.	**DMI-05l:** Deleted Train Trip acknowledgement	Brakes remain applied not allowing any further movement (Operational / RAM impact	Vehicle cannot proceed in any direction.	None.	The train brakes will remain applied, the train stays in TR mode and further movement will be blocked.

Top-Level DMI Hazard	Line No.	Hazardous Situation	Barriers / Shaping Factors	Immediate Effect	Mitigation & Controls	Comment

	57.	**MMI-6:** Falsification of Virtual Balise Cover (failure mode deletion, see comment)	Trackside may send a new list of Virtual Balise Cover that shall replace the older one	**LOSS**
				This means that
				if 'Set VBC' is deleted:
				(E1) A balise that should have been ignored will be read, or
				if 'Remove VBC' is deleted:
				(E2) A balise that should have been read will be ignored
				This could have virtually any effect inside ETCS. As bounding case, LOSS is used.
					As for Falsification of Virtual Balise Cover (failure mode corruption).	The failure referred to here is that the driver intends to set or remove a VBC marker for a balise, but the input is deleted in the transmission so that the VBC information doesn't reach the ETCS On-Board.
						This is a sub-case of MMI-6 (failure mode corruption) and therefore covered by that analysis. Further modelling in Event Tree not warranted.
						SUBSET-079 **[Ref 3]** considers this as Core Hazard. However, it is a matter of definitions and included in this study anyway for completeness.

The following Notes apply to Hazard Schedule:

Note 1: Intentionally deleted.

Note 2: Plain text messages are not explicitly addressed in this safety study, as it is agreed that they shall not be used for safety applications unless e.g. other information/communications between the two parties concerned is provided – see clause 3.2.1.6.

Note 3: Applies in L0, but also L1 and L2 (still outside the $ETCS_{CH}$) for modes:

- LS since ETCS does not have all information necessary to safely supervise the train speed and distance
- SR for a degraded situation or Start of Mission
- OS since ETCS does not supervise approach to an obstruction
- SH since $ETCS_{CH}$ only covers supervision to Ceiling Speed
- FS and OS degraded with a verbal caution (written order) to run at reduced speed or be prepared to stop short of an obstruction.

The LS mode is similar to FS in the sense that the ETCS On-Board performs speed and distance monitoring based on the received most restrictive speed profile, movement authority, release speed, gradient, etc. However, in LS mode the information given to ETCS from the infrastructure is not expected to be sufficient to safely supervise the train. Therefore:

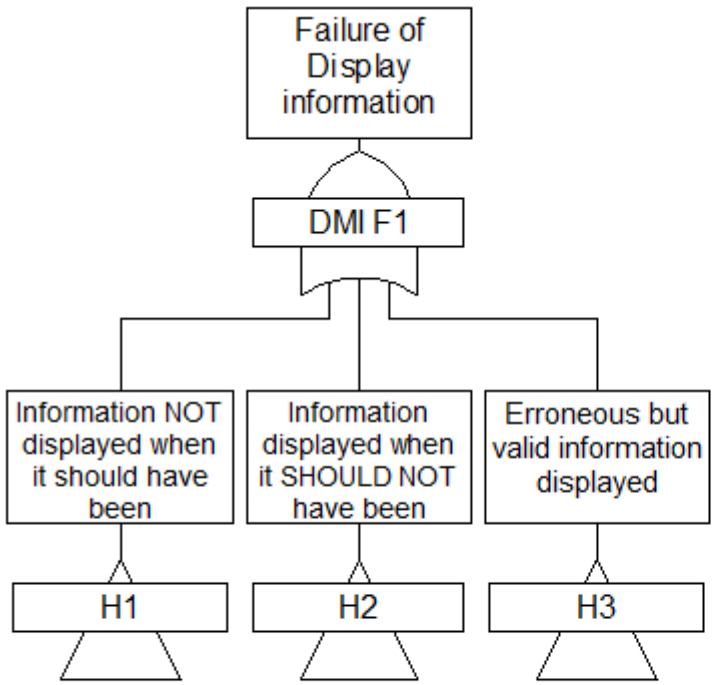
- it is expected (since the ETCS anyway doesn't have sufficient information) that the national safety integrity requirements for the ETCS in this mode are less demanding than the ones stated in SUBSET-091 [Ref 5]
- to maintain the total railway safety, a larger responsibility would instead be allocated to the driver's respect for existing line-side information (signals, speed boards etc).

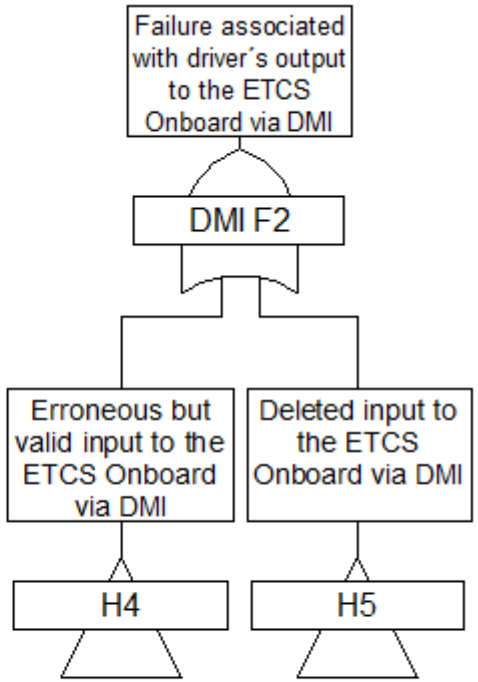
Although MMI-2a.1 is a failure in the ETCS On-Board, and would as such receive less demanding safety integrity requirements in LS mode according to the first bullet, the problem is that it impairs the driver's ability to respect the line-side information according to the second bullet. Therefore, the LS mode case is not treated differently in the event trees than other modes, but the general method of analysing the hazardous situation in its operational context all the way out to the consequence of the harm is still appropriate.

Note 4: L1 and L2 considered to apply as experience of application situations where there is a requirement for a train to closely approach a buffer stop, means that supervision margins cannot accommodate this close approach, and the Supervised Location (SvL) may be designed to be

beyond the buffer stop position, and a final approach at too high a speed due to a DMI failure could result in a collision, and is non Core Hazard as managed outside of the ETCS supervision. However, the hazard is in fact no different to the existing situation without ETCS in that a driver approaches a Buffer Stop and could be at risk if their speed indication was incorrect.

Appendix C Fault Trees





Appendix D Event Trees

D.1 Notes to read in conjunction with Event Tree models

1 It is unfortunate that the Primary Event Tree sheets contain internal page cross references for the transfers to Secondary trees. These are shown on the figures in Appendix D.3, but have no relevance outside of the Event Tree tool, and do not relate to page numbering of this report.

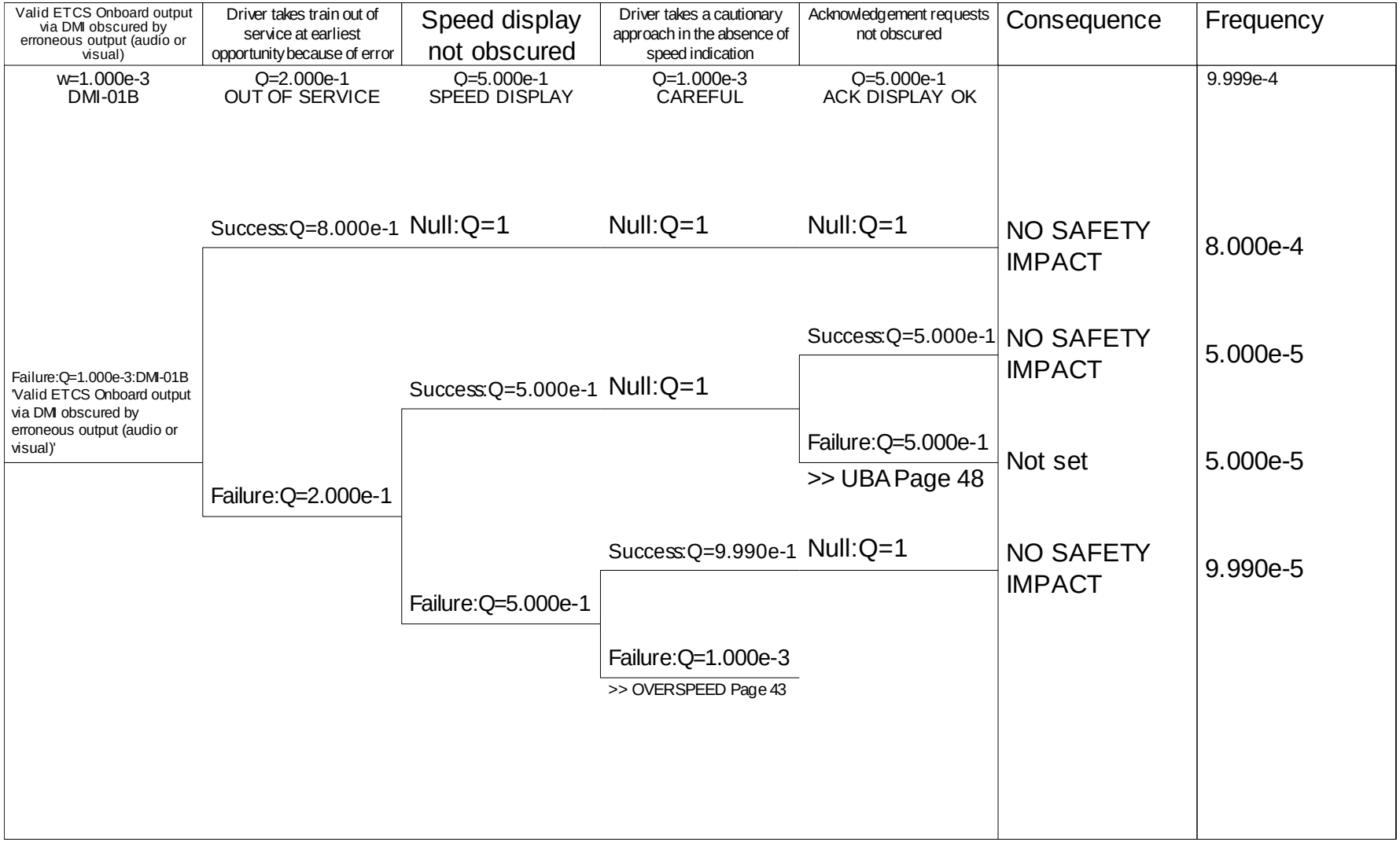
2 Note boxes have been added to the trees to clarify some aspects of the modelling, though the following Event Trees should be read in conjunction with the Hazard Schedule in Appendix B to provide the full context and explanation of the scenarios and barriers. The notes included in the trees can only be brief compared to fuller rationale presented in the full Hazard Schedule.

3 Likewise, the title of each event must be brief to be readable within the column header. A fuller description of each event, and what considerations it encompasses, is presented in Appendix E.

4 Where an erroneous DMI display or action has occurred, the ‘success’ leg of the Event Tree is assigned a consequence of “Possible Driver Distraction” to reflect the driver’s initial reaction and response to the failure (e.g. fault finding, determining that the display is erroneous and deciding what to do next). Unless specifically appropriate, ‘Distraction’ is not considered in the ‘failure’ legs of the models as in these situations the driver is either not aware of the change or has taken alternative action.

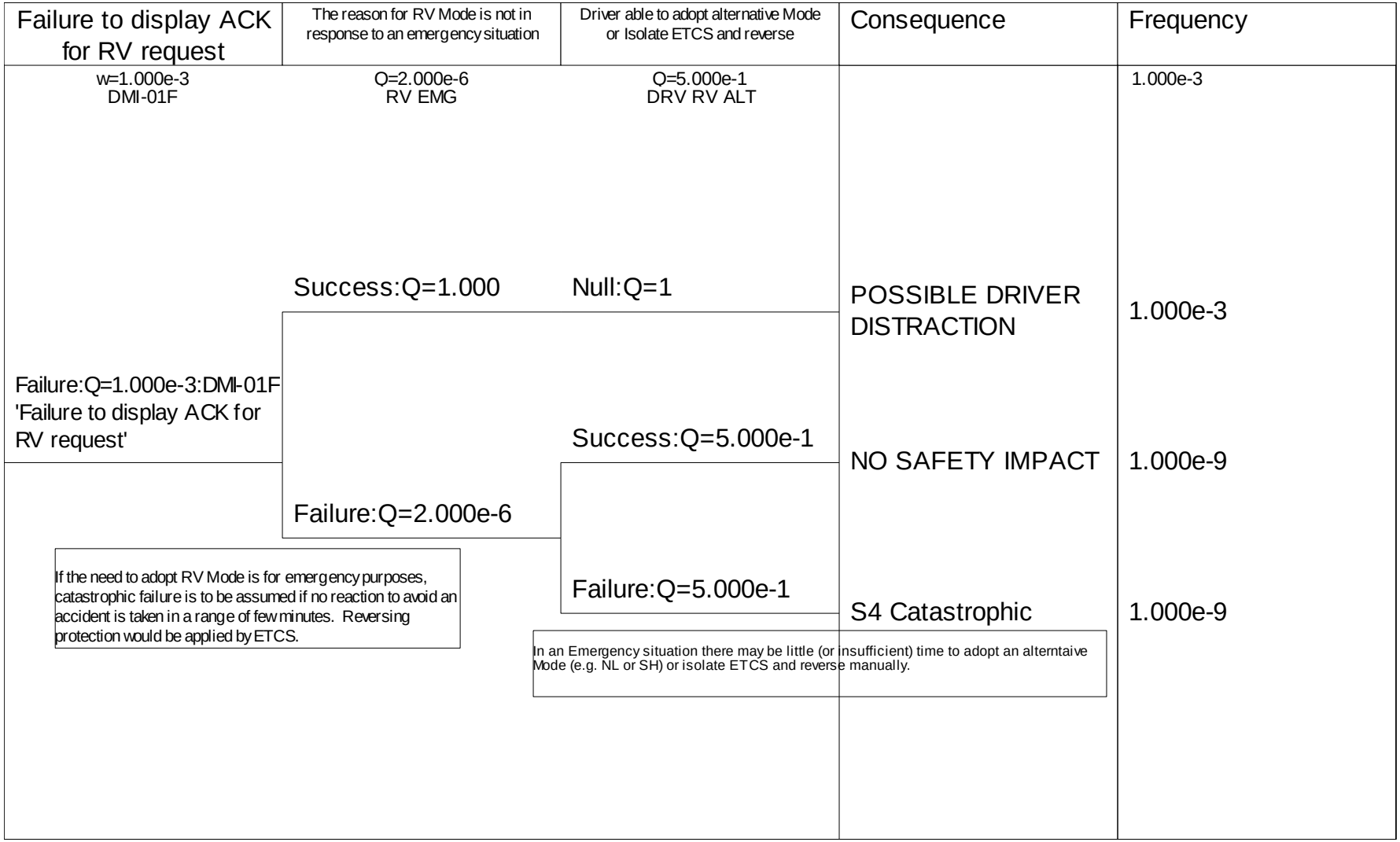
D.2 Primary Event Trees (Hazardous Situation development)

Failure to provide Warning indication	Driver respects the permitted speed plus a margin	Consequence	Frequency
w=5.000e-4 DMI-01A If driver respects the permitted speed plus a margin, brakes remain as not applied	Q=1.000e-1 DRV OVERSPEED		5.000e-4
Failure:Q=5.000e-4:DMI-01A 'Failure to provide Warning indication'	Failure:Q=1.000e-1 >> UBA Page 48	Not set	5.000e-5
	Success:Q=9.000e-1	NO SAFETY IMPACT	4.500e-4



Failure to display request for acknowledgement	Deletion of Acknowledgement message do not lead to UBA	Consequence	Frequency
w=1.000e-4 DMI-01C	Q=5.000e-1 ACK MISS NOT UBA		1.000e-4
Failure:Q=1.000e-4:DMI-01C 'Failure to display request for acknowledgement'	Success:Q=5.000e-1	NO SAFETY IMPACT	5.000e-5
	Failure:Q=5.000e-1	Not set	5.000e-5
	>> UBA Page 48		

Failure to display Geographical Position data	Driver chooses not to derive / estimate data in place of the 'missing' correct data	Driver's estimate of missing GPI data is sufficiently accurate	Consequence	Frequency
w=1.000 DMI-01D	Q=1.000e-1 NO GPI DATA	Q=1.000e-1 GPI DATA OK		1.000
Failure:Q=1.000:DMI-01D 'Failure to display Geographical Position data'	Success:Q=9.000e-1	Null:Q=1	NO SAFETY IMPACT	9.000e-1
	Failure:Q=1.000e-1	Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-2
		Failure:Q=1.000e-1	Not set Transfer to DMI-03A. As DMI-03A is an initiating event in its own right cannot transfer to it within the model, but risk is bounded by DMI-03A due to the barriers listed here which reduce the frequency of the data being incorrect.	1.000e-2



Failure to display Air Tightness Control	Different scenarios	There is no external accident which invokes the need for ATC	The train is not in the area of the external accident	Driver applies Air Tightness control without ETCS notification because of lineside signalling, written instructions...	Consequence	Frequency
w=1.000e-4 DMI-01G		Q=2.000e-6 EXTERNAL ACCIDENT	Q=1.000 TRAIN IN ACC AREA	Q=1.000e-1 DRV AIR TIGHT		2.000e-4
	Null:Q=1:Tunnels with track condition 'air tightness'	Null:Q=1	Null:Q=1	Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-5
				Failure:Q=1.000e-1	S2 Marginal	1.000e-5
Failure:Q=1.000e-4:DMI-01G 'Failure to display Air Tightness Control'	Light injuries could occur because of pressure chock (ear pain) or particles inside the tunnel	Success:Q=1.000	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	1.000e-4
	Null:Q=1:Special areas with track condition 'air tightness', e.g. around chemical plants	The train is assumed to be stopped or re-routed => Not analysed	Success:Q=0.000	Null:Q=1	Not modelled (National Rules)	0.000
		Failure:Q=2.000e-6	Failure:Q=1.000	Null:Q=1	S4 Catastrophic	2.000e-10
		Severe injuries or casualties because of toxic fumes				

DMI-01h : Failure to present Display Distance to Target information.

The system can only be in one low adhesion style at a time :

- max deceleration (refer to MMI-2C)
- DDT (this case and DMI-3g)
- TTI (refer to DMI-01i and DMI-3h)
- None (full responsibility of project)

Event tree for DMI-01h is exactly the same as those for MMI-2C.

The target for DMI-01h is then exactly the same as for MMI-2C

➔ W=6,7 e-5

The event tree does not need to be updated.

Only MMI-2C should be renamed MMI-2C or DMI-01h or DMI-01i or DMI-03g or DMI-03h and description adapted

DMI-01i : Failure to present Time To Indication information

The system can only be in one low adhesion style at a time :

- max deceleration (refer to MMI-2C)
- DDT (refer to DMI-01h and DMI-3g)
- TTI (this case and DMI-3h)
- None (full responsibility of project)

Event tree for DMI-01i is exactely the same as those for MMI-2C.

The target for DMI-01i is then exactly the same as for MMI-2C

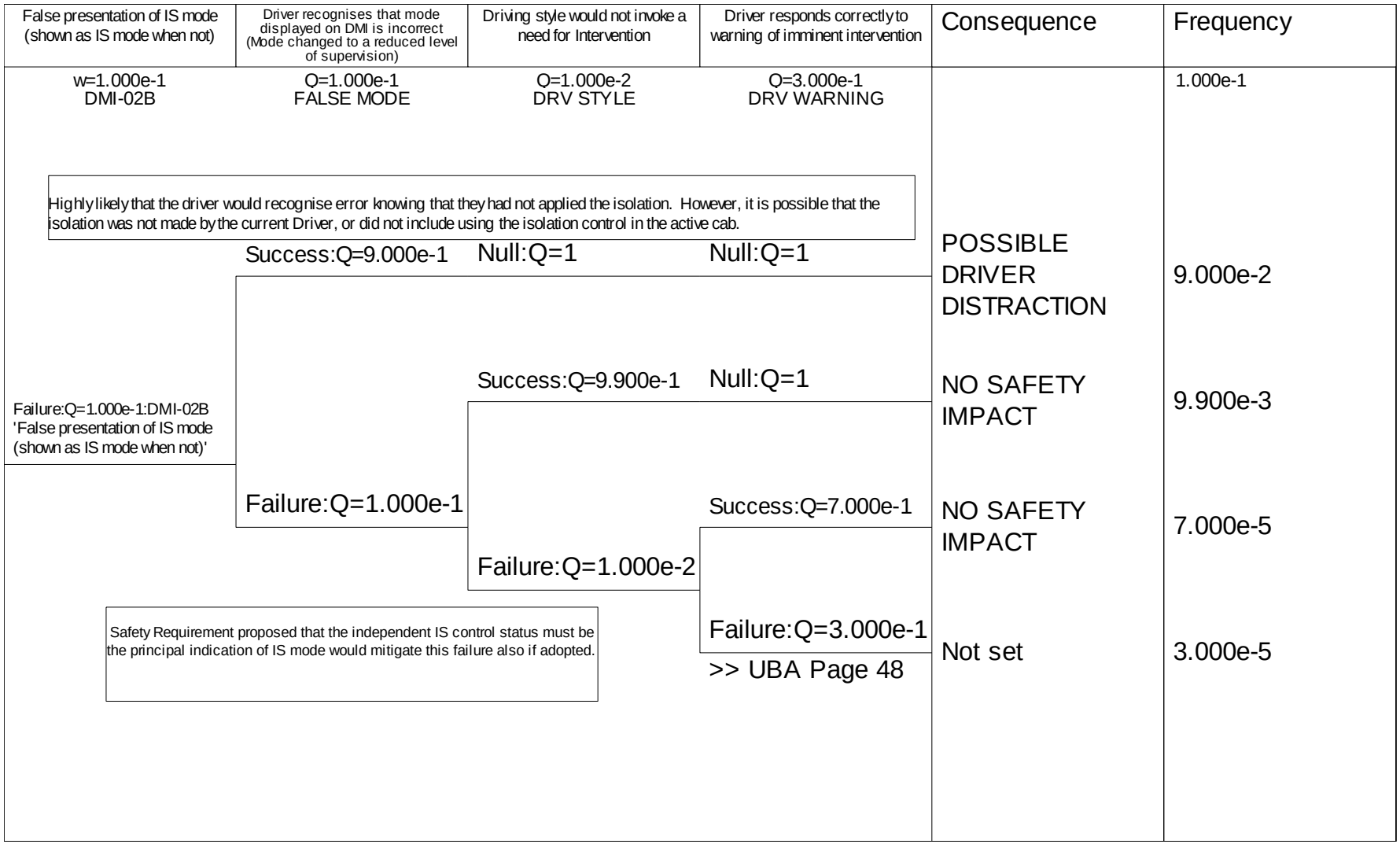
➔ W=6,7 e-5

The event tree does not need to be updated.

Only MMI-2C should be renamed MMI-2C or DMI-01h or DMI-01i or DMI-03g or DMI-03h and description adapted

False presentation of Warning or of 'LX not protected'	Driver recognises that indication from ETCS Onboard is incorrect or missing	Driver adapts the brake effort to not cause passenger injuries	Consequence	Frequency
w=1.000e-4 DMI-02A, -02G	Q=3.000e-1 DRV INDICATION	Q=1.000e-1 DRV ADAPT BRAKING		1.000e-4
Failure:Q=1.000e-4:DMI-02A, -02G 'False presentation of Warning or of 'LX not protected' information'	Success:Q=7.000e-1	Null:Q=1	POSSIBLE DRIVER DISTRACTION	7.000e-5
		Success:Q=9.000e-1	NO SAFETY IMPACT	2.700e-5
	Failure:Q=3.000e-1	Failure:Q=1.000e-1	Not set	3.000e-6
	>> UBA Page 48	>> UBA Page 48		

ET derived for consistency. Situation covers where a driver over-reacts to (the spurious) situation and applies full service brake, with similar, but lesser impact than a UBA.

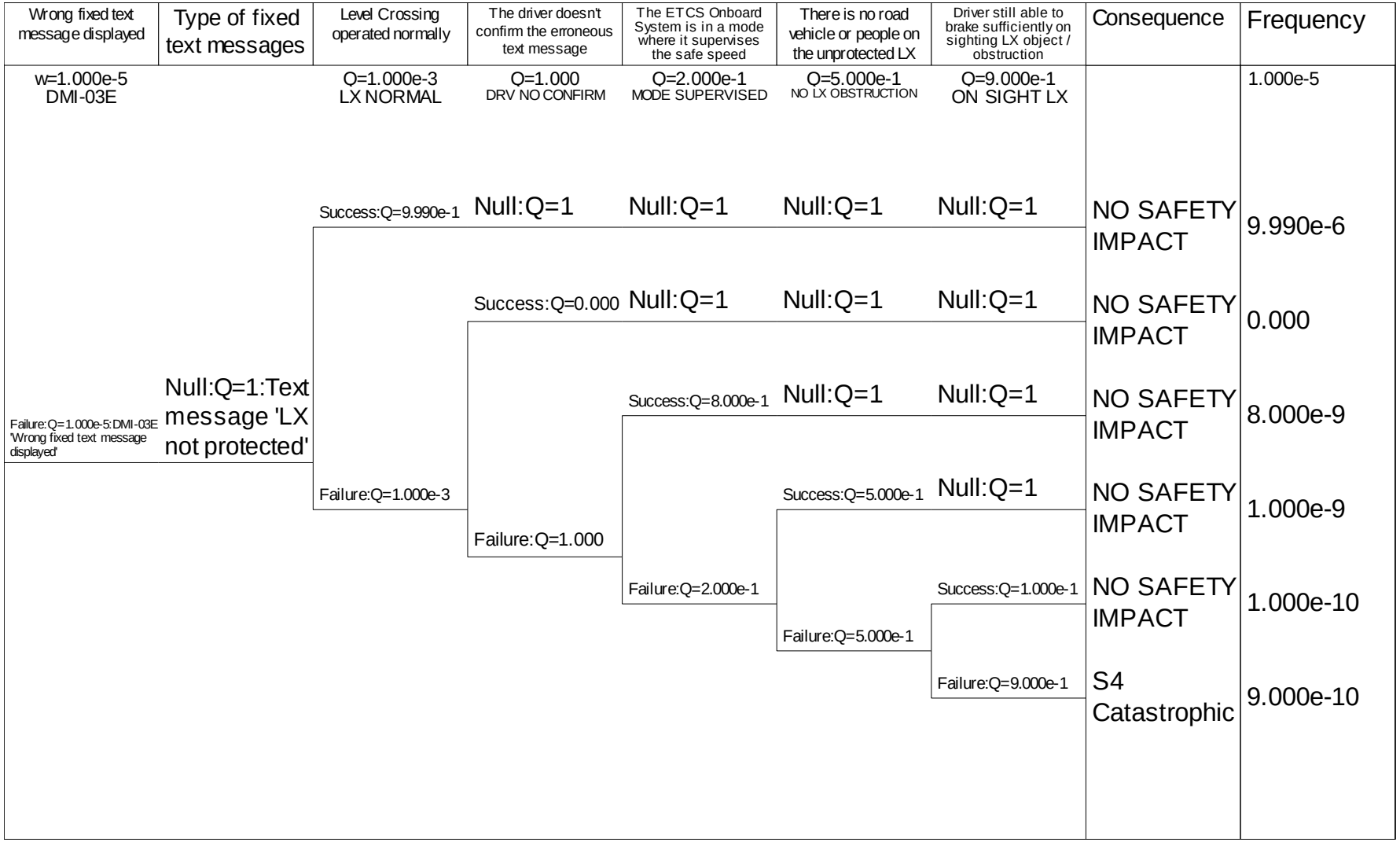


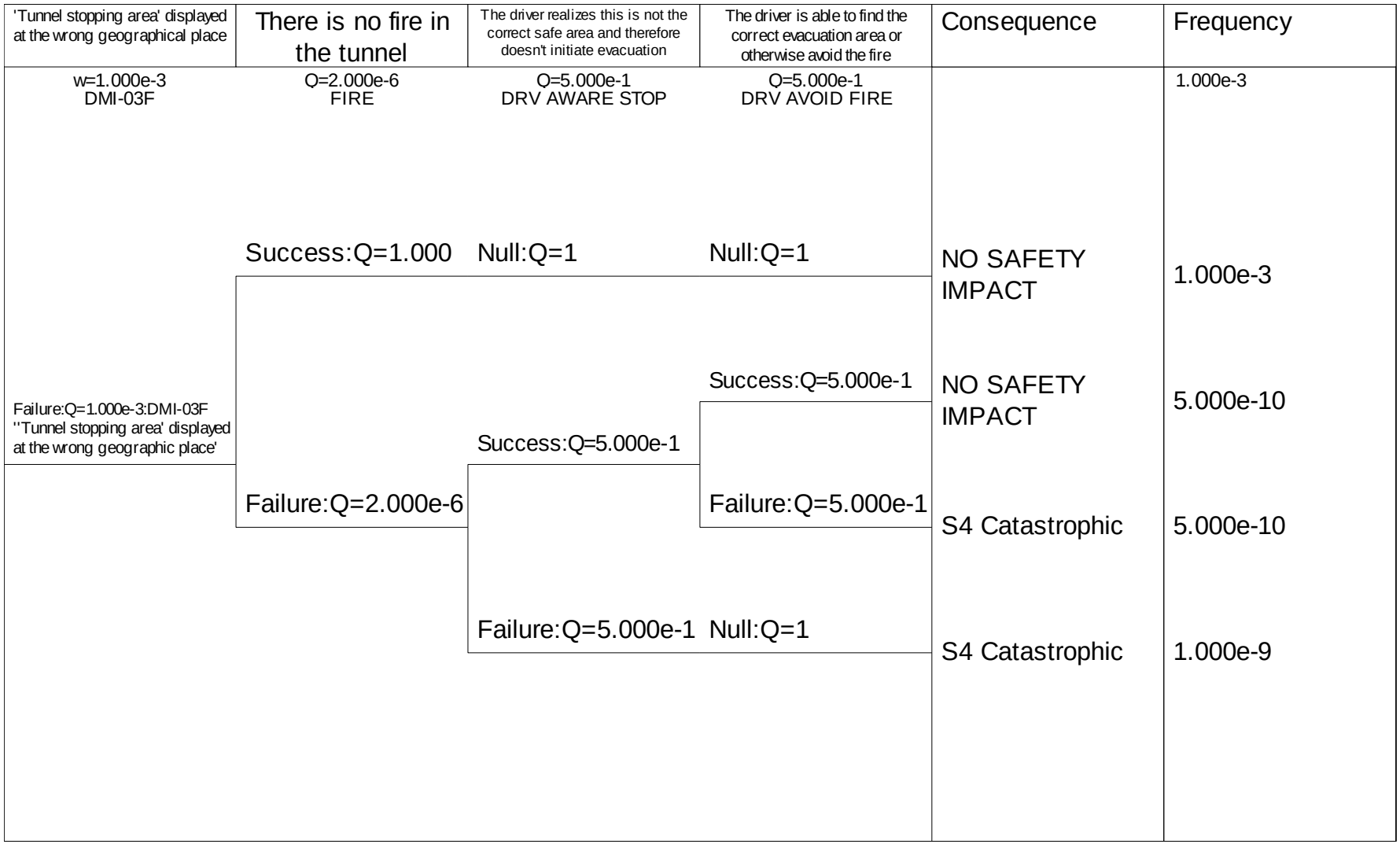
False presentation of brake indication	Driver recognises display erroneous or provides controlled braking response	Consequence	Frequency
w=5.000e-3 DMI-02C	Q=1.000e-2 CONTROLLED BRAKING		5.000e-3
Failure:Q=5.000e-3:DMI-02C 'False presentation of brake indication'	Success:Q=9.900e-1	POSSIBLE DRIVER DISTRACTION	4.950e-3
	Failure:Q=1.000e-2	Not set	5.000e-5

>> UBA Page 48

Considers situations where the driver is provided with an indication that ETCS is applying braking, such that spurious indication without braking being perceived by the driver, may cause the driver to react and apply full service brakes.

Spurious notification of Train Data change (which normally is from source different from the driver)	Driver recognises that indication from ETCS Onboard is incorrect or missing	Consequence	Frequency
w=1.000 DMI-02E	Q=3.000e-1 DRV INDICATION		1.000
Failure:Q=1.000:DMI-02E 'Spurious notification of Train Data change (which normally is from source different from the driver)'	Success:Q=7.000e-1	NO SAFETY IMPACT	7.000e-1
	Failure:Q=3.000e-1	POSSIBLE DRIVER DISTRACTION	3.000e-1





DMI-03g : Wrong Display Distance to Target information

The system can only be in one low adhesion style at a time :

- max deceleration (refer to MMI-2C)
- DDT (this case and DMI-01h)
- TTI (refer to DMI-01i and DMI-3h)
- None (full responsibility of project)

Event tree for DMI-03g is exactly the same as those for MMI-2C.

The target for DMI-03g is then exactly the same as for MMI-2C

➔ W=6,7 e-5

The event tree does not need to be updated.

Only MMI-2C should be renamed MMI-2C or DMI-01h or DMI-01i or DMI-03g or DMI-03h and description adapted

DMI-03h : Wrong Time To Indication information

The system can only be in one low adhesion style at a time :

- max deceleration (refer to MMI-2C)
- DDT (refer to DMI-01h and DMI-3g)
- TTI (this case and DMI-1i)
- None (full responsibility of project)

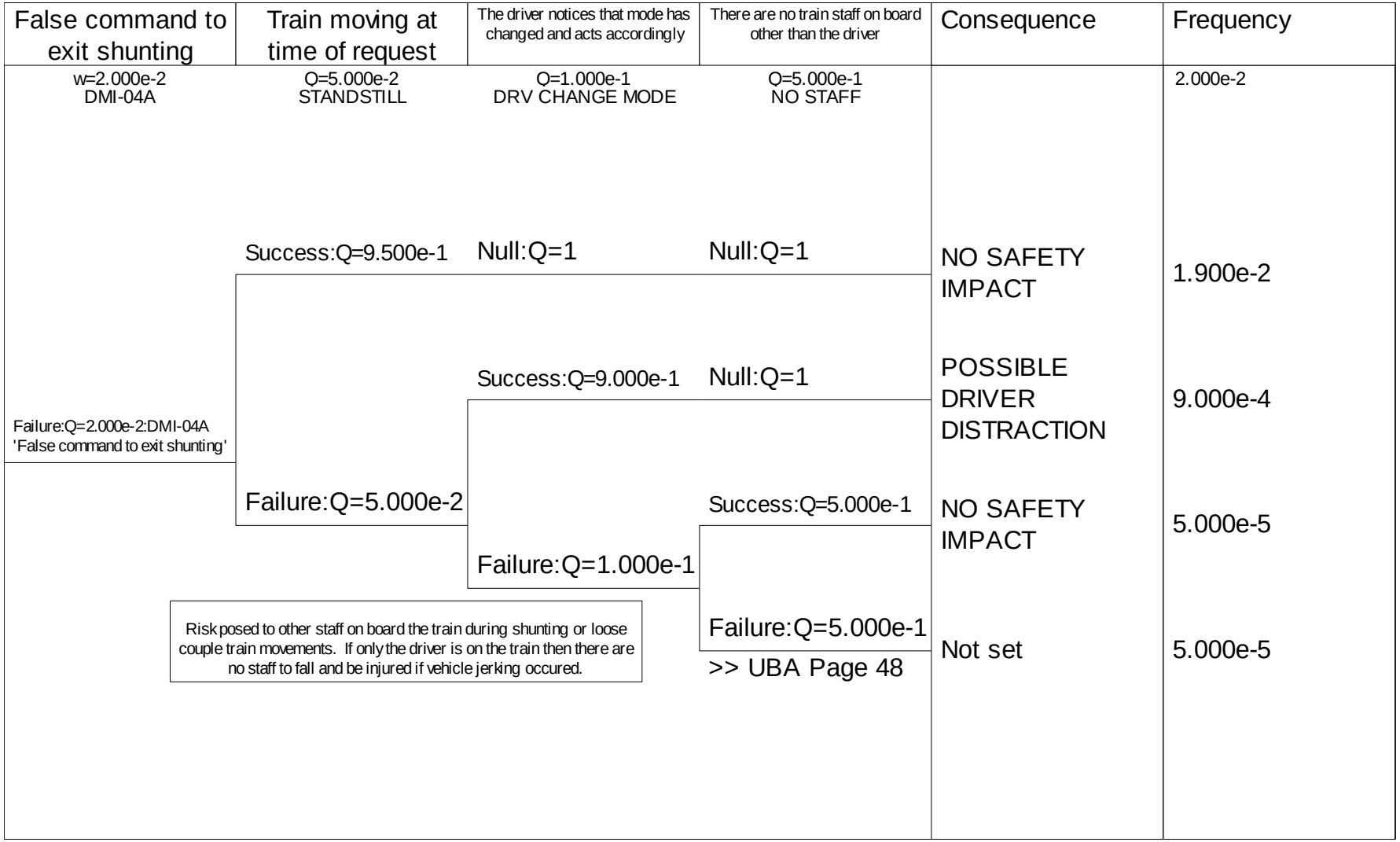
Event tree for DMI-03h is exactly the same as those for MMI-2C.

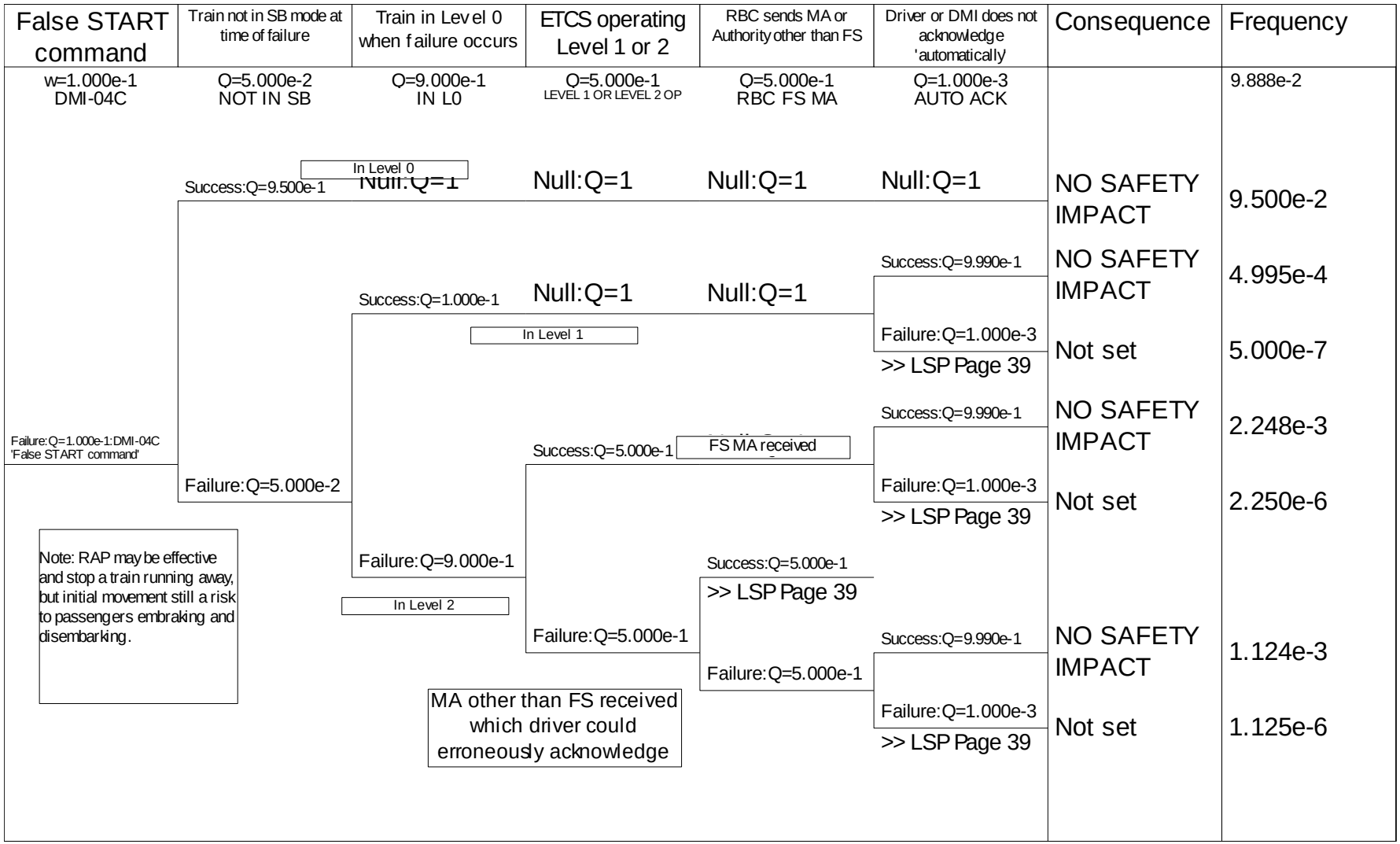
The target for DMI-03h is then exactly the same as for MMI-2C

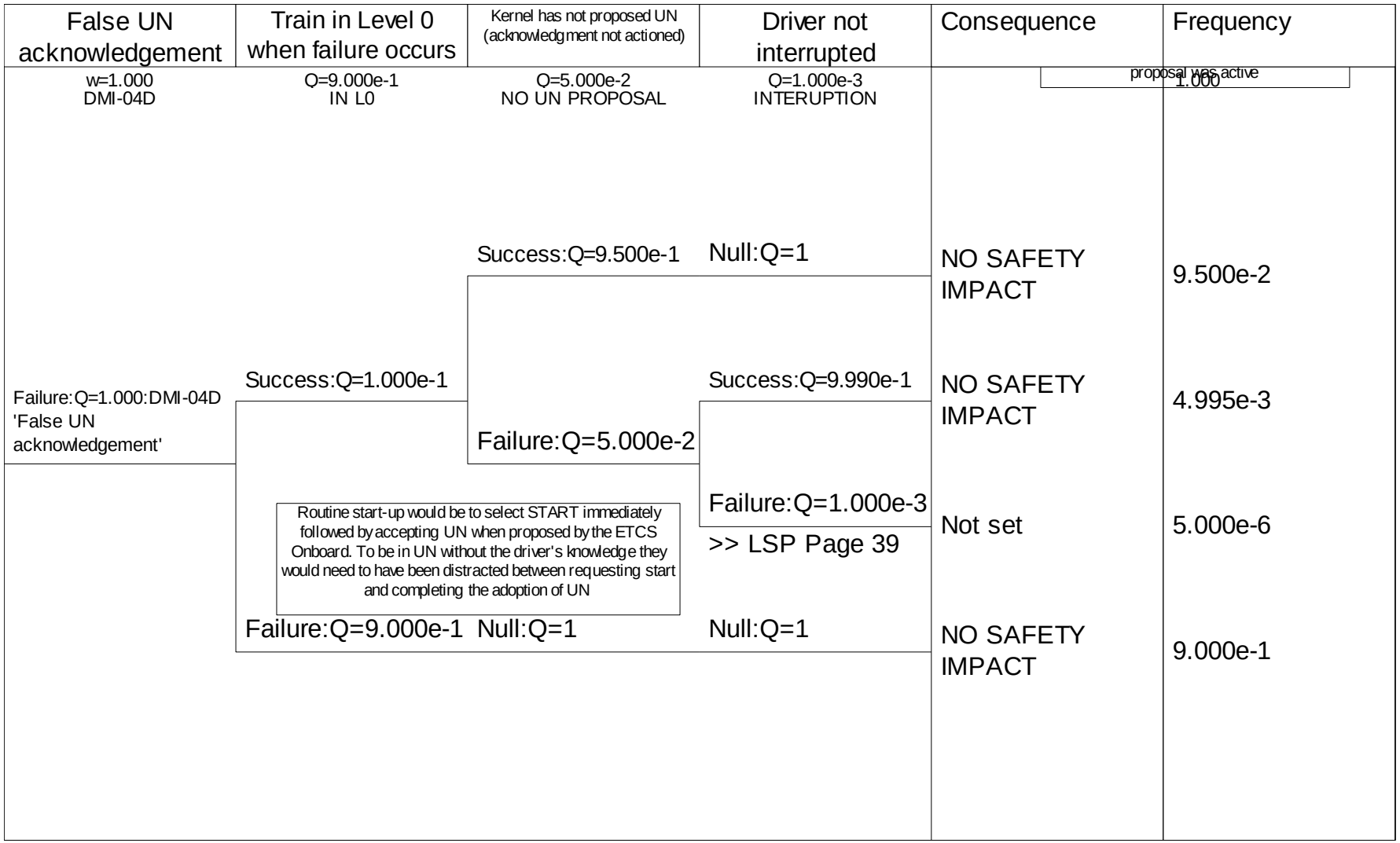
➔ W=6,7 e-5

The event tree does not need to be updated.

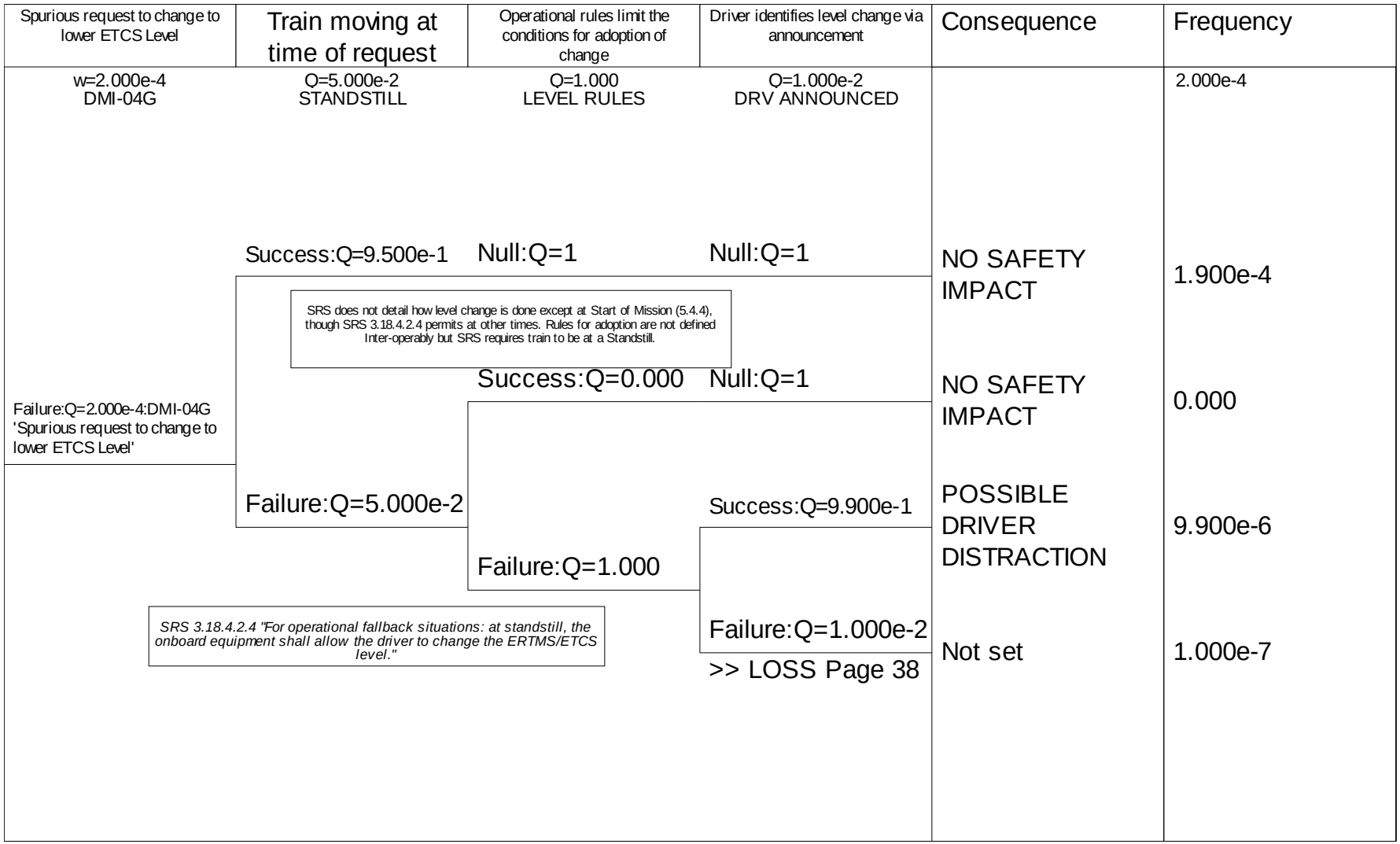
Only MMI-2C should be renamed MMI-2C or DMI-01h or DMI-01i or DMI-03g or DMI-03h and description adapted

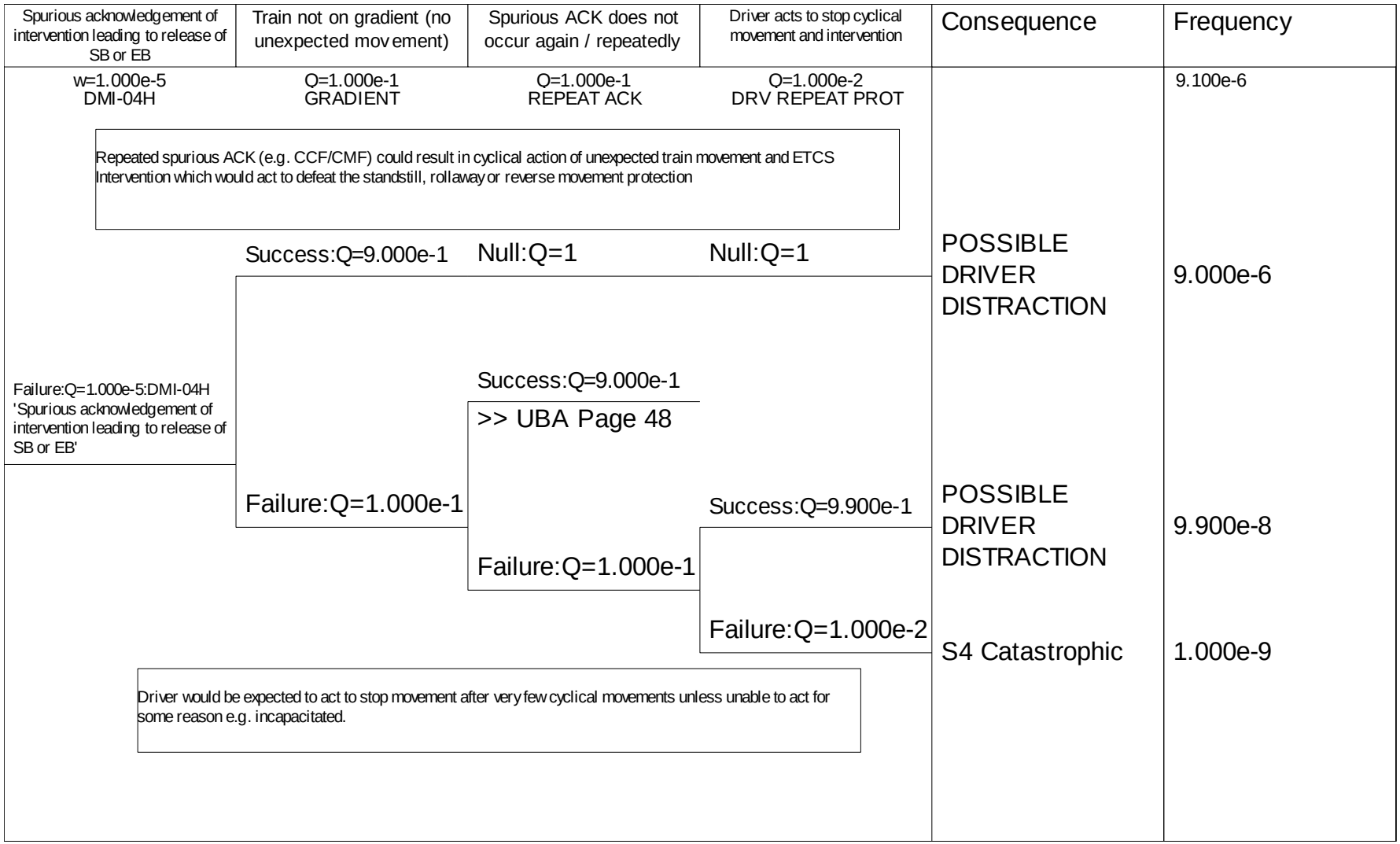






Spurious or wrong language requested distracting the train Driver	Driver takes train out of service at earliest opportunity because of error	Competent in the new language	Consequence	Frequency
w=1.000 DMI-04F	Q=2.000e-1 OUT OF SERVICE	Q=0.000 DRV LANG COMPETENCE		1.000
	Success:Q=8.000e-1	Null:Q=1	POSSIBLE DRIVER DISTRACTION	8.000e-1
Failure:Q=1.000:DMI-04F "Spurious or wrong language requested distracting the train Driver'		Success:Q=1.000	POSSIBLE DRIVER DISTRACTION	2.000e-1
	Failure:Q=2.000e-1	Failure:Q=0.000	Not set	0.000
	The downstream impact should a driver attempt to use a language for which they are not fully conversant, is not a specific risk in itself, but a performance shaping factor of the other situations / failures covered separately.			





False Isolation command	The driver notices that mode has changed and acts accordingly	Consequence	Frequency
w=1.000e-6 DMI-04J	Q=1.000e-1 DRV CHANGE MODE		1.000e-6
Failure:Q=1.000e-6:DMI-04J 'False Isolation command'	Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-7
	Failure:Q=1.000e-1 >> LOSS Page -1	Not set	1.000e-7

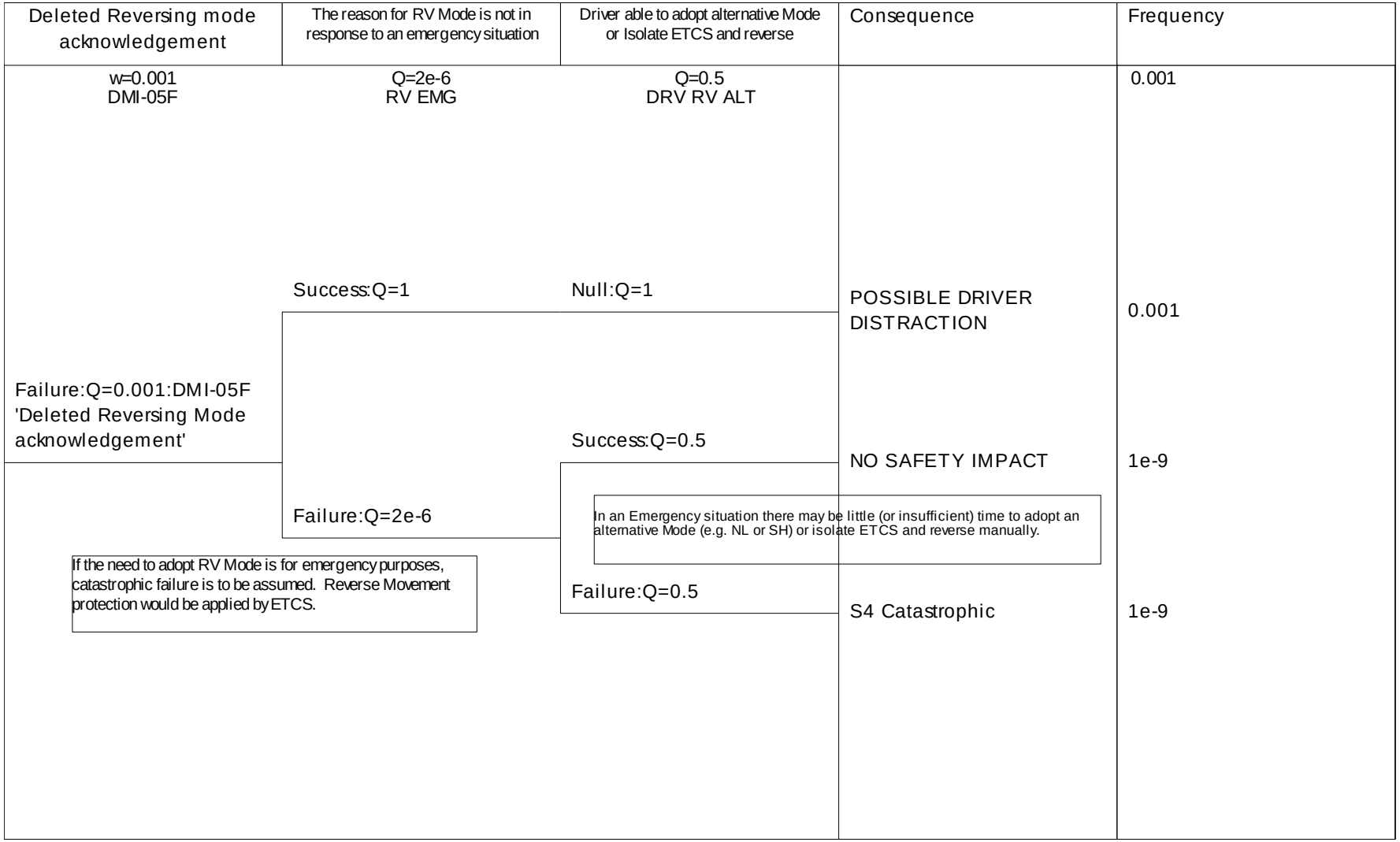
Isolation switch is separated from driver´s screen and doubles as an indication that overrules any indication on the driver´s screen.

Deleted Level transition acknowledgement	Consequence	Frequency
w=5.000e-5 DMI-05A, -05B Failure:Q=5.000e-5:DMI-05A, -05B 'Deleted acknowledgement (a Level transition)' >> UBA Page 48	DMI-05a: Deleted Level transition acknowledgement is just a specific acknowledgment example for the generic situation of DMI-05b. Not set	5.000e-5 5.000e-5

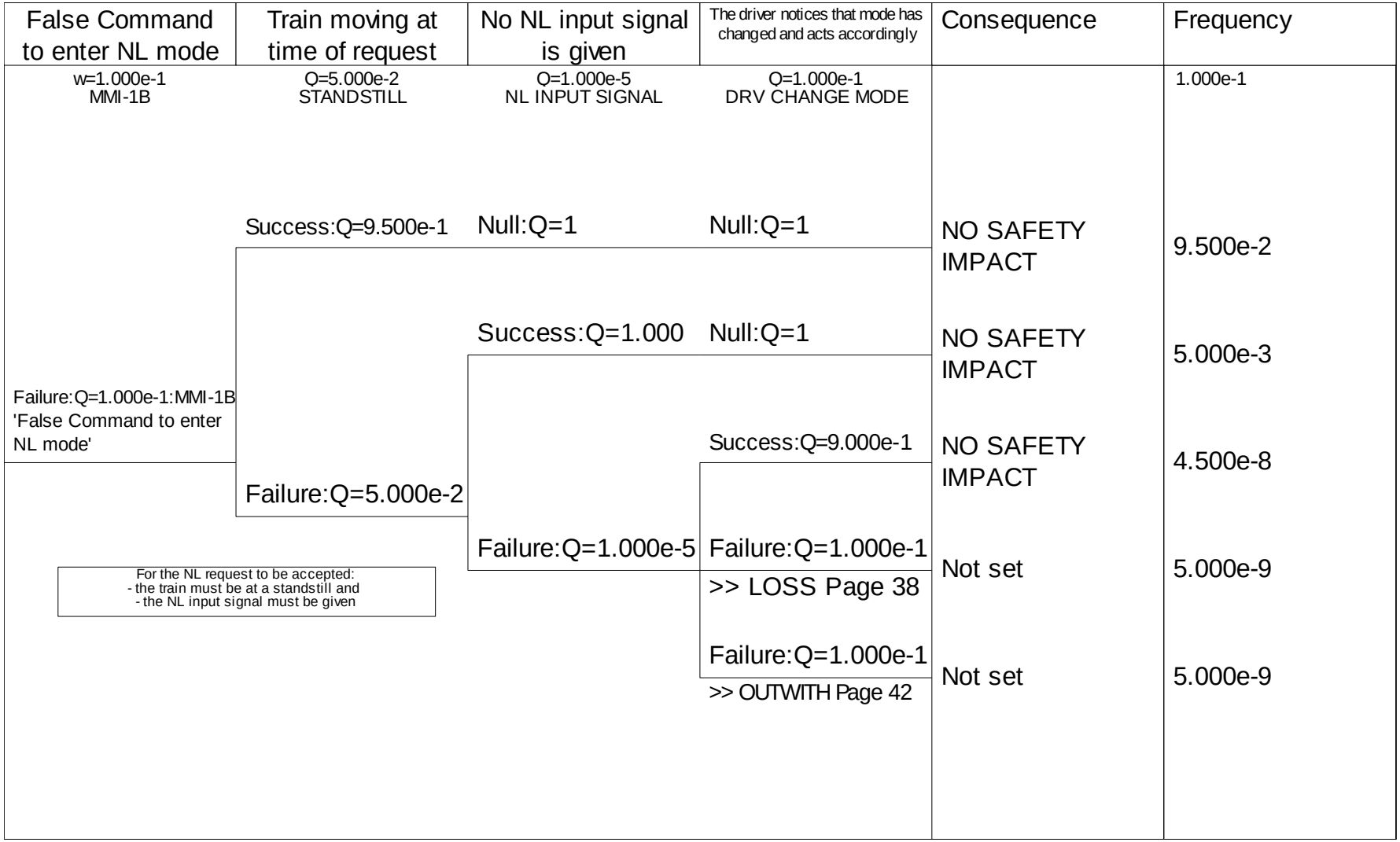
Deleted request for GPI	Driver chooses not to derive / estimate data in place of the 'missing' correct data	Driver's estimate of missing GPI data is sufficiently accurate	Consequence	Frequency
w=1.000 DMI-05C	Q=1.000e-1 NO GPI DATA	Q=1.000e-1 GPI DATA OK		1.000
	Success:Q=9.000e-1	Null:Q=1	NO SAFETY IMPACT	9.000e-1
Failure:Q=1.000:DMI-05C 'Deleted request for GPI'		Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-2
	Failure:Q=1.000e-1	Failure:Q=1.000e-1	Transfer to DMI-03A. As DMI-03A is an initiating event in its own right cannot transfer to it within the model, but risk is bounded by DMI-03A due to the barriers listed here which reduce the frequency of the data being incorrect.	1.000e-2
			Not set	

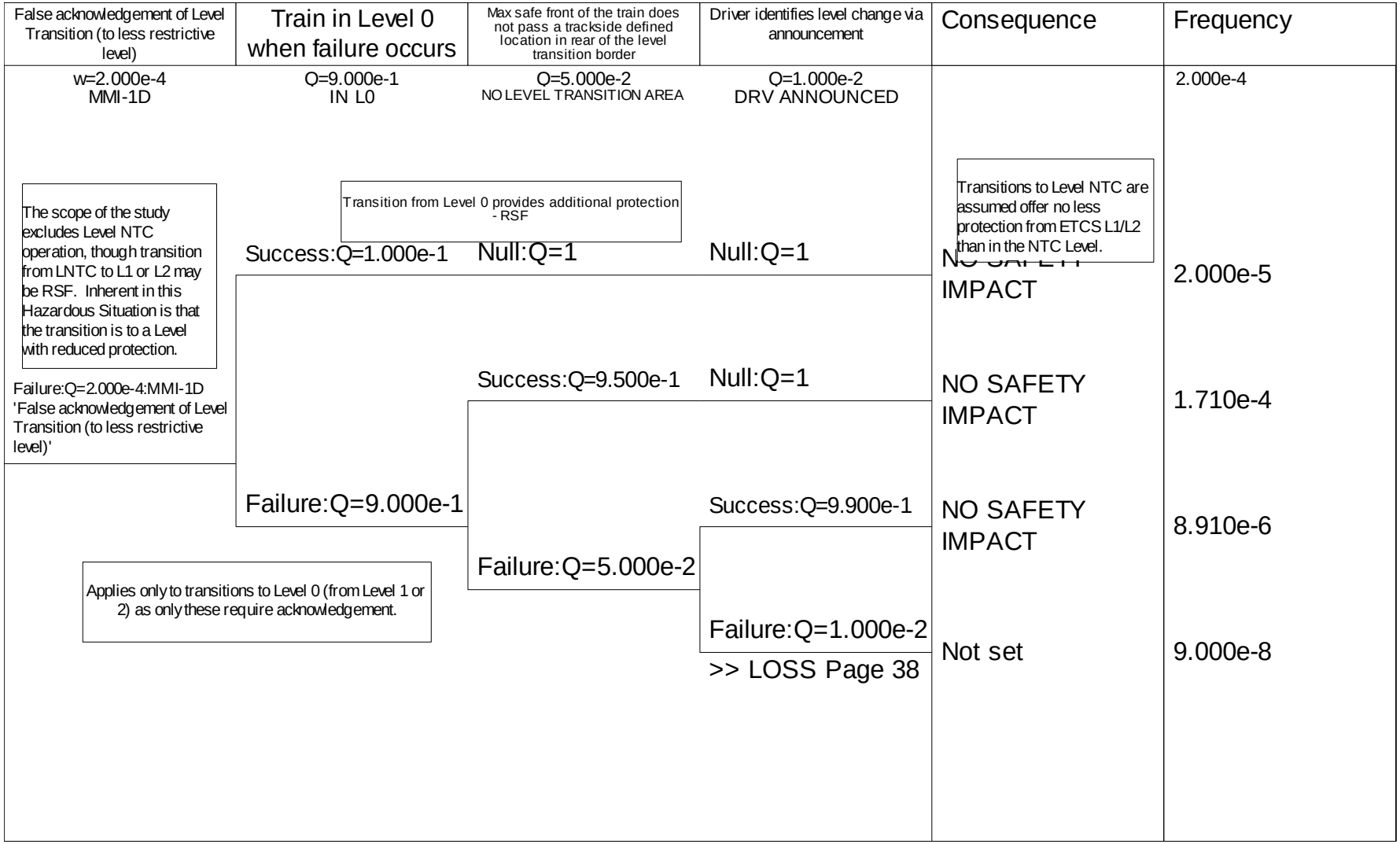
Deleted change of language request	Driver takes train out of service at earliest opportunity because of error	Competent in the new language	Consequence	Frequency
w=1.000 DMI-05D	Q=2.000e-1 OUT OF SERVICE	Q=0.000 DRV LANG COMPETENCE		1.000
	Success:Q=8.000e-1	Null:Q=1	POSSIBLE DRIVER DISTRACTION	8.000e-1
Failure:Q=1.000:DMI-05D 'Deleted change of language request'		The downstream impact should a driver attempt to use a language for which they are not fully conversant, is not a specific risk in itself, but a performance shaping factor of the other situations / failures covered separately.		
		Success:Q=1.000	POSSIBLE DRIVER DISTRACTION	2.000e-1
	Failure:Q=2.000e-1			
		Failure:Q=0.000	Not set	0.000

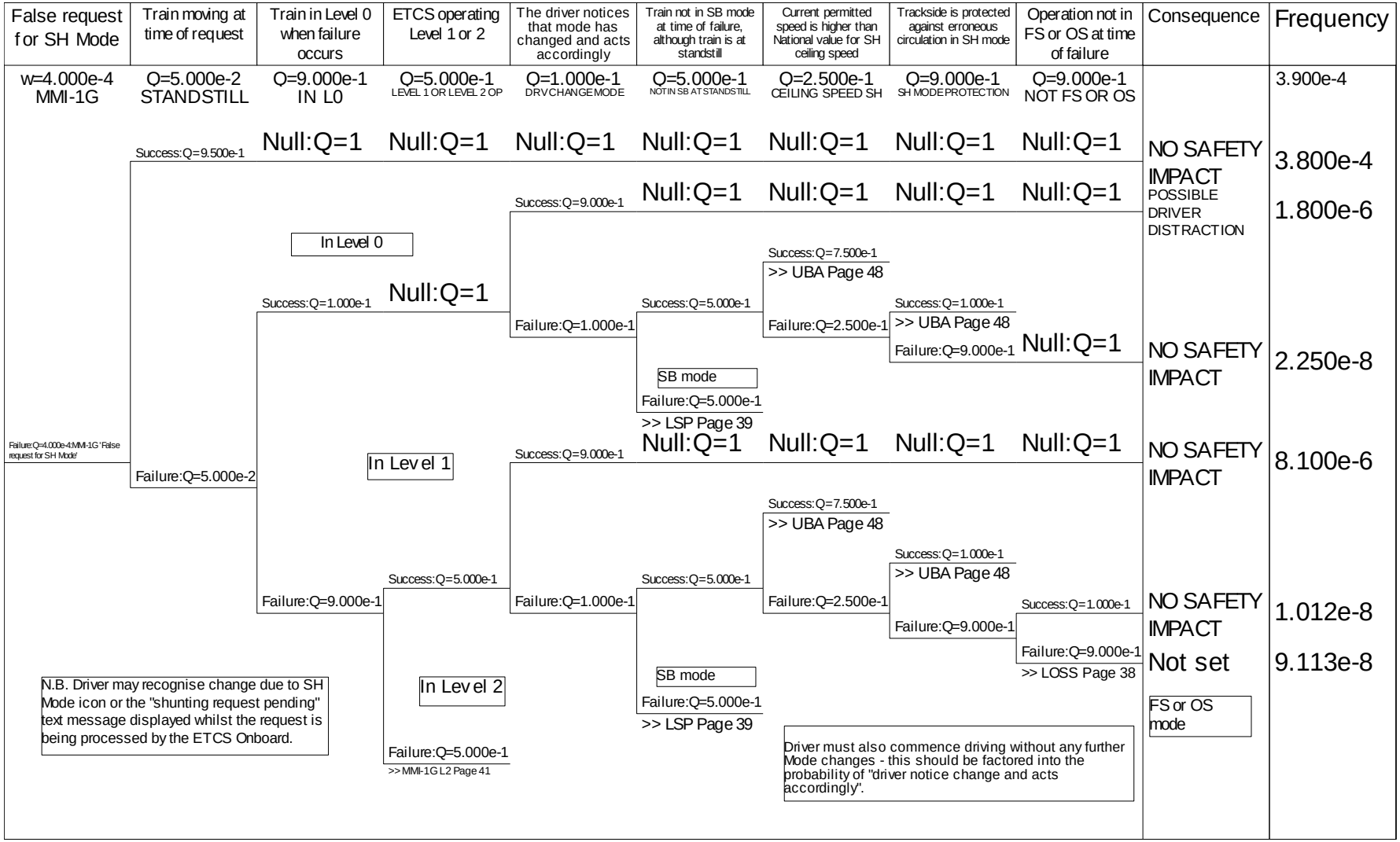
Deleted driver request to apply Track Adhesion Factor	Driver recognises that Adhesion Factor 'slippery rail' indication from ETCS Onboard is missing	Consequence	Frequency
w=1.000e-4 DMI-05E	Q=1.000e-3 DRV INDICATION SLIPPERY		1.000e-4
	Success:Q=9.990e-1	NO SAFETY IMPACT	9.990e-5
Failure:Q=1.000e-4:DMI-05E 'Deleted driver request to apply Track Adhesion Factor'		The extent of any overrun will depend upon the safety margins built into the ETCS application design and the level of poor adhesion encountered.	
	Failure:Q=1.000e-3	Not set	1.000e-7
	>> OVERSPEED Page 43		
The exact method and information available to a driver to confirm that their request for Track Adhesion Factor to be applied is subject to supplier designs and National Rules.			

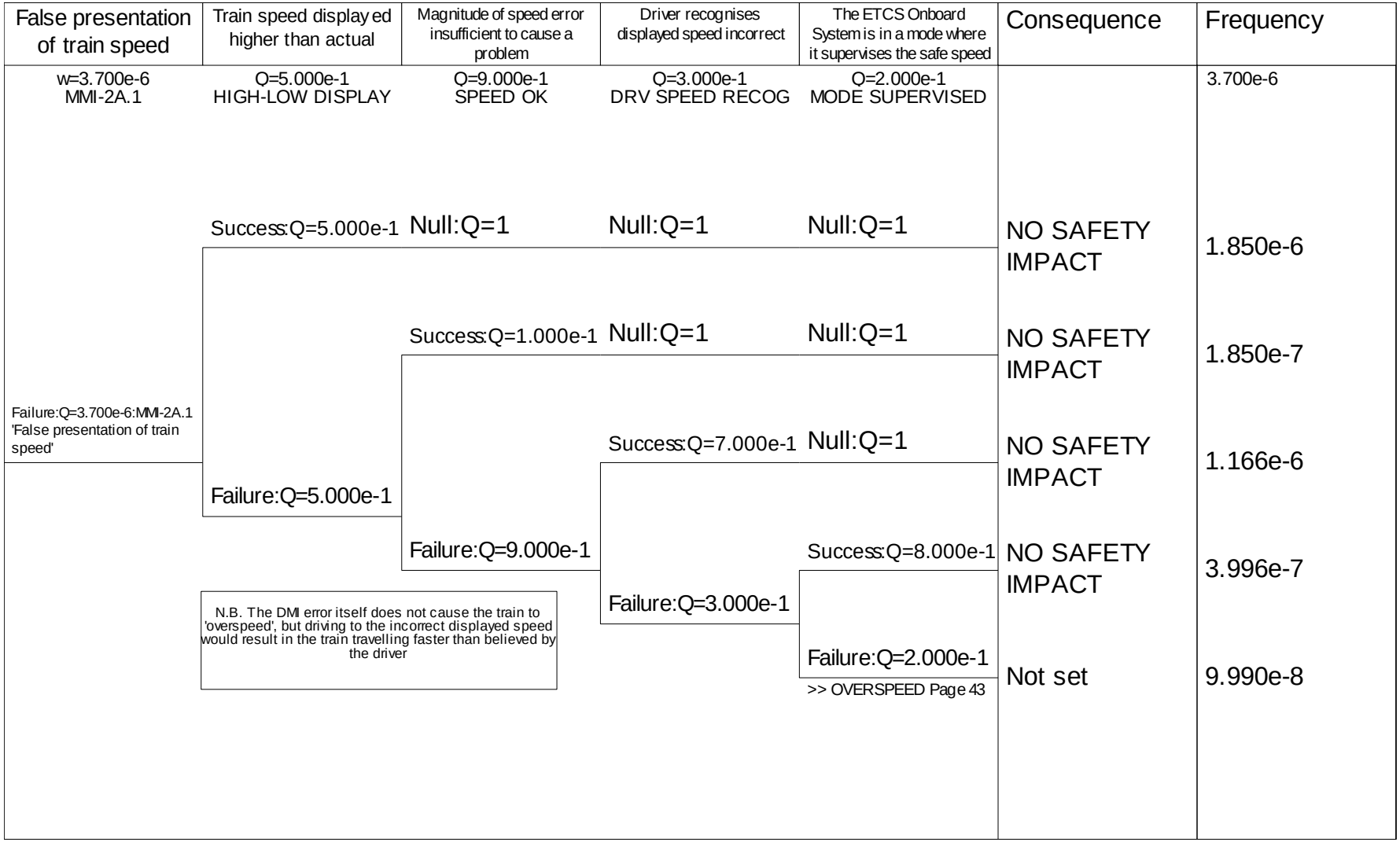


False acknowledgement of mode change to less restrictive mode	ETCS Onboard rejects the spurious request as the conditions to apply or accept the request are not in place	The driver notices that mode has changed and acts accordingly	Consequence	Frequency
w=2.000e-5 MMI-1A	Q=5.000e-2 ETCS ONBOARD REJECTS	Q=1.000e-1 DRV CHANGE MODE		2.000e-5
	Success:Q=9.500e-1	Null:Q=1	NO SAFETY IMPACT	1.900e-5
Failure:Q=2.000e-5:MMI-1A 'False acknowledgement of mode change to less restrictive mode'		Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-7
	Failure:Q=5.000e-2	Failure:Q=1.000e-1	Not set	1.000e-7
		>> LOSS Page 38		



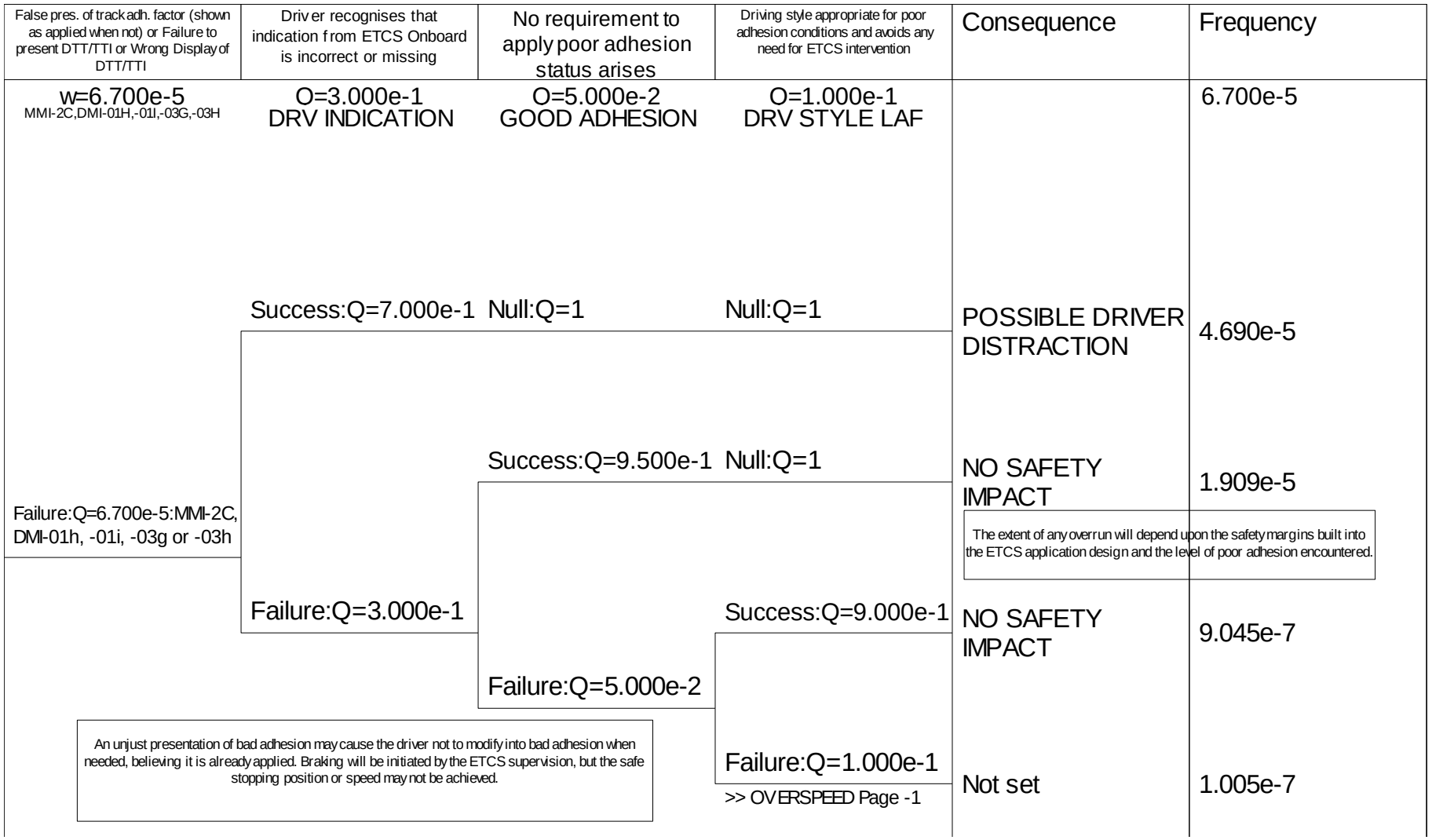






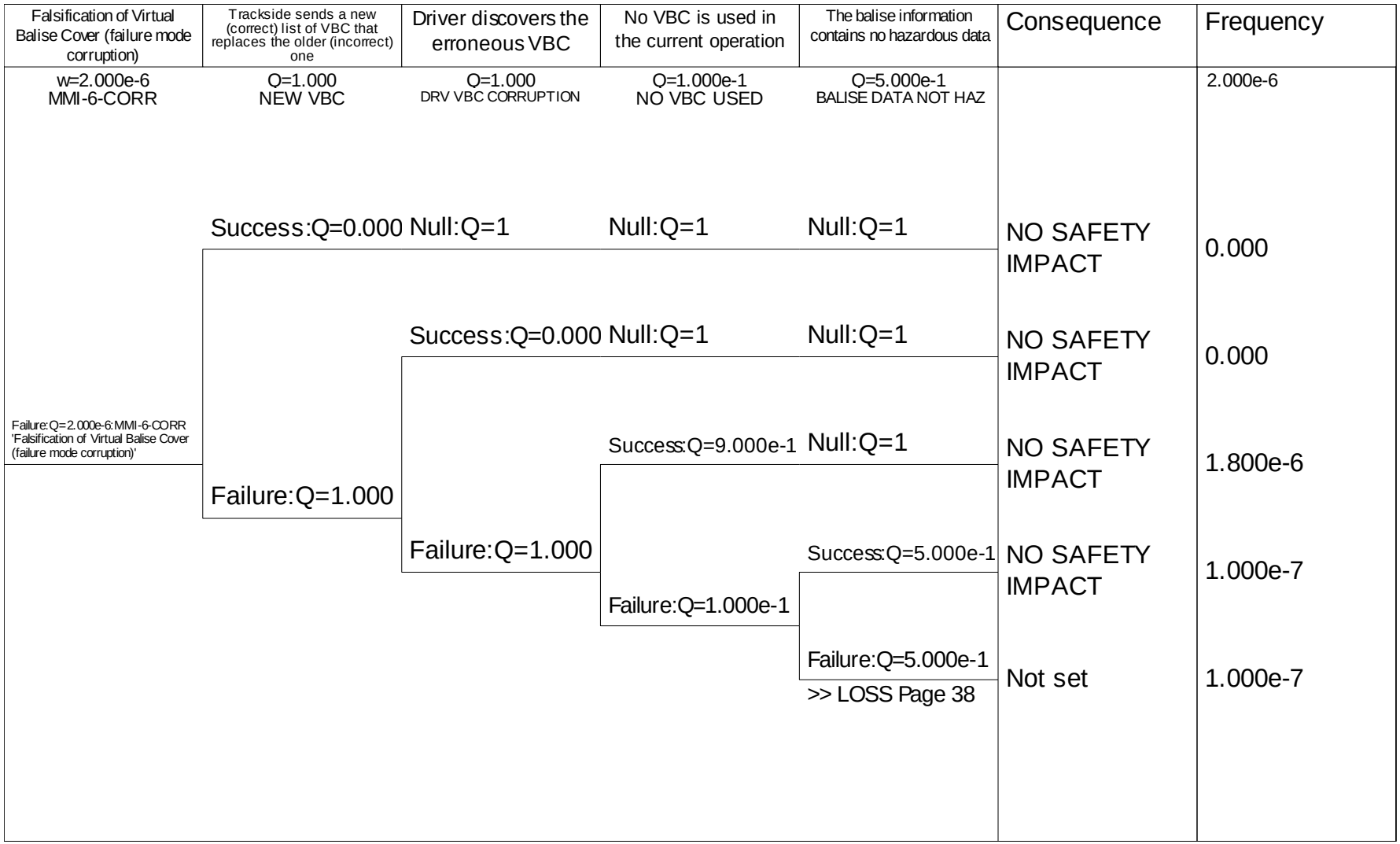
False presentation of mode	The ETCS Onboard System is in a mode where it supervises the safe speed	Driver recognises that mode displayed on DMI is incorrect (Mode changed to a reduced level of supervision)	Consequence	Frequency
w=5.000e-6 MMI-2B	Q=2.000e-1 MODE SUPERVISED	Q=1.000e-1 FALSE MODE		5.000e-6
	Success:Q=8.000e-1	Null:Q=1	POSSIBLE DRIVER DISTRACTION	4.000e-6
Failure:Q=5.000e-6:MMI-2B 'False presentation of mode'		Success:Q=9.000e-1	POSSIBLE DRIVER DISTRACTION	9.000e-7
	Failure:Q=2.000e-1			
		Failure:Q=1.000e-1	Not set	1.000e-7
		>> LOSS Page 38		

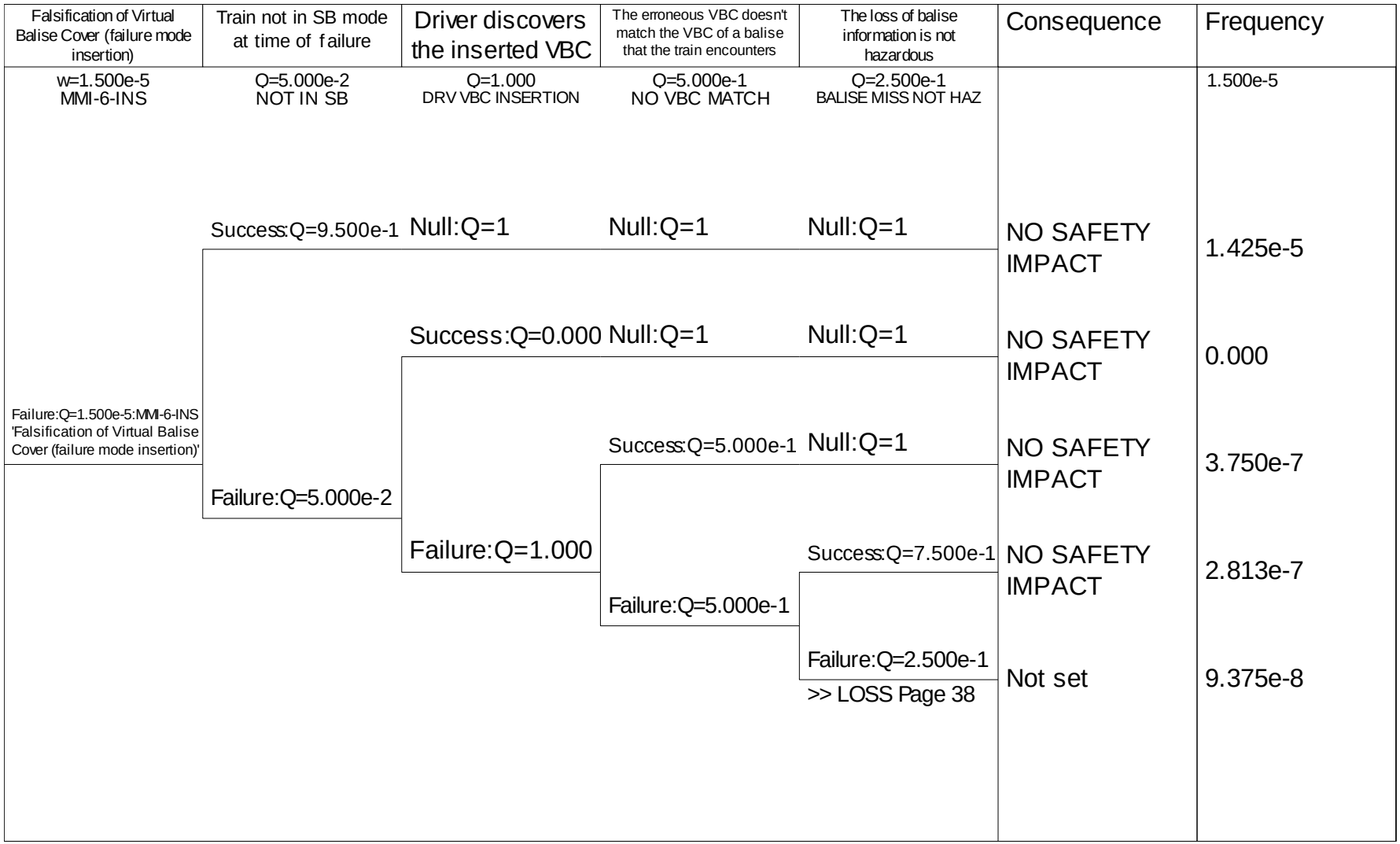
Note: Acknowledgment of Mode change to a lower level of supervision should alert a driver to examine the displayed information. Most onerous if the Mode displayed has changed to a 'lower' Mode, but the ETCS Onboard is in a yet 'lower' Mode.



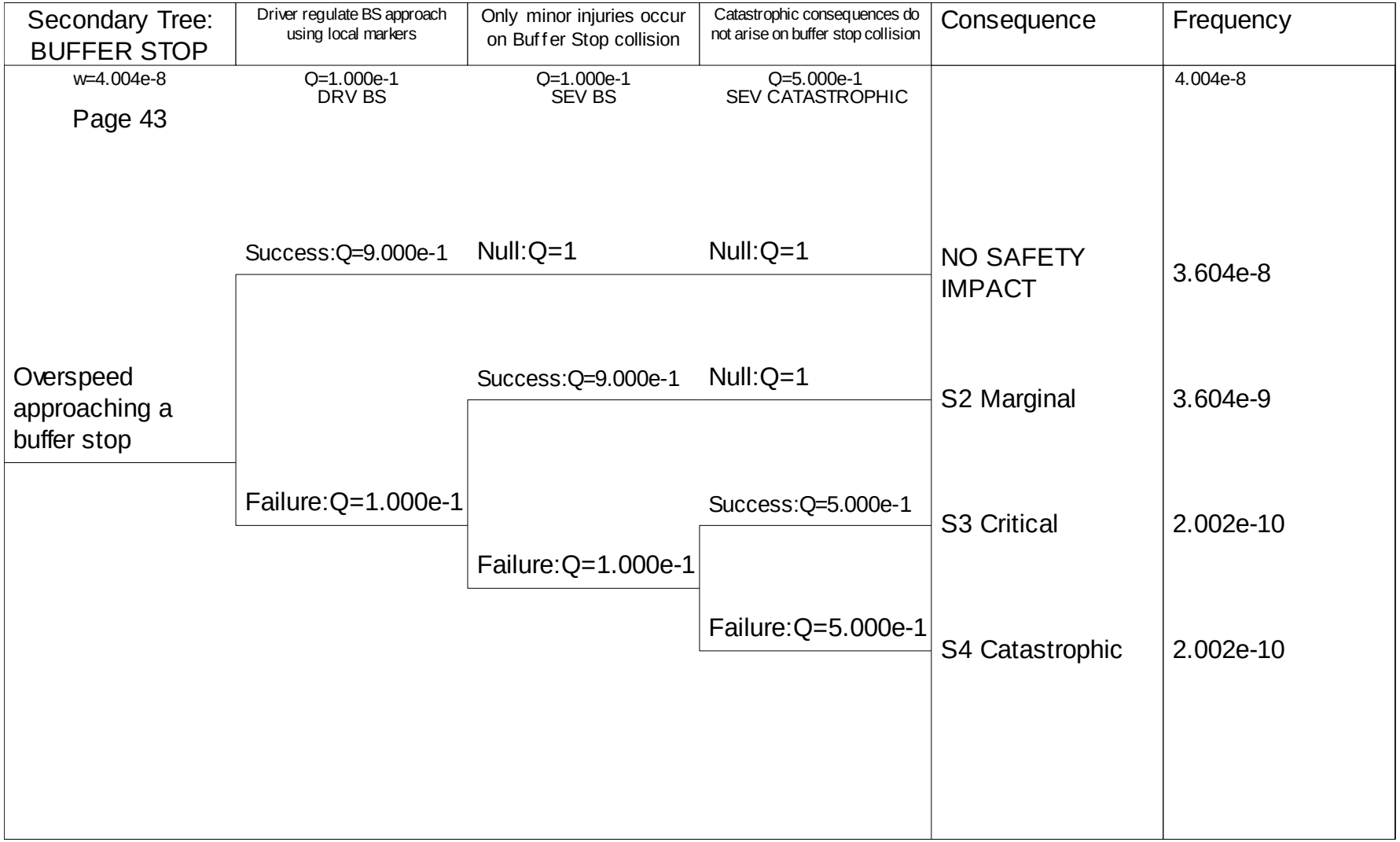
Failure to display Override status (failure mode deletion), including false enabling of override selection	Driver recognises that the Override indication from ETCS Onboard is missing	Override times out before any need for ETCS protection arises	Consequence	Frequency
w=1.000e-4 MMI-2F-DEL	Q=1.000e-2 DRV INDICATION NO OVERRIDE	Q=1.000e-1 TIME OUT		1.000e-4
Failure can arise if a driver mistakenly requested Override but assume not applied as Override status not displayed via DMI, or, driver inadvertently applied it and was not aware due to status not being displayed.				
	Success:Q=9.900e-1	Null:Q=1	POSSIBLE DRIVER DISTRACTION	9.900e-5
Failure:Q=1.000e-4:MMI-2f-DEL 'Failure to display Override status (Failure mode Deletion), including false enabling of override selection'		Success:Q=9.000e-1	NO SAFETY IMPACT	9.000e-7
	Failure:Q=1.000e-2	Failure:Q=1.000e-1	Not set	1.000e-7
		>> LOSS Page 38		

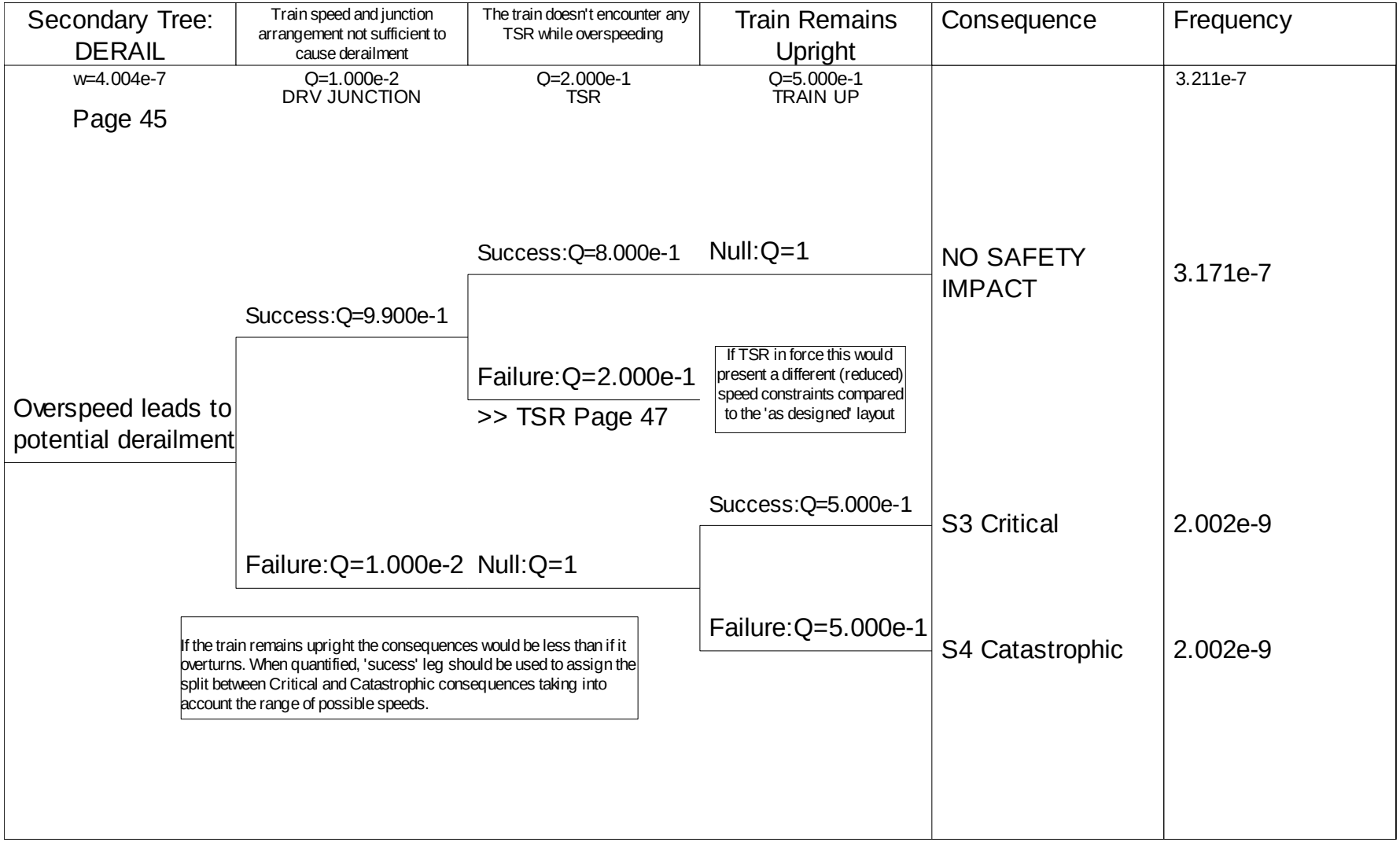
Failure to display Override status (failure mode insertion), including false enabling of override selection	Driver recognises that the Override indication form ETCS Onboard is incorrect	Consequence	Frequency
w=5.000e-3 MMI-2F-INS	Q=1.000e-2 DRV INDICATION OVERRIDE		5.000e-3
Failure:Q=5.000e-3:MMI-2f-INS 'Failure to display Override status (failure mode insertion), including false enabling of override selection'	Success:Q=9.900e-1	NO SAFETY IMPACT	4.950e-3
	Failure:Q=1.000e-2	Not set	5.000e-5
	>> UBA Page 48		



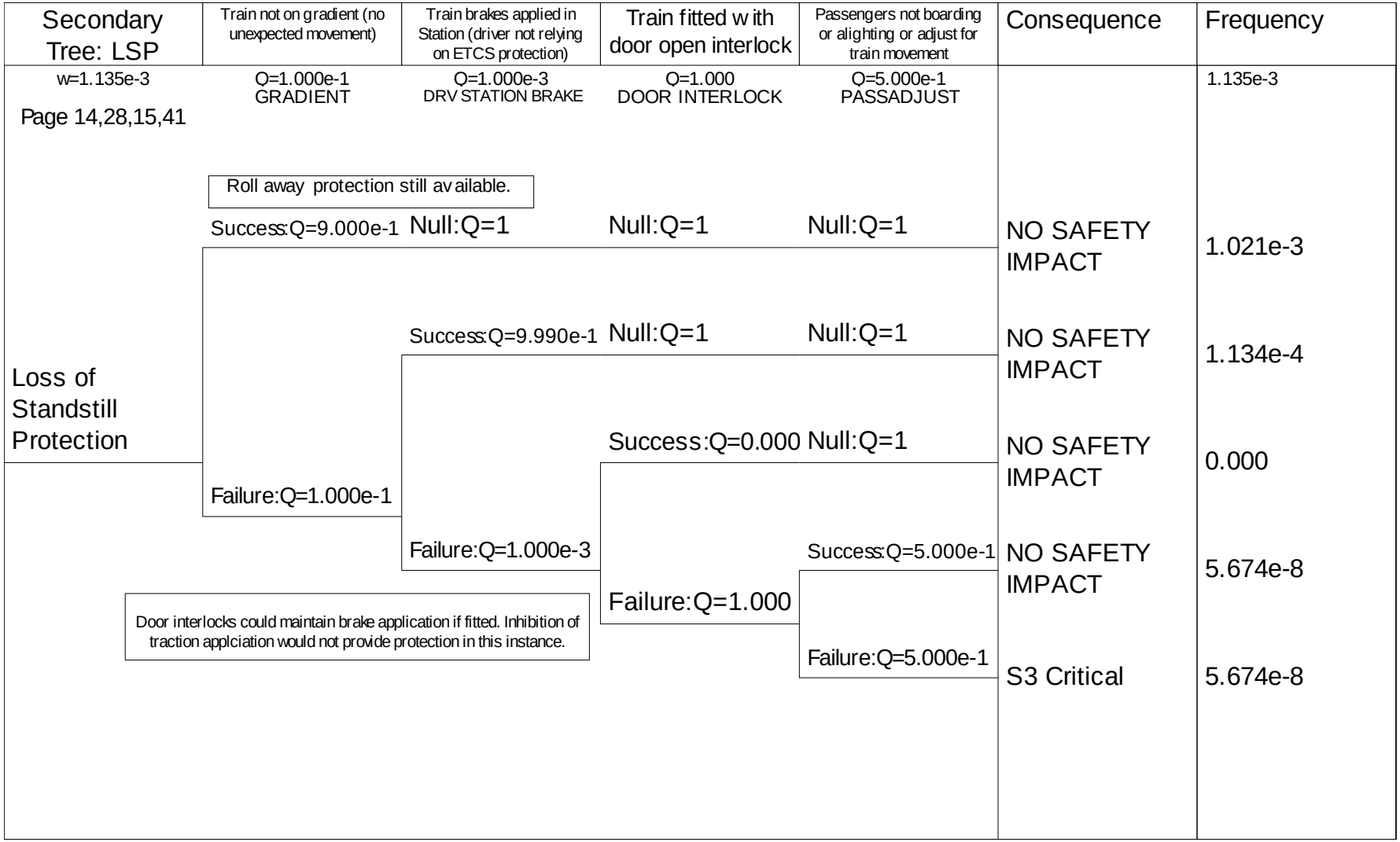


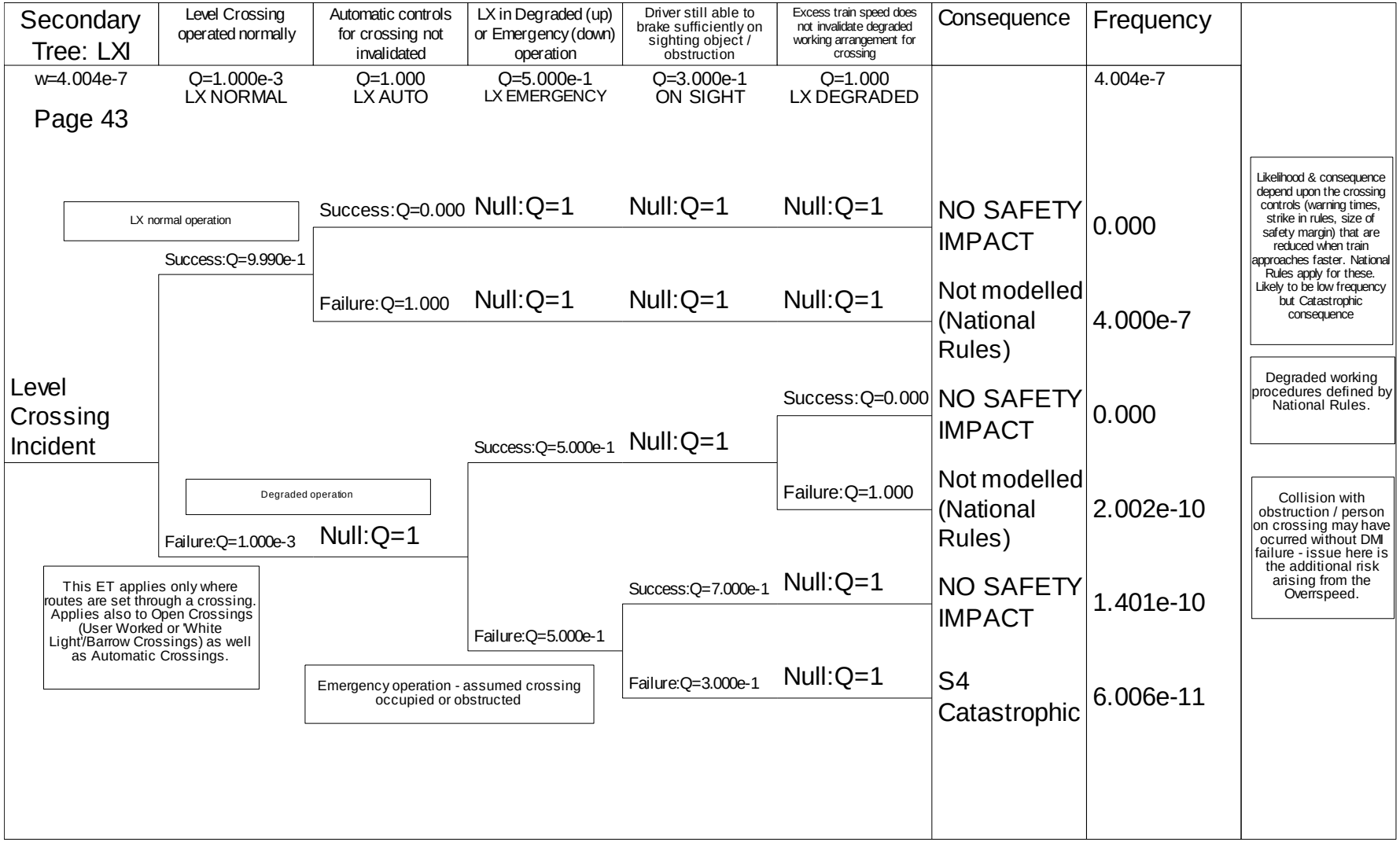
D.3 Secondary Event Trees (Immediate Effects and Consequences)

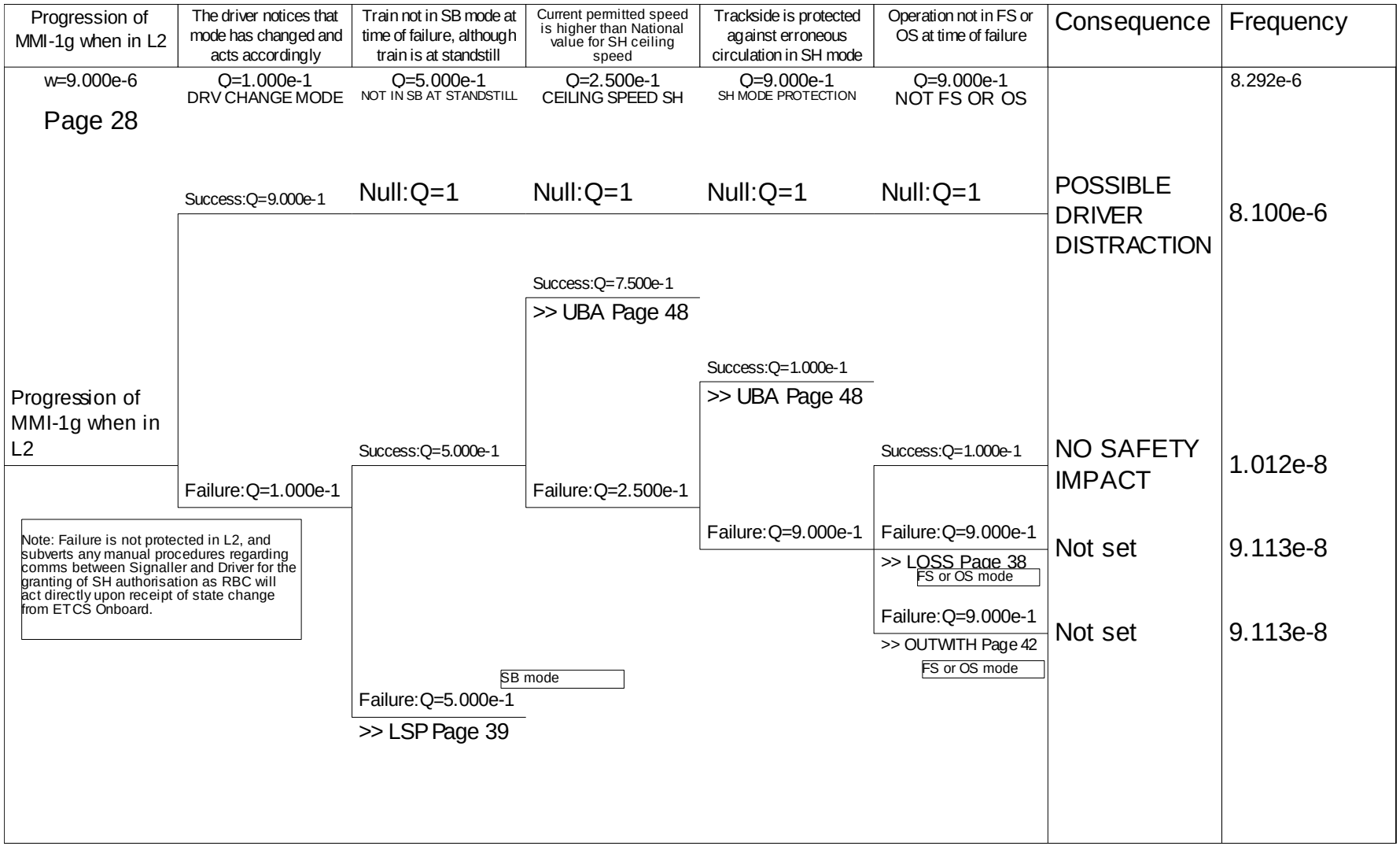




Secondary Tree: LOSS	Driving style would not invoke a need for Intervention	Consequence	Frequency
w=9.710e-7 Page 25,17,32,19,26,30,35,34,28,41,...	Q=1.000e-2 DRV STYLE		9.710e-7
Only a driving style that does not exceed any safety limits is a barrier for all transfers to LOSS. Where Level change also occurs route knowledge and from L2 possibly loss of MA information may also alert driver to the reduced supervision & protection			
	Success:Q=9.900e-1	NO SAFETY IMPACT	9.613e-7
No or reduced level of ETCS supervision or protection			
	Failure:Q=1.000e-2	S4 Catastrophic	9.710e-9
Warning and Intervention will not arise in the current Mode which the driver is not aware of. Worst case is where a driver's style relied upon Warnings to prompt a response or action.			





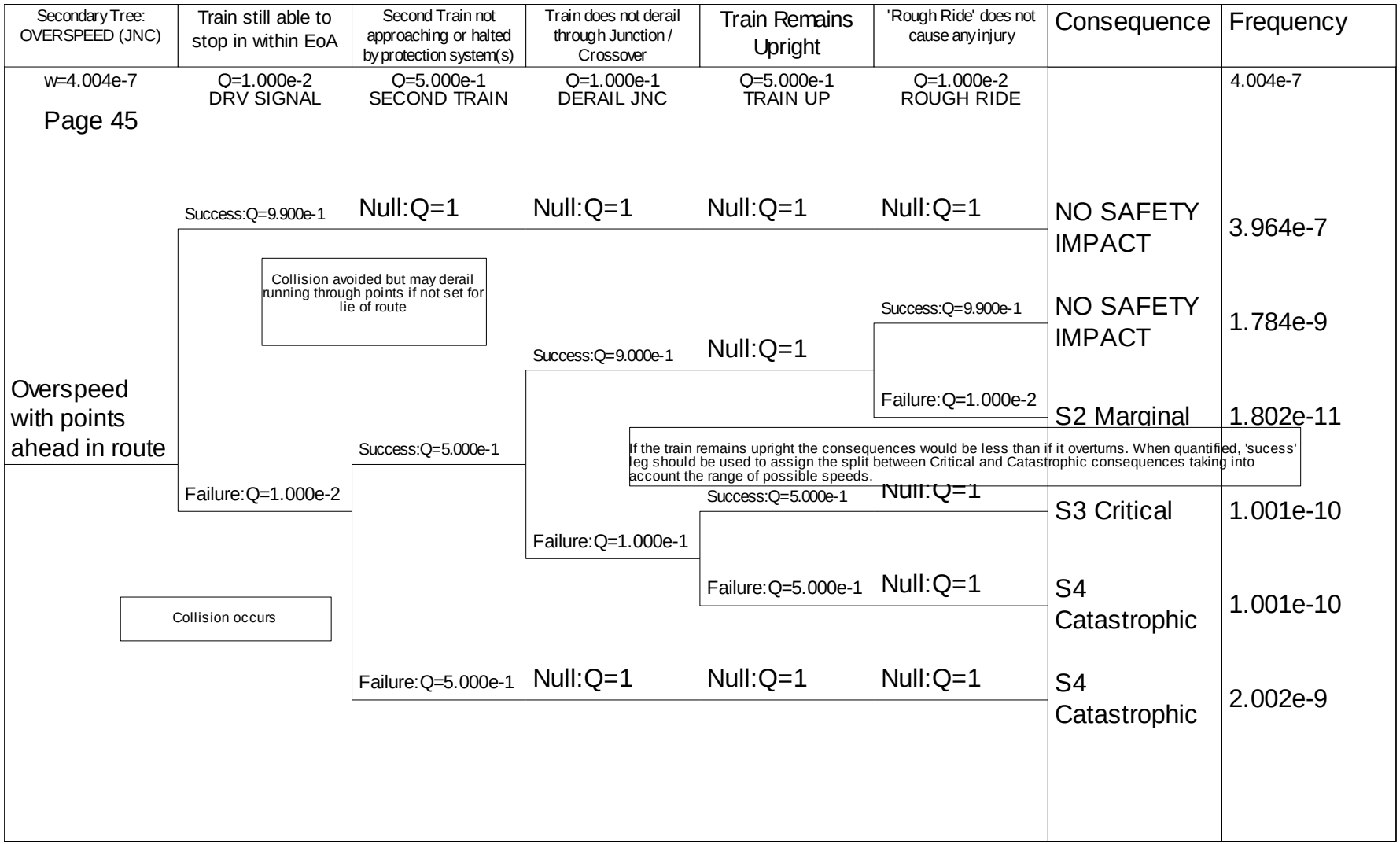


Secondary Tree: OUTWITH	Operational Rules require check of MA before starting away	Driving style would not invoke a need for Intervention	Consequence	Frequency
w=9.613e-8 Page 26,41	Q=1.000 START AWAY	Q=1.000e-2 DRV STYLE		9.613e-8
Operation outside the control of the signaller and signalling system	Success:Q=0.000	Null:Q=1	NO SAFETY IMPACT	0.000
	Failure:Q=1.000	Success:Q=9.900e-1	NO SAFETY IMPACT	9.516e-8
		Failure:Q=1.000e-2	S4 Catastrophic	9.613e-10

If L2 area retains trackside signalling, as the Signaller has not provided a valid MA for the train, the status of trackside signalling may alert driver to the failure (e.g. Controlled signals remain at Red). However, this will depend on National Rules.

Operating outside of RBC (if L2) or interlocking protection. Train detection supports interlocking so will not set conflicting routes, but incidents could arise with the affected train inc. collision, points run through, LX usage and engineering work.

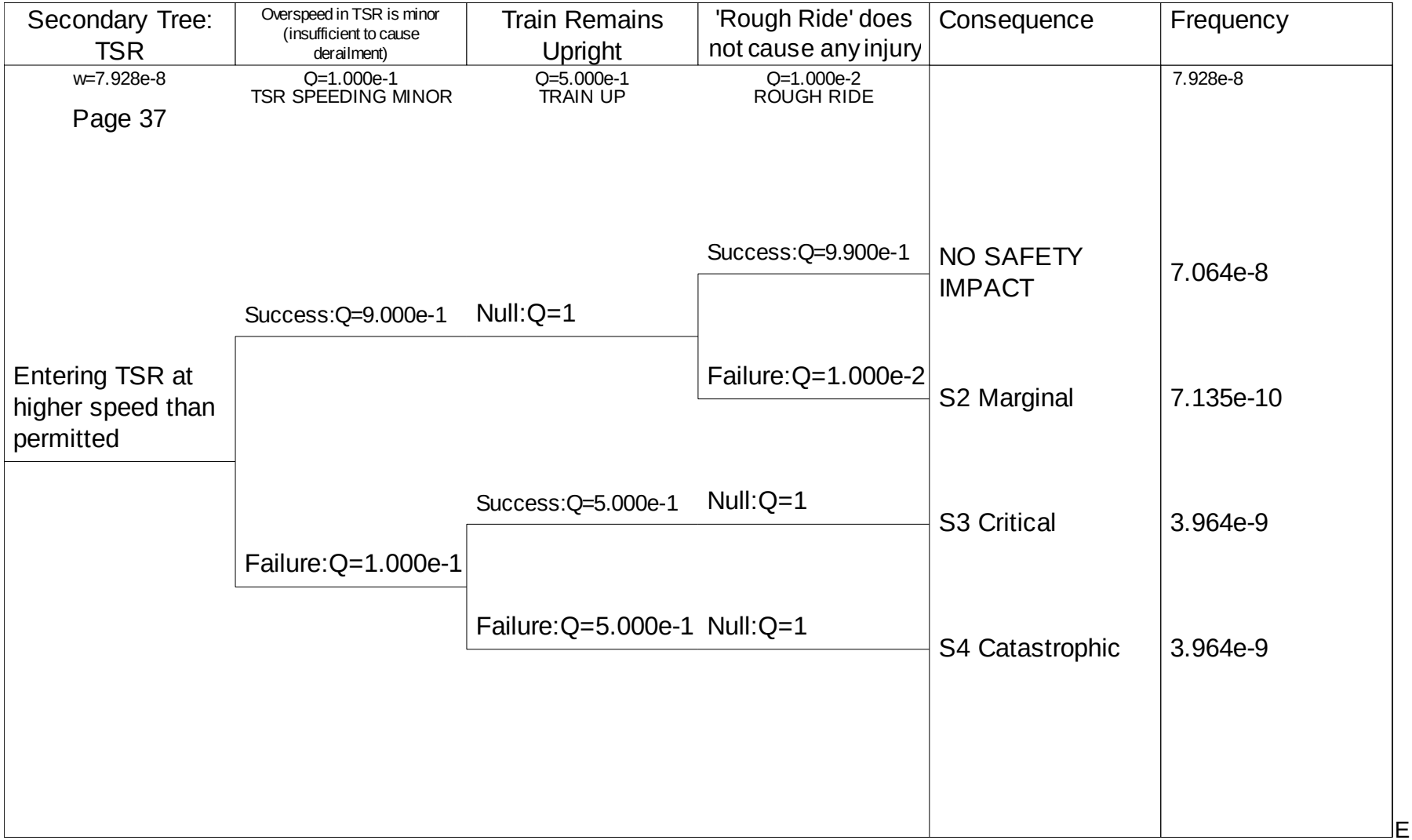
Secondary Tree: OVERSPEED Sht 1	Possible failure impacts	Buffer Stop not approached before fault revealed	Driver still able to brake sufficiently on sighting object / obstruction	No impact with any structure or stationary vehicle occurs	Train does not enter a route for which it is incompatible (e.g. track gauge, traction)	Consequence	Frequency	
w=4.004e-7 Page 2,23,31,29		Q=1.000e-1 PROB-BS	Q=3.000e-1 ON SIGHT	Q=1.000 STRUCTURE	Q=1.000 UNSUITABLE		1.562e-6	Requires national factors of trains, structures and rules to assess fully
DMI Failure results in Train Overspeed	Null:Q=1:STRUCTURE GAUGE	Null:Q=1	Null:Q=1	Success:Q=0.000	Null:Q=1	NO SAFETY IMPACT	0.000	
				Failure:Q=1.000	Null:Q=1	Not modelled (National Rules)	4.004e-7	
	Null:Q=1:INCOMPATIBLE	Null:Q=1	Null:Q=1	Null:Q=1	Success:Q=0.000	NO SAFETY IMPACT	0.000	Most likely a RAM issue not safety. Concern may be at a track gauge change point if overrun.
					Failure:Q=1.000	Not modelled (National Rules)	4.004e-7	
	Null:Q=1:BUFFER STOP	Success:Q=9.000e-1	Null:Q=1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	3.604e-7	
		Failure:Q=1.000e-1 >> BUFFER STOP Page 36						
	Null:Q=1:LX INCIDENT >> LXI Page 40							National Rules for degraded operation and maintenance apply [Written Order and use of on-track equipment]
	Null:Q=1:OBJECT	Null:Q=1	Success:Q=7.000e-1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	2.803e-7	
			Failure:Q=3.000e-1	Null:Q=1	Null:Q=1	Not modelled (National Rules)	1.201e-7	
	Null:Q=1:More Immediate Effects >> OVERSPEED SHT 2 Page 45							

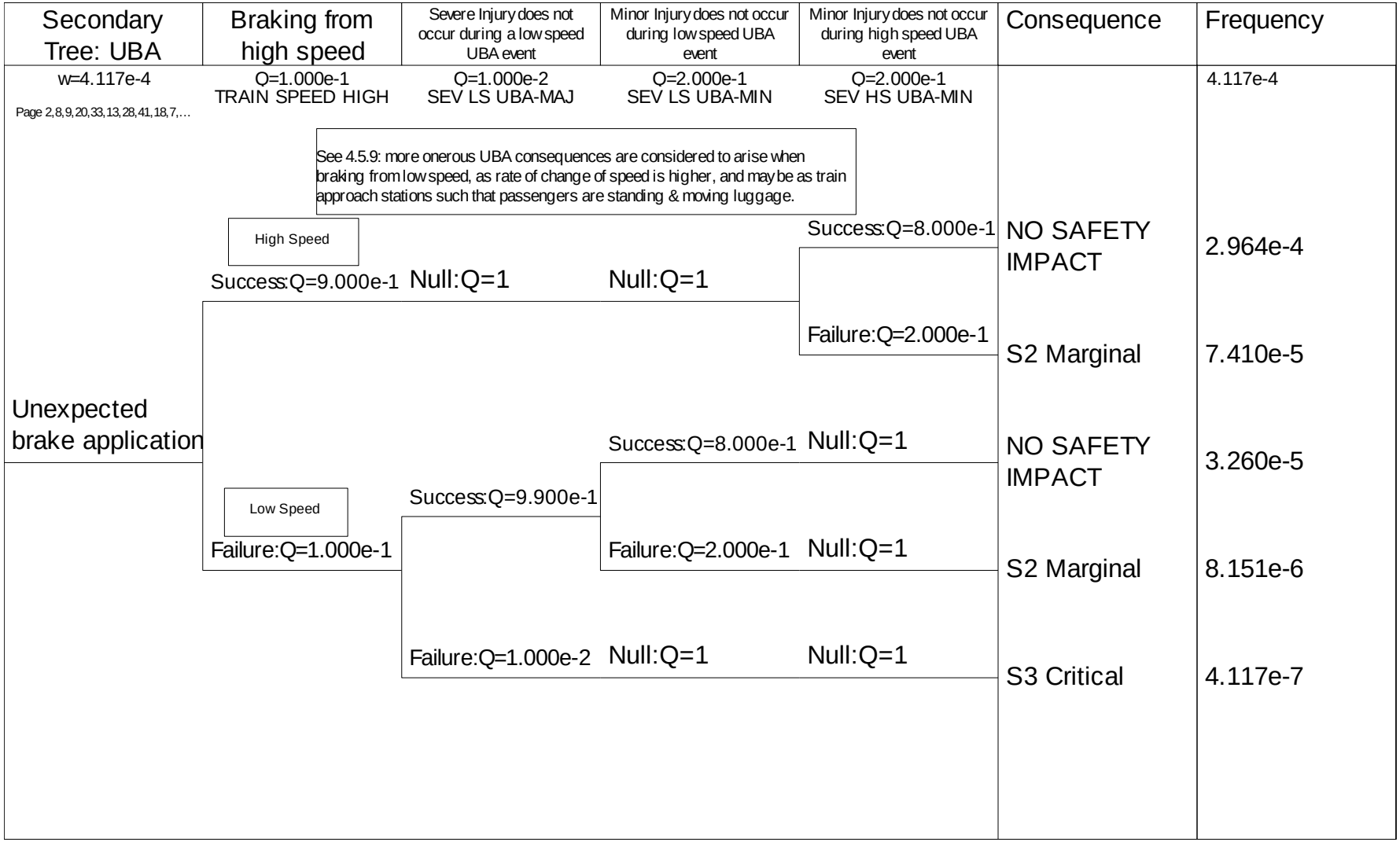


Secondary Tree: OVERSPEED Sht 2	Possible failure impacts	Overrun of intended stopping point not within a Non-Stopping Zone	Train still able to stop in within EoA	Track ahead of EoA is clear	'Rough Ride' does not cause any injury	Consequence	Frequency	
w=4.004e-7 Page 43		Q=1.000 NON STOP	Q=1.000e-2 DRV SIGNAL	Q=5.000e-1 LINE CLEAR	Q=1.000e-2 ROUGH RIDE		1.201e-6	
Overspeed Sht 2	Null:Q=1:ROUGH RIDE	Null:Q=1	Null:Q=1	Null:Q=1	Success:Q=9.900e-1	NO SAFETY IMPACT	3.964e-7	Specific factors for why Non Stopping Zone was set along with National recovery rules apply
					Failure:Q=1.000e-2	S2 Marginal	4.004e-9	
	Null:Q=1:Derailment >> DERAIL Page 37							
	Null:Q=1:Collision with another train >> OVERSPEED (INC) Page 44							
	Null:Q=1:Train overshoots platform stop position >> PLATFORM STOP Page 46							
	Null:Q=1:NON STOP ZONE	Success:Q=0.000	Null:Q=1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	0.000	
		Failure:Q=1.000	Null:Q=1	Null:Q=1	Null:Q=1	Not modelled (National Rules)	4.004e-7	
	Null:Q=1:COLLISION (Plain Line)	Null:Q=1	Success:Q=9.900e-1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	3.964e-7	
				Success:Q=5.000e-1	Null:Q=1	NO SAFETY IMPACT	2.002e-9	
			Failure:Q=1.000e-2	Failure:Q=5.000e-1	Null:Q=1	S4 Catastrophic	2.002e-9	

Secondary Tree: PLATFORM STOP	Driver compensates using local markers on Platform positioning	Train doors still open onto platform	Selective Door Opening available and used or driver / guard manage egress safely	Passengers do not attempt to disembark at an inappropriate location	Consequence	Frequency
w=4.004e-7 Page 45	Q=1.000 DRV STN	Q=5.000e-1 PLATFORM	Q=5.000e-1 SDO YES	Q=1.000e-1 PASSSTAYON		4.004e-7
Train approaches platform at higher actual speed than displayed on DMI	Success:Q=0.000	Null:Q=1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	0.000
	Failure:Q=1.000	Success:Q=5.000e-1	Null:Q=1	Null:Q=1	NO SAFETY IMPACT	2.002e-7
		Failure:Q=5.000e-1	Success:Q=5.000e-1	Null:Q=1	NO SAFETY IMPACT	1.001e-7
			Failure:Q=5.000e-1	Success:Q=9.000e-1	NO SAFETY IMPACT	9.009e-8
				Failure:Q=1.000e-1	S3 Critical	1.001e-8

SDO is a separate train system if fitted and not an ETCS related function





Appendix E Event Tree Data Description

This list should be read together with the event trees in Appendix D in order to set each base event in relation to the scenario where it is used.

Base Event	Description	Source / Justification	Value (probability of event failure)
ACK DISPLAY OK	Acknowledgement requests not obscured	If the area(s) of the DMI screen associated with displaying requests from the ETCS On-Board for acknowledgement were obscured a driver may miss the request. This event represents the probability that an acknowledgement would be obscured by the erroneously displayed information on the DMI screen.	0.5
ACK MISS NOT UBA	Deletion of Acknowledgement message do not lead to UBA	There are some messages to be acknowledged which do not lead to brake application. These messages are, for instance, messages provided when train is at standstill (TRIP acknowledgement, PT distance exceeded, reversing distance exceeded…) or other messages like permissive level transition, or text messages.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
AUTO ACK	Driver or DMI does not acknowledge 'automatically'	This event reflects either: 1. A situation where a driver automatically responds to a DMI displayed request, as a reflex or if occupied with other things at the time, without realising the full consequences of the action, or 2. A further failure of the DMI to falsely send the Acknowledgment without it being input by the driver. These situations could lead to entering a mode which the driver was not aware of, with potentially a reduced level of supervision and protection. Failures of type 2 are believed highly unlikely since such function will in most cases be a systematic error introduced during design and thus found during testing. Therefore, driver failures are believed to be the dominating type. Category A in the table in Section 5.6 is appropriate, since the driver will have to actively acknowledge a command they know that they haven't given.	0.001

Base Event	Description	Source / Justification	Value (probability of event failure)
BALISE DATA NOT HAZ	The balise information contains no hazardous data	This refers to the case that a balise in a construction area is erroneously read by the ETCS On-Board (hazard E1 in the analysis of MMI-6-CORR). Since the balise is not yet commissioned for traffic, it could theoretically contain any data intended for test purposes. Due to the complexity of the ETCS functions, most erroneous data will only have an impact on the availability of the ETCS supervision. Here, it is estimated that 50% will not cause any hazardous situation.	0.5
BALISE MISS NOT HAZ	The loss of balise information is not hazardous	This refers to the case that a balise in a traffic area is erroneously missed by the ETCS On-Board (hazard E2 in the analysis of MMI-6-INS). The value of the expected fraction of unlinked balise groups could be argued as a proper value for this probability. However, it is likely that several (perhaps all) balises in a construction area will have the same VBC Identity, which would mean that several (perhaps all) balises will be missed is E2 happens. To cater for this possibility, a significantly higher value than the fraction of unlinked balise groups is used.	0.25

Base Event	Description	Source / Justification	Value (probability of event failure)
CAREFUL	Driver takes a cautionary approach in the absence of speed indication	Even if the train's speed display is obscured, provided a driver takes a precautionary approach, supported by lineside signalling / route information, then speed limits might not be breached. This refers to the case when the speed limit is not supervised by the ETCS On-Board system, otherwise there would be no hazard. If the driver has no speed information and is not supervised by the ETCS On-Board system, it must be considered as a grave error to choose to continue the mission and exceed speed limits. This point to category A in the table in Section 5.6.	0.001

Base Event	Description	Source / Justification	Value (probability of event failure)
CEILING SPEED SH	Current permitted speed is higher than National value for SH ceiling speed	The event concerns the mode changing to SH without the Driver's knowledge. The change to SH mode will have to occur when the train is at standstill in order to be actuated, according to SUBSET-026 [Ref 1]. If the driver then sets off without noticing the unintended mode change he will accelerate the train up to a certain speed. If this speed is higher than the National value set for ceiling speed in SH, the ETCS On-Board would intervene and brake the train to a standstill (UBA). If the speed remains below this, movement will continue in SH Mode with reduced supervision and protection levels, and possibly outside of the interlocking or Signaller's control. Since it is likely that the national value for SH ceiling speed is quite low, the most probably outcome of this scenario is UBA.	0.25

Base Event	Description	Source / Justification	Value (probability of event failure)
CONTROLLED BRAKING	Driver recognises that display is erroneous or provides controlled braking response	Having been provided with a false display that braking was being applied by the ETCS (when it is not), the driver either recognises the display to be false, as there is no sensation of braking, or the driver's response is to apply a controlled (low-jerk) braking response (which may be a trained driving style, covering the ETCS braking so as to retain control when the ETCS intervention ceases). The failure of this event really represents the case when the driver over-reacts and applies full emergency brake although there is no operational reason. The reason could be that they think ETCS really should have braked (because of the indication of brake effort) but that the ETCS-brakes are malfunctioning (because there is no sensation of brakes being applied). This point to category B in the table in Section 5.6.	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
DERAIL JNC	Train does not derail through Junction / Crossover	The event addresses the scenario where a train has passed the protecting signal at Danger due to overspeeding and runs through the points at relatively low speed (as significant braking will have occurred even if the run-through was not prevented). In such circumstances, it is not certain that a train would derail, as margins exist regarding excessive speed, and some point operating equipment is designed to include a frangible link which breaks in the event of a run-through rather than derailing the train.	0.1
DOOR INTERLOCK	Train fitted with door open interlock	In the event that Standstill protection had been defeated and the station was on a gradient, the train may still be prevented from moving if door open interlocks were fitted on that particular rolling stock which independently maintains a brake application. This is not credited, since ETCS should not make any specific assumptions on train functions.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV ADAPT BRAKING	Driver adapts the brake effort to not cause passenger injuries	When the driver is warned about an unprotected level crossing or an operational situation which could be potentially hazardous, they will brake the train. This event signifies the probability that they are able to do this in a manner which doesn't cause any passenger injuries (people being thrown around or falling down in the train). The adopted value is believed to be a compromise between the two plausible situations: • If a 'last minute' warning is received then a significant braking effort will be required. The main goal of the driver will be to stop the train before the apparent point of danger is reached. Adapting brake effort to avoid injury is assumed to be secondary and the probability of "failure" would thus be one. • If the warning is not last minute then some adaptation of brake effort will be possible although this will dependent on time/ distance to apparent point of danger and also skill. A significantly lower probability of failure is reasonable, category B or C in Section 5.6.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV AIR TIGHT	Driver applies Air Tightness control without ETCS notification because of lineside signalling, written instructions…	If the need to apply Air Tightness control is for protection (e.g. due to atmospheric conditions or air pressure considerations), then injury could occur directly if the driver does not apply through their knowledge of the route. This event reflects the probability that a driver would apply air tightness controls when needed due to their experience of driving the route, even without the reminder / request to do so via the DMI. Note: there may be other reminders to a driver of the need for Air Tightness Control provided to manage the requirement on unfitted ETCS rolling stock or from pre-ETCS operation. The event is used for the scenario of tunnels with track condition 'air tightness': The driver would know/see that a tunnel is approaching and also know that the air intakes must be closed before entering tunnels. They also know that they are responsible for the action, even if it is natural to expect a reminder from ETCS. This would point to category C in Section 5.6.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV ANNOUNCED	Driver identifies level change via announcement	The faulty Level transition is likely to be discovered by the driver (by comparing the DMI display and the lineside signage). The hazardous case is believed to be a faulty change from Levels 1, 2 or 3 to Level 0 or NTC. If this is requested during Start of Mission, then the driver will always have to acknowledge the change, which will act as an additional alert. Category B in the table in Section 5.6 is appropriate.	0.01
DRV AVOID FIRE	The driver is able to find the correct evacuation area or otherwise avoid the fire	This event signifies the probability that the driver is able to find the correct tunnel stopping area, providing that they have discovered that the DMI displays the wrong area during a fire. Since this is a stressful situation and the correct area might even be behind the train, the category D in Section 5.6 is used.	0.5
DRV AWARE STOP	The driver realizes this is not the correct safe area and therefore doesn't initiate evacuation	If there is good visibility in the tunnel, the driver might discover that there is no evacuation possibility at the place where the DMI indicates the tunnel stopping area. Conservatively, category D in Section 5.6 is used.	0.5

DRV BS	Driver regulates BS approach using local markers	Buffer stops are a location where the train must always stop, unlike locations such as signals, junctions, level crossings, stations, where the need to stop will vary according to the local signalling conditions, service pattern and the effects of perturbation (impact of service affecting failures). Moreover, Buffer Stops are a very unforgiving stop location, and any collision will always lead to conditions that a driver would always wish to avoid – not only a collision, but the attendant reporting, incident investigation and potential implications to their future career. Therefore, every approach the Driver will have made to them will have involved stopping, and once the Driver realises that the train is routed towards the Buffers, they may be expected to adopt a driving strategy/tactic that is suitable for stopping. The Driver's approach is also likely to be based upon achieving a local benchmark, such as 30mph at the end of the platform, after which they will drive using train handling skills and route information responsive to largely out of cab information, including direct sighting of the stop location. Use of the DMI speed indication at this time (after the local benchmark) will be more as a 'check' than prime information source. The approach will probably include a greater than average degree of contingency (i.e. it will be slower) than other stop targets due to the unforgiving nature of Buffer Stops. The more experienced the Driver, the less the significant the indicated speed on the DMI will be in order for them to achieve the intended stop. These factors significantly reduce the possibility that the braking will be misjudged even if the DMI is indicating an incorrect speed. Overall	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
		driver skills in this regard are high, and the likelihood of a novice driver being present when such a DMI failure occurred such that they were more reliant on the indicated speed would balance their lower skill level. Overall a low probability of the failure would be expected. Notes on ETCS application design at buffer stops: If it is necessary for the train to be able to draw close to the buffers (e.g. to within 2m in some instances in the UK in order to fully platform the train), then it is likely that the Supervised Location (SvL) cannot be positioned at the Buffer Stop itself, as this will be too close to the EOA (located at the intended stop location) to allow a workable release speed for such a close approach. A possible solution to this, necessary if the infrastructure cannot be changed, is to position the SvL beyond the buffers, possibly supported by the use of OS mode to indicate to the Driver that the train is not 'fully' supervised. Whilst undesirable, unless such practices are formally prohibited, it could arise, and hence is captured in the Event Tree.	

Base Event	Description	Source / Justification	Value (probability of event failure)
		Although the above reasoning indicates a low failure probability, it is decided to use a conservative approach because of the complexity that the erroneous speed indication adds to the otherwise quite straightforward situation. Category C in Section 5.6 is used.	
DRV CHANGE MODE	The driver notices that mode has changed and acts accordingly	The driver recognises that the operating Mode has changed abnormally or without their request and acts accordingly, taking the responsibility that the operational rules requires for the new mode. They may recognise the new mode due to the new Mode status icon displayed. In the case of change to IS mode, the isolation switch itself serves as the indication. This base event is a barrier to the following DMI failure modes: • MMI-1b “False Command to enter NL mode'” • DMI-04j “False Isolation command” • MMI-1a “False acknowledgement of mode change to less restrictive mode” • MMI-1g L2 ”False request for SH Mode”	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
		• DMI-04a “False command to exit shunting’” • MMI-1g “False request for SH Mode” Note 1: The likelihood may also be affected by Operational Rules regarding any requirements placed on a driver before starting away e.g. to check the MA as a last action before setting off. Note 2: As change can only occur at Standstill (except for the change to IS mode), the Driver must also commence driving without any further Mode changes - this should be factored into the probability of this event. Since the base event covers many different operational situations, it will inevitably not be exactly suited for all the above failure modes. The adopted figure is believed to be conservative for most of the situations. Category C in Section 5.6 is used.	
DRV INDICATION	Driver recognises that indication from ETCS On-Board is incorrect	Driver is able to recognise that the indication from ETCS On-Board is incorrect and acts accordingly. Separate values are considered for some situations; see DRV INDICATION XXX events below.	0.3

Base Event	Description	Source / Justification	Value (probability of event failure)
		Refers to the driver discovering the following DMI errors: • MMI-2C: False presentation of track adhesion factor (shown as applied when not) • DMI-02E: Notification of spurious Train Data change (which normally is from source different from the driver) • DMI-02A, -02G: False presentation of Warning or of 'LX not protected' • DMI-01H, -01I, -03G, -03H: Failure to present or wrong presentation of TTI or DDT Failure category D in Section 5.6 is used in order to be generic.	
DRV INDICATION NO OVERRIDE	Driver recognises that Override indication from ETCS On-Board is missing	The Override is active, which means that the driver has activated the function. In this case, they should be able to easily recognize that the Override status is missing. Failure category B in Section 5.6 is used.	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV INDICATION OVERRIDE	Driver recognises that Override indication from ETCS On-Board is incorrect	The Override is not active, which means that the driver has not activated the function. In this case, they should be able to easily recognize that the Override status is faulty. Failure category B in Section 5.6 is used.	0.01
DRV INDICATION SLIPPERY	Driver recognises that Adhesion Factor “slippery rail” indication from ETCS On-Board is missing	The driver has just selected the Adhesion Factor “slippery rail” and expects a feedback from ETCS On-Board via DMI. They will most probably react if there is no such indication. Failure category A in Section 5.6 is used.	0.001

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV JUNCTION	Train speed not sufficient to cause derailment	Whilst not to the same extent as approaching a Buffer Stop, a driver will be aware of the reduced speed limits for junctions and crossovers, and seek to manage their speed through the junction. The train speed may also be below the derailment speed even with an incorrect speed displayed via DMI, and the arrangement of the junction and alignment may not be onerous. For a lower speed turnout or crossover, there may also be speed boards advising of the speed reduction. Overall, a probability that the driver does not regulate the train speed sufficiently, to a magnitude that derailment would occur, even with an incorrect train speed displayed on the DMI is expected to be low. Category C in Section 5.6 is generally the most optimistic value for driver mistakes in this analysis. It is not believed appropriate to use in this scenario (mainly connected to MMI-2A.1), since after all the driver is presented with false information via the DMI. Instead, category B in Section 5.6 is used.	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV LANG COMPETENCE	Competent in the new language	If the driver is competent in the language in which DMI is now erroneously presenting information, then they may use it. If not, the driver should take ETCS out of service if the required language cannot be restored; this is however already credited with the event OUT OF SERVICE in the scenario.	0
DRV NO CONFIRM	The driver doesn't confirm the erroneous text message	There is a chance that the corrupted fixed text message doesn't make sense to the driver, or that it is operationally out of its context. In such case, they might not confirm the message and therefore invoke the safe reaction defined by trackside. However, since there are no harmonized rules in the scope of the TSI CCS on how to set the qualifier for text confirmation, this barrier is not credited.	1.0
DRV OVERSPEED	Driver respects the permitted speed plus a margin.	Driver does not rely on warning indication while driving and respects the permitted speed plus a margin.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV REPEAT PROT	Driver acts to stop cyclical movement and intervention	After Intervention, a repeated spurious ACK for brake release could result in a cyclic action of train movement and Intervention if the train were on a gradient. In many cases relatively large train movements would be required before the situation became catastrophic, and hence many cycles of intervention and unexpected movement, though in the worst case this could be relatively few cycles if the train had halted very close to a fouling point. It is considered unlikely that a Driver would not act to stop train movement after one or two further Interventions as it would be clear that some problem existed, and thus the probability of this event is potentially more the likelihood that a the Driver was incapacitated or not present for some reason. However, since it is not likely that there will exist procedures or training for such an event, Category B in Section 5.6 is used.	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV RV ALT	Driver able to adopt alternative Mode or Isolate ETCS and reverse	After intervention whilst starting to Reverse, the Driver may have time to adopt an alternative Mode that permits reverse movement (e.g. NL or SH), or isolate ETCS and reverse manually. This will be consequent on the nature of the emergency, the time available, and the driver's understanding of why there was an intervention. Given the scenario that there is an emergency, it is not certain that the driver will have time enough to first understand that there has been an ETCS malfunction and then to adopt an alternative way of reversing before the potential accident (technical means include selecting SH mode or isolating the ETCS On-Board). Given the complex and stressful situation, a value in the mid range of category D in section 5.6 is used.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV SIGNAL	Train still able to stop within EoA	Driver approaching a red signal in Level 0 in a L1 fitted area, or L1/L2 in SR, and hence ETCS is not supervising to halt in rear of the signal. In L1/L2 SR, a driver is expected to be driving cautiously in the anticipation of a problem or the need to stop. It is likely in such instances that driver will be able to stop in rear of the junction fouling point even if approaching at some higher speed than thought, due to a DMI error. The limiting case is considered to be in Level 0 when the driver is driving utilising trackside signals. The driver should be aware that the signal ahead could be at red from the aspect of the previous signal, and thus be prepared to stop at the next signal. However, It may also be relatively late on the approach when a driver realised the extent of the overspeed. In L0 or overlay areas National protection system(s) (e.g. ATP, TPWS) may act automatically to halt the train, possibly within the overlap or short of the fouling point (if protecting a junction).	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
		It is possible that the signal ahead has reverted to Red unexpectedly, such that the driver is not anticipating this on the basis of the last signal observed. In such instances, a driver may not always be able to stop in rear of the signal, and the train will in all probability not be able to stop short of the fouling point. The severity of the accident may be marginally increased as a result of the higher speed, but the DMI failure is not considered likely to define whether an accident occurs or not, and can therefore be discounted in this modelling. Category B in Section 5.6 is used.	

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV SPEED RECOG	Driver recognises displayed speed incorrect	The difficulty for a human in identifying a speed error increases with train speed, and immediately following a reduction in speed. Both of these are relevant when braking to a target. Note: In practice, there will be a range of probabilities that a driver recognises the failure and duration of a hazardous situation before the fault is revealed, which will relate to the individual drivers skills and the magnitude of the error in the displayed speed. The larger the error, the higher the likelihood of fault being revealed quickly. However, even if the duration between a fault occurring and it being revealed is small, there still exists a potential that a harmful situation will develop due to the unfortunate juxtaposition of the timing of the fault and the location of the train. The probability of DRV SPEED RECOG therefore also reflects the unfortunate probability that a harmful situation develops before the fault is revealed. Category D in Section 5.6 is used.	0.3

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV STATION BRAKE	Train brakes applied in Station (driver not relying on ETCS protection)	It is possible that, on the basis that ETCS functionality provides Standstill protection, all drivers may not apply the train brakes at every station. This event reflects the likelihood that brakes were not applied when stationary at stations. Operational Rules may differ on the requirements in this respect as well as possible driving styles or lapses by individual drivers however it is brought forward as a safety requirement SReq09 that the driver is not supposed to rely on ETCS to remain at standstill. Thus, this can be seen as a failure and category A in the table in Section 5.6 is used.	0.001

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV STN	Driver compensates using local markers on Platform positioning	The driver will be expecting to stop at the Station, and will generally have experience in stopping the train at the prescribed location. The Driver can be expected to exercise greater care if the consequences of failing to stop in the intended location are greater, for example if there is a starter signal at danger. However, the driver is expected to regulate the braking effort according to the speed indications of the DMI. By the time the driver discovers that the speed is too high to stop at the intended position, there is a large risk that it will be too late (the platform markers are at the platform, not before). The barrier is not credited at all.	1.0
DRV STYLE	Driving style would not invoke a need for Intervention	Even though the driver is unaware that they are operating in a Mode with a reduced (or substantially no) supervision and protection, lineside signalling / route information may mean that they drive in a manner where the need for intervention or protection does not arise, and hence the lack of it does not lead to harm. The event is used in scenarios:	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
		• MMI-2B “False presentation of mode”. Here, the driver is presented with the information that the ETCS On-Board system operates in FS mode, while it is actually in e.g. SR or UN mode. The driver is unaware of this fault because barrier FALSE MODE has failed. Since in the lower level modes there will be no planning area for the driver to base their driving on, it is likely that they will base the driving on other types of information such as route information, wayside signals and boards. The situation will however be quite confusing for the driver, and therefore only category B in Section 5.6 can be justified. • Secondary event tree LOSS “No or reduced level of ETCS protection”. This event tree connects to many different hazardous situations. As a bounding case, it is considered that category B in Section 5.6 can be used also here.	

Base Event	Description	Source / Justification	Value (probability of event failure)
		• DMI-02B “False presentation of IS mode (shown as IS mode when not)”. Here, the driver thinks that the ETCS On-Board operates in IS mode and that he is therefore fully responsible. The event therefore signifies that some limit supervised by the ETCS On-Board is breeched. Since there is no way for the driver to know what limits are actually supervised and category B in Section 5.6 can be used also here. In summary, category B in Section 5.6 is believed appropriate. This is slightly more conservative than the figure used for driver failures in the safety analysis for the ETCS Core Hazard, see Section 10.1.4 in SUBSET-091 [Ref 5]. This extra conservatism is justified by the fact that in these situations, due to the DMI indication failure, it would be unclear to the driver where to retrieve information for train operation (from the DMI or from route information/wayside signals) and to what extent the ETCS On-Board supervises the train.	
DRV STYLE LAF	Driving style appropriate for poor adhesion conditions and avoids any need for ETCS intervention	In case of Max Deceleration	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
		The driver is aware of the poor adhesion conditions. Whilst he believes that the Low Adhesion compensation factor in the ETCS is applied though it has not been, he is likely to moderate his driving style appropriate to the conditions, and the availability of other cues and route information (planning area) allows him to drive at an appropriate speed. A slightly more pessimistic value than for DRV STYLE is believed appropriate, since it is difficult for the driver to manually adapt the speed of the train in approach of a target. It could well be the case that drivers adapt a driving style of relying on the brake curves of ETCS to moderate their driving in poor adhesion conditions. Or in case of DDT or TTI The driver is aware of the poor adhesion conditions. Whilst he believes on additional info (TTI, DDT), he is likely to moderate his driving style appropriate to the conditions and consider an appropriate speed. A slightly more pessimistic value than for DRV STYLE is believed appropriate, since it is difficult for the driver to manually adapt the speed of the train in approach of a target.	

Base Event	Description	Source / Justification	Value (probability of event failure)
		It could well be the case that drivers adapt a driving style relying only on TTI or DDT info to evaluate time to start braking to moderate their driving in poor adhesion conditions. Category C in Section 5.6 is used.	
DRV VBC CORRUPTION	Driver discovers the erroneous VBC	The only check that the driver is expected to perform is the validation of the set VBC; this is already contained in the initiating event MMI-6-CORR. It is considered very unlikely that the driver will again – during a mission – go into the set+validation window of the DMI and check that is was really the correct VBC. The barrier is not used at all and therefore the failure probability is set to one.	1.0
DRV VBC INSERTION	Driver discovers the inserted VBC	In this case, the driver has not tried to activate a VBC, so he has no reason to perform the check.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
DRV WARNING	Driver responds correctly to warning of imminent intervention	The driver may believe that ETCS is isolated, as IS mode is erroneously displayed on the DMI. When ETCS warns of approaching intervention a driver may therefore not believe this to be correct and ignore it, leading to ETCS applying the train brakes. This event reflects the likelihood that a driver ignores the warning of intervention in this situation. N.B As there has already been an initial DMI mode display error, there could be further DMI errors (or a common failure) which may also mean that the Warning is not presented to the driver. Therefore, this barrier is not credited to any great extent. Also, the scenario (DMI-02B) involves already two driver barriers; therefore it is not reasonable to further credit the driver in any decisive manner. Category D in Section 5.6 is used.	0.3

Base Event	Description	Source / Justification	Value (probability of event failure)
EXTERNAL ACCIDENT	There is no external accident which invokes the need for ATC	This is the probability for an accident in an external system, e.g. chemical power plant, which causes toxic fumes or other atmospheric conditions which can cause death or serious injury. In such an extreme situation, the closure of the fresh air intake on a train in the area could indeed act as a barrier against an accident with catastrophic consequences. It is very difficult to estimate the probability for such an event, but here the probability of a tunnel fire (see event FIRE) is used to estimate a probability which probably is in the same order of magnitude.	$2*10^{-6}$
FALSE MODE	Driver recognises that mode displayed on DMI is incorrect (mode changed to a reduced level of supervision)	Similar to “DRV INDICATION”, but applying specifically to the Mode displayed on the DMI rather than indications and other status displays. Note: For a change to a lower level of supervision and protection, the Driver will have had to accept an ACK of mode change.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
		If the displayed mode did not change, this might be recognisable from the rest of the displayed information, as the ETCS On-Board would not be issuing the data relevant to the mode displayed. A more onerous situation would be where the mode displayed had changed to one of reduced supervision and protection from that originally, but the actual change in the ETCS On-Board was to a mode with even lower levels of supervision and protection (e.g. FS to SH but OS is displayed). Note also, that a driver may be engaged with other activities and responding to external stimuli, and may not examine the mode change in detail, simply providing the ACK Confirmation to avoid intervention. Even though the mode displayed may not have changed, unless the driver recognises that the displayed information is incorrect for the mode displayed, they may trust the DMI and simply query what the 'ACK' had been about, rather than assume that the mode had changed and the displayed mode icon was wrong.	

Base Event	Description	Source / Justification	Value (probability of event failure)
		Transition to NL mode does not require acknowledgement, and so no stimuli for the driver to check the DMI for the changed mode, however, transition to this mode requires a specific request by Driver, who would therefore be looking for the change. Spurious request of mode change is covered as separate Hazardous Situations (e.g. MMI-1b) and does not apply where this event is used. Refers to the driver discovering the following DMI errors: • MMI-2B: False presentation of mode • DMI-02B: False presentation of IS mode (shown as IS mode when not) The category C in Section 5.6 is used as a generic representation, although more positive figure could be pursued for some modes (e.g. IS) if necessary.	
FIRE	There is no fire in the tunnel	This is the probability that there is a fire in a tunnel where the ETCS On-Board shows the wrong distance to the tunnel stopping area. Thus, it is not only the probability that there is a fire in any tunnel, but in a tunnel where track condition “tunnel stopping area” is used.	$2*10^{-6}$

Base Event	Description	Source / Justification	Value (probability of event failure)
		The probability for fire in any tunnel (when a train is passing it) is set to $2*10^{-6}$. This is based on the following statistics: • During the years 2006-2010 there were 19 726 railway accidents during $2.1*10^{10}$ train-km in the EU countries <ref: ERA's Common Safety Indicators database >. • Out of the investigation material that is available to ERA, tunnel fires accounted for 0.4 % of the total amount of accidents. If applying that rate for the total figure of 19 726 accidents, there were 79 tunnel fires during $2.1*10^{10}$ train-km. • To translate this into a probability per tunnel passage, infrastructure statistics from one country is studied. United Kingdom has approximately 300 tunnels <ref: comparison of various sources> in 16 000 track km <ref: UIC Railisa database>, which means an average density of $1.88*10^{-2}$ tunnels per km. If assuming that o United Kingdom's tunnel-per-km rate is representative to the EU countries, and	

Base Event	Description	Source / Justification	Value (probability of event failure)
		○ the traffic is equally distributed between track with tunnels and track without tunnels (so that train-km can be set equal to track-km) it would mean that the EU countries has $1.88*10^{-2} * 2.1*10^{10} = 3.9*10^{8}$ tunnel passages during the period for which there were 79 tunnel fires. • The probability for a tunnel fire during one tunnel passage becomes $79 / 3.9*10^{8} = 2.0*10^{-7}$. • Even if the assumptions and statistics above are believed reliable, there could be uncertainties. Therefore a safety margin of 10 is taken into account, which means that the probability for FIRE is finally set to $2*10^{-6}$. In the long run, the aim should be that all tunnels use track condition “tunnel stopping area” since it is a safety enhancing feature; therefore the above figure is not further decreased.	

Base Event	Description	Source / Justification	Value (probability of event failure)
GOOD ADHESION	No requirement to apply poor adhesion status arises	If no need for poor adhesion adjustment of the ETCS arises whilst the DMI error is present, then the harmful situations of not having it applied when it should be would not arise, and the potential for the DMI failure to result in harm would not develop. [The braking distance indicated on the DMI will not be less than that required to achieve the braking target.] Bad adhesion conditions could occur when fallen leafs cover the rail or when snow/rain is present. Most modern trains have sanding equipment which could mitigate the bad adhesion when deployed. This would justify quite a low figure for the failure of this event. It is assumed that 5% of the time, there would be a real need for reduced adhesion in the brake curve calculations.	0.05

Base Event	Description	Source / Justification	Value (probability of event failure)
GPI DATA OK	Driver's estimate of missing GPI data is sufficiently accurate	If no Geographic Position information is displayed to a driver, and they decide to compensate for the missing information by estimating their position, provided their estimate is reasonably accurate, there is minimal risk that the signaller's action in response to the information would result in a dangerous situation developing. This will depend upon the driver's skill and the nature and availability of other sources of position information. This point to category C in the table in Section 5.6.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
GRADIENT	Train not on gradient (no unexpected movement)	Used in two situations: 1. In secondary tree LSP when having lost standstill protection, the train will not roll away unless it is on a sufficient gradient (to overcome static friction in the train). Roll away protection would still be available. 2. In DMI-04h to determine if train movement occurs after an ETCS Intervention if the train brakes are removed by ETCS due to a spurious ACK without the driver's knowledge. Consideration will need to be given to both situations in quantifying the even probability, as the likelihood of being on gradient may differ between the two (as Situation 1 will only arise in Station areas, whereas situation 2 could occur anywhere on the Infrastructure). Also, in the case of situation 2, it is also likely that the brake controller will be in a position under which train movement could occur if on a gradient as the train was in motion prior to the Intervention.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
HIGH-LOW DISPLAY	Train speed displayed higher than actual	The failure mode of the DMI speed display could result in a higher speed than actual being displayed as well as a lower speed (a higher speed simply being a performance issue in that a driver may travel more slowly than intended). In the absence of any knowledge regarding the internal components of the DMI, the failure could be assumed to have an equal chance of giving an erroneously high displayed speed as of a lower one.	0.5
IN L0	Train in Level 0 when failure occurs	Event to separate out situations where operation is in Level 0 as the subsequent consequences of interest are only applicable to that level. It is assumed that an ETCS On-Board is in Level 0 no more than 10 % of the total time, since operation in Level 0 is deemed much less frequent than in the other levels.	0.9

Base Event	Description	Source / Justification	Value (probability of event failure)
INTERUPTION	Driver not interrupted	Routine start-up would be that the driver selects START and then immediately acknowledges UN mode when proposed by the ETCS On-Board. To be in UN without the driver's knowledge they would need to have been distracted in the short time between selecting START and completing the deliberate adoption of UN. Highly unlikely in conjunction with the prior DMI error, but recorded as potentially possible.	0.001
ETCS ON-BOARD REJECTS	ETCS On-Board rejects the spurious request as the conditions to apply or accept the request are not in place	The specific spurious request or response generated by DMI error is of a type where it requires the ETCS On-Board to be expecting it, and if the input to the ETCS On-Board does not arrive within this designated acceptance window it will not be accepted. The acceptance window is defined by: - there is a request to perform the mode change in question - train at standstill This event is used as a barrier in the following case: - MMI-1A: False acknowledgement of mode change to less restrictive mode	0.05

Base Event	Description	Source / Justification	Value (probability of event failure)
		It is possible that DMI failure modes could result in repeated, periodic or constant spurious request to the ETCS On-Board. To avoid situations where a standing fault is present which would be acted upon once the acceptance criteria became effective, the ETCS design or application procedures should alert a maintainer where multiple or repeated provocations of the ETCS On-Board have occurred. This is assumed to be implemented by defensive programming techniques standard for SIL4 systems. The same value as for STANDSTILL is conservatively used, even if more conditions apply in certain situations. If needed to reduce this conservatism, the probability that there is a request pending could be taken into account. However, this would mean looking individually at each mode change scenario that requires an acknowledgement.	

Base Event	Description	Source / Justification	Value (probability of event failure)
LEVEL 1 OR LEVEL 2 OP	ETCS operating Level 1 or 2	Event to separate out situations where operation is in Level 1 rather than Level 2, as the subsequent consequences of interest are different for different operational Levels. The probability is used in situations where it has already been decided that Level 0 is not used. Here, it is assumed that it is just as likely to operate in Level 1 as it is to operate in Level 2.	0.5
LEVEL RULES	Operational rules limit the conditions for adoption of change	The SRS details how level change is implemented at Start of Mission (5.4.4). SUBSET-026 [Ref 1] clause 3.18.4.2.4 permits the Driver to initiate a Level change at other times. The Table of Priority protection as well as any additional Operational Rules may provide mitigation, which is considered here. The requirement that the train is at a Standstill is managed as a separate event. Since no such Operational Rules are harmonized within the scope of the TSI CCS, this barrier is not credited.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
LINE CLEAR	Track ahead of EoA is clear	Whilst a train may be travelling faster than it should be (Overspeed) such that it has not been possible to stop within the permitted movement authority, braking will have been applied and the overrun will be of limited length. A collision would only occur if there was another train or obstruction within a relatively short distance ahead of the EOA. This event represents the probability that a collision occurs after exceeding the EoA (i.e. a “SPAD” or exceeding the SvL). An obstruction could include engineering work or on track vehicles.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
LX AUTO	Automatic controls for crossing not invalidated	This event determines if the level of (excess) approach speed is sufficient that the normal operation and safety margins of crossing operation are achieved. Strike in times and barrier lowering sequences will be affected by the higher approach speed. Whilst it is likely that the crossing will still operate safely due to the safety margins inherent in the application design, this will need to be addressed taking into account Operational Rules for crossing operation and design in conjunction with the magnitude of Overspeed occurring. The event is not credited as a barrier, but can be quantified if there is a need to analyse all level crossing scenarios which are depending on Operational Rules.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
LX DEGRADED	Excess train speed does not invalidate degraded working arrangement for crossing	In a similar manner to “LX AUTO”, this event addresses the likelihood that the higher approach speed does not fundamentally alter safe use of the crossing in the particular circumstances of degraded operation of the crossing. Note: The DMI failure itself may not be the cause of the collision, which may have been unavoidable irrespective of the increased speed of approach. N.B. The emergency situation modelled in another path on the tree does not consider the crossing controls, as it addresses the situation where an emergency stop by the driver is required to the situation ahead (which is outside the control of the signalling system), and so this goes directly to stopping the “ON SITE” event which considers if the train can stop where it needs starting from the increased approach speed. The event is not credited as a barrier, but can be quantified if there is a need to analyse all level crossing scenarios which are depending on Operational Rules.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
LX EMERGENCY	LX in Degraded (up) or Emergency (down) operation	This event simply splits between the degraded/abnormal crossing operation (e.g. to manage an abnormal load or use of the crossing) and an Emergency situation, such where the crossing is not clear due to mis-use, failure or incident. This probability is impossible to estimate. However, in order not to neglect any scenario it is here assuming that half of the cases belong to each category.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
LX NORMAL	Level Crossing operated normally	This event probability is the likelihood that the train approaches a crossing operating normally rather than in some form of abnormal or degraded mode of operation. This event is quantified according to the OVERSPEED scenario where it simply represents the right-side failure of the level crossing equipment. A conservative value is used. This event is used for various overspeed scenarios related to level crossings, but also for the case when there is a failure to display the information “LX not protected”. It is plausible that this information will also be used for level crossings which are not equipped with any level crossing protection system at all. In that case, the event signifies the fraction of level crossings which are unequipped but where catastrophic consequences can still occur.	0.001

Base Event	Description	Source / Justification	Value (probability of event failure)
MODE SUPERVISED	The ETCS On-Board System is in a mode where it supervises the safe speed	This event signifies that when the driver tries to exceed the safe speed limit, the ETCS On-Board System will stop this by first warning the driver and then braking the train. Used in the scenario MMI-2a.1 and MMI-2b. Although the description of the scenario for MMI-2a.1 describes a level crossing case which is potentially not supervised even in FS mode, it is believed that the most significant failures of this event is when the system is in e.g. UN or LS or when a manual speed restriction has been given to the driver. This is estimated to constitute less than 20% of a typical mission.	0.2

Base Event	Description	Source / Justification	Value (probability of event failure)
NEW VBC	Trackside sends a new (correct) list of VBC that is appended to the older (incorrect) one	This mitigation is only valid if the VBC is corrupted outside the construction area, so that a new correct packet 6 is received at the border of the construction area when entering it. However, if the train is anyway going to pass a balise group giving packet 6, it is not likely that the driver will receive the order to manually define VBCs, anyway. Furthermore, if the falsified VBC matches a balise that was used a long time ago, there is no reason for the infrastructure owner to retain the removal order in Packet 6. In summary, this is a very weak barrier and not credited at all.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
NL INPUT SIGNAL	No NL input signal is given	According to requirements for rolling stock contained in SUBSET-034 [Ref 7], a NL input signal is only given if the driver's brake controller is isolated and a travel direction is selected in the cabin. Therefore, the only possible failures are: - The train is not configured according to SUBSET-034. This is clearly outside the scope of the ETCS specifications and should not be further considered here. - There is a failure in the train interface falsely giving the NL input signal. Due to the second failure, this event is assigned a typical probability for non-safety requirement (whether the NL input signal is a safety function or not is not a question that is further pursued here).	0.00001

Base Event	Description	Source / Justification	Value (probability of event failure)
NO GPI DATA	Driver chooses not to derive / estimate data in place of the 'missing' correct data	When required to use GPI and none is displayed via DMI when requested to do so, the driver has a choice of what to do. If the driver reports that no information is available, Operational Rules are assumed to take over and ensure safe recovery from the situation [Assumption A11]. This event reflects the probability that a driver believes they have sufficient understanding of their position to estimate where they are, and does so to replace the missing GPI data. Having decided to estimate replacement data, event “GPI DATA OK” reflects the potential for their estimate to be sufficiently incorrect that it leads to a dangerous situation. This point to category C in the table in Section 5.6.	0.1
NO LEVEL TRANSITION AREA	Train is not running on a level transition area	This event determines the probability of max safe front of the train does not pass a trackside defined location in rear of the level transition border. This area is estimated to be very small compared with the rest of the track. It is assumed the conservative value of 0.05.	0.05

Base Event	Description	Source / Justification	Value (probability of event failure)
NO LX OBSTRUCTION	There is no road vehicle or people on the unprotected LX	Even if the train runs through an unprotected level crossing without the driver being aware of this, there is by pure luck a certain probability that there will be no people or road vehicle to collide with. It cannot be justified to credit this barrier in any decisive way, but it is shown more for completeness. A probability of 0.5 is believed to be appropriate.	0.5
NO STAFF	There are no train staff on board other than the driver	This event only occurs in a scenario where the DMI has issued a spurious command to exit SH mode. The driver is not aware that the mode changed from SH to SB, and if accelerates, ETCS will intervene and apply the brakes after a distance which is a national value, likely a small one (default 2 m). The concern is that if shunting is being undertaken in sidings with loosely coupled vehicles, a sudden jerk motion could occur resulting injury to other people on the train. This event therefore reflects the possibility that staff are On-Board the train during such operations.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
NO UN PROPOSAL	ETCS On-Board has not proposed UN (acknowledgment not actioned)	A spurious UN acknowledgement would only be accepted by the ETCS On-Board if there was a valid UN proposal active at the time of receipt. This is unlikely except at routine start-up, where a normal sequence of events would be to select START immediately followed by accepting UN when proposed by the ETCS On-Board. To have a conservative estimation, the time spent in SB is used. Set to 0.05.	0.05
NO VBC MATCH	The erroneous VBC doesn't match the VBC of a balise that the train encounters	It is likely that when commissioning balises that have been tagged with packet 0, the VBC marker will not be removed. Therefore, it can be expected that after a while, most NID_VBCMK will be in use. This probability is therefore quite high.	0.5
NO VBC USED	No VBC is used in the current operation	This is a risk reduction measure to the scenario MMI-6, failure mode corruption. It is justified by the fact that VBC are not used for all train operation / parts of the infrastructures. Most likely, failures in components causing VBC corruption will be discovered from other reasons even when the function is not used, because other more frequent functions are using the same components.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
NON STOP	Overrun of intended stopping point not within a Non-Stopping Zone	The train is in Overspeed and has been unable to stop within the intended distance (manual braking by the driver). Having overrun the intended stopping point, this event reflects the probability that the train has come to a halt within a designated Non Stopping Zone. The event is not credited as a barrier, but can be quantified if there is a need to analyse all non-stopping zone scenarios which are depending on Operational Rules.	1.0
NOT FS OR OS	Operation not in FS or OS at time of failure	Event reflects the likelihood that the train is in FS or OS at the time of the DMI failure since the harmful consequences (e.g. loss of supervision and protection) only arise from these Modes of operation.	0.9

Base Event	Description	Source / Justification	Value (probability of event failure)
NOT IN SB	Train not in SB mode at time of failure	The DMI failure scenario can only develop further if the train was in SB at the time of the fault. If the DMI failures are random events, this reflects the time that the train is at risk (in SB mode). Systematic DMI failures which occur only or specifically because the train is in SB mode are assumed found during testing and therefore neglected. Standing faults manifesting themselves once the mode switches to SB are assumed to be mitigated by defensive programming techniques standard for SIL4 systems.	0.05
NOT IN SB AT STANDSTILL	Train not in SB mode at time of failure, although train is at standstill	This is the same event as NOT IN SB, here with the condition that earlier in the scenario it has already been factored in that the train is at standstill. Thus, this event signifies the probability that the ETCS On-Board is in SB mode given that the train is at standstill. This would be a higher figure than for NOT IN SB.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
ON SIGHT	Driver still able to brake sufficiently on sighting object / obstruction	Whilst the train may be in Overspeed, travelling faster than the driver believes or than it should, and the driver is unaware of an obstruction ahead, there remains the probability that the combination of actual train speed, sighting distances and driver's skill permits the train to be brought to a stand in rear of the object / obstruction. Consideration may also be given, in some situations (emergencies), to the fact that a collision may have occurred even without the DMI failure. In such cases the event probability would reflect the likelihood that a collision occurs only due to the effect of the DMI failure. Category D in Section 5.6 is used to cover the wide variety of situations where this event is referred, although in specific situations (e.g. when driving on manual permission) a more optimistic value could be justified.	0.3

Base Event	Description	Source / Justification	Value (probability of event failure)
ON SIGHT LX	Driver still able to brake sufficiently on sighting LX object / obstruction	The same event as ON SIGHT, but here it is specifically for the scenario approaching an unprotected level crossing without any warning given to the driver about this. There could be a timing issue where the train and the object/obstruction (most likely road vehicle) arrive at the crossing at the same time, leaving the driver with no chance to brake. A value in the upper range of category D in Section 5.6 is believed reasonable.	0.9
OUT OF SERVICE	Driver realizes the error and takes train out of service.	This event is involved in two scenarios: 1. Selection of languages: If the driver were unable to reselect the required language, as the DMI / ETCS On-Board system is clearly faulty a driver would be expected to take the train out of service. This event reflects the probability that they do not do so, either due to current circumstances (e.g. operational pressures, culture or Operational Rules), or they mistakenly believe they can operate with the failure present. 2. Obscuring of operational data: If the operational data on the DMI (allowed speed, target distances etc.) are not visible to the driver, he/she would most likely immediately stop operation.	0.2

Base Event	Description	Source / Justification	Value (probability of event failure)
		The probability reflects that the driver doesn't discover the error or doesn't take the train out of service as a result of the discovery. The probability that the driver discovers such an error would be quite high, because the operation they want to perform (select language, look at speed dial) is not possible because of the relevant data being obscured. The probability used here (0.2) is the result of first assuming that the driver will discover the error with a probability of 0.9 and then take the train out of service with a probability of 0.9.	
PASSADJUST	Passengers not boarding or alighting or adjust for train movement	The train has begun to move inadvertently following loss of standstill protection. If boarding / alighting is not in progress, or passengers are able to adjust to the train movement, then no injury will arise. If passengers cannot, then the worst case is that they may fall between the moving train and platform coping.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
PASSSTAYON	Passengers do not attempt to disembark at an inappropriate location	Faced with no platform or a much longer step from a train (e.g. onto a platform ramp), most passengers would not attempt to exit the train at that location, and would move along the train to a suitable exit. Train staff may also be present at the doorway either to open the doors or greet new passengers. A driver should be aware that they have not stopped at the correct position and they and/or the Guard may take action either through not releasing the door controls or informing passengers not to exit certain carriages. Nevertheless, passengers may still attempt to disembark and injure themselves doing so, particularly if passengers did not notice the problem, underestimated the hazard posed, felt under pressure to leave the train, were averse to moving to another carriage or simply fell out. This point to category C in the table in Section 5.6.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
PLATFORM	Train doors still open onto platform	Even if a driver overshoots the platform stopping location, it is likely that the train doors will still open onto the platform. As the situation is always an over-run, the train would need to be substantially away from the correct location, or the stopping point is particularly onerous with regard to the available platform length.	0.5
PROB-BS	Buffer Stop not approached before fault revealed	Whilst some routes will have a terminal station at the end of each journey, many routes may involve no approaches to buffer stops. A probability that a train will approach a Buffer Stop before the fault is revealed is considered through this event.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
RBC FS MA	RBC sends MA other than FS	The hazardous situation develops only if the MA sent by the RBC is for Full Supervision (FS). Any other type of MA is not a problem in this instance. This event reflects the likelihood that the next MA received from the RBC after this DMI failure is for FS. From an operational point of view, the goal of the RBC is always to send an FS MA. So, as long as the conditions are fulfilled, this is what the RBC can be expected to do. The conditions are depending on Operational Rules and interlocking functions (known train position, route locked under train, information about obstacles up to start of route etc.). As an initial guess, it is here estimated that in half of the cases, the RBC is able to fulfil all conditions.	0.5
REPEAT ACK	Spurious ACK does not occur again / repeatedly	Situation arises following issue of a spurious ACK by the DMI to the ETCS On-Board's request for acknowledgement to release the emergency or service brake after an ETCS Intervention; DMI-04H "Spurious acknowledgement of intervention leading to release of SB or EB".	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
		When this event is called upon in the Event Tree model it has already been determined that the train is on a gradient (preceding Event GRADIENT). Event “REPEAT ACK” determines the likelihood that the DMI failure repeats, providing one or more further spurious acknowledgements, potentially continuously (e.g. due to a CCF/CMF). As the rest of the ETCS On-Board system is working correctly, the unexpected train movement due to the train being on gradient when the brakes are removed (if the Train Controller was in a position that permitted the brakes to be removed), would cause a further ETCS Intervention, which if acting cyclically, would act to defeat the standstill, rollaway or reverse movement protection.	

Base Event	Description	Source / Justification	Value (probability of event failure)
		The probability that DMI-04H is cyclic is impossible to estimate on a generic level without knowledge of the actual implementation. A possible source of failures could be an error on the DMI screen activating the area of the acknowledgement button constantly. However, the ACK button is an up-type button[11] without repeat function, according to [Ref 6]; therefore a constantly activated area on the screen will not lead to repeated acknowledgements sent to the Kernel. Systematic faults that cause repeated acknowledgements are believed to be found during testing with a fairly high probability. It is believed to be conservative to use the value 0.1 as probability.	
ROUGH RIDE	'Rough Ride' does not cause any injury	A rough ride is only likely to cause minor injury at most, and even then only in certain circumstances. This event considers the likelihood of a minor injury (Marginal consequence) occurring. A severe injury occurring is considered sufficiently remote to not require consideration.	0.01

[11] The button is considered as activated when it goes from being ‘pressed’ to ‘not pressed’.

Base Event	Description	Source / Justification	Value (probability of event failure)
RV EMG	The reason for RV Mode is not in response to an emergency situation	This event reflects the probability that the need to reverse is **not** in response to, or to avoid, an emergency situation where the train will be at risk if it is unable to reverse promptly. If the need to adopt RV Mode is for emergency purposes then there may be insufficient time to adopt an alternative mode (such as NL or SH), or to isolate ETCS and reverse, and catastrophic failure is assumed. Although the intended purpose of this mode is to handle emergency situations, it is estimated that the vast majority of cases where reversing is actually used, is very small. More probable is that the driver merely wants to adjust the stop position of the train in front of a signal or at a station stop. It is reasonable that the need for reversing in an emergency situation arises mainly due to tunnel fires. Therefore, the same value as for the FIRE event is used here. The figure must of course be considered as highly uncertain because of the many assumptions.	$2*10^{-6}$

Base Event	Description	Source / Justification	Value (probability of event failure)
SDO YES	Selective Door Opening available and used	Many modern trains of the type that ETCS would be fitted to have Selective Door Opening. If available, as the driver will be aware that they have passed the designated platform stopping position, they would be expected to refrain from opening the doors for carriages where a safe exit was potentially not available. Even if Selective Door Opening was not available, a driver could manage the situation by refraining from opening the doors until station or train staff had been advised and alternative arrangements put in place which is addressed under the event PASSSTAYON.	0.5
SECOND TRAIN	Second Train not approaching or halted by protection system(s)	Having passed the fouling point of the junction the likelihood of another train approaching is high. It is possible that the train for which the signal was being held at red for has already passed, or if sufficiently far away, or that ETCS or other National protection systems (e.g. ATP, TPWS) may be able to stop the approaching train in time, but it is difficult to take much credit in such situations. Applies in L1 & L2 where overlaid on a trackside signalling system.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
SEV BS	Only minor injuries occur on Buffer Stop collision	In most instances the resultant speed of impact with a Buffer Stop would be low, as at least some, if not the majority, of any overspeed on approach will have been managed by the driver, even if not fully successful in reducing this to zero. Also, modern buffer stop designs provide energy absorption, though not all Buffers are of such designs. The likelihood that the collision results in a severe injury is considered through this event, though it is not just a function of speed but contains some element of luck as to the severity of injury relating to the specific nature of passengers involved, luggage being carried, passenger loadings at the time, type of Buffer Stop present, etc.	0.1
SEV CATASTROPHIC	Catastrophic consequences do not arise on buffer stop collision	This refers to cases when there are not only minor injuries in a buffer stop collision. It is assumed in half the cases, fatalities will occur (catastrophic).	0.5
SEV LS UBA-MAJ	Severe Injury does not occur during a low speed UBA event	Severe unexpected braking is not likely to always lead to a severe injury, but persons could fall awkwardly causing a broken limb, especially the elderly, and if on approach to a station there could be more passengers standing and also handling luggage in preparation for alighting.	0.01

Base Event	Description	Source / Justification	Value (probability of event failure)
SEV LS UBA-MIN	Minor Injury does not occur during low speed UBA event	This event signifies the probability that there is anyway a minor injury given that there is no major injury.	0.2
SEV HS UBA-MIN	Minor Injury does not occur during high speed UBA event	This event signifies the probability that there is an injury when braking from high speed. For high-speed braking, only minor injuries are considered plausible.	0.2
SH MODE PROTECTION	Trackside is protected against erroneous circulation in SH mode	Some areas might be protected against erroneous circulation in SH mode. For instance, balises can be programmed with Stop-if-in-SH packet or List-of-balises-in-SH. In addition, in L2, RBC could not grant the entry into SH mode.	0.9
SPEED DISPLAY	Speed display not obscured	The erroneous DMI information which is obscuring useful / required DMI information could obscure a range of possible DMI data. This event determines if it is the speed information that is obscured or not. If it is, then the failure is akin to having no or incorrect speed information. A large part of the DMI screen is devoted to the speed display.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
SPEED OK	Magnitude of speed error insufficient to cause a problem	Conceptually the magnitude of the DMI error may not result in any hazard occurring, being close to the actual train speed. However, for a generic DMI, the error could be anything, and could also be an 'offset' or a true speed delayed in being displayed. Accordingly little or no credit can be taken for this. Assuming that a 20 km/h error is no safety issue, and that the range of speed display is in average 200 km/h, only 10% of the errors are "safe".	0.9
STANDSTILL	Train moving at time of request	The request to the ETCS On-Board arising from various potential DMI failures will only be accepted if the train is at a standstill. This event reflects the probability that the train is stationary when the fault occurs. Standing faults manifesting themselves once the train is at standstill are assumed to be mitigated by defensive programming techniques standard for SIL4 systems.	0.05

Base Event	Description	Source / Justification	Value (probability of event failure)
START AWAY	Operational Rules require check of MA before starting away	If a driver is required by Operational Rules to confirm that a valid MA is available before starting away, then the DMI failure would be revealed. This event can only be evaluated taking into account Operational Rules and the timings at which a driver would check (or recheck) for an MA before starting away. This failure of this event is not quantified, i.e. no credit is taken for the driver checking the MA before starting. The reason for this very conservative approach is that no such rules are harmonized within the scope of the TSI CCS and the fact that no credit needs to be taken because the frequency of the scenario is sufficiently low compared to the risk acceptance criteria. However, if needed, this can be further explored, since it is believed that all Operational Rules in Europe require either a technical authorisation (which would imply the driver checking the MA) or a manual authorisation (which would imply there is no hazard) before any vehicle movement can take place.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
STRUCTURE	No impact with any structure or stationary vehicle occurs	The affected train in Overspeed will be subjected to additional forces and a certain element of additional leaning will occur. It is unlikely that the safe kinetic envelope would be breached due to the additional train speed, but it is potentially possible. This event reflects the probability that the train leans sufficiently to collide with infrastructure, or potentially a stationary train on an adjacent track (trains passing each other would both be subjected to leaning forces in the same direction, but a stationary train would not, thereby leaving it nearer to the affected train). The event is not credited as a barrier, but can be quantified if there is a need to analyse all structure collision scenarios which are depending on Operational Rules.	1.0

Base Event	Description	Source / Justification	Value (probability of event failure)
TIME OUT	Override automatically removed before any issue arises	Override will be automatically removed for any one of a variety of reasons as detailed in SUBSET-026 [Ref 1] Section 5.8.4, most likely due to expiry of the Nationally set values for time out time and distance travelled. This event therefore reflects that a situation requiring ETCS supervision and protection is encountered in this limited period. Considering that the initial failure (driver accidently requesting override) is not linked to a certain operational situation, the probability for TIME OUT can be set to the fraction between validity of override and the average time to the need for a speed decrease. Typical values are believed to be 60 sec and 10 minutes, respectively. Note: The value shall not take into account the probability for the need of ETCS intervention; this comes later in the secondary event tree LOSS.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
TRAIN IN ACC AREA	The train is not in the area of the external accident	This concerns the scenario that there has been a serious accident in an external system, e.g. chemical power plant, causing toxic fumes. In such a scenario, there is a chance that the train hasn't entered the hazardous area yet, and therefore could be stopped or re-routed. If so, the closing of the air intakes is not a safety issue, as it would if the train is already inside the hazardous area. This potential barrier is not credited, since it is impossible to estimate.	1.0
TRAIN SPEED HIGH	Braking from high speed	Braking from high speed is unlikely to result in any significant harm as the jerk rate (rate of change of deceleration) is generally lower than that which arises when severe braking from a relatively low speed occurs. This probability for failure of this event considers the likelihood that the situation occurs when the train is at low speed.	0.1

Base Event	Description	Source / Justification	Value (probability of event failure)
TRAIN UP	Train Remains Upright	Should a train derail the consequences are more onerous if the train does not remain upright. Many of the derailment situations will be at relatively low speed, such as run through of points or an excess speed through a slow speed crossover as the Overspeed has in effect caused late braking rather than no braking. In such circumstances a train would be expected to remain upright in most cases For higher speed derailment the situation is more dependent upon the specific alignment of the track and adjacent infrastructure, but a train will often remain upright, especially a fixed train-set. Here, it is assumed that in 50% of the derailment cases, the train remains upright.	0.5

Base Event	Description	Source / Justification	Value (probability of event failure)
TSR	The train doesn't encounter any TSR while overspeeding	This event represents the probability that although the train is overspeeding due to a DMI error, there is no derailment over a TSR, simply because no TSR is encountered. Obviously, the value is depending on how frequently such speed restrictions occur in the railway infrastructure and on how long the DMI failure prevails undetected. The analysis in Annex A of SUBSET-088 Part 3 [Ref 4] assumes a mission profile of 0.4 TSRs per hour during an average journey. Regarding the duration of the DMI error, it is believed likely that the driver will discover it when decreasing the speed of the train. A duration of 30 minutes can be assumed. Thus, during the period of the undisclosed error, 0.2 TSRs will be passed. From this, the approximation is derived that in 80% of the cases, no TSR will be encountered.	0.2

Base Event	Description	Source / Justification	Value (probability of event failure)
TSR SPEEDING MINOR	Overspeed in TSR is minor (insufficient to cause derailment)	The failure of this event reflects the (low) probability that the additional speed of the train due to the DMI error is sufficient to result in a derailment due to the reason for the TSR (e.g. poor track quality) and the magnitude of the overspeed. N.B. even if derailment does not occur, damage could arise to the track exacerbating whatever situation required the TSR to be placed.	0.1
UNSUITABLE	Train does not enter a route for which it is incompatible (e.g. track gauge, traction)	Due to the additional speed that the driver is unaware of, it is possible that a driver may overshoot their intended stopping position. If the position was related to some form of incompatibility, e.g. a change of gauge location, change of traction technology or possibly a gauge infringement (low bridge or tunnel wall – which was approached to allow turning or platform changing), a hazard could arise. The event is not credited as a barrier, but can be quantified if there is a need to analyse all incompatibility scenarios which are depending on Operational Rules.	1.0

Appendix F ETCS Core Hazard DMI related Hazardous Events

The existing safety analysis of the ETCS system reported in SUBSET-088 [Ref 4] (e.g. Part 3 Chapter 4) and 091 [Ref 5] identified subsidiary hazardous situations associated with the DMI. The complete list of currently identified hazardous situations is repeated below, including a comment how the event is covered in this DMI study when the event id is not directly used here.

Event Id.	Event Description	Comment regarding this DMI study
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 (RAP, 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	This refers to the supervised speed and distance limits. Thus only relevant for $ETCS_{CH}$.
MMI-2b	False presentation of mode	
MMI-2c	False presentation of track adhesion factor	
MMI-2d	Failure to present Entry in FS/OS information	Considered in HAZID as only applicable to Core Hazard and thus not studied further

Event Id.	Event Description	Comment regarding this DMI study
MMI-2e	False presentation of train data/additional data	Considered in SUBSET-079 [Ref 3] as ETCS Core Hazard, so it is not studied further here. A special case is the “Notification of Train Data change from source different from the driver”, where non-Core hazards can exist. This is discussed in connection with **DMI-02e**.
MMI-2f	Failure to display Override status (contains deletion and insertion failure modes), including false enabling of override selection	
MMI-2g	Failure to present acknowledgement message to a less restrictive mode	Considered as fully mitigated by the ETCS On-Board supervision of mode acknowledgement and thus not studied further. DMI-01c is considered as the generalisation of MMI-2g, and includes all the acknowledgement messages.
MMI-2h	False presentation of TAF request	Considered in HAZID as only applicable to Core Hazard and thus not studied further
MMI-2i	Failure to present LX “not protected” information	
MMI-2j	False presentation of reversing allowed	Considered in HAZID as only applicable to Core Hazard and thus not studied further
MMI-2k	False presentation of level transition announcement	Considered in HAZID as not having hazardous consequences
MMI-3	Falsification of driver’s train data/additional data input stored On-Board	Considered in HAZID as out of scope, partly on unclear grounds. Anyway, MMI-3 is clearly ETCS Core Hazard, so it is not studied further here.
MMI-4	Falsification of SR speed/distance data	Considered in HAZID as only applicable to Core Hazard and thus not studied further
MMI-5	Falsification of train integrity confirmation input	Considered in HAZID as out of scope (unclear why, possibly because this is a Level 3 safety function)
MMI-6	Falsification of Virtual Balise Cover	

Appendix G Hazard Log, Safety Requirements, Constraints and Exported Requirements

G.1 Safety Requirements

Hazard ID	Hazard Description	Hazardous Situation	HS Description	ID	Safety Requirement	Notes / Comment
				SReq01	No longer used	
				SReq02	No longer used	
				SReq03	No longer used	
				SReq04	No longer used	
				SReq05	No longer used	
				SReq06	No longer used	
H3	Erroneous but valid information displayed	DMI-03a	Incorrect Geographical Position data displayed	SReq07	The trackside application (engineering in combination with operational rules) must not put any safety reliance on the Geographic Position Information.	SReq07 is a prerequisite for this analysis. It originates from the fact that only the estimated position (and not the safe confidence interval) as calculated by the ETCS On-Board is presented to the driver.

Hazard ID	Hazard Description	Hazardous Situation	HS Description	ID	Safety Requirement	Notes / Comment
					Some example scenarios to avoid are presented in Appendix I.	
				SReq08	No longer used	
H4		DMI-04c, DMI-04d, MMI-1g	False START command False UN acknowledgement False request for SH Mode	SReq09	Drivers should not rely upon Standstill Protection as the primary means of holding the train stationary.	To ensure rollaway does not occur in the event that Standstill protection was removed by a DMI failure. N.B. this may be common practice in many administrations but this safety requirement is recorded to ensure that it is verified as applied in each application.
				SReq10	No longer used	
				SReq11	No longer used	
				SReq12	No longer used	
				SReq13	No longer used	

Hazard ID	Hazard Description	Hazardous Situation	HS Description	ID	Safety Requirement	Notes / Comment
				SReq14	No longer used	

Whilst not formal safety requirements the following points are noted from the assessment:

Note: Where practicable, menus, alerts and requests to the driver should not obscure other valuable information to the driver, e.g. speed information, such that a spuriously presented display does not obscure important information. In this respect, adherence to the DMI specification alone may be sufficient if the DMI display is not also presenting additional information provided the suitability of which has been ergonomically assessed.

Note: There is benefit if the ACK request message included detail of the specific proposed change rather than just a “generic” ACK statement that relied upon the rest of the DMI displayed information for a driver to determine what the change had been.

Note: The ability for a driver to be able to review recent commands and messages (rather than just alarms) would permit checking back what had just occurred. For example, if an acknowledgement was provided by a driver as a reflex response due to the current driver priorities (to avoid Intervention), and there was a need to look back to the specific details subsequently when time was available to determine exactly what had been accepted.

G.2 Constraints and Exported Requirements

The Constraints and Exported Requirements referred to in Section 6.6 are listed here.

Due to the constraints and scope of the study, the results must be viewed within the context of a number of key assumptions or aspects that are to be addressed outside of this study. These are in addition to the Safety Requirements arising from the study. Principal amongst these are:

1 Ref clause 3.2.1.4: The DMI is treated only as an interface, with consideration limited to the display of information to the Driver and the Driver’s interaction with it (e.g. requests and acknowledgements). Justification of the ergonomic suitability of the DMI itself is outside the scope of this study.

2 Ref clause 3.2.1.6: 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. For example:

{

- { a written order }

and/or

- { confirmation from driver is requested by Q_TEXTCONFIRM (>0) and this acknowledge is sent to RBC requested by Q_TEXTREPORT }

}

And

{

- confirmation from driver is requested by Q_TEXTCONFIRM (>1) :brake reaction if driver does not acknowledge the message

}

- Note: The trackside design shall pay attention that the message will be effectively considered by using adequate start and end conditions.

3 intentionally deleted

4 Ref clause 3.2.1.7: There is no harmonized specification within the scope of the TSI CCS for the communication between the driver and ETCS On-Board via DMI. Accordingly, the behaviour of the ETCS On-Board in receipt of erroneous data via the DMI cannot be determined. The response of the ETCS On-Board to the receipt of invalid data via the DMI will need to be addressed by each product supplier for their system design.

5 Intentionally deleted.

6 Intentionally deleted.

7 Intentionally deleted.

8 Ref clause 3.2.1.8: Recovery from situations where a failure in the DMI has caused ETCS brake intervention depends upon Operational Rules and the specific circumstances at the location. Sufficiency of the rules and procedures regarding recovery from such situations is therefore not modelled.

9 Ref DMI-03d in Appendix B: After a trip, the driver shall assume that there is a dangerous situation and he shall perform all actions necessary to handle this situation with the help of the signalman who knows which train movements are safe. There should be no need to place any reliance on the DMI output Trip Reason. This constraint shall be exported to the operational rules.

10 Ref DMI-02e in Appendix B: According to SUBSET-026 section 5.17, there is a possibility to require the driver to validate train data coming from sources other than the driver. Such a validation not only assures that the data is correct according to the driver's judgment, but also makes sure that the driver is made aware of a certain change in train data. Therefore, this validation shall be applied for data which could be safety critical for the driver to know about. This includes the following train data: train length and maximum train speed.

11 Ref DMI-03e "Acknowledgement" in Appendix B: The text message "Acknowledgement" shall only be used by the trackside in situations where the driver is responsible to observe the existing line-side information (signals, speed boards etc.) and national operating rules, such as lines where Limited Supervision is the normal operating mode. The reason is that text messages is not regarded as a safety function and therefore must not be used to command a shift of safety responsibility but only to serve as a reminder to a driver who is already responsible.

12 Ref 3.2.1.7A The ETCS On-Board is designed according to principles of defensive programming which is mandatory for SIL4 systems. This means here that some sort of safe reaction is invoked if the system detects input from the DMI which should not be possible to give, e.g. Start command in FS mode, and thereby would indicate a DMI fault.

13 Ref DMI-04j "False Isolation command" in Appendix B: A control separate to the driver's screen (although part of the DMI concept) is provided to initiate ISOLATION mode (IS) and is required to be used when IS Mode is adopted. This separate isolation control doubles as an indication that overrules any indication on the DMI screen because the IS control interfaces directly with the train brake circuits

14 Ref DMI-01c in Appendix B: CR1166 says it is undefined when the timer shall start. Thus, it has been considered in this analysis that the timer starts counting when the ETCS On-Board outputs the ACK, so that a deleted ACK will cause a timer elapse.

Appendix H Cut-set lists

H.1 Reading Notes

This Appendix shows all Cut-sets for each consequence S2, S3 and S4. They are listed in descending order, so that the Cut-Set with the highest frequency comes first.

Each Cut-set consists of a number of events, listed in the chronological order defined by the Event Tree, i.e. with the DMI Hazardous Situation used as initiating event (DMI-xx/MMI-xx)) first and the barriers in consecutive order after. The events are separated by a point sign (“.”).

If an event appears **without** a minus sign, it means that it is the failure of the event that is involved in the Cut-set. If an event appears **with** a minus sign, it is the success of the event that is involved.

H.2 Cut-sets for Consequence S2 “one or more light injuries”

Number	Frequency	Cut-set
1	1.00E-05	DMI-01G. DRV AIR TIGHT
2	9.00E-06	DMI-01B. OUT OF SERVICE. -SPEED DISPLAY. ACK DISPLAY OK. -TRAIN SPEED HIGH. SEV HS UBA-MIN
3	9.00E-06	DMI-02C. CONTROLLED BRAKING. -TRAIN SPEED HIGH. SEV HS UBA-MIN
4	9.00E-06	DMI-05A, -05B. -TRAIN SPEED HIGH. SEV HS UBA-MIN
5	9.00E-06	MMI-2F-INS. DRV INDICATION OVERRIDE. -TRAIN SPEED HIGH. SEV HS UBA-MIN
6	9.00E-06	DMI-04A. STANDSTILL. DRV CHANGE MODE. NO STAFF. -TRAIN SPEED HIGH. SEV HS UBA-MIN
7	9.00E-06	DMI-01A. DRV OVERSPEED. -TRAIN SPEED HIGH. SEV HS UBA-MIN
8	9.00E-06	DMI-01C. ACK MISS NOT UBA. -TRAIN SPEED HIGH. SEV HS UBA-MIN
9	5.40E-06	DMI-02B. FALSE MODE. DRV STYLE. DRV WARNING. -TRAIN SPEED HIGH. SEV HS UBA-MIN
10	5.40E-06	DMI-02A, -02G. DRV INDICATION. -TRAIN SPEED HIGH. SEV HS UBA-MIN
11	9.90E-07	DMI-05A, -05B. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
12	9.90E-07	MMI-2F-INS. DRV INDICATION OVERRIDE. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
13	9.90E-07	DMI-04A. STANDSTILL. DRV CHANGE MODE. NO STAFF. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
14	9.90E-07	DMI-01A. DRV OVERSPEED. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
15	9.90E-07	DMI-01C. ACK MISS NOT UBA. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
16	9.90E-07	DMI-01B. OUT OF SERVICE. -SPEED DISPLAY. ACK DISPLAY OK. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
17	9.90E-07	DMI-02C. CONTROLLED BRAKING. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN

18	5.94E-07	DMI-02B. FALSE MODE. DRV STYLE. DRV WARNING. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
19	5.94E-07	DMI-02A, -02G. DRV INDICATION. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
20	1.62E-07	DMI-04H. GRADIENT. -REPEAT ACK. -TRAIN SPEED HIGH. SEV HS UBA-MIN
21	6.08E-08	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. -TRAIN SPEED HIGH. SEV HS UBA-MIN
22	6.08E-08	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. -TRAIN SPEED HIGH. SEV HS UBA-MIN
23	1.78E-08	DMI-04H. GRADIENT. -REPEAT ACK. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
24	1.35E-08	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. -TRAIN SPEED HIGH. SEV HS UBA-MIN
25	6.68E-09	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
26	6.68E-09	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
27	2.03E-09	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. -TRAIN SPEED HIGH. SEV HS UBA-MIN
28	2.03E-09	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. -TRAIN SPEED HIGH. SEV HS UBA-MIN
29	1.49E-09	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
30	1.01E-09	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. ROUGH RIDE

[12] MMI-2C or DMI-01h or DMI-01i or DMI-03g or DMI-03h

31	1.00E-09	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. ROUGH RIDE
32	1.00E-09	DMI-05E. DRV INDICATION SLIPPERY. ROUGH RIDE
33	9.99E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. ROUGH RIDE
34	9.05E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. PROB-BS. DRV BS. -SEV BS
35	9.00E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. PROB-BS. DRV BS. -SEV BS
36	9.00E-10	DMI-05E. DRV INDICATION SLIPPERY. PROB-BS. DRV BS. -SEV BS
37	8.99E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. PROB-BS. DRV BS. -SEV BS
38	4.50E-10	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. -TRAIN SPEED HIGH. SEV HS UBA-MIN
39	2.23E-10	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
40	2.23E-10	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN
41	4.95E-11	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. -SEV LS UBA-MAJ. SEV LS UBA-MIN

H.3 Cut-sets for Consequence S3 “single fatality and/or single serious injury”

Number	Frequency	Cut-set
1	5.63E-08	DMI-04C. NOT IN SB. IN L0. LEVEL 1 OR LEVEL 2 OP. -RBC FS MA. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
2	5E-08	DMI-01B. OUT OF SERVICE. -SPEED DISPLAY. ACK DISPLAY OK. TRAIN SPEED HIGH. SEV LS UBA-MAJ
3	5E-08	DMI-02C. CONTROLLED BRAKING. TRAIN SPEED HIGH. SEV LS UBA-MAJ
4	5E-08	DMI-05A, -05B. TRAIN SPEED HIGH. SEV LS UBA-MAJ
5	5E-08	MMI-2F-INS. DRV INDICATION OVERRIDE. TRAIN SPEED HIGH. SEV LS UBA-MAJ
6	5E-08	DMI-04A. STANDSTILL. DRV CHANGE MODE. NO STAFF. TRAIN SPEED HIGH. SEV LS UBA-MAJ
7	5E-08	DMI-01A. DRV OVERSPEED. TRAIN SPEED HIGH. SEV LS UBA-MAJ
8	5E-08	DMI-01C. ACK MISS NOT UBA. TRAIN SPEED HIGH. SEV LS UBA-MAJ
9	3E-08	DMI-02B. FALSE MODE. DRV STYLE. DRV WARNING. TRAIN SPEED HIGH. SEV LS UBA-MAJ
10	3E-08	DMI-02A, -02G. DRV INDICATION. TRAIN SPEED HIGH. SEV LS UBA-MAJ
11	2.51E-09	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV STN. PLATFORM. SDO YES. PASSSTAYON
12	2.5E-09	DMI-05E. DRV INDICATION SLIPPERY. DRV STN. PLATFORM. SDO YES. PASSSTAYON
13	2.5E-09	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV STN. PLATFORM. SDO YES. PASSSTAYON

14	2.5E-09	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV STN. PLATFORM. SDO YES. PASSSTAYON
15	9.95E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. -TRAIN UP
16	9.9E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. -TRAIN UP
17	9.9E-10	DMI-05E. DRV INDICATION SLIPPERY. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. -TRAIN UP
18	9.89E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. -TRAIN UP
19	9E-10	DMI-04H. GRADIENT. -REPEAT ACK. TRAIN SPEED HIGH. SEV LS UBA-MAJ
20	5.03E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV JUNCTION. -TRAIN UP
21	5E-10	DMI-05E. DRV INDICATION SLIPPERY. DRV JUNCTION. -TRAIN UP
22	5E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV JUNCTION. -TRAIN UP
23	5E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV JUNCTION. -TRAIN UP
24	3.38E-10	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. SEV LS UBA-MAJ
25	3.38E-10	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. SEV LS UBA-MAJ

26	2.5E-10	DMI-04D. -IN L0. NO UN PROPOSAL. INTERUPTION. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
27	1.13E-10	DMI-04C. NOT IN SB. IN L0. -LEVEL 1 OR LEVEL 2 OP. AUTO ACK. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
28	7.5E-11	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. -CEILING SPEED SH. TRAIN SPEED HIGH. SEV LS UBA-MAJ
29	5.63E-11	DMI-04C. NOT IN SB. IN L0. LEVEL 1 OR LEVEL 2 OP. RBC FS MA. AUTO ACK. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
30	5.03E-11	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. PROB-BS. DRV BS. SEV BS. -SEV CATASTROPHIC
31	5E-11	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. PROB-BS. DRV BS. SEV BS. -SEV CATASTROPHIC
32	5E-11	DMI-05E. DRV INDICATION SLIPPERY. PROB-BS. DRV BS. SEV BS. -SEV CATASTROPHIC
33	5E-11	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. PROB-BS. DRV BS. SEV BS. -SEV CATASTROPHIC
34	2.51E-11	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. -TRAIN UP
35	2.5E-11	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. -TRAIN UP
36	2.5E-11	DMI-05E. DRV INDICATION SLIPPERY. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. -TRAIN UP

37	2.5E-11	DMI-04C. NOT IN SB. -IN L0. AUTO ACK. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
38	2.5E-11	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. -TRAIN UP
39	2.25E-11	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. NOT IN SB AT STANDSTILL. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
40	2.25E-11	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. NOT IN SB AT STANDSTILL. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
41	1.13E-11	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. SEV LS UBA-MAJ
42	1.13E-11	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. SEV LS UBA-MAJ
43	5E-12	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. NOT IN SB AT STANDSTILL. GRADIENT. DRV STATION BRAKE. DOOR INTERLOCK. PASSADJUST
44	2.5E-12	MMI-1G. STANDSTILL. -IN L0. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. -SH MODE PROTECTION. TRAIN SPEED HIGH. SEV LS UBA-MAJ

H.4 Cut-sets for Consequence S4 “fatalities and/or serious injuries”

Number	Frequency	Cut-set
1	1E-09	MMI-1A. ETCS ON-BOARD REJECTS. DRV CHANGE MODE. DRV STYLE
2	1E-09	MMI-2F-DEL. DRV INDICATION NO OVERRIDE. TIME OUT. DRV STYLE
3	1E-09	MMI-2B. MODE SUPERVISED. FALSE MODE. DRV STYLE
4	1E-09	DMI-04H. GRADIENT. REPEAT ACK. DRV REPEAT PROT
5	1E-09	DMI-04G. STANDSTILL. LEVEL RULES. DRV ANNOUNCED. DRV STYLE
6	1E-09	MMI-6-CORR. NEW VBC. DRV VBC CORRUPTION. NO VBC USED. BALISE DATA NOT HAZ. DRV STYLE
7	1E-09	DMI-01F. RV EMG. DRV RV ALT
8	1E-09	DMI-04J. DRV CHANGE MODE. DRV STYLE
9	1E-09	DMI-03F. FIRE. DRV AWARE STOP
10	1E-09	DMI-05F. RV EMG. DRV RV ALT
11	9.95E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. TRAIN UP
12	9.9E-10	DMI-05E. DRV INDICATION SLIPPERY. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. TRAIN UP
13	9.9E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. TRAIN UP
14	9.89E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. -DRV JUNCTION. TSR. TSR SPEEDING MINOR. TRAIN UP
15	9.38E-10	MMI-6-INS. NOT IN SB. DRV VBC INSERTION. NO VBC MATCH. BALISE MISS NOT HAZ. DRV STYLE

16	9.11E-10	MMI-1G. STANDSTILL. IN L0. -LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. SH MODE PROTECTION. NOT FS OR OS. DRV STYLE
17	9.11E-10	MMI-1G. STANDSTILL. IN L0. LEVEL 1 OR LEVEL 2 OP. DRV CHANGE MODE. -NOT IN SB AT STANDSTILL. CEILING SPEED SH. SH MODE PROTECTION. NOT FS OR OS. DRV STYLE
18	9E-10	DMI-03E. LX NORMAL. DRV NO CONFIRM. MODE SUPERVISED. NO LX OBSTRUCTION. ON SIGHT LX
19	9E-10	MMI-1D. IN L0. NO LEVEL TRANSITION AREA. DRV ANNOUNCED. DRV STYLE
20	5.03E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV SIGNAL. LINE CLEAR
21	5.03E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV JUNCTION. TRAIN UP
22	5.03E-10	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV SIGNAL. SECOND TRAIN
23	5E-10	DMI-03F. FIRE. -DRV AWARE STOP. DRV AVOID FIRE
24	5E-10	DMI-05E. DRV INDICATION SLIPPERY. DRV SIGNAL. LINE CLEAR
25	5E-10	DMI-05E. DRV INDICATION SLIPPERY. DRV SIGNAL. SECOND TRAIN
26	5E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV JUNCTION. TRAIN UP
27	5E-10	DMI-05E. DRV INDICATION SLIPPERY. DRV JUNCTION. TRAIN UP
28	5E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV SIGNAL. SECOND TRAIN
29	5E-10	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV SIGNAL. LINE CLEAR
30	5E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV SIGNAL. LINE CLEAR
31	5E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV JUNCTION. TRAIN UP

32	5E-10	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV SIGNAL. SECOND TRAIN
33	2E-10	DMI-01G. EXTERNAL ACCIDENT. TRAIN IN ACC AREA
34	5.03E-11	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. PROB-BS. DRV BS. SEV BS. SEV CATASTROPHIC
35	5E-11	MMI-1B. STANDSTILL. NL INPUT SIGNAL. DRV CHANGE MODE. DRV STYLE
36	5E-11	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. PROB-BS. DRV BS. SEV BS. SEV CATASTROPHIC
37	5E-11	DMI-05E. DRV INDICATION SLIPPERY. PROB-BS. DRV BS. SEV BS. SEV CATASTROPHIC
38	5E-11	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. PROB-BS. DRV BS. SEV BS. SEV CATASTROPHIC
39	2.51E-11	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. TRAIN UP
40	2.5E-11	DMI-05E. DRV INDICATION SLIPPERY. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. TRAIN UP
41	2.5E-11	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. TRAIN UP
42	2.5E-11	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. DRV SIGNAL. -SECOND TRAIN. DERAIL JNC. TRAIN UP
43	1.51E-11	MMI-2C[12]. DRV INDICATION. GOOD ADHESION. DRV STYLE LAF. LX NORMAL. LX EMERGENCY. ON SIGHT
44	1.5E-11	DMI-01B. OUT OF SERVICE. SPEED DISPLAY. CAREFUL. LX NORMAL. LX EMERGENCY. ON SIGHT
45	1.5E-11	DMI-05E. DRV INDICATION SLIPPERY. LX NORMAL. LX EMERGENCY. ON SIGHT
46	1.5E-11	MMI-2A.1. HIGH-LOW DISPLAY. SPEED OK. DRV SPEED RECOG. MODE SUPERVISED. LX NORMAL. LX EMERGENCY. ON SIGHT

Appendix I Examples of scenarios to be avoided when using Geographical Positioning Information

This appendix contains some scenarios with a potentially hazardous effect associated with faulty GPI information given to the driver. The error could be caused by a discrepancy between the real position and the estimated position, or by a display error to the driver via DMI.

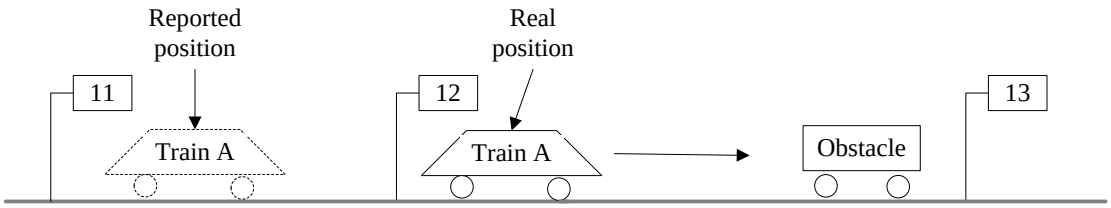
The scenarios should be checked as a part of fulfilling safety requirement SReq07 in Appendix G.

Scenario 1: Erroneous manual exempt from running On-Sight

The TSI for the operation subsystem, Annex A, allows the signaller to exempt the driver from running on sight in SR if the signaller can establish that the track is free, and if allowed by non-harmonized rules. If using GPI as one element of establishing that the track is free, the following potentially hazardous scenario is possible.

Train A is standing between signals 12 and 13, with an obstacle in front of the train (circumstances not allowing visual contact). The driver requests a manual permission to continue driving towards signal 13. Since the driver cannot see the next signal (13), they use the GPI function to extract the train's position. However, an error in the GPI displayed to the driver places the train between signals 11 and 12 instead of at the real position. The driver reports the erroneous position to the signalman, who then authorises train A to continue "up to signal 12". The signalman also exempts train A from running on sight because they know the obstacle is placed after signal 12. The driver of train A uses the manual permission and starts off at high speed. There is a subsequent risk of collision between train A and the obstacle.

The scenario assumes that the driver doesn't realize that the manual permission allows them to go up to a signal that is already passed.

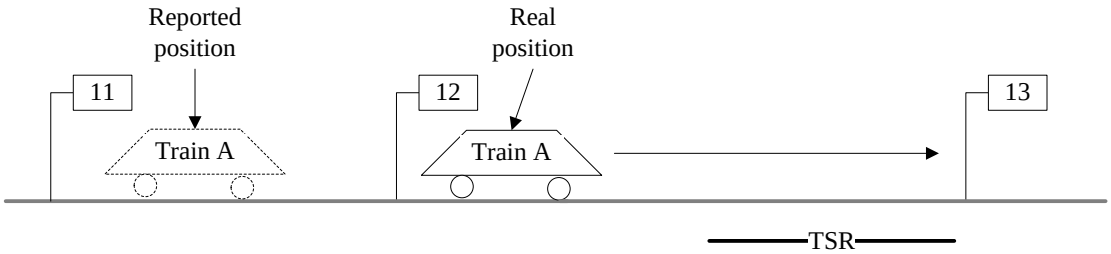


Scenario 2: Erroneous manual neglect of Temporary Speed Restriction

A manual authority shall contain any temporary speed restrictions (TSRs) that the driver has to respect. If the signaller uses GPI as a means establishing whether a TSR shall be included in the manual authority or not, the following potentially hazardous scenario is possible.

Train A is standing between signals 12 and 13, with a TSR in front of the train. The driver requests a manual permission to continue driving towards signal 13. Since the driver cannot see the next signal (13), they use the GPI function to find out the train's position. However, an error in the GPI displayed to the driver places the train between signals 11 and 12 instead of at the real position. The driver reports the erroneous position to the signalman, who then authorises train A to continue "up to signal 12". The signalman doesn't include the TSR in the authority because they know the TSR is placed after signal 12. The driver of train A uses the manual permission and starts driving without respecting the TSR. There is a subsequent risk for an accident against which the TSR was supposed to protect.

The scenario assumes that the driver doesn't realize that the manual permission allows them to go up to a signal that is already passed.



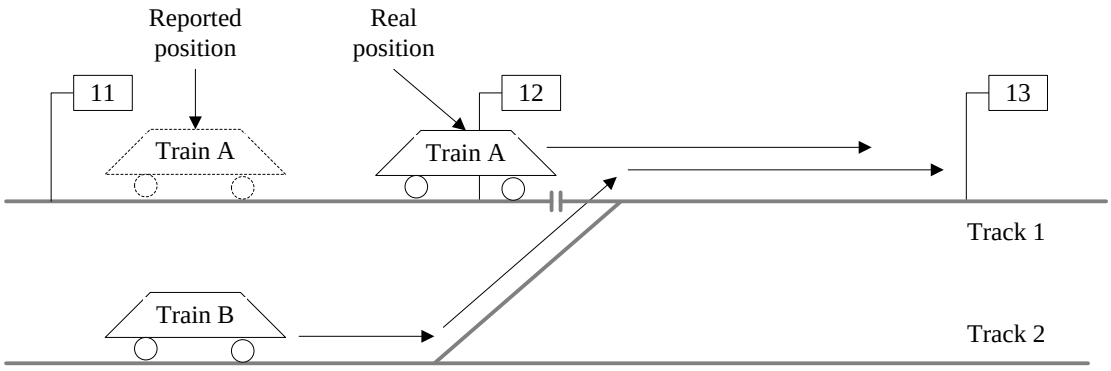
Scenario 3: Erroneous manual permission to pass point

Train A is standing on track 1 between signal 12 and a point, see figure below. At least the front cab has passed signal 12, so that the driver cannot see it anymore. The driver requests a manual permission to continue through the point. Since the driver cannot see the next signal (13), they use the GPI function to find out the train's position. However, an error in the GPI displayed to the driver places the train between signals 11 and 12 instead of at the real position. The driver reports the erroneous position to the signalman, who then authorises train A to continue "up to signal 12". The driver of train A uses the manual permission and starts off through the point, still not spotting signal 13.

At the same time, the signalman sets a route for train B to change track and continue on track 1, see figure below. Depending on interlocking engineering[13], there is a certain chance that this route will not be accepted by the interlocking because of train A violating national rules for flank protection. However, if the route is accepted, there is a subsequent risk of collision between trains A and B.

The scenario assumes that the driver doesn't realize that the manual permission allows them to go up to a signal that is already passed.

Note: If the real position of train A would instead be between signals 11 and 12, there would be no hazard, since manual permissions are always relating to a certain signal and not to a certain distance.



[13] Train A must not be already on the next track circuit which must be free for the setting of the route for train B; the join between the 2 track circuits is usually behind signal 12, the maximum distance being implementation dependent.