

# ILNAS

Institut luxembourgeois de la normalisation  
de l'accréditation, de la sécurité et qualité  
des produits et services

## ILNAS-EN 50128:2011

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

Bahnanwendungen -  
Telekommunikationstechnik,  
Signaltechnik und  
Datenverarbeitungssysteme - Software

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

06/2011



## Avant-propos national

Cette Norme Européenne EN 50128:2011 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 50128:2011.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

### **CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR**

Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

**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

<b>8.3 Documents en sortie.....</b>	<b>57</b>
<b>8.4 Exigences .....</b>	<b>57</b>
<b>9 Déploiement et maintenance du logiciel .....</b>	<b>62</b>
<b>9.1 Déploiement du logiciel.....</b>	<b>62</b>
<b>9.2 Maintenance du logiciel .....</b>	<b>64</b>
<b>Annexe A (normative) Critères de sélection des techniques et mesures .....</b>	<b>67</b>
A.1 Tableaux d'articles .....	68
A.2 Tableaux détaillés .....	76
<b>Annexe B (normative) Principaux rôles et responsabilités relatifs au logiciel .....</b>	<b>82</b>
<b>Annexe C (informative) Résumé du contrôle des documents .....</b>	<b>91</b>
<b>Annexe D (informative) Bibliographie des techniques .....</b>	<b>93</b>
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/Graphe 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
<b>Bibliographie .....</b>		<b>132</b>

## 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.