ČESKÁ TECHNICKÁ NORMA

ICS 35.240.60; 45.020; 35.080 **Duben 2012**

Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy

ČSN EN 50128
ed. 2
34 2680

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

Applications ferroviaires – Systemes de signalisation, de télécommunication et de traitement – Logiciels pour systemes
de commande et de protection ferroviaire

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software
für Eisenbahnsteuerungs- und Überwachungssysteme

Tato norma je českou verzí evropské normy EN 50128:2011. 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 50128:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

S účinností od 2014-04-25 se nahrazuje ČSN EN 50128 (34 2680) z dubna 2003, která do uvedeného data platí souběžně s touto normou.

Národní předmluva

Souběžně s touto normou je v souladu s předmluvou k EN 50128:2011 dovoleno do 2014-04-25 používat dosud platnou ČSN EN 50128 (34 2680) z dubna 2003.

Změny proti předchozí normě

Do této normy byly přidány požadavky na management softwaru a organizaci, definice rolí a kompetencí, nasazení a údržbu. Byla vložena nová kapitola týkající se nástrojů, která je založená na EN 61508-2:2010. Byly aktualizovány tabulky v příloze A.

Informace o citovaných dokumentech

EN 50126-1:1999 zavedena v ČSN EN 50126-1:2001 (33 3502) Drážní zařízení – Stanovení a prokázání

bezpo-
ruchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces

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

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

EN ISO 9001 zavedena v ČSN EN ISO 9001 ed. 2 (01 0321) Systém managementu kvality – Požadavky

ISO/IEC 90003:2004 zavedena v ČSN ISO/IEC 90003:2005 (36 9043) Softwarové inženýrství – Směrnice pro použití ISO 9001:2000 na počítačový software

ISO/IEC 9126 soubor zavedena pouze ISO/IEC 9126-1 v ČSN ISO/IEC 9126-1 (36 9020) Softwarové inženýrství – Jakost produktu – Část 1: Model jakosti

Souvisící ČSN

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

ČSN EN 61131-3:2003 (18 7050) Programovatelné řídicí jednotky – Část 3: Programovací jazyky

ČSN EN 61158-2 ed. 4:2011 (18 4020) Průmyslové komunikační sítě – Specifikace sběrnice pole – Část 2: Specifikace fyzické vrstvy a definice služby

ČSN IEC 61713:2001 (01 0692) Zajištění spolehlivosti softwaru pomocí procesů jeho životního cyklu – Návod k použití

ČSN ISO/IEC 14598 soubor (36 9028) Informační technologie – Hodnocení softwarového produktu

Vypracování normy

Zpracovatel: CTN ACRI Praha, IČ 63832721, Mgr. Martin Vlček, Ph.D.

Technická normalizační komise: TNK 126 Elektrotechnika v dopravě

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

EVROPSKÁ NORMA EN 50128
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Červen 2011

ICS 35.240.60; 45.020; 93.100 Nahrazuje EN 50128:2001

Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy

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

Applications ferroviaires – Systemes de signalisation, de télécommunication et de traitement – Logiciels pour systemes de commande et de protection ferroviaire

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme

Tato evropská norma byla schválena CENELEC dne 2011-04-25. 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 komitéty Belgie, Bulharska, 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, 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

Řídicí centrum: Avenue Marnix 17, B-1000 Brusel

Ref. č. EN 50128:2011 E

Předmluva

Tuto evropskou normu vypracovala SC 9XA Sdělovací a zabezpečovací systémy a systémy zpracování dat, technické komise CENELEC/TC 9X Elektrická a elektronická drážní zařízení.

Text návrhu byl předložen k formálnímu hlasování a byl schválen CENELEC jako EN 50128 dne 2011-04-25.

Tento dokument nahradí EN 50128:2001.

Významné změny ve vztahu k předešlému vydání EN 50128:2001 jsou následující:

- byly přidány požadavky na management softwaru a organizaci, definice rolí a kompetencí, nasazení a údržbu;
- byla vložena nová kapitola týkající se nástrojů, založená na EN 61508-2:2010;
- byly aktualizovány tabulky v příloze A.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN a CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech 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	(dop)	2012-04-25
• nejzazší datum zrušení národních norem, které jsou s EN v rozporu	(dow)	2014-04-25

Tuto evropskou normu je třeba používat spolu s EN 50126-1:1999 „*Drážní zařízení Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces*“ a EN 50129:2003 „*Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy*“.

Obsah

Strana

Obrázky

Tabulky

Tato norma je částí skupiny souvisejících norem. Další normy jsou EN 50126-1:1999 „Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces“ a EN 50129:2003 „Drážní zařízení – Elektronické zabezpečovací systémy“.

EN 50126-1 se zabývá systémovými otázkami systému v nejširším měřítku, zatímco předmětem EN 50129 je schvalovací proces pro jednotlivé systémy, které mohou existovat v rámci drážního řídicího a ochranného systému jako celku. Tato norma se soustředí na metody, které je třeba použít za účelem poskytnutí softwaru, který vyhovuje požadavkům na integritu bezpečnosti, které jsou na něj kladeny na základě těchto širších úvah.

Tato norma stanovuje soubor požadavků, které musí být během vývoje, nasazení a údržby jakéhokoliv bezpečnostně relevantního software pro drážní řídicí a ochranné aplikace splněny. Definuje požadavky ohledně organizační struktury, vztahu mezi organizacemi a rozdělení odpovědnosti týkající se vývoje, nasazení a údržby. Tato norma také stanovuje kritéria pro kvalifikaci a odbornost personálu.

Klíčové v této evropské normě jsou otázky týkající se úrovně integrity bezpečnosti softwaru. Tato evropská norma určuje pět úrovní integrity bezpečnosti softwaru, kde 0 je nejnižší úroveň a 4 nejvyšší úroveň. Čím vyšší je riziko, které je následkem poruchy softwaru, tím vyšší bude úroveň integrity bezpečnosti softwaru.

Tato evropská norma určuje techniky a opatření pro 5 úrovní integrity bezpečnosti softwaru. Požadované techniky a opatření pro úrovně integrity bezpečnosti softwaru 0-4 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 bezpečnosti 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 předmětem EN 50126-1 a EN 50129.

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

EN 50126-1 a EN 50129 vyžadují, aby byl použit systematický přístup pro:

a. identifikaci nebezpečí, hodnocení rizik a dospění k rozhodnutím založeným na kritériích rizika;
b. identifikaci nezbytného omezení rizika pro splnění kritérií akceptování rizika;
c. definování celkové specifikace požadavků na bezpečnost systému pro bezpečnostní opatření potřebných pro dosažení požadovaného omezení rizika;
d. volbu vhodné architektury systému;
e. plánování, monitorování a řízení technických a manažerských činností potřebných pro převedení specifikace požadavků na bezpečnost systému do bezpečnostně relevantního systému s validovanou integritou bezpečnosti.

Jak dochází k rozložení specifikace na návrh obsahující bezpečnostně relevantní systémy a komponenty, provádí se další přidělování úrovní integrity bezpečnosti. V konečném důsledku to vede k požadovaným úrovním integrity bezpečnosti softwaru.

Současný stav je takový, že ani použití metod zajištění kvality (tak zvaná 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 v návrhu.

Principy použité při vývoji sofwaru 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 trasovatelnost;
- auditovatelné dokumenty;
- validaci;
- hodnocení;
- řízení konfigurace a řízení změn;
- vhodné zvážení otázek organizace a kompetencí personálu.

Specifikace požadavků na bezpečnost systému identifikuje všechny funkce bezpečnosti přidělené softwaru a určuje jejich úroveň integrity bezpečnosti. Postupnost 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 bezpečnosti softwaru (7.2 a 7.3);
b. návrh, vývoj a testování softwaru podle plánu zajištění kvality softwaru, úrovně integrity bezpečnosti softwaru a životního cyklu softwaru (7.4 a 7.5);
c. integrace softwaru do cílového 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 (kapitola 6.1), verifikaci (kapitola 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 nebo algoritmy (8).

V normě jsou rovněž 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. Je však uveden názorný životní cyklus a soubor dokumentace (5.3, obrázek 3 a 4 a v článku 7.1).

Tabulky jsou sestaveny tak, že obsahují různé techniky/opatření, které jsou tříděny vzhledem k úrovním 0-4 integrity bezpečnosti softwaru. Tabulky jsou v příloze A. V tabulkách jsou uvedeny odkazy na bibliografii uvádějící stručný popis jednotlivých technik/opatření s odvolávkami na další zdroje informací. Bibliografie technik je v příloze D.

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 řídicích a ochranných aplikacích. Je zaměřena na použití v kterékoliv oblasti, kde jde o bezpečnost. Tyto systémy mohou být realizovány s využitím jednoúčelových mikroprocesorů, programovatelných logických automatů, multiprocesorových distribuovaných systémů, větších systémů s ústředním procesorem nebo pomocí jiných architektur.

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

1.3 Tato evropská norma není relevantní pro software, u kterého nebyly zjištěny dopady na bezpečnost, tedy pro takový software, jehož porucha nemůže ovlivnit identifikované bezpečnostní funkce.

1.4 Tato evropská norma platí pro veškerý bezpečnostně relevantní software používaný v drážních řídicích a ochranných systémech zahrnující:

- 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) (Programmable logic controller ladder logic).

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 Sofware vyvinutý v souladu s jakoukoliv verzí této evropské normy se považuje za vyhovující a nepodléhá požadavkům na již existující software.

1.7 Tato evropská norma bere v úvahu, že při moderním návrhu aplikací se často využívá generický software, který je vhodný jako základ pro různé aplikace. Takový generický software je pak konfigurován pomocí dat, algoritmů nebo obojího, pro vytvoření spustitelného softwaru pro aplikace. Obecné kapitoly 1 až 6 a 9 této evropské normy platí pro generický software stejně jako pro aplikační data nebo algoritmy. Kapitola 7 platí pouze pro generický software, zatímco kapitola 8 stanoví specifické požadavky pro aplikační data nebo algoritmy.

1.8 Tato evropská norma se nezabývá obchodními otázkami. Ty mají být základní částí jakékoliv smluvní dohody. Všechny kapitoly této evropské normy budou vyžadovat v jakékoliv obchodní situaci pečlivé uvážení.

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. Hodnotitel musí analyzovat důkazy poskytnuté v dokumentaci softwaru a potvrdit, zda je stanovení povahy a rozsahu softwarových změn dostatečné. Nicméně se velmi doporučuje použití této evropské normy během vylepšení a údržby existujícího softwaru.