

English Version

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

This European Standard was approved by CENELEC on 2017-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

| | |
|--|----|
| European foreword..... | 5 |
| Introduction..... | 6 |
| 1 Scope..... | 7 |
| 2 Normative references..... | 8 |
| 3 Terms and definitions..... | 8 |
| 4 Abbreviations..... | 8 |
| 5 Safety process..... | 9 |
| 5.1 Risk assessment and hazard control..... | 9 |
| 5.2 A. Risk assessment..... | 10 |
| 5.2.1 General..... | 10 |
| 5.2.2 Conducting risk assessment..... | 11 |
| 5.3 B. Outcome of the risk assessment..... | 11 |
| 5.4 C. Hazard control..... | 11 |
| 5.5 D. Revision of risk assessment..... | 12 |
| 5.6 Responsibilities..... | 13 |
| 6 Safety demonstration and acceptance..... | 13 |
| 6.1 Introduction..... | 13 |
| 6.2 Safety demonstration and safety acceptance process..... | 13 |
| 6.3 Responsibility in managing the Safety Case..... | 17 |
| 6.4 Modifications after safety acceptance..... | 17 |
| 6.5 Dependencies between Safety Cases..... | 17 |
| 6.6 Relationship between safety cases and system architecture..... | 18 |
| 7 Organisation and Independence of Roles..... | 19 |
| 7.1 General..... | 19 |
| 7.2 Early phases of the lifecycle (phases 1 to 4)..... | 19 |
| 7.3 Later phases of the lifecycle (starting from phase 5)..... | 20 |
| 7.4 Personnel Competence..... | 21 |
| 8 Risk assessment..... | 22 |
| 8.1 Introduction..... | 22 |
| 8.2 Risk Analysis..... | 22 |
| 8.2.1 General..... | 22 |
| 8.2.2 The risk model..... | 22 |
| 8.2.3 Techniques for the consequence analysis..... | 24 |
| 8.2.4 Expert Judgement..... | 25 |
| 8.3 Risk acceptance principles and risk evaluation..... | 25 |
| 8.3.1 Use of Code of Practice..... | 25 |
| 8.3.2 Use of a reference system..... | 26 |
| 8.3.3 Use of Explicit Risk Estimation..... | 27 |
| 8.4 Application of explicit risk estimation..... | 28 |
| 8.4.1 Quantitative approach..... | 28 |
| 8.4.2 Variability using quantitative risk estimates..... | 30 |
| 8.4.3 Qualitative and semi-quantitative approaches..... | 31 |

| | | |
|---------|---|----|
| 9 | Specification of System Safety Requirements | 32 |
| 9.1 | General | 32 |
| 9.2 | Safety requirements | 32 |
| 9.3 | Categorization of Safety Requirements | 32 |
| 9.3.1 | General | 32 |
| 9.3.2 | Functional safety requirements | 33 |
| 9.3.3 | Technical safety requirements | 34 |
| 9.3.4 | Contextual safety requirements..... | 34 |
| 10 | Apportionment of functional Safety Integrity requirements..... | 35 |
| 10.1 | Deriving and apportioning system safety requirements | 35 |
| 10.2 | Functional safety integrity for electronic systems | 35 |
| 10.2.1 | Deriving functional safety requirements for electronic systems..... | 35 |
| 10.2.2 | Apportioning safety requirements | 35 |
| 10.2.3 | Safety Integrity Factors..... | 38 |
| 10.2.4 | Functional safety integrity and random failures | 38 |
| 10.2.5 | Systematic aspect of functional safety integrity | 38 |
| 10.2.6 | Balanced requirements controlling random and systematic failures | 38 |
| 10.2.7 | The SIL table | 39 |
| 10.2.8 | SIL allocation..... | 40 |
| 10.2.9 | Apportionment of TFFR after SIL allocation | 40 |
| 10.2.10 | Demonstration of quantified targets | 40 |
| 10.2.11 | Requirements for Basic Integrity | 41 |
| 10.2.12 | Prevention of misuse of SILs | 42 |
| 10.3 | Safety Integrity for non-electronic systems – Application of CoP..... | 42 |
| 11 | Design and implementation..... | 43 |
| 11.1 | Introduction | 43 |
| 11.2 | Causal analysis | 43 |
| 11.3 | Hazard identification (refinement)..... | 44 |
| 11.4 | Common cause analysis | 44 |
| | Annex A (informative) ALARP, GAME, MEM | 46 |
| A.1 | ALARP, GAME, MEM as methods to define risk acceptance criteria | 46 |
| A.2 | ALARP (As Low As Reasonably Practicable) | 47 |
| A.2.1 | General | 47 |
| A.2.2 | Tolerability and ALARP..... | 48 |
| A.3 | Globalement Au Moins Equivalent (GAME) principle | 48 |
| A.3.1 | Principle | 48 |
| A.3.2 | Using GAME..... | 49 |
| A.3.2.1 | General | 49 |
| A.3.2.2 | Basic principles | 49 |
| A.3.2.3 | Using GAME to construct a qualitative safety argument | 49 |
| A.3.2.4 | GAME using quantitative risk targets | 49 |
| A.4 | Minimum Endogenous Mortality MEM | 50 |
| | Annex B (informative) Using failure and accident statistics to derive a THR | 52 |
| | Annex C (informative) Guidance on SIL Allocation | 53 |
| | Annex D (informative) Safety target apportionment methods | 55 |
| D.1 | Analysis of the system and methods | 55 |