

Information on the document

| | |
|--|----------------------|
| European Union Agency for Railways | |
| Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013 | |
| Reference : | ERA-REC-116-2015-GUI |
| Version : | 1.1 |
| Date: | 18/05/2017 |

| | |
|-------------------------------|--|
| Document elaborated by | European Union Agency for Railways Rue Marc LEFRANCQ, 120 BP 20392 F-59307 Valenciennes Cedex France |
| Document Type: | Guide |
| Document Status: | Public |

| | Name | Function |
|----------------------------|---|--|
| Released by | Josef DOPPELBAUER | Executive Director |
| Reviewed by | Christopher CARR Jean-Marie DECHAMPS | Head of Safety Unit Head of Management Sector |
| Written by (Author) | Dragan JOVICIC | Safety Unit - Project Officer |

Information on the document

DOCUMENT INFORMATION

Amendment Record

Table 1: Document history.

| Version Date | Author(s) | Section Number | Modification Description |
|---------------------------|----------------|--|---|
| Version 1.0 23/12/2016 | Dragan JOVICIC | - | First official version of the document made publically available via the web page of the European Union Agency for Railways. The document was developed in collaboration with the EU railway stakeholders. |
| Version 1.1 18/05/2017 | Dragan JOVICIC | Footnote ⁽¹⁹⁾ on page 103 | Clarification that the footnote was added by the European Union Agency for Railways. It was not part of the text of the example proposed by the authors. |

Table of Contents

| | |
|---|-----------|
| DOCUMENT INFORMATION | 2 |
| Amendment Record | 2 |
| TABLE OF CONTENTS | 3 |
| List of Figures | 6 |
| List of Tables..... | 7 |
| 0. INTRODUCTION..... | 8 |
| 0.1. Scope of this document | 8 |
| 0.2. Structure for this guide | 9 |
| 0.3. Reference documents..... | 11 |
| 0.4. Definitions..... | 11 |
| 0.5. Abbreviations..... | 12 |
| EXPLANATIONS OF THE LEGAL TEXT..... | 13 |
| 1. SCOPE OF USE OF THE CSM DESIGN TARGETS (CSM-DT) | 13 |
| 1.1. What are the CSM-DT ? | 13 |
| 1.2. Is use of CSM-DT mandatory (Proposer’s responsibility)?..... | 13 |
| 1.3. When to use the CSM-DT?..... | 15 |
| 1.4. What technical systems do CSM-DT apply to? | 15 |
| 2. HOW DO THE CSM-DT FIT WITHIN THE OVERALL CSM RISK ASSESSMENT PROCESS? | 18 |
| 3. CONSIDERATION OF SYSTEMATIC FAILURES AND INTEGRATION OF THE TECHNICAL SYSTEM INTO THE RAILWAY SYSTEM..... | 22 |
| 3.1. Overall requirements in point 2.5.7. of Regulation 2015/1136..... | 22 |
| 3.2. Additional guidance on point 2.5.7. of Regulation 2015/1136..... | 23 |
| 4. CHOICE OF THE APPROPRIATE SEVERITY CLASS/CATEGORY | 26 |
| 4.1. Introduction | 26 |
| 4.2. Explanation of terminology in point 2.5.5 (see details in section § 4.4.1.)..... | 26 |
| 4.3. Explanation of the definition of a “technical system” | 28 |
| 4.4. Process proposed for selecting the appropriate CSM-DT class/category | 29 |
| 4.5. Precautions for the selection of the appropriate CSM-DT class/category | 34 |
| 5. APPLICATION OF CSM-DT AND USE OF BARRIERS | 38 |
| 5.1. Level of function to which the CSM-DT is applied | 38 |
| 5.2. Use of barriers..... | 38 |
| 5.3. Conditions for the use of barriers (intentional safety measures)..... | 39 |
| 5.4. Barriers not permanently present | 40 |
| 5.5. Level of application of CSM-DT | 40 |

| | |
|--|-----------|
| ANNEX 1 : LIST OF INFORMATIVE EXAMPLES OF TECHNICAL FUNCTIONS AND THE APPLICABLE CSM-DT CLASS/CATEGORY | 42 |
| ANNEX 2 : INFORMATIVE PRACTICAL EXAMPLES ILLUSTRATING THE LEVEL WHERE CSM-DT CAN BE APPLIED AND THE USE OF EXTERNAL BARRIERS .. | 50 |
| ANNEX 3 : EXAMPLE OF THE SWISS NATIONAL SAFETY AUTHORITY ON THE USE OF CSM-DT (STANDARDISED LEVEL CROSSING SYSTEM) | 53 |
| A3.1 Input references for this example..... | 53 |
| A3.2 (Preliminary) system definition..... | 53 |
| A3.3 Significance of the change | 55 |
| A3.4 Hazard identification and classification | 55 |
| A3.4.1 Hazard identification – Use of Failure Mode and Effect Analysis (FMEA) | 55 |
| A3.4.2 Hazard classification | 57 |
| A3.5 Broadly acceptable risks ?..... | 59 |
| A3.6 Selection of the risk acceptance principle | 59 |
| A3.6.1 Proposer’s decision..... | 59 |
| A3.6.2 Are harmonised design targets suitable for Level Crossing System? | 60 |
| A3.6.3 Allocation of the most credible CSM-DT category..... | 61 |
| A3.7 Apportionment of the CSM-DT value to the different contributing parts of the logical condition | 63 |
| A3.7.1 Different sub-functions of the MICRO level crossing system | 63 |
| A3.7.2 Supporting tools – Formal Modelling using Extended Deterministic and Stochastic Petri nets (EDSPN) | 64 |
| A3.7.3 Building the EDSPN model of the Level Crossing System | 64 |
| A3.7.4 Analysing the safety integrity of the entire Level Crossing System | 67 |
| A3.7.5 Analysis of the safety integrity of the single level crossing function | 69 |
| A3.7.6 Analysis of the influence of the hazard detection rate..... | 70 |
| A3.7.7 Setting up the safety requirements for the MICRO Level Crossing System..... | 71 |
| A3.7.8 Final decision on the (safety) requirements for the MICRO level crossing system | 72 |
| A3.8 Hazard Log/Record..... | 73 |
| A3.9 Conclusions | 73 |
| ANNEX 4 : EXAMPLES FROM REPRESENTATIVE BODIES ON THE USE OF CSM-DT | 75 |
| A4.1 Example 1 : Emergency brake control of a locomotive | 75 |
| A4.2 Example 2 : Train door opening authorisation | 83 |
| A4.3 Example 3 : Control of the traction cut-off..... | 91 |
| A4.4 Example 4 : Transmit traction and brake command..... | 94 |
| A4.5 Example 5 : Level crossing case study..... | 100 |

| | |
|---|------------|
| ANNEX 5: AGENCY EXAMPLE ON THE USE OF CSM-DT (TRAINBORNE HOT BOX DETECTOR) | 109 |
| A5.1 (Preliminary) system definition..... | 109 |
| A5.2 Significance of the change | 111 |
| A5.3 Hazard identification and classification | 112 |
| A5.3.1 Hazard identification – Use of Failure Mode and Effect Analysis (FMEA) | 112 |
| A5.3.2 Hazard classification | 113 |
| A5.4 Broadly acceptable risks ?..... | 114 |
| A5.5 Selection of the risk acceptance principle | 115 |
| A5.5.1 Proposer’s decision..... | 115 |
| A5.5.2 Are harmonised design targets suitable for trainborne Hot Box Detection? | 116 |
| <i>Approach of the question by point 2.5.5. in Annex I of Reg. 2015/1136.....</i> | <i>116</i> |
| <i>Approach of the same question from another angle through point 2.5.9. of Reg. 2015/1136.....</i> | <i>117</i> |
| A5.5.3 Allocation of the most credible CSM-DT category..... | 119 |
| A5.6 Apportionment of the CSM-DT value to the different contributing parts of the logical condition | 121 |
| A5.6.1 Supporting tools – Use of Fault Tree Analysis (FTA) techniques | 121 |
| A5.6.2 FTA of the trainborne Hot Box Detection function and available information | 121 |
| A5.6.3 Setting up the safety requirements for the Hot Box Detector – Alternative solutions | 125 |
| A5.6.3.1 Communication means for indication of Hot Box Event | 125 |
| A5.6.3.2 Case 1 : safety requirements when using a single Hot Box Detector..... | 126 |
| A5.6.3.3 Case 2 : safety requirements when using redundant Hot Box Detectors | 128 |
| <i>Common Cause Failure analysis requirements</i> | <i>128</i> |
| A5.6.3.4 Final decision on the (safety) requirements for the trainborne Hot Box Detectors | 132 |
| A5.7 Completeness of the risk assessment..... | 132 |
| A5.8 Hazard Log/Record..... | 133 |
| A5.9 Conclusion..... | 133 |
| A5.10 Appendix to Annex 5 : Supporting RAMS tools in the example..... | 136 |
| A5.10.1 Failure Mode and Effect Analysis tool (FMEA) | 136 |
| A5.10.2 Fault Tree Analysis Tool (FTA)..... | 136 |
| A5.10.3 Building/modelling, reduction and calculation of a Fault Tree..... | 137 |

List of Figures

| | |
|--|-----|
| Figure 1: Flowchart for the applicability test of the CSM-DT. | 16 |
| Figure 2: Use of CSM-DT within in the overall CSM risk assessment process. | 19 |
| Figure 3: Requirements for risk acceptance when applying CSM-DT and possible means of compliance. | 23 |
| Figure 4: Quantitative and Qualitative requirements conveyed by the CSM-DT. | 25 |
| Figure 5: Process proposed for the allocation of the appropriate CSM-DT class/category. | 30 |
| Figure 6: Failure of a function of a technical system without external barriers. | 40 |
| Figure 7: Failure of a function of a technical system with the presence of an external barrier through another technical system. | 41 |
| Figure 8: Failure of a function of a technical system with the presence of an external barrier through non-technical means (e.g. an operational barrier). | 41 |
| Figure 9: Level of function to which CSM-DT is applied. Simplified approach of an axle Counter with an external barrier through a technical system. | 51 |
| Figure 10: Conventional ATP with the use of an external non-technical system barrier. | 52 |
| Figure 11: Schematic representation of the MINI and MICRO Level Crossings (LCS). | 53 |
| Figure 12: Elements of the class of used Petri nets. | 64 |
| Figure 13: Dynamics in the Petri net. | 64 |
| Figure 14: Risk estimation for the H1or2 hazard defined in section § A3.6.3. | 65 |
| Figure 15: Risk estimation for the H3 hazard defined in section § A3.6.3. | 65 |
| Figure 16: The modules of the MICRO level crossing model in the π -Tool. | 66 |
| Figure 17: Dependence of the accident rate on LC from the failure rate of the LCS. | 67 |
| Figure 18: Dependence of the accident rate on level crossings in function of the failure rate of the single technical functions. | 70 |
| Figure 19: Dependence of the accident rate at a MICRO level crossing in function of the failure disclosure time (FDT) of its different technical functions. | 71 |
| Figure 20: Emergency braking functionality. | 76 |
| Figure 21: FTA of solution 1 for the emergency braking command. | 80 |
| Figure 22: FTA of solution 2 for the emergency braking command. | 81 |
| Figure 23: FTA of solution 3 for the emergency braking command. | 82 |
| Figure 24: Example of a train door opening control system. | 83 |
| Figure 25: Door control system. | 84 |
| Figure 26: Flow of information for the door control system. | 85 |
| Figure 27: Door control system – Solution 1. | 88 |
| Figure 28: Door control system – Solution 2. | 89 |
| Figure 29: Door control system – Solution 2 : all doors open at standstill. | 90 |
| Figure 30: Door control system – Solution 2. : all doors open during circulation. | 90 |
| Figure 31: System definition for the traction cut-off under ETCS. | 91 |
| Figure 32: Hazard scenarios for a failure of the traction cut-off system. | 92 |
| Figure 33: Event-tree for automatic traction cut-off (scenario 2) | 93 |
| Figure 34: System definition of the “transmit traction and brake demand”. | 95 |
| Figure 35: Interfaces of the „master controller “sub-function. | 95 |
| Figure 36: Link between the required CSM-DT and the safety performance that should be required for the Master Controller without taking into account any barrier. | 98 |
| Figure 37: Event tree for back-calculating the safety requirement for the Master Controller based on requirement for the “transmit traction and brake demand”. | 99 |
| Figure 38: Overview of automated level crossing. | 101 |
| Figure 39: Functional FTA for the switch-on function (O1) of the automated level crossing. | 106 |
| Figure 40: Causal analysis (FTA) for the automated level crossing. | 106 |
| Figure 41: Schematic representation of the events and contributors to the trainborne hot box detection function. | 110 |
| Figure 42: Article 4 criteria in Reg. 402/2013. | 111 |
| Figure 43: Logical condition leading directly to a failure of the trainborne hot box detection function. | 117 |
| Figure 44: Fault Tree of the trainborne Hot Box Detection function with one detector. | 122 |
| Figure 45: Fault Tree of a redundant trainborne Hot Box Detection function. | 129 |
| Figure 46: Example of a Fault Tree Analysis. | 137 |

List of Tables

| | |
|--|-----|
| Table 1: Document history. | 2 |
| Table 2: Table of reference documents. | 11 |
| Table 3: Table of terms. | 11 |
| Table 4: Table of abbreviations. | 12 |
| Table 5: Description of risk assessment activities for defining the applicable CSM-DT class/category. | 20 |
| Table 6: Only possible cases of CSM-DT vs. number of (affected persons; victims). | 34 |
| Table 7: Functions of the MINI and MICRO LCS. | 54 |
| Table 8: Application parameters of the MINI and MICRO LCS. | 54 |
| Table 9: Functional FMEA of the MICRO level crossing system. | 57 |
| Table 10: Hazard classification within the functional FMEA the MICRO level crossing system. | 58 |
| Table 11: Assessment of risk acceptability within the functional FMEA of the MICRO level crossing system. | 59 |
| Table 12: Allocation of the most credible CSM-DT category to the hazards identified in the FMEA. | 62 |
| Table 13: Assumptions about the behaviour of an individual person at the greatest danger. | 68 |
| Table 14: Example 1 of a possible apportionment of the overall safety requirement down to the different sub-functions of the MICRO level crossing system. | 72 |
| Table 15: Example 2 of a possible apportionment of the overall safety requirement down to the different sub-functions of the MICRO level crossing system. | 72 |
| Table 16: Example of Hazard Record for the Swiss example of a MICRO level crossing system. ^[CSM RA] | 74 |
| Table 17: Functional FMEA of the emergency brake. | 77 |
| Table 18: Hazard classification within the functional FMEA of the emergency brake. | 77 |
| Table 19: Input information for quantitative risk assessment of the emergency brake. | 79 |
| Table 20: Functional FMEA of the door control system. | 86 |
| Table 21: Hazard classification in the functional FMEA of the door control system. | 87 |
| Table 22: Hazards of the door control system that need further risk assessment. | 88 |
| Table 23: Allocation of CSM-DT class/category for the traction cut-off system. | 93 |
| Table 24: Main function and sub-functions of the “transmit traction and brake demand”. | 96 |
| Table 25: Hazard Identification and Classification of the “transmit traction and brake demand”. | 96 |
| Table 26: Allocation of the CSM-DT class/category for the “transmit traction and brake demand”. | 97 |
| Table 27: Functional description of the automated level crossing. | 101 |
| Table 28: Risk matrix for the automated level crossing. | 104 |
| Table 29: Example of a functional FMEA for the automated level crossing. | 105 |
| Table 30: Example of detection mechanisms and detection times for the automated level crossing. | 107 |
| Table 31: Functional FMEA of a trainborne Hot Box Detection. | 113 |
| Table 32: Hazard classification within the functional FMEA of a trainborne Hot Box Detection. | 114 |
| Table 33: Assessment of risk acceptability within the functional FMEA of a trainborne Hot Box Detection. | 115 |
| Table 34: Allocation of the most credible CSM-DT category to the hazards identified in the FMEA. | 120 |
| Table 35: Example of available RAMS input information. | 124 |
| Table 36: FTA results with one Hot Box Detector. | 127 |
| Table 37: FTA results with redundant Hot Box Detectors – Test interval 300 h. | 130 |
| Table 38: FTA results with redundant Hot Box Detectors – Test interval 3600 h. | 131 |
| Table 39: Example of Hazard Record for the Hot Box Detector example. ^[CSM RA] | 134 |

0. INTRODUCTION

0.1. Scope of this document

- 0.1.1. This document provides guidance on the application of the Commission implementing Regulation (EU) 2015/1136 of 13 July 2015 which amends the implementing Regulation (EU) No 402/2013 on the common safety method (CSM) for risk assessment {Ref. 1}, referred to hereafter "CSM for risk assessment".
- 0.1.2. The aim of this document is to explain how the harmonised design targets in point 2.5.5. of the Annex of Regulation 2015/1136 should be applied. This document should support a consistent interpretation and application of Regulation (EU) N°402/2013 on the CSM for risk assessment, and Regulation (EU) 2015/1136, when the quantitative part of the explicit risk estimation principle is used by the proposer to demonstrate, according to section § 4. of this document, the risk acceptability of hazards arising from failures of functions of technical systems.

To facilitate the reading of the document and the implementation of Regulation 2015/1136 :

- (a) the harmonised design targets are referred to hereafter as CSM Design Targets (CSM-DT);
- (b) the parts of the guide related to the general risk assessment process of [CSM RA] Annex I of Regulation 402/2013 are identified in Annexes 3, 4 and 5 hereafter in the same way as the first line of the present bullet point, i.e. with square brackets containing the "[CSM RA]" text inside and the exponent formatting;
- (c) the parts of the guide specific to the implementation of Regulation 2015/1136 [CSM-DT] are identified in Annexes 3, 4 and 5 hereafter in the same way as the first line of the present bullet point, i.e. with square brackets containing the "[CSM-DT]" text inside and the exponent formatting.

IMPORTANT NOTE :

The examples contained in the annexes can only be considered as informative examples which illustrate how Regulations 402/2013 and 2015/1136 can be applied. As they do not constitute complete and exhaustive risk assessments, there is no guarantee that all reasonably foreseeable hazards were identified. Additional risk assessment might be necessary to identify any potential hazards and ensure that appropriate risk control measures are identified and implemented. Thereby the examples in the annexes may not be copied without analysing beforehand the specific circumstances and needs of a technical system for any specific project under assessment.

- 0.1.3. This document does not contain any legally binding requirements. It represents the views of the European Union Agency for Railways and not those of other EU institutions and bodies. It is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.

Information on the document

- 0.1.4. This document contains only explanatory information of potential help for concerned users who directly or indirectly need to apply the CSM for risk assessment. It may serve as a clarification tool however without dictating in any manner mandatory procedures to be followed and without establishing any legally binding practice. This document provides explanations on the provisions contained in Regulation (EU) 2015/1136 and should be helpful for the understanding of the legal requirements described therein. Actors may continue to use their own existing methods for the compliance with Regulation (EU) N°402/2013 on the CSM for risk assessment and Regulation (EU) 2015/1136.
- 0.1.5. The guide document needs to be read and used together with the legal text to facilitate its understanding and application. It does not replace or otherwise amend the CSM Regulation.

0.2. Structure for this guide

- 0.2.1. Although the guide may appear to be a standalone document for reading purposes, it does not substitute the legal text.

0.2.2. Only where necessary, some text from Regulation 2015/1136 is copied in the present guide using the "Bookman Old Style" Italic Font, identical to the formatting and red colour of the present text. If a complete paragraph is copied, then the text is also surrounded by a box frame, as the present paragraph. This formatting enables to easily distinguish the original text of Regulation from the additional explanations provided in this document.

- 0.2.3. Basically, the document is structured to describe the purpose and application of the CSM-DT in the main body of the document whilst examples of its application are provided in related annexes. It is divided into the following parts:
- (a) **Introduction:** it explains the scope and aim of the guide and provides the list of reference documents;
 - (b) **Explanation of the legal text:**
 - (1) section 1. describes the scope of use of the CSM-DT, including the assessment of their applicability to the technical system under assessment, the type of technical system that is expected to be assessed using the CSM-DT and the broader use of the CSM-DT for quantitative risk assessments;
 - (2) section 2. shows how the definition of the applicable CSM-DT class/category fits within the overall risk assessment process defined in the appendix to Annex I of the CSM for risk assessment;
 - (3) section 3. further explores the application of the CSM-DT and discusses the requirements for considering also :
 - (i) the control of risks associated with the systematic failures (via recognised standards), and;
 - (ii) the safe integration of the technical system into the overall railway system;
 - (4) section 4. describes the terminology used for the CSM-DT and proposes a process for selecting the appropriate severity class/category defined in point 2.5.5 of the legal text;
 - (5) section 5. deals with the cases where failures of technical systems do not directly result in an accident. The section explains then how to use the CSM-DT to derive quantitative safety requirements when "barriers" external to the technical system under assessment are used to prevent the accident.

Information on the document

These sections are respectively supported and illustrated by informative examples in Annexes 1, 2, 3, 4 and 5.

(c) **Annexes with informative examples :**

- (1) Annex 1 provides for information a list of examples of technical functions indicating which CSM-DT would be the most appropriate;
- (2) Annex 2 describes for information practical short examples of the functional level at which the CSM-DT can be applied and the use of external barriers;
- (3) Annex 3 is a very detailed example of the Swiss NSA on the use the CSM for risk assessment and of CSM-DT for defining the safety requirements for upgrades of existing level crossings;
- (4) Annex 4 contains all examples of use of CSM-DT that have been proposed by the representative bodies (CER, EIM, UNIFE).
- (5) Annex 5 contains a very detailed example of risk assessment and use of CSM-DT when the accident does **not directly** result as a consequence of failure of a function of the technical system under assessment;

As pointed out in point (c) in section § 0.1.2. above, the examples contained in those annexes are purely indicative. They do not represent an exhaustive definition of the safety requirements for the considered cases. They must be used with precautions and only as one possible way to define the applicable quantitative requirements for the design of a technical system. Additional information and guidance on how to perform more detailed and exhaustive risk assessment can be found in relevant standards referenced to in the sections below of this guide.

Information on the document

0.3. Reference documents

Table 2: Table of reference documents.

| {Ref. N°} | Title | Reference | Version |
|-----------|---|--|--|
| {Ref. 1} | Commission implementing Regulation (EU) N°402/2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 | Commission Regulation (EU) N°402/2013 OJ L 121; 3.5.2013, p.8 | 30 April 2013 |
| {Ref. 2} | Commission implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method on risk evaluation and assessment | Commission Regulation (EU) 2015/1136 OJ L 185; 14.7.2015, p.6 | 13 July 2015 |
| {Ref. 3} | RAMS book of Alain VILLEMEUR on the "Reliability, Availability, Maintainability and Safety of complex industrial systems" The book deals with reliability, human factors and IT systems matters in complex industrial systems. French title of the book : "Sûreté de fonctionnement des systèmes industriels", Fiabilité, Facteurs humains, Informatisation – Auteur : Alain VILLEMEUR – Editions Eyrolles. | Author of the book : Alain VILLEMEUR | Eyrolles editions |
| {Ref. 4} | Book of Claude LIEVENS on the "safety of systems", Cepadues editions, from the French high national school on aeronautics and space (SUP'AERO). French title : « Sécurité des Systèmes », Ecole Nationale Supérieure de l'Aéronautique et de l'Espace (SUP'AERO), Claude LIEVENS, CEPADUES-EDITIONS | Author of the book : Claude LIEVENS | Cepadues editions |
| {Ref. 5} | Railway Applications – Communication, Signalling and Processing Systems – Safety related Electronic Systems for Signalling | EN 50129 | February 2003 |
| {Ref. 6} | Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process (the standard itself) | EN 50126-1 | September 1999 incorporates corrigendum May 2010 |
| {Ref. 7} | Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 2: Guide to the application of EN 50126-1 for Safety | EN 50126-2 (Guideline) | February 2007 |
| {Ref. 8} | Functional safety of electrical/electronic/programmable electronic safety-related systems | IEC 61508 | 2.0 |
| {Ref. 9} | Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive | ERA/GUI/01-2008/SAF | 1.1 06/01/2009 |
| {Ref. 10} | Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation | ERA/GUI/02-2008/SAF | 1.1 06/01/2009 |

0.4. Definitions

Table 3: Table of terms.

| Term | Definition |
|-----------------|---------------------------------------|
| Agency | The European Union Agency for Railway |
| Guide/Guideline | The application guide on CSM-DT |

0.5. Abbreviations

Table 4: Table of abbreviations.

| Abbreviation | Meaning |
|--------------|---|
| ATP | Automatic Train Protection |
| CCF | Common Cause Failure |
| CER | Community of European Railways |
| CMF | Common Mode Failure |
| CoP | Code of Practice |
| CSM | Common Safety Method |
| CSM-DT | CSM Design Target |
| CSI | Common Safety Indicator |
| E/E/PE | Electrical, Electronic and Programmable Electronic |
| EC | European Commission |
| ECM | Entity in Charge of Maintenance |
| EIM | European Rail Infrastructure Managers |
| FDT | Failure Detection Time |
| FMEA | Failure Mode and Effect Analysis |
| FMECA | Failure Mode, Effects and Criticality Analysis |
| HBD | Hot Box Detector |
| HBE | Hot Box Event |
| HDT | Hazard Detection Time |
| IM | Infrastructure Manager |
| LC | Level Crossing |
| LCS | Level Crossing System |
| LX | Level Crossing |
| NRV | National Reference Value |
| NNR | Notified National Rule |
| NSA | National Safety Authority |
| PTU | Swiss Public Transport Union (Verband öffentlicher Verkehr VöV) |
| Ref. Syst. | Reference System |
| RSD | Railway Safety Directive |
| RU | Railway Undertaking |
| SIL | Safety Integrity Level |
| SMS | Safety Management System |
| THR | Tolerable Hazard Rate |
| TS | Technical System (used in flowcharts in the document) |
| UNIFE | Union of European Railway Industries |
| WSF | Wrong Side Failure |

EXPLANATIONS OF THE LEGAL TEXT

1. SCOPE OF USE OF THE CSM DESIGN TARGETS (CSM-DT)

1.1. What are the CSM-DT ?

1.1.1. The CSM-DT, or harmonised design targets as set out in point 2.5.5. in the Annex of Regulation 2015/1136, are harmonised quantitative safety requirements. They “**can be used**”⁽¹⁾ as quantitative safety requirements for the random hardware failures of electrical, electronic and programmable electronic (E/E/PE) technical systems, for both infrastructure and rolling stock (i.e. fixed installations and movable equipment).

When the CSM-DT are used for the design of those technical systems, then the risks arising from failures of functions of those technical systems can be considered as acceptable if :

(a) the applicable category of harmonised design target is achieved [this relates to the compliance with point 2.5.7(a) in the Annex of Regulation 2015/1136];

and also

(b) the requirements in points 2.5.7(b) and 2.5.7(c) in the Annex of Regulation 2015/1136 are fulfilled.

This is further explained in section § 3. of this document.

1.1.2. The CSM-DT represent functional safety requirements. They correspond to the current safety levels and European approaches to quantitative risk assessment in railways. These railway safety levels are similar to the corresponding safety levels of civil aviation.

1.1.3. The CSM-DT do not represent a national safety level such as common safety targets (CSTs) nor national reference values (NRVs). Nor is CSM-DT a general risk acceptance criterion for the whole railway system of a Member State and/or any kind of railway component.

1.1.4. The CSM-DT are established mainly to support mutual recognition of technical systems (refer to sections § 1.3. and § 1.4.). Due to the complexity of the architecture and diversity of the overall railway system, the definition of an overall risk acceptance criterion covering all contributors for safety is currently not possible.

1.2. Is use of CSM-DT mandatory (Proposer’s responsibility)?

1.2.1. The **use of CSM-DT is not mandatory**. Indeed, **Regulation 402/2013 does not impose any order of priority**⁽²⁾ between the three risk acceptance principles. For the analysis, the

⁽¹⁾ The meaning of “can be used” is explained in section § 1.2. of this document.

⁽²⁾ Recital (11) of Regulation 402/2013 clarifies that “ the proposer should be responsible for the choice of the principle to apply “. Point 2.1.4 in the Annex of Regulation 402/2013 strengthens further the proposer’s responsibility by underlying that the CSM “ assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer “.

Explanations on the legal text

evaluation and the acceptance of risks associated to hazards that arise from a significant change, without prejudice to the obligation to comply with the applicable TSIs or a Notified National Rule(s), the proposer is free to choose one of the following three risk acceptance principles :

- (a) application of codes of practice;
- (b) comparison with a similar reference system;
- (c) explicit risk estimation.

The CSM for risk assessment leaves thus the freedom and responsibility to the proposer to use the risk acceptance principle(s), or a combination of those, which make(s) the risk(s) acceptable.

1.2.2. Regulation 2015/1136 does not question this overall proposer's responsibility. Mostly, it does neither impose any priority order among the three risk acceptance principles :

- (a) point 2.5.1. in the Annex of Regulation 2015/1136 is a slight rewording of the same point in Regulation 402/2013. It does not thus set out any priority order.

Independently on whether appropriate codes of practice or similar reference systems might exist, and thus could be used, the proposer remains responsible for the decision to use, or not to use, the explicit risk estimation for demonstrating the risk acceptability. Furthermore, although the proposer might decide to use explicit risk estimation, he can either use qualitative or quantitative risk control measures, or when necessary both qualitative and quantitative ones, to demonstrate the risk acceptability.

- (b) reciprocally, point 2.5.4. in the Annex of Regulation 2015/1136 stresses that :

If the proposer decides to use either codes of practice or reference systems for demonstrating the acceptability of the identified risks, the proposer is not obliged to perform additional explicit risk estimation, neither quantitative nor qualitative.

- (c) **the only explicit restriction in Regulation 2015/1136** : point 2.5.6. in the Annex explicitly stresses that the harmonised design targets (CSM-DT) “... *shall ...*” *neither be used “... for the design of purely mechanical technical systems”* nor for controlling “*the hazards arising from the purely mechanical part ...*” of a mixed technical system⁽³⁾. Thereby, CSM-DT cannot be used for mechanical systems but the use of (qualitative, quantitative or both) explicit risk estimation is not forbidden for the control of hazards arising from a purely mechanical (or a part of a) technical system.
- (d) Regulation 2015/1136 does not mention pneumatic technical systems. The use of CSM-DT is thus not forbidden for such technical systems provided the proposer demonstrates the risk acceptability and the CSM assessment body accepts the demonstration.

⁽³⁾ Point 2.5.6. in the Annex of Regulation 2015/1136 defines a “mixed technical system” as a technical system composed of both a purely mechanical part and a purely electrical, electronic and programmable electronic part.

Explanations on the legal text

1.3. When to use the CSM-DT?

1.3.1. The CSM-DT can be used in the following case :

- (a) when carrying out a significant change under the meaning of Article 4 of Regulation 402/2013;
- (b) for technical systems : refer to section § 1.4. of this document;
- (c) when the proposer decides to perform quantitative risk assessment in the scope of application of the explicit risk estimation risk acceptance principle.

Conversely, when in the scope of explicit risk estimation the proposer demonstrates that the risk is acceptable with the use of qualitative explicit risk control measures, the proposer is not obliged to perform additional quantitative risk assessments;

- (d) to set up the quantitative safety requirements for the design of a technical system (see section § 1.1. above).
- (e) to support the mutual recognition of the results of risk assessments of technical systems.

1.3.2. Although the CSM-DT are used primarily when mutual recognition is desired, they may be applied also for other purposes at the discretion of the proposer, if the proposer can demonstrate the risk acceptability.

1.3.3. According to points 2.5.6. and 2.5.11. in the Annex of Regulation 2015/1136, the CSM-DT are “ *the most demanding design targets that can be required for mutual recognition* ”. When they are used, mutual recognition is automatically ensured under the provisions of Article 15(5) of Regulation 402/2013.

1.3.4. More demanding design targets⁽⁴⁾ than the CSM-DT may be requested for a technical system, through a notified national rule, only if it is necessary to maintain the existing level of safety in the Member State where the change is introduced.

1.3.5. Figure 1 below shows a possible decision process for determining the applicability of the CSM-DT for a technical system. This is further explained in the sections below. The decision process for the selection of the CSM-DT class/category among the two severity classes [i.e. (a) or (b) in point 2.5.5. in the Annex of Regulation 2015/1136] is further detailed in section § 4. of this document.

1.3.6. CSM-DT do not apply for operational and organisational significant changes.

1.4. What technical systems do CSM-DT apply to?

1.4.1. The CSM-DT can be used for the design of technical systems of both the infrastructure and rolling stock, i.e. for fixed installations and movable equipment.

1.4.2. Figure 1 below shows the steps and questions that need to be considered and answered in order to determine whether to apply or not the CSM-DT to the technical system under assessment.

⁽⁴⁾ This is a possibility foreseen in point 2.5.10. in the Annex of Regulation 2015/1136.

Explanations on the legal text

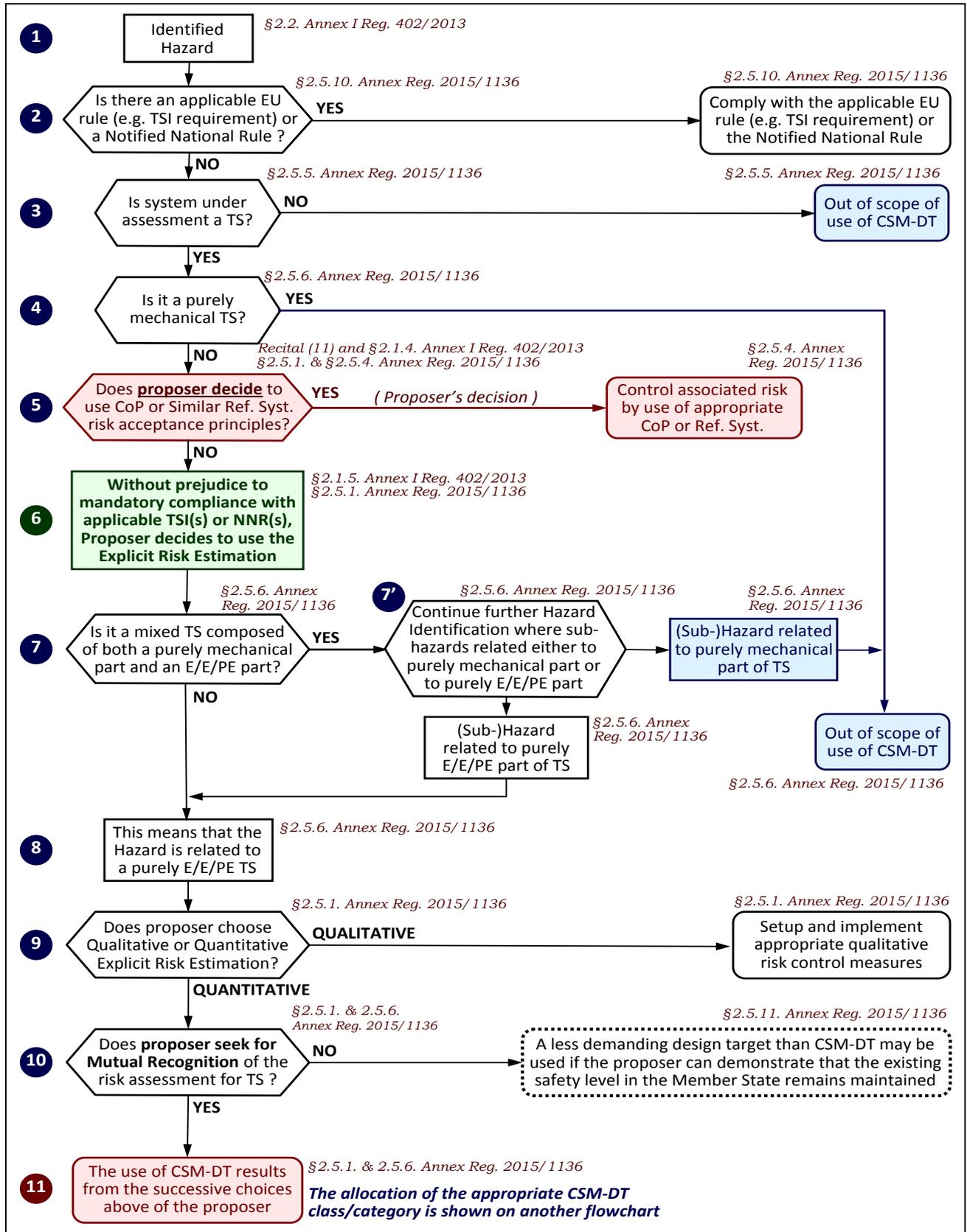


Figure 1: Flowchart for the applicability test of the CSM-DT.

Explanations on the legal text

- 1.4.3. Regulation 2015/1136 states explicitly that the CSM-DT should be applied for the design of Electrical, Electronic and Programmable Electronic (E/E/PE)⁽⁵⁾ technical systems. Technical systems can also be a mix of E/E/PE, as well as also having mechanical and/or pneumatic parts. The use of CSM-DT does not override the obligation to comply with applicable EU (e.g. TSI requirements) or a Notified National Rule(s)). It does neither override the proposer's responsibility to choose the risk acceptance principle he wants to apply (refer to the explanations in section § 1.2. above) for any of those types of technical systems.
- 1.4.4. Conversely, as described in section § 1.2.2.(c) above, point 2.5.6. in the Annex of Regulation 2015/1136 stresses that the CSM-DT shall not be used for the design of purely mechanical technical systems (e.g. wheel axles) or for the design of the mechanical part of a mixed technical system⁽⁶⁾. It does not recommend any specific approach for that.
- Although the application of (qualitative, quantitative or both) explicit risk estimation remains an option for the control of hazards arising from a purely (or a part of a purely) mechanical technical system, it is preferable to use either the "Code of Practice" or "Reference System" risk acceptance principle for the control of risks arising from failures of mechanical technical systems.
- 1.4.5. The proposer may also apply quantitative explicit risk estimation for the design of a technical system without using the CSM-DT. This requires an acceptance criterion either derived from or based on requirements contained in EU legislation or in notified national rules. The risk assessment should then be agreed by the CSM assessment body. According to Article 15(5) of Regulation 402/2013, in this case mutual recognition may be limited.
- 1.4.6. For E/E/PE technical systems approved methods exist in recognised standards (e.g. CENELEC 5012x series of standards or IEC 61508 standard) to demonstrate the achievement of quantified design targets and to cope with systematic failures which cannot be quantified. This is explained with more details in section 3.

⁽⁵⁾ Refer to first paragraph of point 2.5.6. in the Annex of Regulation 2015/1136.

⁽⁶⁾ Point 2.5.6. in the Annex of Regulation 2015/1136 defines a "mixed technical system" as a technical system composed of both a purely mechanical part and a purely electrical, electronic and programmable electronic part.

2. HOW DO THE CSM-DT FIT WITHIN THE OVERALL CSM RISK ASSESSMENT PROCESS?

2.1. This chapter describes how the definition of the CSM-DT fits within the overall risk assessment process of Regulation 402/2013. As explained in section § 1.2. above, at this step of the risk assessment, it is presumed that the proposer has selected the explicit risk estimation principle and has chosen quantitative risk assessment for controlling one or more hazards arising from failures of the technical system.

A detailed process on the choice of the appropriate severity class/category between the points 2.5.5(a) and 2.5.5(b) of the Annex of Regulation 2015/1136 is given in section § 4. of this document.

2.2. The place of CSM-DT within the CSM for risk assessment is illustrated in the flowchart in Figure 2. This is the overall CSM risk assessment process of the appendix to Annex I of Regulation 402/2013. The activities specific to the definition of the applicable severity class/category are then added (refer to the red shadow boxed in Figure 2) to show how the definition of the CSM-DT fits within that overall process.

2.3. Figure 2 does not address the factors associated with when explicit risk estimation principle may be applied. These aspects are addressed in chapter § 1. of this document, as well as elsewhere within the CSM for risk assessment and its existing guidelines (see {Ref. 9} and {Ref. 10}).

2.4. When applying the CSM for risk assessment, the definition of the applicable CSM-DT class/category has three major parts (delineated by the blue lines in Figure 2) :

(a) **A. Definition of the functional failures of the technical system under assessment** to be considered for the comparison with the two CSM-DT classes/categories. *These are activities (1) - (3);*

(b) **B. Selection of the CSM-DT severity class/category** (defined by point 2.5.5(a) and 2.5.5(b) in the Annex of Regulation 2015/1136) against which the estimated frequency of the functional failure of the technical system will be compared. *These are the activities (4) - (8);*

(c) **C.** In accordance with the existing provisions of the CSM for risk assessment (Regulation 402/2013) :

(1) **comparison of the estimated frequency** of failure of each defined function [*i.e. the calculated safety performance of the function of the technical system*] **with the CSM-DT applicable** for that function [*i.e. the harmonised design target*], and;

(2) definition of the associated safety requirements for the technical system.

This is the activity (9).

2.5. Each of the activities specific to the definition of the applicable CSM-DT class/category is described below with a reference to the identifying label in Figure 2 :

Pre-conditions :

- Significant Change requiring application of process in Annex I of Reg. 402/2013, or where application of that Regulation is required (e.g. as part of a Vehicle Authorisation)
- The proposer decides to apply the quantitative part of the Explicit Risk Estimation Principle

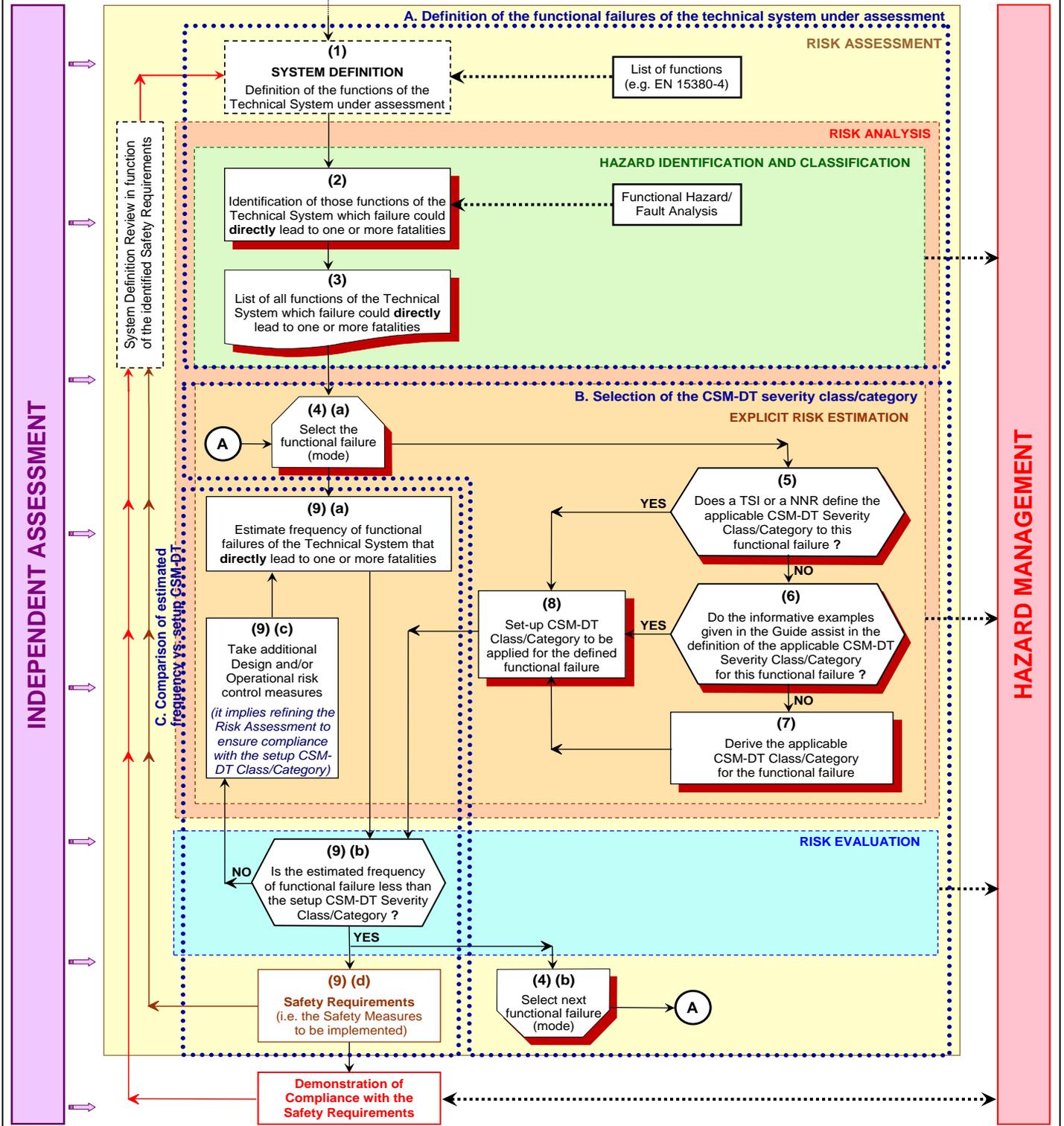


Figure 2: Use of CSM-DT within in the overall CSM risk assessment process.

Explanations on the legal text

Table 5: Description of risk assessment activities for defining the applicable CSM-DT class/category.

| No. | Activity/Output | Description |
|-----|---|---|
| (1) | Definition of the functions of the technical system under assessment | The CSM-DT apply to the functional failures of technical systems. As such, the functions of the technical system under assessment need to be defined. This can be done through reference to standard lists of functions; for example included within the CCS TSI, the EN 15380-4 ⁽⁷⁾ standard or other applicable lists. The functions should be limited to those provided by technical means. |
| (2) | Identification of those functions of the technical system which failure could lead directly to one or more fatalities | As defined in the regulatory text, the CSM-DT apply to functions of technical systems which failures have the potential to lead “directly” to one or more fatalities. As such, these functional failures should be defined from the Functional Hazard/Fault Analysis conducted as part of the safety justification of the technical system. It should be noted that functions of technical systems should be defined at the lowest level which failure could lead directly to a fatal consequence. This may involve the aggregating of lower level detailed functions of specific equipment and protection systems. <u>Note</u> : this activity focusses on failures having the potential to lead “directly” to one or more fatalities, i.e. those which in the risk assessment flowchart in Annex I of Regulation 403/2013 are not broadly acceptable. The risk assessment will of course capture all identified hazards and risks with various severity consequences. |
| (3) | List of all functions of the technical system which failure could directly lead to one or more fatalities | From activities defined in (1) and (2) above, a list is established with all the functional failures of the technical system which could result in a loss of life [fatality(ies)]. |
| (4) | Select one functional failure and derive the appropriate CSM-DT. | The process applies in turn to each of the functional failures defined in (3) above. This is depicted in the process diagram by repeating the activities between (4)(a) and (4)(b) for each identified functional failure. |
| (5) | Does the applicable TSI define the severity class/category applicable to this functional failure? | Where an EU (e.g. a TSI) or a notified national rule (NNR) defines the likely consequence and the functional failure, the EU/TSI or NNR should be used to select the respective CSM-DT severity class/category. |
| (6) | Do the informative examples given in this guidance (in Annex 1) assist in the definition of the applicable CSM-DT class/category for this functional failure? | Where not defined by the TSIs, the informative examples used in this guidance document could be used as the next preference to assist in the definition of the CSM-DT severity class/category to be applied to the functional failure of the technical system under assessment. As the examples contained in Annex 1 of this guideline are purely informative, they should not be applied without analysing the specific circumstances and needs of the technical system for the project under assessment. Consequently, the proposer needs to check whether the considered example is applicable to its specific case. |

⁽⁷⁾ EN 15380-4: Railway applications. Classification system for railway vehicles. Function groups.

Explanations on the legal text

Table 5: Description of risk assessment activities for defining the applicable CSM-DT class/category.

| No. | Activity/Output | Description |
|-----------------------|--|---|
| (7) | Derive the CSM-DT class/ category applicable to the functional failure | Where neither the TSIs nor this guidance document help to define the applicable CSM-DT severity class/category (e.g. for innovative systems), the regulatory text and this guidance document should be used to determine the CSM-DT severity class/category to be used. |
| (8) | Select the CSM-DT classes/categories to be applied for the defined functional failure(s) | Arising from activities (5) – (7) above, the CSM-DT severity class/category should be selected for each functional failure of the technical system under assessment. A more detailed process for the choice of the most appropriate severity class/category is given in section § 4. of this document. |
| (9)(a) - (9)(d) | Conduct existing CSM for risk assessment activities to compare the estimated functional failure frequency with the setup CSM-DT and incorporate this into the safety justification of the technical system | In accordance with the existing provisions of the CSM for risk assessment, the frequency of the defined functional failure should be estimated. This can involve the use of techniques such as FMECAs or fault tree analyses (FTAs). The estimated frequency can then be compared with the required CSM-DT class/category. Where this comparison does not demonstrate compliance with the required CSM-DT, then (as for other non-compliances) changes to the design and/or operation of the technical system and/or the risk assessment may be required such that compliance with the CSM-DT can be demonstrated. In accordance with the CSM for risk assessment, compliance against the CSM-DT as a justification of control of the applicable hazards should be recorded within the Hazard Record. Safety requirements reflecting the justification of the control of the hazard should be defined. |

3. CONSIDERATION OF SYSTEMATIC FAILURES AND INTEGRATION OF THE TECHNICAL SYSTEM INTO THE RAILWAY SYSTEM

3.1. Overall requirements in point 2.5.7. of Regulation 2015/1136

3.1.1. The CSM for risk assessment only defines the safety requirements that have to be complied with in order to render the risk acceptable when applying CSM-DT. Applying the regulation without the accompanying standards such as EN 5012x, or IEC 61508, or rules derived out of these standards dealing with functional safety of E/E/PE systems, is not recommended. However, the legal text does not prescribe any specific way to demonstrate compliance with the requirements, so other means of demonstration are acceptable, provided they represent good engineering practice and are acceptable to the CSM assessment body.

3.1.2. Point 2.5.7. in the Annex of Regulation 2015/1136 defines the following three basic requirements the proposer has to fulfil when using Explicit Risk Estimation :

(a) “The compliance with the applicable harmonised design target has been demonstrated”.

The demonstration needs to be done in a quantitative way in compliance with the prescriptions of recognised standards. The demonstration of compliance with the design target covers only the random part of the failure rate. It should be noted that whilst this clearly includes random hardware failures there exist further contributors to this random failure integrity : see point (b) below.

(b) “The associated systematic failures and systematic faults are controlled in accordance with safety and quality processes commensurate with the harmonised design target applicable to the technical system under assessment and defined in commonly acknowledged relevant standards”.

The control of systematic failures is at least equally important as the control of random failures. Stringent safety and quality processes have to be applied during the development, the operation and the maintenance of the technical system in order to control the systematic failures and systematic faults that can be introduced during those steps of the life-cycle of the technical system. Such processes are described in recognised standards, e.g. covered by various safety integrity concepts (e.g. defining SILs for computerised safety-related equipment).

(c) “The application conditions for the safe integration of the technical system under assessment into the railway system shall be identified and registered in the hazard record in accordance with point 4. In accordance with point 1.2.2, these application conditions shall be transferred to the actor responsible for the demonstration of the safe integration.”.

The requirement for safe integration is an existing part of the risk management process of the CSM (e.g. Annex I, point 1.2.7 in Regulation 402/2013). The technical system cannot be considered individually but needs to be analysed in its operational environment within the railway system. The CSM-DT is a contributor to the safe integration and does not guarantee safe integration by itself (see in particular the use of barriers explained later in the guideline). The proposer needs thus to identify the application conditions to be verified for the safe integration of the technical system within its operational environment.

Explanations on the legal text

3.1.3. Figure 3 illustrates the overall requirements from the legal text and possible means of compliance for the proposer.

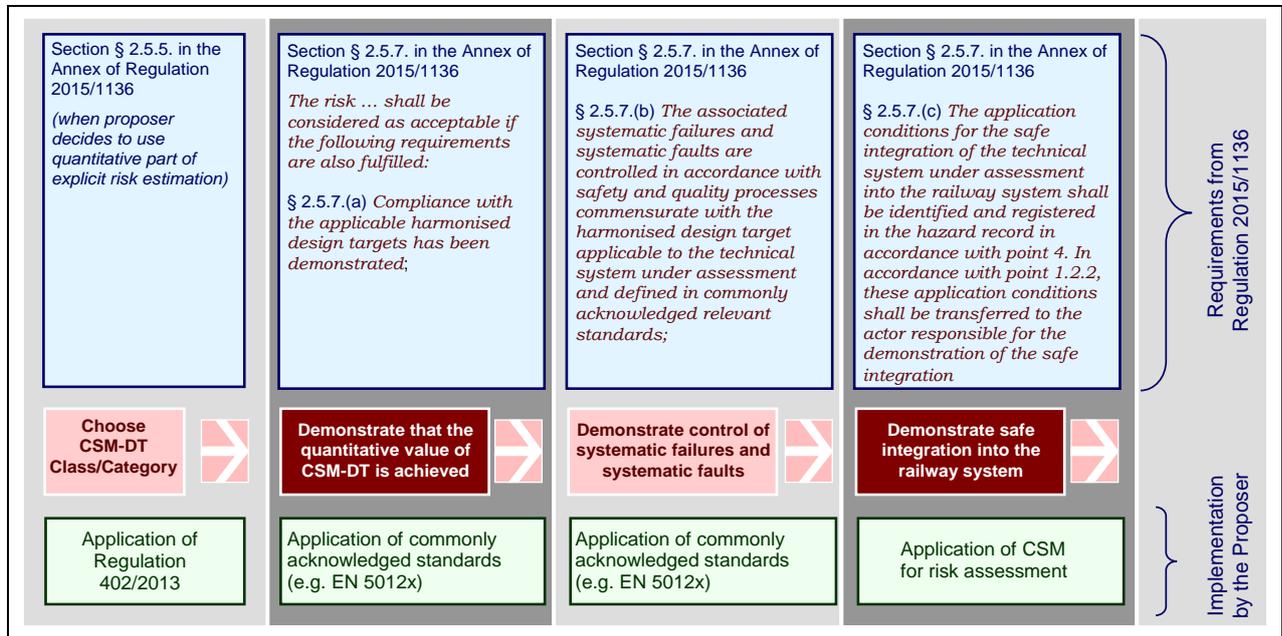


Figure 3: Requirements for risk acceptance when applying CSM-DT and possible means of compliance.

3.1.4. The safety of a railway system is adequately demonstrated only when all three legal requirements of point 2.5.7. in the Annex of Regulation 2015/1136 are fulfilled. The process of demonstration can be divided between different stakeholders like manufacturer and operator. The responsibility for the demonstration should be defined accordingly.

3.2. Additional guidance on point 2.5.7. of Regulation 2015/1136

3.2.1. According to point 2.5.7 in the Annex of Regulation 2015/1136 and the associated explanations in section § 3.1.2. above, the single compliance with the quantitative value of a CSM-DT is not sufficient for the risk acceptance. The CSM-DT can therefore be considered as semi-quantitative requirements that convey requirements for the control of risks arising from both the random hardware failures and the systematic failures/ errors⁽⁸⁾ of the technical system under assessment.

3.2.2. The systematic failures/errors of the technical system potentially resulting from human errors during the development process of the technical system (i.e. specification, design, implementation, testing and validation) need thus also to be covered by appropriate risk control measures. The human errors during the operation and maintenance of the technical systems are not covered by the CSM-DT. Those errors need to be covered by appropriate

⁽⁸⁾ *The terms “fault, error, failure” are closely related with each other although they have different meanings (see e.g. IEC 60050 standard). According to the definition 3.1.5. in the CENELEC 50129 standard, “error means a deviation from the intended design which could result in unintended system behaviour or failure”.*

Explanations on the legal text

operational and maintenance processes, procedures and working instructions of the management system of the company using or maintaining the technical system.

- 3.2.3. According to appendices A.3 and A.4 of the CENELEC 50 129 standard, the systematic failures/errors are not quantifiable and thus the quantitative target of CSM-DT needs to be demonstrated for the random hardware failures only, while the systematic failures/errors are addressed by qualitative methods⁽⁹⁾. *"Because it is not possible to assess systematic failure integrity by quantitative methods, safety integrity levels are used to **group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realisation of a system to a stated integrity level.**"*
- 3.2.4. Similarly, according to the CENELEC standards, the integrity of the software of technical systems is not quantifiable. The CENELEC 50 128 standard, provides guidance for the development process of safety related software in function of the requested safety integrity level. That includes the design, verification, validation and quality assurance processes for the software development.
According to the CENELEC 50 128 standard; for a programmable electronic control system, implementing safety functions, the highest possible safety integrity level for the software development process is SIL 4. According to the CENELEC 50129 standard (see footnote (24) on page 127), SIL 4 is appropriate for a function with a quantitative tolerable hazard rate of 10^{-9} h^{-1} and SIL 2 is appropriate for a function with a quantitative tolerable hazard rate of 10^{-7} h^{-1} .
- 3.2.5. Therefore, as the systematic failures/errors cannot be quantified, they need instead to be managed qualitatively by putting in place a quality and safety process that are compatible/commensurate with the safety integrity level required for the technical system under assessment. As explained in sections § 5.2 and § 5.3 of the CENELEC 50129 standard :
- (a) the purpose of the quality process is *"to minimise the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system"*;
 - (d) the purpose of the safety process is *"to reduce further the incidence of safety related human errors throughout the life-cycle and thus minimise the residual risk of safety related systematic faults."*
- 3.2.6. Guidance for managing the incidence of systematic failures/errors, as well as guidance for possible design measures to protect against Common Cause/Mode Failures (CCF/CMF) and to ensure that the technical system enters a fail-safe state in case of such failures/errors, is provided e.g. in the IEC 61508 or CENELEC 50 126-1, 50 128 and 50 129 standards. The CENELEC 50 126-2 guide gives additional guidance. :

In particular, the CENELEC 50 128 standard provides guidance for the development process of safety related software in function of the safety integrity level (SIL 0 to SIL 4) that is requested for railway control and protection system (i.e. CCS).

⁽⁹⁾ *According to the CENELEC 50 126, 50 128 and 50 129 standards, the quantitative figure dealing with random hardware failures must be always linked to a safety integrity level to manage the systematic failures/errors. Therefore, the CSM-DT figures also require that an adequate process is put in place to correctly manage also the systematic failures/errors.*

Explanations on the legal text

3.2.7. The application of the processes in the flowcharts in Figure 1 and Figure 5 and the compliance with the CSM-DT can be summarised as represented in Figure 4.

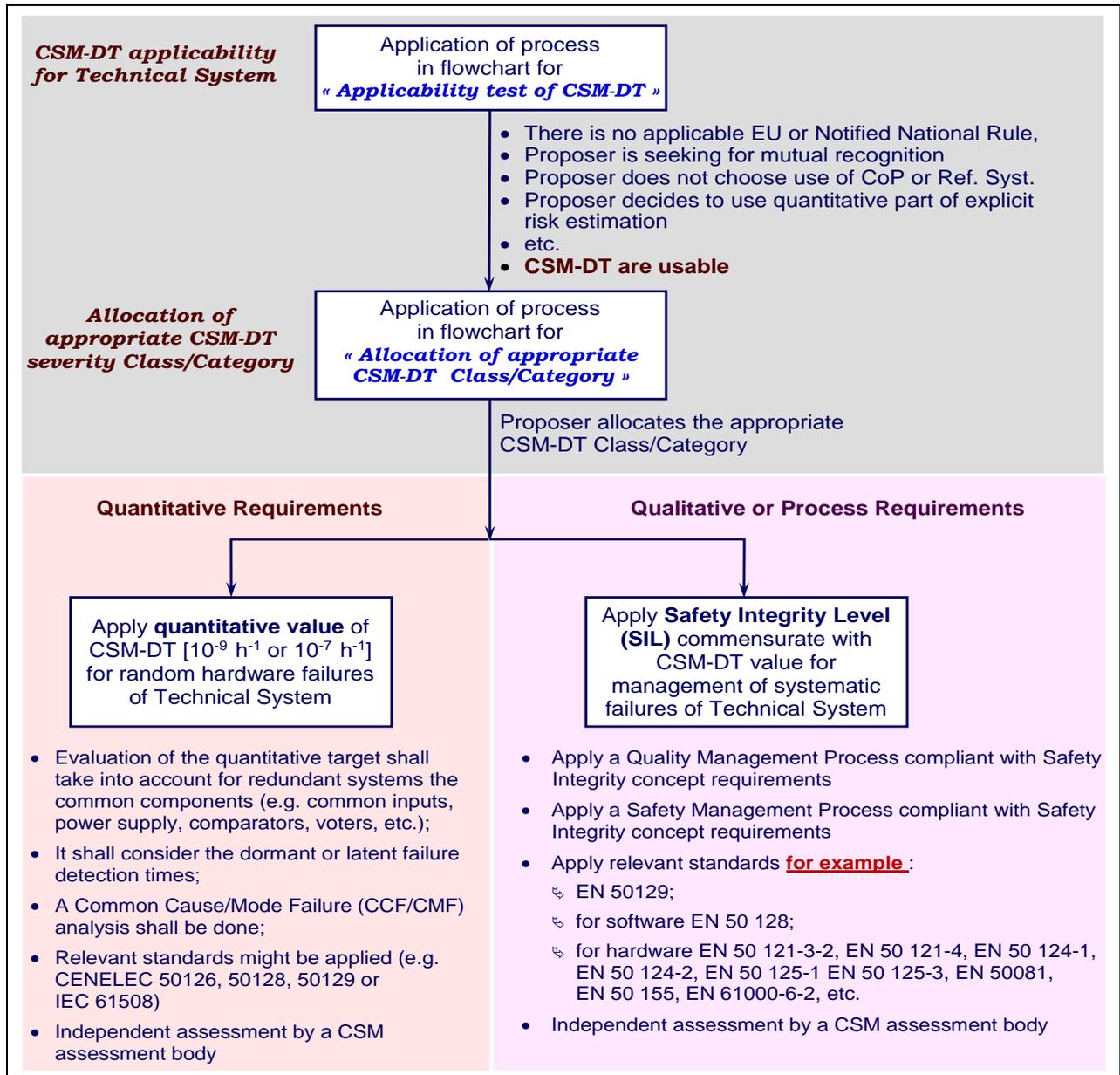


Figure 4: Quantitative and Qualitative requirements conveyed by the CSM-DT.

4. CHOICE OF THE APPROPRIATE SEVERITY CLASS/CATEGORY

4.1. Introduction

4.1.1. Chapter 1. describes the scope of use of harmonised design targets (CSM-DT); Figure 1 proposes a process for helping the proposer with the decision to use, or not to use, the quantitative part of explicit risk estimation and the CSM-DT for demonstrating the risk acceptability for the hazards arising from failures of a function of a technical system.

4.1.2. This chapter further explains how to select the most appropriate CSM-DT between the two severity classes/categories that are defined in points 2.5.5(a) and 2.5.5(b) in the Annex of Regulation 2015/1136. Indeed, each severity class/category is linked to a different quantitative design target. Hereinafter these severity classes/categories are respectively denoted as "Class/Category (a)" and "Class/Category (b)". A process flowchart is also proposed in Figure 5 to help the proposer to allocate the appropriate severity class/category.

4.2. Explanation of terminology in point 2.5.5 (see details in section § 4.4.1.)

4.2.1. The choice between the two severity classes/categories (a) and (b) is already predetermined by the wording and terminology of the legal text of point 2.5.5. in the Annex of Regulation 2015/1136. The understanding of the legal text is greatly facilitated when replacing the relevant text⁽¹⁰⁾ by the corresponding definitions of Article 1 of Regulation 2015/1136. Point 2.5.5 becomes then :

*Where hazards arise as a result of **failures of functions of a technical system**, without prejudice to points 2.5.1 and 2.5.4, the following harmonised design targets shall apply to those failures :*

*(a) where a failure has a **credible potential** to lead **directly** to an accident **typically affecting a large number of people** and **resulting in multiple fatalities**, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to 10^{-9} per operating hour.*

*(b) where a failure has a **credible potential** to lead **directly** to an accident **typically affecting a very small number of people** and **resulting in at least one fatality**, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to 10^{-7} per operating hour.*

The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure.

4.2.2. What does this terminology then mean? – "Dissection" of the words in the legal text

(a) " *Where hazards arise as a result of failures of functions of a technical system ...* " means that CSM-DT apply to technical systems. Among the whole set of the scenarios identified by the explicit risk estimation, the CSM-DT apply only to the wrong side failures of technical systems that could potentially lead to an accident : refer to section § 1.3.;

⁽¹⁰⁾ Definition (23) of "catastrophic accident", definition (35) of "critical accident", definition (36) of "highly improbable" and definition (37) of "improbable".

Explanations on the legal text

- (b) "... , *without prejudice to points 2.5.1 and 2.5.4,...* " means that the use of CSM-DT is not mandatory. CSM-DT are not standalone requirements but are integrated into the overall CSM risk assessment framework where codes of practice or comparison with similar reference systems can be used instead. Without prejudice to the obligation to comply with applicable EU (e.g. TSIs) or a notified national rule(s), the proposer is the only responsible for the decision to use, or not to use, the explicit risk estimation for demonstrating the risk acceptability. Refer also to section § 1. and in particular to points (a) and (b) in section § 1.2.2.;
- (c) "... *the following harmonised **design targets** shall apply to those failures...* " means that CSM-DT are used to setup the safety requirements for the design of the technical system. It does not mean that this will be the actual safety performance achieved by the related technical system on the field;
- (d) "*where a failure has a **credible**...* " means it must be plausible that the particular failure of the technical system can result in an accident with the severity consequences considered in point 2.5.5. Hypothetical and not reasonable scenarios need not to be considered (refer to point 4.2.2.(j) below);
- (e) "... **potential**..." means that when the failure of the technical system occurs, it is quite possible that it results in an accident with the severity consequences considered in point 2.5.5. This is a conservative assumption which further reinforces the meaning of the term "**credible**". In practice, when a failure of a technical system occurs most of the time the consequence is not as severe as considered in a predictive risk assessment. For example a train derailment is not necessarily catastrophic or a spurious train door opening does not result with one fatality yet it is considered that the first event has a potential to lead to multiple fatalities and the second one to at least one fatality;
- (f) "... *to lead **directly** to an accident...* " means in this context that no effective barriers external to the technical system under assessment exist that may prevent an accident due to the failure of the technical system.
- If the consequence does not directly result from a failure of the technical system, CSM-DT do not apply straightforward to the technical system. The impact of mitigating effects or safety barriers (e.g. a human action or another technical system preventing the accident) could be taken into account in the safety analysis;
- (g) "***typically affecting**...* " allows to discriminate between the two accident severity consequences of point 2.5.5 based on the number of people exposed to risk and thus on the magnitude of risk :
- (1) "***typically affecting a large number of people **and** resulting in multiple fatalities** " means that many people might be exposed to risk and might be killed, or;*
- (2) "***typically affecting a very small number of people **and** resulting in at least one fatality**" means that only a few people might be exposed to risk and to fatality;*
- If the failure of a function of the technical system does not result in any fatality, that failure is outside the scope of use of CSM-DT.
- (h) "... *the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to...* " :
- (1) "*10⁻⁹ per operating hour*" for class/category (a);
- (2) "*10⁻⁷ per operating hour*" for class/category (b);

Provided that :

- (3) all the conditions here above are fulfilled, and;

Explanations on the legal text

- (4) it is demonstrated during the predictive risk assessment of the design of the technical system that the frequency of occurrence of the failure of the technical system is less than the applicable quantitative value

then the associated risk is acceptable and does not have to be reduced further from the quantitative point of view if the clauses (b) and (c) in point 2.5.7. are also fulfilled (refer to section § 3.1.2. of this document).

- (i) The “*operating hour*” relates directly to the function which causes the failure mode. This relates to the cumulative operating times of the considered technical system :
- (1) where the technical system is part of a train, the appropriate “*operating hour*” metric might be the average number of operating hours per day;
 - (2) where the technical system is a non-train-based system, the appropriate “*operating hour*” metric might be the average number of operating hours per day of the technical system.

- (j) “*The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure*” :

When the clauses (a) and (b) in point 2.5.5. are correctly applied, this sentence is redundant. It does not provide additional requirements; it reminds that the allocation of the most appropriate CSM-DT class/category needs to be based on the most credible unsafe consequence taking into account :

- (1) the number of people exposed to risk, i.e. either “a very small number of people” [class/category (b)] or “a large number of people” [class/category (a)], and;
- (2) the typical credible unsafe consequence of the type of accident [i.e. either multiple fatalities or a few fatalities] that might potentially (i.e. it is plausible) result from the failure of the technical system

This sentence suggests thus that the “more stringent” CSM-DT class/category which is credible is selected; it excludes the obligation to consider the “worst case and hypothetical scenarios” that are not plausible to happen.

- 4.2.3. Failures that have a typical credible potential of **less than one fatality** (i.e. that are limited to potential injury(ies) without the occurrence of a fatality) are also within the scope of Regulation 402/2013, but they are **not covered by the harmonised CSM-DT**. For such failures, other ways to determine whether an acceptable level of risk has been achieved have to be selected (e.g. application of a code of practice, comparison with a similar reference system or explicit risk estimation with appropriate acceptance criteria). The proposer may also use non-harmonised quantitative criteria for the acceptance of the associated risk(s).

4.3. Explanation of the definition of a “technical system”

- 4.3.1. Article 3(22) of Regulation 402/2013 defines a technical system as follows :

(22) *‘technical system’ means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;*

Explanations on the legal text

- 4.3.2. This definition of a technical system covers the scope of the technical system: *"technical system means a product or an assembly of products including the design, implementation, and support documentation."* Accordingly, it consists of and includes :
- (a) the physical parts constituting the technical system;
 - (b) the associated software (if any);
 - (c) the design and the implementation of the technical system, including if applicable the configuration or parameterisation of a generic product to specific requirements of the specific application;
 - (d) the supporting documentation necessary for :
 - (1) the development of the technical system;
 - (2) the operation and maintenance of the technical system.
- 4.3.3. The notes associated to this definition specify further the scope of the technical system:
- (a) *"The development of a technical system starts with its requirements specification and ends with its acceptance"*. It includes the phases 1 to 10 of the V-Cycle represented in Figure 10 of the CENELEC 50 126-1 Standard {Ref. 6};
 - (b) *"Although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system"*. This means that the errors due to human interactions with the technical system during the operation and the maintenance of the technical system are not part of the technical system itself and of its definition. Nevertheless, the design of the interfaces with the human operators needs to take them into account in order to minimise the probability of human errors due to a poor design of the relevant interfaces with the human operators;
 - (c) *" The maintenance process is described in the maintenance manuals but is not itself part of the technical system."* This means that the CSM-DT need not be applied to the operation and maintenance of the technical system; these rely strongly on processes and actions performed by human personnel.
However, in order to support the maintenance of technical systems, the technical system definition must include any relevant requirements (e.g. periodic preventive maintenance, or corrective maintenance in case of failures, requirements), with a sufficient level of details. But how the maintenance needs to be organised and achieved on the related technical system is not part of the technical system definition but in the corresponding maintenance manuals.

4.4. Process proposed for selecting the appropriate CSM-DT class/category

- 4.4.1. In order to allocate the right severity class/category to the considered hazard, the decision process in Figure 5 can be used. The following successive checks could be applied :
- (a) Results from previous steps of risk assessment and the process in Figure 1 :
 - (1) **Step 1** : the identified hazard arises as a result of a function of a technical system;
 - (2) **Step 2** : the CSM-DT are applicable for the hazard. Independently on whether appropriate codes of practice or similar reference systems might exist, and could be applied, the proposer decides to use the quantitative part of explicit risk estimation for demonstrating the risk acceptability⁽¹¹⁾;

⁽¹¹⁾ Refer to the explanations in sections § 1.2., § 1.3. and § 1.4. of this document.

Explanations on the legal text

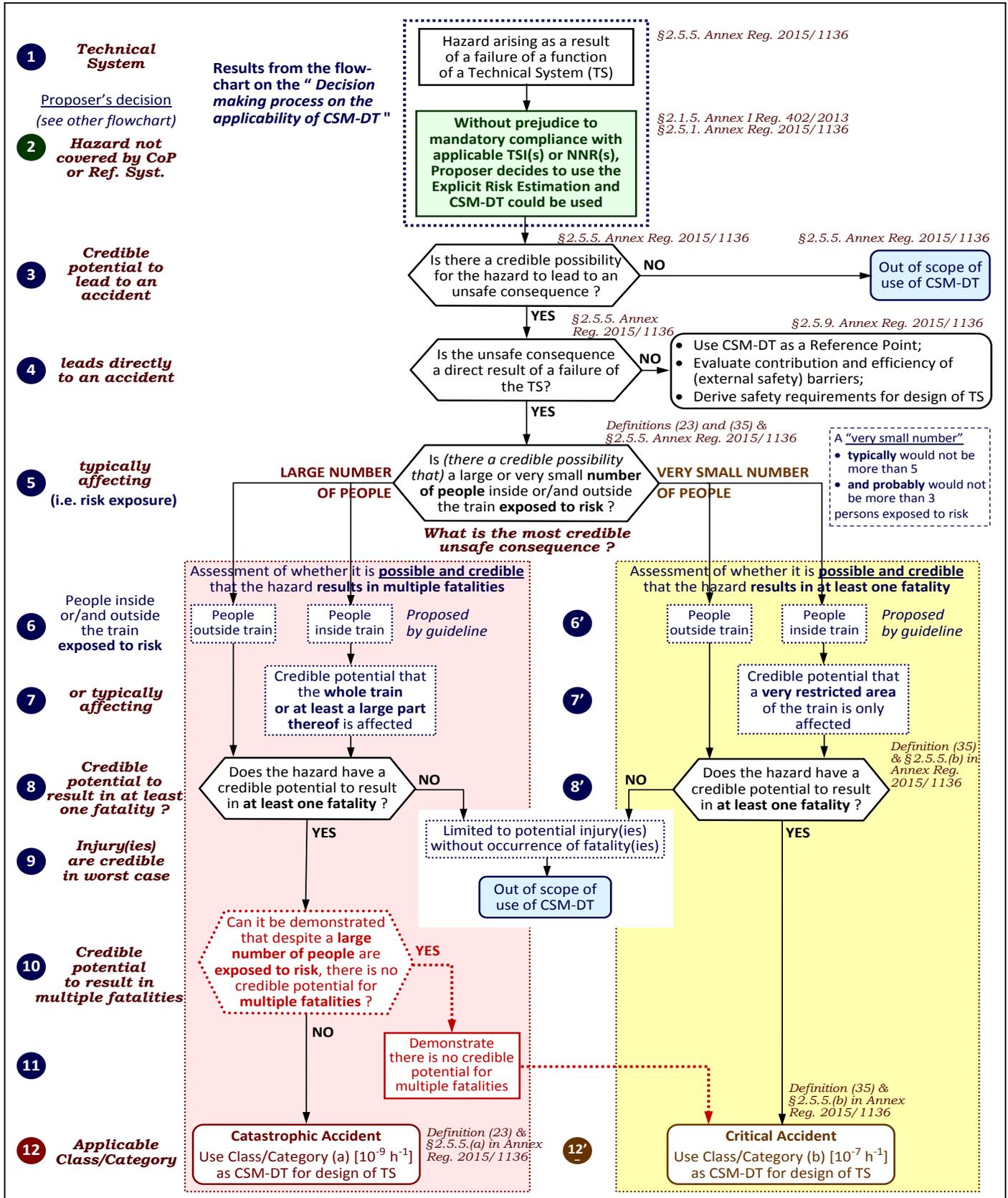


Figure 5: Process proposed for the allocation of the appropriate CSM-DT class/category.

Explanations on the legal text

- (b) **Step 3** : is there a credible possibility that the hazard leads to an unsafe consequence?

When it is not plausible that the hazard leads to an unsafe consequence, the hazard control falls outside the scope of use of CSM-DT.

- (c) **Step 4** : is the unsafe consequence a direct result of a failure of a function of the technical system?

CSM-DT are not applicable straightforward for failures that do not directly lead to an unsafe consequence. However if barriers external to the technical system under assessment exist, then the CSM-DT may still be applied. The quantitative safety requirements for the design of the technical system can be derived using the CSM-DT as a reference point and taking into account the contribution and effectiveness of the level of control provided by the external safety barriers. See section 5. for more details.

- (d) **Step 5** : is (there a credible possibility that) **a large number of people**, or on the contrary **a very small number of people**, for example those inside or/and outside the train or vehicle, are typically affected by the unsafe consequence (accident)?

The notion of “**number of people affected**” by the unsafe consequence (accident) or “**number of people exposed to risk**” is introduced as a discriminator to characterise the **magnitude of the risk** under assessment. “*Number of people affected/exposed to risk*” does not refer to the actual number of fatalities resulting from the accident, since anyway this information is unknown at the moment of a predictive risk assessment. “*Number of people affected/exposed to risk at any one time*” is used to estimate whether the accident has mainly a **limited local effect** or whether it has a **widespread potential effect**.

When the number of people exposed to risk and the severity of the accident consequence are not obvious, point 2.5.5 in the Annex of Regulation 2015/1136 requires to select the most credible unsafe consequence between severity classes/categories (a) and (b). The more demanding class/category needs still to be credible. This excludes thus the obligation to consider the “worst case and hypothetical scenarios” that are not plausible to happen.

Assessment of whether it is possible and credible that the hazard results in multiple fatalities or conversely in a very small number of fatalities

Depending on whether there is a credible possibility that **a large number of people**, or conversely **a very small number of people**, are exposed to risk, the left or the right branch of the process in Figure 5 above will need to be considered.

- (e) **Steps 6 and 6'** : the assessment of the consequence severity needs to consider all the people, both inside and outside the train, who are exposed to risk : train passengers, train driver(s), trackside workers, people living or working along the railway line, etc. :

“People outside the train” : for example, a derailment at a level crossing of a freight train transporting dangerous goods has a **credible potential** to result in multiple fatalities also for the people living or working along the railway line. Similarly, the collision of a freight train catching up a passenger train ahead exposes to risk also the passengers of that train.

Consequently, for these two examples, in addition to the freight train driver and the road users of the level crossing, those other categories of people who are also exposed

Explanations on the legal text

to risk, need to be considered carefully for the selection of the appropriate consequence severity class/category.

- (f) **Step 7 and 7'** : when assessing the consequence of failures of technical systems of a Rolling Stock, usually the following alternative and complementary questions could be asked in order to determine the applicable consequence severity class/ category :

- (1) **step 7** : *“Is there a credible potential (i.e. possibility) that the whole train, or at least a large part thereof, is affected by the unsafe consequence (accident)?”*

In that case, it is equivalent to asking the question *“Is a large number of persons affected?”*. The concept is somewhat similar to what is used in civil aviation (“loss of a plane”).

The whole train is affected where serious damage can be credibly expected in different parts of the train, e.g. several cars or parts of the train. This will usually be the case if trains are derailling at high speed or two trains are colliding at high speed. In those cases class (a) should be chosen.

- (2) **step 7'** : *“Is there a credible potential (i.e. possibility) that a very restricted area of the train is affected by the unsafe consequence (accident)?”*

Conversely, an accident might typically be limited to some specific part of the train, e.g. the untimely opening of a single door or some collisions at a low speed with an obstacle which only affect the front of the train.

If the concept of “whole train affected” is not applicable for estimating the consequences of the studied hazard then the more general concept “number of persons affected” should be used.

- (g) **Steps 8 and 8'** : does the hazard have a credible potential (i.e. possibility) to result in multiple fatalities (step 8) or in at least one fatality (step 8')?

The purpose of this check is to answer the question : **“Can or cannot the accident credibly and possibly result in death of people?”** At this moment of the risk assessment, we should be in either the left or right branch of flowchart in Figure 5 :

- (1) if the answer is “YES”, the considered severity class/category of CSM-DT should be applied for the design of the technical system (see below);
- (2) if the answer is “NO”, it is not credible to have any fatality and the consequence is limited to potential (light) injury(ies). Then , the control of the associated hazard falls outside the scope of use of CSM-DT (i.e. step 9).

The allocation of the correct severity class/category of CSM-DT depends on the “number of people exposed to risk” **and** the possible and credible outcome of the accident. Consequently, it is neither possible, nor important nor necessary to determine the actual number of fatalities resulting from the accident and to look for a quantitative difference between “at least one fatality” and “multiple fatalities”. This information is anyway unknown in predictive risk assessments.

What is the credible potential for the accident consequence severity?

In practice, referring to point (d) in section § 4.4.1. above, the maximum number of fatalities is limited by the total number of people exposed to risk, i.e. the entire population of either the “large number of people” or the “very small number of people”. So, in principle in a predictive risk assessment :

Explanations on the legal text

(3) **step 8** : in case of a “large number of people” affected by the accident, usually the maximum number of fatalities cannot be limited to a reasonably small number of people (*if there is a credible potential for that type of accident*). It is plausible that the entire population of the whole set “large number of people” could be killed.

If it is plausible that only a few people could be killed, then it is highly probable that a very small number of people would actually be exposed to risk. So, the second branch of the flowchart in Figure 5 should have been considered;

(4) **step 8'** : in case of a “very small number of people” affected by the accident, the maximum number of fatalities is very limited :

- (i) **typically** “at least one fatality” would **not be more than 5** fatalities, and;
- (ii) **probably** “at least one fatality” would **not be more than 3** fatalities.

Note about the “potential for fatalities” :

It must also be stressed that the predictive risk estimation has only to assess the potential for fatality(ies). Distinction cannot be made between “fatality” and “severe injury” since the question seeks for the “potential or possibility” and not for the actual outcome that can be retrieved from statistics of events that occurred in the past. For this reason, in terms of potential consequence of the accident, it is impossible to know whether a failure of a function of a technical system can be limited to a “severe injury”, can lead to immediate death or whether the “severe injury” will end up with death after some time. The only difference that can be made during the predictive risk estimation is either :

- (9) “there is a potential for the person to die” due to the failure of a function of the technical system, or;
- (10) “it is not possible for the person to die” due to the failure of a function of the technical system. In the worst case, it may lead to an injury but this injury cannot kill the person.

(h) **Step 9** : this is the result of the risk assessments done in steps 8 and 8' :

When a failure of a function of a technical system is limited to potential injury(ies) without the occurrence of fatality(ies), the control of the associated hazard falls outside the scope of use of CSM-DT : see also section § 4.2.3. above;

(i) **Step 11** : large number of people exposed to risk but particular operational conditions :

When there is potential for death of people but it can be demonstrated that despite a “large number of people” are exposed to risk there is no credible potential for “multiple fatalities” but for “at least one fatality”, due for example to particular operational conditions (e.g. train operated at low speeds, low traffic density, etc.), then :

- (1) the proposer must provide the justifications that there is no credible potential for multiple fatality;
- (2) the proposer must register those justifications in the Hazard Record of the risk assessment to enable the monitoring of their validity during the entire life-cycle of the technical system under assessment;
- (3) the justification must be independently assessed by the CSM assessment body;
- (4) the proposer is allowed to allocate the CSM-DT class/category (b).

Explanations on the legal text

- (j) **Steps 10 and 12** : these are the results of the risk assessment in step 8 when a “large number of people are exposed to risk” :

When there is credible potential for a failure of a function of a technical system to lead typically to multiple fatalities, and possibly to the death of most of the people exposed to risk, the severity class/category (a) needs to be applied for the design of the technical system.

- (k) **Step 8’ and 12’** : these are the results of the risk assessment in step 8’ when a “very small number of people are exposed to risk” :

When there is credible potential for a failure of a function of a technical system to lead to at least one fatality, and in the worst case to the death of the entire population of the “very small number of people exposed to risk”, the severity class/category (b) needs to be applied for the design of the technical system.

- 4.4.2. Based on the arguments provided in steps 8 to 12 above, Table 6 summarises the possible cases of allocation of CSM-DT with respect to the number of persons affected by the accident (i.e. exposed to risk) and the estimated number of fatalities which is credible.

Table 6: Only possible cases of CSM-DT vs. number of (affected persons; victims).

| number of people affected by the accident (i.e. exposed to risk) estimated number of fatalities (i.e. credible potential for) | large number of people | very small number of people |
|--|--|---|
| multiple fatalities | <p><u>Case 1</u></p> <p>Class/Category (a)</p> <p>$[10^{-9} h^{-1}]$</p> | <p><u>Case 4</u></p> <p>Class/Category (b) - $[10^{-7} h^{-1}]$</p> <p>Not possible – Number of victims limited to whole number of people in the group</p> <p>A “very small number of people” affected</p> <ul style="list-style-type: none"> • typically would not be more than 5 • and probably would not be more than 3 |
| at least one fatality | <p><u>Case 2 – two mutually exclusive possibilities</u></p> <p>(a) Probably Class/Category (a) - $[10^{-9} h^{-1}]$ as the potential for fatality cannot reasonably be limited to a very small number of people but to the whole number of people in the group</p> <p>(b) Class/Category (b) - $[10^{-7} h^{-1}]$ when it can be demonstrated for particular operational conditions (e.g. train operated at low speeds, low traffic density, etc.)</p> <p>With the obligation to justify that despite a large number of people are exposed to risk there is no credible potential for multiple fatalities</p> | <p><u>Case 5</u></p> <p>Class/Category (b)</p> <p>$[10^{-7} h^{-1}]$</p> |
| limited to potential injury(ies) without occurrence of any fatality | <p><u>Case 3</u></p> <p>Out of scope of use of CSM-DT</p> | <p><u>Case 6</u></p> <p>Out of scope of use of CSM-DT</p> |

4.5. Precautions for the selection of the appropriate CSM-DT class/category

- 4.5.1. The accident category should be credible and should be the category which can typically be expected for the accident resulting from the defined hazard. The estimation of the severity of an accident caused by a failure of a function of a technical system should be based on the possible outcome of that accident. The parameter “number of people affected by the accident” does not refer to the actual number of fatalities that will result from the accident, since anyway this information is unknown at the moment of a predictive risk assessment.

Explanations on the legal text

- 4.5.2. A predictive risk assessment must disregard the good luck circumstances where the consequence of a failure of a technical system might be less severe as considered⁽¹²⁾. On the contrary, the severity class/category needs to be determined based on the assessment of the “potential or possibility” of “what could happen” in case of accident.

Although historical statistical data of accidents might be used to support the choice, the setting of the severity class/category for the considered category of accidents cannot be based just on “the actual number of fatalities” observed through this historical statistics.

When statistical data is used as input to risk assessment, the adequacy of this data to the system under assessment needs to be verified. Indeed, often the required information (i.e. data, causal connections as well as interrelations or interactions between the constituents of the system, ... standing behind the statistical data) is not fully available or not known. Therefore expert judgement is an indispensable tool for using the statistical data carefully in the risk assessment process. When reliable/dependable data does not exist, the **expert judgement**⁽¹³⁾ is the only approach to reaching an informed judgement of the severity class/category to allocate.

Annex 1 presents the railway experience developed by the sector in the last years in respect of the choice of severity classes.

- 4.5.3. In the case that a failure of a function of a technical system could lead to different severity classes/categories of accidents, the “more stringent” or “more demanding” CSM-DT should be applied. This is the intention of the last sentence in point 2.5.5 in the Annex of

⁽¹²⁾ *In practice, statistics show that when a failure of a technical system occurs most of the time the actual consequence and outcome is not as severe as considered in the predictive risk assessment. For example a train derailment is not necessarily catastrophic or a spurious train door opening does not systematically result with one fatality.*

⁽¹³⁾ **Expert judgement** : to make it a credible basis for risk assessment, the draft of the CENELEC prEN 50126-2:2016-10 (E) standard requires that [the text below is a quotation from that draft standard]

“... expert judgement should be made as objective as possible. This implies :

- Check/estimation should not be the opinion of a single person. Agreement among several (independent) experts and approved knowledge enhances the confidence in an assessment.
- Experts have adequate knowledge of the area in question.
- All necessary areas of expertise (which may arrive at differing classifications) should be included in the judgement.
- If the expert judgement is applied to estimate the frequency and consequences of hazards (or of accidents), a clear understanding of the categories promotes a common interpretation.
- The results of expert judgement are documented. This ensures the transparency and plausibility of the conclusions. It demonstrates the integrity and enables third parties to trace the conclusion.
- The documentation is refined if new information becomes available.

The documentation should include:

- The participants and respective areas of expertise.
- Information like references to publications, sources, assumptions, deliberately excluded aspects with justification, rationale of conclusion, etc.”

Explanations on the legal text

Regulation 2015/1136 : *“The choice ... shall result from the most credible unsafe consequence of the failure”* : refer also to point (j) in section § 4.2.2. above.

- 4.5.4. For very specific functions implemented with the use of technical systems (e.g. rolling stock and technical systems used exclusively for shunting operations), expert judgement needs to be applied for determining the applicable severity class.

The setting up of the severity class/category cannot be based on the average number of fatalities observed through historical statistics but does neither need to consider the worst case scenario that is not plausible. It can be based on the credible potential outcome of the accident.

- 4.5.5. If sufficient and trusted statistical information is available and is representative for the accidents resulting from the functional failure of the technical system, then this information can be used to support the choice of the severity class/category. It is then necessary to justify the result in each application and to trace the decisions, in order for the independent assessment body to be able to assess the results. It is important that, if statistical data are used, it covers a sufficient period of time and a statistically representative number of items of similar use (in order to prove the applicability and representativeness of this data to the case under consideration).

Statistics might be used to derive quantitative safety requirements from a reference point that is based on a CSM-DT class/category. See the examples in Annex 5, Annex 3 and Annex 4.

If statistical data is used, then expert judgement is necessary to justify its use, and in particular to justify that the statistical data is :

(a) **statistically significant**

→ *“Are there sufficient data points to be able to determine the most credible unsafe consequences?”*

(b) **with sufficient quality**

→ *“Is the data of sufficient quality and reliability? Could the data be censored?”*
Indeed data might be available only for accidents with higher consequences. For lower consequence severities of accidents statistics might not be made available.

(c) **representative of the system under consideration**

→ *“If national or international accident statistics are used, then can this data be representative of accidents resulting from functional failures of the particular technical system under consideration?”*

(d) **representative of future accidents scenarios**

→ *“Accident consequences may change over time due to changes in passenger numbers, passenger-kilometer, train-kilometer, ton-kilometer of transported freight, rolling stock crashworthiness etc.”*

If statistical data exists that does not meet the criteria (a) to (d) above, then it can still be used provided that it is supplemented with suitable expert judgment. If statistical data is used then in order for the independent assessment body to be able to assess the choice of the severity class/category, the decision making process should be fully documented.

Explanations on the legal text

- 4.5.6. It is essential to document the reasons for a decision on the severity class/category in detail, to make the allocation process traceable. All pre-conditions should be documented to allow the independent assessment body, for example, to understand the reasons why the decision has been taken.

5. APPLICATION OF CSM-DT AND USE OF BARRIERS

5.1. Level of function to which the CSM-DT is applied

- 5.1.1. When quantitative risk assessment is performed in the scope of explicit risk estimation, the CSM-DT applies to failures of functions of a technical system only if the failures can lead **directly** to the accident.
- 5.1.2. In practice, a technical function can be delivered sometimes by a combination of technical systems. To avoid the misapplication of the CSM for risk assessment, the setting up of the applicable severity class/category (i.e. of the CSM-DT class) should not be applied to a single technical system of such an architecture without considering the way the technical function is actually delivered. Examples of such cases are given in Annex 2, Annex 5, Annex 3 and Annex 4.
- 5.1.3. The CSM-DT may be applied at any functional level, if the criteria laid down in the definitions for the CSM-DT concept are fulfilled. The prerequisites are that an accident can actually result as a direct consequence of a failure of a function of the considered technical system. This limits consequently the application of CSM-DT to a few rather high level functions of the railway system.
- 5.1.4. In many railway applications there are also additional safety measures in place outside the technical system under assessment. So the CSM-DT can often not be applied to a single technical system. The CSM-DT can still be applied in this case if the technical system is defined as the overall architecture. In this case the quantitative requirement should be broken down taking into account the relevant part of its overall architecture (see Figure 7).
- 5.1.5. The cases described above are illustrated by Figure 6 to Figure 8 and further more in Annex 2, Annex 5, Annex 3 and Annex 4.

5.2. Use of barriers

- 5.2.1. If barriers, or in general additional external safety measures, are taken into account for the definition of CSM-DT, then it has to be assured that all barriers (or safety measures) are external to the technical system under assessment and that appropriate independence between the barriers is assured. Those external barriers (or safety measures) become a necessary part for the safety of the overall architecture.
- 5.2.2. The design targets in the CSM for risk assessment are harmonised quantitative requirements to be used for the design of electrical, electronic and programmable electronic technical systems within the European railway system. Safety barriers however normally depend on national circumstances, national rules, requirements and established practices. Therefore, the assessment of safety barriers is currently not harmonized across Europe. The proposer is free to include safety barriers into its risk assessment to control the identified risks, and the proposer is fully responsible for the safety of the assessed system. The use of barriers however may impact mutual recognition, as Article 15(5) of the CSM for risk assessment requires a demonstration that the system is "*used under the same functional, operational and environmental conditions as the already accepted system and that equivalent risk acceptance criteria have been applied*". The equivalence of the safety barriers used in one Member State needs thus to be demonstrated with those used in the other Member State.

Explanations on the legal text

- 5.2.3. The requirement for functional failures to lead directly to an accident also determines the level at which the design targets may be applied. In case external barriers exist to prevent the accident, the design targets may still be applicable, if the barriers are implemented by technical functions. In such a case the design targets may be applicable at a higher functional level.
- 5.2.4. As referred to in point 2.5.9 of Regulation 2015/1136, if an external barrier is implemented the proposer may use less demanding design targets for the technical system if he can demonstrate that the use of those external barriers does not reduce the overall safety level within the system definition. This is illustrated in Figure 7 and Figure 8.
- 5.2.5. External barriers should ideally be derived in consultation with the stakeholder delivering or operating the barrier. External barriers may also be of operational nature, i.e. an operator action included within a documented procedure. Operator or passenger actions which (whilst expected) are not implemented within procedures cannot be claimed as external barriers. External barriers should be identified as an "application condition" for the technical system and need to be included in the Hazard Record.
- 5.2.6. External barriers are outside the technical function under assessment. Normally the responsibility for an external barrier is not with the supplier of the technical system, but rather the operator or maintainer of the technical system. Internal barriers are part of the technical solution, and are considered in the safety analysis and demonstration of compliance with the CSM-DT of the supplier. In the risk assessment of the technical system, external barriers may be taken into account only if the conditions are clearly defined and the responsibility to control the external barriers can be allocated.
- 5.2.7. Any external barrier that has been defined during the risk assessment process needs to be documented as a "safety-relevant application condition"; it also needs to be registered in the Hazard Record of the project. For any specific application of the technical system, the validity of the barrier should be monitored, and in particular whether it is as effective as assumed in the safety-relevant application condition. The CSM for risk assessment uses also the term "safety measure". Both external and internal barriers can be viewed as safety measures.
- 5.2.8. The use of barriers is illustrated in Figure 6 to Figure 8 below.

5.3. Conditions for the use of barriers (intentional safety measures)

- 5.3.1. Barriers should be intentionally implemented in the railway system. They either reduce the frequency of occurrence of a hazard or mitigate the severity of the potential consequence of that hazard. This does not mean that the barrier is only implemented for this purpose; the barrier(s) may also serve other functional purposes as well.
- 5.3.2. So long as the barrier is part of the documented safety analysis, it needs to be part of the railway system specifications and to be monitored by the organisation responsible for the equipment or operation which implements the barrier. Consideration of barriers is allowed even though the barrier may be used outside its originally intended purpose. However, demonstration of the barrier effectiveness is necessary.

5.4. Barriers not permanently present

5.4.1. Generally external barriers should only be considered if they are permanently present. If barriers are only present under certain constraints (e.g. operating conditions or specific circumstances that cannot be controlled) then their use needs to be considered with precautions. The risk assessment should take into consideration both the effect of the presence and of the absence of the barriers in the railway system. The railway system needs to be able to achieve the required safety level also when the barrier is not present in the system.

5.5. Level of application of CSM-DT

5.5.1. Figure 6 corresponds to an example where the failure of a function of the technical system under assessment has the potential to lead directly to an accident. There is no external barrier that could prevent the accident to happen.

In this case, the CSM-DT applies immediately to the functional failure of the technical system under assessment.

5.5.2. Figure 7 corresponds to an example where the failure of a function of the technical system under assessment does not directly lead to the accident. Other external technical system(s) constitute barrier(s) that prevent(s) the only failure of the technical system under assessment to result in an accident. Only a combination of failure of the technical system under assessment and of the external barrier can lead to the accident.

In this case, it is necessary to consider a higher level function which failure has the potential to lead directly to the accident. The CSM-DT will then apply to the functional failure of that higher level function.

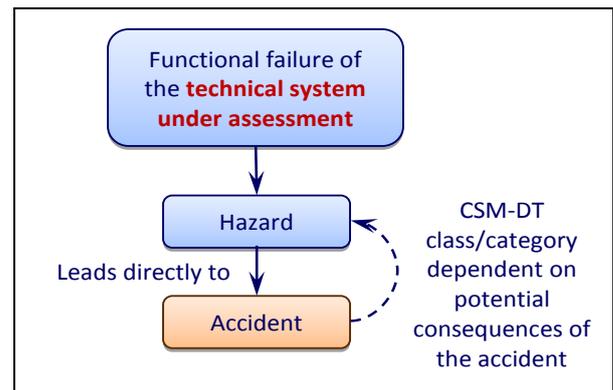


Figure 6: Failure of a function of a technical system without external barriers.

5.5.3. Figure 8 corresponds to an example where the failure of a function of the technical system under assessment does not directly lead to the accident. External non-technical barrier(s) exist (e.g. operational barriers); they prevent the failure of the technical system under assessment to result in an accident. Only a combination of failure of the technical system under assessment and of that external barrier can lead to the accident.

In this case, it is necessary to consider a higher level function which failure has the potential to lead directly to the accident. But since it is not solely composed of technical systems, the proposer can still decide to use the CSM-DT. However in this specific case, mutual recognition is not necessarily assured by the application of CSM-DT as the consideration of the non-technical system barriers may vary between Member States.

Explanations on the legal text

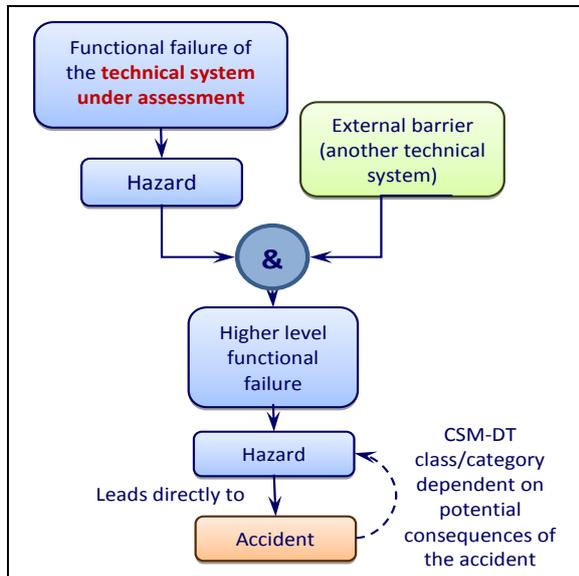


Figure 7: Failure of a function of a technical system with the presence of an external barrier through another technical system.

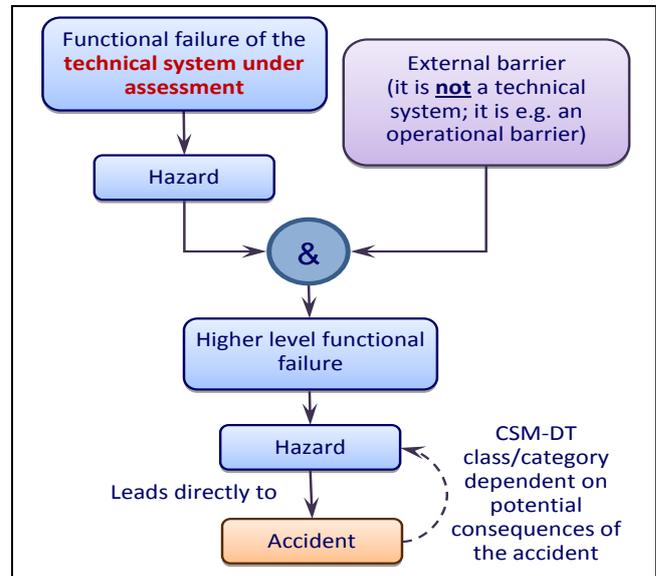


Figure 8: Failure of a function of a technical system with the presence of an external barrier through non-technical means (e.g. an operational barrier).

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

ANNEX 1: LIST OF INFORMATIVE EXAMPLES OF TECHNICAL FUNCTIONS AND THE APPLICABLE CSM-DT CLASS/CATEGORY

- A1.1. The list of examples in this annex is provided by the representative bodies (CER, EIM, UNIFE). Those examples are intended to help explain the CSM-DT concept. They have been collected from several sources, including functions of technical systems from the CCS TSI, from European Standards such as EN 15380 complemented with expert knowledge from the rail sector using brainstorming techniques.
- A1.2. The examples should be considered as informative only. They should not be applied without first analysing the specific circumstances and needs of the technical system for the project under assessment. The proposer should undertake a full functional hazard analysis, including the consequence analysis to determine the severity category for each identified hazard. If the proposer chooses to use one of the examples in the annex, then he should first demonstrate that the technical system under assessment fits with the project and has similar use and application conditions to those stated in the example.
- A1.3. The list of examples is not aiming to be exhaustive and does not limit the application of the harmonised design targets, particularly in the case of innovative functions; however, it aims to provide a broad coverage of the most common types of functions where it is most likely that the harmonised design targets will be used. The examples provided in this guide are providing guidance for the CSM-DT concept. These examples may not be used without demonstration that the example fits with the project (e.g. application condition, similar use etc.)
- A1.4. **Structure of the examples**
- The examples are structured according to the following scheme :
- (a) ID - Identifier
 - (b) Hazard arising from failures of functions of the technical system
 - (c) Function of the technical system that the design target is applied to
 - (d) Accident type caused directly by the hazard
 - (e) Direct consequence?
 - (f) Large number of persons affected?
 - (g) At least one fatality (when a very small number of people is exposed to risk)?
 - (h) Multiple fatalities (when a large number of people is exposed to risk)?
 - (i) Severity class/category assigned according to CSM-DT?
 - (j) Level to which the harmonised design target is applied to
 - (k) Full description of scenario causing Fatality/Fatalities
 - (l) Assumptions and remarks

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|--|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| 1 | Total or partial loss of braking effort, whole train | Generate a deceleration as requested by the driver or ATP system | Collision or Derailment | Y | Y | Y | Y | (a) | Train level | Losses of braking to the extent that the train will not stop before entering a section of track which could be normally be occupied by another train. Train derailment at a high speed | Shunting at low speed in a shunting area can be excluded. This case would not apply where there are controls in place to ensure that high speed collisions cannot occur, e.g. at a depot where shunting and other trains operate at low speed and there are controls to prevent trains entering inadvertently onto the main line. |
| 2 | One door being unlocked (with train crew not correctly informed of this door status) or released and opened in inappropriate areas (e.g. wrong side of train) or situations (e.g. train running) | Ensure that door is closed when required | Fall | Y | N | Y | N | (b) | Element level (per door) | One bodyside door is opened when the train is moving or when the opened door is not adjacent to a platform. | This case is addressed in Clause 4.2.5.5.8 of the Commission Regulation (EU) 1302/2014 [Loc & Pas TSI] |
| 3 | Several doors being unlocked (with train crew not correctly informed of this door | Ensure that all doors are closed when required | Fall | Y | Y | Y | Y | (a) | Train level | Scenarios where there are likely to be passengers standing next to bodyside doors and more than one bodyside door is opened when the train is moving or when the | Passengers usually standing near the external doors. This case is addressed in Clause |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|---|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | status) or released and opened in inappropriate areas (e.g. wrong side of the train) or situations (e.g. train running) for units in which some passengers stay in standing position in the door area in normal operation | | | | | | | | | opened doors are not adjacent to a platform. | 4.2.5.5.8 of the Commission Regulation (EU) 1302/2014 [Loc & Pas TSI] |
| 4 | Several doors being unlocked (with train crew not correctly informed of this door status) or released and opened in inappropriate areas (e.g. wrong side of the train) or situations (e.g. train running) for units in which passengers are not supposed to stay in the standing | Ensure that all doors are closed when required | Fall | Y | N | Y | N | (b) | Train level | Scenarios where there are not likely that passengers will standing next to bodyside doors (e.g. where there is a seat reservation system) and more than one bodyside door is opened when the train is moving or when the opened doors are not adjacent to a platform. | Passengers <u>not</u> usually standing near the external doors. This case is addressed in Clause 4.2.5.5.8 of the Commission Regulation (EU) 1302/2014 [Loc & Pas TSI] |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|--|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|--|---|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | position in the door area (long distance) | | | | | | | | | | |
| 5 | Gauge infringement due to non-retraction of external step | Ensure retraction of step when required | Impact | Y | N | Y | N | (b) | Element level (per door) | Injury to nearby passengers arising from an un-retracted step striking a platform. | Passenger stands inside the safety area near the platform edge. The injury arises from the uncontrolled detachment of the step from the train and the detached step striking a passenger. A detachment of the step is not considered to be able to trigger a catastrophic accident on another train (e.g. it will not trigger a derailment)" |
| 6 | Spurious retraction of steps | Ensure steps are not retracted when not required | Impact | Y | N | Y | N | (b) | Element level (per door) | Entrapment of a passenger between the train and the platform arising from the unrequested retraction of the door steps and the passenger not being noticed | |
| 7 | Movement of train with passenger trapped in bodyside door. | Ensure the train shall only move off when all doors are closed and locked. | Impact | Y | N | Y | N | (b) | Element level (per door) | A person that has been trapped between the doors is not noticed/does not release him/herself and the train moves off. | |
| 8 | Train moves off at station with one bodyside door open | Ensure no movement of train when doors are opened at | Fall | Y | Y | Y | N | (b) | Element level (per door) | Passengers falling from a train which moves off with one body-side doors opened. | During transfer of passengers in station. |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|---|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | | standstill | | | | | | | | | |
| 10 | Train moves off train at station with more than one bodyside door opened | Ensure no movement of train when doors are opened at standstill | Fall | Y | Y | Y | Y | (a) | Train level | Passengers falling from a train which moves off with all/more than one bodyside doors opened. | During transfer of passengers in station. |
| 11 | Uncoupling in movement | Ensure train integrity | Fall | Y | N | Y | N | (b) | Element level (per coupling) | Passengers falling from an inter-vehicle gangway due to the failure and separation of the inter-vehicle coupling. | Depends on likelihood of passengers on gangways. For example two units with electronic coupling. Note: the function "train integrity" (emergency brake if uncoupling in movement) is considered functional in this line; its failure is studied in line 12 of this table. |
| 12 | Undetected train uncoupling | Ensure decoupled parts of the train come to standstill | Collision | Y | Y | Y | Y | (a) | Train level | | Train running on the mainline |
| 13 | Switch undetected in wrong position | Ensure correct supervision of switch status | Derailment | Y | Y | Y | Y | (a) | Per element | If a switch is undetected in a wrong position, the interlocking is not aware of the wrong switch position and a train route may be set based on this wrong information. This failure may be caused by failure of the switch supervision function and is caused only by the technical function. As train | Train running on the mainline |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|-------------------------|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | | | | | | | | | | drivers rely on correct switch setting and supervision, there exists no barrier. In some lucky circumstances the accidents can be prevented e.g. if the switch is in the straight direction instead of turning, but this does not count as a barrier. The resulting accident type would be a derailment, usually of the whole train or at least a large part thereof, and on a mainline the typical accident severity would be multiple fatalities. Thus all criteria for severity class (a) are fulfilled. | |
| 14 | Wrong permissive signal aspect given | Ensure correct signal aspect is given | Derailment or collision with a mainline train | Y | Y | Y | Y | (a) | Per element | If a wrong permissive signal is given, e. g. green instead of red or an excessive speed, the train driver may follow this wrong information. This failure may be caused by failure of the signal supervision function and is caused only by the technical function. As train drivers rely on correct signal setting and supervision, there exists no barrier. In some lucky circumstances the accidents can be prevented e. g. if the signal is obviously wrong in this situation, but this does not count as a barrier. The resulting accident type could be a derailment or a collision, usually with damage of the whole train or at | Mainline signal |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|------------------------------------|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | | | | | | | | | | least a large part thereof, and on a mainline the typical accident severity would be multiple fatalities. Thus all criteria for severity class (a) are fulfilled. | |
| 15 | Wrong permissive signal aspect given in shunting area | Ensure correct signal aspect is given | Derailment or collision but not with a mainline train | Y | N | Y | N | (b) or less | Per element | The example is the same as in no 14, but the signal is a shunting signal with no possible connection to main line operation. In shunting trains are operated a low speed, say below 40 km/h and usually shunting with passengers on the train is not allowed. Thus neither the whole train is affected, usually only particular cars would derail or would be damaged and the typical accident severity is at most one fatality, e. g. of the train driver. Depending on the particular operational circumstances the severity class would be (b) (or even less). | Shunting signal |
| 16 | Movement authority not enforced by the train | Ensure correct enforcement of movement authority | Derailment or collision | Y | Y | Y | Y | (a) | Train level | Here a movement authority is not enforced on the train. The failure is usually caused by the onboard automatic train protection system only. As a consequence the train may pass a danger point and the credible accident scenario is derailment or collision. In driverless trains or trains with cab signalling only, there exists no barrier as the driver cannot check the movement | Driverless or High Speed operation |

Annex 1 : List of informative examples of technical functions and the applicable CSM-DT class/category

| A | B | C | D | E | F | G | H | I | J | K | L |
|----|--|---|---|---------------------|-----------------------------------|-----------------------|---------------------|---|--|---|--|
| ID | Hazards arising from failures of functions of the technical system | Function of the technical system that the Design Target is applied to | Accident type caused directly by the hazard | Direct consequence? | Large number of persons affected? | At least one fatality | Multiple fatalities | Severity class assigned according to CSM-DT | Level to which the Design Target is applied to | Full Description of Scenario Causing Fatality/Fatalities | Assumptions and Remarks |
| | | | | | | | | | | authority. Again on mainlines the whole train will be affected and typically results in multiple fatalities. So all criteria for severity class (a) are met. Refer also to line 1 of this table. | |
| 17 | Movement authority not enforced | Ensure correct enforcement of movement authority | Derailment or collision | N | Y | Y | Y | N.A. | Train level | The example is the same as in no 16 but here a driver has to obey signals in addition and the train protection system only has to react if the driver is making a mistake. So the hazard does not lead directly to an accident as the driver acts as an additional barrier. So the design targets from the CSM for risk assessment is not applicable in this example. | Conventional lines have barriers like the driver |

ANNEX 2 : INFORMATIVE PRACTICAL EXAMPLES ILLUSTRATING THE LEVEL WHERE CSM-DT CAN BE APPLIED AND THE USE OF EXTERNAL BARRIERS

A2.1. Example 1: Axle Counter - Level of function to which CSM-DT apply

A2.1.1. Description of the technical system under assessment :

- (a) **System definition** : an axle counter that detects the passing of a train between two points on a track section. A "counting head" (or "detection point") is installed at each end of the track section. As each train axle passes the counting head at the start of the track section, a counter increments. As the train passes a similar counting head at the end of the track section, the counter decrements. If the net count is evaluated as zero, the section is presumed to be clear for a second train;
- (b) **Considered failure** : an incorrect counting of train axles can lead to the non-detection of the presence of a train in the track section. Another failure mode is the detection of the presence of a train in the section whereas there is no train (i.e. false detection);
- (c) **Severity** : the non-detection of a train in the section has the potential to lead directly to a train collision (the false detection disturbs the traffic operation). The severity class to be considered for the non-detection function is thus "catastrophic".

A2.1.2. Consider the following function of a single axle "counting head" (assumed to be the technical system under assessment) : "**count the number of axles**". In practice, a typical axle counter uses two "counting heads". So if one "counting head" fails, then the failure is detected by the evaluation unit of the axle counter thanks to the information available from the second "counting head". Therefore the functional failure "incorrect counting of number of axles" of one single "counting head" does not lead directly to an accident; so the CSM-DT cannot be applied to the individual "counting head". CSM-DT should be applied at a higher level function (see below) which requires the simultaneous failure of the technical system under assessment (i.e. first counting head) and of the additional external barrier (i.e. of the second counting head) : see Figure 9.

A2.1.3. Consider then the function of the "whole axle counter" : "**detect the presence of a train**" inside a track section. As the axle counter consists of multiple "counting heads" and of an "evaluation unit", the failure of the high level function "detect the presence of a train" has the potential to lead directly to an accident. The CSM-DT apply thus to this functional failure (see Figure 9 which is a simplified representation of Figure 7 for this example). The accident is a direct consequence of the functional failure and at the level where the design target is applied to, there does not exist any other intentional and planned barrier that may prevent the accident.

Remark : it must be noted that the safety of the function "detect the presence of a train" depends also on the overall architecture of the whole railway system, and in particular on the logic implemented in the Interlocking. Indeed, the Interlocking might have also surveying functions of a correct sequencing of "a new track section is occupied" before releasing a previously occupied section. The presence of such a function might impact the severity class/category of the CSM-DT assigned to the function "detect the presence of a train" of the axle counter.

Annex 2 : Informative practical examples illustrating the level where CSM-DT can be applied and the use of external barriers

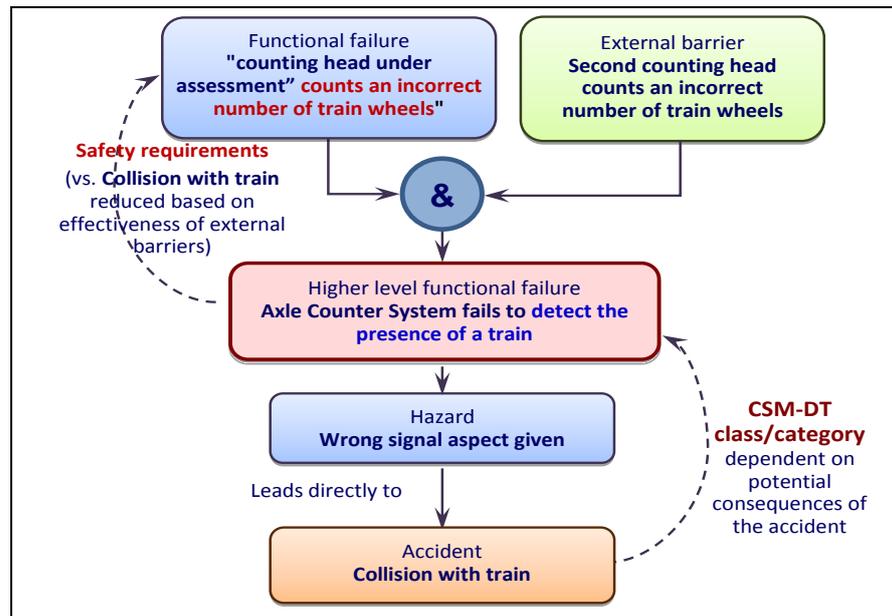


Figure 9: Level of function to which CSM-DT is applied. Simplified approach of an axle Counter with an external barrier through a technical system.

A2.2. Example 2: ATP – Use of barriers (operational measure)

A2.2.1. Description of the technical system under assessment :

- System definition** : a conventional automatic train protection system (ATP) where trackside signals are still present. The train driver is always required to respond to trackside signal information. The function of the ATP is to supervise the driver and to apply the brakes if the driver fails to slow down or to stop the train when required by the trackside signalling;
- Considered failure** : non application of brakes when needed ;
- Severity** : the non-application of brakes when needed has the potential to lead directly to a train collision or derailment. The severity class to be considered for that function is thus "catastrophic".

A2.2.2. When the lineside signalling is present, the failure of the ATP to apply the brakes does not directly cause an accident as the train driver is required operationally to respond to trackside signals. The CSM-DT does not thus need to be applied to the single failure of the ATP technical system. CSM-DT are to be applied at a higher level function which requires the simultaneous failure of both the ATP technical system under assessment and of the train driver to obey to lineside signalling (see Annex 1, example 17). The train driver can thus be considered as an "external barrier" for the ATP system under assessment : see Figure 10 which is a representation of Figure 8 for this example.

Remark : the design of the ATP system or parts of it (e.g. internal sensors or channels) can use also redundancy principles where a second sensor or channel can act as an internal barrier. As they are part of the technical system under assessment, internal barriers may be used to reduce the requirements for individual components of the internal architecture of the technical system. These considerations are nevertheless outside the scope of application of CSM-DT.

Annex 2 : Informative practical examples illustrating the level where CSM-DT can be applied and the use of external barriers

A2.2.3. Note: In the above example the actions of the train driver as defined in an operational rule may be considered as a safety measure in the context of the CSM for risk assessment process.

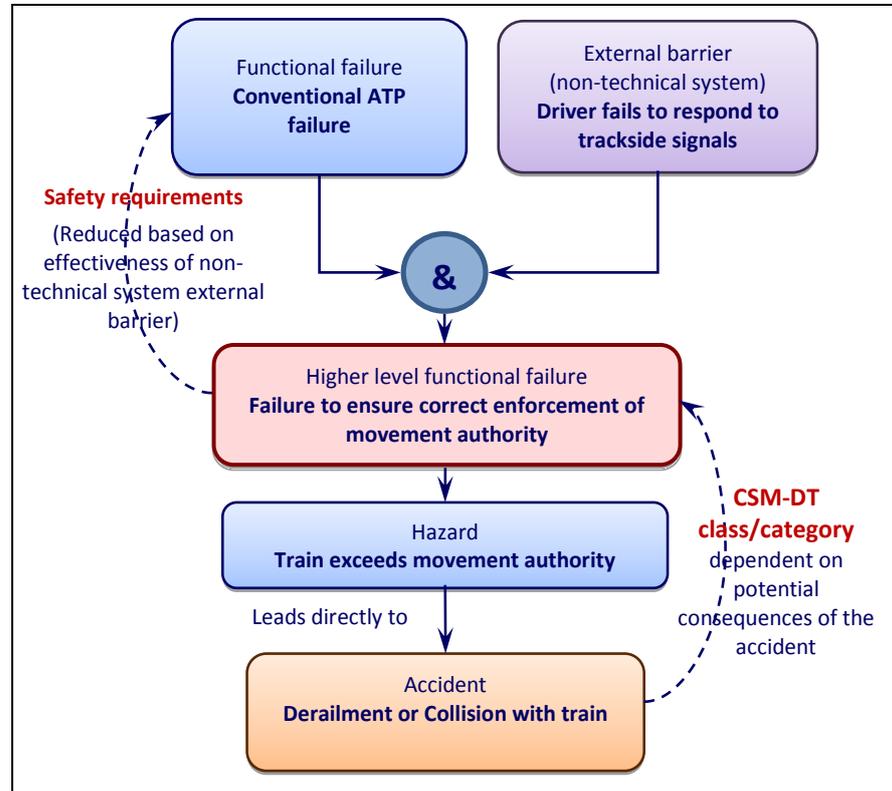


Figure 10: Conventional ATP with the use of an external non-technical system barrier.

ANNEX 3: EXAMPLE OF THE SWISS NATIONAL SAFETY AUTHORITY ON THE USE OF CSM-DT (STANDARDISED LEVEL CROSSING SYSTEM)

A3.1 Input references for this example

- [CH-NSA Ref. 1] R RTE 25931 (SN 671 512) Basic level crossing documentation, technical railway regulations RTE (in German). Swiss Public Transport Union (VöV) 2012;
- [CH-NSA Ref. 2] IEC 62551 ed 1.0: Analysis techniques for dependability - Petri net techniques. IEC 2012;
- [CH-NSA Ref. 3] EN 50126: Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999;
- [CH-NSA Ref. 4] http://www.iqst.de/?page_id=1406
- [CH-NSA Ref. 5] Slovak R.; Meuli H.: Petri Net-Based Validation of New Safety Requirements of the CSM Regulation in relation to Standardised Level Crossings in Switzerland. In Proceedings of 10th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT), Braunschweig 2014.

A3.2 (Preliminary) system definition [§ 2.1.2 in Annex I of Reg. 402/2013] ^[CSM RA]

[G 1] Existing railway system before the change :

- (a) Level crossing systems (LCS) are designed to provide a broad application range in the current European praxis. Due to this design decision, the LCS safety requirements become rather demanding. Consequently, both the LCS development and production costs are high. Nevertheless, many level crossings (LC) on secondary lines remain equipped with only passive level crossing signs like the St. Andrew cross due to the high LCS acquisition costs.
- (b) This preliminary system definition is describing the main purpose of the level crossing system which is to warn the road users about the railway traffic. An important aspect within this preliminary system definition represents the operation conditions from road side and railway traffic side points of view.

[G 2] Intended change to the railway system :

A new level crossing system should be used only for secondary lines with low or medium intensive traffic conditions (defined further). Due to its low acquisition costs it should be possible to equip a much higher number of contemporary passive level crossings.

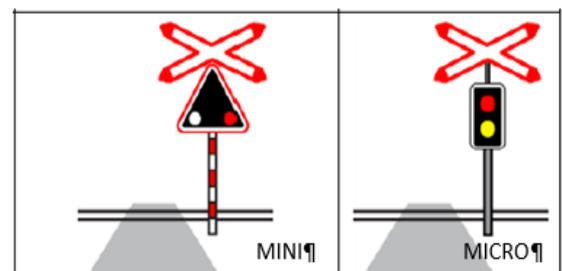


Figure 11: Schematic representation of the MINI and MICRO Level Crossings (LCS).

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

[G 3] **Differences between the existing railway system and the change under assessment :**

In order to promote the development of relatively low-cost level protection systems, **which would allow more danger points to be equipped** using limited funding, the Swiss Public Transport Union (PTU) has drawn up functional specifications for a simple, standardised type of LCS called MICRO (see Figure 11). The MICRO LCS is considered to be a simplification of the existing MINI LCS which is equipped with flashing lights.

[G 4] Table 7 lists the functions of these two types of LCS which are illustrated in Figure 11.

Table 7: Functions of the MINI and MICRO LCS.

| Function | MINI LCS | MICRO LCS |
|---|----------|-----------|
| Warn the road user against the danger on LC | X | X |
| Inform the train driver on the LC system activation | X | |
| Warn the road user against the LC system failure | | X |

[G 5] The MINI LCS and MICRO LCS differ in their application range. Table 8 summarises the main differences in their application parameters in accordance with the Swiss standard SN 671 512 [CH-NSA Ref. 1].

Table 8: Application parameters of the MINI and MICRO LCS.

| Application parameters | MINI | MICRO |
|--|-------------------|---------------------|
| Maximum density of road traffic [vehicles/h] | 6 ⁽¹⁴⁾ | 1.5 ⁽¹⁵⁾ |
| Visibility for road traffic | irrelevant | adequate |
| Maximum density of rail traffic [trains/h] | 10 | 10 |
| Maximum speed of trains [km/h] | 100 | 100 |
| Maximum number of tracks | 1 | 1 |
| Maximum hazard detection time [h] | 1 | 8 |

[G 6] An important difference between the MINI and MICRO LCS is that :

- the MINI LCS must be mandatorily applied with a trackside fitted control light or protection signal which signals a faulty level crossing to the train driver. Provided that the train driver is following the indications given by the control light or protection signal, the train driver can stop the train before it reaches the faulty level crossing;
- MICRO LCS is just equipped with a flashing yellow light that warns road users when it is defective (faulty). Therefore, in case of a fault, the responsibility for passing over the level crossing lies fully on the road user. For this reason, road users must be able to check that the track is safe to be crossed in case a MICRO LCS is installed at a level crossing.

With the application of a MICRO LCS, the possibility that a road user is misjudging his ability to safely pass over the level crossing situation while a train is approaching has to be considered as an important risk.

(14) This is equal to 8 persons equivalents/h

(15) This equal to 2 persons equivalents/h

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 7] Another important difference between the MINI and MICRO LCS is the requirement related to the **hazard detection time (HDT)**. As the MICRO LCS does not provide any interface to the train driver it is highly unlikely that a system hazard will be detected within the same time interval as for the MINI LCS. Taking into account the first application parameter listed in Table 8, the road traffic flow at the MICRO LCS must be much smaller than at the LCS MINI. Consequently, the probability of the hazard detection by a third party at the MICRO LCS must be also much smaller than at the MINI LCS. Therefore, the HDT of the MICRO LCS is set to 8 hours.

A3.3 Significance of the change [Art. 4 of Reg. 402/2013] ^[CSM RA]

- [G 1] Article 4 of Regulation 402/2013 is used to evaluate the significance of the change.

- [G 2] Article 4(1) – “**Impact on safety or is it safety related?**”

The change under assessment is safety related. In case of a faulty MICRO LCS, the train driver is not provided with any information about the fault. Consequently, the train driver is instructed to pass a MICRO LCS with the maximum allowed speed on the particular line. In the particular case that a road user is misjudging the indications given by the faulty MICRO LCS while a train is approaching, a collision of the road user and the train becomes highly probable at the LC.

- [G 3] The other criteria defined in Article 4(2) may be assessed in the following way :

- (a) “**low failure consequences?**” → no, a collision of a train with a road vehicle can result in fatalities and serious injuries;
- (b) “**low novelty?**” → no, all other types of level crossings used in Switzerland are protected with signals or control lights (see point [G 7] in section § A3.2);
- (c) “**low complexity?**” → no, a level crossing provides several system coordinated functions which contribute to avoid accidents;
- (d) “**easy monitoring?**” → no, level crossings are often operated automatically far away from railway nodes with no direct possibility of visual monitoring by the infrastructure manager;
- (e) “**high reversibility?**” → yes, the option of keeping the passive level crossing signs can be considered;
- (f) “**additionality?**” → no, as the road user expects an active MICRO LCS to be working on the same safety level as other types of level crossings.

- [G 4] **Decision** : based on the answers to all the questions mentioned above, the proposer considers the change under assessment as significant. Another proposer might decide that the change is not significant.

No matter what the decision is, whenever a change impacts the safety a risk assessment must be carried out to demonstrate that the risks arising from the change remain on an acceptable level.

A3.4 Hazard identification and classification [§ 2.2 in Annex I of Reg. 402/2013] ^[CSM-DT]

A3.4.1 Hazard identification – Use of Failure Mode and Effect Analysis (FMEA)

- [G 1] Hazards represent commonly all states of a system that may provoke dangerous situations causing highly likely fatalities or injuries. In connection with the change assessed, the

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

particular hazards are equal to all states of the MICRO LCS that provoke situations in which at the level crossing the road user is not warned about the imminent passing of a train. These include all the technical failures of the MICRO LCS functions which cause a late warning of the road user, or the premature stopping of the warning, before the train reaches, during its approaching or while passing over the level crossing.

- [G 2] For example, a functional “Failure Mode and Effect Analysis” (FMEA)⁽¹⁶⁾ analysis can be used to identify the hazards arising from the change under assessment.
- [G 3] The following tasks are done for identifying the hazards related to the MICRO LCS functions :
- (a) an FMEA table is elaborated systematically and progressively (see Table 9);
 - (b) the functions in the system definition (see section § A3.2) are assessed using generic failure modes and, where necessary, adapted to the specificities of the MICRO LCS;
 - (c) the potential consequences of the different failures modes are identified for every assessed function at the level of both the MICRO LCS and the related train.
- [G 4] The potential consequences of a collision of a train with a road vehicle were identified based on the operational conditions of the MICRO LCS listed in section § A3.2. In particular, a potential derailment of a (freight) train with high number of fatalities among passengers (potentially also involving third parties, in case of release of danger goods) is not considered for the following reasons :
- (a) compared to other existing level crossing types there is much less probability of such a kind of accident due to line operations where MICRO level crossing are used : local railway lines (single track line with maximum 10 trains/h) and very low road traffic density (1,5 road vehicle/h);
 - (b) in addition to that, this kind of extreme consequences of a level crossing accident has never been registered in any Swiss accident database;
 - (c) the consequences from a collision on a level crossing at a factory siding, where a transport of danger goods is credible, are further reduced by applying a speed limit of 10 km/h for railway tracks in factory sidings [Swiss “*Railway service regulation (FDV) 300.4 Art. 3.6.5.*”]

⁽¹⁶⁾ *The IEC 60812 standard explains how to carry out an FMEA at different indenture levels of a system.*

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

Table 9: Functional FMEA of the MICRO level crossing system.

| N° | Functional failure modes | Cause | HAZARD - Consequence at level of technical system | Consequences at train level |
|--|---|--|---|---|
| <i>For the purposes of this example, the failures of the road user based on intentional ignoring of red flashing lights are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change and human factors aspects related with misinterpretation of the yellow flashing light (visualisation of the detected failure state of level crossing system) and in case where due a hazardous system state no warning the road user is given</i> | | | | |
| 1. | Warning does not start | LCS failed | Road user is not warned against train arrival when required | Road user is not informed to stop in front of the LC and may collide with a passing train on the LC |
| 2. | Warning starts when not required | LCS failed | Spurious warning against train arrival | <ul style="list-style-type: none"> Road user is unnecessarily required to stop in front of the LC Road traffic operation is unnecessarily disturbed |
| 3. | Warning is delayed in response | LCS failed | Road user is not warned against train arrival when required | Road user is not informed on time to stop in front of the LC and may collide with a passing train on the LC |
| 4. | Warning of the road user is not terminated after passing of the train | LCS failed | Warning of the road user is not terminated after train passing | <ul style="list-style-type: none"> Road user is unnecessarily required to stop in front of the LC Road traffic operation is unnecessarily disturbed |
| 5. | Warning of the road user is terminated before the train is passing the LC | LCS failed | Road user is not warned against the train arrival when required | Road user is not informed on time to stop in front of the LC and may collide with a passing train on the LC |
| 6. | LCS is in a constant degraded state (yellow flashing light) | LCS detected a failure of one of its functions | Indication of the degraded state by yellow flashing light | Road user is informed to cross the LC on his own responsibility |
| 7. | LCS switches to a degraded state during the warning | LCS detected a failure of one of its functions | Indication of the degraded state by yellow flashing light starts immediately after the warning (red constant light) | Road user misinterprets the change of the warning from red to yellow and starts to pass the LC and thus may likely collide with a passing train |

A3.4.2 Hazard classification

- [G 1] The different hazards and potential consequences of accident(s) arising from failures of the level crossing warning functions are identified in Table 9.
- [G 2] The seven functional failure modes originating from the FMEA and presented in Table 9. are classified in the following five categories :
- failure modes 1 and 5** are resulting in the “non-warning” of the road user. Due to the lack of this information the road user is not informed about the urgent necessity to stop in front of the level crossing he intends to pass;
 - failure modes 2 and 4** are resulting in a spurious warning of road users possibly intending to pass the level crossing. The road traffic operation is then unnecessarily disturbed;

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- (c) **failure mode 3** is resulting in a too late “warning”. The lack of this information to the road user may hinder him to stop safely before the danger zone of the level crossing;
- (d) **failure mode 6** is resulting in operation of the level crossing in full responsibility of the road user;
- (e) **failure mode 7** is resulting in a situation causing a high misinterpretation potential by the road user resulting in a dangerous entering of the level crossing.

[G 3] The hazard classification presented in the previous section is presented in Table 10. It is the same table as Table 9 above where the redundant lines are masked.

Table 10: Hazard classification within the functional FMEA the MICRO level crossing system.

| N° | Functional failure modes | Cause | HAZARD - Consequence at level of technical system | Consequences at train level |
|---|---|--|---|---|
| <i>For the purposes of this example, the failures of the road driver based on intentional ignoring of red flashing lights are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change and human factors aspects related with misinterpretation of the yellow flashing light (visualisation of the detected failure state of level crossing system) and in case where due a hazardous system state no warning the road user is given.</i> | | | | |
| 1. | Warning does not start | LCS failed | Road user is not warned against train arrival when required | Road user is not informed to stop in front of the LC and may collide with a passing train on the LC |
| 2. | Warning starts when not required | LCS failed | Spurious warning against train arrival | <ul style="list-style-type: none"> • Road user is unnecessarily required to stop in front of the LC • Road traffic operation is unnecessarily disturbed |
| 3. | Warning is delayed in response | LCS failed | Road user is not warned against train arrival when required | Road user is not informed on time to stop in front of the LC and may collide with a passing train on the LC |
| 4. | | | | |
| 5. | | | | |
| 6. | LCS is in a constant degraded state (yellow flashing light) | LCS detected a failure of one of its functions | Indication of the degraded state by yellow flashing light | Road user is informed to cross the LC on his own responsibility |
| 7. | LCS switches to a degraded state during the warning | LCS detected a failure of one of its functions | Indication of the degraded state by yellow flashing light starts immediately after the warning (red constant light) | Road user misinterprets the change of the warning from red to yellow and starts to pass the LC and thus may likely collide with a passing train |

A3.5 Broadly acceptable risks ? [§ 2.2.2 and § 2.2.3. in Annex I of Reg. 402/2013] ^[CSM-DT]

[G 1] The risks associated to failure modes 2 and 6 do not result in an unsafe situation. They may thus be considered broadly acceptable from the safety point of view. In that case, they do not require the identification and implementation of any specific risk control measure. However, considering that the spurious indication of the degraded state of the level crossing might be misunderstood by the road user as an indication of an absence of the train, it requires a suitable information measure at the level crossing. Consequently, it should also be considered in the context of the overall risk assessment with an increased violation probability of the road user.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 2] The risks associated to failure modes 1 and 3 have the potential to result in an unsafe situation (collision with person or road vehicle) with fatalities. As the road user is either not informed or informed too late about the imminent passing of a train at the level crossing, he cannot stop safely in front of the level crossing. Therefore, those risks are not broadly acceptable.
- [G 3] The risk associated to failure mode 7 could lead to an increased probability of misinterpretation of the warning indication due to a change of indication to a degraded state. The red warning light followed by the yellow flashing light may be misunderstood by the road user as an indication of a clearance of the level crossing by the train. This could lead the road user to enter the danger zone at that moment which can then result in a collision (train is approaching the area of the level crossing).
- [G 4] The assessment of the risk acceptability is documented in Table 11.

Table 11: Assessment of risk acceptability within the functional FMEA of the MICRO level crossing system.

| N° | HAZARD - Consequence at level of technical system | Consequences at train level | Potential accident | Potential for at least 1 fatality |
|---|---|---|--|--|
| <i>For the purposes of this example, the failures of the road driver based on intentional ignoring of red flashing lights are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change and human factors aspects related with misinterpretation of the yellow flashing light (visualisation of the detected failure state of level crossing system) and in case where due a hazardous system state no warning the road user is given.</i> | | | | |
| 1. | Road user is not warned against train arrival when required | Road user is not informed to stop in front of the LC and may collide with a passing train on the LC | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) |
| 2. | Spurious warning against train arrival | <ul style="list-style-type: none"> Road user is unnecessarily required to stop in front of the LC Road traffic operation is unnecessarily disturbed | No – Specific operational procedures must be defined to prescribe the actions of the road user | NO (i.e. risk is broadly acceptable) |
| 3. | Road user is not warned against train arrival when required | Road user is not informed on time to stop in front of the LC and may collide with a passing train on the LC | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) |
| 4. | | | | |
| 5. | | | | |
| 6. | Indication of the degraded state by yellow flashing light | Road user is informed to cross the LC on his own responsibility | Yes - but operation in full responsibility of the road user | NO (i.e. risk is broadly acceptable) |
| 7. | Indication of the degraded state by yellow flashing light starts immediately after the warning (red constant light) | Road user misinterprets the change of the warning from red to yellow and starts to pass the LC and thus may likely collide with a passing train | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) |

A3.6 Selection of the risk acceptance principle [§ 2.1.4. in Annex I of Reg. 402/2013] ^[CSM-DT]

A3.6.1 Proposer's decision

- [G 1] Regulation 402/2013 allows the proposer to select one of among the following three risk acceptance principles for controlling the identified hazards :

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- (a) use of relevant Codes of Practice;
- (b) comparison to similar Reference Systems, and;
- (c) use of Explicit Risk Estimation.

As the change under assessment is realised by an innovative system without having the possibility to apply a Code of Practice or a comparison with a Reference System, the proposer decides to carry out an Explicit Risk Estimation, based on one of the two categories of the harmonised design targets defined in (EU) Regulation 2015/1136 [i.e. CSM-DT].

A3.6.2 Are harmonised design targets suitable for Level Crossing System?

[G 1] According to point § 2.5.5. in Annex I of Reg. 2015/1136, “*where hazards arise as a result of failures of functions of a technical system ...*” and “*where a failure has a credible potential to lead directly to ... a catastrophic ... or a critical accident*”, the most credible category of harmonised design targets (i.e. CSM-DT) can be set up as the quantitative requirement applicable for the design of the associated technical system.
In this case, “*the associated risk does not have to be reduced further if ...*” compliance with that quantitative design target is demonstrated.

[G 2] The term “directly” mentioned in the section above is defined as following in point 2.5.8.(a) of Annex I in Reg. 2015/1136 : “*The term « directly » means that the failure of the function has the potential to lead to the type of accident referred to in point 2.5.5 without the need for additional failures to occur*”.

[G 3] A single failure of the level crossing does not lead directly to a catastrophic consequence or a critical accident.

[G 4] **What are thus the conditions which have a credible potential to LEAD DIRECTLY to an accident in case of failure of the level crossing?**

Based on the (preliminary) system definition mentioned in section § Annex 4: A3.2, it can be concluded that :

IF the following two conditions are met **during the same period of time** :

- (a) the MICRO level crossing is faulty. *In concrete terms, this means that “the function warning the road user about the train approaching the level crossing is failed”;*

AND

- (b) there is a road user in the danger zone of the level crossing or approaching it

THEN

- (c) there is “*a credible potential to lead directly to ... a catastrophic ... or a critical accident*”

[G 5] Although a combination of events and failures is necessary to lead to the undesired consequence (hence an “AND” in the condition above) in practice, it is still a single functional failure of the level crossing function. Thus, the harmonised Design Targets are applicable to derive from that condition the quantitative requirements which shall be used for the design of the MICRO level crossing.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

A3.6.3 Allocation of the most credible CSM-DT category

- [G 1] The allocation of the most credible CSM-DT category is relying on the potential consequence of the accident resulting from the identified risk.
- [G 2] To help allocating the most credible CSM-DT category [i.e. either (10^{-9} h^{-1}) or (10^{-7} h^{-1})], it is necessary first to consider the number of people exposed to the particular risk and second to answer the following two questions :
- (a) Is the “*accident typically affecting a large number of people and resulting in multiple fatalities*”?
If yes, the accident category is “catastrophic” and the first CSM-DT category (10^{-9} h^{-1}) applies.
 - (b) Is the “*accident typically affecting a very small number of people and resulting in at least one fatality*”?
If yes, the accident category is “critical” and the second CSM-DT category (10^{-7} h^{-1}) applies.

- [G 3] If the answer to the two questions mentioned in the section above is not straight forward, answering the following equivalent questions might be helpful :
- (a) Is the considered accident affecting only a specific area of the train and thus exposing a risk only to the passengers located in that area? or
 - (b) Is the considered accident affecting the whole train and thus exposing to risk all train passengers or moreover to other trains or many third parties external to the railway perimeter respectively (e.g. persons living in the vicinity of the track in case of derailment)?

- [G 4] Irrespective of the set of questions used, their answers remain the same. The CSM-DT categories applicable for the different identified hazards are documented in Table 12.
- [G 5] In this example, the consequence severity of every identified risk is already considered in the hazard identification and classification (see section § A3.4, the assessment of the acceptability of risks (see section § A3.5) and the assessment of the applicability of CSM-DT (see section § A3.6).
- [G 6] The previous FMEA tables identify three different hazards with “*a credible potential to lead directly to a critical accident*” (collision of a train with road user) :
- (a) 1st hazard : road user is not warned against arrival of train when required.
 - (b) 2nd hazard : warning of the road user is terminated prematurely before the arrival of the train.
 - (c) 3rd hazard : indication of the degraded state by yellow flashing light immediately after the warning (red constant light) before the arrival of the train.

Nevertheless, as the second hazard leads to the same possible consequence as the first one, it is considered as an additional possible cause of the first hazard. Therefore, these two hazards can be analysed as a single one – **H1or2**: LCS faulty (Warning off).

- [G 7] The third hazard has the same possible consequences as the other two hazards. However the operating conditions are slightly different. Therefore this hazard will be analysed separately **H3**: LCS faulty (Warning by yellow flashing light).

**Annex 3 : Example of the Swiss NSA on the use of CSM-DT
(Standardised Level Crossing System)**

Table 12: Allocation of the most credible CSM-DT category to the hazards identified in the FMEA.

| N° | HAZARD – Consequence at level of technical system | Consequences at train level | Potential accident | Potential for at least 1 fatality | Consequence limited to a specific area of train | Associated CSM-DT |
|--|---|---|--|--|---|-------------------|
| <p><i>For the purposes of this example, the failures of the road driver based on intentional ignoring of red flashing lights are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change and human factors aspects related with misinterpretation of the yellow flashing light (visualisation of the detected failure state of level crossing system) and in case where due a hazardous system state no warning the road user is given.</i></p> | | | | | | |
| 1. | Road user is not warned against arrival of train when required | Road user is not informed to stop and prevent a collision with a train on the level crossing | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) | Yes (head of the train exposed to risk) + (road user) | $10^{-7} h^{-1}$ |
| 2. | Spurious warning against arrival of a train | <ul style="list-style-type: none"> Road user is required to stop on level crossing whereas not necessary Road traffic operation disturbed | No – Specific operational procedures must be defined to prescribe the actions of the road user | NO (i.e. risk is broadly acceptable) | Not applicable | Not applicable |
| 3. | Warning of the road user is terminated before the arrival of the train | Road user is not informed on time to stop and prevent a collision with a train on the level crossing | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) | Yes (head of the train exposed to risk) + (road user) | $10^{-7} h^{-1}$ |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | Indication of the degraded state by yellow flashing light | Road user is informed to cross the level crossing in his own responsibility | Yes - but operation in full responsibility of the road user | NO (i.e. risk is broadly acceptable) | Not applicable | Not applicable |
| 7. | Indication of the degraded state by yellow flashing light starts immediately after the warning (red constant light) before arrival of the train | Road user misinterprets the change of the warning from red to yellow and enters the level crossing with high potential of a collision with a train | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | YES (i.e. risk not broadly acceptable) | Yes (head of the train exposed to risk) + (road user) | $10^{-7} h^{-1}$ |
| <p>Remark: In practice all FMEA tables above including the present one, are one single table where columns are added to address every additional need. However for the purpose of this example, and to facilitate the reading and understanding of the analysis, only the relevant lines and columns were kept. The other ones were masked.</p> | | | | | | |

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

[G 8] In conclusion, if following the “**logical condition**” is met:

(a) there is a road user in the danger zone of the level crossing or approaching it;

AND during the same period of time⁽¹⁷⁾

(b) the function warning the road user about the danger of a train approaching the level crossing is failed; **OR** the level crossing has entered into the degraded state during the warning just before the arrival of the train,

there is “*a credible potential to lead directly to a critical accident*” ... “*typically affecting a very small number of people and resulting in at least one fatality*”

[G 9] The associated risk is acceptable if the frequency of occurrence of that logical condition mentioned in the section above is “... *demonstrated to be less than or equal to 10⁻⁷ per operating hour*”. The most credible CSM-DT category applicable to that logical condition is therefore 10⁻⁷ h⁻¹.

A3.7 Apportionment of the CSM-DT value to the different contributing parts of the logical condition [§ 2.2.5. in Annex I of Reg. 402/2013]

A3.7.1 Different sub-functions of the MICRO level crossing system [CSM-DT]

[G 1] The aim of the apportionment is to setup the safety requirements for every technical part contributing to the implementation of the functional specification of a level crossing. In the particular case of the MICRO LCS these are :

- (a) **Train recognition** – activates the road user warning when a train enters the approaching area of the level crossing;
- (b) **Road user warning** – informs the road user about the imminent approaching of a train by activating red steady lights on the MICRO LCS;
- (c) **Train clearing recognition** – deactivates the road user warning after the train has left completely the level crossing area;
- (d) **Failure recognition of all other functions** – detects a failure state of any of other technical parts of the level crossing system and leads the system to a defined degraded state;
- (e) **Fault display** – informs the road user about the faulty state of the level crossing by activating a yellow flashing light.

⁽¹⁷⁾ “During the same period of time” means that the “level crossing system has failed” AND either the failure is not yet detected OR the train driver is not informed on failure of the level crossing system

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

A3.7.2 Supporting tools – Formal Modelling using Extended Deterministic and Stochastic Petri nets (EDSPN) ^[CSM-DT]

[G 1] The apportionment of the CSM-DT is calculated on the basis of the creation of a formal model for the level crossing equipped with the MICRO LCS. The model is built up by Petri nets (see [CH-NSA Ref. 2]). The use of Petri nets is a widely spread method to describe stochastic and deterministic dynamic systems. In the present case, a class of EDSPN is used with the net elements shown in Figure 12. For the modelling and analysis, the software π -Tool was applied (see [CH-NSA Ref. 4]).

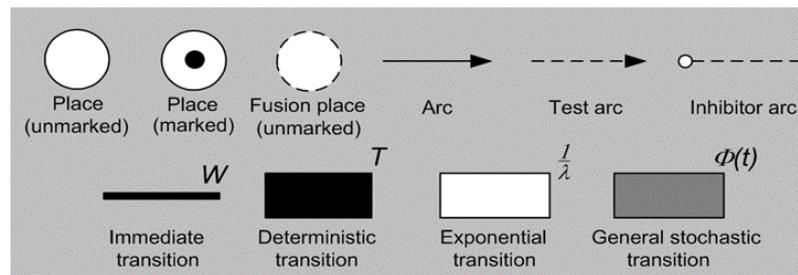


Figure 12: Elements of the class of used Petri nets.

[G 2] An event in a Petri net model can only occur if all its input places are marked with a token. The state change is untimed (transitions as narrow bars – see Figure 13). Allocating timed (deterministic or stochastic) parameters to the transitions (black or white rectangles) enables modelling of the system temporary dynamic behaviour in addition to its logical behaviour.

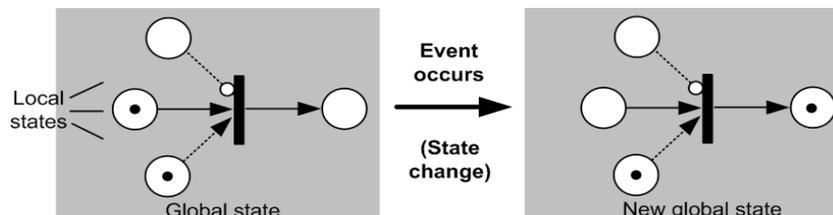


Figure 13: Dynamics in the Petri net.

[G 3] In order to enable the ergonomics and the traceability to be retained in the case of more complex situations, Petri nets offer the option of developing hierarchical and modular models. The so-called “fusion places” play a key role in this respect. They mirror existing places and can be used in several parts of the model. Fusion places always have the tokens of their original places. They link the parts of the model (modules or hierarchical refinements) together to form a complete model.

A3.7.3 Building the EDSPN model of the Level Crossing System ^[CSM-DT]

[G 1] The modelling process of a level crossing equipped with a MICRO level crossing system is based on the knowledge of the operational activities, the dangerous situations, the functions of the level crossing systems and the types of functional failures according to their identification and classification by the FMEA (see sections § A3.4.1 and § A3.4.2). The overall functions of the level crossing system (see Table 7 in section § A3.2) are made of a set of dedicated technical sub-functions (or sub-systems) needed for the implementation of the level crossing system : refer to section § A3.7.1.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 2] The EDSPN model, build in the π -Tool, allows to calculate the resulting risk at the level crossing for the road users in the form of a frequency of accidents. The EDSPN model takes into account the different functions and sub-functions of the level crossing system with their specific failure frequencies and the intensity of the road and railway traffic density. In addition to that, the probability of road users to prevent an accident in case of failure of one or more functions of the level crossing system can be modelled and evaluated by specifying the weighting of the untimed (immediate) transitions (W) (see Figure 12 and Figure 13).
- [G 3] Even if there is no other technical function of the level crossing system protecting the road user from the accident, the real operation conditions give the road vehicle driver a significant opportunity to avoid a collision with the train. This opportunity is set by law, which prescribes for MICRO level crossings the obligation to guarantee to the road users and road vehicle drivers a full visibility on the track around the level crossing in a similar way as at a passive level crossing. These satisfactory visibility conditions on the track are necessary to the road users/drivers during degraded operation of the level crossing to avoid accidents. When these particular visibility conditions cannot be guaranteed by the infrastructure, the installation of this type of MINI level crossing is not permitted legally.
- [G 4] The following two figures represents the estimated potential for risk reduction in case of accident for the hazards H1or2 (Figure 14) and the hazard H3 (Figure 15) which are defined in point [G 6] in section § A3.6.3 above.

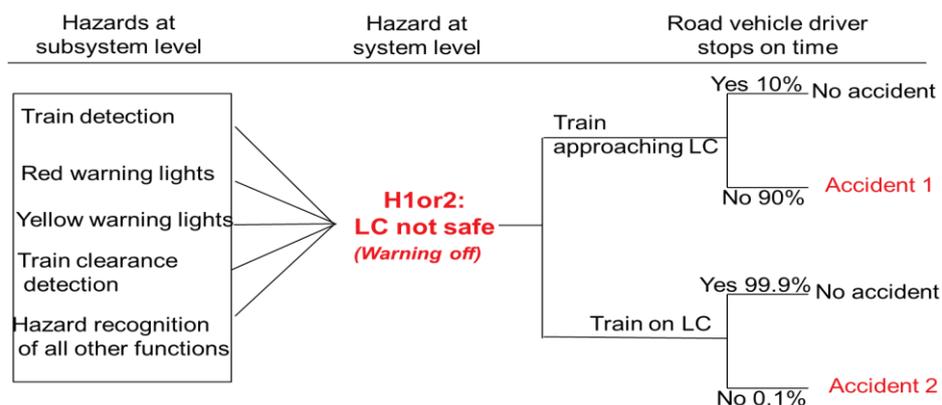


Figure 14: Risk estimation for the H1or2 hazard defined in section § A3.6.3.

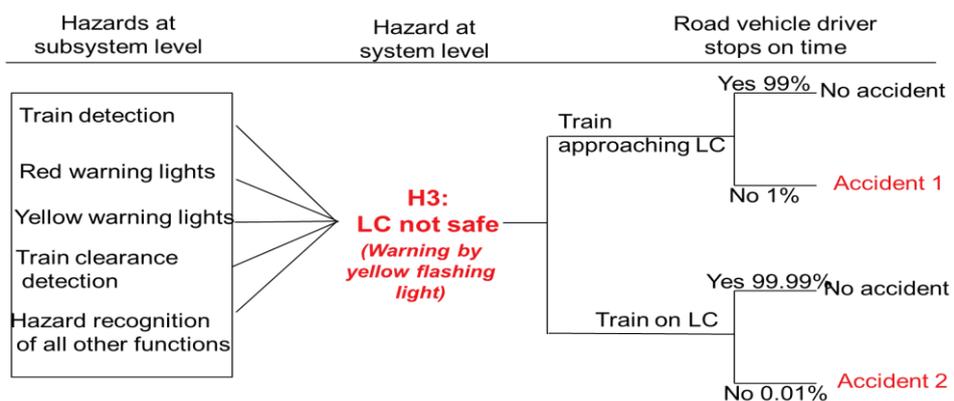


Figure 15: Risk estimation for the H3 hazard defined in section § A3.6.3.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 5] Accident 1 and Accident 2 in Figure 14) and Figure 15 correspond to two different types of collisions between a train and a road vehicle :
- Accident 1 represents a collision where the train hits the road vehicle or a road user/person in the danger zone of the level crossing;
 - Accident 2 represents a situation where (e.g. due to bad visibility conditions) a road vehicle collides with a train which is passing or standing on the level crossing.
- [G 6] Figure 16 shows the top level of the level crossing EDSPN model, which consists of seven model parts.

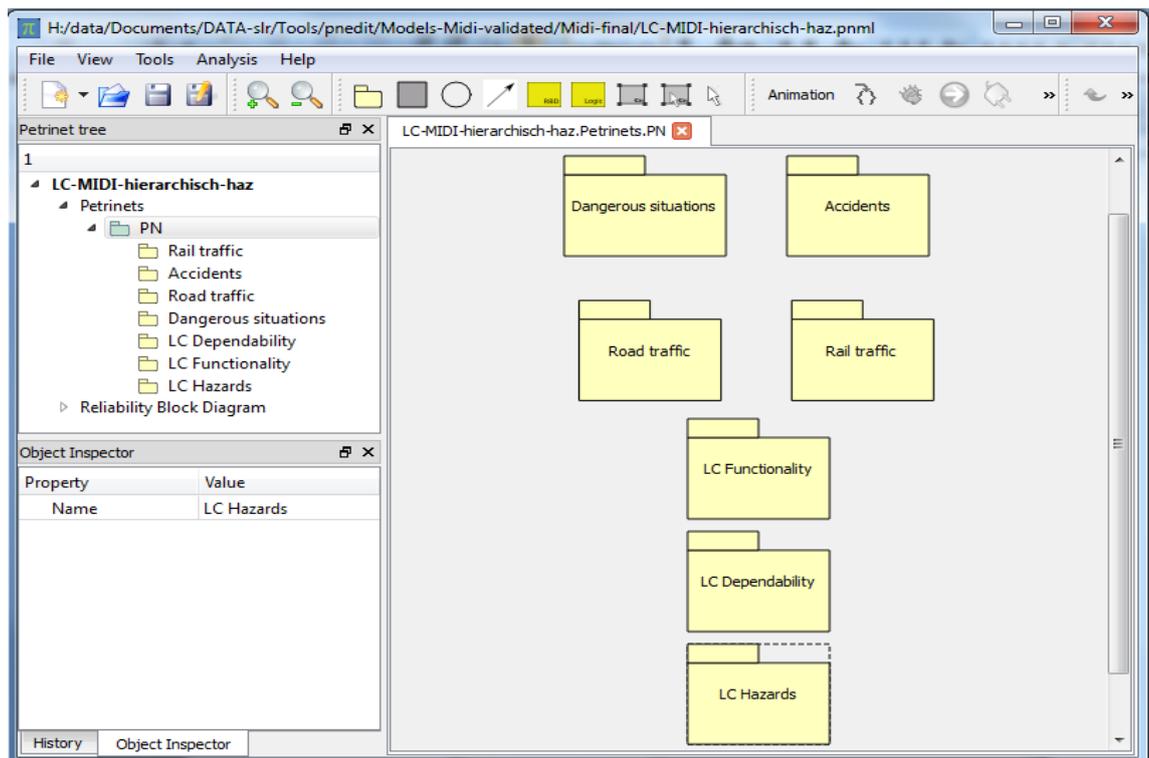


Figure 16: The modules of the MICRO level crossing model in the π -Tool.

- [G 7] Those seven parts of the model are :
- Dangerous situations : operational situations which could lead to an accident on the level crossing;
 - Accidents : types of collisions between a road vehicle and rail traffic;
 - Road traffic : traffic on the road, accident prevention and mistakes made by road users (deliberate or negligent disregard of the red light was not taken into consideration);
 - Rail traffic : train operations;
 - LC functionality : functions of the MICRO level crossing system;
 - LC dependability (dependability of the functions of the LCS) : types of hazardous failure of the system functions, together with rates of hazardous failures and disclosure of failures;

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- (g) LC hazards (dependability of the entire LCS) : hazardous failures of the entire level crossing system depending on the hazardous failures of the system functions and the current operational situation (see Figure 15).

All the different parts of the model are linked to another by shared places (fusion places).

[G 8] When the EDSPN model is built, subsequent qualitative and quantitative analyses can be carried out :

- (a) The qualitative analysis supports the modelling process by means of an animation with manual or automatic activation of the transitions (state change) and of checks for untimed cycles and deadlocks based on calculations of the state space in the form of a reachability graph. This significantly reduces the work involved in verifying and validating the model. The animation of the model dynamics in particular allows technical experts without an in-depth knowledge of Petri nets to take part directly in the validation process;
- (b) Using a quantitative model analysis, the Petri net π -Tool calculates the rates for all the transitions in the model. For all the places the tool calculates the probability of a steady system state occurring (steady state analysis).

A3.7.4 Analysing the safety integrity of the entire Level Crossing System ^[CSM RA]

[G 1] The analysis of the accident frequency in relation to the hazard rate of the entire level crossing system is presented in Figure 17. It confirms the correct choice of the design target CSM-DT of 10^{-7} per hour. As it can be seen, the resulting accident rate is at this value of the failure rate of the LCS (x-axis) lower than the limit of the individual risk of the level crossing user derived from the risk acceptance criterion MEM from the annex of the European standard EN 50126 [CH-NSA Ref. 3].

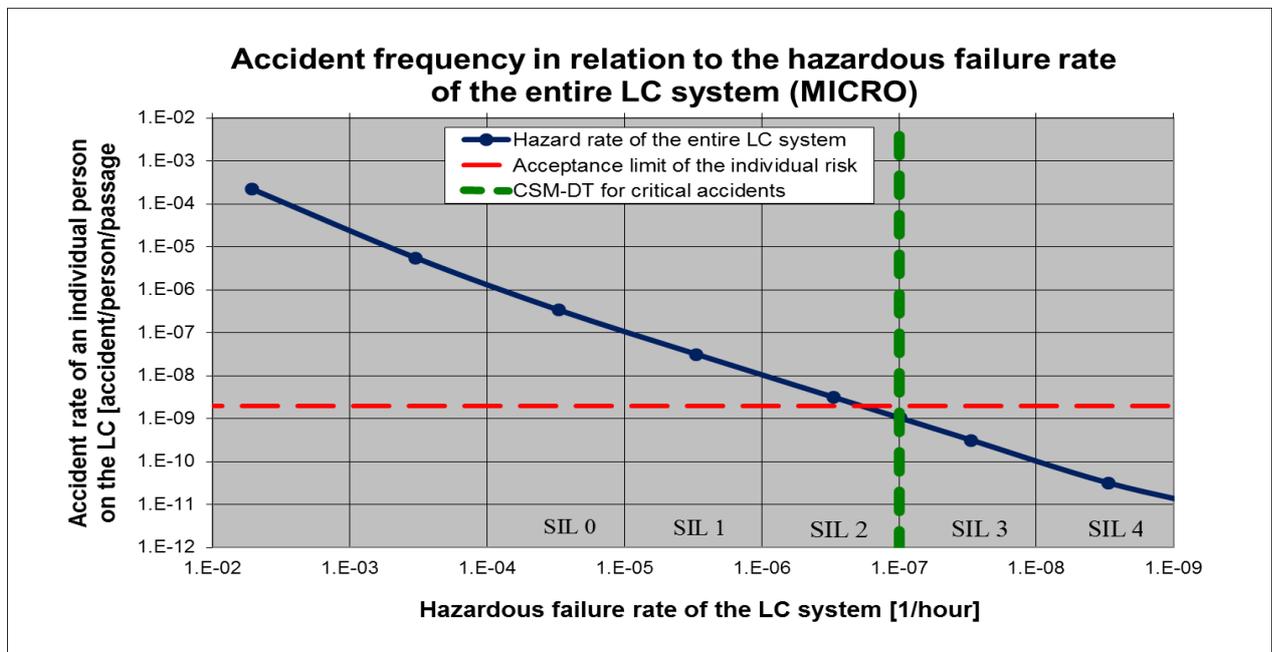


Figure 17: Dependence of the accident rate on LC from the failure rate of the LCS.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 2] An assessment of the level crossing users individual risk serves to an independent validation for correct allocation of the design targets (not necessarily required when applying CSM-DT). In the standard EN 50126 informative Annex D the maximum value of the acceptable individual risk related to a technical system is defined as $R_{iAcc} = 10^{-5}$ fatalities per person per year.
- [G 3] The general safety requirement R_{iAcc} defined in the standard EN 50126 relates to a risk exposure duration of one year. However, this duration does not correspond to the time that an individual person is exposed to the risks at level crossings. The corresponding conversion is based on an estimate of the maximum exposure time during which road users can be exposed to the risks of the technical failure of the level crossings. This estimation is calculated on the basis of the assumptions presented in Table 7.

Table 13: Assumptions about the behaviour of an individual person at the greatest danger

| Assumptions about behaviour | |
|--|------|
| Maximum duration of exposure each time a pedestrian passes over a level crossing in [s] | 9 |
| Maximum duration of exposure each time a road vehicle passes over a level crossing in [s] | 6 |
| Maximum number of times per day an individual pedestrian passes over a level crossing | 6 |
| Maximum number of times per day an individual road vehicle occupant passes over a level crossing | 8 |
| Resulting exposure times | |
| Exposure time for pedestrians on level crossings per year in [h] | 5.5 |
| Exposure time for road vehicles on level crossings per year in [h] | 4.8 |
| Total exposure time on level crossings per year in [h] | 10.3 |

- [G 4] Based on the assumptions in Table 7 :
- (a) the maximum exposure time for an individual person to the risks of a level crossing is $E_{max LC} = 10.3$ hours per year. Accordingly the following permitted individual risk per hour and per second of exposure time on the level crossing accounts for [CH-NSA Ref. 5] :

$$R_{iLCmax} = \frac{R_{iAcc}}{E_{max LC}} = \frac{10^{-5}}{10.3} = 9.7 \cdot 10^{-7} D/P/h = 2.7 \cdot 10^{-10} \text{ Fatalities / Person / second} \quad (CH-2)$$

- (b) The permitted risks of a fatality for pedestrians and occupants of road vehicles passing over a level crossing can be derived from this :

- (1) Pedestrian :

$$R_{iLCmax P} = R_{iLCmax} \cdot E_{max LC_P} = 2.7 \cdot 10^{-10} \cdot 9 = 2.4 \cdot 10^{-9} \text{ Fatalities / Person / passage} \quad (CH-3)$$

- (2) Vehicle occupant :

$$R_{iLCmax V} = R_{iLCmax} \cdot E_{max LC_V} = 2.7 \cdot 10^{-10} \cdot 6 = 1.6 \cdot 10^{-9} \text{ Fatalities / Person / passage} \quad (CH-4)$$

The two limits have the same order of magnitude, which means that the joint risk acceptance value R_{iLCmax} of $2 \cdot 10^{-9}$ Fatalities/Person/Passage can be used for further analysis of both groups of people.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

[G 5] Similarly to the wording in point 2.5.5. in the Annex of Regulation 2015/1136, the following severity consequence can be considered in this example : “ ... for a failure that has a typical credible potential to lead directly to an accident affecting an individual person and resulting in fatality and/or severe injury ...”. This corresponds to the typical potential severity class/category of an accident at a level crossing.

[G 6] In order to validate the proposed value of 10^{-7} per hour, the conservative assumption was made that every accident at a level crossing leads to a fatality. Therefore, the following acceptance criterion can be used for the subsequent analyses (whereby a fatality factor was deliberately not taken into consideration) :

$$R_{iLC_{max}} = 2 \cdot 10^{-9} \text{ Fatalities / Person / passage} = 2 \cdot 10^{-9} \text{ Accidents / Person / passage} \quad (CH-5)$$

The tolerable rate of level crossing accidents is visualised by the red dashed line in Figure 17.

A3.7.5 Analysis of the safety integrity of the single level crossing function ^[CSM RA]

[G 1] The EDSPN model can be further used for the apportionment of the system safety requirements on the single technical sub-functions listed in section § A3.7.1.

[G 2] For the configuration of a MICRO level crossing system, the failure of each individual sub-function is indicated visually to the users of the level crossing by illuminating the yellow light. This visual indication is thus a risk control measure of the level crossing system which prevents an accident from occurring, but it is possible for the level crossing users to misinterpret this behaviour. As a result of the very low road traffic density where this type of level crossing is used, this type of fault indication is adequate from the perspective of the operational risk. The EDSPN level crossing model includes the accidents caused by the misinterpretation of the yellow flashing light by the road user (as indicated on Figure 16).

[G 3] Figure 18 below presents the resulting accident rate in function of the hazardous failure rate of individual technical functions of the MICRO level crossing system. It assumes that all the considered technical functions have the same hazard rate.

[G 4] The analysis of the EDSPN model of the level crossing did not look in more detail at the dependence of the accident rate from different variations of hazardous failure rates of the single technical functions. It is probable that if the decisive functions were to have a safer design, the safety requirements for the other functions could be reduced.

[G 5] The small black arrows are showing the system hazard rate corresponding to a particular value of the hazard rate of the single technical function. Respecting the chosen design target of the entire level crossing system of 10^{-7} hazards per hour it can be evaluated that the hazard rate of a single technical function does not have to be higher than $3.3 \cdot 10^{-7}$ hazards per hour.

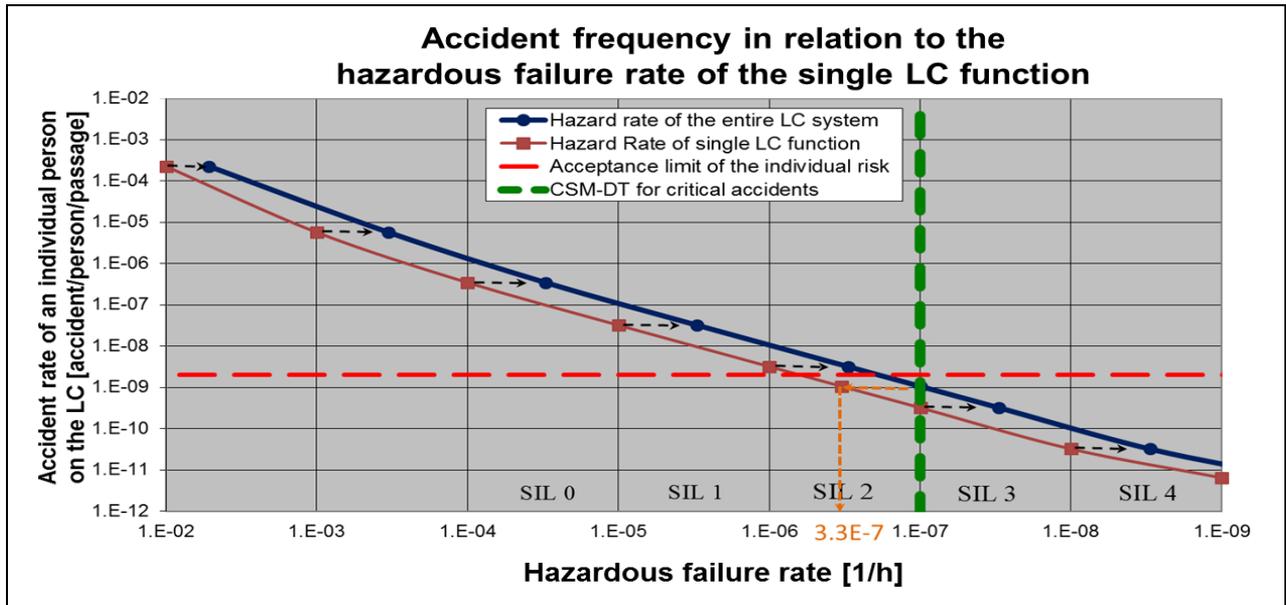


Figure 18: Dependence of the accident rate on level crossings in function of the failure rate of the single technical functions.

A3.7.6 Analysis of the influence of the hazard detection rate ^[CSM RA]

- [G 1] In contrast to the MINI level crossing with a failure disclosure time (FDT) of 1 hour, the MICRO level crossing system requires a longer FDT up to 8 hours due to low traffic flows and consequently, due to the low probability of the hazard detection by a third party. The failure disclosure time (FDT) of both systems is included in the EDSPN dependability models of each technical function of the MICRO level crossing system.
- [G 2] The dependence of the accident rate at a MICRO level crossing with respect to the failure disclosure time (FDT) of its different technical functions is presented in Figure 19 below. Similarly to the assumption above concerning the hazard rate, it also assumed that all technical functions of the MICRO level crossing system have the same FDT.
- [G 3] As illustrated in Figure 19, the influence of the failure disclosure time on the system hazard rate is only significant when the level crossing hazard rate is higher than 10^{-5} hazards per hour (horizontal dashed line towards left of the measurement point for increasing failure disclosure time). This influence is not relevant for systems with the required design target of 10^{-7} per hour. Nevertheless, Figure 19 indicates that the FDT does influence the accident rate on the level crossing (vertical shift upwards of the measurement point). This takes into account the consequence of a possible misinterpretation of the yellow flashing light (indicating degraded system state) by the road user.
- [G 4] As already shown in Figure 17 for a system hazard rate of 10^{-7} per hour (CSM-DT), even with a failure detection time (FDT) of 8 hours, the resulting accident rate lies below the acceptable accident rate derived from the criterion MEM for the individual risk. Nevertheless a further prolongation of the FDT (one day and more) would be unacceptable based on that criterion.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

- [G 5] If the failure detection time (FDT) over one day cannot be prevented by the level crossing operational means it would be necessary to require a lower system hazard rate than 10^{-7} per hour.
- [G 6] On the contrary, Figure 19 shows that if the failure detection time (FDT) is reduced to 1 hour, there is a direct positive impact on the level crossing accident rate; it is reduced more or less by factor 6.

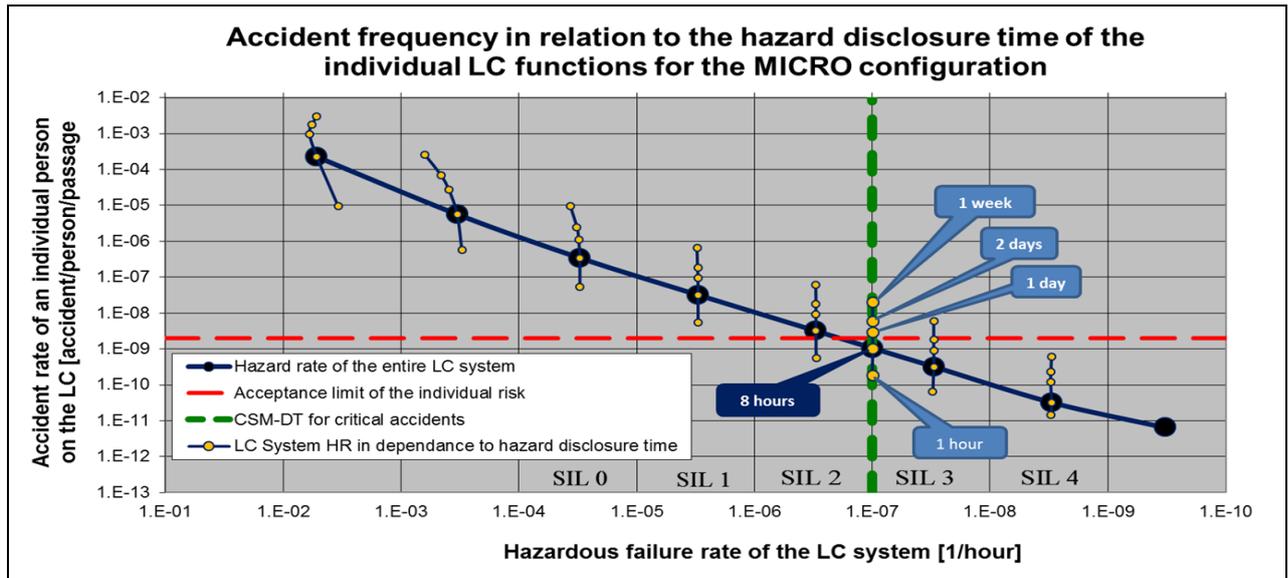


Figure 19: Dependence of the accident rate at a MICRO level crossing in function of the failure disclosure time (FDT) of its different technical functions.

A3.7.7 Setting up the safety requirements for the MICRO Level Crossing System ^[CSM-DT]

- [G 1] The risk assessment presented above sets up a quantitative safety requirement of at least 10^{-7} hazards/h for the MICRO level crossing system based on the chosen design target. With the use of the EDSPN models presented in section A3.7.3 it is possible to identify the hazard rates of the main technical functions allowing to meet the required safety requirement on the system level.
- [G 2] Taking into account the different sub-functions of the MICRO level crossing system (refer to section § A3.7.1), Table 14 gives one possible apportionment of the system safety requirement with the assumption that a failure detection time (FDT) of at maximum 8 h can be guaranteed for all the MICRO level crossing system functions. The same quantitative requirement is allocated to every sub-function.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

Table 14: Example 1 of a possible apportionment of the overall safety requirement down to the different sub-functions of the MICRO level crossing system.

| Technical system function | Tolerable hazard rate |
|---|-------------------------------------|
| Train recognition | $3.3 \times 10^{-7} \text{ h}^{-1}$ |
| Warning lights | $3.3 \times 10^{-7} \text{ h}^{-1}$ |
| Train clearing recognition | $3.3 \times 10^{-7} \text{ h}^{-1}$ |
| Fault display (Yellow flashing light) | $3.3 \times 10^{-7} \text{ h}^{-1}$ |
| Hazard recognition of all other functions | $3.3 \times 10^{-7} \text{ h}^{-1}$ |

[G 3] The EDSPN model can be used for verifying another possible apportionment of the design target of the entire system down to the hazard rates of the individual single sub-functions of the system. Table 15 shows such an example of an alternative apportionment where two sub-functions shall achieve a lower failure rate of 10^{-8} per hour.

Table 15: Example 2 of a possible apportionment of the overall safety requirement down to the different sub-functions of the MICRO level crossing system.

| Technical system function | Tolerable hazard rate |
|---|-----------------------------------|
| Train recognition | $1 \times 10^{-8} \text{ h}^{-1}$ |
| Warning lights | $1 \times 10^{-8} \text{ h}^{-1}$ |
| Train clearing recognition | $1 \times 10^{-6} \text{ h}^{-1}$ |
| Fault display (Yellow flashing light) | $1 \times 10^{-6} \text{ h}^{-1}$ |
| Hazard recognition of all other functions | $1 \times 10^{-6} \text{ h}^{-1}$ |

A3.7.8 Final decision on the (safety) requirements for the MICRO level crossing system ^[CSM-DT]

[G 1] Several alternative technical options and sets of safety requirements, with corresponding acceptable failure detection times, are analysed in the previous sections. The final proposer's decision on which technical solution to use, and thus on the necessary accompanying maintenance activities at defined intervals, needs to be taken based on a balance between the following considerations :

- the cost of the level crossing. The higher the quantitative safety requirement is, the more expensive the technical equipment is;
- the local geographic and operational conditions;
- the frequency, testability and maintenance costs of the level crossing system;
- the availability of the level crossing system and the acceptability of the new operational rules for both the road users and train drivers in case of a degraded state of the level crossing system.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

A3.8 Hazard Log/Record [§ 4 in Annex I of Reg. 402/2013] ^[CSM RA]

- [G 1] Point 4 in Annex I of Regulation 402/2013 requires the creation of a Hazard Record (some risk assessment and risk management literature uses the “Hazard Log” terminology).
- [G 2] The proposer will use the Hazard Record from the preliminary risk assessment phase, through the design and implementation, until the acceptance of the system under assessment.
- [G 3] There is no mandatory format for the Hazard Record. The proposer is free to define its own format/template, based on the project needs. The least information to be registered in the Hazard Record is defined in point 4.1.2 in Annex I of Regulation 402/2013.
- [G 4] An example of a Hazard Record is shown in Table 16 above. It contains the safety requirements identified in the risk assessment, including the quantitative safety requirements to be applied by the manufacturer for the design of the level crossing system (i.e. technical system under assessment).

A3.9 Conclusions ^[CSM-DT]

- [G 1] The predictive risk assessment demonstrates that the occurrence of the hazard (i.e. “*Level crossing system failed*”) is acceptable if the following risk control measures are put in place :
- (a) the safety requirements set out in section § A3.7.7 are used for the design of the level crossing system (i.e. technical system under assessment).
The quantitative requirements are based on the most credible category of harmonised design targets (i.e. CSM-DT), in case of failure of the road user warning function.
 - (b) the sight condition of the road user on the track will be kept free;
 - (c) the road user is adequately informed on the meaning of the yellow flashing light indicating the degraded state of the level crossing system and the transfer of the full responsibility for crossing the track on himself;
 - (d) the level crossing system is safely integrated within the railway infrastructure providing automatically information on his degraded state to the infrastructure manager.
- [G 2] Those safety requirements are registered in the Hazard Record in Table 16.

Annex 3 : Example of the Swiss NSA on the use of CSM-DT (Standardised Level Crossing System)

Table 16: Example of Hazard Record for the Swiss example of a MICRO level crossing system. ^[CSM RA]

| N° HZD | Origin | HAZARD – Consequence at level of technical system | Consequences at train level | Potential accident | Cause | Actor in charge | Risk control measure | Used risk acceptance principle | Exported | Status |
|---|----------------------|--|--|--|--|-----------------|---|---|----------|--------|
| <p>Limitations of risk assessment : For the purposes of this example, the failures of the road driver based on intentional ignoring of red flashing lights are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change and human factors aspects related with misinterpretation of the yellow flashing light (visualisation of the detected failure state of level crossing system) and in case where due a hazardous system state no warning the road user is given.</p> | | | | | | | | | | |
| <p>Assumptions for the risk assessment of the MICRO level crossing :</p> <p>(a) rail traffic density : 10 trains per hour; (b) road traffic density : 1.5 vehicles per hour or an equivalence of 2 pedestrians per hour</p> | | | | | | | | | | |
| 1. | Line 1-5 of Table 11 | Road user is not warned about the arrival of train when required | Road user is not informed to stop and prevent a collision with a train on the level crossing | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | Level crossing system failed | Manufac turer | <ul style="list-style-type: none"> Quantitative safety requirements set out in section A3.7.7 depending on selected option among Table 14 and Table 15 | • Explicit risk estimation | YES | Open |
| | | | | | | IM | <ul style="list-style-type: none"> Keeping full visibility on the track around the level crossing for road users to minimise negative consequences of the hazard Guarantee the maximal hazard disclosure time | <ul style="list-style-type: none"> Explicit risk estimation SMS rules (CoP) | NO | Open |
| | | | | | | RU | Sensibilisation of the train drivers for the reporting of any incorrect functioning of the level crossing system | SMS rules (CoP) | YES | Open |
| 2. | Line 6-7 of Table 11 | Indication of the degraded state by yellow flashing light | Road user is informed to cross the level crossing in his own responsibility | <ul style="list-style-type: none"> Collision train with road vehicle Collision train with person | Level crossing system detected a failure of one of his functions | Manufac turer | Level Crossing System must inform the IM on his degraded state | • Explicit risk estimation | YES | Open |
| | | | | | | IM | <ul style="list-style-type: none"> Keeping free sight on track for road users to minimise negative consequences of the hazard Suitable information of road driver about the meaning of the yellow flashing lights especially (indicating the responsibility of the road user) If the free sight on the track cannot be guaranteed, additional measures have to be implemented (e.g. the use of the level crossing should be prohibited to the road user in case of warning by yellow flashing light) | • SMS rules | NO | |

ANNEX 4: EXAMPLES FROM REPRESENTATIVE BODIES ON THE USE OF CSM-DT

A4.1 Example 1 : Emergency brake control of a locomotive

A4.1.1 Introduction

[G 1] This example is focused on the application of CSM-DT. It is thus assumed that the following choices were obviously made in the previous steps of the risk assessment :

- (a) the change is significant;
- (b) the associated risk is not broadly acceptable;
- (c) the proposer has decided to use the “explicit risk estimation” risk acceptance principle.

A4.1.2 Preliminary System Definition ^[CSM RA]

A4.1.2.1 Generic description

[G 1] The function under assessment is “carry out emergency braking”.

[G 2] The purpose of this function is to stop the train with maximum pneumatic braking performance when triggered either :

- (a) manually by the driver :
 - (1) through the position “emergency braking” of the braking actuator, or;
 - (2) through one of the red punch buttons (mushroom push button) : see point (2) in section § 4.2.4.4.1 of the Annex in the Loc & Pas TSI [Regulation 1302/2014];
- (b) automatically by one of the safety equipment : see point (3) in section § 4.2.4.4.1 of the Annex in the Loc&Pas TSI [Regulation 1302/2014].

This safety equipment may monitor the driver compliance with :

- (1) the speed limitations;
- (2) the lineside signals;
- (3) etc.

When the driver does not comply with the instructions/rules applicable at the train location, the safety equipment reacts through an emergency brake application.

Examples of such safety equipment :

- (4) ERTMS/ETCS;
- (5) KVB;
- (6) TVM;
- (7) LZB/PZB;
- (8) ZUB;
- (9) etc.

[G 3] The emergency brake command is sent to all brake actuators which then trigger the braking, e.g. through the brake callipers which in turn apply pressure on the axle disk via braking pads.

Note : the longer a train is, the more brake actuators it has. Usually, there is one brake disk and calliper per axle.

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.1.2.2 Limits / scope of this study

- [G 1] This example focusses on the safety equipment only although the safety study would be similar for the driver's command also.
- [G 2] In addition to that, the following **assumptions** are made :
- (a) the train under assessment is composed of 16 brake actuators (8 bogies);
 - (b) only one single type of safety equipment is active (e.g. either ERTMS/ETCS or KVB trainborne system; both systems cannot be active at the same time;
 - (c) neither of the "safety equipment" listed above is assessed in this example;
 - (d) in particular in case of use of KVB, the study would not be purely technical, as the driver has also information independent from the KVB system. This separate information allows the driver to drive the train safely without trainborne KVB system (in France, KVB is only a "parachute" to driver's lack of attention);
 - (e) the system under assessment is a train. Consequently, only the technical systems installed inside the Rolling Stock are considered within this function. Safety equipment generally have on-board equipment and trackside equipment. Only such on-board equipment is considered in this study.

A4.1.2.3 Functional analysis

- [G 1] As represented in Figure 20, the emergency brake functionality is composed of the following three sub-functions :
- (a) provide the emergency brake command from a safety equipment (e.g. speed control, signal acknowledgment and obedience, ...);
 - (b) transmit the command to the train actuators;
 - (c) actuate the braking devices (braking blocks, magnetic braking devices, etc.).



Figure 20: Emergency braking functionality.

- [G 2] These three sub-functions are analysed in further in section § A4.1.4.

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.1.3 Hazard identification and classification ^[CSM-DT]

A4.1.3.1 Hazard identification

[G 1] The hazard identification is done using a functional failure mode analysis (FMEA).

Table 17: Functional FMEA of the emergency brake.

| Function | N° | Functional failure modes | Technical local consequence (Hazard) | Consequences for train |
|-----------------|----|---|--------------------------------------|---|
| Emergency brake | 1. | Does not start | Emergency brake not issued | No braking |
| | 2. | Starts when not asked to | Inopportune emergency brake | Train is stopped, operation is hindered |
| | 3. | Does not stop when asked to | Emergency brake stays active | Train is stopped, operation is hindered |
| | 4. | Stops when not asked to | Incomplete emergency brake | Incomplete braking (braking distance not respected) |
| | 5. | Delay in response | Delay in emergency braking | Braking distance not respected |
| | 6. | Degraded output (e.g. wrong output value) | Partial braking command | Braking distance not respected |

A4.1.3.2 Hazard classification

[G 1] The hazards identified in Table 17 are listed and the potential consequences of the accident(s) that can arise from of a failure of the technical system are assessed.

[G 2] The appropriate CSM-DT class/category is then chosen, using the identified potential accident.

Table 18: Hazard classification within the functional FMEA of the emergency brake.

| N° | Technical local consequence (Hazard) | Consequences for train | Potential accident | Potential for at least 1 fatality? | Accident limited to a specific area of the train | Associated CSM-DT |
|----|--------------------------------------|---|---|------------------------------------|--|-------------------|
| 1. | Emergency brake not issued | No braking | Collision, derailment | Yes | No (Large number of people affected) | 1,00E-09 |
| 2. | Inopportune emergency brake | Train is stopped, operation is hindered | May result in minor passenger injuries where passengers fall | No | No | NA |
| 3. | Emergency brake stays active | Train is stopped, operation is hindered | None (no safety impact, as long as no train is accepted to circulate on the line where this train is stopped) | NA | NA | NA |
| 4. | Incomplete emergency brake | Braking distance not respected | Collision, derailment | Yes | No (Large number of people affected) | 1,00E-09 |
| 5. | Delay in emergency braking | | | | | |
| 6. | Partial braking command | | | | | |

Annex 4 : Examples from representative bodies on the use of CSM-DT

- [G 3] The consequence of “braking distance not respected” may differ depending on the design, and thus could lead to a more permissive design target (if assurance is given that the achieved braking distance can never be longer than an acceptable percentage of the normal braking distance).
- [G 4] Since the technical design is not yet chosen in this example, the more demanding design target is kept for the time being.
- [G 5] Since the hazards 1, 4, 5 and 6 lead more or less to the same consequence, the example will focus only on the hazard 1 “total absence of braking” for defining the safety requirements for the “emergency braking command”.

A4.1.4 Application of the selected risk acceptance principle : “explicit risk estimation” [CSM-DT]

A4.1.4.1 Proposed solutions

- [G 1] Being still during the design phase, three different solutions are proposed. The selected risk acceptance principle is used to evaluate the adequacy of each of these proposals to the required safety target.
- [G 2] The use of explicit risk estimation helps choosing between those three proposals, based on the comparison between the associated solutions (e.g. achievable safety performance vs. other criteria such as cost, availability, heavier or lighter operational and/or maintenance procedures, etc.).
- [G 3] The following solutions are proposed :
- (a) **Solution 1** : “simple” design based on the use of one technical system
- (1) a single safety equipment receives all braking commands and transmits them to the braking actuators (e.g. a single relay, or a single programmable component, ...);
 - (2) the safety equipment is only active in the cabin occupied by the train driver,;
 - (3) the driver uses the information provided by the safety equipment to operate safely the train

This is typically the case a trainborne ERTMS/ETCS technical sub-system where SIL 4 compliance is required.

- (b) **Solution 2** : duplicated design based on the use of two technical systems
- (1) the braking commands are duplicated;
 - (2) there is a safety equipment in each cabin, both of them are active (including the one of the cabin not occupied by the train driver) and both equipment transmit the braking command;
- In practice this means that when the conditions for an emergency braking are met (e.g. in case of overspeed), the train braking actuators receive two independent emergency braking commands (i.e. one command from the safety equipment of each cabin).
- (c) **Solution 3** : “simple” design based on the use of both a technical system and the train driver
- (1) the safety equipment is active only in the cabin occupied by the train driver (i.e. identical to solution 1);

Annex 4 : Examples from representative bodies on the use of CSM-DT

- (2) however based on lineside signalling information, independently from the safety equipment the train driver can also transmit an emergency braking command. This solutions assumes thus that the task is fitted with lineside signals and that the train driver is properly trained to obey these signals.

A4.1.4.2 Quantitative RAMS inputs

- [G 1] The following components cab cause the hazard; summarises the associated failure rates and associated detection & negation (or repair) time.

Table 19: Input information for quantitative risk assessment of the emergency brake.

| N° | Component | Failure | Rate of occurrence | Source of information | D&NT ⁽¹⁸⁾ | Additional explanations on the D&NT |
|----|---|--|---|--|---------------------------------|--|
| 1. | Braking actuator | Brake pads not applied on the disk | 10^{-6} / h | Monitoring through experience on similar trains (REX) | 10 h | When a driver enters a cabin, the brake is tested, and each actuator's state is detected (both in "applied" and "not applied"). A failure will lead to the isolation of the actuator, and possibly to speed limitation (or even cancelation of the mission if too many failures) Maintenance will be carried out at the end of the day if a speed limitation is present, or immediately if the train is cancelled. |
| 2. | Q(ECH) URG | Relay blocked in "no emergency brake command" position | 10^{-7} / h | Monitoring through experience on similar trains (REX) | 10 h | When a driver enters a cabin, the brake is tested, and each actuator's state is detected (both in "applied" and "not applied"). A failure will lead to all brake actuators being detected as failed, thus the mission will be cancelled. |
| 3. | RB(IS) Q(ECH) URG | Isolating valve blocked in position "isolated" | 10^{-7} / h | Monitoring through experience on similar trains (REX) | 10 h | Maintenance will thus be carried out immediately. |
| 4. | VE-URG | Valve blocked in "no emergency brake command" position | 10^{-7} / h | Monitoring through experience on similar trains (REX) | 10 h | <i>Note: if this component is doubled, then a specific detection system is generally put in place, in which case the failure will be repaired at the end of the day.</i> |
| 5. | Safety equipment | No emergency brake command issued by the safety equipment | 10^{-9} / h | ETCS requirement used for this example | 10 h | <i>If this was not the case, the D&NT would be the preventive maintenance where this component would be tested (not only the function, but each of the redundant components individually)</i> |
| 6. | Driver (<i>in case of solution 3</i>) | The driver does not issue an emergency braking while the situation requires it | 10^{-3} <i>This is a probability, not a rate</i> | Monitoring of drivers effectiveness (e.g. number of not applied signal / number of signals passed by the driver) | Not applicable to a probability | |

- [G 2] As the train is made of 16 independent braking actuators, the failure of all actuators during the same time interval is negligible compared to the failure of the command. Applying the Formula 3 from the Appendix in section § A5.10.3 below, when taking a failure rate of an actuator of 10^{-6} h^{-1} , the actuators being tested every day (i.e. every 10 hours of real operation), the failure rate of the failure of all actuators would be :

⁽¹⁸⁾ D&NT designates the "Detection plus Negation Time", i.e. the time necessary for detecting the failure of the defective component, repairing and testing before returning it to service.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

$$(10^{-6} \times 10)^{16} \times \left(\frac{16}{10}\right) = 1,6 \cdot 10^{-75} \text{ h}^{-1}$$

[G 3] Therefore, further risk assessment can focus only the “emergency braking command”, using for example the fault tree methodology.

A4.1.4.3 Solution 1

[G 1] As explained in section § A4.1.4.1, with solution 1 the emergency braking command is provided by one single technical safety equipment. The command is then transmitted to the brake actuators via the emergency braking components :

- (a) one of the active technical safety equipment sends an emergency brake command;
- (b) the pneumatic Q(ECH)URG relay receives that command and transmits it to the VE-URG electro-valve;
- (c) the VE-URG electro-valve transforms this electric command into a pneumatic depression, except if RB(IS)Q(ECH)URG is in the “isolated” position as required by point (1) of clause § 4.2.4.10 of Loc&Pas TSI [Regulation 1302/2014].
- (d) the pneumatic depression (spread over the whole train) triggers then the brake actuators.

[G 2] Failures of such a technical solution can be modelled as represented on the FTA in Figure 21, using the input data from Table 19.

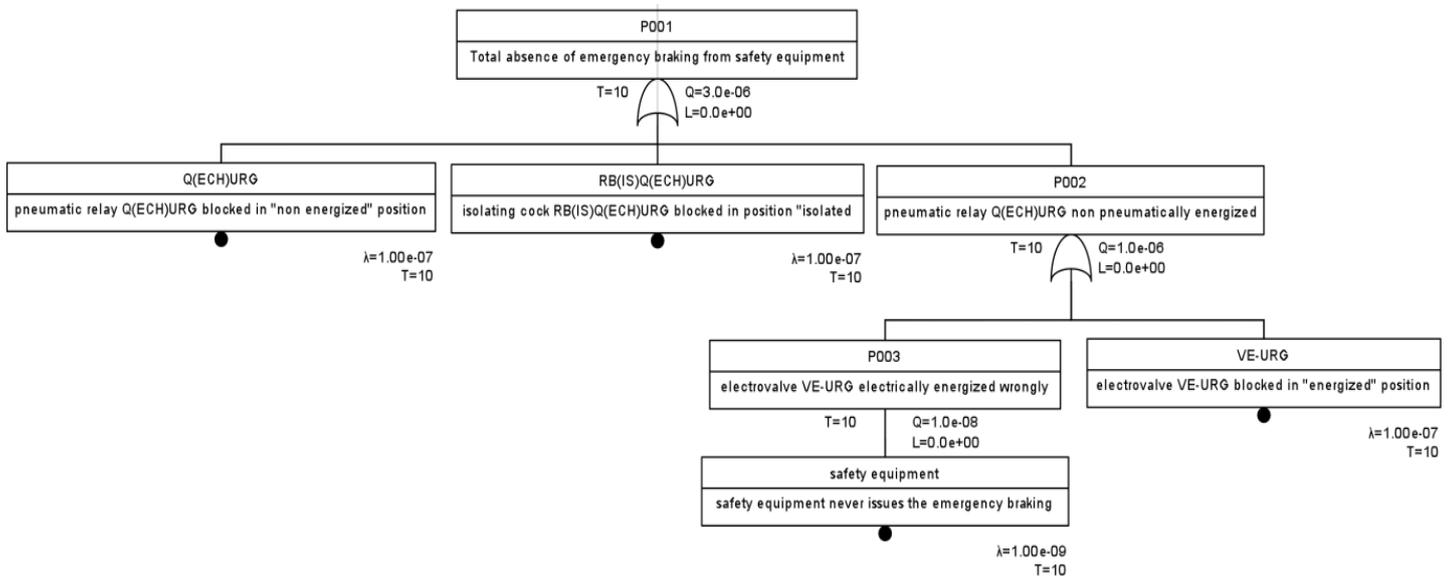


Figure 21: FTA of solution 1 for the emergency braking command.

[G 3] The failure rate estimated for the top event (total absence of emergency brake command from the technical safety equipment) is $3,0 \cdot 10^{-6} \text{ h}^{-1}$. Therefore solution 1 cannot be used as it does not permit to achieve the harmonised design target setup in Table 18 ($1,0 \cdot 10^{-9} \text{ h}^{-1}$). Several single failures could cause the identified hazard and thus result in the absence of command of emergency brake. This solution would thus require a re-design of the technical system in order the reduce further the resulting risk.

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.1.4.4 Solution 2

[G 1] Solution 2 is similar to solution 1 with the exception that all command components are duplicated. The pneumatic depression is triggered by two independent commands, one from every cabin. This is taken into account in the FTA in Figure 22.

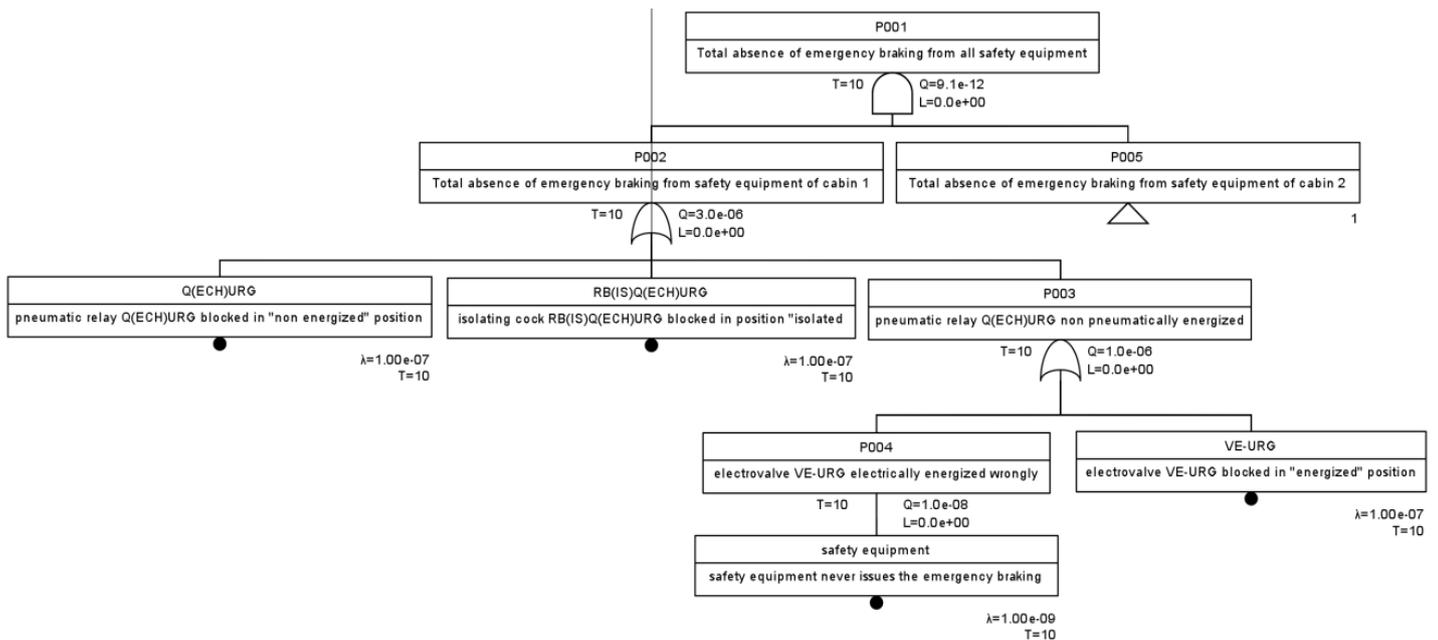


Figure 22: FTA of solution 2 for the emergency braking command.

[G 2] With solution 2, the technical safety equipment is active in each cabin. This permit would permit the use of a less demanding safety requirement for the safety equipment of each cabin. With the same input information as solution 1, the estimated failure rate for the top event (total absence of emergency brake command due to a simultaneous failure of the technical safety equipment in both cabins) would be $9,1 \cdot 10^{-12} \text{ h}^{-1}$. The harmonised design target setup in Table 18 ($1,0 \cdot 10^{-9} \text{ h}^{-1}$) would thus be achieved. However, in practice it is not common to leave the technical safety equipment active in the non-occupied cabin.

A4.1.4.5 Solution 3

[G 1] With solution 3, based on lineside signalling information, the train driver can also transmit an emergency braking command independently from the safety equipment (see section § A4.1.4.1).

Note : operation on high speed lines does not allow the use of solution 3, as the driver is not able to obey lineside signals in a sufficiently low reaction time.

[G 2] For this option, it is assumed that the probability that the driver does not trigger the emergency braking command, whereas it is needed based on lineside signalling, is 1/1000 (probability of 10^{-3}).

Annex 4 : Examples from representative bodies on the use of CSM-DT

- [G 3] With solution 3, the technical safety equipment is active only in the cabin occupied by the train driver. The safety equipment is considered as “parachute” of the driver. So, the emergency braking should primarily be commanded by the driver. The harmonised design target setup in Table 18 ($1,0 \cdot 10^{-9} \text{ h}^{-1}$) is reached (i.e. estimated failure rate of $4.0 \cdot 10^{-10} \text{ h}^{-1}$) under the following conditions :
- the train driver is provide with the relevant information independently from the technical safety equipment (e.g. through lineside signalling) so that he can order the emergency braking independently from the safety equipment;
 - the train speed limit allows for this information to be treated by the train driver (e.g. on high speed lines, the use of only lineside signalling is not sufficient to operate safely trains);
 - the train driver is given an appropriate training to permit him operating trains based on lineside signalling information (so, he knows well when to push on the emergency brake button).
- [G 4] **Note:** since with solution 3 the hazard is not a result of a failure of a “purely technical” function, the application of the CSM-DT is no longer “automatic”. The “reliability” of the driver to obey correctly the lineside signalling could be different from one country to another one. It would thus have an impact on the mutual recognition of the results of the risk assessment.

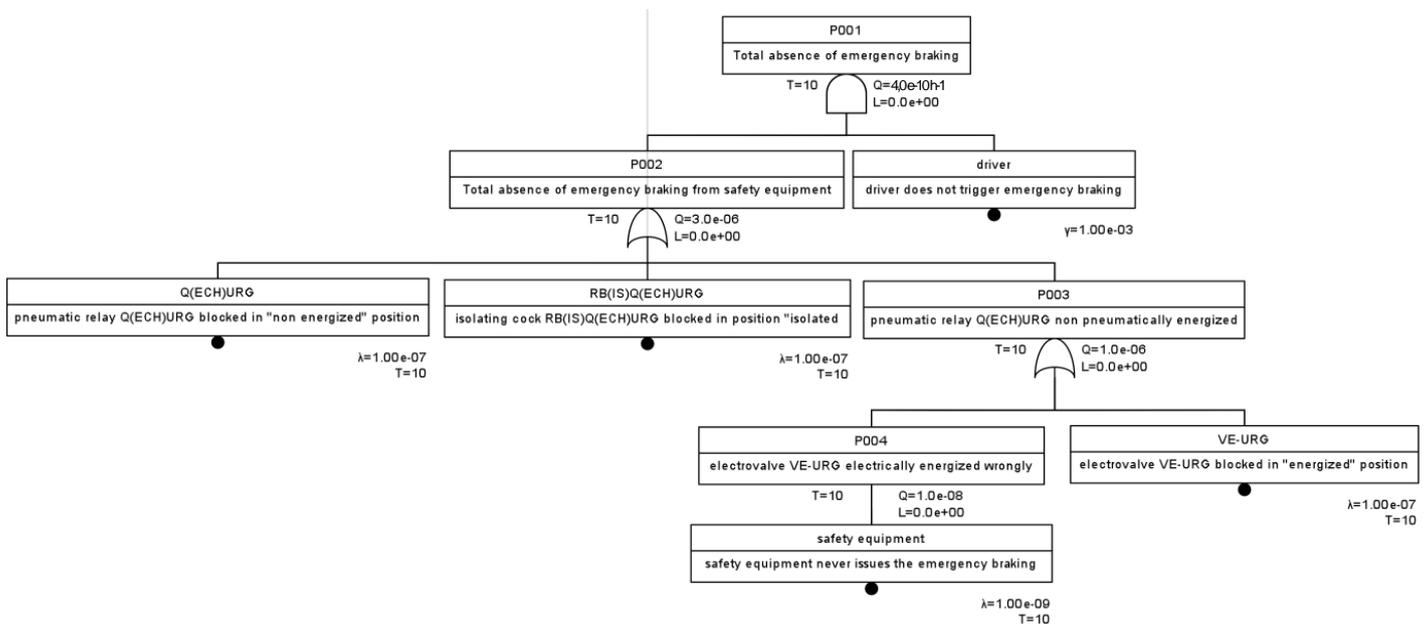


Figure 23: FTA of solution 3 for the emergency braking command.

A4.1.5 Conclusion ^[CSM-DT]

- [G 1] In order to reach the safety target setup in section § A4.1.3.2 and Table 18, two options are possible :
- if the rolling stock needs to be operated in several/many countries, solution 2 is preferable to ensure the cross acceptance of the use of a purely technical system which is compliant with a CSM-DT;

Annex 4 : Examples from representative bodies on the use of CSM-DT

- (b) if the rolling stock is operated in used in a single or a few countries where the assumed train driver reliability of 10^{-3} is agreed, solution 3 might be used.

[G 2] The operational constraints linked to this example would then be the following :

- (a) monitor during the train operation the actual failure rate of the components used in the risk assessment in order to verify the assumptions made in the risk assessment;
- (b) ensure that the train operation and maintenance is carried out according to the D&NT that was taken in the risk assessment (see Table 19);
- (c) if solution 3 is chosen :
- (1) ensure through proper recruitment and training that the train driver understands the lineside signalling he may encounter on the lines where the train is operated;
 - (2) monitor the actual train driver reliability and obedience to lineside signalling in order to verify the input information used in the risk assessment.

A4.2 Example 2 : Train door opening authorisation

A4.2.1 Introduction

[G 1] This example is focused on the application of CSM-DT. It is thus assumed that the following choices were obviously made in the previous steps of the risk assessment :

- (a) the change is significant;
- (b) the associated risk is not broadly acceptable;
- (c) the proposer has decided to use the “explicit risk estimation” risk acceptance principle.

A4.2.2 Preliminary System Definition ^[CSM RA]

A4.2.2.1 Generic description

[G 1] The function under assessment is “open/close the train doors”.

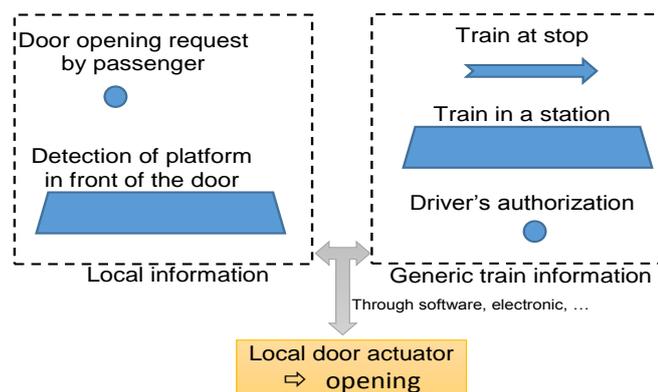


Figure 24: Example of a train door opening control system.

[G 2] The purpose of this function is to allow or forbid passengers to get onboard the train or to leave the train. The access to train is permitted at a station platform. Leaving the train is not permitted where there is no platform or when the train is in movement.

Annex 4 : Examples from representative bodies on the use of CSM-DT

- [G 3] Each train door is equipped with an actuator (e.g. electric motor). The actuator is commanded by a local door command system which receives information valid for the whole train (e.g. train speed, opening authorisation from the driver or from a train controller). Depending on the train, the door opening may occur automatically or only if a passenger issues an opening request (e.g. by pushing a button on the train door).

A4.2.2.2 Limits/scope of the study

- [G 1] The train under consideration is **not a suburban train**. Therefore it is considered that only a few people might be standing in front of the door; passengers are supposed to be sitting in other areas of the train. So, if a single train door opens while not requested to, only a small amount of passengers will be endangered.
- [G 2] The train speed information is provided by a speed measurement system (e.g. tachymeter).
- [G 3] All train generic information (train at stop, train in a station, etc.) is grouped into a common failure named “central controller”, where the failure may come from the central controller itself, or from a failure or combination of failures from the information sent to the central controller (e.g. “speed detector always sends a 0 km/h speed”).
- [G 4] The opening authorisation can be ordered by the driver or automatically [*if a technical system is installed*] provided the train is at station at a platform and it is at stop. An example of such an automatic system would be :
- (a) the train is at stop if the train speed is measured to be below 0,5 km/h;
 - (b) the train is detected to be at station at a platform : several solutions are possible :
 - (1) there is an emitter on the platform informing that the train has reached the station platform;
 - (2) the detection is on the train (e.g. a radar, a camera, GPS, etc.).
- [G 5] This example of application of CSM-DT will however cover only the case of a train passenger who is requesting the opening of the doors.
- [G 6] The system under assessment is the door system of a train. Only the technical components installed inside the rolling stock are considered in this function. The door control technical systems are generally on-board equipment, although there might be equipment on a platform (e.g. PRM zone detection). For the purpose of this example, only on-board equipment is considered.

A4.2.2.3 Functional analysis

- [G 1] The door control system is designed in the following way:

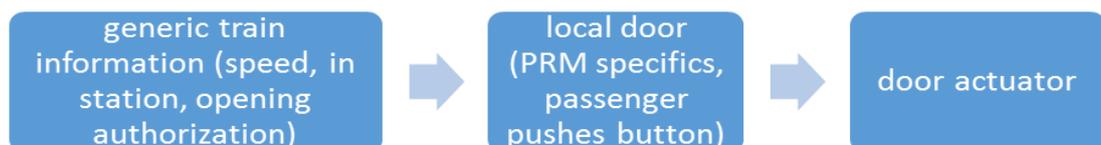


Figure 25: Door control system.

Annex 4 : Examples from representative bodies on the use of CSM-DT

[G 2] For example, the information flow for this example is the following for a door opening :

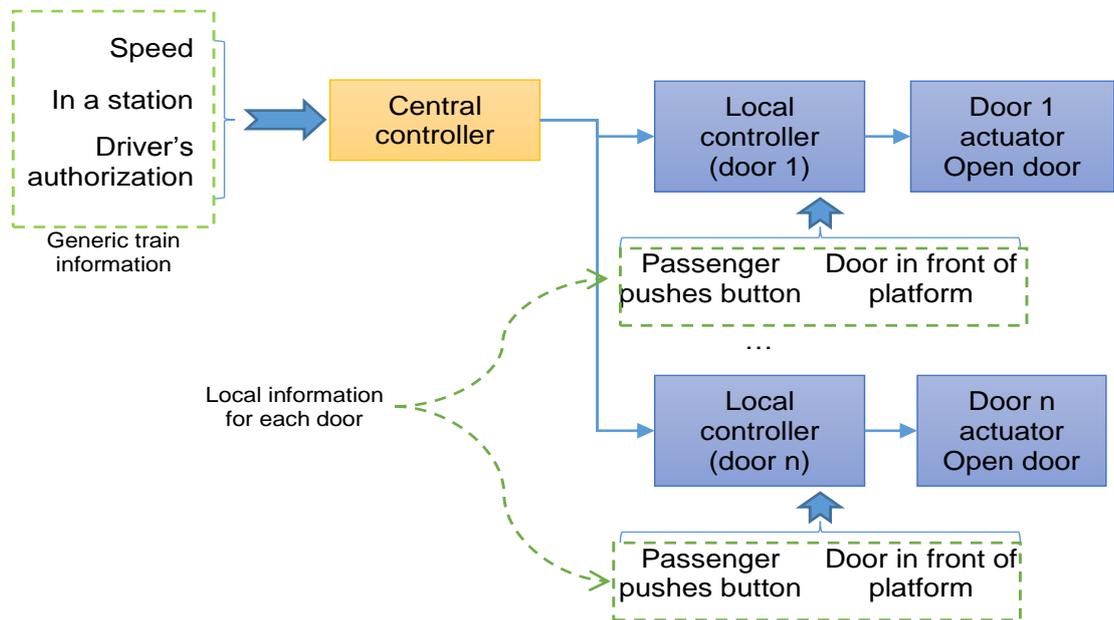


Figure 26: Flow of information for the door control system.

A4.2.3 Hazard identification and classification ^[CSM-DT]

A4.2.3.1 Hazard identification

[G 1] For the door control system, in order to ensure that all hazards are identified, both the “train door opening” and “train door closing” functions are studied. Furthermore, since the consequences may greatly differ, the following circumstances (which are not failures, and thus do not need to be quantified in the quantitative demonstration) need to be taken into account when evaluating the consequences of such functional failures :

- (a) at stop or during circulation;
- (b) a single door or more than one door are concerned.

[G 2] The hazard identification is done using a functional failure mode analysis (FMEA).

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

Table 20: Functional FMEA of the door control system.

| Function | Functional Failure modes | Technical local consequence (Hazard) | At stop | During circulation | Single door | Several / all doors | Consequences for train |
|---|---|---|---------|--------------------|-------------|--|---|
| Door opening | Does not start | Door does not open | X | NA | X | | Single door: passenger traffic is delayed, train is delayed |
| | | | X | NA | | X | Several doors / all doors: emergency evacuation hindered / impossible |
| | Starts when not asked to | Door open when not authorized | X | | X | | Single door at stop: fall of a passenger (the one leaning on the door) |
| | | | | X | X | | Single door during circulation: fall of multiple passengers (aspiration effect) |
| | | | X | X | | X | Several doors / all doors: fall of multiple passengers |
| | Does not stop when asked to | Door stays open (cannot close) | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| | Stops when not asked to | Door stops opening (incomplete opening) | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| Delay in response | Delay in door opening | X | NA | X | X | Passenger traffic is delayed, train is delayed | |
| Degraded output (e.g. wrong output value) | Door opens abruptly / too fast | X | NA | X | X | Passenger may have light injury | |
| Door closing | Does not start | Door does not close | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| | Starts when not asked to | Door closes when not asked to | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| | Does not stop when asked to | Door stays closed (cannot open) | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| | Stops when not asked to | Door stops closing (incomplete closing) | X | NA | X | X | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled |
| | Delay in response | Delay in door closing | X | NA | X | X | Passenger traffic is delayed, train is delayed |
| | Degraded output (e.g. wrong output value) | Door closes abruptly / too fast | X | NA | X | X | Passenger may have light injury |

A4.2.3.2 Hazard classification

[G 1] The hazards identified in Table 20 are listed and the potential consequences of the accident(s) that can arise from of a failure of the technical system are assessed.

[G 2] The appropriate CSM-DT class/category is then chosen in Table 21, using the identified potential accident.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

Table 21: Hazard classification in the functional FMEA of the door control system.

| N° | Technical local consequence (Hazard) | Consequences for train | Potential accident | Potential for at least 1 fatality? | Accident limited to a specific area of the train | Associated CSM-DT |
|-----|---|---|---|------------------------------------|--|-------------------|
| 1. | Door opens abruptly / too fast | Passenger may have light injury | Light injury for 1 person | No | NA | NA |
| 2. | Door closes abruptly / too fast | | | | | |
| 3. | Delay in door opening | Passenger traffic is delayed, train is delayed | None (no safety impact, only train delay) | NA | NA | NA |
| 4. | Delay in door closing | | | | | |
| 5. | Door stays open (cannot close) | Train is delayed (until the door(s) is/are condemned). If too many doors malfunction, the train will be cancelled | None (no safety impact, only train delay) | NA | NA | NA |
| 6. | Door stays closed (cannot open) | | | | | |
| 7. | Door stops opening (incomplete opening) | | | | | |
| 8. | Door stops closing (incomplete closing) | | | | | |
| 9. | Door does not close | | | | | |
| 10. | Door closes when not asked to | | | | | |
| 11. | Door does not open | Several doors / all doors: emergency evacuation hindered / impossible | Potential for multiple fatalities in case of situation requiring evacuation (e.g. fire) | Yes | No | 1,00E-09 |
| 12. | Door open when not authorized | Several doors / all doors: fall of multiple passengers | Potential for multiple fatalities | Yes | No | 1,00E-09 |
| 13. | Door open when not authorized | Single door at stop: fall of a passenger (the one leaning on the door) | Potential of fatality | Yes | Yes | 1,00E-07 |
| 14. | Door open when not authorized | Single door during circulation: fall of multiple passengers (aspiration effect) | Potential for multiple fatalities | Yes | No | 1,00E-09 |
| 15. | Door does not open | Single door: passenger traffic is delayed, train is delayed | None (no safety impact, only train delay) | NA | NA | NA |

[G 3] The hazard about the train evacuation (i.e. line 11 in Table 21) will not be studied here since it is not a direct event [there is no consequence if there is no initiating event (e.g. fire) which requires the evacuation of the train].

[G 4] As presented in the preliminary system definition in § A4.2.2, the door control system consists of a central controller and of a local controller per door. Thus, a problem concerning more than one door is more likely (including in terms of probability) to be due to a failure in the central controller rather than due to the failure of multiple local controllers.

[G 5] The hazards which will be studied can thus be regrouped as follows in Table 22 :

Annex 4 : Examples from representative bodies on the use of CSM-DT

Table 22: Hazards of the door control system that need further risk assessment.

| N° | Line N° in Table 21 | Hazard | CSM-DT |
|----|---------------------|---|----------|
| H1 | 13 | Single door opens during stop when not authorized | 1,00E-07 |
| H2 | 12 | All doors open during stop when not authorised | 1,00E-09 |
| H3 | 14 | At least one door open during circulation when not authorised | 1,00E-09 |

A4.2.4 Application of the selected risk acceptance principle : “explicit risk estimation” ^[CSM-DT]

A4.2.4.1 Assumptions

[G 1] It is considered that each controller (both local and central) contains software.

[G 2] From the applicable CSM-DT, several options exist : see below.

A4.2.4.2 Solution 1

[G 1] Each local controller receives information from the central controller, and thus commands the door opening/closing :

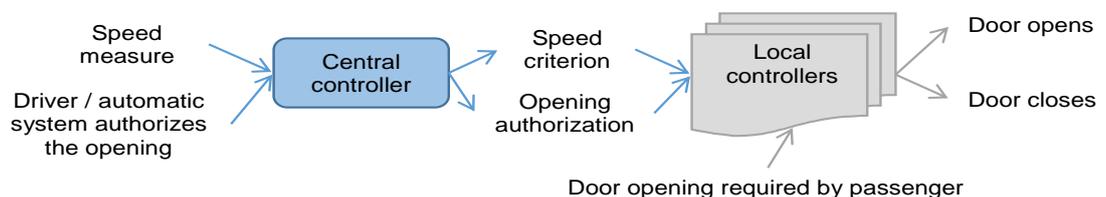


Figure 27: Door control system – Solution 1.

[G 2] The information required for the event “all doors open during circulation” is “train speed” (information sent = train is not at stop, since speed is above x km/h, e.g. 0,5 km/h).

[G 3] The information required for the event “all doors open during stop when not authorised” is “door opening authorisation given by the driver (or an independent automatic system)”.

[G 4] Due to hazard H1, the local controllers have a required design target of 10^{-7} h^{-1} .

[G 5] Due to hazards H2 and H3, the central controller has a required design target of 10^{-9} h^{-1} .

[G 6] From the design target setup for H1, it is confirmed that a failure of several local controllers is negligible compared to the failure of the central controller. Therefore, for H2 and H3, the study can concentrate on the central controller.

As the train is made of e.g. 6 doors, the total failure of all local controllers is negligible compared to the failure of the central controller. If the failure rate of a local controller is 10^{-7} h^{-1} , and since those are tested daily (i.e. every 10 hours of operation), applying the Formula 3 from the Appendix in section § A5.10.3 below, the failure rate of the failure of all actuators would be :

Annex 4 : Examples from representative bodies on the use of CSM-DT

$$(10^{-7} \times 10)^6 \times \left(\frac{6}{10}\right) = 6 \cdot 10^{-37} \text{ h}^{-1}$$

[G 7] **Note :** using SIL, this target alone would mean that the door/close function will have to be SIL2 for the local controllers and SIL4 for the central controller. However this is not that simple :

A systematic failure (e.g. error in programming) may result in all doors opening at the same time, since they all receive the same input in terms of speed criterion and opening authorisation. This will depend whether local controllers only use generic train information or also local information :

(a) in the case only generic train information is used by local controllers, the most demanding requirement (10^{-9} h^{-1}) may need to be used for the local controllers as well (since it is unlikely that in terms of software the functions used in each of the hazards will be totally separated). This is because the local controllers cannot be considered independent (they will all react in the same way due to the identical inputs);

Therefore, hazards H2 and H3 may be triggered by a systematic failure of all local controllers, thus it would mean that the door open/close function will have to be SIL4 for all controllers (both central and local).

(b) If however (as it is considered in this example) local information is used as well, then independence can be proven between the local controllers. Therefore a SIL2 will indeed be sufficient.

A4.2.4.3 Solution 2

[G 1] It is considered that achieving a 10^{-9} h^{-1} is quite difficult. Thus, a different design is proposed:

[G 2] Another option would be to ensure that the speed criterion is directly delivered (as usable inputs) by the speed measurement system.

[G 3] Thus, the design would change to the one in Figure 28

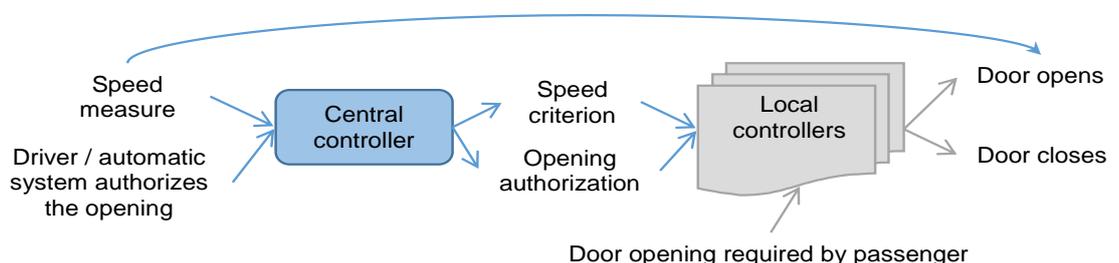


Figure 28: Door control system – Solution 2.

[G 4] In that case, the hazard H1 would still require a 10^{-7} h^{-1} for the local controllers.

[G 5] However for the hazards H2 and H3, the local and central controllers would not require a 10^{-9} h^{-1} anymore, since the speed measure is sufficient to prevent the door opening.

Annex 4 : Examples from representative bodies on the use of CSM-DT

[G 6] The fault trees for H2 would thus be as represented in Figure 29.

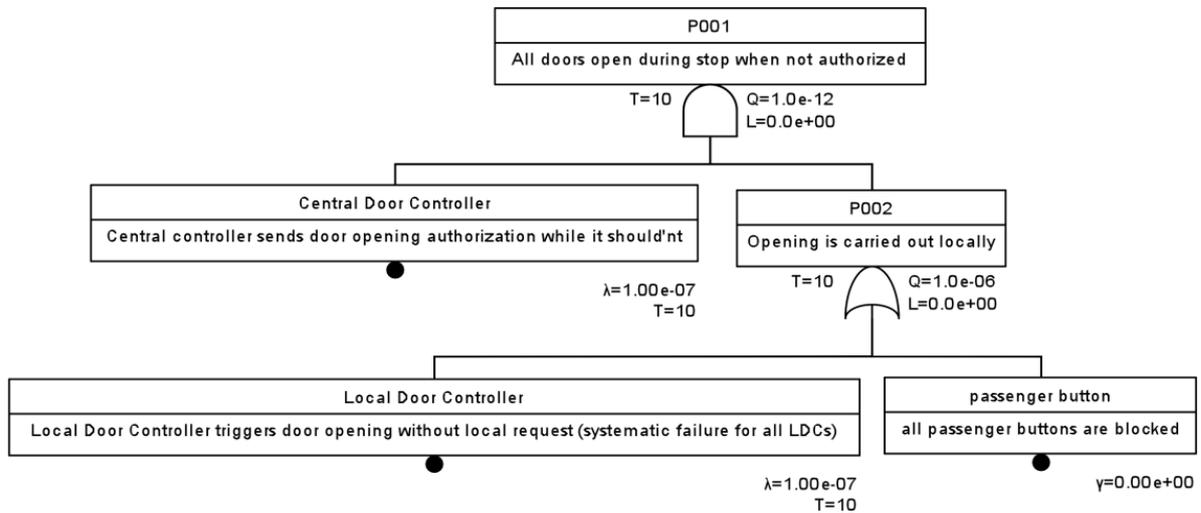


Figure 29: Door control system – Solution 2 : all doors open at standstill.

[G 7] The fault trees for H3 would thus be as represented in Figure 30.

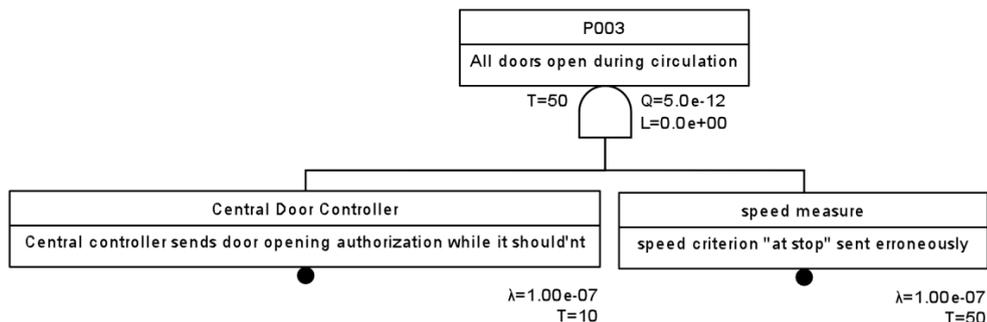


Figure 30: Door control system – Solution 2. : all doors open during circulation.

A4.2.5 Conclusion [CSM-DT]

[G 1] The chosen design (and other alternative designs, e.g. separating opening authorization as well, having automatic opening instead of passenger requested opening, etc.) will depend on the cost and performance of each design.

[G 2] The more complex the functions requested are (e.g. interrupt and provide again the opening authorisation depending on specific situations, like time during leaving the platform of the station), the more likely it is to see purely software orientated solutions (where independence is more difficult to ensure than with purely electronic systems, thus may require independent barriers for specific hazards).

A4.3 Example 3 : Control of the traction cut-off

A4.3.1 Preliminary system definition ^[CSM RA]

[G 1] The traction cut-off is a command from the ETCS onboard equipment to the braking system of the train (see Figure 31).

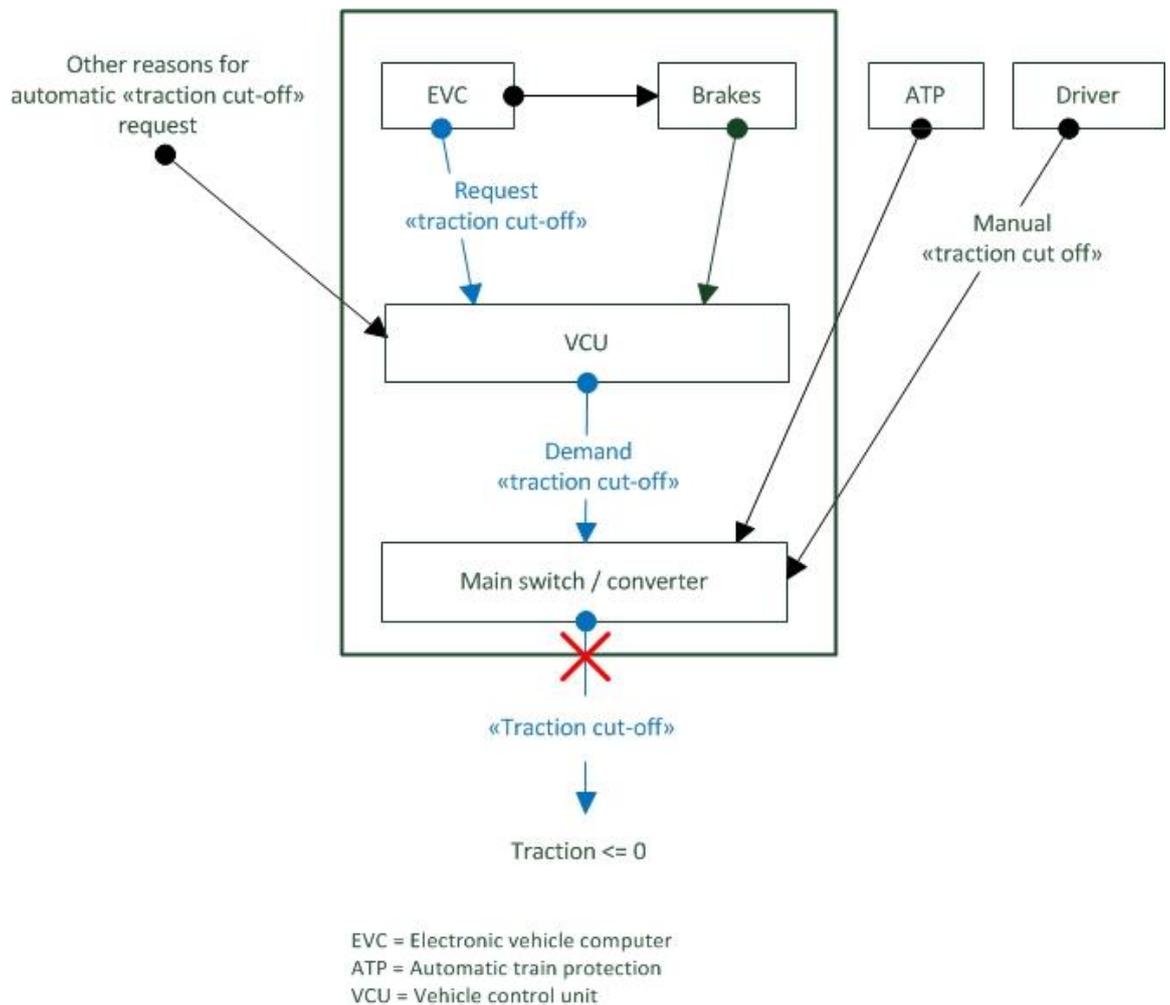


Figure 31: System definition for the traction cut-off under ETCS.

- [G 2] The safety requirement is derived for the situation where the request for traction cut-off is automatic and triggered by the Electronic Vehicle Computer (EVC).
- [G 3] Requests from other sources to of the traction cut-off such as brakes, the Automatic Train Protection (ATP) system or the train driver are also possible but they are not covered in the analysis.
- [G 4] Nevertheless, the train driver is considered as an external barrier because he can cut traction off manually, even if the technical system (i.e. the EVC) fails.

A4.3.2 Hazard Scenarios ^[CSM-DT]

- [G 1] If automatic traction cut-off fails, the train may receive a brake application request while the traction is still on, thus reducing the efficiency of braking. The hazard caused by a traction cut-off failure therefore consists of the train not stopping at the defined location.

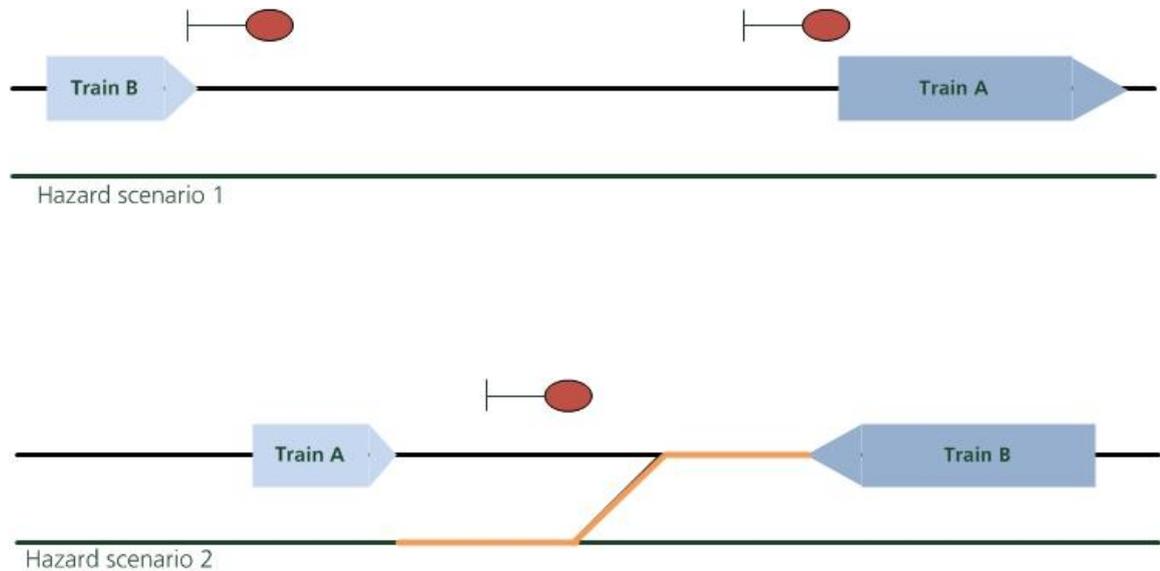


Figure 32: Hazard scenarios for a failure of the traction cut-off system.

- [G 2] The hazards were originally developed as part of the quantitative risk analysis for the Loetschberg Base Tunnel in Switzerland. Two hazard scenarios are of main relevance for the analysis (see Figure 32):
- (a) Hazard Scenario 1 : a short train has to stop due to a train ahead being at standstill;
 - (b) Hazard Scenario 2 : a short train has to stop before a switch due to a route conflict
- [G 3] The analysis concentrates on short trains because their braking characteristics are less favourable than for longer trains.

A4.3.3 Choice of the appropriate severity class ^[CSM-DT]

- [G 1] The appropriate severity class/category of CSM-DT is derived from the flowchart in Figure 5, based on the decision process described in section § 4.
- [G 2] In this example barriers external to the technical system under assessment are present. Therefore the failure of the function of the technical system under assessment alone does not directly lead to the accident.
- [G 3] Only a combination of failure of the technical system under assessment and of the external barriers can lead to the accident. In this case, it is necessary to consider a higher level function incorporating the technical function and the barriers. This higher level function then has a potential to lead directly to the accident.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

Table 23: Allocation of CSM-DT class/category for the traction cut-off system.

| Hazard | Credible potential for direct consequences? | Accident typically results in at least one fatality | Typically a large number of people is affected? | Accident typically results in fatalities? | CSM-DT |
|--------|---|---|---|---|--------------------------------|
| 1 | yes* | yes | yes | yes | Class (a), 10 ⁻⁹ /h |
| 2 | yes* | yes | yes | yes | Class (a), 10 ⁻⁹ /h |

*for higher level function incorporating the external barriers

A4.3.4 Consequence analysis [CSM-DT]

[G 1] The event tree for the Hazard Scenario 2 is illustrated in Figure 33.

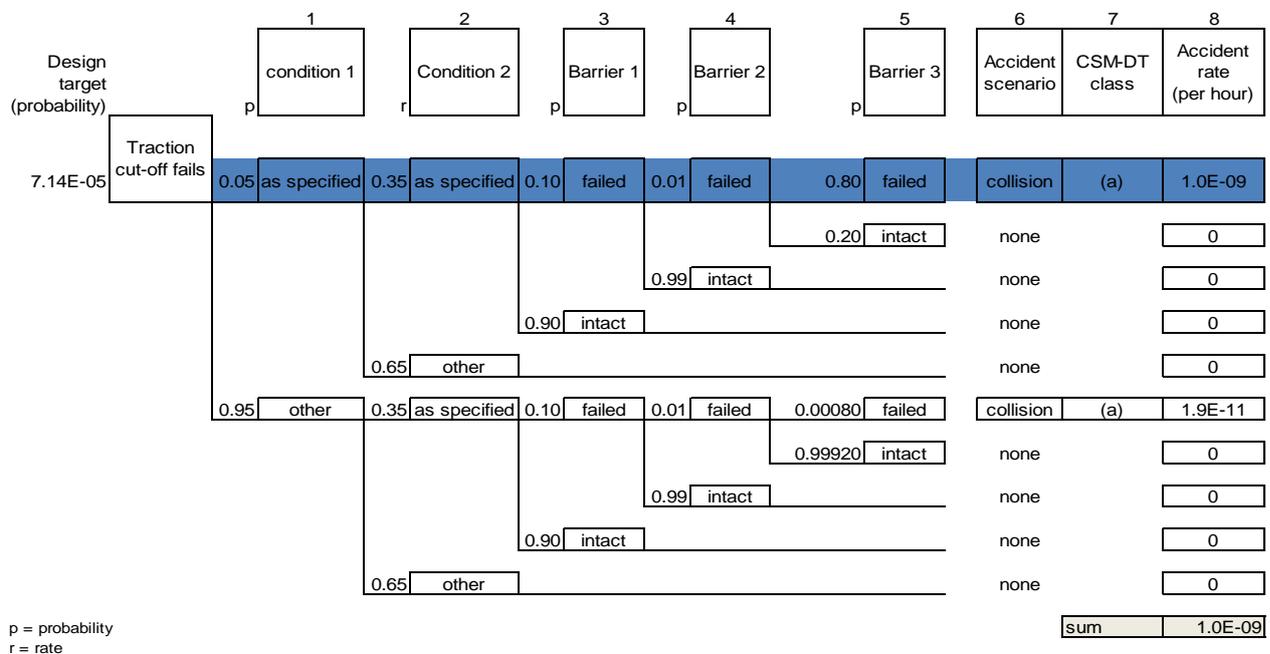


Figure 33: Event-tree for automatic traction cut-off (scenario 2)

[G 2] The event tree in Figure 33 represents the stopping of a train before a switch due to a route conflict :

- (a) the event tree starts with the probability of functional failure of the traction cut-off;
- (b) the event tree analysis takes into account the effects from two types of operational conditions ('Condition 1' and 'Condition 2') which are relevant for the hazard scenario. 'Condition 1' depends on whether the train is short or long one;
- (c) the event tree analysis takes into account the effects from three barriers ('Barrier 1', 'Barrier 2', 'Barrier 3'). The barriers represent technical and operational measures external to the technical function (see section § 5. above). 'Barrier 3' depends on 'Condition 1';

Annex 4 : Examples from representative bodies on the use of CSM-DT

- (d) the resulting accident scenario is described as a train entering an occupied track section and colliding with a second train already present in that track section;
- (e) the severity of the accident scenario collision is given by CSM-DT class (a) with an acceptable rate of occurrence of $\leq 10^{-9} \text{ h}^{-1}$, since there is a potential for multiple fatalities for this scenario. As shown in Figure 33 there are two separate paths that can result in an accident and which require the CSM-DT class (a). The accident rate for the critical path, i.e. the path with the higher accident rate is set to 10^{-9} h^{-1} and divided by the product of the values for operational conditions and barriers (columns one to five in Figure 33) in order to derive the design target for the function.

A4.3.5 Conclusions ^[CSM-DT]

- [G 1] This process results in an acceptable probability of $7 \cdot 10^{-5}$ for the automatic traction cut-off and represents the minimum safety requirement for this function.
- [G 2] Hazard Scenario 1 was investigated in the same way as Hazard Scenario 2 but it was found to be the non-restricting scenario and is therefore not described in detail.

A4.4 Example 4 : Transmit traction and brake command

A4.4.1 Introduction ^[CSM-DT]

- [G 1] The example focusses on the application of CSM-DT. Before applying the CSM-DT, the significance of the change was assessed, it was decided that the risks are not broadly acceptable and that the hazards are to be controlled by “explicit risk estimation”.

A4.4.2 Disclaimer ^[CSM-DT]

- [G 1] The illustrated example does not contain all details. It cannot thus be fully comprehensive. Several assumptions are taken to show how the allocation of CSM-DT can be done. In a real system, much more influencing parameters, scenarios and interactions must be considered in order to finally derive a complete and consistent set of safety requirements. The resulting figures and quantitative outcomes are thus purely fictive.
- [G 2] Furthermore, it is assumed implicitly that the design of the technical system is carried out in compliance with specific safety and quality processes, commensurate with the allocated CSM-DT class/category, to control appropriately the systematic failures. Moreover the safe integration is not considered in the example.

A4.4.3 System Definition ^[CSM RA]

- [G 1] The function under assessment is FD1 “Transmit traction and brake demand” predefined in German TeSiP which is equivalent to function JCE of EN 15380-4. The main functional elements are represented in Figure 34.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

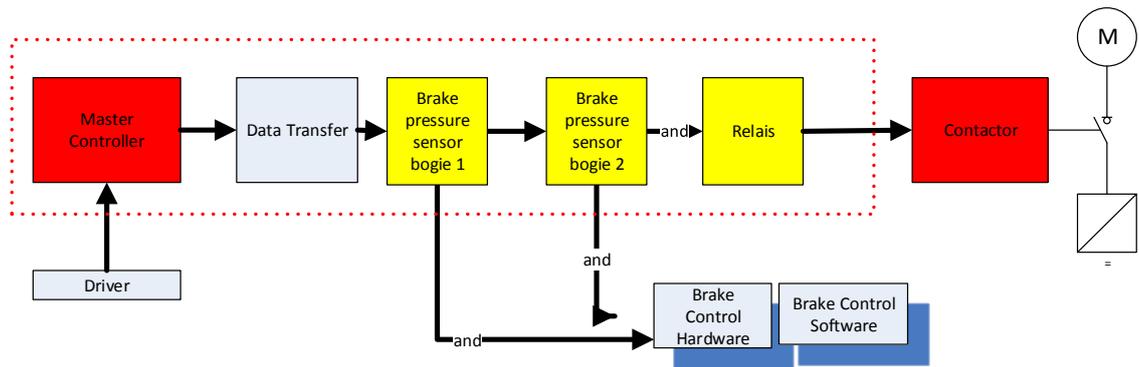


Figure 34: System definition of the “transmit traction and brake demand”.

- [G 2] The Master Controller is a control element used by the operator to activate the driving cab, define the direction of movement and set a throttle notch position.
- [G 3] The cab is activated by the operator when inserting a key into the controller. The key must be moved forward or backward to set a direction of motion. There is a throttle handle which controls 8 power levels delivered to traction motors. Moving the throttle handle forwards gives traction power while moving the handle backwards gives a dynamic brake effort.
- [G 4] The technical function comprises a lot of sub-functions. The illustrated example considers only a part of the elements in Figure 35. The functionality of the Master Controller used to control the traction demand requested by the train driver is considered within the example.
- [G 5] The function “F1 Define Set Point” has interfaces to “T_direction control switch”, “T_onboard network” and “S_status direction control switch” for receiving or sending information (data transfer). Refer to Table 24.
- [G 6] The example under assessment is represented in Figure 35. The status of the train direction control switch is defined based on information from interfaces 1 to 4.

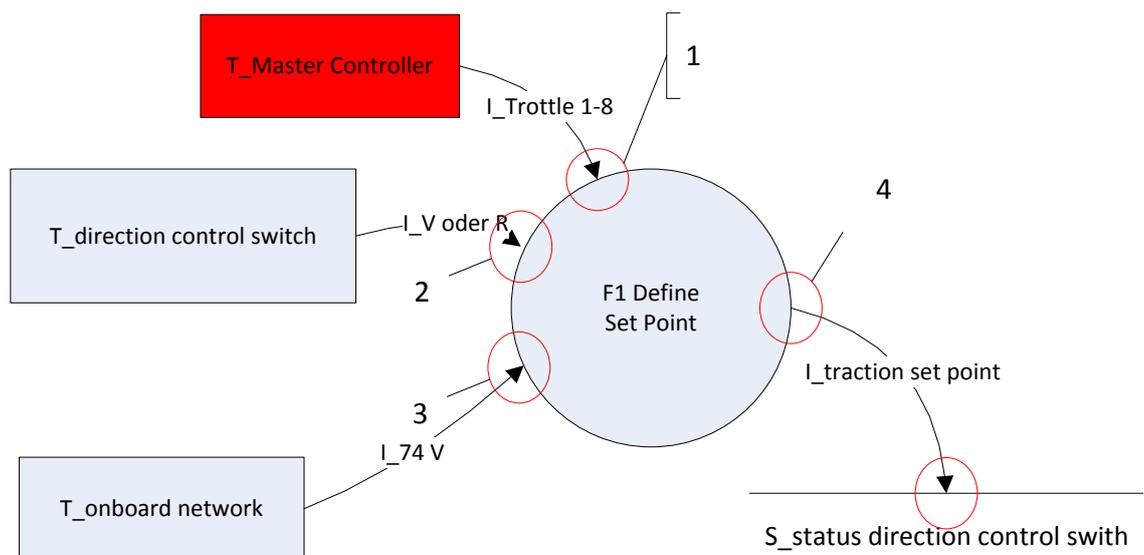


Figure 35: Interfaces of the „master controller “sub-function.

Annex 4 : Examples from representative bodies on the use of CSM-DT

[G 7] In reality, this main function has much more interfaces and sub-functions. However, they are not relevant for illustrating how the CSM-DT can be applied.

Table 24: Main function and sub-functions of the “transmit traction and brake demand”.

| Function | Interface | Source | Information | Target |
|------------------------------------|-----------|----------------------------|----------------------|-----------------------------------|
| Transmit traction and brake demand | 1 | T_Master controller | I_Throttle 1-8 | F1 Define set point |
| | 2 | T_direction control switch | I_V oder R | F1 Define set point |
| | 3 | T_onboard network | I_74 V | F1 Define set point |
| | 4 | F1 Define set point | I_traction set point | S_status direction control switch |

A4.4.4 Hazard Identification ^[CSM-DT]

[G 1] The hazard identification is done by a team of experts using different methods. The failure of the different sub-functions, and the possible failure modes, were analysed. An extract of the hazard identification is provided in Table 25. 5 hazards with impact on the safety are identified.

Table 25: Hazard Identification and Classification of the “transmit traction and brake demand”.

| Interface | Source | Information | Target | Failure mode | Hazard | Classification |
|-----------|----------------------------|----------------------|-----------------------------------|-----------------------------------|-----------------------------------|--|
| 1 | T_Master controller | I_Throttle 1-8 | F1 Define set point | Set point is not defined | No traction demand | No safety consequences |
| | | | | Set point is defined continuously | Untimely traction demand | Safety consequences possible (Haz1) |
| 2 | T_direction control switch | I_V oder R | F1 Define set point | Set point is defined continuously | No traction demand | No safety consequences |
| | | | | Set point is defined continuously | Untimely traction demand possible | Safety consequences possible (Haz2) |
| | | | | Set point is defined wrongly | Wrong side movement | Not considered in the specific situation |
| 3 | T_onboard network | I_74 V | F1 Define set point | Set point is not defined | No traction demand | No safety consequences |
| | | | | Set point is defined continuously | Untimely traction demand | Safety consequences possible (Haz3) |
| 4 | F1 Define set point | I_traction set point | S_status direction control switch | Set point is not defined | No traction demand | No safety consequences |
| | | | | Set point is defined continuously | Untimely traction demand | Safety consequences possible (Haz4) |
| | | | | Set point is defined too high | Strong jerk | Safety consequences possible (Haz5) |
| | | | | Set point is defined too low | No sufficient acceleration | No safety consequences |

A4.4.5 Hazard Classification and allocation of CSM-DT ^[CSM-DT]

[G 1] The identified hazards occur when the vehicle is unintentionally set in motion while the train driver is present in the locomotive. The assessment focusses mainly on the operator's actions in the cabin, the operator's requests for traction control commands and to the traction system and the parameters that are needed before traction can actually be applied to the motors.

Annex 4 : Examples from representative bodies on the use of CSM-DT

- [G 2] The allocation of CSM-DT is done using the flowchart in Figure 5, based on the decision process described in section § 4.
- [G 3] For the hazards identified in the example, the decision process leads to the allocation of a CSM-DT for each hazard, taking into account the parameters “credible potential for the consequence severity”, “direct”, “affected people” and “resulting severity”.

Table 26: Allocation of the CSM-DT class/category for the “transmit traction and brake demand”.

| Haz | Credible potential for direct consequences? | Accident typically results in at least one fatality? | Accident typically affects a large number of people? | Accident typically results in multiple fatalities? | CSM-DT |
|-----|---|--|--|--|--------|
| 1 | yes | yes | yes | yes | 1E-9 |
| 2 | yes | yes | no | N/A | 1E-7 |
| 3 | yes | yes | yes | no | 1E-7 |
| 4 | yes | yes | yes | no | 1E-7 |
| 5 | yes | yes | no | N/A | 1E-7 |

- [G 4] The allocated CSM-DT class/category for each hazard in function of the specific situations is summarised in Table 26. The most demanding design target is required for hazard 1 as an untimely traction demand could lead to train overspeed in operation and result in a collision or derailment where there is credible potential to affect a large number of people and to result in a large number of fatalities.
- (a) For hazard 2 it is assumed that only the train driver is exposed to risk, therefore as a large number of people is affected, the failure cannot result in multiple fatalities.
- (b) For hazard 3 and hazard 4, the consequences of the untimely traction demand are limited due to the specific operational scenario where during the coupling procedure the train speed is limited as the train has to stop before the coupling can start. Although a large number of people is affected, it can be considered reasonably that the number of fatal injuries is limited. Therefore the criteria “Accident typically results in multiple fatalities” is not fulfilled. As in point 2.5.5. of Regulation 2015/1136 the parameters “large number of people affected” and “multiple fatalities” are linked by an **“AND”-gate**, the harmonised design target of 10^{-9} h^{-1} is not to be applied; the operational procedure ensures that the coupling procedure can only start when the initial speed is 0 and the two train must stand close to each other. Therefore, according to Regulation 2015/1136, a design target of 10^{-7} h^{-1} is sufficient for controlling a hazard that can lead to a critical accident.
- (c) For hazard 5, a strong jerk is expected, in case that the traction demand is too high. Although the whole train is affected it is not credible that such a scenario will lead to multiple fatalities.
- [G 5] Without modelling all the necessary conditions that need to be fulfilled to result in a direct consequence, the same CSM-DT class/category would need to be allocated to the Master Controller than to the overall function “transmit traction and brake demand”. This is illustrated in Figure 36.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

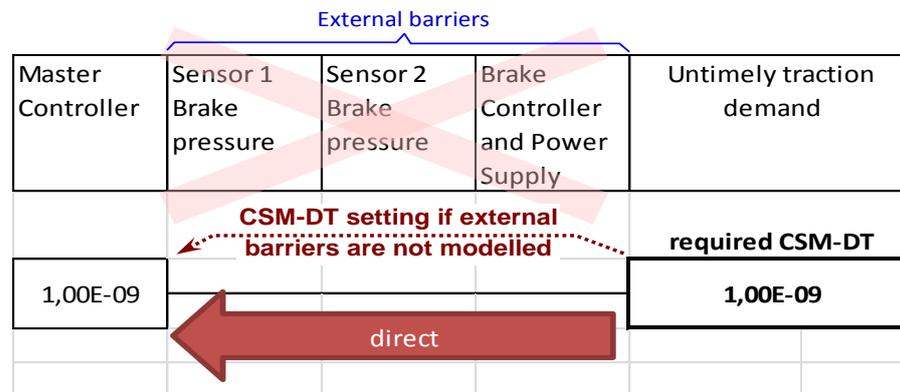


Figure 36: Link between the required CSM-DT and the safety performance that should be required for the Master Controller without taking into account any barrier.

[G 6] In practice, the allocation of the CSM-DT for the Master Controller from the overall safety requirement of the function “transmit traction and brake demand” needs to take into account the operational specificities, such as the active barriers, the operational conditions, the operational rules etc. So, as the single failure of the Master Controller does not directly lead to an accident, a less demanding safety requirement can be setup for the Master Controller than for the overall “transmit traction and brake demand” function : see section § A4.4.6 below.

A4.4.6 Consideration of the existing safety barriers ^[CSM-DT]

[G 1] In practice the overall safety requirement of 10^{-9} h^{-1} of the “transmit traction and brake demand” function needs to be apportioned down to the different contributors taking into account the barriers external of the function of the Master Controller under assessment.

[G 2] The risk assessment below will just focus on hazard 1 from Table 26 above.

[G 3] For hazard 1, the following barriers can prevent the failure of the Master Controller to result directly in the identified accident :

- (a) two independent Brake Pressure Sensors (if braking is used, then the pressure will be detected, and the traction will be cut off automatically);
- (b) Brake Controller and Power Supply (the brake controller cuts automatically (via the power supply contactor) the traction when a pressure sensor detects a braking).

[G 4] For the purposes of the example, it is assumed that :

- (a) the Brake Pressure sensors work with a safety performance of 90%, and;
- (b) the Brake Controller and the Power Supply work with a safety performance of 50%.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

| | Master Controller | Sensor 1 Brake pressure | Sensor 2 Brake pressure | Brake Controller and Power Supply | Untimely traction demand |
|-----------------------|----------------------|-------------------------------|-------------------------------|--|-----------------------------|
| Risk Reduction factor | | 0,9 | 0,9 | 0,5 | |
| | | 0,9 | | | no consequences |
| | 2,00E-07 | | | | |
| | | | 0,9 | | no consequences |
| | | 0,1 | | | |
| | | | | 0,5 | no consequences |
| | | | 0,1 | | |
| | | | | 0,5 | consequence possible |
| | | | | | 1,00E-09 |

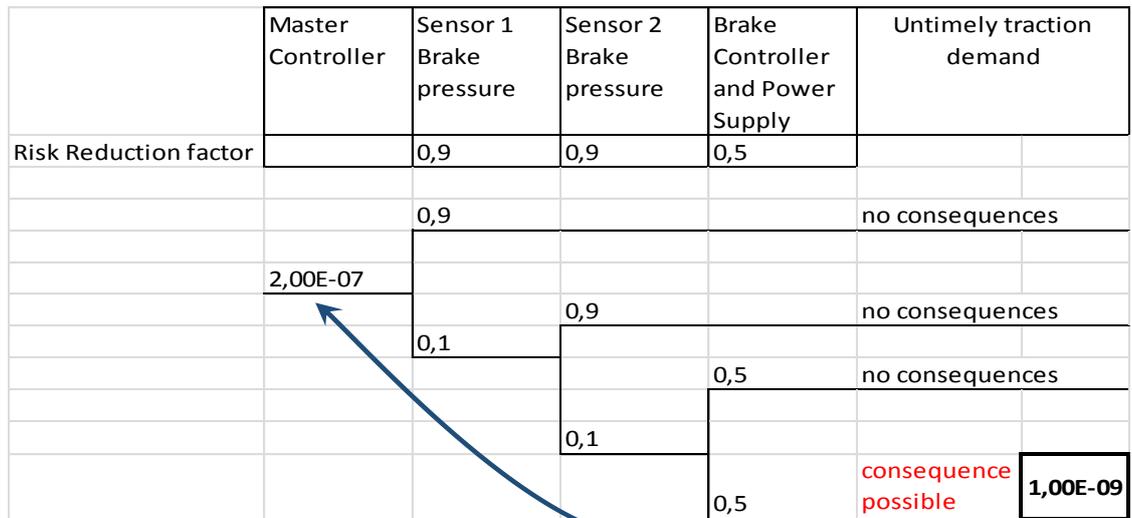


Figure 37: Event tree for back-calculating the safety requirement for the Master Controller based on requirement for the “transmit traction and brake demand”.

[G 5] When the safety architecture of the “transmit traction and brake demand” function, the external barriers (see Figure 36 above) and their safety performance are taken into account (see assumptions in point [G 4] of section § A4.4.6), the event tree in Figure 37 can be built.

A4.4.7 Conclusion ^[CSM-DT]

The event tree in Figure 37 shows that the overall safety requirement of 10^{-9} h^{-1} setup for the “transmit traction and brake demand” function is achieved if the failure rate of the Master Controller (i.e. technical system under assessment) is less than or equal to $2 \cdot 10^{-7} \text{ h}^{-1}$. This is the quantitative safety requirement to be used for the design of the Master Controller.

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.5 Example 5 : Level crossing case study

A4.5.1 References

- [Ex-5 Ref. 1] Heilmann, A., Peters, H., Braband, J.: Sicherheitsanalyse nach CENELEC (Signal + Draht, Nr. 7+8, 1998, 10-15
- [Ex-5 Ref. 2] DKE: Electric signaling systems for railways – Part 103: Identification of safety requirements for technical functions in railway signaling, DIN V 0831-103, 2014
- [Ex-5 Ref. 3] CENELEC: Railway applications - Systematic allocation of safety integrity requirements, CLC/TR 50451:2005

A4.5.2 Introduction ^[CSM-DT]

- [G 1] This example considers some practicalities of the explicit risk assessment approach referred to in EU Regulations 402/2013 and 2015/1136 on the CSM for risk assessment and the CENELEC EN 50129:2003 standard. The example has been used since 1997 in order to validate all concepts in EN 50129 (see e.g. the CENELEC TR 50451 [Ex-5 Ref. 3]). The methodology is explained step by step by means of an example. It starts with the system definition down to the SIL allocation.
- [G 2] **Disclaimer :** in order to illustrate clearly the major aspects of Regulation 2015/116, a “simplified example” of an automated level crossing (LX) is used. Neither the functionality nor the analyses bear any direct resemblance to the features of a particular type of level crossing. The major aim is to present an example of a methodology, not to provide a detailed realistic analysis. For more realistic analyses the reader is sent to [Ex-5 Ref. 1].

A4.5.3 System Definition ^[CSM RA]

- [G 1] The example considers a particular type of automatic level crossing which uses light signals to warn the road user and a distant (monitoring) signal to tell the train driver whether the level crossing is protected or not. It is similar to the German type Hp-ÜS or the Swiss type MINI. It is permitted to be used for a line speed up to 160 km/h. And **it is assumed that appropriate road traffic regulations are in place** which lowers the level of risk. As an extension, barriers might be added too, e.g. if required by particular regulations. It should be noted that extensive operational experience and accident data are available.
- [G 2] As a full system definition is beyond the scope of this example, only an informal functional description is given here – sufficient for the purpose of the example. Table 27 provides an overview of the principal functional units in our example level crossing.
- [G 3] Under fault-free operation, the level crossing functions as follows :
- an approaching train is detected by the switch-on element (01) and indicated to the controller (07);
 - the controller issues the command to activate the road signals (04) and waits until an indication of successful switch-on has been received;
 - the controller issues the command to activate the distant signal. The default position is off (which is the danger aspect). When the distant signal is off, an approaching train must stop at the LX and the driver may then have to switch on the LX manually using a key as the fall-back mode;
 - traversal of the LX by the train is detected by a switch-off element (02) and indicated to the controller;

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

- (e) the controller issues the command to switch off the distant signal. After a delay the road signals are switched off.

Table 27: Functional description of the automated level crossing.

| No. | Functional unit | Remarks |
|-----|-----------------|--|
| 01 | LX switch-on | Triggers activation of the LX when a train approaches (implemented by means of wheel detection equipment, e.g. an axle counter). |
| 02 | LX switch-off | Triggers deactivation of the LX once a train has left the crossing (implemented by means of wheel detection equipment, e.g. an axle counter). |
| 03 | LX monitoring | Displays the state of the LX to the train driver or interlocking (implemented e.g. by means of a distant signal) to allow monitoring of LX operation. |
| 04 | Road signalling | Displays the state of the LX to road users |
| 05 | Normalisation | Returns the LX to the normal position (no protection) if it is switched on and then not switched off within a certain time (due e.g. to a detector failure or the train stopping before the LX etc.). |
| 06 | Power supply | Consists of the normal power supply system or, as a fall-back level, a battery capable of operating the LX for a limited period, e.g. 2 hours. The battery voltage is remotely controlled by the interlocking. |
| 07 | Controller | Operates and controls the LX. A programmable electronic device which contains application software, site-specific data etc. |

[G 4] The overview of the level crossing is given in Figure 38.

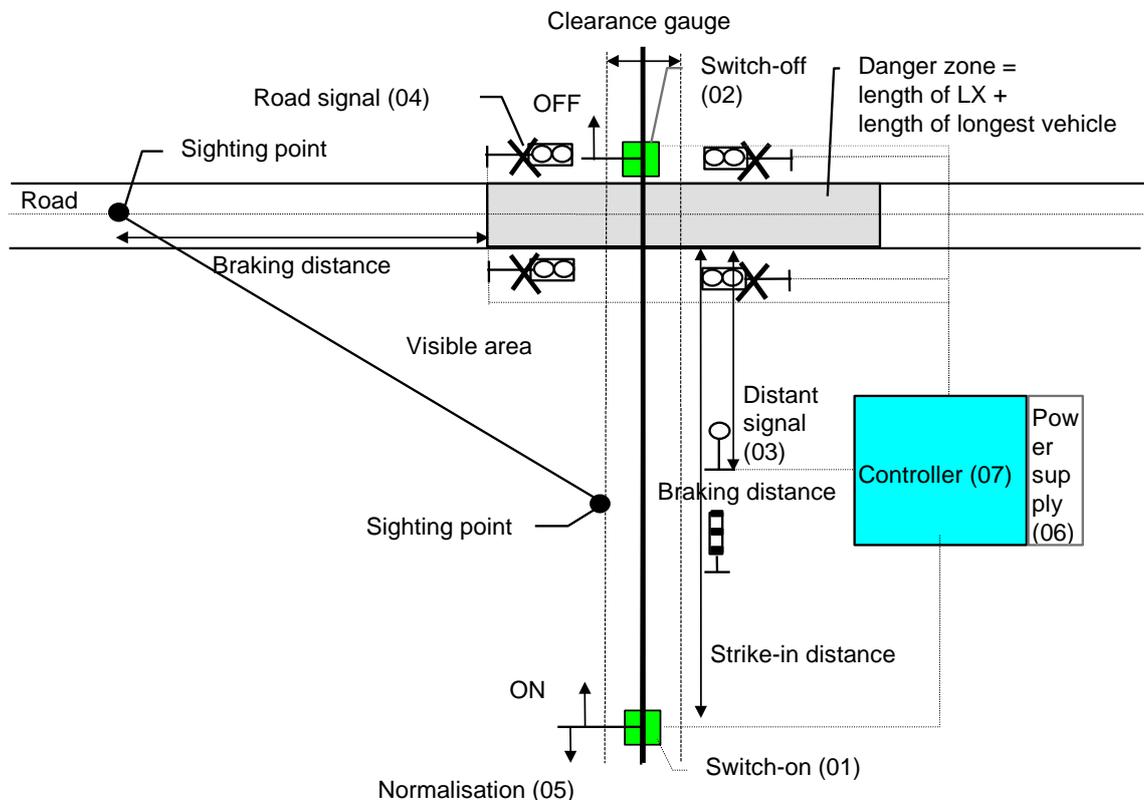


Figure 38: Overview of automated level crossing.

Annex 4 : Examples from representative bodies on the use of CSM-DT

- [G 5] The switch-on and switch-off functions are defined here as simple switches, without duplication. The triggering of switch-on does not mean that the level crossing as a whole is switched on, merely that the information that a train is approaching the level crossing is transmitted; the subsequent actions being performed by the controller.

A4.5.4 Hazard Identification ^[CSM-DT]

- [G 1] The safety function under assessment in the example is the protection of the level crossing (both for the train and the public, e.g. road users). The hazard identification was performed by functional failure analysis and validated by historical event data. Generally the following functional failures can be derived :

- (a) level crossing not protected when train is approaching (undetected);
- (b) level crossing not protected while train is in danger zone;
- (c) level crossing protected unnecessarily long.

Note : in case of a "level crossing with barriers" there may be additional functional failures that can be considered in the risk assessment.

- [G 2] A complete analysis is not performed for this example; instead, one hazard H="failure of LX to protect public from train" is considered. It is interpreted as covering situation (a) in the point above in which the level crossing should warn the public (of approaching trains), but fails to do so.

- [G 3] It should be noted that from the perspective of the risk analyst, only boundary hazards need to be considered here. An event such as "switch-on fails to detect train" is not a boundary hazard that needs to be considered at this level because, although it might lead to an accident if it occurred at a level crossing, in the example (see analysis below) it is only the cause of a hazard, not a hazard in its own right at system level (Other built-in functions exist which could detect the failure of a track circuit.). The hazard classification is neither provided here as it seems obvious that the hazard is not broadly acceptable.

A4.5.5 Explicit Risk Estimation ^[CSM-DT]

- [G 1] The criterion in point 2.5.5. in the Annex of regulation 2015/1136 is applied directly :

Where hazards arise as a result of failures of functions of a technical system, without prejudice to points 2.5.1 and 2.5.4, the following harmonised design targets shall apply to those failures :

- (a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.*
- (b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable.*

The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure.

- [G 2] The first question to ask is whether the failure has credible potential to lead directly to an accident?

If the protection function of the automated level crossing fails there is a slight chance that either the road user or the train driver might prevent the accident. However as both have a

Annex 4 : Examples from representative bodies on the use of CSM-DT

high level of trust in the automation and they have no experience with such rare failures happening there is a sufficiently credible potential for an accident and this possibility is neglected as it depends rather on good luck. It is to note that also detection of the hazard by the train driver is unlikely as there are no barriers at the level crossing. If there were barriers there would be a chance for the train driver to notice open barriers while passing over the level crossing. Also in this example the train and road traffic density can be neglected, because failure detection does not depend on these densities. It is very likely that only an accident or a near-miss might detect the failure.

[G 3] The next question is whether at least a critical accident (“an accident typically affecting a very small number of people and resulting in at least one fatality”) is triggered.

As level crossing accidents occur frequently, the severity may also be assessed statistically as the outcome does not depend on the causes. So even as most collisions are not caused by technical systems, the severity of the collision will be more or less the same.

It must be noted that the statistical data must be evaluated carefully by experts. This is also required by CENELEC EN 50126, which demands assessment of the adequacy of the information, and where appropriate, data or other statistics, used as input to risk assessment. If dependable data are not available the choice has to be made by expert judgement only.

Taking for example recent data from the Railway Safety Performance report of the European Union Agency for Railways (Ref. TR-AB-14-001-EN-C), it can be found that in 2012 for EU-28 states, 372 fatalities resulted from 373 reported level crossing accidents. The statistics do not distinguish between collision and derailment, so also derailments are included with respect to their frequency of occurrence. Almost all fatalities were level crossing users, but one employee. The evaluations of the statistics also show that less than 1% of the significant accidents reported are potentially serious (significant and serious accidents as defined in the Railway Safety Directive). The statistics for earlier years are comparable, it can be concluded that the data are representative for EU-28 and that level crossing accidents typically result in at least one fatality⁽¹⁹⁾ (and in more than 99% of the cases not more). Based on those statistics, it can also be concluded that only a very small number of people⁽¹⁹⁾ are affected as in level crossing accidents typically only road⁽¹⁹⁾ users are affected and this is a very small group, e.g. in Germany the average number of car occupants is 1.4.

[G 4] At the next step, it is necessary to distinguish between classes (a) and (b) in point 2.5.5 of Regulation 2015/1136. This choice is to be based on “the most credible unsafe consequence of the failure”. So, it is necessary to decide whether it is more credible that a critical or a catastrophic accident (“an accident typically affecting a large number of people and resulting in multiple fatalities”) occurs. From the discussion above, it can be concluded that in a level crossing accident typically a few persons⁽¹⁹⁾ are affected and only on average one person is killed. So the choice is clearly class (b) leading to a design target (THR) of 10^{-7} per operating hour.

⁽¹⁹⁾ Footnote added by the European Union Agency for Railways : *As the current safety requirements for protection systems at level crossings vary significantly among the Member States of the European Union, the validity of this assumption and thus the level crossing risk acceptance needs to be verified in function of the current experience in the considered Member State. Indeed, depending on whether appropriate road traffic regulations exist and may be, or may not be, taken into account for the risk assessment, the allocated safety requirements might be different in function of the Member State.*

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.5.6 Validation ^[CSM RA]

[G 1] The result derived by application of the explicit risk acceptance criterion from Regulation 2015/1136 can be compared now with results from other risk acceptance principles.

[G 2] The first comparison is with the application of the first risk assessment principle, Code of Practice.

In Germany a dedicated risk assessment standard exists [Ex-5 Ref. 2], which explicitly considers level crossings as an example. It covers a general hazard, which is similar to the hazard H="failure of LX to protect public from train", and several more particular hazards. The derived design target is 3×10^{-8} per operating hour. It is to note that this result is based on classifying the credible consequences in class F, which is defined by one fatality as a typical consequence. This result is based on statistical evaluation of the accident database of Deutsche Bahn AG.

[G 3] The second comparison is with similar Reference Systems. In Germany level crossings are designed according to requirements based on [Ex-5 Ref. 1]. The risk analysis was based on the risk matrix shown in Table 28. In the calibration of the matrix only two categories are used, tolerable and intolerable. It is important to note that also here the credible consequence was evaluated to "critical" and not "catastrophic". The resulting requirement for the design target is "remote" and not "improbable" or "incredible". The corresponding quantitative target is comparable to [Ex-5 Ref. 2].

It is to note that according to EN 50126:1998 standard, "tolerable" is defined as "Acceptable with adequate control and with the agreement of the Railway Authority". Both conditions are fulfilled in Germany and so "remote" is the appropriate choice.

Table 28: Risk matrix for the automated level crossing.

| Frequency of occurrence of a hazardous event per LX per year | Risk Levels | | | |
|--|--|-------------|-------------|--------------|
| Frequent | Intolerable | | | Intolerable |
| Probable | Tolerable | Intolerable | | |
| Occasional | | Tolerable | Intolerable | |
| Remote | | | Tolerable | Intolerable |
| Improbable | | | | Tolerable |
| Incredible | Tolerable | | | |
| | Insignificant | Marginal | Critical | Catastrophic |
| | Severity Levels of Hazard Consequence | | | |

[G 4] The overall conclusion is that **in Germany** also the two other risk acceptance principles would lead to similar results as the explicit risk estimation. It is to note that in both examples no SIL allocation was performed at this level, but after apportionment to the last independent functional level (compare to Figure 40).

A4.5.7 Conclusion ^[CSM-DT]

[G 1] The process of safety analysis on the basis of Regulation 402/2013 and the approach to derive the applicable CSM design target are explained through this example. It is very important to acknowledge that the actual results depend on the system environment and the system architecture design, as well as on the current experience of every Member State with the protection of level crossings (refer to the footnote 19 on page 103 above).

Annex 4 : Examples from representative bodies on the use of CSM-DT

A4.5.8 Appendix to Example 5 : Hazard Control^[CSM-DT]

- [G 1] This appendix to the example 5 shows how the risk assessment could be continued to the apportionment of safety requirements and SIL allocation, which is not treated in detail in Regulations 402/2013 and 2015/1136, but would provide the link to the CENELEC standards. It is additional material not necessary for the derivation of CSM-DT but which needs to be part of the results from the overall risk assessment.
- [G 2] From the design target, the level crossing could be implemented either as a monolithic function (leading to SIL 3 for the level crossing by the application of EN 50129 SIL table - see footnote (24) on page 127) or by trying to find independent functions at a lower level and allocate a SIL at this level, the lowest level where independence can be demonstrated. In Order to allocate a SIL level, the lower level functions must be independent with respect to both random and systematic faults.
- [G 3] The analysis below discusses in detail only the switch-on and related functions. In a simplified functional FMEA one might discover entries like in Table 29.

Table 29: Example of a functional FMEA for the automated level crossing.

| No. | Function | Failure mode | Effect | Hazard | Remarks |
|-----|---------------|---|--|--|--|
| 01 | Switch-on | Late or no detection of train | Late or no protection of LX | Possible if LX monitoring also fails | |
| ... | | | | | |
| 03 | LX monitoring | Distant signal shows wrong aspect ("green") | Train driver will never stop at distant signal | Possible if strike-in also fails | |
| ... | | | | | |
| 06 | Power supply | Complete immediate failure | LX may remain in an undefined or given state | Possible if road signals are off and distant signal shows "green" aspect | Details depend on operational procedures |
| ... | | | | | |
| 07 | Controller | Undetected incorrect output | LX may change to any state | Yes, if command is on the wrong side | |
| ... | | | | | |

- [G 4] From the FMEA in Table 29, it can be seen that the switch-on (01) and monitoring functions (03) are related. Only a failure of both functions can create a hazard. There are, however, common causes which could lead to simultaneous failure of both functions. Failure of the controller or power supply (it is assumed here that this will always lead to the hazard, to keep things simple; in fact, not every failure of these functions does usually lead to a hazard). So it is possible to separate the common causes and redefine the functions. This could be represented using a fault tree as shown in Figure 39.
- [G 5] Assuming these were the only Common Cause Failures (for the sake of brevity, a detailed analysis is not given here), the switch-on (01) and monitoring (03) functions are independent because the AND relationship between the two functions holds regardless of whether the cause of the failure is random or systematic (no distinction was made in the above FMEA table). If this AND gate is exploited in the causal analysis, the two functions must also be implemented independently. This would lead to an SRAC.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

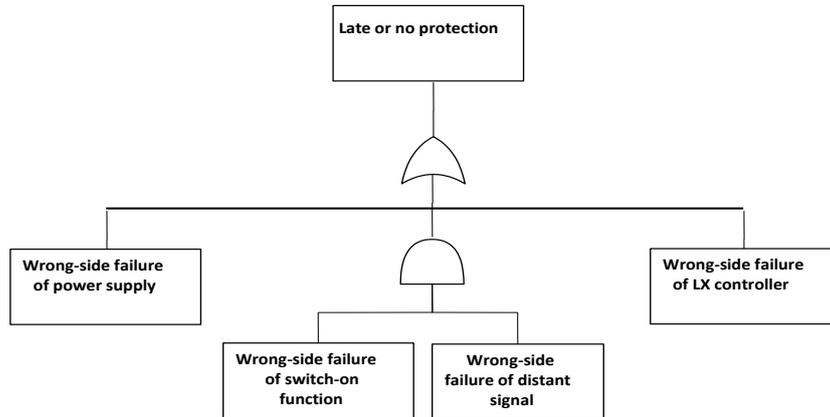


Figure 39: Functional FTA for the switch-on function (O1) of the automated level crossing.

[G 6] Figure 40 shows the upper part of a fault tree, such as it might result from a complete functional failure mode and effect analysis (FMEA) of the functional description. In this description common cause failures (CCFs) are not taken into account for each level, but were collected at the first level. As the first step, the tolerable hazard rate from the top was apportioned to the next level down. Hazard rates of 10^{-8} h^{-1} to $4 \times 10^{-8} \text{ h}^{-1}$ respectively were thus obtained for the two sublevels in the example.

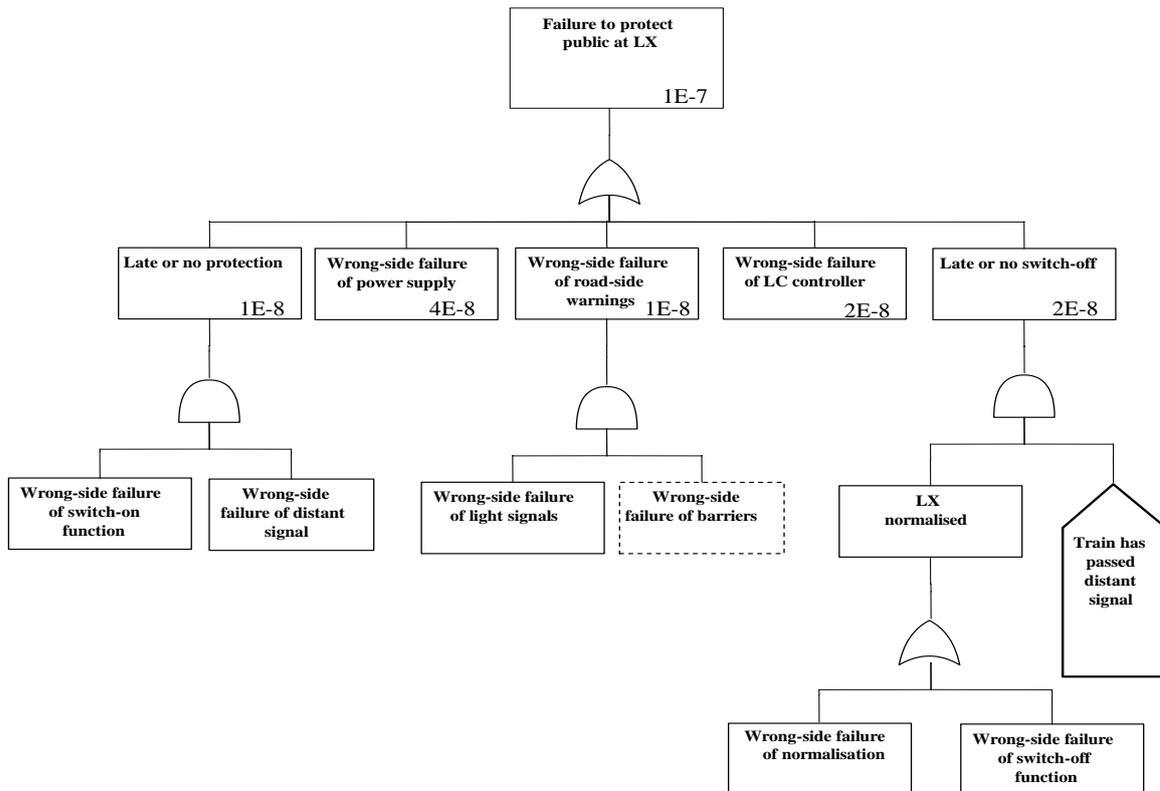


Figure 40: Causal analysis (FTA) for the automated level crossing.

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

- [G 7] For some functions, SIL may directly be allocated, e.g. for the level crossing controller SIL 3 is obtained.
- [G 8] To exploit the AND gate in the apportionment process, it is necessary to look at the failure detection mechanisms and failure detection rates for the two functions. Failure of the switch-on function is detected by the train driver of the next approaching train, but detection of a distant signal failure depends on further operational details (failure means that the signal never shows the danger aspect). Some railways require train drivers to observe the change of signal aspect during the approach. If this is not required from the operational point of view, the failure may be detected either after an incident or during regular maintenance. The results are summarised in Table 30.

Table 30: Example of detection mechanisms and detection times for the automated level crossing.

| No. | Function | Failure detection mechanism | Average failure detection time | Remarks |
|-----|------------|-----------------------------|--------------------------------|---|
| 01 | Switch-on | Monitoring | 8 hours | If switch-on fails, the distant signal shows a restrictive aspect. The driver then stops before the LX and notifies the control centre. The failure is detected. He can then pass the LX in fall-back mode. |
| 03 | Monitoring | Train driver | 24 hours | If the train driver is required to observe a change of signal. |
| | | Maintenance | 1 year | |

- [G 9] Applying the first set of parameters, the tolerable hazard rates for the two functions THR_{01} and THR_{03} would have to meet the requirements of the following formula:

$$THR_s \approx \frac{THR_{01}}{DR_{01}} \times \frac{THR_{03}}{DR_{03}} \times (DR_{01} + DR_{03})$$

where DR is detection rate from EN 50129.

- [G 10] Thus the following equation must be satisfied:

$$1 \times 10^{-8} \approx \frac{THR_{01}}{DR_{01}} \times \frac{THR_{03}}{DR_{03}} \times (DR_{01} + DR_{03})$$

$$= \frac{THR_{01}}{1/8} \times \frac{THR_{03}}{1/24} \times (1/8 + 1/24)$$

- [G 11] If the requirements were apportioned equally, the result would be

$$THR_{01} = THR_{03} \leq 2 \times 10^{-5} h^{-1}$$

- [G 12] Using the SIL table from EN 50129, SIL0 is obtained in both cases. But a different apportionment is possible: if the THR for switch-on is defined as $10^{-4} h^{-1}$, the result is $THR_{03}=3 \times 10^{-6} h^{-1}$, corresponding to SIL1. It is to note that in all examples appropriate independence has been assumed and needs to be maintained in the implementation.

- [G 13] With the second set of parameters, the situation changes. Here the requirements would be :

**Annex 4 : Examples from representative bodies
on the use of CSM-DT**

$$\begin{aligned}1 \times 10^{-8} &\approx \frac{THR_{01}}{DR_{01}} \times \frac{THR_{03}}{DR_{03}} \times (DR_{01} + DR_{03}) \\ &= \frac{THR_{01}}{1/8} \times \frac{THR_{03}}{1/8760} \times (1/8 + 1/8760)\end{aligned}$$

[G 14] Keeping the requirement for switch-on as $THR_{01}=2 \times 10^{-5} h^{-1}$, the result would be:

$$THR_{03} \leq 6 \times 10^{-8} h^{-1},$$

which is equivalent to SIL3. This shows the immense importance of the failure detection mechanisms and rates.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

ANNEX 5 : AGENCY EXAMPLE ON THE USE OF CSM-DT (TRAINBORNE HOT BOX DETECTOR)

A5.1 (Preliminary) system definition [§ 2.1.2 in Annex I of Reg. 402/2013] ^[CSM RA]

[G 1] Existing railway system before the change :

The technical system is an existing high speed (passenger) train already in service. The prevention of hazards that cause the overheating of wheelsets and axleboxes is controlled by appropriate maintenance and operational procedures of the safety management system of the railway undertaking which operates those passenger trains. Predeparture checks, periodic planned maintenance inspections and preventive maintenance operations of Rolling Stock are put in place to prevent, detect and, when necessary, correct emerging failures of wheelsets and axleboxes (e.g. wheel bearing fatigue, loss of bearing lubrication in axleboxes, defective brakes or any other cause).

In addition to those preventive maintenance and operational procedures, technical systems outside the train are also used during operation to further prevent train derailments caused by the overheating of wheelsets or axleboxes. Those technical systems, called “hot box detectors”, are laid down along the railway line at regular distances. The function of those “trackside hot box detectors” is to scan passing trains for the overheating of wheelsets and axleboxes in order to alarm the traffic control center who will in turn :

- (a) inform the driver by radio for stopping the train at an appropriate and agreed location, before a fire appears or before the affected wagon, and possibly the whole train, derails
- (b) reduce the speed of trains arriving in the opposite direction on adjacent tracks for mitigating the lateral shock risks caused by the blast at the crossing of two trains and which can potentially lead to the derailment of the train with a hot box.

[G 2] Intended change to the railway system (see Figure 41) :

- (a) For existing high speed passenger trains, already in service, instead of detecting the overheating of wheelsets and axleboxes only by functions of the infrastructure, the “hot box detection functionality” is also installed onto the train :
 - (1) The function of those “trainborne hot box detectors” is the same. They monitor the temperature of wheelsets and axleboxes in the area of bogies;
 - (2) In case of detection of overheating, a lamp is lit in the driver’s cabin. The train driver can then stop safely the train at an appropriate location and verify whether additional operational actions might be necessary, for example for proceeding the journey further with a restricted speed.

Advanced functions outside the scope of the present example :

- (i) some trainborne hot box detection systems might also indicate to the driver the temperature increase gradient, i.e. the speed at which the wheelset and axlebox temperature increases. This information influences the operational procedures and the emergency of the driver’s reaction for stopping the train safely at an appropriate location;
- (ii) some trainborne hot box detection systems might also locate accurately the coach number, axle number and side of the train where the wheelset or axle box is overheating.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (3) The function under assessment is the “detection of a hot box event⁽²⁰⁾ and the indication of the event to the driver” by a trainborne hot box detection system.
- (b) **Limitations for the risk assessment :** this example considers a risk assessment done by a railway undertaking which decides to fit some of its trains with a new trainborne hot box detection system. The existing infrastructure hot box detection system is not removed; it continues to be used. The manner those two systems are used [i.e. trainborne system alone or both trainborne and trackside ones], with any necessary operational procedures, is not covered by the risk assessment below. That shall be analysed and evaluated in a separate risk assessment.

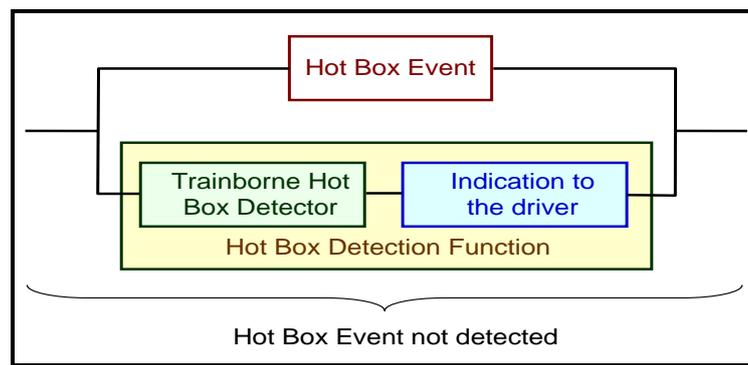


Figure 41: Schematic representation of the events and contributors to the trainborne hot box detection function.

[G 3] **Differences between the existing railway system and the change under assessment :**

- (a) The trackside functions “hot box detection” and “hot box information to the driver by radio” are replaced by new trainborne functions for “hot box detection” and the associated “visual and/or audible indication to the driver” using for example a wired connection or a train communication bus.
- (b) In addition to that, the following differences between the existing infrastructure hot box detection system and the trainborne hot box detection system under assessment are of importance :

- (1) existing infrastructure hot box detection system : trackside detectors are laid down at regular distances along the railway line. Consequently, if one “trackside hot box detector” fails and does not detect a “hot box event”, the hot box event will be detected by the next healthy trackside hot box detector. This architectural choice of the infrastructure allows to tolerate failures of one “trackside hot box detector” as another healthy detector is crossed after a defined distance. So, although a “hot wheelset or axlebox” might occur in the vicinity of a malfunctioning “trackside hot box detector”, the Hot Box Event remains undetected only during the time needed to reach the next trackside hot box detector.

For example, if trackside hot box detectors are placed every 25 km, and if the train is running at a speed of 250 km/h, the next trackside hot box detector is crossed after 6 minutes.

⁽²⁰⁾ “Hot box event” should be understood as an increase of temperature of a wheelset or axlebox.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (2) new trainborne Hot Box Detection system : if the Hot Box Detector fails, then a hot box event can no longer be detected on the train as long as the detector is not repaired. The risk assessment shall thus consider the necessity to introduce or not redundancy in the hot box detection function.
- (3) the hot box event detection is continuous with the new trainborne system whereas it is intermittent with the existing trackside system (a detection is possible every 6 minutes, with the assumption that trackside detectors are spaced by 25 km and the train operates at speed of 250 km/h).
- (c) With the trainborne Hot Box Detection system, the hot box event information is not automatically available to the infrastructure manager. The Traffic Controller cannot thus enforce the necessary speed reduction on adjacent tracks to mitigate the lateral shock risks caused by the blast at the crossing of two trains.

A5.2 Significance of the change [Article 4 of Reg. 402/2013] ^[CSM RA]

[G 1] The criteria of Article 4 of Regulation 402/2013 are used as represented in Figure 42.

[G 2] Article 4(1) – “Impact on safety or is it safety related?”

The change under assessment impacts the safety. In case of failure of trainborne functions “hot box detection” or “visual and/or audible indication to the driver”, a “hot box event” is not detected. A fire or a derailment may then occur with potentially catastrophic consequences.

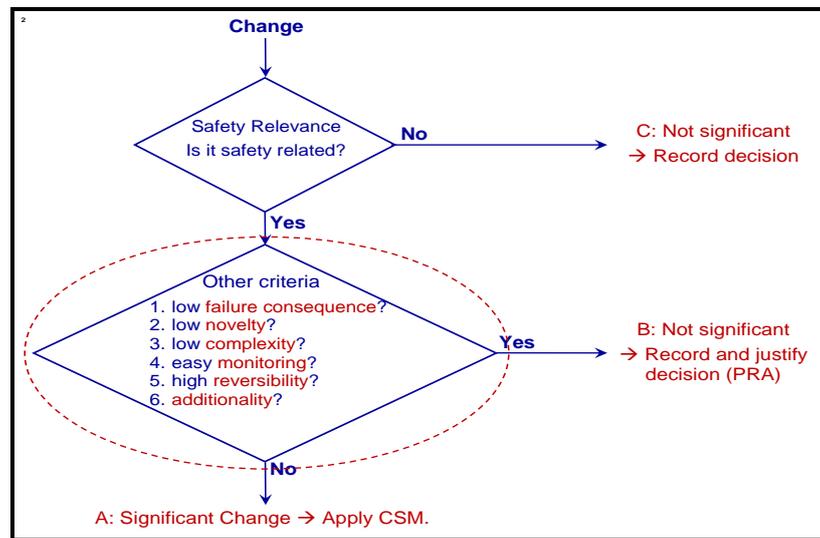


Figure 42: Article 4 criteria in Reg. 402/2013.

[G 3] Article 4(2) – The other criteria in Article 4 may be assessed in the following way :

- (a) “**low failure consequences?**” → no as the failure to detect a hot box event could result in catastrophic consequences (i.e. multiple fatalities) in case of derailment;
- (b) “**low novelty?**” → no. Although an equivalent function or detectors were used by the trackside to inform by radio train drivers on hot box events, the risk assessor (i.e. proposer) might decide that the technology is completely new on trains. Indeed, new operational procedures are needed for testing regularly the Hot Box Detector functionality, for managing the Hot Box Event alarms, for communicating those alarms

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

to the Traffic Controller in order to enforce speed reductions on adjacent tracks, etc. This new function on the train requires thus also coordination with the infrastructure manager for defining the appropriate risk control measures at the interface between the railway undertaking and the infrastructure manager;

- (c) **“low complexity?”** → no as additional trainborne equipment needs to be installed at a convenient location and has to be maintained;
- (d) **“easy monitoring?”** → no as the trainborne hot box detectors need to be tested and maintained regularly;
- (e) **“high reversibility?”** → yes as the technical option for keeping the existing **trackside** hot box detectors can be considered;
- (f) **“additionality?”** → not applicable as this is the first time this type of change is considered on the trainborne.

[G 4] **Decision** : based on the answers to all those questions, the proposer considers the change is significant. Another proposer might decide that the change is not significant.

No matter what the decision is, whenever a change impacts the safety a risk assessment must be done to keep the risks arising from the change to an acceptable level. A CSM assessment body is required only if the change is significant.

A5.3 Hazard identification and classification [§ 2.2 in Annex I of Reg. 402/2013] ^[CSM-DT]

A5.3.1 Hazard identification – Use of Failure Mode and Effect Analysis (FMEA)

[G 1] A functional “Failure Mode and Effect Analysis” (FMEA) analysis can be used for identifying the hazards arising from the change under assessment. For more information about the FMEA tool, refer to the Appendix in section § A5.10.1 below.

[G 2] The principles of the FMEA are applied on the trainborne Hot Box Detection function :

- (a) an FMEA table is built systematically and progressively : see Table 31 below;
- (b) the functions of the system definition (see section § A5.1 above) are assessed, using generic failure modes (e.g. function does not start, it starts when not needed, it does not stop when needed, it stops when not needed, delay in response) and, where necessary, adapted to the specificities of the Hot Box Detector;
- (c) then the potential consequences of the different failures modes are identified for every assessed function at the level of both the technical system under assessment and the whole train.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

Table 31: Functional FMEA of a trainborne Hot Box Detection.

| N° | Function | Functional failure modes | Cause | HAZARD - Consequence at level of technical system | Consequences at train level |
|--|------------------------------|--|---|---|---|
| <p><i>For the purposes of this example, the failures of the driver are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change. It is thus assumed that the associated human factor aspects are properly analysed and controlled through the Safety Management System of the railway undertaking.</i></p> <p><i>For example, when the hot box detection function is achieved by a trainborne system, as Hot Box Events can occur at any moment of time and at any location of the track, operational procedures need be defined with the infrastructure manager (IM) in order to manage a safe stopping of the train at an appropriate and agreed location, including thus the necessity to enforce by the IM a speed reduction for trains on adjacent tracks in order to manage the risks caused by the blast at the crossing of two trains.</i></p> | | | | | |
| 1. | Trainborne Hot Box Detection | Detection does not start | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely. |
| 2. | | Detection starts when not required | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> Driver required to stop the train whereas not necessary Traffic operation disturbed |
| 3. | | Detection does not stop when required | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> Driver required to stop the train whereas not necessary Traffic operation disturbed |
| 4. | | Detection stops when not required | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Hot Box Event not detected any more by technical system whereas still required | In case of a Hot Box Event, the driver can be misled (e.g. believes it is a false alarm) and could ignore the alarm whereas he shall stop the train safely. |
| 5. | | Detection is delayed in response | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety | In case of a Hot Box Event, the driver is informed too late and might not stop the train safely. |
| 6. | | Detection degraded (e.g. wrong output level) | | Not applicable. The hot box detection is a binary output | Not applicable. The hot box detection is a binary output |

A5.3.2 Hazard classification

[G 1] Table 31 above identifies the different hazards and potential consequences at the train level that can arise from failures of the trainborne hot box detection function.

[G 2] Although the FMEA identifies six functional failure modes, they can be classified in four categories :

- failure modes 1 and 4** resulting in the “non-detection” of a Hot Box Event and therefore to the lack of information to the driver for stopping the train safely;
- failure modes 2 and 3** resulting in a spurious detection of a Hot Box Event and thus disturbing the traffic operation;
- failure mode 5** resulting in a too late “detection” of a Hot Box Event and therefore a late information to the driver for stopping the train safely;
- failure mode 6** which is physically not possible for the system under assessment.

[G 3] This hazard classification can be represented as shown in Table 32 below. It is the same table as Table 31 above where the redundant lines are masked.

**Annex 5 : Agency example on the use of CSM-DT
(Trainborne Hot Box Detection System)**

Table 32: Hazard classification within the functional FMEA of a trainborne Hot Box Detection.

| N° | Function | Functional failure modes | Cause | HAZARD - Consequence at level of technical system | Consequences at train level |
|--|------------------------------|--|---|---|--|
| <p><i>For the purposes of this example, the failures of the driver are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change. It is thus assumed that the associated human factor aspects are properly analysed and controlled through the Safety Management System of the railway undertaking.</i></p> <p><i>For example, when the hot box detection function is achieved by a trainborne system, as Hot Box Events can occur at any moment of time and at any location of the track, operational procedures need be defined with the infrastructure manager (IM) in order to manage a safe stopping of the train at an appropriate and agreed location, including thus the necessity to enforce by the IM a speed reduction for trains on adjacent tracks in order to manage the risks caused by the blast at the crossing of two trains.</i></p> | | | | | |
| 1. | Trainborne Hot Box Detection | Detection does not start | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely. |
| 2. | | Detection starts when not required | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> Driver required to stop the train whereas not necessary Traffic operation disturbed |
| 3. | | | | | |
| 4. | | | | | |
| 5. | | Detection is delayed in response | <ul style="list-style-type: none"> Hot Box Detector failed Failure of indication system | Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety | In case of a Hot Box Event, the driver is informed too late and might not stop the train safely. |
| 6. | | Detection degraded (e.g. wrong output level) | | Not applicable. The hot box detection is a binary output | Not applicable. The hot box detection is a binary output |

A5.4 Broadly acceptable risks ? [§ 2.2.2 & § 2.2.3. in Annex I of Reg. 402/2013] ^[CSM-DT]

[G 1] The risks associated to failure modes 2, 3 and 6 do not result in an unsafe situation. They may thus be considered broadly acceptable from the safety point of view. In that case, they do not require the identification and implementation of any specific risk control measure. However, considering that a spurious detection of a hot box event stops the train when not necessary and disturbs the traffic operation, from the economic point of view the proposer might consider the associated risk as non-broadly acceptable.

Observation : the spurious detection of a Hot Box Event requires also the definition of “specific operational procedures” to be applied by the driver in such a case. It is worth noting that frequent spurious detections may result in real detections being unintentionally ignored. The overall risk assessment should consider that risk in the assessment of Human Factors.

[G 2] The risks associated to failure modes 1, 4 and 5 have the potential to result in an unsafe situation (fire or derailment) with fatalities. As the driver is not informed, or is informed too late, about a Hot Box Event, he cannot stop the train safely. Therefore, those risks are not broadly acceptable.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

Table 33: Assessment of risk acceptability within the functional FMEA of a trainborne Hot Box Detection.

| N° | HAZARD - Consequence at level of technical system | Consequences at train level | Consequences at train level - Potential accident | Potential for at least 1 fatality |
|--|---|--|---|--|
| <p><i>For the purposes of this example, the failures of the driver are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change. It is thus assumed that the associated human factor aspects are properly analysed and controlled through the Safety Management System of the railway undertaking.</i></p> <p><i>For example, when the hot box detection function is achieved by a trainborne system, as Hot Box Events can occur at any moment of time and at any location of the track, operational procedures need be defined with the infrastructure manager (IM) in order to manage a safe stopping of the train at an appropriate and agreed location, including thus the necessity to enforce by the IM a speed reduction for trains on adjacent tracks in order to manage the risks caused by the blast at the crossing of two trains.</i></p> | | | | |
| 1. | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely. | <ul style="list-style-type: none"> • Fire • Derailment | YES (i.e. risk not broadly acceptable) |
| 2. | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> • Driver required to stop the train whereas not necessary • Traffic operation disturbed | No – Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm | NO (i.e. risk is broadly acceptable) |
| 3. | | | | |
| 4. | | | | |
| 5. | Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety | In case of a Hot Box Event, the driver is informed too late and might not stop the train safely. | <ul style="list-style-type: none"> • Fire • Derailment | YES (i.e. risk not broadly acceptable) |
| 6. | Not applicable. The hot box detection is a binary output | Not applicable. The hot box detection is a binary output | Not applicable | Not applicable |

[G 3] The assessment of the risk acceptability is documented in Table 33 above. It is the same table as Table 31 and Table 32 above where the redundant lines, and columns not relevant for the risk acceptance, are masked and the last two columns are added.

A5.5 Selection of the risk acceptance principle [§ 2.1.4. in Annex I of Regulation 402/2013] ^[CSM-DT]

A5.5.1 Proposer's decision

[G 1] Regulation 402/2013 allows the proposer to select one risk acceptance principle among three for controlling the identified hazards and risks to an acceptable level :

- (a) use of relevant Codes of Practice;
- (b) comparison to similar Reference Systems, and;
- (c) use of Explicit Risk Estimation.

As the change under assessment is an innovative trainborne system, the proposer decides to carry out an Explicit Risk Estimation, based on one of the two categories of harmonised design targets defined in (EU) Regulation 2015/1136 [i.e. CSM-DT].

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

A5.5.2 Are harmonised design targets suitable for trainborne Hot Box Detection?

Approach of the question by point 2.5.5. in Annex I of Reg. 2015/1136

[G 1] According to point 2.5.5. in Annex I of Reg. 2015/1136, “*where hazards arise as a result of failures of functions of a technical system ...*” and “*where a failure has a credible potential to lead directly to ... a catastrophic ... or a critical accident*”, the most credible category of harmonised design targets (i.e. CSM-DT) can be setup as the quantitative requirement applicable for the design of the associated technical system.

In that case, “*the associated risk does not have to be reduced further if ...*” compliance with that quantitative design target is demonstrated.

[G 2] The term directly is defined as follows in point 2.5.8.(a) of Annex I in Reg. 2015/1136 : “*The term « directly » means that the failure of the function has the potential to lead to the type of accident referred to in point 2.5.5 without the need for additional failures to occur*”.

[G 3] The single failure of the Hot Box Detector “part” of the trainborne hot box detection function does not lead directly to a catastrophic consequence.

[G 4] **What are thus the conditions which have a credible potential to LEAD DIRECTLY to an accident in case of failure of the trainborne Hot Box Detection function?**

Based on the (preliminary) system definition in section § A5.1 above and the associated schematic representation of the “trainborne hot box detection function” (see Figure 41 above), it can be concluded that :

IF the following two conditions are met **during the same period of time** :

(a) the “trainborne hot box detection function” is failed. In practice this means :

- (1) either the trainborne “Hot Box Detector” is failed, or;
- (2) the indication of Hot Box Event is not transmitted to the driver through the communication means (e.g. wired connection or train bus), or;
- (3) both do not work any more;

AND

(b) the wheelset under the supervision of the considered technical system detecting the “Hot Box Event” is overheating;

THEN

(c) there is “*a credible potential to lead directly to a catastrophic accident*” ... “*typically affecting a large number of people and resulting in multiple fatalities*”.

As the driver is not informed about the Hot Box Event, he will not enforce a progressive train deceleration for stopping the train safely. All train passengers are therefore exposed to fire or train derailment risk.

[G 5] Although a combination of events and failures is necessary to lead to the catastrophic consequence (hence an “AND” in the condition above) in practice, it is still a hazard related to the trainborne hot box detection function. The harmonised design targets can thus be applied to derive from that condition the quantitative requirements which shall be used for the design of the trainborne Hot Box Detector.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- [G 6] Indeed, if the conditions listed in point [G 4] above are met during the same period of time, and if having in mind the definitions in Article 3(23) and 3(36) of Reg. 2015/1136, those conditions are included in the text of point 2.5.5. of Reg. 2015/1136, the following remains true :

the risk that a Hot Box Event is not detected by the trainborne hot box detection “*does not have to be reduced further if the frequency of ...*” occurrence of the conditions listed in point [G 4] of section § A5.5.2 above is “*... demonstrated to be less than or equal to 10^{-9} per operating hour*”.

- [G 7] Therefore, the risk is acceptable if the frequency of occurrence of the logical condition in point [G 4] of section § A5.5.2 above is “*... demonstrated to be less than or equal to 10^{-9} per operating hour*”. This is summarised in Figure 43 below.

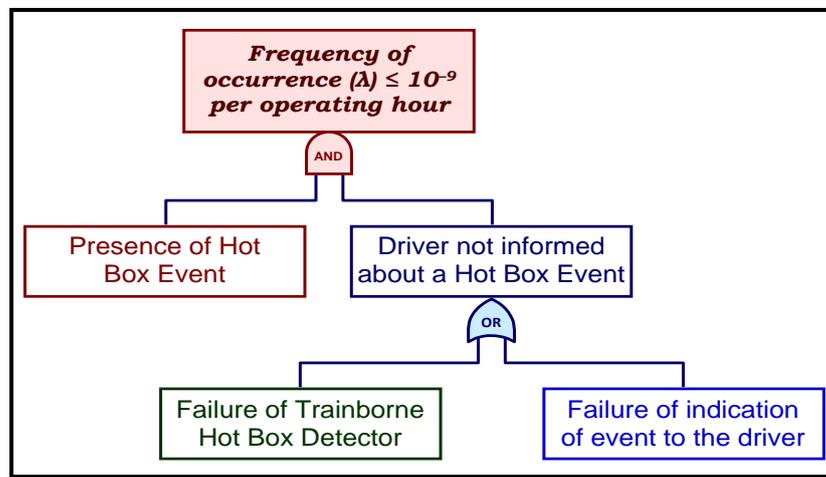


Figure 43: Logical condition leading directly to a failure of the trainborne hot box detection function.

Approach of the same question from another angle through point 2.5.9. of Reg. 2015/1136

- [G 8] The same question (i.e. *Are harmonised design targets suitable for trainborne Hot Box Detection?*) can be analysed from another angle.

Indeed, point 2.5.9. in Annex I of Reg. 2015/1136 permits also the use of harmonised design targets for deriving the quantitative requirements that shall applied to the design of the trainborne Hot Box Detector. Point 2.5.9 states that :

- (a) “*where the failure of a function of the technical system under assessment does not lead directly to the risk under consideration, ...*”

This condition is true. As explained in point [G 4] of section § A5.5.2 above, the single failure of either the trainborne Hot Box Detector or of the “the indication of the Hot Box Event to the driver” (or of both failures) does not result in the accident as long as the third condition is not fulfilled, i.e. as long as there is no Hot Box Event on the train.

- (b) “*... the application of less demanding design targets shall be permitted if the proposer can demonstrate that the use of barriers as defined in Article 3(34) allows the same level of safety to be achieved*”.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

[G 9] **What barriers external to the Hot Box Detection system under assessment are put in place to prevent the accident?**

- (a) The prevention of hazards causing the overheating of wheelsets and axleboxes is controlled by appropriate maintenance and operational procedures of the safety management system of the railway undertaking that operates those trains. Pre-departure checks, periodic planned maintenance inspections and preventive maintenance operations of Rolling Stock are put in place to prevent, detect and, when necessary, correct emerging failures of wheelsets and axleboxes (e.g. wheel bearing fatigue, loss of bearing lubrication in axleboxes, defective brakes or any other cause).
- (b) Those provisions in the SMS constitute barriers or “*risk control measures outside the system under assessment ...*” (i.e. outside the trainborne Hot Box Detector and Hot Box Event indication) “... *that either reduce the frequency of occurrence of the ...*” Hot Box “... *hazard or mitigate the severity of the potential consequences of that hazard*”.
- (c) The effectiveness of those external barriers/risk control measures has a direct impact on the actual frequency of occurrence of Hot Box Events. The proposer (i.e. railway undertaking) has statistics of the actual frequency of occurrence of Hot Box events for the fleet it manages. Those statistics reflect the effectiveness, and thus the level of protection, of the maintenance and operational procedures the railway undertaking has in place in the safety management system.
- (d) The knowledge of the frequency of occurrence of Hot Box Events can therefore be used to derive the permissible frequency of occurrence of failures of “the trainborne Hot Box Detector and Hot Box Event indication”.

- (e) Based on these inputs, the same conclusion can be deduced for the quantitative requirements that shall be used for the design of the trainborne Hot Box Detector :
 - (1) less demanding design targets than the ones set out in point 2.5.5. of Reg. 2015/1136 shall be permitted if the use of barriers outside the trainborne Hot Box Detection function (i.e. operational and maintenance risk control measures of the SMS) allows the same level of safety to be achieved as the one in point 2.5.5.
 - (2) the associated risk is then acceptable :

IF when the following conditions are met :

 - (i) the “trainborne hot box detection function” is failed. In practice this means that :
 - ↳ either the trainborne “Hot Box Detector” is failed, or;
 - ↳ the indication of Hot Box Event is not transmitted to the driver through the communication means (e.g. wired connection or train bus), or;
 - ↳ both do not work any more;

AND at the same time

 - (ii) the wheelset or axlebox under the supervision of the considered Hot Box Detector is overheating;

the frequency of occurrence of those conditions is “... *demonstrated to be less than or equal to 10^{-9} per operating hour*”. This can also be represented by Figure 43 above.

- [G 10] In conclusion, regardless of the angle from which the question is analysed, the conclusions are identical :

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (a) the harmonised design targets can be used for deriving the quantitative requirements to be used for the design of the trainborne Hot Box Detection function;
- (b) the permissible quantitative requirements for the trainborne Hot Box Detection are dependent on the frequency of occurrence of Hot Box Events (see point (d) below);
- (c) the frequency of occurrence of Hot Box Events is dependent on the effectiveness of operational and maintenance risk control measures (external to the technical system under assessment) to prevent or mitigate effectively wheelset and axlebox hazards. The continuous achievement of safety performance is ensured by the compliance with Regulation 1078/2012 on the CSM for monitoring;
- (d) the statistical return of experience through the monitoring of the SMS is an input information necessary to derive the permissible frequency of occurrence of failures of the trainborne Hot Box Detection function (“the trainborne Hot Box Detector and Hot Box Event indication”) : see Figure 43 above.

A5.5.3 Allocation of the most credible CSM-DT category

[G 1] The allocation of the most credible CSM-DT category is based on the potential consequence of the accident resulting from the identified risk.

[G 2] To help allocating the most credible CSM-DT category [i.e. either (10^{-9} h^{-1}) or (10^{-7} h^{-1})], it is necessary to consider the number of people exposed to risk and to answer the following two questions :

- (a) Is the “*accident typically affecting a large number of people and resulting in multiple fatalities*”?
If yes, the accident category is “catastrophic”; the first CSM-DT category (10^{-9} h^{-1}) applies.
- (b) Is the “*accident typically affecting a very small number of people and resulting in at least one fatality*”?
If yes, the accident category is “critical”; the second CSM-DT category (10^{-7} h^{-1}) applies.

[G 3] If the answer to those questions is not straight forward, answering the following equivalent questions might be of help :

- (a) Is the considered accident limited to a specific area of the train and thus exposes to risk only the passengers located in that area? or
- (b) Is the considered accident affecting the whole train and thus exposes to risk all train passengers or are other trains or many third parties external to the railway premises exposed to risk (e.g. persons living in the vicinity of the track in case of derailment)?

[G 4] Whatever set of questions is used, the answers are the same. The CSM-DT categories applicable for the different identified hazards are documented in Table 34 below.

[G 5] For this example, the consequence severity of every identified risk is already considered in the hazard identification and classification (see section § A5.3 above), the assessment of the acceptability of risks (see section § A5.4 above) and the assessment of the applicability of CSM-DT (see section § A5.5 above).

[G 6] The previous FMEA tables identify two different hazards with “*a credible potential to lead directly to a catastrophic accident*” (fire or derailment) :

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (a) 1st hazard : Hot Box Event not detected by technical system when required;
 (b) 2nd hazard : Hot Box Event may not be detected on time (i.e. the detection is delayed) to permit actions to be put in place to ensure the safety.

[G 7] As the second hazard relates anyway to the same possible consequence, that hazard can rather be considered as an additional possible cause of the first hazard. Therefore, these two hazards can be analysed as a single one.

Table 34: Allocation of the most credible CSM-DT category to the hazards identified in the FMEA.

| N° | HAZARD – Consequence at level of technical system | Consequences at train level | Consequences at system level - Potential accident | Potential for at least 1 fatality | Consequence limited to a specific area of train | Associated CSM-DT |
|--|---|--|---|--|---|----------------------------------|
| <p><i>For the purposes of this example, the failures of the driver are neither considered nor the associated risk control measures proposed. This FMEA only focusses on the technical aspects of the change. It is thus assumed that the associated human factor aspects are properly analysed and controlled through the Safety Management System of the railway undertaking.</i></p> <p><i>For example, when the hot box detection function is achieved by a trainborne system, as Hot Box Events can occur at any moment of time and at any location of the track, operational procedures need be defined with the infrastructure manager (IM) in order to manage a safe stopping of the train at an appropriate and agreed location, including thus the necessity to enforce by the IM a speed reduction for trains on adjacent tracks in order to manage the risks caused by the blast at the crossing of two trains.</i></p> | | | | | | |
| 1. | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely. | <ul style="list-style-type: none"> • Fire • Derailment | YES (i.e. risk not broadly acceptable) | NO (whole train exposed to risk) | 10 ⁻⁹ h ⁻¹ |
| 2. | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> • Driver required to stop the train whereas not necessary • Traffic operation disturbed | No – Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm | NO (i.e. risk is broadly acceptable) | Not applicable | Not applicable |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety | In case of a Hot Box Event, the driver is informed too late and might not stop the train safely. | <ul style="list-style-type: none"> • Fire • Derailment | YES (i.e. risk not broadly acceptable) | NO (whole train exposed to risk) | 10 ⁻⁹ h ⁻¹ |
| 6. | Not applicable. The hot box detection is a binary output | Not applicable. The hot box detection is a binary output | Not applicable | Not applicable | Not applicable | Not applicable |
| <p>Remark: In practice all FMEA tables above [Table 31, Table 32 and Table 33 above], including the present one, are one single table where columns are added to address every additional need. However for the purpose of this example, and to facilitate the reading and understanding of the analysis, only the relevant lines and columns were kept. The other ones were masked.</p> | | | | | | |

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

[G 8] In conclusion, as explained in two different ways in section § A5.5.2 above and Figure 43 above, if following **“logical condition”** is met:

(a) the wheelset or axlebox under the supervision of the considered Hot Box Detector “Hot Box Event” is overheating;

AND during the same period of time⁽²¹⁾

(b) either the Hot Box Detector is defective and does not report the event **OR** there is a failure of “indication of the Hot Box Event to the driver” or both of these failures;

there is *“a credible potential to lead directly to a catastrophic accident” ... “typically affecting a large number of people and resulting in multiple fatalities”*

[G 9] The associated risk is acceptable if the frequency of occurrence of that logical condition is *“... demonstrated to be less than or equal to 10⁻⁹ per operating hour”*. The most credible CSM-DT category **applicable to that logical condition** is therefore 10⁻⁹ h⁻¹.

A5.6 Apportionment of the CSM-DT value to the different contributing parts of the logical condition [§ 2.2.5. in Annex I of Reg. 402/2013]^[CSM-DT]

A5.6.1 Supporting tools – Use of Fault Tree Analysis (FTA) techniques

[G 1] The different causes of the non-detection of a Hot Box Event are already implicitly identified by the hazard identification and classification (see section § A5.3 above) and during the assessment of the acceptability of risks (see section § A5.4 above) and of the applicability of CSM-DT (see section § A5.5 above) to the system under assessment.

[G 2] In practice, Fault Tree Analyses (FTAs) can be used to identify and analyse systematically all conditions and factors that can cause or may potentially cause or contribute to the occurrence of a defined undesired event, called in the FTA terminology “top event”. For more information about the FTA tool, refer to the Appendix in section § A5.10.2 below. Other methods than fault tree analyses are also usable for the allocation of quantitative design targets.

[G 3] In practice, the building/modelling, reduction and calculation of the FTA are performed using specific software tools. Usually, those tools enable also to calculate the sensitivity of the top event and to determine the most critical contributing causes.

A5.6.2 FTA of the trainborne Hot Box Detection function and available information

[G 1] From the risk assessment in the sections above, it results that the risk associated to failures of the trainborne Hot Box Detector is acceptable if the frequency of occurrence of the logical condition in point [G 8] of section § A5.5.3 above is *less than or equal to 10⁻⁹ per operating hour* (see also Figure 41 above).

⁽²¹⁾ *“During the same period of time” means that the “hot box detector has failed” AND either the failure is not yet detected OR the hot box detector is not yet repaired at the moment when the hot box event also occurs.*

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- [G 2] The logical condition expressed in Figure 41 above can be modelled by the FTA in Figure 44 below. This FTA identifies and analyses systematically the conditions and factors that can cause or may potentially cause or contribute to the occurrence of the event “driver not aware of a Hot Box Event” (i.e. “non-detection of a Hot Box Event”). The building of this logical tree is based on the system definition which shall describe the functioning and the architecture of the trainborne Hot Box Detection function.

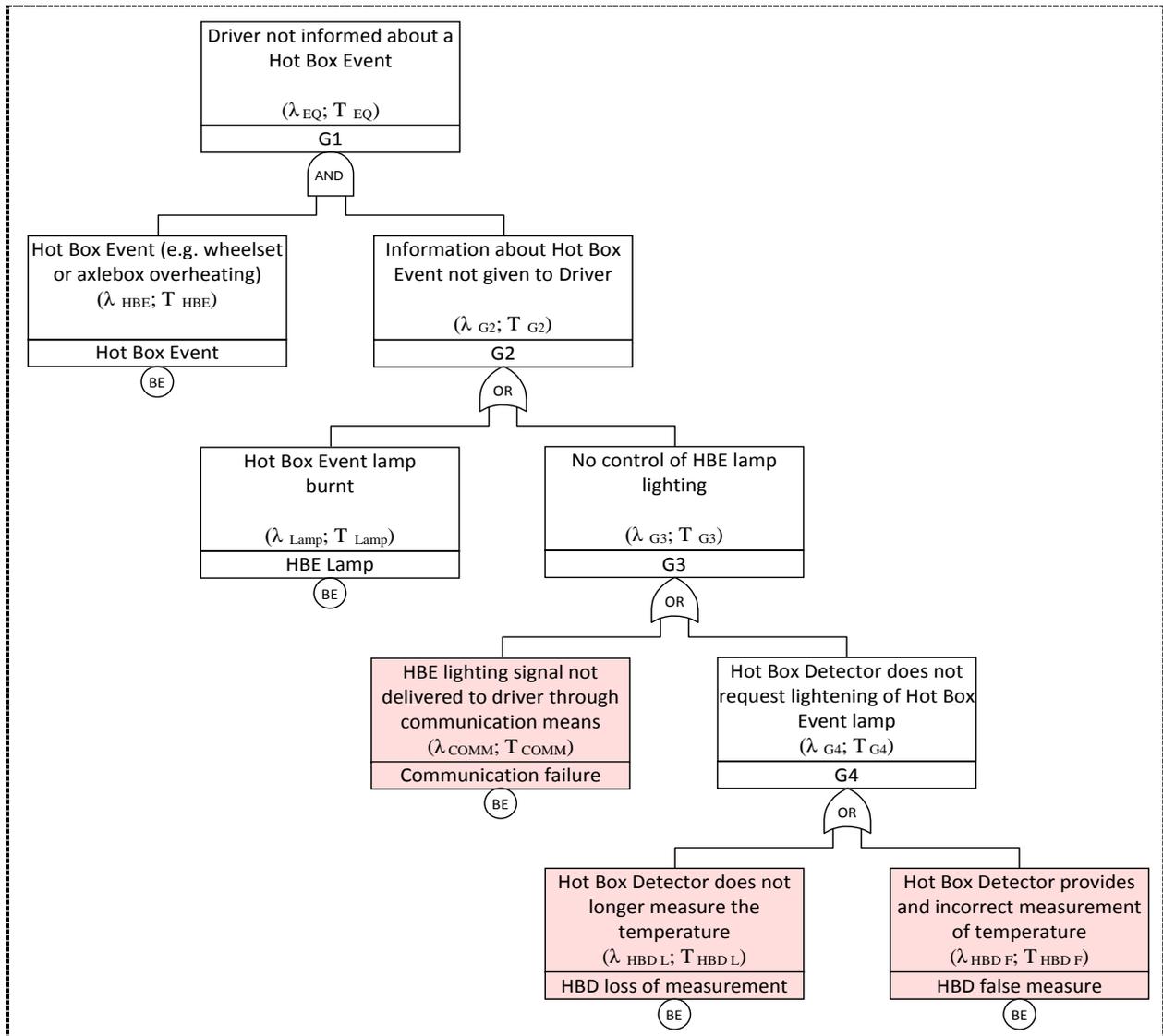


Figure 44: Fault Tree of the trainborne Hot Box Detection function with one detector.

- [G 3] **Qualitative analysis of the FTA :** confirms the conclusions of the risk assessment above
- When a Hot Box Event occurs** due for example to the overheating of a wheelset or an axlebox, the hazard might be undetected, **if during the same period of time**, the following failures also occur (this is the **AND gate** in the FTA in Figure 44) :
- (a) the lamp indicating to the driver a Hot Box Event is burnt;
- OR**

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (b) the signal controlling the lighting of the Hot Box Event lamp is not delivered by the used communication means (e.g. a wired connection or a train bus);

OR

- (c) the Hot Box Detector is defective and does not longer measure the temperature of the wheelset and axlebox;

OR

- (d) the Hot Box Detector is partially defective and measures an incorrect value of temperature below the ceiling that triggers the detection signal.

- [G 4] **Quantitative analysis of the FTA** shall be used in practice for deriving the quantitative requirements to be applied for the design of the trainborne Hot Box Detection function.

The maximum permissible frequency of occurrence of the top event is specified in section [G 1] above: *“The risk associated to the absence of detection of a Hot Box Event is acceptable if the frequency of occurrence of those simultaneous events is less than or equal to 10^{-9} per operating hour”*.

This 10^{-9} h^{-1} value, and the formulas in the Appendix in section § A5.10.3 below, can then be used for deriving the maximum permissible frequency of occurrence, and for setting up any other relevant safety requirements, for the different contributors of the trainborne Hot Box Detection function.

- [G 5] **What other input information does the proposer have for the FTA?**

- (a) the target value for the top event is known [10^{-9} h^{-1}]: see point [G 4];
- (b) the frequency of occurrence of Hot Box Events can be derived from the proposer’s experience (REX) and the monitoring of those events on similar trains.

As explained in the previous sections [see point [G 9] in section § A5.5.2 above], operational and maintenance provisions are put in place in the railway undertaking SMS. Either when taking the train for the first journey of the day or during regular monthly maintenance activities, verifications are done to detect failures of wheelsets and axleboxes that can cause or may potentially cause a hot box event.

The driver is also trained to be able to detect some unusual changes of the dynamic behaviour of the train or suspicious train vibrations.

- (c) the failure rate of the Hot Box Event lamp can be taken from relevant standards for the right category of lamp used for the purpose;
- (d) the safety requirements, including the quantitative targets, for the design of the Hot Box Detector need then to be derived from the FTA in Figure 44 above and the formulas in the Appendix in section § A5.10.3 below.

In practice, specific software tools are used for building/modelling and calculating the FTA. Those formulas are included in the tool. So the calculations do not need to be done manually.

- [G 6] Table 35 below summarises an example of available RAMS input information.

**Annex 5 : Agency example on the use of CSM-DT
(Trainborne Hot Box Detection System)**

Table 35: Example of available RAMS input information.

| N° | Basic events | Description in the FTA | Rate of occurrence | Source of information | D&NT ⁽²²⁾ | Mean D&NT | Additional explanations |
|----|-------------------------|--|-------------------------------------|--|----------------------|-----------|--|
| 1. | Hot Box Event | Hot Box Event (e.g. wheelset or axlebox) overheating (<i>this shall trigger the hot box detection</i>) | 10^{-5} h^{-1} | Monitoring through experience on similar trains (REX) | 10 h | 5h | Operational and maintenance provisions are put in place in the RU SMS to permit the detection of wheelset and axlebox failures for the first journey with the train (i.e. pre-departure checks). The driver is also trained for detecting unusual changes of dynamic behaviour of the train and suspicious train vibrations |
| 2. | HBE lamp | Hot Box Event lamp burnt | 10^{-7} h^{-1} | IEC 62380 standard | 10 h | 5h | The driver's cabin is tested every day, including the good functioning of the Hot Box Event indication lamp. Diversity in the indication can also be envisaged, e.g. use of two lamps – one for indicating a Hot Box Event, the other one for informing that the Hot Box Detection system is defective |
| 3. | HBD loss of measurement | Hot Box Detector does not longer detects measure the temperature | To define by risk assessment | Shall be demonstrated by the supplier of Hot Box Detector | 300 h | 150 h | To be tested once a month during regular maintenance activities. This could be an initial objective in order not to constraint the train operation based on this data. Then depending on the final failure rate allocated by the risk assessment (e.g. if it appears not to be feasible), this number may be changed for example by imposing more constraints on either the train operation or on the maintenance of the Hot Box Detection functionality. |
| 4. | HBD false measure | Hot Box Detector provides an incorrect temperature measurement | To define by risk assessment | Shall be demonstrated by the supplier of Hot Box Detector | 300 h | 150 h | To be tested once a month during regular maintenance activities |
| 5. | Communication failure | HBE lighting signal not delivered to driver through communication means | To define by risk assessment | Shall be verified for implementation of Hot Box Detection function | 300 h | 150 h | Different technical options are possible for informing the driver. The communication of information shall satisfy the requirements identified in the current risk assessment |

⁽²²⁾ *D&NT designates the maximum “Detection plus Negation Time”, i.e. the maximum time necessary for detecting the failure of the defective component, repairing and testing before returning it to service. The formulas in the Appendix in section § A5.10.3 use the mean Detection plus Negation Time; it is based on the assumption that statistically **in average** a failure will occur at the half of the detection time interval.*

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

Assumptions for the risk assessment in Table 35 above :

- (a) trains are operated 10 hours a day. The mean detection and negation time is then 5 h for the failures detectable by the daily tests;
- (b) trains are operated 30 days a month; the regular monthly maintenance activities take place every 300 hours of operation. The mean detection and negation time is then 150 h for the failures detectable during the periodic planned maintenance.
- (c) when the train is not in operation, there is no degradation of the failure rate of the trainborne hot box detection system;
- (d) when a failure is detected during daily tests or planned periodic maintenance, the train is not returned to operation before all failures are repaired and the system is completely tested. The time to repair is thus not considered in the calculations.

A5.6.3 Setting up the safety requirements for the Hot Box Detector – Alternative solutions

A5.6.3.1 Communication means for indication of Hot Box Event

[G 1] The risk assessment identifies the failure of the chosen “communication mean” as a possible cause for the absence of indication of a Hot Box Event to the driver. This cause is a sub-hazard of the main hazard identified earlier in the risk assessment.

[G 2] Depending on the used option for implementing the indication sub-function of the Hot Box Detection function, the risk control measures for the sub-hazard are different :

- (a) **Technical option N 1** : communication of the message through a wired connection

The proposer decides to use well-known codes of practice which enable to :

- (1) transfer to the train driver the indication about a detected Hot Box Event;
- (2) inform the driver about the interruption of the wired connection and therefore about the loss of indication of a possible Hot Box Event.

- (b) **Technical option N 2** : communication of the message through the train bus

Depending on whether the train communication bus is a safe or non-safe transmission means, different types of risk control measures will have to be implemented.

For the current examples, let us consider the train bus as a non-safe transmission means. The “indication of the detection of a Hot Box Event” to the driver shall then be protected against the following possible threats and transmission errors :

- (1) repetition of messages;
- (2) deletion or loss of messages;
- (3) insertion of messages;
- (4) resequencing or wrong sequence of messages;
- (5) corruption or data falsification of messages;
- (6) delaying of messages;
- (7) masquerade⁽²³⁾ of messages;

⁽²³⁾ *Masquerade is a type of inserted message [by another (unknown) source] which is a non-authentic message but which could appear to be authentic and is possibly unsafe.*

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

To reduce at an acceptable level the risk associated with the threats listed in the preceding section, the proposer can use well known codes of practice with appropriate protective measures for :

- (8) message authenticity;
- (9) message integrity;
- (10) message timeliness;
- (11) message sequence;

The CENELEC EN 50159 standard suggests the following set of known defences :

- (12) sequence numbering;
- (13) time stamping;
- (14) use of time-out;
- (15) feedback messages between transmitter and receiver;
- (16) source and destination identifiers;
- (17) identification procedures;
- (18) use of safety codes (CRC checks);
- (19) cryptographic techniques.

Implementing those defences, allows to consider that the remaining or residual risk of “loss of indication of a detected Hot Box Event to the driver” is reduced to an acceptable level.

Whatever of these two technical options is chosen, relevant operational procedures need to be written to define the actions to be taken by the driver in case of loss of the communication means between the Hot Box Detectors and the driver’s cabin.

[G 3] The demonstration of compliance with those safety requirements allows therefore the non-quantification of the basic event “communication failure” in the FTA in Figure 44.

[G 4] **Remark :** the mechanical constraints (size, weight, etc.) and physical interface between the Hot Box Detector and the train shall also be specified and communicated to the manufacturer to permit a safe integration of the Hot Box Detector into the train once it will be manufactured, supplied, installed and used.

A5.6.3.2 Case 1 : safety requirements when using a single Hot Box Detector

[G 1] Input data for the FTA :

- (a) The values from Table 35 above are introduced into the FTA in Figure 44 above. Then, the FTA is calculated with the formulas in the Appendix in section § A5.10.3 below.

In practice, specific software tools are used for building/modelling and calculating the FTA. Those formulas are included in the tool and the calculations are automatic.

- (b) The top event in the FTA can then be calculated for different values of the failure rate of the Hot Box Detector. The mean detection plus negation time is used in those formulas, assuming therefore that statistically in average a failure will occur at the half of the detection time interval.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

[G 2] **Results from the calculations :** $\lambda_{TOP\ EVENT}$ shall be less than $10^{-9} h^{-1}$

The permissible quantitative requirement for the Hot Box Detector can then be obtained by simulating the frequency of occurrence achieved by the top event when modifying the value of the failure rates for the two contributing failure modes of the Hot Box Detector (i.e. $\lambda_{HBD\ L}$ and $\lambda_{HBD\ F}$ with the assumption the overall failure rate of the Hot Box Detector [$\lambda_{HBD\ Total}$] is apportioned equally [50 %] to each failure mode).

Table 36: FTA results with one Hot Box Detector.

| Input data | Iteration of possible values for HBD | | | Achieved top event |
|-----------------------------------|---|--|--|---|
| | $\lambda_{HBD\ Total}$ (100%) | $\lambda_{HBD\ F}$ (50%) | $\lambda_{HBD\ L}$ (50%) | $\lambda_{TOP\ EVENT}$ |
| $T_{HBD\ L} = 300\ h$ | $2.0 \cdot 10^{-7} h^{-1}$ | $1.0 \cdot 10^{-7} h^{-1}$ | $1.0 \cdot 10^{-7} h^{-1}$ | $3.2 \cdot 10^{-10} h^{-1}$ |
| $T_{HBD\ F} = 300\ h$ | $4.0 \cdot 10^{-7} h^{-1}$ | $2.0 \cdot 10^{-7} h^{-1}$ | $2.0 \cdot 10^{-7} h^{-1}$ | $6.3 \cdot 10^{-10} h^{-1}$ |
| $\lambda_{HBE} = 10^{-5} h^{-1}$ | $6.0 \cdot 10^{-7} h^{-1}$ | $3.0 \cdot 10^{-7} h^{-1}$ | $3.0 \cdot 10^{-7} h^{-1}$ | $9.4 \cdot 10^{-10} h^{-1}$ |
| $\lambda_{Lamp} = 10^{-7} h^{-1}$ | $7.0 \cdot 10^{-7} h^{-1}$ | $3.5 \cdot 10^{-7} h^{-1}$ | $3.5 \cdot 10^{-7} h^{-1}$ | $1.1 \cdot 10^{-9} h^{-1}$ |
| $T_{HBE} = 10\ h$ | (A detected hot box event is repaired within one day) | | | |
| $T_{Lamp} = 10\ h$ | (The HBE lamp is tested every day) | | | |

[G 3] **Analysis of the results from the FTA and the risk assessment**

- (a) the maximum permissible frequency of occurrence of the top event is achieved (i.e. less than $10^{-9} h^{-1}$) if the following requirements are fulfilled :
- (1) the total failure rate of the Hot Box Detector is less than $6 \cdot 10^{-7} h^{-1}$. It corresponds to the equivalent failure rate of gate G4 in the FTA in Figure 44;
 - (2) the Hot Box Detector is tested completely every 300 h of operation. This is the "Detection plus Negation Time" for the maintenance activities on wheelsets and axleboxes. The FTA calculations use the mean detection plus negation time (see footnote (22) above on page 124);
 - (3) the Hot Box Event lamp is tested every day (i.e. every 10 hours of operation);
- (b) a failure rate of $6 \cdot 10^{-7} h^{-1}$ is a demanding quantitative safety requirement for the Hot Box Detector. The value is at the border between SIL 2 and SIL 3 requirements for a technical system in the CENELEC 5012x standards⁽²⁴⁾. In addition to that, the Hot Box Detector must be tested completely, and if necessary its functionality restored, every 300 hours during dedicated monthly maintenance activities.

⁽²⁴⁾ This is the Table A.1 of the SIL-Table in Annex A of the CENELEC 50129:2003 standard.

Table A.1 – SIL-table

| Tolerable Hazard Rate – THR – per hour and per function | Safety Integrity Level – SIL |
|--|---------------------------------|
| $10^{-9} \leq THR < 10^{-8}$ | 4 |
| $10^{-8} \leq THR < 10^{-7}$ | 3 |
| $10^{-7} \leq THR < 10^{-6}$ | 2 |
| $10^{-6} \leq THR < 10^{-5}$ | 1 |

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

A5.6.3.3 Case 2 : safety requirements when using redundant Hot Box Detectors

[G 1] If the cost of a non-redundant Hot Box Detector architecture, with demanding safety requirements and short maintenance intervals, is not acceptable, the use of redundant Hot Box Detectors with higher frequency of occurrence of failure, tested also at longer maintenance intervals, can be considered.

[G 2] Also, if the loss of the Hot Box Detector during the operation is not acceptable, the Hot Box Detector function needs to be duplicated. Indeed, without redundancy of detection (see option in section § A5.6.3.2 above), the loss of the Hot Box Detection might not only disturb traffic operation but requires also unplanned corrective maintenance to be done.

This is a significant difference between the existing infrastructure hot box detection system and the trainborne hot box detection system under assessment :

(a) existing infrastructure hot box detection system : failures of “trackside hot box detectors” are controlled by installing detectors at regular distances along the railway line. This architectural choice of the infrastructure allows to tolerate failures of one “trackside hot box detector” as another detector is crossed after a defined distance. So, although a “hot wheelset or axlebox” might occur in the vicinity of a malfunctioning “trackside hot box detector”, the Hot Box Event remains undetected only during the time needed to reach the next trackside hot box detector.

(b) new trainborne Hot Box Detection system : if a non-redundant Hot Box Detector fails, then a hot box event can no longer be detected on the train as long as the detector is not repaired.

[G 3] With a redundant detection of the Hot Box Event, the logical condition expressed in Figure 41 above can be modelled by the FTA in Figure 45 below. Compared to the FTA in Figure 44 above, the gates G5 and G6 are added to model the manner failures of the two Hot Box Detectors can contribute to the occurrence of the “non detection of a Hot Box Event”.

Common Cause Failure analysis requirements

[G 4] The FTA in Figure 45 below, and the formulas in the Appendix in section § A5.10.3 below, require that the failures of the two Hot Box Detectors are independent with respect to random faults. Although the two Hot Box Detectors are physically independent, when subject to the same external influences (e.g. environmental stresses such as electromagnetic interferences – [EMI], electrostatic discharge [ESD], climatic, mechanical and chemical conditions or power supply fluctuations) they might fail in the same way (e.g. drift of detection threshold) and not detect a Hot Box Event.

Requirements from CCF-Analysis : to mitigate the risk of non-detection of a Hot Box Event by the two Hot Box Detectors, the temperature sensors of the two Hot Box Detectors shall either be of different technology (or suppliers) or from a different manufacturing batch. This requires also different labelling of products and a proper configuration management process.

**Annex 5 : Agency example on the use of CSM-DT
(Trainborne Hot Box Detection System)**

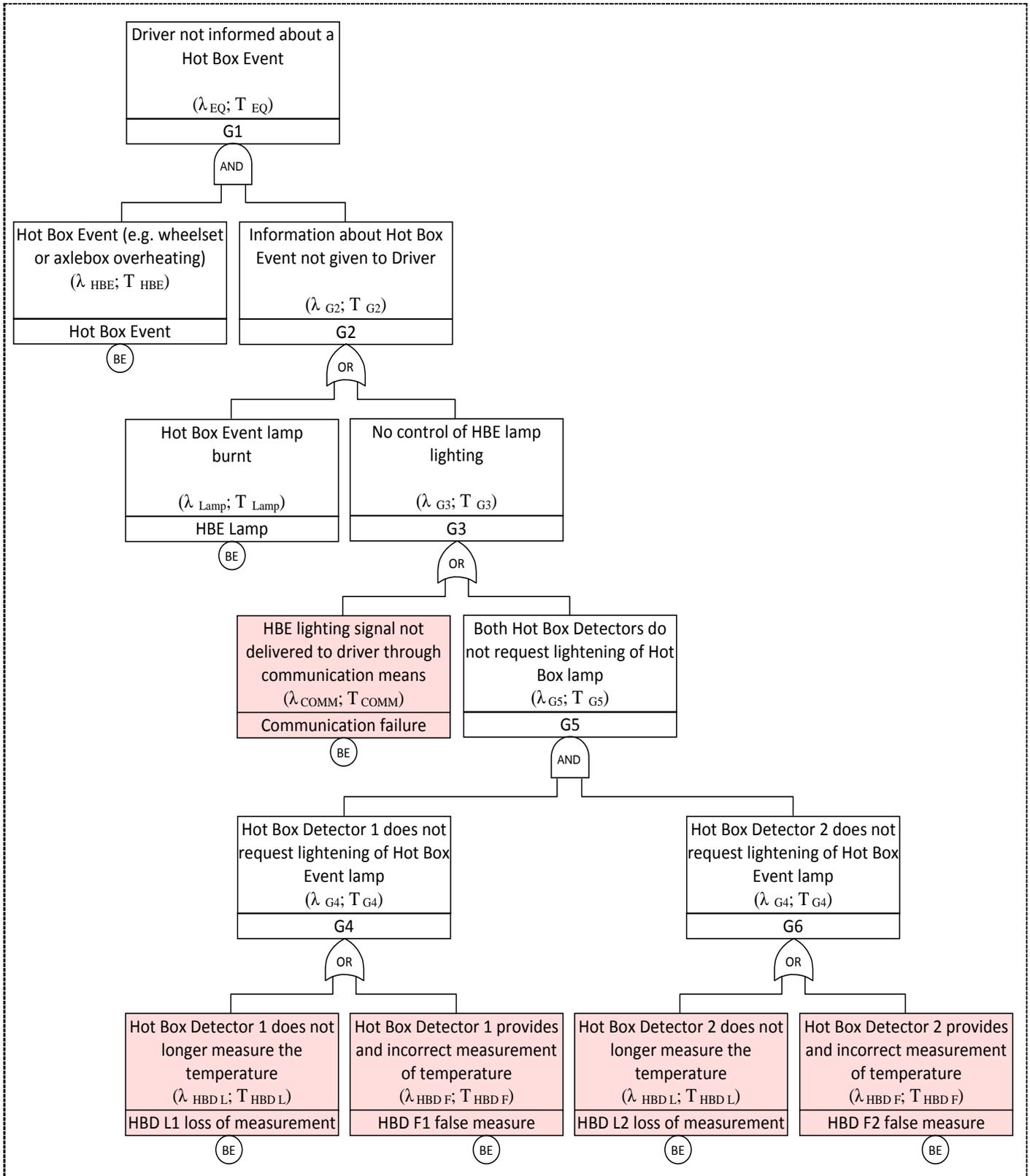


Figure 45: Fault Tree of a redundant trainborne Hot Box Detection function.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

[G 5] Input data for the FTA :

- (a) The values from Table 35 above are introduced into the FTA in Figure 45 above. Then, the FTA is calculated with the formulas⁽²⁵⁾ in the Appendix in section § A5.10.3 below.
- (b) The top event in the FTA can then be calculated for different values of the failure rate of the Hot Box Detector. The mean detection plus negation time is used in those formulas, assuming therefore that statistically in average a failure will occur at the half of the detection time interval.
- (c) The calculations below are done with two different values of this test interval :
 - (1) monthly test interval, i.e. $T_{HBD L} = T_{HBD F} = 300$ h in the FTA in Figure 45;
 - (2) 6 month test interval, i.e. $T_{HBD L} = T_{HBD F} = 3600$ h in the FTA in Figure 45.

[G 6] Results of calculation with a monthly test interval : $\lambda_{TOP EVENT}$ shall be less than $10^{-9} h^{-1}$

The permissible quantitative requirement for the Hot Box Detector can then be obtained by simulating the frequency of occurrence achieved by the top event when modifying the value of the failure rates for the two contributing failure modes of the Hot Box Detector (i.e. $\lambda_{HBD L}$ and $\lambda_{HBD F}$ with the assumption that the overall failure rate of the Hot Box Detector [$\lambda_{HBD Total}$] is apportioned equally [50 %] to each failure mode).

Table 37: FTA results with redundant Hot Box Detectors – Test interval 300 h.

| Input data | Iteration of possible values for HBD | | | Achieved top event |
|-----------------------------------|--|--|--|--|
| | $\lambda_{HBD Total}$ (100%) | $\lambda_{HBD F}$ (50%) | $\lambda_{HBD L}$ (50%) | $\lambda_{TOP EVENT}$ |
| $T_{HBD L} = 300$ h | $2.0 \cdot 10^{-5} h^{-1}$ | $1.0 \cdot 10^{-5} h^{-1}$ | $1.0 \cdot 10^{-5} h^{-1}$ | $1.06 \cdot 10^{-10} h^{-1}$ |
| $T_{HBD F} = 300$ h | $4.0 \cdot 10^{-5} h^{-1}$ | $2.0 \cdot 10^{-5} h^{-1}$ | $2.0 \cdot 10^{-5} h^{-1}$ | $3.94 \cdot 10^{-10} h^{-1}$ |
| $\lambda_{HBE} = 10^{-5} h^{-1}$ | $6.0 \cdot 10^{-5} h^{-1}$ | $3.0 \cdot 10^{-5} h^{-1}$ | $3.0 \cdot 10^{-5} h^{-1}$ | $8.74 \cdot 10^{-10} h^{-1}$ |
| $\lambda_{Lamp} = 10^{-7} h^{-1}$ | $7.0 \cdot 10^{-5} h^{-1}$ | $3.5 \cdot 10^{-5} h^{-1}$ | $3.5 \cdot 10^{-5} h^{-1}$ | $1.19 \cdot 10^{-9} h^{-1}$ |
| $T_{HBE} = 10$ h | <i>(A detected hot box event is repaired within one day)</i> | | | |
| $T_{Lamp} = 10$ h | <i>(The HBE lamp is tested every day)</i> | | | |

[G 7] Analysis of those results from the FTA and the risk assessment in Table 37 above :

- (a) the maximum permissible frequency of occurrence of the top event is achieved (i.e. less than $10^{-9} h^{-1}$) if the following requirements are fulfilled :
 - (1) the total failure rate of the Hot Box Detector is less than $6 \cdot 10^{-5} h^{-1}$. It corresponds to the equivalent failure rate of gates G4 and G6 in the FTA in Figure 45;
 - (2) the Hot Box Detector is tested completely every 300 h of operation. This is the “Detection plus Negation Time” for the maintenance activities on wheelsets and axleboxes. The FTA calculations use the mean detection plus negation time (see footnote (22) above on page 124);

⁽²⁵⁾ In practice, as for section § A5.6.3.2, specific software tools are used for building/modelling and calculating the FTA. The formulas are included in the tool and the calculations are automatic. The permissible quantitative requirement for the Hot Box Detector can then be obtained by simulating the frequency of occurrence achieved by the top event when modifying the value of the failure rates for the two contributing failure modes of the Hot Box Detectors.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- (3) the Hot Box Event lamp is tested every day (i.e. every 10 hours of operation);
- (b) a failure rate of $6 \cdot 10^{-5} \text{ h}^{-1}$ is a less demanding quantitative safety requirement for the Hot Box Detector than for the technical option in section § A5.6.3.2 above (difference of two orders of magnitude compared to $6 \cdot 10^{-7} \text{ h}^{-1}$). **But the Hot Box Detector must still be tested completely**, and if necessary its functionality restored, **every 300 hours** of operation during dedicated **monthly maintenance activities**. This time interval can still be considered short or too demanding.

[G 8] **Results of calculation** with a 6 month test interval : $\lambda_{\text{TOP EVENT}}$ shall be less than 10^{-9} h^{-1}

The permissible quantitative requirement for the Hot Box Detector can then be obtained by simulating the frequency of occurrence achieved by the top event when modifying the value of the failure rates for the two contributing failure modes of the Hot Box Detector (i.e. $\lambda_{\text{HBD L}}$ and $\lambda_{\text{HBD F}}$ with the assumption the overall failure rate of the Hot Box Detector [$\lambda_{\text{HBD Total}}$] is apportioned equally [50 %] to each failure mode).

Table 38: FTA results with redundant Hot Box Detectors – Test interval 3600 h.

| Input data | Iteration of possible values for HBD | | | Achieved top event |
|--|---|------------------------------------|------------------------------------|---|
| | $\lambda_{\text{HBD Total}} (100\%)$ | $\lambda_{\text{HBD F}} (50\%)$ | $\lambda_{\text{HBD L}} (50\%)$ | $\lambda_{\text{TOP EVENT}}$ |
| $T_{\text{HBD L}} = 3600 \text{ h}$ | $2.0 \cdot 10^{-6} \text{ h}^{-1}$ | $1.0 \cdot 10^{-6} \text{ h}^{-1}$ | $1.0 \cdot 10^{-6} \text{ h}^{-1}$ | $1.40 \cdot 10^{-10} \text{ h}^{-1}$ |
| $T_{\text{HBD F}} = 3600 \text{ h}$ | $4.0 \cdot 10^{-6} \text{ h}^{-1}$ | $2.0 \cdot 10^{-6} \text{ h}^{-1}$ | $2.0 \cdot 10^{-6} \text{ h}^{-1}$ | $5.31 \cdot 10^{-10} \text{ h}^{-1}$ |
| $\lambda_{\text{HBE}} = 10^{-5} \text{ h}^{-1}$ | $5.0 \cdot 10^{-6} \text{ h}^{-1}$ | $2.5 \cdot 10^{-6} \text{ h}^{-1}$ | $2.5 \cdot 10^{-6} \text{ h}^{-1}$ | $8.25 \cdot 10^{-10} \text{ h}^{-1}$ |
| $\lambda_{\text{Lamp}} = 10^{-7} \text{ h}^{-1}$ | $6.0 \cdot 10^{-6} \text{ h}^{-1}$ | $3.0 \cdot 10^{-6} \text{ h}^{-1}$ | $3.0 \cdot 10^{-6} \text{ h}^{-1}$ | $1.18 \cdot 10^{-9} \text{ h}^{-1}$ |
| $T_{\text{HBE}} = 10 \text{ h}$ | (A detected hot box event is repaired within one day) | | | |
| $T_{\text{Lamp}} = 10 \text{ h}$ | (The HBE lamp is tested every day) | | | |

[G 9] **Analysis of those results from the FTA and the risk assessment in Table 38 above :**

- (a) the maximum permissible frequency of occurrence of the top event is achieved (i.e. less than 10^{-9} h^{-1}) if the following requirements are fulfilled :
- (1) the total **failure rate of the Hot Box Detector is less than $5 \cdot 10^{-6} \text{ h}^{-1}$** . It corresponds to the equivalent failure rate of gates G4 and G6 in the FTA in Figure 45;
 - (2) the **Hot Box Detector is tested completely every 3600 h** of operation (6 months). This is the “*Detection plus Negation Time*” for the maintenance activities on wheelsets and axleboxes. The FTA use the mean detection plus negation time (see footnote (22) above on page 124);
 - (3) the Hot Box Event lamp is tested every day (i.e. every 10 hours of operation);
- (b) a failure rate of $5 \cdot 10^{-6} \text{ h}^{-1}$ is a less demanding quantitative safety requirement for the Hot Box Detector than for the technical option in section § A5.6.3.2 above (difference of one order of magnitude compared to $6 \cdot 10^{-7} \text{ h}^{-1}$). In addition to that, the complete set of tests and inspections of Hot Box Detectors, and if necessary the restoring of their functionality, can be realised every 3600 hours during the “6 month maintenance activities”. This time interval is 6 times longer than in the previous two cases.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

A5.6.3.4 Final decision on the (safety) requirements for the trainborne Hot Box Detectors

- [G 1] Several alternative technical options and sets of safety requirements, with corresponding acceptable maintenance intervals, are analysed in the previous sections. The final proposer's decision on which technical solution to use, and thus on the necessary accompanying maintenance activities at defined intervals, needs to be taken based on a balance between the following considerations :
- (a) the cost of the Hot Box Detector. The higher the quantitative safety requirement is, the more expensive the technical equipment is;
 - (b) the frequency, testability and maintenance costs of the Hot Box Detector;
 - (c) the availability of the Hot Box Detector and whether it is acceptable or not that a loss of the a non-redundant Hot Box Detector disturbs the traffic operation.

A5.7 Completeness of the risk assessment ^[CSM-DT]

- [G 1] The purpose of the risk assessment of the trainborne Hot Box Detection function is to define the quantitative safety requirements to be applied for the design of trainborne Hot Box Detectors, based on the categories of harmonised design targets defined in Regulation 2015/1136. Those quantitative safety requirements cover only the random hardware failure rate of the Hot Box Detector.
- [G 2] Although the risk assessment in the sections above goes beyond the scope of CSM-DT, it is not entirely complete. For example, in order to be able to install and integrate safely the Hot Box Detection function in the train, additional requirements, including other specific safety requirements, need to be defined by the overall risk assessment. Among others :
- (a) to comply with point (b) in point 2.5.7. in the Annex of Regulation 2015/1136, "*the risks associated with the systematic failures and systematic faults of the ...*" Hot Box Detector need also to be "*... controlled in accordance with safety and quality processes commensurate with the harmonised design target ...*" selected in section § A5.6 above. See section § 3.above for more details.
 - (b) as already mentioned in the sections above, the mechanical constraints (size, weight, etc.) and physical interface requirements between the Hot Box Detector and the train shall also be specified and communicated to the manufacturer;
 - (c) based on the architecture of the rolling stock, among others installation constraints need to be defined (e.g. the most appropriate location on the bogies) in order to :
 - (1) enable the detection by the same Hot Box Detector of the overheating of all four wheelsets of the monitored bogey;
 - (2) control the risks of damaging either :
 - (i) the Hot Box Detector housing, or;
 - (ii) the wiring interface for the indication to the driver of a detected Hot Box Event, or both;by the projections of ballast, snow and ice in winter conditions that can occur due to dynamic turbulences underneath the train created at high speeds;
 - (d) relevant operational procedures need to be written to define the necessary actions to be taken by the driver in case of loss of the communication means between the Hot Box Detectors and the driver's cabin;
 - (e) the Human Factor aspects related to the operational rules in case of detection of a Hot Box Event need to be analysed and controlled through the Safety Management System of the railway undertaking;
 - (f) etc.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- [G 3] All requirements for the Hot Box Detector, and in particular the quantitative safety requirements, must then be transferred to the manufacturer. Although other tools can be used, it is likely that the manufacturer will also use Fault Tree Analyses for demonstrating the achievement of the applicable quantitative safety requirements.

A5.8 Hazard Log/Record [§ 4 in Annex I of Reg. 402/2013] [CSM RA]

- [G 1] Point 4 in Annex I of Regulation 402/2013 requires the creation of a Hazard Record (some risk assessment and risk management literature uses the “Hazard Log” terminology).
- [G 2] The proposer will use the Hazard Record from the preliminary risk assessment phase, through the design and implementation, until the acceptance of the system under assessment.
- [G 3] There is no mandatory format for the Hazard Record. The proposer is free to define its own format/template, based on the project needs. The least information to be registered in the Hazard Record is defined in point 4.1.2 in Annex I of Reg. 402/2013.
- [G 4] An example of a Hazard Record is shown in Table 39 below. It contains the safety requirements identified in the risk assessment, including the quantitative safety requirements to be applied by the manufacturer for the design of the Hot Box Detector (i.e. technical system under assessment).

A5.9 Conclusion [CSM-DT]

- [G 1] The predictive risk assessment demonstrates that the occurrence of the hazard (i.e. “*Hot Box Event not detected by technical system when required*”) is acceptable if the following risk control measures are put in place :
- the safety requirements set out in section § A5.6.3.4 above are used for the design of the Hot Box Detector (i.e. technical system under assessment).

The quantitative requirements are based on the most credible category of harmonised design targets (i.e. CSM-DT) and on the technical option selected by the proposer among the ones studied in sections § A5.6.3.2 and § A5.6.3.3 above.
 - the Hot Box Detection lamp is tested every day (i.e. every 10 hours) in accordance with a dedicated procedure to be included in the Train Driver’s Manual;
 - the Hot Box Detector is tested in accordance with appropriate maintenance procedures at a time interval commensurate with the quantitative requirement set out for the Hot Box Detector in section § A5.6.3.4 above. Those procedures are clearly written and part of the safety management system of the railway undertaking;
 - the Hot Box Detection is safely integrated within the train in compliance with the requirements to be identified by the additional risk assessments referred to in section § A5.7 above.
- [G 2] Those safety requirements are registered in the Hazard Record in Table 39 below.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

Table 39: Example of Hazard Record for the Hot Box Detector example. [CSM RA]

| N° HZD | Origin | HAZARD – Consequence at level of technical system | Consequences at train level | Potential accident | Cause | Actor in charge | Risk control measure | Used risk acceptance principle | Exported | Status |
|---|--------------------|--|--|--|---|-------------------|---|---|----------|--------|
| Limitations of the risk assessment : | | | | | | | | | | |
| <p>(a) This example considers a risk assessment done by a railway undertaking which decides to fit some of its trains with a new trainborne hot box detection system. The existing infrastructure hot box detection system is not removed; it continues to be used. The manner those two systems are used [i.e. trainborne system alone or both trainborne and trackside ones], with any necessary operational procedures, is not covered by this risk assessment. That shall be analysed and evaluated in a separate risk assessment.</p> <p>(b) For the purposes of this example, the failures of the driver are neither considered nor the associated risk control measures proposed. The risk assessment only focusses on the technical aspects of the change. It is thus assumed that the associated human factor aspects are properly analysed and controlled through the Safety Management System of the railway undertaking.</p> <p>For example, when the hot box detection function is achieved by a trainborne system, as Hot Box Events can occur at any moment of time and at any location of the track, operational procedures need be defined with the infrastructure manager (IM) in order to manage a safe stopping of the train at an appropriate and agreed location, including thus the necessity to enforce by the IM a speed reduction for trains on adjacent tracks in order to manage the risks caused by the blast at the crossing of two trains.</p> <p>(c) The environmental constraints are also neither specified nor the associated risks assessed. For example, the use of Hot Box Detectors in very hot countries, outside a specified range, could generate an unacceptable rate of false alarms. Those aspects are not addressed by the present risk assessment.</p> | | | | | | | | | | |
| Assumptions for the risk assessment : | | | | | | | | | | |
| <p>(a) trains are operated 10 hours a day;</p> <p>(b) trains are operated 30 days a month, i.e. regular monthly maintenance activities take place either every 300 hours or every 3600 hours of operation depending on the selected option among the ones studied in sections § A5.6.3.2 and § A5.6.3.3.</p> | | | | | | | | | | |
| 1. | Line 1 of Table 33 | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely. | <ul style="list-style-type: none"> • Fire • Derailment | Hot Box Detector failed | RU | <ul style="list-style-type: none"> • Set necessary requirements in contract + Contractor management through SMS procedures • Depending on selected option among sections § A5.6.3.2 and § A5.6.3.3 plan maintenance activities at appropriate intervals | <ul style="list-style-type: none"> • SMS rules (CoP) • Explicit risk estimation | No | Open |
| 2. | | | | | | Manu- facturer | Quantitative safety requirement set out in section § A5.6.3.4 above depending on selected option among sections § A5.6.3.2 and § A5.6.3.3 | Explicit risk estimation | Yes | Open |
| 3. | Section § A5.6.3.1 | | | | Hot Box Detector damaged by external causes | RU | Measures identified in relation to section § A5.7 to protect against damages to Hot Box Detector and interfacing wires due to projections of ballast, snow and ice in winter conditions that can occur due to dynamic turbulences underneath the train at high speeds | Internal Codes of Practice | No | Open |

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

Table 39: Example of Hazard Record for the Hot Box Detector example. [CSM RA]

| N° HZD | Origin | HAZARD – Consequence at level of technical system | Consequences at train level | Potential accident | Cause | Actor in charge | Risk control measure | Used risk acceptance principle | Exported | Status |
|--------|---|---|--|--|-------------------------------|------------------|--|--|----------|--------|
| 4. | Line 1 of Table 33 | | | | Failure of indication system | RU | <ul style="list-style-type: none"> Depending on selected technical option in section § A5.6.3.1 apply relevant Codes of Practice Application of relevant operational procedures defining the actions to be taken by the driver in case of loss of the communication means between the Hot Box Detectors and the driver's cabin | <ul style="list-style-type: none"> Codes of practice SMS rules (CoP) | No | Open |
| 5. | Line 2 of Table 33 | Spurious detection of a Hot Box Event | <ul style="list-style-type: none"> Driver required to stop the train whereas not necessary Traffic operation disturbed | No | Hot Box Detector failed | Manu-facturer | Quantitative safety requirement set out in section § A5.6.3.4 depending on selected option among sections § A5.6.3.2 and § A5.6.3.3 | Explicit risk estimation | Yes | Open |
| | | | | | Failure of indication system | RU | Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm | <ul style="list-style-type: none"> Codes of practice SMS rules (CoP) | No | Open |
| 6. | Line 5 of Table 33 | Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety | In case of a Hot Box Event, the driver is informed too late and might not stop the train safely. | <ul style="list-style-type: none"> Fire Derailment | Hot Box Detector failed | Manu-facturer | Quantitative safety requirement set out in section § A5.6.3.4 depending on selected option among sections § A5.6.3.2 and § A5.6.3.3 | Explicit risk estimation | Yes | Open |
| | | | | | Failure of indication system | RU | <ul style="list-style-type: none"> Depending on selected technical option in section § A5.6.3.1 apply relevant Codes of Practice Application of relevant operational procedures defining the actions to be taken by the driver in case of loss of the communication means between the Hot Box Detectors and the driver's cabin | <ul style="list-style-type: none"> Codes of practice SMS rules (CoP) | No | Open |
| 7. | CCF-Analysis in point [G 4] in § A5.6.3.3 | Hot Box Event not detected by technical system when required | In case of a Hot Box Event, the driver is not informed and cannot stop the train safely | <ul style="list-style-type: none"> Fire Derailment | CCF to both Hot Box Detectors | RU Manu-facturer | The temperature sensors of the two Hot Box Detectors shall either be of different technology (or suppliers) or from a different manufacturing batch. This requires also different labelling of products and a proper configuration management process | <ul style="list-style-type: none"> Codes of practice Explicit risk estimation SMS rules | Yes | Open |

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

A5.10 Appendix to Annex 5 : Supporting RAMS tools in the example ^[CSM RA]

A5.10.1 Failure Mode and Effect Analysis tool (FMEA) ^[CSM RA]

- [G 1] The FMEA is a powerful tool. It is a forward or inductive analysis, or still called bottom-up analysis, which main purpose is to evaluate the effects of potential failures on the system under assessment. It enables to determine how single failures of items (functions or physical components) can affect the safety and the availability of the system under assessment.
- [G 2] From the safety point of view, the FMEA analysis is essential for assessing systematically the impact of identified failures on the safety of the whole system. It identifies :
- (a) the different potential failure modes of the item;
 - (b) the possible causes responsible for the identified failure mode;
 - (c) the effects of the failure mode at local level and at subsystem or system level;
 - (d) the associated failure rate, where necessary;
 - (e) the possibilities to detect and localise the fault (failures);
 - (f) the corresponding detection time;
 - (g) the implemented provisions to control the effects.
- [G 3] The determination of the failure effects is facilitated by the identification of the links between the functions and the manner these functions are achieved.
- [G 4] The IEC 60812 standard describes in detail how to apply the FMEA tool. It describes among others how to carry out an FMEA at different indenture levels of a system.

A5.10.2 Fault Tree Analysis Tool (FTA) ^[CSM RA]

- [G 1] The FTA is a deductive (backward or top-down analysis) method, complementary to Failure Mode and Effect Analysis (FMEA). It is a rigorous technique by which many events that interact to produce other events can be related by using simple logical relationships (AND, OR, NAND, NOR, etc. gates). These relationships permit a methodical and progressive building of a tree structure that represents the architecture and functioning of the system under assessment.
- [G 2] Progress in the synthesis of the fault tree is recorded graphically by arranging those contributing failures into a tree structure using the connection symbols/gates. When a contributing failure cannot be divided further, or when it is decided to limit the analysis of a subsystem, the corresponding branch is terminated with a basic event.
- [G 3] When the FTA structure is established, subsequent deductive analyses can take place :
- (a) **a qualitative analysis** : the FTA method enables to describe or model the dysfunctioning of the system under assessment and to determine the combinations of failures (called "basic events") which lead to the undesired event ("top event").

The purpose of the qualitative analysis is to reduce the fault tree to a logically equivalent form in terms of the specific combinations of basic events sufficient to cause the undesired/top event to occur. Each combination of causes constitutes a "Minimal Cut Set" (MCS) of failure modes for the tree. The number of events in a Minimal Cut Set is called the order of the Minimal Cut Set.
 - (b) **a quantitative analysis** : the FTA method enables to compute the probability or frequency of occurrence of the undesired/top event.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

The purpose of the quantitative analysis is to transform the established logical tree structure into an equivalent probability or frequency of occurrence form and to numerically calculate the probability or frequency of occurrence of the undesired top event from the probabilities/frequencies of occurrence of the different basic events.

[G 4] An example of FTA is given in Figure 46 below.

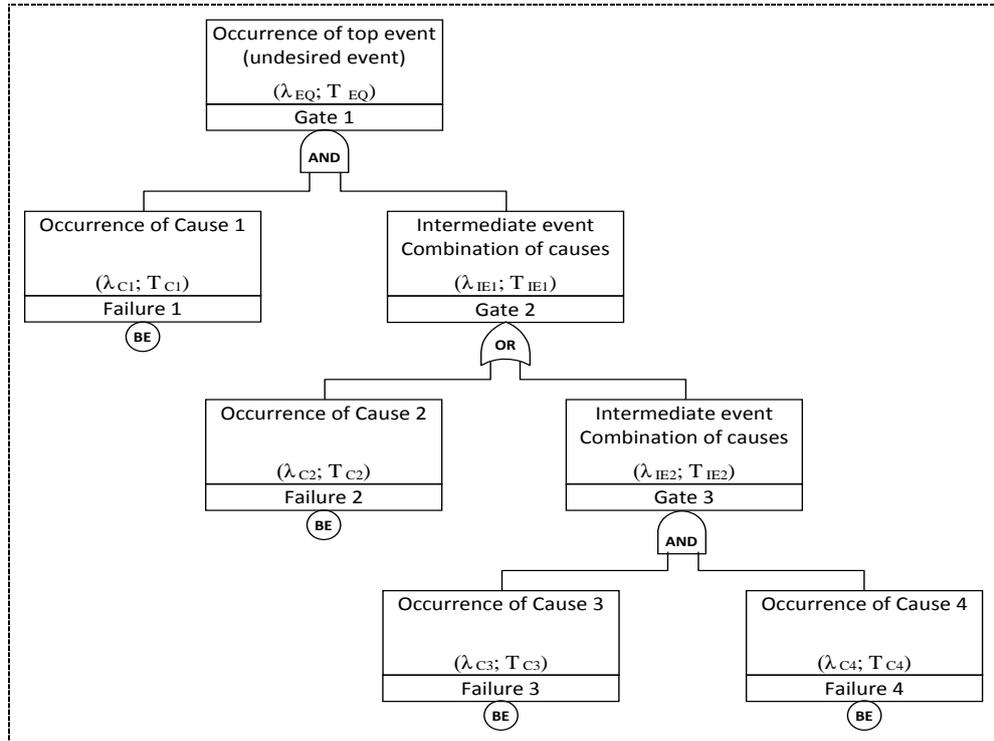


Figure 46: Example of a Fault Tree Analysis.

[G 5] The FTA method is explained in the IEC 61025 standard.

[G 6] FTAs are usually used to demonstrate the achievement of quantitative requirements and safety targets set out for the system under assessment. So, although other tools might be possible, the manufacturer will usually also use FTAs for demonstrating that their products comply with the quantitative requirements set out in the contracts with railway undertakings and infrastructure managers.

A5.10.3 Building/modelling, reduction and calculation of a Fault Tree ^[CSM RA]

[G 1] In practice, and especially for complex technical systems, the building/modelling, reduction and calculation of Fault Tree Analyses (FTAs) are performed using specific software tools. Usually, those tools enable also to calculate the sensitivity of the top event and to determine the most critical contributing causes.

[G 2] In absence of a software tool for building/modelling, reduction and calculation of an FTA, for the purpose of the example in Annex 5 and this guide, the calculation of the frequency of occurrence of the top event of an FTA can be done using the formulas below from section § 8.4.2. of Alain VILLEMEUR RAMS book, Eyrolles editions, on the “Reliability, Availability, Maintainability and Safety of complex industrial systems” {Ref. 3}.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

The French title of {Ref. 3} is : “Sûreté de fonctionnement des systèmes industriels”, Fiabilité, Facteurs humains, Informatisation, Auteur : Alain VILLEMEUR – Editions Eyrolles.

(a) **For an OR gate :**

$$\lambda_{EQ} = \sum \lambda_i$$

Formula 1

$$T_{EQ} = \frac{\sum (\lambda_i \times T_i)}{\sum \lambda_i}$$

Formula 2

(b) **For an AND gate :**

$$\lambda_{EQ} = \prod (\lambda_i \times T_i) \times \sum \frac{1}{T_i}$$

Formula 3

$$T_{EQ} = \frac{1}{\sum \frac{1}{T_i}}$$

Formula 4

(c) **Where :**

- (1) λ_i is the failure rate or frequency of occurrence of the considered basic event;
- (2) T_i is the **mean** “Detection plus Negation Time” of the considered basic event;
- (3) λ_{EQ} is the equivalent failure rate or frequency of occurrence;
- (4) T_{EQ} is the equivalent **mean** “Detection plus Negation Time”;
- (5) ‘i’ is the number of contributing events to the underneath gate.

[G 3] {Ref. 3} deals with reliability, human factors and IT system matters in complex industrial systems. Formula 1, Formula 2, Formula 3 and Formula 4 are valid for the asymptotic failure rates (i.e. where failure rates $[\lambda]$ are constant over time); the exact solutions could be determined by the use of Markov models.

[G 4] Those formulas are based on the “Lambda-Mu” (λ - μ) method, where with the assumption that $\lambda_i/\mu_i \ll 1$:

(a) $M(\infty) = 1/T_{EQ}$

(b) $\mu_i = 1/T_i$

(c) T_i corresponds to MTTR, i.e. the Mean Time To Restore (detection, repair and return to service) of the system under assessment.

[G 5] Equivalent formulas can also be found in sections IV-3.2.2. and IV-3.2.3. of the book of Claude LIEVENS on the “safety of systems”, Cepadues editions, from the French high national school on aeronautics and space (SUP’AERO) {Ref. 4}.

The French title of {Ref. 4} is : Sécurité des Systèmes », Ecole Nationale Supérieure de l’Aéronautique et de l’Espace (SUP’AERO), Claude LIEVENS, CEPADUES-EDITIONS.

Annex 5 : Agency example on the use of CSM-DT (Trainborne Hot Box Detection System)

- [G 6] Formula 3 and Formula 4 above are equivalent to the formulas (A.1) below, for an AND gate with only two inputs, from the footnote of section § A.4.2.2.1 in the Appendix A of the CENELEC 50129 standard in force at the date of publication of this guide.

$$THR_S = \frac{FR_A}{SDR_A} \times \frac{FR_B}{SDR_B} \times (SDR_A + SDR_B) \quad \text{and} \quad SDR_S \approx SDR_A + SDR_B \quad (A.1)$$

Where :

- (a) FR's stand for potential hazardous Failure Rates of the respective basic events;
- (b) SDT stands for the safe down time;
- (c) SDR stands for the safe down rate, i.e. $SDR = SDT^{-1}$;
- (d) if periodic testing times are used as detection times for the failures, then (A.1) may be used with Mean Test Times.

Then, $SDT = 1/SDR = T/2 + \text{negation time}$.