



SLOVENSKI STANDARD

SIST EN 50128:2011

01-september-2011

Nadomešča:
SIST EN 50128:2002

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Programska oprema za železniške krmilne in zaščitne sisteme

Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme

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

Ta slovenski standard je istoveten z: EN 50128:2011

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50128:2011

en,fr

NORME EUROPÉENNE
EUROPÄISCHE NORM
EUROPEAN STANDARD

EN 50128

Juin 2011

ICS 35.240.60; 45.020; 93.100

Remplace EN 50128:2001

Version française

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

Bahnanwendungen -
Telekommunikationstechnik,
Signaltechnik und
Datenverarbeitungssysteme -
Software für Eisenbahnsteuerungs- und
Überwachungssysteme

Railway applications -
Communication, signalling and processing
systems -
Software for railway control and protection
systems

La présente Norme Européenne a été adoptée par le CENELEC le 2011-04-25. Les membres du CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme Européenne.

Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Secrétariat Central ou auprès des membres du CENELEC.

La présente Norme Européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CENELEC dans sa langue nationale, et notifiée au Secrétariat Central, a le même statut que les versions officielles.

Les membres du CENELEC sont les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède et Suisse.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Bruxelles

Sommaire

Foreword	5
Introduction	7
1 Domaine d'application	10
2 Références normatives.....	11
3 Termes, définitions et abréviations.....	11
3.1 Termes et définitions	11
3.2 Abréviations	15
4 Objectifs, conformité et niveaux d'intégrité de sécurité du logiciel	16
5 Organisation et gestion du développement logiciel	17
5.1 Organisation, rôles et responsabilités.....	17
5.2 Compétence du personnel	21
5.3 Questions relatives au cycle de vie et à la documentation	21
6 Assurance du logiciel.....	24
6.1 Test du logiciel.....	24
6.2 Vérification du logiciel.....	26
6.3 Validation du logiciel	28
6.4 Évaluation du logiciel	29
6.5 Assurance Qualité du Logiciel.....	31
6.6 Contrôle des modifications et des évolutions	34
6.7 Outils et langages	35
7 Développement de logiciel générique	39
7.1 Cycle de vie et documentation pour logiciel générique.....	39
7.2 Exigences relatives au logiciel	39
7.3 Architecture et Conception	42
7.4 Conception du Composant.....	48
7.5 Réalisation et Test des composants.....	51
7.6 Intégration.....	52
7.7 Tests d'Ensemble du Logiciel / Validation Finale.....	54
8 Développement de données d'application ou d'algorithmes d'application : systèmes configurés par des données d'application ou par des algorithmes d'application	56
8.1 Objectifs.....	56
8.2 Documents en entrée.....	57

8.3 Documents en sortie.....	57
8.4 Exigences	57
9 Déploiement et maintenance du logiciel	62
9.1 Déploiement du logiciel.....	62
9.2 Maintenance du logiciel	64
Annexe A (normative) Critères de sélection des techniques et mesures	67
A.1 Tableaux d'articles	68
A.2 Tableaux détaillés	76
Annexe B (normative) Principaux rôles et responsabilités relatifs au logiciel	82
Annexe C (informative) Résumé du contrôle des documents	91
Annexe D (informative) Bibliographie des techniques	93
D.1 Intelligence artificielle - Correction des défauts	93
D.2 Programmes analysables	93
D.3 Tests en avalanche/en surcharge.....	94
D.4 Analyse des valeurs aux limites	94
D.5 Rattrapage par régression	95
D.6 Schémas de cause et de conséquence	95
D.7 Listes de contrôle	95
D.8 Analyse de Flux de Contrôle	96
D.9 Analyse des défaillances de mode commun	96
D.10 Analyse du flux de données	97
D.11 Organigrammes des données	97
D.12 Enregistrement et analyse des données	98
D.13 Tables de décision (Tables de vérité)	99
D.14 Programmation défensive	99
D.15 Normes de codage et Guide de style	100
D.16 Programmation diversifiée	100
D.17 Reconfiguration dynamique	101
D.18 Tests de classes d'équivalence et de partition d'entrée	101
D.19 Codes de détection et de correction d'erreurs	102
D.20 Supposition d'erreurs	102
D.21 Insertion d'erreurs	102
D.22 Analyse par arbre des événements	103
D.23 Inspection de Fagan	103
D.24 Programmation par assertion des défaillances	103
D.25 AEEL – Analyse des Effets des Erreurs du Logiciel	104
D.26 Détection des défauts et diagnostic	105
D.27 Automates à états finis/Schémas de transitions d'état	105
D.28 Méthodes formelles	106
D.28.1 CSP - Processus Séquentiels de Communication	107
D.28.2 CCS - Algèbre des Systèmes de Transmission	107
D.28.3 HOL - Logique d'Ordre Supérieur	107
D.28.4 LOTOS	108
D.28.5 OBJ	108
D.28.6 Logique temporelle	109

D.28.7 VDM - Méthode de Développement de Vienne	109
D.28.8 Méthode Z	109
D.28.9 Méthode B	110
D.28.10 Vérification du modèle	111
D.29 Preuve formelle	111
D.30 Rattrapage par progression	112
D.31 Dégradation contrôlée	112
D.32 Analyse d'impact	112
D.33 Masquage d'informations/Encapsulation	113
D.34 Tests d'interface	113
D.35 Sous-ensemble de langage	114
D.36 Mémorisation des cas exécutés	114
D.37 Métriques	114
D.38 Approche modulaire	115
D.39 Modélisation des performances	115
D.40 Exigences en matière de performance	116
D.41 Tests probabilistes	116
D.42 Simulation de processus	117
D.43 Prototypage/Animation	118
D.44 Bloc de rattrapage	118
D.45 Temps de réponse et contraintes de place mémoire	118
D.46 Rattrapage par ré-exécution	118
D.47 Sécurité Contrôlée	119
D.48 Gestion de la configuration du logiciel	119
D.49 Langages de programmation à fort typage	119
D.50 Tests structurels	120
D.51 Schémas de structure	120
D.52 Méthodologie structurée	121
D.53 Programmation structurée	121
D.54 Langages de programmation adaptés	122
D.55 Réseaux de Pétri temporels	123
D.56 Révisions structurées/ Revues de la conception	123
D.57 Programmation orientée objet	124
D.58 Traçabilité	124
D.59 Métaprogrammation	125
D.60 Programmation procédurale	125
D.61 Graphes séquentiels de fonction	126
D.62 Schéma à contact	126
D.63 Diagramme fonctionnel	126
D.64 Graphe d'états ou Diagramme d'états	126
D.65 Modélisation de données	127
D.66 Diagramme de flux de commande/Grappe de flux de commande	127
D.67 Diagramme de séquence	128
D.68 Méthodes de spécification en tableaux	129
D.69 Langage spécifique à l'application	129
D.70 UML (Unified Modeling Language, langage de modélisation unifié)	129
D.71 Langages spécifiques à un domaine	130
Bibliographie	132

Avant-propos

La présente Norme Européenne a été préparée par le SC 9XA, Systèmes de signalisation, de télécommunications et de traitement, du comité technique CENELEC TC 9X, Applications électriques et électroniques dans le domaine ferroviaire.

Le texte du projet a été soumis au vote formel et a été approuvé par le CENELEC comme EN 50128 le 2011-04-25.

Ce document remplace l'EN 50128:2001.

Les principales modifications par rapport à l'EN 50128:2001 sont énumérées ci-après :

- des exigences relatives à la gestion et à l'organisation, à la définition des rôles et des compétences, au déploiement et à la maintenance des logiciels ont été ajoutées;
- un nouvel article concernant les outils a été ajouté, fondé sur l'EN 61508-2:2010;
- les Tableaux dans l'Annexe A ont été mis à jour.

L'attention du lecteur est attiré sur la possibilité que certains éléments de ce document peuvent être couverts par des brevets. Le CEN et le CENELEC ne sauraient être tenus pour responsable de l'identification de tels brevets.

Les dates suivantes ont été fixées:

- | | | |
|--|-------|------------|
| – date limite à laquelle l'EN doit être mise en application au niveau national par publication d'une norme nationale identique ou par entérinement | (dop) | 2012-04-25 |
| – date limite à laquelle les normes nationales conflictuelles doivent être annulées | (dow) | 2014-04-25 |

Il convient de lire la présente Norme Européenne conjointement à l'EN 50126-1:1999 «Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1 : Exigences de base et procédés génériques» et à l'EN 50129:2003 «Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation».

Figures

Figure 1 – Démarche illustrative relative au logiciel.....	9
Figure 2 – Illustration de la structure organisationnelle préférentielle	18
Figure 3 – Cycle de vie de développement 1.....	23
Figure 4 – Illustration d'un cycle de vie de développement 2	24

Tableaux

Tableau 1 - Relation entre les classe d'outils et les paragraphes applicables	38
Tableau A.1– Problèmes liés au cycle de vie et Documentation (5.3)	68
Tableau A.2 – Spécification des Exigences du Logiciel (7.2)	70
Tableau A.3 – Architecture du Logiciel (7.3).....	71
Tableau A.4– Conception et mise en œuvre du logiciel (7.4).....	72
Tableau A.5 – Vérification et Tests (6.2 et 7.3)	73
Tableau A.6 – Intégration (7.6)	73
Tableau A.7– Tests d'Ensemble du Logiciel (6.2et 7.7)	73
Tableau A.8 – Techniques d'analyse logicielle (6.3).....	74
Tableau A.9 – Assurance Qualité du logiciel (6.5).....	74
Tableau A.10 – Maintenance du Logiciel (9.2)	74
Tableau A.11 – Techniques de préparation des données (8.4).....	75
Tableau A.12 – Normes de codage	76
Tableau A.13 – Analyse et Tests dynamiques.....	76
Tableau A.14 – Test fonctionnel/boîte noire	77
Tableau A.15 – Langages de programmation textuels	77
Tableau A.16 – Langages diagrammatiques pour algorithmes d'application	78
Tableau A.17 – Modélisation	78
Tableau A.18 – Tests de Performance	78
Tableau A.19 – Analyse statique	79
Tableau A.20 – Composants	79
Tableau A.21 – Couverture des tests pour le code	80
Tableau A.22 – Architecture de logiciel orienté objet	81
Tableau A.23 – Conception détaillée orientée objet	81
Tableau B.1 — Spécification du Rôle du Gestionnaire des Exigences	82
Tableau B.2 — Spécification du Rôle du Concepteur	83
Tableau B.3 — Spécification du Rôle du Réalisateur	84
Tableau B.4 — Spécification du Rôle du Chargé des tests.....	85
Tableau B.5 — Spécification du Rôle du Chargé de vérification	86
Tableau B.6 — Spécification du Rôle du Chargé d'intégration.....	87
Tableau B.7 — Spécification du Rôle du Chargé de Chargé de validation	88
Tableau B.8 — Spécification du Rôle du Chargé d'évaluation	89
Tableau B.9 — Spécification du Rôle du Chef de projet	90
Tableau B.10 — Spécification du Rôle du Gestionnaire de la Configuration	90
Tableau C.1 — Résumé du Contrôle des Documents	91

Introduction

La présente Norme Européenne fait partie intégrante d'un groupe de normes connexes. Les autres documents de ce groupe sont les EN 50126-1:1999 «*Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) – Partie 1 : Exigences de base et procédés génériques*» et EN 50129:2003 «*Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation*».

L'EN 50126-1 traite des systèmes au niveau le plus général, tandis que l'EN 50129 traite des processus d'approbation des systèmes individuels qui peuvent exister dans le cadre du système ferroviaire global de contrôle-commande et de protection. La présente Norme Européenne 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.

La présente Norme Européenne fournit un ensemble d'exigences que le développement, le déploiement et la maintenance de tout logiciel de sécurité destiné aux applications ferroviaires de contrôle-commande et de protection doivent respecter. Elle définit les exigences concernant la structure organisationnelle, la relation entre organisations et la répartition des responsabilités impliquées dans les activités de développement, de déploiement et de maintenance. Des critères de qualification et d'expertise du personnel sont également fournis dans la présente Norme Européenne.

Le concept clé de la présente Norme Européenne est celui des niveaux d'intégrité de la sécurité logicielle. La présente Norme Européenne traite de cinq niveaux d'intégrité de sécurité logicielle dans lesquels 0 correspond au niveau le plus bas et 4 au niveau le plus élevé. Plus le risque résultant d'une défaillance logicielle est élevé, plus le niveau d'intégrité de la sécurité logicielle est élevé.

La présente Norme Européenne a identifié des techniques et mesures applicables aux cinq niveaux d'intégrité de la sécurité logicielle. Les techniques et mesures requises pour les niveaux 0 à 4 d'intégrité de la sécurité logicielle sont indiquées dans les tableaux de l'Annexe A (normative). 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 Européenne 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.

Le processus de spécification des fonctions de sécurité allouées au logiciel fait partie du domaine d'application des normes EN 50126-1 et EN 50129.

La présente Norme Européenne spécifie les mesures nécessaires au respect de ces exigences.

Les EN 50126-1 et EN 50129 exigent qu'une approche systématique soit adoptée en ce qui concerne :

- a) l'identification des situations dangereuses, l'évaluation des risques et la prise de décisions en fonction de critères de risque,
- b) l'identification de la réduction des risques nécessaire au respect des critères d'acceptation de risque;
- c) 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,
- d) le choix d'une architecture système adaptée,
- e) 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 l'intégrité de la sécurité est validée.

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

L'état actuel de la technique est tel que ni l'application des méthodes d'assurance qualité (mesures d'évitement des défauts et mesures de détection des défauts), ni l'application d'approches logicielles à tolérance aux pannes ne peuvent garantir la sécurité absolue du logiciel. Il n'existe aucun moyen connu de prouver l'absence de défauts dans un logiciel de sécurité même 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 composants vérifiés et des bibliothèques de composants,
- une documentation claire et la traçabilité,
- des documents aptes à être audités,
- la validation,
- l'évaluation,
- la gestion de configuration et le contrôle des modifications, et
- l'étude appropriée des questions de compétence de l'organisation et du personnel.

La Spécification des exigences de sécurité du système identifie toutes les fonctions de sécurité allouées au logiciel et détermine leur niveau d'intégrité de la sécurité du système. Les étapes fonctionnelles successives de l'application de la présente Norme Européenne sont montrées à la Figure 1 et consistent à :

- a) définir la Spécification des Exigences du Logiciel et, en parallèle, considérer l'architecture du logiciel. La stratégie de sécurité pour le logiciel et le niveau d'intégrité de la sécurité logicielle (7.2 et 7.3) sont développés dans l'architecture du logiciel;
- b) 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 (7.4 et 7.5);
- c) intégrer le logiciel sur le matériel cible et vérifier la fonctionnalité (7.6);
- d) accepter et déployer le logiciel (7.7 et 9.1);
- e) si la maintenance du logiciel est requise pendant la vie opérationnelle, réactiver le cas échéant la présente Norme Européenne (9.2).

Un certain nombre d'activités se déroulent pendant le développement du logiciel, parmi lesquelles les tests (6.1), la vérification (6.2), la validation (6.3), l'évaluation (6.4), l'assurance qualité (6.5) et le contrôle des modifications et des évolutions (6.6).

Des exigences sont données en ce qui concerne les outils (6.7) et les systèmes qui sont configurés par des données d'application ou par des algorithmes d'application (8).

Des exigences sont également fournies en ce qui concerne l'indépendance des rôles et la compétence du personnel impliqué dans le développement du logiciel (5.1, 5.2 et Annexe B).

La présente Norme n'impose pas l'utilisation d'un cycle de vie spécifique de développement du logiciel. Cependant des ensembles illustratifs de cycle de vie et de documentation sont fournis en 5.3, Figure 3, Figure 4 et en 7.1.

Des tableaux ont été établis pour classer diverses techniques/mesures par rapport aux niveaux 0 à 4 d'intégrité de la sécurité logicielle. Les tableaux sont dans 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 de techniques est dans l'Annexe D.

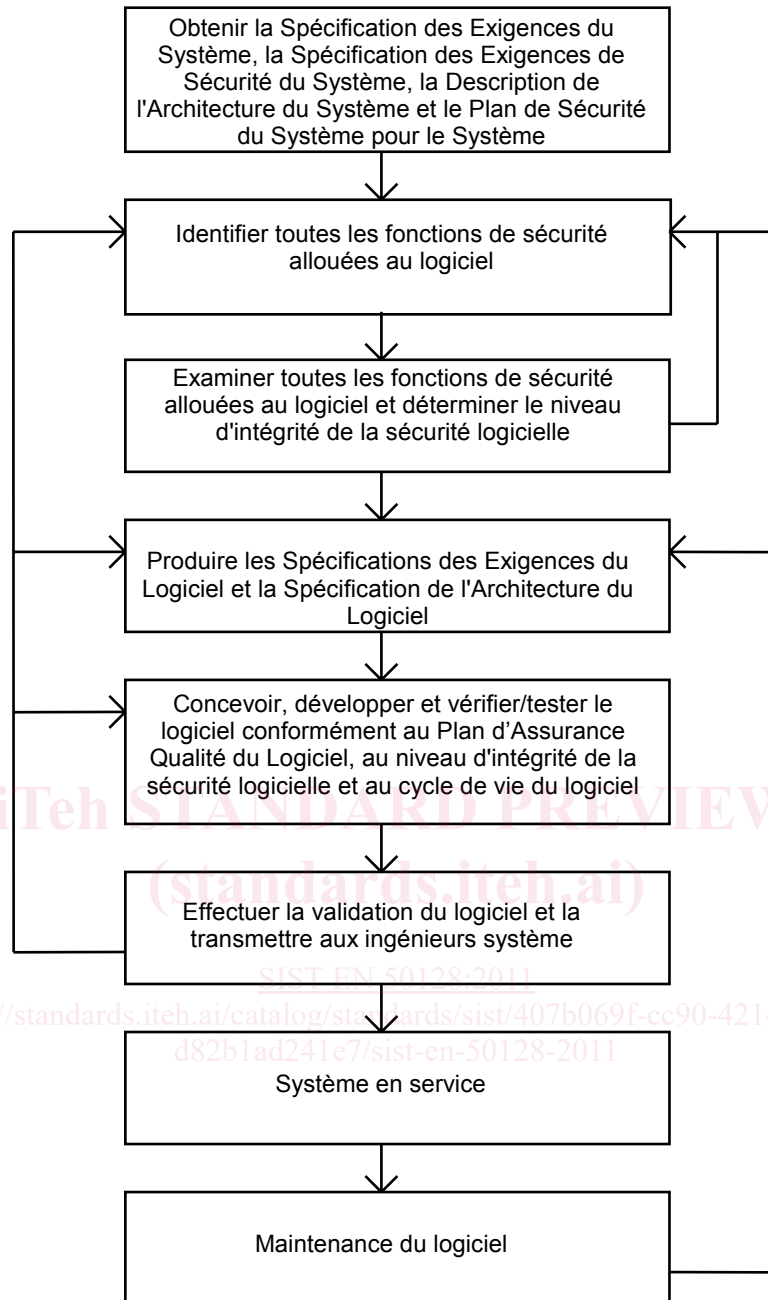


Figure 1 – Démarche illustrative relative au logiciel

1 Domaine d'application

1.1 La présente Norme Européenne spécifie les exigences de processus et les techniques applicables au développement de logiciel pour des systèmes électroniques programmables utilisés dans les applications ferroviaires de contrôle-commande et de protection. Elle est destinée à être utilisée dans tout domaine comportant des implications de sécurité. Ces systèmes peuvent être mis en œuvre à l'aide de microprocesseurs dédiés, de contrôleurs logiques programmables, de systèmes multiprocesseurs distribués, de grands systèmes dotés d'un calculateur central ou à l'aide d'autres architectures.

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

1.3 La présente Norme Européenne n'est pas pertinente pour les logiciels qui ont été identifiés comme n'ayant aucun impact sur la sécurité, c'est-à-dire pour les logiciels dont les défaillances ne peuvent pas affecter de fonctions de sécurité identifiées.

1.4 La présente Norme Européenne s'applique à tous les logiciels de sécurité utilisés dans des systèmes de contrôle-commande et de protection du ferroviaire, y compris :

- la programmation d'applications,
- les systèmes d'exploitation,
- les outils,
- les microprogrammes.

La programmation d'applications inclut la programmation de haut niveau, la programmation de bas niveau et la programmation spécifique personnalisée (par exemple : la logique à contacts d'un contrôleur logique programmable).

1.5 La présente Norme Européenne traite également de l'utilisation de logiciels et d'outils préexistants. Ces logiciels peuvent être utilisés si les exigences spécifiques en 7.3.4.7 et 6.5.4.16 relatives aux logiciels préexistants et aux outils 6.7 sont satisfaites.

1.6 Un logiciel développé selon une version quelconque de la présente Norme Européenne sera considéré conforme et non soumis aux exigences relatives aux logiciels préexistants.

1.7 La présente Norme Européenne considère que la conception moderne d'applications utilise fréquemment des logiciels génériques qui conviennent comme base pour diverses applications. Ces logiciels génériques sont ensuite configurés par des données et/ou des algorithmes, afin de produire le logiciel exécutable pour l'application. Les Articles généraux 1 à 6 et 9 de la présente Norme Européenne s'appliquent aux logiciels génériques ainsi qu'aux données d'application et algorithmes d'application. L'Article spécifique 7 s'applique uniquement pour les logiciels génériques alors que l'Article 8 fournit les exigences spécifiques pour les données d'application et algorithmes d'application.

1.8 La présente Norme Européenne ne vise pas les problèmes commerciaux. Il convient toutefois de les traiter comme une partie essentielle de tout accord contractuel. Il conviendra également que tous les articles de la présente Norme Européenne soient considérés soigneusement dans toute situation commerciale.

1.9 La présente Norme Européenne n'est pas destinée à être rétroactive. Elle s'applique donc principalement aux nouveaux développements et n'est applicable dans son intégralité aux systèmes existants que s'ils font l'objet de modifications importantes. Pour les modifications mineures, seul le paragraphe 9.2 s'applique. Le Chargé d'évaluation doit analyser les preuves fournies dans la documentation du logiciel pour confirmer si, oui ou non, la détermination de la nature et de l'étendue des modifications du logiciel sont adéquates. Cependant, il est hautement recommandé d'appliquer la présente Norme Européenne pendant les mises à niveau et la maintenance des logiciels existants.

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).

EN 50126-1:1999	Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1 : Exigences de base et procédés génériques
EN 50129:2003	Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation
EN ISO 9000	Systèmes de management de la qualité - Principes essentiels et vocabulaire (ISO 9000:2005)
EN ISO 9001	Systèmes de management de la qualité - Exigences (ISO 9001:2008)
ISO/CEI 90003:2004	Ingénierie du logiciel – Lignes directrices pour l'application de l'ISO 9001:2000 aux logiciels informatiques
Série ISO/CEI 9126	Génie du logiciel -- Qualité des produits

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1

évaluation

processus d'analyse afin de déterminer si un logiciel, qui peut inclure des processus, de la documentation, des composants logiciels et/ou matériels de systèmes et sous-systèmes, satisfait aux exigences spécifiées et afin de formuler un jugement sur le fait que le logiciel répond à l'objectif attendu. L'évaluation de la sécurité est une évaluation axée sur les propriétés de sécurité d'un système, mais sans s'y limiter

3.1.2

chargé d'évaluation

entité qui mène à bien une évaluation

3.1.3

logiciel standard disponible dans le commerce (COTS, en anglais commercial off-the-shelf software)

logiciel défini par les besoins du marché, disponible dans le commerce et dont l'adéquation aux besoins a été démontrée par un large éventail d'utilisateurs

3.1.4

composant

partie constitutive de logiciel qui a des interfaces et un comportement bien définis par rapport à la conception et à l'architecture du logiciel et satisfait aux critères suivants :

- elle est conçue conformément à “Composants” (voir Tableau A.20);
- elle couvre un sous-ensemble spécifique des exigences relatives au logiciel;
- elle est clairement identifiée et a une version indépendante au sein du système de gestion de configuration ou est une partie d'un ensemble de composants (par exemple : sous-systèmes) qui ont une version indépendante

3.1.5**gestionnaire de la configuration**

entité qui est chargée de mettre en œuvre et d'exécuter les processus pour la gestion de configuration des documents, logiciels et outils connexes, y compris la gestion des modifications et des évolutions

3.1.6**client**

entité qui achète un système de contrôle-commande et de protection du ferroviaire comprenant le logiciel

3.1.7**concepteur**

entité qui analyse et transforme des exigences spécifiées en solutions de conception acceptables qui ont le niveau prescrit d'intégrité de la sécurité

3.1.8**entité**

personne, groupe ou organisation qui remplit un rôle tel que défini dans la présente Norme européenne

3.1.9**erreur, faute**

défaut, méprise ou inexactitude pouvant conduire à une défaillance ou à un écart par rapport au comportement ou à la performance prévu(e)

3.1.10**défaillance**

différence inacceptable entre la performance requise et la performance observée

3.1.11**tolérance aux "fautes"**

capacité propre à un système à délivrer d'une manière correcte et continue un service tel qu'il est spécifié, en présence d'un nombre limité de défauts matériels ou logiciels

3.1.12**micrologiciel**

logiciel stocké dans une mémoire morte ou dans une mémoire semi permanente telle qu'une mémoire flash, d'une manière qui est fonctionnellement indépendante du logiciel applicatif

3.1.13**logiciel générique**

logiciel pouvant être utilisé pour une grande variété d'installations simplement en fournissant des données et/ou algorithmes propres à l'application

3.1.14**réalisateur**

entité qui transforme des choix de conception en leur réalisation physique

3.1.15**intégration**

processus d'assemblage d'éléments de logiciel et/ou de matériel, selon la spécification de conception et d'architecture, et de tests de l'ensemble intégré

3.1.16**chargé d'intégration**

entité qui mène à bien l'intégration du logiciel

3.1.17**logiciel préexistant**

logiciel développé avant l'application dont il est ici question, incluant les logiciels COTS (standards disponibles dans le commerce) et libres.

3.1.18**logiciel libre**

code source à la disposition du grand public avec des restrictions de droits d'auteur assouplies ou inexistantes

3.1.19**contrôleur logique programmable**

système de commande informatisé, doté d'une mémoire programmable par l'utilisateur pour le stockage des instructions, pour réaliser des fonctions spécifiques

3.1.20**gestion de projet**

conduite administrative et/ou technique d'un projet, y compris les aspects de sécurité

3.1.21**chef de projet**

entité qui mène à bien la gestion de projet

3.1.22**fiabilité**

aptitude d'une entité à réaliser une fonction dans des conditions données, pendant une période de temps donnée

3.1.23**robustesse**

aptitude d'un élément à détecter et gérer les situations anormales

3.1.24**gestionnaire des exigences**

entité qui mène à bien la gestion des exigences

3.1.25**gestions des exigences**

processus consistant à identifier, documenter, analyser, classer par ordre de priorité et accepter par accord les exigences et ensuite contrôler les modifications et évolutions et communiquer avec les parties prenantes. Il s'agit d'un processus continu tout au long d'un projet

3.1.26**risque**

combinaison du taux d'occurrence d'accidents et d'incidents occasionnant un dommage (causé par une situation dangereuse) et de la gravité de ce dommage

3.1.27**sécurité**

absence de niveaux inacceptables de risque de dommage aux personnes

3.1.28**autorité de tutelle**

organisme chargé de certifier que les logiciels ou services relatifs à la sécurité sont conformes aux exigences de sécurité statutaires applicables

3.1.29**fonction de sécurité**

fonction qui met en œuvre tout ou partie d'une exigence relative à la sécurité

3.1.30**logiciel de sécurité**

logiciel qui exécute des fonctions de sécurité

3.1.31**logiciel**

création intellectuelle comprenant les programmes, les procédures, les règles, les données et toute documentation associée en rapport avec le fonctionnement d'un système

3.1.32**référentiel logiciel**

ensemble complet et cohérent du code source, des fichiers exécutables, des fichiers de configuration, des scripts d'installation et de la documentation qui sont nécessaires à une version diffusée d'un logiciel. Les informations concernant les compilateurs, les systèmes d'exploitation, les logiciels préexistants et les outils