

Drážní zařízení – Požadavky na vývoj softwaru

ČSN
EN 50716

34 2680

Railway Applications – Requirements for software development

Applications ferroviaires – Exigences pour le développement de logiciels

Sektorübergreifende Software-Norm für Eisenbahnen

Tato norma je českou verzí evropské normy EN 50716:2023. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 50716:2023. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

S účinností od 2026-10-30 se nahrazuje ČSN EN 50128 ed. 2 (34 2680) z dubna 2012 a ČSN EN 50657 (34 1518) z března 2018, které do uvedeného data platí souběžně s touto normou.

Národní předmluva

Upozornění na používání této normy

Souběžně s touto normou je v souladu s předmluvou k EN 50716:2023 dovoleno do 2026-10-30 používat dosud platnou ČSN EN 50128 ed. 2 (34 2680) z dubna 2012 a ČSN EN 50657 (34 1518) z března 2018.

Změny proti předchozím normám

Přehled hlavních změn v porovnání s EN 50128:2011 a EN 50657:2017 je uveden v Evropské předmluvě.

Souvisící ČSN

ČSN EN 50126-1 ed. 2:2019 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti udržitelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS

ČSN EN 50126-2:2019 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti,

pohotovosti udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti

ČSN EN ISO/IEC 27000:2020 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN IEC 62443 (soubor) (18 0304) Průmyslové komunikační sítě – Bezpečnost sítě a systému

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

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

TNI POKYN ISO/IEC 51:2015 (76 3503) Bezpečnostní hlediska – Směrnice pro jejich začlenění do norem

ČSN IEC 60050-821:2019 (330050) Mezinárodní elektrotechnický slovník – Kapitola 821: Drážní signalizační a zabezpečovací zařízení

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 50657:2018 (34 1518) Drážní zařízení – Zařízení drážních vozidel – Palubní software drážních vozidel

ČSN EN 50129 ed. 2:2021 (34 2675) Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy

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

ČSN EN ISO 9001:2016 (01 0321) Systémy managementu kvality – Požadavky

ČSN ISO/IEC/IEEE 90003:2019 (36 9035) Softwarové inženýrství – Směrnice pro použití ISO 9001:2015 na počítačový software

ČSN EN 50562:2019 (34 1523) Drážní zařízení – Pevná trakční zařízení – Proces, ochranná opatření a prokázání bezpečnosti elektrických trakčních soustav

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „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 2016/797/EU ze dne 11. května 2016, o interoperabilitě železničního systému v Evropské unii (přepřacované znění). V České republice je tato směrnice zavedena zákonem č. 266/1994 Sb., o drahách, v platném znění.

Nařízení Komise (EU) č. 1302/2014 ze dne 18. listopadu 2014, o technické specifikaci pro interoperabilitu subsystému kolejová vozidla – lokomotivy a kolejová vozidla pro přepravu osob železničního systému v Evropské unii. V České republice je toto nařízení zavedeno zákonem č. 266/1994 Sb., o drahách, v platném znění.

Upozornění na národní poznámky

Do této normy byly k článkům 3.1.1, 3.1.2, 3.1.15, 3.1.30, 3.1.43, 8.4.5.1, C.2, D.8, D.27 a D.37 doplněny národní poznámky upřesňujícího charakteru.

Vypracování normy

Zpracovatel odborného překladu: ACRI – Asociace podniků českého železničního průmyslu, IČO 63832721

Technická normalizační komise: TNK 126 Elektrotechnika v dopravě

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat na e-shopu.

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
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50716

Listopad 2023

ICS 35.240.60
EN 50128:2011/AC:2014;
EN 50128:2011/A1:2020;
EN 50657:2017/A1:2023

Nahrazuje EN 50128:2011;

EN 50657:2017;

EN 50128:2011/A2:2020;

Drážní zařízení – Požadavky na vývoj softwaru

Railway Applications – Requirements for software development

Applications ferroviaires – Exigences pour le développement de logiciels

Sektorübergreifende Software-Norm für Eisenbahnen

Tato evropská norma byla schválena CENELEC dne 2023-10-30. 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 komitety Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, 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: Rue de la Science 23, B-1040 Brusel

© 2023 CENELEC Veškerá práva pro využití v jakékoliv formě a jakýmikoliv prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN 50716:2023 E

Evropská předmluva.....	10
Úvod.....	11
1..... Rozsah platnosti.....	14
2..... Citované dokumenty.....	14
3..... Termíny, definice a zkratky.....	15
3.1..... Termíny a definice.....	15
3.2..... Zkratky.....	20
4..... Shoda úrovně integrity softwaru.....	21
5..... Management softwaru a organizace.....	22
5.1..... Organizace a nezávislost rolí.....	22
5.1.1... Cíl.....	22
5.1.2... Požadavky.....	22
5.2..... Kompetence personálu a odpovědnosti.....	24

5.2.1...

Cíle.....	
.....	24

5.2.2...

Požadavky.....	
.....	24

5.3..... Otázky životního cyklu

a dokumentace.....	
25	

5.3.1...

Cíle.....	
.....	25

5.3.2...

Požadavky.....	
.....	25

6..... Zajištění

softwaru.....	
.....	26

6.1..... Testování

softwaru.....	
.....	26

6.1.1...

Cíl.....	
.....	26

6.1.2... Vstupní

dokumenty.....	
.....	26

6.1.3... Výstupní

dokumenty.....	
.....	26

6.1.4...

Požadavky.....	
.....	26

6.2..... Verifikace

softwaru.....	
.....	27

6.2.1...

Cíl.....	
.....	27

6.2.2... Vstupní

dokumenty.....	27
6.2.3... Výstupní dokumenty.....	27
6.2.4... Požadavky.....	27
6.3..... Validace softwaru.....	28
6.3.1... Cíl.....	28
6.3.2... Vstupní dokumenty.....	28
6.3.3... Výstupní dokumenty.....	29
6.3.4... Požadavky.....	29
6.4..... Posouzení softwaru.....	29
6.4.1... Cíl.....	29
6.4.2... Vstupní dokumenty.....	30
6.4.3... Výstupní dokumenty.....	30
6.4.4... Požadavky.....	30
6.5..... Prokazování kvality softwaru.....	

... 31

6.5.1...

Cíle.....
..... 31

6.5.2... Vstupní

dokumenty.....
..... 31

6.5.3... Výstupní dokumenty.....	
.....	31
6.5.4...	
Požadavky.....	
.....	31
6.6..... Řízení modifikací a změn.....	
.....	33
6.6.1...	
Cíle.....	
.....	33
6.6.2... Vstupní dokumenty.....	
.....	33
6.6.3... Výstupní dokumenty.....	
.....	33
6.6.4...	
Požadavky.....	
.....	33
6.7..... Podpůrné nástroje a jazyky.....	
.....	34
6.7.1...	
Cíle.....	
.....	34
6.7.2... Vstupní dokumenty.....	
.....	34
6.7.3... Výstupní dokumenty.....	
.....	34
6.7.4...	
Požadavky.....	
.....	34
7..... Vývoj softwaru.....	
.....	36

7.1..... Životní cyklus a dokumentace softwaru.....	36
7.1.1...	
Cíle.....	36
7.1.2...	
Požadavky.....	36
7.2..... Požadavky na software.....	37
7.2.1...	
Cíle.....	37
7.2.2... Vstupní dokumenty.....	37
7.2.3... Výstupní dokumenty.....	37
7.2.4...	
Požadavky.....	37
7.3..... Architektura a návrh.....	39
7.3.1...	
Cíle.....	39
7.3.2... Vstupní dokumenty.....	39
7.3.3... Výstupní dokumenty.....	39
7.3.4...	
Požadavky.....	39
7.4..... Návrh komponenty.....	

..... 45

7.4.1...

Cíle.....
..... 45

7.4.2... Vstupní

dokumenty.....
..... 45

7.4.3... Výstupní

dokumenty.....
..... 45

7.4.4...

Požadavky.....
..... 45

7.5..... Implementace a testování

komponenty..... 47

7.5.1...

Cíle.....
..... 47

7.5.2... Vstupní

dokumenty.....
..... 47

7.5.3... Výstupní

dokumenty.....
..... 47

7.5.4...

Požadavky.....
..... 47

7.6.....

Integrace.....
..... 48

7.6.1...

Cíle.....
..... 48

7.6.2... Vstupní

dokumenty.....
..... 48

7.6.3... Výstupní

dokumenty.....
..... 48

7.6.4...

Požadavky.....	
.....	48

7.7..... Celkové testování softwaru / Závěrečná

validace.....	49
---------------	----

7.7.1...

Cíle.....	
.....	49

7.7.2... Vstupní dokumenty.....	49
7.7.3... Výstupní dokumenty.....	49
7.7.4... Požadavky.....	50
8..... Vývoj aplikačních dat: systémy konfigurované aplikačními daty.....	51
8.1..... Cíle.....	51
8.2..... Vstupní dokumenty.....	51
8.3..... Výstupní dokumenty.....	52
8.4..... Požadavky.....	52
8.4.1... Proces vývoje aplikace.....	52
8.4.2... Specifikace požadavků na aplikaci.....	53
8.4.3... Architektura a návrh.....	53
8.4.4... Tvorba aplikačních dat.....	53
8.4.5... Integrace aplikace a testování.....	54
8.4.6... Validace a posouzení	

aplikace.....	
55	
8.4.7... Procedury a nástroje přípravy	
aplikace.....	55
9..... Nasazení a údržba	
softwaru.....	
.....	55
9.1..... Nasazení	
softwaru.....	
.....	55
9.1.1...	
Cíl.....	
.....	55
9.1.2... Vstupní	
dokumenty.....	
.....	55
9.1.3... Výstupní	
dokumenty.....	
.....	55
9.1.4...	
Požadavky.....	
.....	56
9.2..... Údržba	
softwaru.....	
.....	57
9.2.1...	
Cíl.....	
.....	57
9.2.2... Vstupní	
dokumenty.....	
.....	57
9.2.3... Výstupní	
dokumenty.....	
.....	57
9.2.4...	
Požadavky.....	
.....	57
Příloha A (normativní) Kritéria pro výběr technik	
a opatření.....	60

Příloha B (normativní) Klíčové role a odpovědnosti souvisící s vývojem softwaru.....	70
Příloha C (informativní) Návod na vývoj softwaru.....	76
Příloha D (informativní) Bibliografie technik.....	88
Příloha ZZ (informativní) Vztah mezi touto evropskou normou a základními požadavky směrnice EU 2016/797/EU, které mají být pokryty.....	113
Bibliografie.....	115

Seznam obrázků

Obrázek 1 – Názorná mapa postupu vývoje softwaru.....	13
Obrázek 2 – Znázornění doporučené organizační struktury.....	23
Obrázek C.1 – Lineární model životního cyklu příklad 1 (Vodopád).....	77
Obrázek C.2 – Lineární model životního cyklu příklad 2 (V model).....	78
Obrázek C.3 – Iterativní model životního cyklu příklad 1.....	79
Obrázek C.4 – Iterativní model životního cyklu příklad 2.....	80
Obrázek C.5 – Příklad iterativního vývoje pracovního produktu.....	80
Obrázek C.6 – Iterativní model životního cyklu příklad 3.....	81

Seznam tabulek

Tabulka 1 – Vztah mezi třídami nástroje a příslušnými číslováními články.....	36
Tabulka A.1 – Problematika životního cyklu a dokumentace (5.3).....	61
Tabulka A.2 – Specifikace požadavků na software (7.2).....	63
Tabulka A.4 – Návrh a implementace softwaru (7.3, 7.4 a 7.5).....	64
Tabulka A.5 – Analýza a testování komponent softwaru (6.2 a 7.4).....	64
Tabulka A.6 – Analýza a testování integrace softwaru (7.3 a 7.6).....	65
Tabulka A.7 – Analýza a testování celkového softwaru (6.2 a 7.2).....	65
Tabulka A.8 – Záměrně ponecháno prázdné.....	65
Tabulka A.9 – Prokazování kvality softwaru (6.5).....	65
Tabulka A.10 – Údržba softwaru (9.2).....	66
Tabulka A.11 – Techniky přípravy dat (8.4).....	66
Tabulka A.12 – Kódovací standardy.....	66
Tabulka A.13 – Dynamická analýza a testování.....	67
Tabulka A.14 – Záměrně ponecháno prázdné.....	67
Tabulka A.15 – Vhodné programovací jazyky.....	67
Tabulka A.16 – Záměrně ponecháno prázdné.....	68
Tabulka A.17 –	

Modelování.....	68
Tabulka A.18 - Testování výkonnosti.....	68
Tabulka A.19 - Statická analýza.....	68
Tabulka A.20 - Komponenty.....	69
Tabulka A.21 - Pokrytí kódu testem.....	69
Tabulka B.1 - Specifikace role manažera pro požadavky.....	70
Tabulka B.2 - Specifikace role návrháře.....	71
Tabulka B.3 - Specifikace role implementátora.....	71
Tabulka B.4 - Specifikace role testera.....	72
Tabulka B.5 - Specifikace role verifikátora.....	72
Tabulka B.6 - Specifikace role validátora.....	73
Tabulka B.7 - Specifikace role posuzovatele.....	74
Tabulka B.8 - Specifikace role manažera projektu.....	74
Tabulka B.9 - Specifikace role manažera konfigurace.....	75
Tabulka C.1 - Typické přizpůsobení architektury a návrhu pro modelování.....	84

Tabulka C.2 – Typické přizpůsobení implementace a testování komponent pro modelování..... 85

Tabulka C.3 – Typické přizpůsobení technik/opatření kódovacích standardů pro modelování..... 85

Tabulka ZZ.1 – Soulad mezi touto evropskou normou, nařízením Komise 2016/919 o technické specifikaci pro interoperabilitu subsystémů „Řízení a zabezpečení“ železničního systému v Evropské unii* a směrnicí (EU) 2016/797..... 113

Tabulka ZZ.2 – Soulad mezi touto evropskou normou, nařízením Komise (EU) č. 1302/2014 o technické specifikaci pro interoperabilitu subsystému „kolejová vozidla – lokomotivy a osobní kolejová vozidla“ železničního systému v Evropské unii* a směrnicí (EU) 2016/797..... 114

Evropská předmluva

Tento dokument (EN 50716:2023) vypracovala technická komise CLC/TC 9X *Elektrické a elektronické zařízení pro železnice*.

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) 2024-10-30
- nejzazší datum zrušení národních norem, které jsou s dokumentem v rozporu (dow) 2026-10-30

Tento dokument nahrazuje EN 50128:2011 a EN 50657:2017 a všechny jejich změny a opravy (pokud existují).

EN 50716:2023 obsahuje v porovnání s EN 50128:2011 a EN 50657:2017 tyto významné technické změny:

- bylo provedeno větší sjednocení s EN 50126-1:2017 a EN 50126-2:2017, včetně definic;
- kapitola 5: byly přepsány požadavky, aby se zjednodušila srozumitelnost (přičemž stávající možnosti organizace zůstaly v podstatě nezměněny);
- byla aktualizována příloha A, aby lépe odpovídala etapám životního cyklu;
- v informativní příloze C byla doplněna nová kapitola C.1 s dalším návodem týkajícím se modelů životního cyklu;
- v informativní příloze C byla doplněna nová kapitola C.2 s návodem pro modelování při vývoji softwaru;
- byly doplněny další pokyny pro komponenty softwaru s různými úrovněmi integrity softwaru;
- byly zobecněny požadavky na programovací jazyky.

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

Tento dokument se používá společně s EN 50126-1 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS* [1] a EN 50126-2 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti* [2].

Pro drážní pevná zařízení (řízení a napájení elektrické trakce) platí EN 50562 *Drážní zařízení – Pevná trakční zařízení – Proces, ochranná opatření a prokázání bezpečnosti elektrických trakčních soustav* [20].

Tento dokument byl vypracován na základě normalizačního požadavku uděleného CENELEC Evropskou komisí. Stálý výbor států ESVO následně tyto žádosti za své členské státy schvaluje.

Vztah k legislativě EU viz informativní příloha ZZ, která je nedílnou součástí tohoto dokumentu.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CENELEC.

Úvod

Tento dokument se zaměřuje na metody, které musí být použity k vytvoření softwaru, který splňuje požadavky na integritu softwaru.

Tento dokument stanovuje sadu požadavků na vývoj, nasazení a údržbu jakéhokoli softwaru určeného pro železniční aplikace. Definuje požadavky týkající se organizační struktury, vztahů mezi organizacemi a rozdělení odpovědnosti za činnosti spojené s vývojem, nasazením a údržbou. V tomto dokumentu jsou rovněž stanovena kritéria pro kvalifikaci a odbornost personálu.

Klíčovým konceptem tohoto dokumentu jsou úrovně integrity softwaru. Tento dokument se zabývá pěti úrovněmi integrity softwaru, přičemž základní integrita je nejnižší a úroveň integrity 4 nejvyšší. Čím vyšší je riziko vyplývající z poruchy softwaru, tím vyšší má být úroveň integrity softwaru.

POZNÁMKA 1 Koncept základní integrity použitý v tomto dokumentu byl poprvé představen v souboru EN 50126 ([1] [2]).

Tento dokument určuje techniky a opatření pro pět úrovní integrity softwaru. Požadované techniky a opatření pro základní integritu a pro úrovně integrity bezpečnosti 1 až 4 jsou uvedeny v normativních tabulkách v příloze A. Požadované techniky pro úroveň 1 jsou stejné jako pro úroveň 2 a požadované techniky pro úroveň 3 jsou stejné jako pro úroveň 4. Tento dokument nedává návod k určení úrovně integrity softwaru, která by odpovídala danému riziku. Toto rozhodnutí bude záviset na mnoha faktorech zahrnujících charakter aplikace, rozsahu, v jakém ostatní systémy vykonávají funkce související s bezpečností, a na sociálních a ekonomických faktorech.

Definice procesu specifikace funkcí souvisejících s bezpečností přiřazených softwaru je v rozsahu platnosti EN 50126-1 a EN 50126-2.

Tento dokument určuje opatření, která jsou nezbytná pro splnění těchto požadavků.

Soubor EN 50126 ([1] [2]) vyžaduje, aby byl použit systematický přístup pro:

- a) identifikaci nebezpečí, posuzování 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, sledování a řízení technických a řídicích činností nezbytných k převedení požadavků na bezpečnost systému do systému souvisejícího s bezpečností na ověřené úrovni integrity bezpečnosti.

Jak dochází k rozkládání specifikací na návrh obsahující bezpečnostně relevantní systémy a komponenty, pro-vádí se další přidělování úrovní integrity bezpečnosti. V konečném důsledku to vede k požadovaným úrovním integrity softwaru.

Současný stav techniky je takový, že ani použití metod prokazování 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.

Zásady použité při vývoji softwaru s vysokou integritou zahrnují, ale neomezují se pouze na:

- metody návrhu shora dolů,
- modularitu,
- verifikaci každé etapy životního cyklu vývoje,
- verifikované komponenty a knihovny komponent,
- srozumitelnou dokumentaci a sledovatelnost,
- auditovatelné dokumenty,
- validaci,
- posouzení,
- řízení konfigurace a řízení změn,
- 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 tohoto dokumentu je znázorněno na obrázku 1 a obsahuje:

- f) 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);
- g) návrh, implementaci a testování softwaru podle plánu prokazování kvality softwaru, úrovně integrity softwaru a životního cyklu softwaru (7.4 a 7.5);
- h) integraci softwaru do cílového hardwaru a verifikaci funkčnosti (7.6);
- i) validaci a nasazení softwaru (7.7 a 9.1);
- j) údržba softwaru, je-li vyžadována v průběhu životnosti (9.2).

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

Jsou stanoveny požadavky na podpůrné nástroje (6.7) a na systémy, které jsou konfigurovány aplikačními daty (kapitola 8).

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

Tento dokument nepředepisuje použití určitého životního cyklu vývoje softwaru. V 5.3, 7.1 a v C.1 jsou však uvedeny ilustrativní soubory životních cyklů a dokumentace.

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

POZNÁMKA 2 Některé položky v tomto dokumentu byly záměrně ponechány prázdné. Tím je zajištěno, že číslování zůstane, pokud je to možné a pokud to nemá vliv na srozumitelnost, nezměněno s ohledem na EN 50128 a EN 50657. To má v příslušných případech usnadnit přechod a použití tohoto dokumentu.

Tento dokument nespecifikuje požadavky na vývoj, implementaci, údržbu a/nebo provoz zabezpečovací politiky nebo zabezpečovacích služeb potřebných k naplnění požadavků na kybernetickou bezpečnost, které mohou být požadovány bezpečnostně relevantním systémem. Kybernetické útoky mohou ovlivnit nejen provoz, ale i funkční bezpečnost systému. Pro kybernetickou bezpečnost by měly být použity příslušné normy.

POZNÁMKA 3 Publikace IEC/ISO a CEN/CENELEC, které se zabývají kybernetickou bezpečností do hloubky, jsou [3], [4], [5] a [17].

Může být nutné vyvážit opatření proti systematickým chybám a opatření proti bezpečnostním hrozbám. Příkladem může být potřeba rychlé aktualizace bezpečnostního softwaru vyplývající z bezpečnostních hrozeb, zatímco pokud se jedná o bezpečnostně relevantní software, měl by být před každou aktualizací důkladně vyvinut, testován, validován a schválen.



Obrázek 1 - Názorná mapa postupu vývoje softwaru

1 Rozsah platnosti

1.1 Tento dokument stanovuje postupy a technické požadavky pro vývoj softwaru pro programovatelné elektronické systémy pro použití v:

- řídicích a zabezpečovacích aplikacích;
- aplikacích na palubách kolejových vozidel.

Tento dokument není určen pro použití v oblasti napájení elektrické trakce (pevné instalace) nebo pro napájení a řízení běžných aplikací, např. napájení stanic pro kanceláře, obchody. Na tyto aplikace se obvykle vztahují normy pro distribuci energie a/nebo jiná než železniční odvětví a/nebo místní právní rámce.

1.2 Tento dokument platí výhradně pro software a vzájemné působení mezi softwarem a systémem, jehož součástí je software.

1.3 Záměrně ponecháno prázdné.

1.4 Tento dokument platí pro software používaný v železničních systémech podle článku 1.1, včetně:

- aplikačního programování;
- provozních systémů;
- podpůrných nástrojů;
- firmwaru.

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

1.5 Tento dokument se rovněž zabývá použitím již existujícího softwaru (jak je uvedeno v 3.1.16) a nástrojů. Takový software může být použit, jestliže jsou naplněny zvláštní požadavky v 7.3.4.7 a 6.5.4.16 pro již existující software a v 6.7 pro nástroje.

1.6 Záměrně ponecháno prázdné

1.7 Tento dokument 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.

1.8 Záměrně ponecháno prázdné.

1.9 Tento dokument 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 tohoto dokumentu během upgradu a údržby existujícího softwaru.

1.10 Pro vývoj uživatelsky programovatelných integrovaných obvodů (např. pole programovatelných hradlových polí (FPGA) a komplexních programovatelných logických zařízení (CPLD)) je návod uveden v EN 50129:2018, příloha F, pro funkce související s bezpečností a v EN 50155:2017 pro

funkce nesouvisející s bezpečností. Software běžící na softwarových procesorech uživatelsky programovatelných integrovaných obvodů spadá do rozsahu platnosti tohoto dokumentu.

Konec náhledu - text dále pokračuje v placené verzi ČSN.