ČESKÁ TECHNICKÁ NORMA

ICS 35.080; 35.240.60 **Březen 2018**

Drážní zařízení – Zařízení drážních vozidel – Palubní software drážních vozidel	ČSN EN 50657 34 1518

Railway Applications – Rolling stock applications – Software on Board Rolling Stock

Applications ferroviaires – Applications du matériel roulant – Logiciels embarqués

Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen

Tato norma je českou verzí evropské normy EN 50657:2017. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 50657:2017. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

EN ISO 9000:2015 zavedena v ČSN EN ISO 9000:2016 (01 0300) Systémy managementu kvality – Základní principy a slovník

ISO/IEC 90003:2014 nezavedena

Souvisící ČSN a TNI

ČSN EN 50126-1:2017 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti,
udržovatelnosti a bezpečnosti (RAMS) – Část 1: Obecný RAMS postup

ČSN EN 50126-2:2017 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti,
udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti

ČSN EN 50128 ed. 2:2012 (34 2680) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy

ČSN EN 50129 (34 2675) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování

dat – Elektronické zabezpečovací systémy

ČSN EN 50155 ed. 3 (33 3555) Drážní zařízení – Elektronická zařízení drážních vozidel

ČSN EN 50159 (34 2670) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Komunikace v přenosových zabezpečovacích systémech

ČSN EN 61131-3 ed. 2 (18 7050) Programovatelné řídicí jednotky – Část 3: Programovací jazyky

ČSN EN 61508-2 ed. 2 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností

ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

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

ČSN IEC 60050-903:2015 (33 0050) Mezinárodní elektrotechnický slovník – Část 903: Posuzování rizik

TNI POKYN ISO/IEC 51 (76 3503) Bezpečnostní hlediska – Směrnice pro jejich začlenění do norem

ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Citované předpisy

Směrnice Evropského parlamentu a Rady 2008/57/ES ze dne 17. června 2008, o interoperabilitě železničního systému ve Společenství.

Upozornění na národní poznámky

Do normy byly k článkům 3.1.18, 3.1.34, 8.4.5.1, D.8, D.27, D.37, D.41 a doplněny národní poznámky informativního charakteru.

Vypracování normy

Zpracovatel: ACRI – Asociace podniků českého železničního průmyslu, IČO 63832721, Mgr. Martin Vlček Ph.D.

Technická normalizační komise: TNK 126 Elektrotechnika v dopravě

Pracovník České agentury pro standardizaci: Ing. Pavel Vojík

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

EVROPSKÁ NORMA EN 50657
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Srpen 2017

ICS 35.080;
35.240.60

Drážní zařízení – Zařízení drážních vozidel – Palubní software drážních vozidel

Railways Applications – Rolling stock applications – Software on Board Rolling Stock

Applications ferroviaires – Applications du matériel roulant – Logiciels embarqués

Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen

Tato evropská norma byla schválena CENELEC dne 2017-05-08. Členové CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání
v Řídicím centru CEN-CENELEC 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 Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

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

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

Ref. č. EN 50657:2017 E

Obsah

Strana

Strana

Strana

Strana

Strana

Obrázky

Tabulky

Evropská předmluva

Tento dokument (EN 50657:2017) vypracovala technická subkomise CLC/SC 9XB *Elektrický, elektronický a elektromechanický materiál na palubě drážních vozidel, včetně souvisejícího softwaru*.

Jsou stanovena tato data:

– nejzazší datum zavedení dokumentu na národní úrovni vydáním identické národní normy nebo vydáním oznámení o schválení k přímému používání jako normy národní	(dop)	2018-05-08
– nejzazší datum zrušení národních norem, které jsou s dokumentem v rozporu	(dow)	2020-05-08

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument byl vypracován na základě mandátu uděleného CENELEC Evropskou komisí a Evropským sdružením volného obchodu a pokrývá základní požadavky evropské směrnice (směrnic) EU.

Vztah ke směrnici (směrnicím) EU je uveden v informativní příloze ZZ, která je nedílnou součástí tohoto dokumentu.

Tento dokument upravuje normu EN 50128:2011 (vypracovanou technickou subkomisí CLC/SC 9XA *Komunikační, signalizační a prováděcí systémy*) pro použití v oblasti drážních vozidel. Používá stejnou strukturu a číslování článků jako EN 50128:2011. Pokud se požadavky EN 50128:2011 na kolejová vozidla nevztahují, je příslušný text nahrazen výrazem „záměrně vynecháno“.

Hlavní změny s ohledem na EN 50128:2011 jsou uvedeny v příloze E.

Úvod

Tato evropská norma souvisí a měla by být čtena v návaznosti na soubor EN 50126, *Drážní aplikace – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)*.

Tato evropská norma se zaměřuje na metody, které je potřeba použít při poskytování softwaru, který splňuje požadavky na integritu softwaru, které jsou na něj kladeny v těchto širších souvislostech.

Tato evropská norma stanovuje sadu požadavků, které musí být splněny během vývoje, nasazení a údržby
jakéhokoliv softwaru určeného pro drážní vozidla. Definuje požadavky ohledně organizační struktury, vztahu mezi organizacemi a rozdělení odpovědnosti týkajících se vývoje, nasazení a údržby. Tato evropská norma také
stanovuje kritéria na kvalifikaci a odbornost personálu.

Klíčové v této evropské normě jsou úrovně integrity softwaru. Tato evropská norma určuje pět úrovní integrity softwaru, přičemž základní integrita je nejnižší úroveň a 4 nejvyšší úroveň. Čím vyšší je riziko, které je následkem poruchy softwaru, tím vyšší bude úroveň integrity softwaru.

POZNÁMKA 1 Koncept základní integrity použitý v této evropské normě byl poprvé představen v souboru EN 50126.

Tato evropská norma určuje techniky a opatření pro pět úrovní integrity softwaru. Požadované techniky a opatření pro základní integritu a pro úrovně integrity 1 až 4 jsou uvedeny v normativní příloze A. V této verzi normy jsou požadované techniky pro úroveň 1 stejné jako pro úroveň 2 a požadované techniky pro úroveň 3 jsou stejné jako pro úroveň 4. Tato evropská norma nedává návod k určení úrovně integrity softwaru, která by odpovídala danému riziku. Toto rozhodnutí bude záviset na mnoha faktorech zahrnujících charakter aplikace, rozsah v jakém ostatní systémy vykonávají bezpečnostní funkce a sociální a ekonomické faktory.

Definice procesu specifikace funkcí bezpečnosti přiřazených softwaru je uvedena v rozsahu platnosti souboru EN 50126.

Tato evropská norma určuje opatření, která jsou nezbytná pro splnění těchto požadavků.

Soubor EN 50126 vyžaduje, aby byl použit systematický přístup pro:

a) identifikaci nebezpečí, hodnocení rizik a rozhodování založeným na kritériích rizika;

b) identifikaci nezbytného snížení rizika pro splnění kritérií akceptování rizika;

c) definování celkových požadavků na bezpečnost systému pro bezpečnostní opatření nezbytná pro dosažení požadovaného omezení rizika;

d) volbu vhodné architektury systému;

e) plánování, monitorování a řízení technických a manažerských činností potřebných pro převedení specifikací požadavků na bezpečnost systému do bezpečnostně relevantního systému s validovanou integritou bezpečnosti.

Jak dochází k rozkládání specifikací na návrh obsahující bezpečnostně relevantní systémy a komponenty, provádí se další přidělování úrovní integrity bezpečnosti. V konečném důsledku to

vede k požadovaným úrovním integrity softwaru.

Současný stav je takový, že ani použití metod zajištění kvality (takzvaná opatření pro vyhnutí se vadám a opatření pro detekci vad), ani použití přístupů odolnosti proti vadám softwaru nemůže zaručit absolutní bezpečnost softwaru. Neexistuje žádný známý způsob prokázání absence vad v přiměřeně složitém bezpečnostně relevantním softwaru, zejména absence vad ve specifikaci a návrhu.

Principy použité při vývoji softwaru s vysokou integritou zahrnují níže uvedené položky, ale nejsou omezeny jen na ně:

- metody návrhu shora dolů,
- modularitu,
- verifikaci každé etapy životního cyklu vývoje,
- verifikované komponenty a knihovny komponent,
- srozumitelná dokumentace a sledovatelnost,
- auditovatelné dokumenty,
- validaci,

– hodnocení,

– řízení konfigurace a řízení změn, a

– vhodné zvážení otázek organizace a kompetencí personálu.

Přidělení systémových požadavků na funkce softwaru je provedeno na systémové úrovni. To zahrnuje stanovení požadovaných úrovní integrity softwaru pro funkce. Posloupnost funkčních kroků při aplikaci této evropské normy je znázorněna na obrázku 1 a obsahuje následující kroky:

a) zformulování specifikace požadavků na software a současně zvážení architektury softwaru. Architektura softwaru představuje vytvoření strategie bezpečnosti pro software a pro úroveň integrity softwaru (7.2 a 7.3);

b) návrh, vývoj a testování softwaru podle plánu zajištění kvality softwaru, úrovně integrity softwaru a životního cyklu softwaru (7.4 a 7.5);

c) integrace softwaru na cílovém hardwaru a verifikace funkcionality (7.6);

d) přijmutí a nasazení softwaru (7.7 a 9.1);

e) je-li požadována údržba softwaru během provozního života je tato evropská norma reaktivována podle
potřeby (9.2).

Vývoj softwaru představuje řadu činností. Tyto zahrnují testování (6.1), verifikaci (6.2), validaci (6.3), hodnocení (6.4), zajištění kvality (6.5) a řízení modifikací a změn (6.6).

Norma stanovuje požadavky na podpůrné nástroje (6.7) a na systémy, které jsou konfigurovány aplikačními daty (8).

Rovněž jsou stanoveny požadavky na nezávislost rolí a kompetentnost personálu, který se podílí na vývoji
softwaru (5.1, 5.2 a příloha B).

Tato evropská norma nepředepisuje použití určitého životního cyklu vývoje softwaru. V kapitole 5.3 na obrázcích 3 a 4 a v kapitole 7.1 je však uveden názorný životní cyklus a soubor dokumentace.

Tabulky jsou sestaveny tak, že obsahují různé techniky/opatření, které jsou tříděny vzhledem k úrovním integrity bezpečnosti 1 – 4 a pro základní integritu. Tabulky jsou v příloze A. V tabulkách jsou uvedeny odkazy na biblio-
grafii uvádějící stručný popis jednotlivých technik/opatření s odvolávkami na další zdroje informací. Bibliografie technik je v příloze D.

Tato evropská norma nespecifikuje požadavky na vývoj, implementaci, údržbu a/nebo provoz zabezpečovací politiky nebo zabezpečovacích služeb potřebných k naplnění požadavků na zabezpečení, které mohou být požadovány bezpečnostně relevantním systémem. IT zabezpečení nemusí ovlivnit jen provoz, ale také funkční bezpečnost systému. Pro IT zabezpečení by měly být uplatněny odpovídající normy.

POZNÁMKA 2 IEC/ISO normy, které se zabývají IT zabezpečením do hloubky, jsou normy souboru ISO/IEC 27000, ISO/IEC/TR 19791 a souboru IEC 62443.

Může být nezbytné vyvážit opatření proti systematickým chybám a opatření proti hrozbám v zabezpečení. Příkladem je potřeba rychlých aktualizací softwaru z pohledu zabezpečení vyplývající z bezpečnostních hrozeb zatímco pokud se jedná o bezpečnostně relevantní software, měl by být pečlivě vyvinut, testován, validován a schválen před jakoukoliv aktualizací.

Obrázek 1 – Názorná posloupnost kroků vývoje softwaru

1 Rozsah platnosti

1.1 Tato evropská norma stanovuje postupy a technické požadavky pro vývoj softwaru pro programovatelné elektronické systémy pro použití v drážních aplikacích.

Mimo rozsah platnosti této normy je software, který:

- je součástí zabezpečovacího zařízení (aplikace patřící subkomisi CENELEC SC9XA) instalovaného na palubě vlaků, nebo
- nepřispívá k provozním funkcím kolejových vozidel a je od nich oddělen.

1.2 Tato evropská norma platí výhradně pro software a vzájemné působení mezi softwarem a systémem, jehož je software součástí.

1.3 Bod záměrně vynechán.

1.4 Tato evropská norma platí jak pro bezpečnostně relevantní software, tak pro software, který bezpečnostně relevantní není a zahrnuje například:

- aplikační programování;
- operační systémy;
- podpůrné nástroje;
- firmware.

Aplikační programování zahrnuje programování vyšší úrovně, programování nižší úrovně a specializované programování (např. žebříčková logika programovatelných logických automatů).

1.5 Tato evropská norma se rovněž zabývá použitím již existujícího softwaru a nástrojů. Takový software může být použit, jestliže jsou naplněny zvláštní požadavky 7.3.4.7 a 6.5.4.16 na již existující software a na nástroje podle kapitoly 6.7.

1.6 Software vyvinutý v souladu s platným vydáním EN 50128 je považován za odpovídající této normě. Software již dříve vyvinutý v souladu s jakoukoliv verzí EN 50128 je také považován za odpovídající této normě a není předmětem požadavků na již existující software. Pro software úrovní SIL1 – SIL4, který je v rozsahu platnosti této normy, jsou požadavky zahrnuté v této evropské normě ekvivalentní požadavkům na software úrovní SIL1 – SIL4 v EN 50128:2011.

1.7 Tato evropská norma bere v úvahu, že při moderním návrhu aplikací se často využívá software, který je vhodný jako základ pro různé aplikace. Takový software je pak konfigurován pomocí aplikačních dat pro vytvoření spustitelného softwaru pro aplikace. Tato evropská norma pro takový software platí. Navíc jsou stanoveny specifické požadavky pro aplikační data.

1.8 Bod záměrně vynechán.

1.9 Tato evropská norma nemá být retrospektivní. Platí tedy především pro nový vývoj a jako celek platí pro stávající systémy pouze tehdy, jsou-li podrobeny značným modifikacím. V případě malých změn platí pouze 9.2. Nicméně se doporučuje použití této evropské normy během upgradu a údržby existujícího softwaru.

1.10 Odpovídající kapitoly této normy jsou také použitelné na programovatelné komponenty (např. FPGA a CPLD) jako doplnění použitých hardwarových norem (např. EN 50129, EN 50155, EN 61508-2). Nicméně požadavky, které jsou stanoveny na základě použitých hardwarových norem, již nemusí být znovu požadovány.

Pokud je možné vyčerpávajícím způsobem testovat programovatelnou logiku na všechny možné vstupy a vnitřní logické stavy pak se nemusí tato evropská norma uplatňovat.