IEC 62278-2

Edition 1.0 2025-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Railway applications - 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

ICS 45.060.01

ISBN 978-2-8327-0584-1

IEC 62278-2:2025-07(en-fr)

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
2 Normative references 9
3 Terms and definitions 9
4 Abbreviated terms 9
5 Safety process 10
5.1 Hourglass model for risk assessment and hazard control 10
5.2 A. Risk assessment 11
5.2.1 General 11
5.2.2 Conducting risk assessment 12
5.3 B. Outcome of the risk assessment 12
5.4 C. Hazard control 12
5.5 D. Revision of risk assessment 13
5.6 Responsibilities 14
6 Safety demonstration and acceptance 14
6.1 General 14
6.2 Safety demonstration and safety acceptance process 14
6.3 Responsibility in managing the safety case 18
6.4 Modifications after safety acceptance 18
6.5 Dependencies between safety cases 18
6.6 Relationship between safety cases and system architecture 19
7 Organization and independence of roles 20
7.1 General 20
7.2 Early phases of the life cycle (phases 1 to 4) 21
7.3 Later phases of the life cycle (starting from phase 5) 21
7.4 Personnel competence 23
8 Risk assessment 24
8.1 General 24
8.2 Risk analysis 24
8.2.1 General 24
8.2.2 The risk model 24
8.2.3 Techniques for the consequence analysis 26
8.2.4 Expert judgement 27
8.3 Risk acceptance principles and risk evaluation 28
8.3.1 Use of code of practice 28
8.3.2 Use of a reference system 28
8.3.3 Use of explicit risk estimation 29
8.4 Application of explicit risk estimation 30
8.4.1 Quantitative approach 30
8.4.2 Variability using quantitative risk estimates 33
8.4.3 Qualitative and semi-quantitative approaches 34
9 Specification of system safety requirements 35
9.1 General 35
9.2 Safety requirements 35

9.3 Categorization of safety requirements 35
9.3.1 General 35
9.3.2 Functional safety requirements 36
9.3.3 Technical safety requirements 37
9.3.4 Contextual safety requirements 37
10 Apportionment of functional safety integrity requirements 38
10.1 General 38
10.2 Functional safety integrity for electronic systems 38
10.2.1 General 38
10.2.2 Apportioning safety requirements 38
10.2.3 Safety integrity factors 41
10.2.4 Functional safety integrity and random failures 41
10.2.5 Systematic aspect of functional safety integrity 41
10.2.6 Balanced requirements controlling random and systematic failures 42
10.2.7 The SIL table 42
10.2.8 SIL allocation 43
10.2.9 Apportionment of TFFR after SIL allocation 43
10.2.10 Demonstration of quantified targets 44
10.2.11 Requirements for basic integrity 44
10.2.12 Prevention of misuse of SILs 45
10.3 Safety integrity for non-electronic systems - Application of CoP 45
11 Design and implementation 46
11.1 General 46
11.2 Causal analysis 46
11.3 Hazard identification (refinement) 47
11.4 Common cause failure analysis 48
Annex A (informative) ALARP, GAME, MEM as examples of risk acceptance criteria 50
A.1 ALARP, GAME, MEM as methods to define risk acceptance criteria 50
A.2 ALARP (as low as reasonably practicable) 51
A.2.1 General 51
A.2.2 Tolerability and ALARP 51
A.3 Globalement au moins équivalent (GAME) principle 52
A.3.1 Principle 52
A.3.2 Using GAME 52
A.4 Minimum endogenous mortality (MEM) 53
Annex B (informative) Using failure and accident statistics to derive a THR 56
Annex C (informative) Guidance on SIL allocation 58
Annex D (informative) Safety target apportionment methods 59
D.1 Analysis of the system and methods 59
D.2 Example of qualitative apportionment method 59
D.2.1 General 59
D.2.2 Example of qualitative or semi-quantitative method for barrier efficiency 60
D.3 Example of quantitative apportionment method 62
D.3.1 General 62
D.3.2 Functions with independent failure detection and negation mechanisms 64
D.3.3 Function and independent barrier acting as failure detection and negation mechanism 65

D.3.4 Apportionment of a probability safety target 67
D.3.5 Apportionment of a "per hour" safety target 67
Annex E (informative) Common mistakes in quantification 69
E.1 General 69
E.2 Mixing failure rates with probabilities 69
E.3 Using formulas out of their range of applicability 70
Annex F (informative) Techniques and methods for safety analysis 71
Annex G (informative) Key system safety roles and responsibilities 73
Bibliography 78

Figure 1 – The hourglass model 11
Figure 2 – Illustration of hazards with respect to the system boundary 13
Figure 3 – Example of safety acceptance processes 17
Figure 4 – Examples of dependencies between safety cases 19
Figure 5 – Independence of roles in the early phases (phases 1 to 4) of the life cycle 21
Figure 6 – Independence of roles in later phases of the life cycle (starting from phase 5) 23
Figure 7 – An example of risk model 25
Figure 8 – Tolerable rates in an example of risk model 31
Figure 9 – Requirements classification 36
Figure 10 – Apportionment of functional safety requirements 39
Figure 11 – Categorization of safety integrity measures 42
Figure 12 – Common cause failures 48
Figure 13 – Impact of functional dependence in a fault tree analysis 48
Figure A.1 – Differential risk aversion 54
Figure D.1 – Example of qualitative apportionment method 60
Figure D.2 – Interpretation of failure and repair times 63
Figure D.3 – Combination of two functions with independent failure detection and negation mechanism 64
Figure D.4 – Allocation of safety integrity requirements 65
Figure D.5 – Combination of function and independent barrier acting as failure detection and negation mechanism 66
Figure D.6 – Example of quantified apportionment 68
Figure E.1 – Example of FTA case 69

Table 1 – Examples of hazards 26
Table 2 – SIL quantitative and qualitative measures 43
Table A.1 – Overview of ALARP, GAME, MEM 50
Table D.1 – Efficiency based on the component's failures 61
Table D.2 – Efficiency based on the component's knowledge 61
Table D.3 – Efficiency based on the use of the component 61
Table D.4 – Efficiency based on the maintenance of the component 62
Table F.1 – Techniques and methods for safety analysis 71
Table F.2 – Techniques and measures for BI and SILs 72

Table G.1 – Role specification for designer 73
Table G.2 – Role specification for verifier 74
Table G.3 – Role specification for validator 75
Table G.4 – Role specification for independent safety assessor 76
Table G.5 – Role specification for project manager..... 77

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: Systems approach to safety

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch shall not be held responsible for identifying any or all such patent rights.

IEC 62278-2 has been prepared by IEC technical committee 9: Electric systems and equipment for railways. It is an International Standard.

This first edition, together with IEC 62278-1, cancels and replaces IEC 62278:2002. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) creation of this new Part 2 providing, for the first time, safety-related guidance and methods that support the safety management process provided in IEC 62278-1:2025.

The text of this International Standard is based on the following documents:

Draft	Report on voting
9/3208/FDIS	9/3235/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The IEC 62278 series forms part of the railway sector specific application of IEC 61508. IEC 62278, IEC 62279 and IEC 62425 comprise the railway sector equivalent of the IEC 61508 series so far as railway communication, signalling and processing systems are concerned. When compliance with these documents has been demonstrated, further evaluation of compliance with the IEC 61508 series is not foreseen.

A list of all parts in the IEC 62278 series, published under the general title *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,
– withdrawn, or
– revised.

INTRODUCTION

IEC 62278:2002 was aimed at introducing the application of a systematic RAMS management process in the railway sector. Through the application of IEC 62278:2002 and the experiences gained over the last years, the need for revision and restructuring became apparent with a need to deliver a systematic and coherent approach to RAMS applicable to all the railway application fields including signalling, rolling stock and fixed installations.

This document provides railway duty holders and the railway suppliers with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS.

Processes for the specification and demonstration of RAMS requirements are cornerstones of this document. This document promotes a common understanding and approach to the management of RAMS.

The IEC 62278 series is derived from the European Standard series EN 50126:2017, consisting of EN 50126-1:2017 and EN 50126-2:2017.

With regard to safety, IEC 62278-1 provides a safety management process which is supported by guidance and methods described in this document.

IEC 62278-1 and IEC 62278-2 are independent from the technology used. As far as safety is concerned, IEC 62278 takes the perspective of safety with a functional approach.

The application of this document can be adapted to the specific requirements for the system under consideration.

This document can be applied systematically by the railway duty holders and railway suppliers, throughout all phases of the life cycle of a railway application, to develop railway-specific RAMS requirements and to achieve compliance with these requirements. The system level approach developed by this document facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This document promotes co-operation between the stakeholders of railways in the achievement of an optimal combination of RAMS and cost for railway applications.

The process defined by this document assumes that railway duty holders and railway suppliers have business-level policies addressing quality, performance and safety. The approach defined in this document is consistent with the application of quality management requirements contained within ISO 9001.

1 Scope

This document considers the safety-related generic aspects of the RAMS life cycle and defines methods and tools which are independent of the actual technology of the systems and subsystems.

This document provides:

a) methods for the understanding of the systems approach to safety which is a key concept of IEC 62278;

b) methods to derive the safety requirements and their safety integrity requirements for the system and to apportion them to the subsystems;

c) methods to derive the safety integrity levels (SIL) for the safety-related electronic functions;

d) guidance and methods for the following areas:

   1) safety process;

   2) safety demonstration and acceptance;

   3) organization and independence of roles;

   4) risk assessment;

   5) specification of safety requirements;

   6) apportionment of functional safety requirements;

   7) design and implementation;

e) the user of this document with the methods to assure safety with respect to the system under consideration and its interactions;

f) guidance about the definition of the system under consideration, including identification of the interfaces and the interactions of this system with its subsystems or other systems, in order to conduct the risk analysis.

This document does not specify:

g) RAMS targets, quantities, requirements or solutions for specific railway applications;

h) rules or processes pertaining to the certification of railway products against the requirements of this document;

i) an approval process by the safety authority.

This document is applicable:

j) to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined subsystems and components within these major systems, including those containing software; in particular:

   1) to new systems;

   2) to new systems integrated into existing systems already accepted, but only to the extent and insofar as the new system with the new functionality is being integrated. It is otherwise not applicable to any unmodified aspects of the existing system;

   3) as far as reasonably practicable, to modifications and extensions of existing systems already accepted, but only to the extent and insofar as existing systems are being modified. It is otherwise not applicable to any unmodified aspect of the existing system;

k) at all relevant phases of the life cycle of an application;

l) for use by railway duty holders and the railway suppliers.

This document is not applicable to:

m) any unmodified aspect of the existing system;

n) existing systems which remain unmodified, including those systems already compliant with IEC 62278:2002.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62278-1:2025, *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process*

SOMMAIRE

AVANT-PROPOS 5
INTRODUCTION 7
1 Domaine d'application 8
2 Références normatives 9
3 Termes et définitions 9
4 Abréviations 9
5 Processus de sécurité 10
5.1 Le modèle du sablier pour l'appréciation du risque et la maîtrise des situations dangereuses 10
5.2 A. Appréciation du risque 11
5.2.1 Généralités 11
5.2.2 Réalisation de l'appréciation du risque 12
5.3 B. Résultats de l'appréciation du risque 12
5.4 C. Maîtrise des situations dangereuses 13
5.5 D. Révision de l'appréciation du risque 14
5.6 Responsabilités 14
6 Démonstration et acceptation de la sécurité 14
6.1 Généralités 14
6.2 Processus de démonstration et d'acceptation de la sécurité 15
6.3 Responsabilité de gestion du dossier de sécurité 18
6.4 Modifications après l'acceptation de la sécurité 18
6.5 Dépendances entre les dossiers de sécurité 18
6.6 Relation entre les dossiers de sécurité et l'architecture système 20
7 Organisation et indépendance des rôles 20
7.1 Généralités 20
7.2 Phases précoces du cycle de vie (phases 1 à 4) 21
7.3 Phases ultérieures du cycle de vie (à partir de la phase 5) 22
7.4 Compétences du personnel 23
8 Appréciation du risque 24
8.1 Généralités 24
8.2 Analyse du risque 24
8.2.1 Généralités 24
8.2.2 Modèle de risque 24
8.2.3 Techniques d'analyse des conséquences 27
8.2.4 Expertise 28
8.3 Principes d'acceptation du risque et évaluation du risque 28
8.3.1 Utilisation d'un code de bonne pratique 28
8.3.2 Utilisation d'un système de référence 29
8.3.3 Utilisation de l'estimation du risque explicite 30
8.4 Application de l'estimation du risque explicite 31
8.4.1 Approche quantitative 31
8.4.2 Variabilité sur la base des estimations du risque quantitatives 34
8.4.3 Approches qualitatives et semi-quantitatives 36
9 Spécification des exigences de sécurité du système 36
9.1 Généralités 36

9.2 Exigences de sécurité 36
9.3 Classification des exigences de sécurité 37
9.3.1 Généralités 37
9.3.2 Exigences de sécurité fonctionnelle 37
9.3.3 Exigences de sécurité technique 38
9.3.4 Exigences de sécurité contextuelle 39
10 Allocation des exigences d'intégrité de sécurité fonctionnelle 39
10.1 Généralités 39
10.2 Intégrité de sécurité fonctionnelle des systèmes électroniques 40
10.2.1 Généralités 40
10.2.2 Allocation des exigences de sécurité 40
10.2.3 Facteurs d'intégrité de sécurité 43
10.2.4 Intégrité de sécurité fonctionnelle et défaillances aléatoires 43
10.2.5 Aspect systématique de l'intégrité de sécurité fonctionnelle 44
10.2.6 Équilibre des exigences contrôlant les défaillances aléatoires et systématiques 44
10.2.7 Tableau des SIL 45
10.2.8 Allocation des SIL 46
10.2.9 Allocation du TFFR après affectation des SIL 46
10.2.10 Démonstration des objectifs quantifiés 46
10.2.11 Exigences spécifiques relatives à l'intégrité de base 46
10.2.12 Prévention de la mauvaise utilisation des SIL 48
10.3 Intégrité de sécurité des systèmes non électroniques - Application d'un code de bonne pratique 48
11 Conception et réalisation 49
11.1 Généralités 49
11.2 Analyse des causes 49
11.3 Identification dangers (affinage) 50
11.4 Analyse des défaillances de cause commune 51
Annexe A (informative) Utilisation des méthodes ALARP, GAME et MEM comme exemples de critères d'acceptation du risque 53
A.1 Utilisation des méthodes ALARP, GAME et MEM pour définir les critères d'acceptation du risque 53
A.2 Principe ALARP (aussi bas que cela est raisonnablement possible) 54
A.2.1 Généralités 54
A.2.2 Acceptabilité et ALARP 55
A.3 Principe GAME (globalement au moins équivalent) 55
A.3.1 Principe 55
A.3.2 Utilisation du principe GAME 56
A.4 Principe MEM (mortalité endogène minimale) 57
Annexe B (informative) Utilisation des statistiques de défaillances et d'accidents pour déterminer un THR 59
Annexe C (informative) Lignes directrices relatives à l'allocation des SIL 61
Annexe D (informative) Méthodes d'allocation des objectifs de sécurité 62
D.1 Analyse du système et des méthodes 62
D.2 Exemple de méthode d'allocation qualitative 62
D.2.1 Généralités 62

D.2.2 Exemple de méthode qualitative ou semi-quantitative pour l'efficience de la barrière ... 63
D.3 Exemple de méthode d'allocation quantitative ... 65
D.3.1 Généralités ... 65
D.3.2 Fonctions avec mécanismes indépendants de détection et de passivation des défaillances ... 67
D.3.3 Fonction et barrière indépendante faisant office de mécanisme de détection et de passivation des défaillances ... 69
D.3.4 Allocation d'un objectif de sécurité de probabilité ... 70
D.3.5 Allocation d'un objectif de sécurité "par heure" ... 70
Annexe E (informative) Erreurs courantes de quantification ... 72
E.1 Généralités ... 72
E.2 Confusion entre taux et probabilités de défaillance ... 72
E.3 Utilisation des formules hors de leur plage d'applicabilité ... 73
Annexe F (informative) Techniques et méthodes d'analyse de sécurité ... 74
Annexe G (informative) Rôles et responsabilités essentielles de la sécurité du système ... 76
Bibliographie ... 81

Figure 1 – Le modèle du sablier ... 11
Figure 2 – Représentation des dangers par rapport aux frontières du système ... 13
Figure 3 – Exemple de processus d'acceptation de la sécurité ... 17
Figure 4 – Exemples de dépendances entre des dossiers de sécurité ... 19
Figure 5 – Indépendance des rôles dans les phases précoces du cycle de vie (phases 1 à 4) ... 22
Figure 6 – Indépendance des rôles dans les phases ultérieures du cycle de vie (à partir de la phase 5) ... 23
Figure 7 – Exemple de modèle de risque ... 25
Figure 8 – Taux acceptables dans un exemple de modèle de risque ... 32
Figure 9 – Classification des exigences ... 37
Figure 10 – Allocation des exigences de sécurité fonctionnelle ... 41
Figure 11 – Catégorisation des mesures d'intégrité de sécurité ... 45
Figure 12 – Défaillances de cause commune ... 51
Figure 13 – Influence de la dépendance fonctionnelle dans une analyse par arbre de panne ... 52
Figure A.1 – Aversion différentielle du risque ... 58
Figure D.1 – Exemple de méthode d'allocation qualitative ... 63
Figure D.2 – Interprétation des temps de défaillance et de réparation ... 66
Figure D.3 – Combinaison de deux fonctions avec mécanisme indépendant de détection et de passivation des défaillances ... 67
Figure D.4 – Allocation des exigences d'intégrité de sécurité ... 68
Figure D.5 – Combinaison d'une fonction et d'une barrière indépendante faisant office de mécanisme de détection et de passivation des défaillances ... 69
Figure D.6 – Exemple d'allocation quantifiée ... 71
Figure E.1 – Exemple de cas AAP ... 72

Tableau 1 – Exemples de dangers ... 27

Tableau 2 – Mesures quantitatives et qualitatives du SIL 45
Tableau A.1 – Présentation des méthodes ALARP, GAME et MEM 53
Tableau D.1 – Efficience basée sur les défaillances du composant 64
Tableau D.2 – Efficience basée sur la connaissance du composant 64
Tableau D.3 – Efficience basée sur l'utilisation du composant 64
Tableau D.4 – Efficience basée sur la maintenance du composant 65
Tableau F.1 – Techniques et méthodes d'analyse de sécurité 74
Tableau F.2 – Techniques et mesures pour la BI et les SIL 75
Tableau G.1 – Spécification du rôle du concepteur 76
Tableau G.2 – Spécification du rôle du chargé de vérification 77
Tableau G.3 – Spécification du rôle du chargé de validation 78
Tableau G.4 – Spécification du rôle de l'évaluateur de sécurité indépendant 79
Tableau G.5 – Spécification du rôle du chef de projet 80

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC - entre autres activités - publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications ; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62278-2 a été établi par le comité d'études 9 de l'IEC : Matériels et systèmes électriques ferroviaires. Il s'agit d'une Norme internationale.

Cette première édition, conjointement à l'IEC 62278-1, annule et remplace l'IEC 62278:2002. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente :

a) rédaction de cette nouvelle Partie 2 qui fournit pour la première fois des lignes directrices et des méthodes de sécurité dans le cadre du processus de management de la sécurité défini dans l'IEC 62278-1:2025.

Le texte de cette Norme internationale est issu des documents suivants :

Projet	Rapport de vote
9/3208/FDIS	9/3235/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation du présent document.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détails à l'adresse www.iec.ch/standardsdev/publications.

La série IEC 62278 représente une partie de l'application spécifique au domaine ferroviaire de l'IEC 61508. Les IEC 62278, IEC 62279 et IEC 62425 constituent l'équivalent relatif au secteur ferroviaire de la série IEC 61508 en ce qui concerne les systèmes de communication ferroviaire, de signalisation et de traitement. Dans les cas où la satisfaction aux exigences des documents cités ci-dessus a été démontrée, il n'est pas prévu de démontrer davantage la conformité à la série IEC 61508.

Une liste de toutes les parties de la série IEC 62278, publiées sous le titre général *Applications ferroviaires — Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de l'IEC sous http://webstore.iec.ch dans les données relatives à la publication recherchée. À cette date, la publication sera

– reconduite,
– supprimée, ou
– révisée.

INTRODUCTION

L'IEC 62278:2002 visait à introduire l'application d'un processus systématique de management de la FDMS dans le domaine ferroviaire. L'application de l'IEC 62278:2002 et l'expérience acquise au cours de ces dernières années ont révélé la nécessité de mettre en œuvre une démarche de révision et de restructuration avec la volonté d'établir une approche systématique et cohérente de la FDMS applicable à tous les domaines d'application ferroviaire, notamment la signalisation, le matériel roulant et les installations fixes.

Le présent document fournit aux sociétés d'exploitation ferroviaire et aux industries ferroviaires un processus permettant de mettre en œuvre une démarche cohérente de management de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité, désignée par l'acronyme FDMS.

Les processus relatifs à la spécification et à la démonstration des exigences de FDMS sont les pierres angulaires du présent document. Le présent document encourage une vision et une démarche communes de management de la FDMS.

La série IEC 62278 est dérivée de la série de Normes européennes EN 50126:2017, comprenant l'EN 50126-1:2017 et l'EN 50126-2:2017.

En ce qui concerne la sécurité, l'IEC 62278-1 fournit un processus de management de la sécurité étayé par les lignes directrices et les méthodes décrites dans le présent document.

L'IEC 62278-1 et l'IEC 62278-2 ne sont pas liée à la technologie utilisée. En ce qui concerne la sécurité, l'IEC 62278 adopte la perspective de la sécurité avec une approche fonctionnelle.

L'application du présent document peut être adaptée aux exigences spécifiques pour le système en cours d'examen.

Le présent document peut être systématiquement appliqué par les sociétés d'exploitation et les industries ferroviaires tout au long des phases du cycle de vie d'une application ferroviaire afin de développer des exigences de FDMS spécifiques au domaine ferroviaire et de satisfaire à ces exigences. L'approche système définie par le présent document facilite l'appréciation des interactions relatives à la FDMS entre les éléments des applications ferroviaires, même si elles sont complexes.

Le présent document promeut la synergie entre les parties prenantes du domaine ferroviaire afin de parvenir au meilleur compromis entre les performances de FDMS et les coûts des applications ferroviaires.

Le processus défini par le présent document part du principe que les sociétés d'exploitation et les industries ferroviaires ont développé au niveau de l'entreprise des politiques de qualité, performances et sécurité. L'approche définie dans le présent document est en accord avec l'application des exigences de management de la qualité de l'ISO 9001.

1 Domaine d'application

Le présent document prend en considération les aspects génériques relatifs à la sécurité du cycle de vie FDMS et définit les méthodes et les outils qui sont indépendants de la technologie des systèmes et sous-systèmes.

Le présent document fournit :

a) une présentation de l'approche systématique pour la sécurité, un concept clé de l'IEC 62278 ;

b) les méthodes pour déterminer les exigences de sécurité et leurs exigences d'intégrité de sécurité concernant le système et pour les allouer aux différents sous-systèmes ;

c) les méthodes pour déterminer les niveaux d'intégrité de sécurité (SIL) pour les fonctions électroniques relatives à la sécurité ;

d) des lignes directrices et des méthodes concernant :

   1) le processus de sécurité ;

   2) la démonstration et l'acceptation de la sécurité ;

   3) l'organisation et l'indépendance des rôles ;

   4) l'appréciation du risque ;

   5) la spécification des exigences de sécurité ;

   6) l'allocation des exigences de sécurité fonctionnelle ;

   7) la conception et la réalisation.

e) à l'utilisateur du présent document les méthodes permettant d'assurer la sécurité à l'égard du système en cours d'examen et de ses interactions ;

f) des lignes directrices sur la définition du système en cours d'examen, y compris l'identification des interfaces et interactions du système avec ses sous-systèmes ou d'autres systèmes afin de réaliser l'analyse du risque.

Le présent document ne spécifie pas :

g) les objectifs de FDMS, ni les grandeurs, les exigences ou les solutions pour des applications ferroviaires spécifiques ;

h) les règles ou les processus de certification des produits ferroviaires vis-à-vis des exigences du présent document ;

i) un processus d'homologation par l'autorité de tutelle en matière de sécurité.

Le présent document s'applique :

j) à la spécification et à la démonstration des exigences de FDMS pour toute application ferroviaire et à tout niveau d'une telle application, selon le cas, allant des systèmes ferroviaires complets aux grands systèmes et aux sous-systèmes et équipements (individuels et combinés) de ces grands systèmes, y compris ceux qui comportent des logiciels. Il est notamment applicable :

   1) aux nouveaux systèmes ;

   2) aux nouveaux systèmes intégrés dans des systèmes préexistants acceptés, mais seulement dans la mesure où, et dans la façon dont le nouveau système comprenant la nouvelle fonctionnalité y est intégré. Il ne s'applique cependant pas aux parties inchangées du système existant ;

   3) dans toute la mesure du possible, aux modifications et extensions des systèmes préexistants, mais seulement dans la mesure où, et dans la façon dont les systèmes existants sont modifiés. Il ne s'applique cependant pas aux parties inchangées du système existant ;

k) à toutes les phases concernées du cycle de vie d'une application donnée ;

l) à l'utilisation des sociétés d'exploitation ferroviaire et des industries ferroviaires.

Le présent document ne s'applique pas aux :

m) parties inchangées du système existant ;

n) systèmes existants qui ne sont pas modifiés, y compris ceux déjà conformes à l'IEC 62278:2002.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62278-1:2025, *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process*