SLOVENSKI STANDARD
SIST EN 50159:2010

01-november-2010

Nadomešča:
SIST EN 50159-1:2002
SIST EN 50159-2:2002

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Varnostna komunikacija v prenosnih sistemih

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Ta slovenski standard je istoveten z: **EN 50159:2010**

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 50159:2010 **en,fr**

NORME EUROPÉENNE

EUROPÄISCHE NORM

EUROPEAN STANDARD

EN 50159

Septembre 2010

ICS 35.240.60; 45.020

Remplace EN 50159-1:2001, EN 50159-2:2001

Version française

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

La présente Norme Européenne a été adoptée par le CENELEC le 2010-09-01. 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, 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

Ref. n° EN 50159:2010 F

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. Elle a été soumise au vote formel et a été acceptée par le CENELEC comme EN 50159 le 2010-09-01.

Ce document annule et remplace l'EN 50159-1:2001 et l'EN 50159-2:2001.

Le contenu de ces deux normes a été fusionné; l'Annexe E, informative, fournit un tableau de correspondances entre ces précédentes éditions et le présent document.

La présente Norme Européenne est étroitement liée à l'EN 50129:2003.

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)	2011-09-01
– date limite à laquelle les normes nationales conflictuelles doivent être annulées	(dow)	2013-09-01

Le présent projet de Norme Européenne a été préparé dans le cadre d'un mandat confié au CENELEC par la Commission Européenne et l'Association Européenne de Libre Echange et couvre les exigences essentielles de la Directive 96/48/CE (HSR) reprise par la Directive 2008/57/CE (RAIL). Voir l'Annexe ZZ.

Sommaire

Figures

Tableaux

Introduction

Si un système électronique de sécurité implique un transfert d'informations entre des emplacements différents, le système de transmission fait alors partie intégrante du système de sécurité et il doit être démontré que la communication de bout en bout est sûre, conformément à la EN 50129.

Le système de transmission traité dans la présente norme, destiné au transfert d'informations entre des emplacements différents, n'a pas en général à satisfaire de conditions préliminaires particulières. Du point de vue de la sécurité, il n'est pas, ou pas complètement, sécurisé.

La présente norme traite des exigences à prendre en compte pour la communication d'informations relatives à la sécurité par l'intermédiaire de tels systèmes de transmission.

Bien que les aspects FMD ne soient pas considérés dans la présente norme, il est recommandé de garder à l'esprit qu'ils sont un aspect majeur dans la sécurité globale.

Les exigences de sécurité dépendent des caractéristiques du système de transmission. Afin de simplifier la démonstration de la sécurité du système, les systèmes de transmission ont été répartis en trois classes:

– la classe 1 comprend les systèmes qui sont sous le contrôle du concepteur et qui sont fixes pendant leur durée de vie;

– la classe 2 comprend les systèmes qui sont partiellement inconnues ou non fixés, mais pour lesquels un accès non autorisé peut être exclu;

– la classe 3 comprend les systèmes qui ne sont pas sous le contrôle du concepteur, et pour lesquels un accès non autorisé doit être envisagé.

La classe 1 a été traitée par la EN 50159-1:2001 et les deux autres par la EN 50159-2:2001.

Lorsque des systèmes de communication de sécurité, approuvés selon les normes précédentes, font l'objet de mesures de maintenance et/ou d'extensions, l'Annexe E, informative, peut être utilisée pour établir la correspondance des articles (paragraphes) de la présente norme avec les articles (paragraphes) de la série de normes précédente.

1 Domaine d'application

La présente Norme Européenne s'applique aux systèmes électroniques de sécurité utilisant, à des fins de communication numérique, un système de transmission qui n'a pas été nécessairement conçu pour des applications de sécurité et qui, selon le cas,

– est sous le contrôle du concepteur et est fixe pendant sa durée de vie,

– est partiellement inconnu ou non fixé, mais pour lequel un accès non autorisé peut être exclu,

– n'est pas sous le contrôle du concepteur, et un accès non autorisé est également à envisager.

Les équipements connectés au système de transmission peuvent être des équipements de sécurité ou non.

La présente norme indique les exigences de base nécessaires pour obtenir une communication de sécurité entre les équipements de sécurité connectés au système de transmission.

La présente Norme Européenne s'applique à la spécification des exigences de sécurité des équipements de sécurité connectés au système de transmission, afin d'atteindre le niveau d'intégrité de sécurité alloué.

Les exigences de sécurité sont généralement mises en œuvre dans les équipements de sécurité conçus selon la EN 50129. Dans certains cas, ces exigences peuvent être mises en œuvre dans d'autres équipements du système de transmission, pourvu qu'un contrôle soit assuré par des mesures de sécurité afin d'atteindre le niveau d'intégrité de sécurité alloué.

La spécification d'exigences de sécurité est une condition préalable au dossier de sécurité d'un système électronique de sécurité dont les caractéristiques de la preuve sont définies dans la EN 50129. Cette dernière définit également la preuve de la gestion de la sécurité et la preuve de la gestion de la qualité. Les exigences de communication spécifiées dans le but d'établir la sécurité fonctionnelle et technique sont traitées dans la présente norme.

La présente Norme Européenne ne s'applique pas aux systèmes existants ayant déjà été acceptés avant la parution de la présente norme.

La présente Norme Européenne ne spécifie pas

– le système de transmission,

– les équipements connectés au système de transmission,

– les solutions (destinées par exemple à l'interopérabilité),

– les types de données liés à la sécurité et les types de données non liés à la sécurité.

Un équipement de sécurité connecté par un système de transmission ouvert peut faire l'objet d'un grand nombre de menaces relatives à la sécurité informatique contre lesquelles un programme global, couvrant des aspects techniques, opérationnels et de gestion, doit être défini.

Cependant, en ce qui concerne la sécurité informatique, la présente Norme Européenne traite uniquement des attaques intentionnelles effectuées au moyen de messages adressés aux applications de sécurité.

La présente Norme Européenne ne couvre pas les aspects de sécurité informatique généraux et, en particulier, elle n'aborde pas les aspects de sécurité informatique visant à

– garantir la confidentialité des informations de sécurité,

– empêcher la surcharge du système de transmission.

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 (y compris les éventuels amendements) s'applique.

CLC/TR / EN 50126 (série), *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*

EN 50129:2003, *Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation*

3 Termes, définitions et abréviations

3.1 Termes et définitions

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

3.1.1
date absolue
date référencée par rapport à un temps global, commun à un groupe d'entités utilisant un système de transmission

3.1.2
protection d'accès
processus conçu pour empêcher un accès non autorisé de lire ou de modifier de l'information, soit dans les systèmes de sécurité utilisateur, soit dans le système de transmission

3.1.3
données additionnelles
données inutiles pour les processus utilisateur finals, mais utilisées à des fins de contrôle, de disponibilité et de sécurité

3.1.4
message authentique
message dont l'information est reconnue provenir de la source indiquée

3.1.5
authenticité
état dans lequel une information est valide et réputée avoir été générée par la source déclarée

3.1.6
système de transmission fermé
nombre fixe ou nombre maximum fixe d'éléments reliés par un système de transmission dont les propriétés sont bien connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

3.1.7
communication
transfert d'informations entre applications

3.1.8
confidentialité
propriété de non mise à disposition de l'information à des entités non autorisées

3.1.9
message corrompu
type d'erreur de message dans lequel se produit une corruption des données

3.1.10
techniques cryptographiques
produisent des données de sortie calculées au moyen d'un algorithme utilisant les données d'entrée et une clé comme paramètre

NOTE Si les données de sortie sont connues, le calcul des données d'entrée dans un délai raisonnable est impossible sans connaître la clé. La déduction de la clé des données de sortie dans un délai raisonnable est également impossible, même si les données d'entrée sont connues.

3.1.11
contrôle de redondance cyclique
code cyclique utilisé pour protéger les messages de l'influence des corruptions de données

3.1.12
données
partie d'un message qui représente de l'information (voir aussi « données utilisateur », « données additionnelles », « données redondantes »)

3.1.13
corruption de données
altération de données

3.1.14
défense
mesure introduite dans la conception d'un système de communications de sécurité pour contrer des menaces particulières

3.1.15
message retardé
type d'erreur de message dans lequel un message est reçu plus tard que prévu

3.1.16
message supprimé
type d'erreur de message dans lequel un message est retiré d'un flux de messages

3.1.17
date double
cas où deux entités échangent et comparent leurs dates. Dans ce cas, les dates des entités sont indépendantes les unes des autres

3.1.18
erreur
écart par rapport à la conception prévue, qui pourrait se traduire par un comportement non prévu du système ou par une défaillance

3.1.19
défaillance
écart d'un système par rapport aux performances spécifiées

NOTE Une défaillance est la conséquence d'une panne ou d'une erreur dans le système.

3.1.20
panne
état anormal pouvant conduire à une erreur dans un système

NOTE Une panne peut être aléatoire ou systématique.

3.1.21
message en retour
réponse d'un récepteur à l'émetteur, via un canal de transmission en retour

3.1.22
pirate informatique
personne tentant délibérément de contourner une protection d'accès

3.1.23
danger
condition pouvant conduire à un accident

3.1.24
analyse des dangers
processus d'identification des dangers et d'analyse de leurs causes, ainsi que des écarts par rapport aux exigences pour limiter la probabilité d'occurrence et les conséquences des dangers à un niveau acceptable

3.1.25
données implicites
données additionnelles non transmises, mais connues de l'émetteur et du récepteur

3.1.26
information
représentation de l'état ou des événements d'un processus, dans une forme compréhensible par le processus

3.1.27
message inséré
type d'erreur de message dans lequel un message est ajouté dans le flux de messages

3.1.28
intégrité
état dans lequel une information est complète et non altérée

3.1.29
code de détection de manipulation
fonction concernant l'ensemble du message sans clé secrète

NOTE Par opposition au MAC, aucune clé secrète n'est impliquée. Par « ensemble du message », on comprend également toute donnée implicite du message qui n'est pas envoyée au système de transmission. Le MDC est souvent basé sur une fonction de brouillage.

3.1.30
mascarade de message
insertion d'un message non authentique, déguisé pour passer pour authentique

3.1.31
message
information transmise par un émetteur (source de données) à un ou plusieurs récepteurs (collecteur de données)

3.1.32
code d'authentification de message
fonction cryptographique de l'ensemble du message et d'une clé secrète ou publique

NOTE Par « ensemble du message », on comprend également toute donnée implicite du message qui n'est pas envoyée au système de transmission

3.1.33
cryptage de message
transformation de bits en appliquant une technique cryptographique à un message, suivant un algorithme piloté par clés, afin de rendre plus difficile une lecture fortuite des données. Ne protège pas contre la corruption des données

3.1.34
erreurs de message
ensemble de tous les modes de défaillance de message possibles, pouvant conduire à des situations potentiellement dangereuses ou à une réduction de la disponibilité du système. Plusieurs causes peuvent être associées à un type d'erreur donné

3.1.35
intégrité du message
message dans lequel l'information est complète et non altérée

3.1.36
flux de messages
suite ordonnée de messages

3.1.37
code de sécurité non cryptographique
données redondantes, basées sur des fonctions non cryptographiques, incluses dans un message de sécurité, afin de rendre possible la détection de la corruption des données par une fonction de transmission de sécurité

3.1.38
système de transmission ouvert
système de transmission à un nombre d'utilisateurs inconnu, ayant des propriétés non connues, variables et non sécurisées, utilisé pour des services de télécommunication inconnus et pour lequel il existe un risque d'accès non autorisé

3.1.39
défaillance aléatoire
défaillance qui se produit aléatoirement dans le temps

3.1.40
contrôle de redondance
type de contrôle de l'existence d'une relation prédéfinie entre des données redondantes et des données utilisateur au sein d'un message, pour prouver l'intégrité du message

3.1.41
données redondantes
données additionnelles dérivées des données utilisateur par une fonction de transmission de sécurité

3.1.42
date relative
date référencée par rapport à l'horloge locale d'une entité. En général, il n'y a pas de relation avec les horloges des autres entités

3.1.43
message répété
type d'erreur de message dans lequel un message unique est reçu plus d'une fois

3.1.44
message reséquencé
type d'erreur de message dans lequel l'ordre des messages est modifié dans le flux de messages

3.1.45
état de secours sûr
état sûr d'un équipement ou d'un système de sécurité, déviant par rapport à un état non défaillant et résultant d'une réaction de protection conduisant à une fonctionnalité réduite des fonctions de sécurité, voire des fonctions non liées à la sécurité

3.1.46
sécurité
absence de niveaux de risque inacceptables

3.1.47
dossier de sécurité
démonstration documentée que le produit répond aux exigences de sécurité spécifiées

3.1.48
code de sécurité
données redondantes incluses dans un message de sécurité afin de détecter les corruptions de données par une fonction de transmission de sécurité

3.1.49
niveau d'intégrité de la sécurité
nombre qui indique le degré de confiance requis pour qu'un système remplisse ses fonctions de sécurité eu égard à ses défaillances systématiques

3.1.50
réaction de protection
action qui peut être prise par le processus de sécurité en réponse à un événement (comme une défaillance du système de transmission), pouvant conduire à un état de secours sûr de l'équipement

3.1.51
de sécurité
qui est responsable de la sécurité

3.1.52
fonction de transmission de sécurité
fonction intégrée dans l'équipement de sécurité pour garantir l'authenticité, l'intégrité, la ponctualité et la séquence des données

3.1.53
numéro de séquence
champ de données additionnel contenant un nombre qui varie d'une manière prédéfinie de message à message

3.1.54
identificateur de source et de destination
identificateur assigné à chaque entité. Il peut s'agir d'un nom, d'un nombre ou d'une configuration binaire arbitraire. L'identificateur est utilisé pour une communication de sécurité. Il est habituellement ajouté aux données utilisateurs

3.1.55
défaillance systématique
défaillance d'occurrence répétitive moyennant des combinaisons particulières d'entrées ou des conditions particulières d'environnement

3.1.56
menace
violation potentielle de sécurité

3.1.57
datation
information concernant le moment de la transmission, attachée à un message par l'émetteur

3.1.58
ponctualité
état correspondant à une mise à disposition de l'information au bon moment, conformément aux spécifications

3.1.59
code de transmission
information redondante, ajoutée au message de sécurité ou non du système de transmission non sécurisé, pour assurer l'intégrité du message pendant la transmission

3.1.60
système de transmission
service utilisé par une application pour transmettre des flux de messages entre un nombre de participants, qui peuvent être des sources ou des collecteurs d'information

3.1.61
sécurisé
élément dont les propriétés sont utilisées pour faire la preuve de la sécurité

3.1.62
accès non autorisé
situation dans laquelle des personnes non autorisées ou des pirates informatiques ont accès à et/ou modifient des informations utilisateur ou des informations dans le système de transmission

3.1.63
données utilisateur
données représentant les états ou événements d'un processus utilisateur, sans données additionnelles. Dans le cas d'une communication entre des équipements de sécurité, les données utilisateur contiennent des données de sécurité

3.1.64
message valide
message satisfaisant dans sa forme à toutes les spécifications de l'utilisateur

3.1.65
validité
état satisfaisant à tous les égards aux exigences spécifiées par l'utilisateur

3.2 Abréviations

Pour les besoins du présent document, les abréviations suivantes s'appliquent.

AAP	Analyse par Arbre de Panne (en: FTA, Fault Tree Analysis)
BCH	Code Bose, Ray-Chaudhuri, Hocquenghem
B.M.E.	Erreurs de message de base
BSC	Voie binaire symétrique
CAN	Gestionnaire de réseau de communication
CE	Communauté Européenne
CRC	Contrôle de redondance cyclique
ECB	Mode dictionnaire chiffré électronique
FDMS	Fiabilité, Disponibilité, Maintenabilité et Sécurité (en: RAMS, Reliability, Availability, Maintainability and Safety)
GPRS	Téléphonie sans fil large bande
GSM-R	Système global de communication pour les mobiles ferroviaires
H.E.	Evénement dangereux
HW	Matériel
IEM	Interférence électromagnétique (en: EMI, Electromagnetic Interference)
IT	Technologie de l'information
LAN	Réseau local
MAC	Code d'authentification de message
MDC	Code de détection de manipulation

MD4, MD5	Algorithmes de codification de message
M.H.	Situation dangereuse principale
MTBF	Temps moyen de fonctionnement entre défaillances consécutives
MVB	Bus de communication multifonction pour véhicules
PROFIBUS	Bus de communication de terrain
QSC	Voie q-naire symétrique
SIL	Niveau d'intégrité de la sécurité
SR	Relatif à la sécurité
SRS	Spécification des exigences de sécurité
SW	Logiciel
TX	Transmission
UTC	Temps universel coordonné
WAN	Réseau étendu
Wi-Fi	Réseau local sans fil

4 Architecture de référence

La présente Norme Européenne définit les exigences de sécurité visant à garantir une communication sûre entre des équipements de sécurité via un système de transmission pouvant être soit fermé, soit ouvert. Les équipements connectés au système de transmission peuvent être des équipements de sécurité ou non. Le présent article décrit les configurations possibles de communication de sécurité dans les systèmes de transmission incluant la définition des blocs fonctionnels impliqués. Les exigences particulières qui sont à respectées par ces blocs sont spécifiées dans les articles ultérieurs.

La Figure 1 présente une vue combinée (système de transmission ouvert et fermé) de l'architecture principale, dans laquelle tous les éléments de communication sont liés conformément au flux d'informations, en vue de l'échange d'informations de sécurité entre des équipements de sécurité. L'architecture de référence montre également une interface non liée à la sécurité dont la présence n'est pas systématique. Ce type de configuration est habituellement utilisé pour les messages de diagnostic routés vers un centre de maintenance.

Outre la source et la destination de la communication de sécurité, l'architecture de référence traite d'un système de communication de sécurité qui comprend

– des fonctions de transmission de sécurité intégrées aux équipements de sécurité. Ces fonctions assurent l'authenticité, l'intégrité, la ponctualité et la séquence des données,

– des techniques cryptographiques de sécurité qui protègent le message de sécurité. Ces techniques sont soit intégrées dans les équipements de sécurité, soit mises en œuvre à l'extérieur de ces équipements, en étant toutefois dans ce cas contrôlées par des techniques de sécurité. Ces techniques assurent la protection des messages de sécurité dans un système de transmission de classe 3. Elles ne sont pas requises pour les systèmes de transmission des classes 1 ou 2,

– un système de transmission non lié à la sécurité, ouvert ou fermé, pouvant lui-même inclure des fonctions de protection de transmission et/ou des fonctions de protection d'accès.

Les systèmes de transmission fermés (classe 1) présentent les caractéristiques suivantes:

– le nombre de parties d'équipement – de sécurité ou non – connectable au système de transmission est connu et fixé;

– le risque d'accès non autorisé est considéré comme négligeable;

– les caractéristiques physiques du système de transmission (par exemple, supports de transmission, environnement conformément aux hypothèses de conception, etc.) sont fixées et non altérées pendant le cycle de vie du système.