

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

62279

Première édition
First edition
2002-09

**Applications ferroviaires –
Systèmes de signalisation, de télécommunication
et de traitement –
Logiciels pour systèmes de commande
et de protection ferroviaire**

**Railway applications –
Communications, signalling and
processing systems –
Software for railway control and
protection systems**

© IEC 2002 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission, 3, rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE **XE**

For price, see current catalogue
For price, see current catalogue

SOMMAIRE

AVANT-PROPOS	10
INTRODUCTION	14
1 Domaine d'application	20
2 Références normatives	22
3 Définitions.....	22
4 Objets et conformité.....	30
5 Niveaux d'intégrité de la sécurité logicielle.....	30
5.1 Objet	30
5.2 Exigences.....	32
6 Personnel et responsabilités	34
6.1 Objet	34
6.2 Exigences.....	34
7 Problèmes liés au cycle de vie et documentation	36
7.1 Objets.....	36
7.2 Exigences.....	38
8 Spécification des Exigences du Logiciel	44
8.1 Objets.....	44
8.2 Documents en entrée.....	44
8.3 Documents en sortie.....	44
8.4 Exigences.....	44
9 Architecture du logiciel.....	48
9.1 Objets.....	48
9.2 Documents en entrée.....	48
9.3 Documents en sortie.....	48
9.4 Exigences.....	48
10 Conception et développement du logiciel.....	52
10.1 Objets.....	52
10.2 Documents en entrée.....	52
10.3 Documents en sortie.....	52
10.4 Exigences.....	52
11 Vérification et tests du logiciel.....	58
11.1 Objets.....	58
11.2 Documents en entrée.....	58
11.3 Documents en sortie.....	58
11.4 Exigences.....	60
12 Intégration logiciel/matériel.....	64
12.1 Objets.....	64
12.2 Documents en entrée.....	64
12.3 Documents en sortie.....	66
12.4 Exigences.....	66
13 Validation du logiciel	68
13.1 Objets.....	68
13.2 Documents en entrée.....	68
13.3 Documents en sortie.....	68

CONTENTS

FOREWORD	11
INTRODUCTION	15
1 Scope	21
2 Normative references	23
3 Definitions	23
4 Objectives and conformance	31
5 Software safety integrity levels	31
5.1 Objective	31
5.2 Requirements	33
6 Personnel and responsibilities	35
6.1 Objective	35
6.2 Requirements	35
7 Life cycle issues and documentation	37
7.1 Objectives	37
7.2 Requirements	39
8 Software requirements specification	45
8.1 Objectives	45
8.2 Input documents	45
8.3 Output documents	45
8.4 Requirements	45
9 Software architecture	49
9.1 Objectives	49
9.2 Input documents	49
9.3 Output documents	49
9.4 Requirements	49
10 Software design and implementation	53
10.1 Objectives	53
10.2 Input documents	53
10.3 Output documents	53
10.4 Requirements	53
11 Software verification and testing	59
11.1 Objective	59
11.2 Input documents	59
11.3 Output documents	59
11.4 Requirements	61
12 Software/hardware integration	65
12.1 Objectives	65
12.2 Input documents	65
12.3 Output documents	67
12.4 Requirements	67
13 Software validation	69
13.1 Objective	69
13.2 Input documents	69
13.3 Output documents	69

13.4	Exigences	68
14	Evaluation du logiciel	72
14.1	Objets	72
14.2	Documents en entrée	72
14.3	Documents en sortie	72
14.4	Exigences	72
15	Assurance qualité du logiciel	74
15.1	Objets	74
15.2	Documents en entrée	74
15.3	Documents en sortie	74
15.4	Exigences	74
16	Maintenance du logiciel	78
16.1	Objets	78
16.2	Documents en entrée	78
16.3	Documents en sortie	78
16.4	Exigences	80
17	Systèmes configurés par des données d'application	82
17.1	Objets	82
17.2	Documents en entrée	82
17.3	Documents en sortie	82
17.4	Exigences	84
	Annexe A (normative) Critères de sélection des techniques et mesures	102
	Annexe B (informative) Bibliographie des techniques	122
B.1	Intelligence artificielle – Correction des défauts (référéncé par l'article 9)	122
B.2	Programmes analysables (référéncé par l'article 10)	122
B.3	Tests de surcharge (référéncé par td3)	124
B.4	Analyse des valeurs aux limites (référéncé par td2, td3 et td8)	124
B.5	Rattrapage par régression (référéncé par l'article 9)	126
B.6	Schémas de cause et conséquence (référéncé par l'article 14 et td3)	126
B.7	Outils certifiés et ordinateurs certifiés (référéncé par l'article 10)	128
B.8	Listes de contrôle (référéncé par l'article 14 et td8)	128
B.9	Analyse de flux de contrôle (référéncé par td8)	130
B.10	Analyse des défaillances de mode commun (référéncé par l'article 14)	130
B.11	Analyse du flux de données (référéncé par td8)	132
B.12	Diagrammes des flux de données (référéncé par td5 et td7)	134
B.13	Enregistrement et analyse des données (référéncé par les articles 10 et 16)	136
B.14	Tables de décision (Tables de vérité) (référéncé par l'article 14 et td7)	136
B.15	Programmation défensive (référéncé par l'article 9)	138
B.16	Normes de conception et de codage (référéncé par D.1)	140
B.17	Programmation diversifiée (référéncé par l'article 9)	140
B.18	Reconfiguration dynamique (référéncé par l'article 9)	142
B.19	Tests de classes d'équivalence et de partition des données (référéncé par td2 et td3)	144
B.20	Codes correcteurs et détecteurs d'erreurs (référéncé par l'article 9)	144
B.21	Supposition d'erreurs (référéncé par td2 et td8)	144

13.4	Requirements	69
14	Software assessment	73
14.1	Objective	73
14.2	Input documents	73
14.3	Output documents	73
14.4	Requirements	73
15	Software quality assurance	75
15.1	Objectives	75
15.2	Input documents	75
15.3	Output documents	75
15.4	Requirements	75
16	Software maintenance	79
16.1	Objective	79
16.2	Input documents	79
16.3	Output documents	79
16.4	Requirements	81
17	Systems configured by application data	83
17.1	Objectives	83
17.2	Input documents	83
17.3	Output documents	83
17.4	Requirements	85
Annex A (normative) Criteria for the Selection of Techniques and Measures		103
Annex B (informative) Bibliography of techniques		123
B.1	Artificial Intelligence – Fault Correction (referenced by clause 9)	123
B.2	Analysable Programs (referenced by clause 10)	123
B.3	Avalanche/Stress Testing (referenced by dt6)	125
B.4	Boundary Value Analysis (referenced by dt2, dt3 and dt8)	125
B.5	Backward Recovery (referenced by clause 9)	127
B.6	Cause Consequence Diagrams (referenced by clause 14 and dt3)	127
B.7	Certified Tools and Certified Translators (referenced by clause 10)	129
B.8	Checklists (referenced by clause 14 and dt8)	129
B.9	Control Flow Analysis (referenced by dt8)	131
B.10	Common Cause Failure Analysis (referenced by clause 14)	131
B.11	Data Flow Analysis (referenced by dt8)	133
B.12	Data Flow Diagrams (referenced by dt5 and dt7)	135
B.13	Data Recording and Analysis (referenced by clauses 10 and 16)	137
B.14	Decision Tables (Truth Tables) (referenced by clause 14 and dt7)	137
B.15	Defensive Programming (referenced by clause 9)	139
B.16	Design and Coding Standards (referenced by dt1)	141
B.17	Diverse Programming (referenced by clause 9)	141
B.18	Dynamic Reconfiguration (referenced by clause 9)	143
B.19	Equivalence Classes and Input Partition Testing (referenced by D2 and dt3)	145
B.20	Error Detecting and Correcting Codes (referenced by clause 9)	145
B.21	Error Guessing (referenced by dt2 and dt8)	145

B.22	Insertion d'erreurs (référéncé par td2)	146
B.23	Analyse par arbre des événements (référéncé par l'article 14)	146
B.24	Inspection de Fagan (référéncé par td8)	148
B.25	Programmation par assertion (référéncé par l'article 9).....	148
B.26	SEEA – Analyse des effets des erreurs du logiciel (référéncé par les articles 9, 11 et 14)	150
B.27	Détection des défauts et diagnostic (référéncé par l'article 9)	152
B.28	Analyse par arbre des causes (référéncé par les articles 9 et 14)	152
B.29	Automates à états finis/Schémas de transition d'état (référéncé par td5 et td7).....	154
B.30	Méthodes formelles (référéncé par les article 8 et 10 et td5).....	156
B.31	Preuve formelle (référéncé par l'article 11)	156
B.32	Rattrapage par progression (référéncé par l'article 9)	166
B.33	Dégradation contrôlée	166
B.34	Etude de risque et d'opérabilité HAZOP (Hazard and Operability Study)	168
B.35	Analyse d'impact (référéncé par l'article 16)	170
B.36	Masquage d'informations/Encapsulage (référéncé par td9)	170
B.37	Tests d'interface (référéncé par l'article 10).....	172
B.38	Sous-ensemble de langage (référéncé par l'article 10 et 14).....	172
B.39	Mémorisation des cas exécutés (référéncé par l'article 9).....	174
B.40	Bibliothèque de modules et de composants sécurisés et vérifiés (référéncé par l'article 10).....	174
B.41	Modèles de Markov (référéncé par l'article 14)	176
B.42	Métriques (référéncé par les articles 11 et 14).....	176
B.43	Approche modulaire (référéncé par td1)	178
B.44	Simulation de Monte Carlo	180
B.45	Modélisation des performances (référéncé par td2 et td5).....	180
B.46	Exigences en matière de performance (référéncé par td6).....	182
B.47	Tests probabilistes (référéncé par les articles 11 et 13).....	182
B.48	Simulation du processus (référéncé par td3).....	184
B.49	Prototypage/Animation (référéncé par td3 et td5).....	186
B.50	Bloc de rattrapage (référéncé par l'article 9).....	186
B.51	Schéma bloc de la fiabilité (référéncé par l'article 14)	188
B.52	Temps de réponse et contraintes de place mémoire (référéncé par td6)	188
B.53	Rattrapage par réexécution (référéncé par l'article 9)	188
B.54	Sécurité contrôlée (Safety Bag) (référéncé par l'article 9)	190
B.55	Analyse des chemins insidieux (référéncé par td8)	190
B.56	Gestion de la configuration du logiciel (référéncé par l'article 15).....	192
B.57	Langages de programmation à fort typage (référéncé par l'article 10)	192
B.58	Tests structurels (référéncé par td2).....	194
B.59	Schémas de structure (référéncé par td5).....	196
B.60	Méthode structurée (référéncé par les articles 8 et 10)	198
B.61	Programmation structurée (référéncé par l'article 10)	206
B.62	Langages de programmations adaptés (référéncé par td4)	206
B.63	Exécution symbolique (référéncé par td8).....	208

B.22	Error Seeding (referenced by dt2)	147
B.23	Event Tree Analysis (referenced by clause 14)	147
B.24	Fagan Inspections (referenced by dt8).....	149
B.25	Failure Assertion Programming (referenced by clause 9)	149
B.26	SEEA – Software Error Effect Analysis (referenced by clauses 9, 11 and 14)	151
B.27	Fault Detection and Diagnosis (referenced by clause 9).....	153
B.28	Fault Tree Analysis (referenced by clauses 9 and 14)	153
B.29	Finite State Machines/State Transition Diagrams (referenced by dt5 and dt7)	155
B.30	Formal Methods (referenced by clauses 8 and 10 and dt5)	157
B.31	Normal Proof (referenced by clause 11)	167
B.32	Forward Recovery (referenced by clause 9).....	167
B.33	Graceful Degradation	167
B.34	Hazard and Operability Study (HAZOP)	169
B.35	Impact Analysis (referenced by clause 16).....	171
B.36	Information Hiding / Encapsulation (referenced by dt9)	171
B.37	Interface Testing (referenced by clause 10).....	173
B.38	Language Subset (referenced by clause 10 and dt4).....	173
B.39	Memorising Executed Cases (referenced by clause 9).....	175
B.40	Library of Trusted/Verified Modules and Components (referenced by clause 10)	175
B.41	Markov Models (referenced by clause 14).....	177
B.42	Metrics (referenced by clauses 11 and 14)	177
B.43	Modular Approach (referenced by dt9).....	179
B.44	Monte Carlo Simulation	181
B.45	Performance Modelling (referenced by dt2 and dt5).....	181
B.46	Performance Requirements (referenced by dt6).....	183
B.47	Probabilistic Testing (referenced by clauses 11 and 13).....	183
B.48	Process Simulation (referenced by dt3)	185
B.49	Prototyping/Animation (referenced by dt3 and dt5).....	187
B.50	Recovery Block (referenced by clause 9).....	187
B.51	Reliability Block Diagram (referenced by clause 14).....	189
B.52	Response Timing and Memory Constraints (Referenced by dt6)	189
B.53	Retry/Fault Recovery Mechanisms (referenced by clause 9)	189
B.54	Safety Bag (referenced by clause 9)	191
B.55	Sneak Circuit Analysis (referenced by dt8)	191
B.56	Software Configuration Management (referenced by clause 15).....	193
B.57	Strongly Typed Programming Languages (referenced by clause 10)	193
B.58	Structure Based Testing (referenced by dt2).....	195
B.59	Structure Diagrams (referenced by dt5).....	197
B.60	Structured Methodology (referenced by clauses 8 and 10)	199
B.61	Structured Programming (referenced by clause 10)	207
B.62	Suitable Programming Languages (referenced by dt4).....	207
B.63	Symbolic Execution (referenced by dt8).....	209

B.64	Réseaux de Pétri temporels (référéncé par td5 et td7)	208
B.65	Compilateur éprouvé à l'utilisation (référéncé par l'article 10)	210
B.66	Revue/Examens de la conception (référéncé par td8)	212
B.67	Logique floue (référéncé par l'article 10).....	212
B.68	Programmation orientée objet (référéncé par l'article 10).....	214
B.69	Traçabilité (référéncé par l'article 11)	216
Figure 1	– Niveaux d'intégrité de la sécurité pour les systèmes liés à la sécurité	90
Figure 2	– Démarche de la sécurité du logiciel	92
Figure 3	– Cycle de vie 1 du développement	94
Figure 4	– Cycle de vie 2 du développement	96
Figure 5	– Indépendance en fonction du niveau d'intégrité de la sécurité du logiciel	98
Figure 6	– Relation entre le développement du système générique et le développement du cas spécifique	100
Table de correspondance	des documents	42
Tableau A.1	– Problèmes liés au cycle de vie et documentation (article 7).....	104
Tableau A.2	– Spécification des Exigences du Logiciel (article 8).....	104
Tableau A.3	– Architecture du Logiciel (article 9)	106
Tableau A.4	– Conception et mise en œuvre du Logiciel (article 10).....	108
Tableau A.5	– Vérification et Tests (article 11).....	110
Tableau A.7	– Validation du Logiciel (article 13).....	110
Tableau A.8	– Articles à évaluer	112
Tableau A.9	– Evaluation du logiciel (article 14), Techniques d'évaluation	112
Tableau A.10	– Assurance qualité du logiciel (article 15).....	112
Tableau A.11	– Maintenance du logiciel (article 16).....	114
Tableau A.12	– Normes de conception et de codage (td1) Référéncé par l'article 10	114
Tableau A.13	– Analyse et tests dynamiques (td2) Référéncé par les articles 11 et 14	114
Tableau A.14	– Test fonctionnel/boîte noire (td3) Référéncé par les articles 10, 12, 13 et 14	116
Tableau A.15	– Langages de programmation (td4) Référéncé par l'article 10.....	116
Tableau A.16	– Modélisation (td5) Référéncé par l'article 13	118
Tableau A.17	– Tests de performance (td6) Référéncé par les articles 10, 12 et 13.....	118
Tableau A.18	– Méthodes semi-formelles (td7) Référéncé par les articles 8 et 10	118
Tableau A.19	– Analyse statique (td8) Référéncé par les articles 11 et 14.....	120
Tableau A.20	– Approche modulaire (td9) Référéncé par l'article 10.....	120

B.64	Time Petri Nets (referenced by dt5 and dt7)	209
B.65	Translator Proven In Use (referenced by clause 10)	211
B.66	Walk-throughs/Design Reviews (referenced by dt8)	213
B.67	Fuzzy Logic (referenced by clause 10).....	213
B.68	Object Oriented Programming (referenced by clause 10)	215
B.69	Traceability (referenced by clause 11)	217
Figure 1	– Integrity Levels for Safety-Related Systems	91
Figure 2	– Software Safety Route Map	93
Figure 3	– Development Life Cycle 1.....	95
Figure 4	– Development Life Cycle 2.....	97
Figure 5	– Independence Versus Software Integrity Level	99
Figure 6	– Relationship between Generic System Development and Application Development.....	101
Documents cross-reference table		43
Table A.1	– Life Cycle Issues and Documentation (clause 7).....	105
Table A.2	– Software Requirements Specification (clause 8).....	105
Table A.3	– Software Architecture (clause 9)	107
Table A.4	– Software Design and Implementation (clause 10)	109
Table A.5	– Verification and Testing (clause 11)	111
Table A.6	– Software/Hardware Integration (clause 12)	111
Table A.7	– Software Validation (clause 13).....	111
Table A.8	– Clauses to be assessed	113
Table A.9	– Software Assessment (clause 14) Assessment Techniques	113
Table A.10	– Software Quality Assurance (clause 15)	113
Table A.11	– Software Maintenance (clause 16).....	115
Table A.12	– Design and Coding Standards (dt1) Referenced by clause 10.....	115
Table A.13	– Dynamic Analysis and Testing (dt2) Referenced by clauses 11 and 14.....	115
Table A.14	– Functional/Block Box Test (dt3) Referenced by clauses 10,12, 13 and 14	117
Table A.15	– Programming Languages (dt4) Referenced by clause 10	117
Table A.16	– Modelling (dt5) Referenced by clause 13.....	119
Table A.17	– Performance Testing (dt6) Referenced by clauses 10, 12 and 13.....	119
Table A.18	– Semi-Formal Methods (dt7) Referenced by clauses 8 and 10.....	119
Table A.19	– Static Analysis (dt8) Referenced by clauses 11 and 14	121
Table A.20	– Modular Approach (dt9) Referenced by clause 10.....	121

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**APPLICATIONS FERROVIAIRES –
SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION
ET DE TRAITEMENT –
LOGICIELS POUR SYSTÈMES DE COMMANDE
ET DE PROTECTION FERROVIAIRE**

AVANT-PROPOS

- 1) La CEI (Commission Électrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des documents de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62279 a été établie par le comité d'études 9 de la CEI: Matériel électrique ferroviaire.

La présente norme, basée sur la norme européenne EN 50128 (2001), a été préparée par le sous-comité 9XA: Systèmes de signalisation de télécommunications et de traitement, du Comité Technique 9 de CENELEC: Applications électriques et électroniques dans le domaine ferroviaire. Elle a été soumise aux Comités Nationaux pour vote suivant la procédure par voie express, par les documents suivants:

FDIS	Rapport de vote
9/687/FDIS	9/704/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant contribué à l'approbation de cette norme.

Cette norme doit être lue conjointement avec la CEI 62278 et la norme ENV 50129:1998.

La présente norme ne suit pas les règles de structure des normes internationales comme le spécifie la Partie 2 des Directives ISO/CEI.

NOTE Cette norme a été reproduite sans modifications importantes de son contenu original ou de ses règles structurelles.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RAILWAY APPLICATIONS –
COMMUNICATIONS, SIGNALLING AND PROCESSING SYSTEMS –
SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62279 has been prepared by IEC technical committee 9: Electric railway equipment.

This standard, based on the European Norm EN 50128 (2001), was prepared by subcommittee 9XA: Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X: Electrical and electronic applications for railways. It was submitted to the National Committees for voting under the Fast Track Procedure as the following documents:

FDIS	Report on voting
9/687/FDIS	9/704/RVD

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

This standard shall be read in conjunction with IEC 62278 and ENV 50129:1998.

This standard does not follow the rules for structuring International Standards as given in Part 2 of the ISO/IEC Directives.

NOTE This standard has been reproduced without significant modification to its original content or drafting.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2008. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

The committee has decided that the contents of this publication will remain unchanged until 2008. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

La présente Norme internationale fait partie intégrante d'un groupe de normes connexes. Les autres éléments de ce groupe sont la Norme internationale CEI 62278 et la norme européenne ENV 50129. La CEI 62278 traite des problèmes liés aux systèmes de façon très générale, tandis que la norme ENV 50129 aborde le processus d'approbation des systèmes individuels qui peuvent exister dans le cadre du système global de commande et de protection ferroviaire. La présente norme traite en particulier des méthodes qu'il est nécessaire d'utiliser pour fournir des logiciels répondant aux exigences d'intégrité de la sécurité imposées par ces considérations plus larges.

L'orientation de la présente norme doit beaucoup au travail préalable effectué par le groupe de travail (GT) 9 du comité d'études 65 de la CEI. Le travail du GT 9 a abouti à une norme générique, destinée aux logiciels des systèmes de sécurité, qui est désormais intégrée dans la série de normes CEI 61508*. Un aspect spécifique du travail effectué par le GT 9 est l'inclusion d'une intégrité logicielle de niveau 0, applicable aux logiciels non liés à la sécurité, ainsi que d'une intégrité logicielle de niveaux 1 à 4, applicable aux logiciels liés à la sécurité et critiques pour celle-ci. La présente norme couvre également les cinq niveaux d'intégrité logicielle.

Le travail de l'IRSE (Institution of Railway Signal Engineers) a également été pris en compte, notamment son rapport technique numéro 1 qui traite du même sujet.

Le concept-clé de la présente norme est celui des niveaux d'intégrité de la sécurité logicielle. Plus les conséquences d'une défaillance logicielle sont dangereuses, plus le niveau d'intégrité de la sécurité logicielle est élevé.

La présente norme a identifié des techniques et mesures applicables aux cinq niveaux d'intégrité de la sécurité logicielle dans lesquels 0 correspond au niveau minimum et 4 au niveau le plus élevé. Les niveaux 1 à 4 font référence aux logiciels liés à la sécurité, alors que le niveau 0 s'applique aux logiciels non liés à la sécurité. Ce niveau a été inclus dans la norme de manière normative, de façon à permettre une transition progressive entre les développements du logiciel des systèmes non liés à la sécurité et ceux des systèmes liés à la sécurité. Les techniques et mesures requises pour chaque niveau d'intégrité de la sécurité logicielle et pour le niveau non lié à la sécurité sont indiquées dans les tableaux. Dans la présente version, les techniques requises pour le niveau 1 sont identiques à celles du niveau 2, et les techniques requises pour le niveau 3 sont identiques à celles du niveau 4. La présente norme ne fournit aucune ligne directrice sur le niveau d'intégrité logicielle approprié pour un risque donné. Cette décision sera tributaire de nombreux facteurs, notamment de la nature de l'application, de la limite dans laquelle les autres systèmes assurent des fonctions de sécurité, ainsi que de facteurs socio-économiques.

C'est la fonction de la CEI 62278 et de la norme ENV 50129 de spécifier les fonctions de sécurité affectées au logiciel.

La présente norme spécifie les mesures nécessaires au respect de ces exigences. Le processus est illustré par la Figure 1.

La CEI 62278 et la norme ENV 50129 exigent qu'une approche systématique soit adoptée pour ce qui concerne

- i) l'identification des dangers, des risques et des critères de sécurité;
- ii) l'identification de la réduction des risques nécessaire pour répondre aux critères de sécurité;
- iii) la définition d'une Spécification des Exigences de Sécurité du Système, globale, qui décrit les protections indispensables en vue d'atteindre la réduction des risques requise;

* CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.*

INTRODUCTION

This International Standard is part of a group of related standards. The others are the International Standard IEC 62278 and the European Norm ENV 50129. IEC 62278 addresses system issues on the widest scale, while ENV 50129 addresses the approval process for individual systems which may exist within the overall railway control and protection system. This standard concentrates on the methods which need to be used in order to provide software which meets the demands for safety integrity which are placed upon it by these wider considerations.

This standard owes much of its direction to earlier work done by Working Group (WG) 9 of IEC/TC 65. The work of WG 9 resulted in a generic standard for software for safety systems which is now part of standards of IEC 61508 series*. A particular aspect of the work by WG 9 is its inclusion of Software Integrity Level 0, which covers non-safety software, as well as Software Integrity Levels 1 to 4, which cover safety-related and safety-critical software. This standard also covers all five Software Integrity Levels.

Account has also been taken of the work of the Institution of Railway Signal Engineers (the IRSE), in particular its Technical Report Number 1, which addressed the same topic.

The key concept of this standard is that of levels of software safety integrity. The more dangerous the consequences of a software failure, the higher the software safety integrity level will be.

This standard has identified techniques and measures for 5 levels of software safety integrity where 0 is the minimum level and 4 the highest level. Four of these levels, 1 to 4, refer to safety-related software, whilst level 0 refers to non-safety-related software. This level has been included as normative in order to allow a smooth transition between software developments for non-safety-related systems and those for safety-related systems. The required techniques and measures for each software safety integrity level and for the non-safety-related level are shown in the tables. In this version, the required techniques for level 1 are the same as for level 2, and the required techniques for level 3 are the same as for level 4. This standard does not give guidance on which level of software integrity is appropriate for a given risk. This decision will depend upon the many factors including the nature of the application, the extent to which other systems carry out safety functions and social and economic factors.

It is the function of IEC 62278 and ENV 50129 to specify the safety functions allocated to software.

This standard specifies those measures necessary to achieve these requirements. The process is illustrated in Figure 1.

IEC 62278 and ENV 50129 require that a systematic approach be taken to

- i) identify hazards, risks and risk criteria;
- ii) identify the necessary risk reduction to meet the risk criteria;
- iii) define an overall System Safety Requirements Specification for the safeguards necessary to achieve the required risk reduction;

* IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*.

- iv) le choix d'une architecture de système adaptée;
- v) la planification, le contrôle et la maîtrise des activités techniques et de management nécessaires pour transformer la Spécification des Exigences de Sécurité du Système en un système de sécurité dont le niveau de sécurité (ou intégrité de sécurité) est validé.

Au fur et à mesure que la spécification se décompose en une conception comprenant des composants et des systèmes liés à la sécurité, l'affectation des niveaux d'intégrité de la sécurité est effectuée. Finalement cela conduit aux niveaux d'intégrité de sécurité logicielle requis.

L'état actuel de la technique est tel que ni l'application des méthodes d'assurance qualité (mesures dites d'évitement de «fautes»), ni l'application d'approches logicielles à tolérance aux «fautes» ne peuvent garantir la sécurité absolue du système. Il n'existe aucun moyen connu de prouver l'absence de défauts dans un logiciel lié à la sécurité raisonnablement complexe, en particulier l'absence de défauts de spécification et de conception.

Les principes appliqués dans le développement de logiciels à haute intégrité, incluent, sans s'y limiter

- des méthodes de conception descendante;
- la modularité;
- la vérification de chaque phase du cycle de vie du développement;
- des modules vérifiés et des bibliothèques de modules;
- une documentation claire;
- des documents aptes à être audités; et
- des tests de validation.

Il est indispensable que ces principes et ceux associés soient correctement appliqués. La présente norme spécifie le niveau d'assurance requis afin de le démontrer pour chaque niveau d'intégrité de la sécurité logicielle.

Une fois que la Spécification des Exigences de Sécurité du Système identifiant toutes les fonctions de sécurité affectées au logiciel et déterminant le niveau d'intégrité de la sécurité du système a été obtenue ou produite, les étapes fonctionnelles de l'application de la présente norme, décrites à la Figure 2, sont les suivantes:

- i) définir la Spécification des Exigences du Logiciel et examiner parallèlement l'architecture du logiciel. C'est au travers de l'architecture logicielle qu'est développée la stratégie de base en matière de sécurité pour le logiciel et le niveau d'intégrité de la sécurité logicielle (articles 5, 8 et 9);
- ii) concevoir, développer et tester le logiciel selon le Plan d'Assurance Qualité du Logiciel, le niveau d'intégrité de la sécurité logicielle et le cycle de vie du logiciel (article 10);
- iii) intégrer le logiciel sur le matériel cible (article 12);
- iv) valider le logiciel (article 13);
- v) si la maintenance du logiciel est requise pendant la vie opérationnelle, le cas échéant réactiver la présente norme (article 16).

Un certain nombre d'activités se déroulent au cours du développement du logiciel, parmi lesquelles la vérification (article 11), l'évaluation (article 14) et l'assurance qualité (article 15).

Des exigences sont fournies en ce qui concerne les systèmes configurés par les données d'application (article 17).

Des exigences sont également fournies en ce qui concerne la compétence du personnel impliqué dans le développement du logiciel (article 6).

- iv) select a suitable system architecture;
- v) plan, monitor and control the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety performance (or safety integrity).

As decomposition of the specification into a design comprising safety-related systems and components takes place, further allocation of safety integrity levels is performed. Ultimately this leads to the required software safety integrity levels.

The current state of the art is such that neither the application of quality assurance methods (so-called fault-avoiding measures) nor the application of software fault-tolerant approaches can guarantee the absolute safety of the system. There is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults.

The principles applied in developing high-integrity software include, but are not restricted to

- top-down design methods;
- modularity;
- verification of each phase of the development life cycle;
- verified modules and module libraries;
- clear documentation;
- auditable documents; and
- validation testing.

These and related principles must be correctly applied. This standard specifies the level of assurance required to demonstrate this at each software safety integrity level.

After the System Safety Requirements Specification, which identifies all safety functions allocated to software and determines the system safety integrity level, has been obtained or produced, the functional steps in the application of this standard are shown in Figure 2 and are as follows:

- i) define the Software Requirements Specification and in parallel consider the software architecture. The software architecture is where the basic safety strategy is developed for the software and the software safety integrity level (clauses 5, 8 and 9);
- ii) design, develop and test the software according to the Software Quality Assurance Plan, software safety integrity level and the software life cycle (clause 10);
- iii) integrate the software on the target hardware (clause 12);
- iv) validate the software (clause 13);
- v) if software maintenance is required during operational life then re-activate this standard as appropriate (clause 16).

A number of activities run across the software development. These include verification (clause 11), assessment (clause 14) and quality assurance (clause 15).

Requirements are given for systems which are configured by application data (clause 17).

Requirements are also given for the competency of staff involved in software development (clause 6).

La norme n'impose pas l'utilisation d'un cycle de vie spécifique de développement du logiciel. Cependant un cycle de vie recommandé et un ensemble de documents sont fournis (article 7 et Figures 3 et 4).

Les tableaux ont été établis pour classer diverses techniques/mesures par rapport aux cinq niveaux d'intégrité de la sécurité logicielle. Les tableaux se trouvent à l'annexe A. En référence croisée avec les tableaux, la bibliographie fournit une brève description de chaque technique/mesure avec des références à des sources complémentaires d'informations. La bibliographie se trouve à l'annexe B.

The standard does not mandate the use of a particular software development life cycle. However, a recommended life cycle and documentation set are given (clause 7 and Figures 3 and 4).

Tables have been formulated ranking various techniques/measures against the 5 software safety integrity levels. The tables are in annex A. Cross-referenced to the tables is a bibliography giving a brief description of each technique/measure with references to further sources of information. The bibliography is in annex B.

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – LOGICIELS POUR SYSTÈMES DE COMMANDE ET DE PROTECTION FERROVIAIRE

1 Domaine d'application

1.1 La présente Norme internationale spécifie les procédures et les exigences techniques applicables au développement des systèmes électroniques programmables utilisés dans les applications de commande et de protection ferroviaires. Elle est destinée à être utilisée dans tout domaine comportant des implications de sécurité. Ces applications sont susceptibles d'aller du très critique tel que la signalisation de sécurité au non critique comme les systèmes de gestion de l'information. Il est permis de mettre en oeuvre ces systèmes à l'aide de microprocesseurs dédiés, de contrôleurs logiques programmables, de systèmes multi-processeurs distribués, de grands systèmes dotés d'un ordinateur central ou à l'aide d'autres architectures.

1.2 La présente norme est exclusivement applicable au logiciel et à l'interaction entre le logiciel et le système auquel il appartient.

1.3 Les niveaux d'intégrité de la sécurité logicielle supérieurs à 0 sont destinés à être utilisés pour des systèmes dans lesquels les conséquences d'une défaillance pourraient provoquer la mort. Des considérations économiques ou environnementales, toutefois, peuvent également justifier l'utilisation de niveaux supérieurs d'intégrité de la sécurité logicielle.

1.4 La présente norme s'applique à tous les logiciels utilisés dans le développement et l'implémentation des systèmes de commande et de protection ferroviaires, y compris

- la programmation de l'application;
- les systèmes d'exploitation;
- les outils d'aide;
- le microprogramme.

La programmation de l'application comprend une programmation de haut niveau, une programmation de bas niveau et une programmation spécifique personnalisée (par exemple: la logique à contact du contrôleur logique programmable).

1.5 L'utilisation de logiciel et d'outils standards disponibles sur le marché est également abordée dans la présente norme.

1.6 La présente norme traite également des exigences applicables aux systèmes configurés par des données d'application.

1.7 La présente norme ne vise pas à traiter des problèmes commerciaux. Il convient de les traiter comme une partie essentielle de tout accord contractuel. Tous les articles de la présente norme font l'objet d'une étude soignée dans toute situation commerciale.

1.8 La présente norme n'a pas d'effet rétroactif. Elle s'applique donc principalement aux nouveaux développements et n'est applicable intégralement aux systèmes existants que s'ils font l'objet de modifications importantes. Seul l'article 16 s'applique pour les modifications mineures.

RAILWAY APPLICATIONS – COMMUNICATIONS, SIGNALLING AND PROCESSING SYSTEMS – SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS

1 Scope

1.1 This International Standard specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is aimed at use in any area where there are safety implications. These may range from the very critical, such as safety signalling to the non-critical, such as management information systems. These systems may be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.

1.2 This standard is applicable exclusively to software and the interaction between software and the system of which it is part.

1.3 Software safety integrity levels above zero are for use in systems in which the consequences of failure could include loss of life. Economic or environmental considerations, however, may also justify the use of higher software safety integrity levels.

1.4 This standard applies to all software used in development and implementation of railway control and protection systems including

- application programming;
- operating systems;
- support tools;
- firmware.

Application programming comprises high-level programming, low-level programming and special-purpose programming (for example, Programmable Logic Controller ladder logic).

1.5 The use of standard, commercially available software and tools is also addressed in this standard.

1.6 This standard also addresses the requirements for systems configured by application data.

1.7 This standard is not intended to address commercial issues. These should be addressed as an essential part of any contractual agreement. All the clauses of this standard will need careful consideration in any commercial situation.

1.8 This standard is not intended to be retrospective. It therefore applies primarily to new developments and only applies in its entirety to existing systems if these are subjected to major modifications. For minor changes, only clause 16 applies.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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).

CEI 62278, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)* ¹

CEI 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés* ¹

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts* ¹

ISO 9000:2000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

ISO 9000-3:1997, *Normes pour le management de la qualité et l'assurance de la qualité – Partie 3 – Lignes directrices pour l'application de l'ISO 9001:1994 au développement, à la mise à disposition et à la maintenance du logiciel*

ISO 9001:1994, *Systèmes qualité – Modèle pour l'assurance de la qualité en conception, développement, production, installation et prestations associées*

ENV 50129:1998, *Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation*

¹ A publier.

2 Normative references

The following referenced documents are indispensable for the application 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, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)* ¹

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems* ¹

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems* ¹

ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*

ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software*

ISO 9001:1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

ENV 50129:1998, *Railway applications – Safety related electronic systems for signalling*

¹ To be published.