

**Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy
zpracování dat - Komunikace v přenosových zabezpečovacích
systémech** **ČSN
EN 50159**
34 2670

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

Applications ferroviaires - Systemes de signalisation, de télécommunication et de traitement -
Communication de sécurité sur des systemes de transmission

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

Tato norma je českou verzí evropské normy EN 50159:2010. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 50159:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

S účinností od 2013-09-01 se nahrazuje ČSN EN 50159-1 (34 2670) z dubna 2002 a ČSN EN 50159-2 (34 2670) z května 2002, které do uvedeného data platí souběžně s touto normou.

Národní předmluva

Upozornění na používání této normy

Souběžně s touto normou se mohou do 2013-09-01 používat dosud platné ČSN EN 50159-1 (34 2670) z dubna 2002 a ČSN EN 50159-2 (34 2670) z května 2002, v souladu s předmluvou k EN 50159:2010.

Změny proti předchozím normám

Tato norma zahrnuje požadavky na komunikaci jak v uzavřených, tak v otevřených přenosových systémech, zatímco dosud je tato tematika zahrnuta ve dvou samostatných ČSN: ČSN EN 50159-1 (pro uzavřené systémy) a ČSN EN 50159-2 (pro otevřené systémy). Při revizi byla nová norma značně přepracována a rozšířena, byl doplněn a rozšířen přehled použitých zkratk. Přenosové systémy byly původně rozděleny do dvou kategorií, tato ČSN dělí přenosové systémy do tří kategorií. Byla doplněna rozsáhlá bibliografie (viz Souvisící ČSN) a příloha ZZ. Byly upraveny některé české termíny (např. „stálý přenosový systém“ místo „pevný přenosový systém“, „časové razítko“ místo „časový údaj“,

„hrozba“ místo „ohrožení“, „autorizovaný/neautorizovaný přístup“ místo „oprávněný/neoprávněný přístup“, „informační technologie“ místo „informační techniky“ atd.).

Informace o citovaných normativních dokumentech

CLC/TR/EN 50126 soubor zavedena EN 50126 v ČSN EN 50126-1 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces, ostatní normy souboru nezavedeny*)

EN 50129:2003 zavedena v ČSN EN 50129:2003 (34 2675) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy

Souvisící ČSN

ČSN EN 50128:2003 (34 2680) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy

ČSN IEC 50(191) (01 0102) Mezinárodní elektrotechnický slovník – Kapitola 191: Spožehlivost a akost služieb

ČSN IEC 50(701) (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 701: Telekomunikace, kanály a sítě

ČSN IEC 50(704) (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 704: Přenos

ČSN IEC 50(714) (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 714: Spojování a signalizace v telekomunikacích

ČSN IEC 60050-821 (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 821: Drážní signalizační a zabezpečovací zařízení

ČSN ISO/IEC 2382-8 (36 9001) Informační technologie – Slovník – Část 8: Bezpečnost

ČSN 34 2600 ed. 2 Drážní zařízení – Železniční zabezpečovací zařízení

ČSN 34 2617 Určování a ověřování ukazatelů spolehlivosti železničních zabezpečovacích zařízení

ČSN EN 61025 (01 0676) Analýza stromu poruchových stavů (FTA)

ČSN ISO/IEC 9796-2:2004 (36 9780) Informační technologie – Bezpečnostní techniky– Schémata digitálního podpisu umožňující obnovu zprávy – Část 2: Mechanismy založené na faktorizaci celých čísel

ČSN ISO/IEC 9797-1:2001 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC) – Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9797-2:2006 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC) – Část 2: Mechanismy používající dedikovanou hašovací funkci

ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 1: Všeobecně

ČSN ISO/IEC 10118-2:2002 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací

funkce – Část 2: Hašovací funkce používající n-bitovou blokovou šifru

ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 10118-4:2001 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 4: Hašovací funkce používající modulární aritmetiku

ČSN ISO/IEC 11770-1:1998 (36 9785) Informační technologie – Bezpečnostní techniky – Správa klíčů – Část 1: Struktura

Vypracování normy

Zpracovatel: CTN ACRI Praha, Mgr. Martin Vlček, PhD., IČ 63832721, Radka Horská

Technická normalizační komise: TNK 126 Elektrotechnika v dopravě

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Vincent Csirik

EVROPSKÁ NORMA EN 50159
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Září 2010

ICS 35.240.60; 45.020 Nahrazuje EN 50159-1:2001, EN 50159-2:2001

**Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat –
Komunikace v přenosových zabezpečovacích systémech**

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

Applications ferroviaires – Systemes de signalisation,
de télécommunication et de traitement – Communication de
sécurité sur des systemes
de transmission

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

Tato evropská norma byla schválena CENELEC 2010-09-01. Členové CENELEC jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Ústředním sekretariátu nebo u kteréhokoliv člena CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Ústřednímu sekretariátu, má stejný status jako oficiální verze.

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Maltu, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CENELEC
Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Řídící centrum: Avenue Marnix 17, B-1000 Brusel

© 2010 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmikoli prostředky
jsou celosvětově vyhrazena členům CENELEC.
Ref. č. EN 50159:2010 E

Předmluva

Tuto evropskou normu vypracovala SC 9XA, Sdělovací a zabezpečovací systémy a systémy zpracování dat, technické komise TC 9X CENELEC Elektrická a elektronická drážní zařízení. Byla předložena k formálnímu hlasování a byla schválena CENELEC jako EN 50159 dne 2010-09-01.

Tento dokument nahrazuje EN 50159-1:2001 a EN 50159-2:2001.

Obsah obou norem byl sloučen; v informativní příloze E jsou uvedeny vztahy mezi těmito předcházejícími vydáními a současným dokumentem.

Tato evropská norma úzce souvisí s EN 50129:2003.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN a CENELEC nelze činit odpovědnými za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Byla stanovena tato data:

- nejzazší datum zavedení EN na národní úrovni
vydáním identické národní normy nebo vydáním
oznámení o schválení EN k přímému používání
jako normy národní
- nejzazší datum zrušení národních norem,
které jsou s EN v rozporu

(dop) 2011-09-01

(dow) 2013-09-01

Tato evropská norma byla vypracována na základě mandátu uděleného CENELEC Evropskou komisí a Evropským sdružením volného obchodu a zahrnuje základní požadavky Směrnice Evropského společenství 96/48/ES (HSR), nově vydané jako Směrnice 2008/57/ES (RAIL). Viz přílohu ZZ.

Obsah

Strana

Úvod 9

1 Rozsah platnosti 10

2 Citované normativní dokumenty 10

3 Termíny, definice a zkratky 11

3.1 Termíny a definice 11

3.2	Zkratky	16
4	Referenční architektura	16
5	Hrozby pro přenosový systém	19
6	Třídění přenosových systémů	20
6.1	Všeobecně	20
6.2	Všeobecné aspekty třídění	20
6.3	Kritéria pro třídění přenosových systémů	20
6.4	Vztah mezi přenosovými systémy a hrozbami	21
7	Požadavky na obrany	21
7.1	Předmluva	21
7.2	Všeobecné požadavky	22
7.3	Specifické obrany	23
7.4	Použitelnost obran	28
Příloha A	(informativní) Hrozby pro otevřené přenosové systémy	30
A.1	Přehled systému	30
A.2	Odvození základních chyb zprávy	31
A.3	Hrozby	32
A.4	Možný přístup k vytvoření důkazu bezpečnosti	33
A.5	Závěry	36
Příloha B	(informativní) Kategorie přenosových systémů	38
B.1	Kategorie přenosových systémů	38
B.2	Vztah mezi kategorií přenosových systémů a hrozbami	39
Příloha C	(informativní) Návod pro obrany	40
C.1	Použití časových razítek	40
C.2	Volba a používání bezpečnostních kódů a kryptografických technik	41
C.3	Bezpečnostní kód	45
C.4	Délka bezpečnostního kódu	47
C.5	Komunikace mezi aplikacemi vztahujícími se k bezpečnosti a aplikacemi nevztahujícími se	

k bezpečnosti 50

Příloha D (informativní) Návod pro používání normy 52

D.1 Postup 52

D.2 Příklad 53

Příloha E (informativní) Vztah k předcházejícím normám 56

Příloha ZZ (informativní) Pokrytí základních požadavků směrnic ES 58

Bibliografie 59

Strana

Obrázky

Obrázek 1 – Referenční architektura pro komunikaci vztahující se k bezpečnosti 18

Obrázek 2 – Cyklický přenos zpráv 24

Obrázek 3 – Obousměrný přenos zpráv 24

Obrázek A.1 – Strom nebezpečí 31

Obrázek A.2 – Příčiny hrozeb 34

Obrázek C.1 – Třídění komunikačního systému vztahujícího se k bezpečnosti 41

Obrázek C.2 – Model zobrazení zprávy v přenosovém systému (typ A0, A1) 42

Obrázek C.3 – Použití oddělené vrstvy ochrany přístupu 43

Obrázek C.4 – Model zobrazení zprávy v přenosovém systému (typ B0) 44

Obrázek C.5 – Model zobrazení zprávy v přenosovém systému (typ B1) 45

Obrázek C.6 – Základní model chyby 48

Obrázek C.7 – Komunikace mezi aplikacemi nevztahujícími se k bezpečnosti a aplikacemi vztahujícími se k bezpečnosti 51

Obrázek D.1 – Strom poruchových stavů pro nebezpečí „nehoda“ 53

Obrázek D.2 – Strom poruchových stavů pro případ 1 54

Obrázek D.3 – Strom poruchových stavů pro případ 2 55

Tabulky

Tabulka 1 – Matice hrozby/obrany 29

Tabulka A.1 – Vztah mezi nebezpečnými událostmi a hrozbami 37

Tabulka B.1 – Kategorie přenosových systémů 38

Tabulka B.2 – Vztah hrozba/kategorie 39

Tabulka C.1 – Hodnocení bezpečnostních kódovacích mechanismů 47

Tabulka E.1 – Přiřazení z EN 50159-1:2001 do EN 50159:2010 56

Tabulka E.2 – Přiřazení z EN 50159-2:2001 do EN 50159:2010 57

Úvod

Jestliže elektronický systém vztahující se k bezpečnosti zahrnuje přenos informací mezi různými místy, potom tvoří sdělovací systém nedílnou část systému vztahujícího se k bezpečnosti a je nutno prokázat, že přenos z jednoho konce na druhý konec je v souladu s EN 50129 bezpečný.

Přenosový systém, který je uvažován v této normě, který slouží k přenosu informací mezi různými místy, nemá obecně žádné zvláštní předběžné podmínky, kterým je třeba vyhovět. Z hlediska bezpečnosti je nedůvěryhodný nebo ne zcela důvěryhodný.

Norma je zaměřena na požadavky, které je třeba brát v úvahu pro přenos informací vztahujících se k bezpečnosti v takových přenosových systémech.

Přestože se aspekty RAM v této normě neberou v úvahu, je třeba vzít na vědomí, že jsou hlavním aspektem celkové bezpečnosti.

Požadavky na bezpečnost závisí na charakteristikách přenosového systému. Aby se omezila složitost přístupu k demonstrování bezpečnosti systému, jsou přenosové systémy rozděleny do třech kategorií.

- Kategorie 1 zahrnuje systémy, nad nimiž má projektant kontrolu a které jsou během doby života stálé;
- Kategorie 2 zahrnuje systémy, které jsou částečně neznámé nebo nejsou stálé, neautorizovaný přístup však může být vyloučen;
- Kategorie 3 zahrnuje systémy, nad nimiž nemá projektant kontrolu a kde je nutné vzít v úvahu neautorizovaný přístup.

Na první kategorii se vztahovala EN 50159-1:2001, na ostatní kategorie EN 50159-2:2001.

Pokud u sdělovacích systémů vztahujících se k bezpečnosti, které byly schváleny podle předcházejících norem, dochází k údržbě a/nebo rozšíření, je možné pro nalezení souvislosti kapitol (článků) této normy s kapitolami (články) dřívější řady použít informativní přílohu E.

1 Rozsah platnosti

Tato evropská norma platí pro elektronické systémy vztahující se k bezpečnosti, které používají pro účely digitální komunikace přenosový systém, který nebyl nutně navržen pro aplikace vztahující se k bezpečnosti a který

- je pod kontrolou projektanta a je stálý během doby života, nebo
- je částečně neznámý nebo není stálý, neautorizovaný přístup však může být vyloučen, nebo
- není pod kontrolou projektanta a také je nutné vzít v úvahu neautorizovaný přístup.

K přenosovému systému mohou být připojena jak zařízení vztahující se k bezpečnosti, tak zařízení

nevztahující se k bezpečnosti.

Tato norma udává základní požadavky potřebné pro dosažení komunikace vztahující se k bezpečnosti mezi zařízeními vztahujícími se k bezpečnosti, která jsou připojena k přenosovému systému.

Tato evropská norma platí pro specifikaci bezpečnostních požadavků u zařízení vztahujících se k bezpečnosti, připojených k přenosovému systému, za účelem dosažení stanovených požadavků na integritu bezpečnosti.

Bezpečnostní požadavky jsou obecně implementovány do zařízení vztahujících se k bezpečnosti tím, že jsou navrženy podle EN 50129. V určitých případech mohou být tyto požadavky implementovány do jiných zařízení přenosového systému, pokud je systém řízen pomocí bezpečnostních opatření tak, aby byly splněny stanovené požadavky na integritu bezpečnosti.

Specifikace bezpečnostních požadavků je předpokladem důkazu bezpečnosti elektronického systému vztahujícího se k bezpečnosti, pro nějž jsou požadované doklady definovány v EN 50129. Doklady o řízení bezpečnosti a managementu jakosti je třeba převzít z EN 50129. Předmětem této normy jsou požadavky týkající se komunikace na důkazy funkční a technické bezpečnosti.

Tato evropská norma neplatí pro stávající systémy, které již byly schváleny před vydáním této normy.

Tato evropská norma nespecifikuje:

- přenosový systém;
- zařízení připojená k přenosovému systému;
- řešení (např. vzájemnou součinnost);
- které typy dat se vztahují k bezpečnosti a které nikoliv.

Zařízení vztahující se k bezpečnosti, připojené prostřednictvím otevřeného přenosového systému, může být vystaveno mnoha různým hrozbám vůči bezpečnosti informačních technologií, na ochranu proti nimž musí být definován celkový program, zahrnující aspekty řízení a technické a provozní aspekty.

V této evropské normě se však berou v úvahu, pokud jde o bezpečnost informačních technologií, pouze záměrné útoky prováděné prostřednictvím zpráv u aplikací vztahujících se k bezpečnosti.

Tato evropská norma se nezabývá obecnými aspekty bezpečnosti informačních technologií, zejména těmi, které se týkají

- zajištění důvěrnosti informací vztahujících se k bezpečnosti,
- zabránění přetěžování přenosového systému.

Konec náhledu - text dále pokračuje v placené verzi ČSN.