ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

ILNAS

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

# ILNAS-EN 50128:2001

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

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

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software

03/2001

**Avant-propos national**

Cette Norme Européenne EN 50128:2001 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 50128:2001.

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

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

**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 !

NORME EUROPÉENNE **EN 50128**

EUROPÄISCHE NORM

EUROPEAN STANDARD Mars 2001

ICS 29.280; 45.060.10

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 - Communications, signalling and processing systems - Software for railway control and protection systems

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

La présente Norme européenne a été adoptée par le CENELEC le 2000-11-01. 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, Danemark, Espagne, Finlande, France, Grèce, Irlande, Islande, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, République Tchèque, Royaume-Uni, Suède et Suisse.

CENELEC

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

**Secrétariat Central: rue de Stassart 35, B - 1050 Bruxelles**

© 2001 CENELEC - Tous droits d'exploitation sous quelque forme et de quelque manière que ce soit réservés dans le monde entier aux membres du CENELEC.

## 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 2000-11-01.

Les dates suivantes ont été fixées:

- date limite à laquelle la EN doit être mise en application au niveau national par publication d'une norme nationale identique ou par entérinement (dop) 2001-11-01

- date limite à laquelle les normes nationales conflictuelles doivent être annulées (dow) 2003-11-01

Il convient de lire la présente norme européenne conjointement aux normes EN 50126: "Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)" et EN 50129: "Applications ferroviaires - Systèmes électroniques de sécurité pour la signalisation".

Les annexes appelées "normatives" font partie du corps de la norme.
Les annexes appelées "informatives" ne sont données que pour information.
Dans la présente norme, l'annexe A est normative et l'annexe B est informative.

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

# Sommaire

**page**

Introduction ..... 5

1 Domaine d'application ..... 8

2 Références normatives ..... 8

3 Définitions ..... 9

4 Objets et conformité ..... 12

5 Niveaux d'intégrité de la sécurité logicielle ..... 13

5.1 Objet ..... 13
5.2 Exigences ..... 13

6 Personnel et responsabilités ..... 14

6.1 Objet ..... 14
6.2 Exigences ..... 14

7 Problèmes liés au cycle de vie et documentation ..... 16

7.1 Objets ..... 16
7.2 Exigences ..... 16

8 Spécification des Exigences du Logiciel ..... 19

8.1 Objets ..... 19
8.2 Documents en entrée ..... 19
8.3 Documents en sortie ..... 19
8.4 Exigences ..... 19

9 Architecture du logiciel ..... 21

9.1 Objets ..... 21
9.2 Documents en entrée ..... 21
9.3 Documents en sortie ..... 21
9.4 Exigences ..... 21

10 Conception et développement du logiciel ..... 23

10.1 Objets ..... 23
10.2 Documents en entrée ..... 23
10.3 Documents en sortie ..... 23
10.4 Exigences ..... 23

11 Vérification et tests du logiciel ..... 26

11.1 Objets ..... 26
11.2 Documents en entrée ..... 26
11.3 Documents en sortie ..... 27
11.4 Exigences ..... 27

12 Intégration logiciel/matériel ..... 30

12.1 Objets ..... 30
12.2 Documents en entrée ..... 30
12.3 Documents en sortie ..... 30
12.4 Exigences ..... 31

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

13 Validation du logiciel ..... 32
13.1 Objets ..... 32
13.2 Documents en entrée ..... 32
13.3 Documents en sortie ..... 32
13.4 Exigences ..... 32
14 Evaluation du logiciel ..... 34
14.1 Objets ..... 34
14.2 Documents en entrée ..... 34
14.3 Documents en sortie ..... 34
14.4 Exigences ..... 34
15 Assurance qualité du logiciel ..... 35
15.1 Objets ..... 35
15.2 Documents en entrée ..... 35
15.3 Documents en sortie ..... 35
15.4 Exigences ..... 35
16 Maintenance du logiciel ..... 38
16.1 Objets ..... 38
16.2 Documents en entrée ..... 38
16.3 Documents en sortie ..... 38
16.4 Exigences ..... 38
17 Systèmes configurés par des données d'application ..... 39
17.1 Objets ..... 39
17.2 Documents en entrée ..... 40
17.3 Documents en sortie ..... 40
17.4 Exigences ..... 40
17.4.1 Cycle de vie de la préparation des données ..... 40
17.4.2 Procédures et outils de préparation des données ..... 41
17.4.3 Développement du logiciel ..... 41
Annexe A (normative) Critères de sélection des techniques et mesures ..... 49
Annexe B (informative) Bibliographie des techniques ..... 64

**Figures**

Figure 1 – Niveaux d'intégrité de la sécurité pour les systèmes liés à la sécurité ..... 43
Figure 2 – Démarche de la sécurité du logiciel ..... 44
Figure 3 – Cycle de vie 1 du développement ..... 45
Figure 4 – Cycle de vie 2 du développement ..... 46
Figure 5 – Indépendance en fonction du niveau d'intégrité de la sécurité du logiciel ..... 47
Figure 6 – Relation entre le développement du système générique et le développement du cas spécifique ..... 48

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

## Introduction

La présente norme fait partie intégrante d'un groupe de normes connexes. Les autres éléments de ce groupe sont les normes EN 50126 "Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)" et EN 50129 " Applications ferroviaires - Systèmes électroniques de sécurité pour la signalisation". La norme EN 50126 traite des problèmes liés aux systèmes de façon très générale, tandis que la norme EN 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 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 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 européenne 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 européenne 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 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 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.

C'est la fonction des normes EN 50126 et EN 50129 que de spécifier les fonctions de sécurité affectées au logiciel.

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

Les normes EN 50126 et EN 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;

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.

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

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 ceci 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;

– 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 européenne, décrites à la Figure 2, sont les suivantes:

i) definir 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 européenne, (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).

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop

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.

ILNAS-EN 50128:2001 - Preview only Copy via ILNAS e-Shop