

2024

Strojní zařízení pro zemní práce – Funkční bezpečnost –
Část 4: Návrh a hodnocení softwaru a přenosu dat pro bezpečnostní
části ovládacího systému

ČSN
EN ISO 19014-4

27 8017

idt ISO 19014-4:2020

Earth-moving machinery – Functional safety –
Part 4: Design and evaluation of software and data transmission for safety-related parts of the
control system

Engins de terrassement – Sécurité fonctionnelle –
Partie 4: Conception et évaluation du logiciel et de la transmission des données pour les parties
relatives a la sécurité
du systeme de commande

Erdbaumaschinen – Functionale Sicherheit –
Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante
Steuerungssysteme

Tato norma je českou verzí evropské normy EN ISO 19014-4:2020. Překlad byl zajištěn Českou
agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is Czech version of European Standard EN ISO 19014-4:2020. It was translated by Czech
Standardization Agency. It has same status as official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 19014-4 (27 8017) z února 2021.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 19014-4:2020 do soustavy ČSN.
Zatímco ČSN EN ISO 19014-4 z února 2021 převzala EN ISO 19014-4:2020 vyhlášením jako ČSN,
tato norma ji přejímá překladem.

Informace o citovaných dokumentech

ISO 6750-1 zavedena v ČSN ISO 6750-1 (27 7805) Stroje pro zemní práce – Návod k používání – Část
1: Obsah a provedení

ISO 12100:2010 zavedena v ČSN EN ISO 12100:2011 (83 3001) Bezpečnost strojních zařízení - Všeobecné zásady pro konstrukci - Posouzení rizika a snižování rizika

ISO 13849-1 zavedena v ČSN EN ISO 13849-1 (83 3205) Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Obecné zásady pro konstrukci

ISO 19014-1 zavedena v ČSN EN ISO 19014-1 (27 8017) Strojní zařízení pro zemní práce - Funkční bezpečnost - Část 1: Metodika určení bezpečnostních částí ovládacího systému a požadavky na provedení

ISO 19014-2 zavedena v ČSN EN ISO 19014-2 (27 8017) Strojní zařízení pro zemní práce - Funkční bezpečnost - Část 2: Návrh a hodnocení požadavků na hardware a architekturu bezpečnostních částí ovládacího systému

Souvisící ČSN

ČSN EN ISO 6165 (27 7400) Strojní zařízení pro zemní práce - Základní typy - Identifikace a slovník

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v člancích „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).

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 19014-4

Srpen 2020

ICS 53.100

Strojní zařízení pro zemní práce - Funkční bezpečnost -
Část 4: Návrh a hodnocení softwaru a přenosu dat
pro bezpečnostní části ovládacího systému
(ISO 19014-4:2020)

Earth-moving machinery - Functional safety -
Part 4: Design and evaluation of software and data transmission
for safety-related parts of the control system
(ISO 19014-4:2020)

Engins de terrassement - Sécurité
fonctionnelle -
Partie 4: Conception et évaluation du logiciel
et de la transmission des données pour les
parties relatives à la sécurité du système de
commande
(ISO 19014-4:2020)

Erdbaumaschinen - Funktionale Sicherheit -
Teil 4: Gestaltung und Beurteilung von Software
und Datenübertragung für sicherheitsrelevante
Steuerungssysteme
(ISO 19014-4:2020)

Tato evropská norma byla schválena CEN dne 2020-06-29.

Členové CEN 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 biblio-

grafické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoli člena CEN.

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

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Maltu, 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

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Řídicí centrum CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

© 2020 CEN Veškerá práva pro využití v jakékoliv formě a jakýmikoliv prostředky

Ref. č. EN ISO 19014-4:2020 E

jsou celosvětově vyhrazena národním členům CEN.

Evropská předmluva.....	5
Předmluva.....	6
Úvod.....	7
1..... Předmět normy.....	8
2..... Citované dokumenty.....	8
3..... Termíny a definice.....	8
4..... Vývoj softwaru.....	11
4.1..... Obecně.....	11
4.2..... Plánování.....	11
4.3..... Artefakty.....	12
4.4..... Specifikace požadavků na bezpečnost softwaru.....	13
4.5..... Návrh architektury softwaru.....	14
4.6..... Návrh a kódování softwarového modulu.....	14
4.7..... Výběr jazyka	

a nástroje.....	15
4.8..... Testování softwarových modulů.....	16
4.9..... Integrace a testování softwarového modulu.....	17
4.10.... Validace softwaru.....	18
5..... Parametrizace založená na softwaru.....	18
5.1..... Obecně.....	18
5.2..... Integrita dat.....	19
5.3..... Ověřování parametrizace založené na softwaru.....	19
6..... Ochrana přenosu zprávy související s bezpečností na sběrníkových systémech.....	19
7..... Nezávislost dělením softwaru na oddíly.....	21
7.1..... Obecně.....	21
7.2..... Několik oddílů v samostatné řídicí jednotce.....	21
7.3..... Několik oddílů v rozsahu sítě ECU.....	23
8..... Informace pro používání.....	23
8.1..... Obecně.....	23
8.2..... Návod	

k používání.....	
.....	23
Příloha A (informativní) Popis softwarových technik/opatření.....	24
Příloha B (normativní) Testovací prostředí pro validaci softwaru.....	34
Příloha C (informativní) Výpočet zajištění integrity dat.....	36
Příloha D (informativní) Techniky a opatření pro ochranu přenosu.....	37
Příloha E (informativní) Techniky a opatření pro vnitřní ochranu dat v řídicí jednotce.....	39
Bibliografie.....	
.....	41

Evropská předmluva

Tento dokument (EN ISO 19014-4:2018) vypracovala technická komise ISO/TC 127 *Strojní zařízení pro zemní práce* ve spolupráci s technickou komisí CEN/TC 151 *Stavební stroje a stroje na stavební materiály – Bezpečnost*, jejíž sekretariát zajišťuje DIN.

Této evropské normě je nutné nejpozději do února 2021 udělit status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do února 2021.

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

Podle vnitřních předpisů CEN-CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: 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.

Oznámení o schválení

Text ISO 19014-4:2020 byl schválen CEN jako EN ISO 19014-4:2020 bez jakýchkoliv modifikací.

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržných ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html.

Tento dokument připravila technická komise ISO/TC 127 *Strojní zařízení pro zemní práce, subkomise SC 2 Bezpečnost, ergonomie a obecné požadavky* ve spolupráci s Evropským výborem pro normalizaci (CEN) technické komise CEN/TC 151 *Stavební stroje a stroje na stavební materiály - Bezpečnost*, v souladu s Dohodou o technické spolupráci mezi ISO a CEN (Vídeňská dohoda).

Toto první vydání ISO 19014-4, společně s ostatními částmi souboru ISO 19014, zrušuje a nahrazuje ISO 15998:2008 a ISO/TS 15998-2:2012, které byly technicky zrevidovány.

Hlavní změny v porovnání s předchozími dokumenty jsou následující:

- další požadavky pro vývoj softwaru,
- požadavky pro vývoj parametrizace založené na softwaru,
- požadavky pro přenos bezpečnostních zpráv na komunikační sběrnici a
- požadavky pro validaci softwaru a ověřování úrovně vlastností stroje.

Seznam všech částí souboru ISO 19014 lze nalézt na webových stránkách ISO.

Jakákoliv zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

Tento dokument se zabývá systémy zahrnujícími kombinaci elektrických, elektronických a programovatelných elektronických součástí (elektrické/elektronické/programovatelné elektronické systémy (electrical/electronic/programmable electronic systems; E/E/PES)) používaných pro funkční bezpečnost u strojních zařízení pro zemní práce.

Struktura bezpečnostních norem pro strojní zařízení je následující.

Normy typu A (základní bezpečnostní normy) uvádějí základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být použita u strojního zařízení.

Normy typu B (skupinové bezpečnostní normy) zabývající se jedním nebo více bezpečnostními hledisky nebo jedním nebo více typy bezpečnostních zařízení, které mohou být použity pro větší počet strojních zařízení:

- normy typu B1 se týkají jednotlivých bezpečnostních hledisek (např. bezpečných vzdáleností, teploty povrchu, hluku);
- normy typu B2 se týkají bezpečnostních zařízení (např. dvouručních ovládacích zařízení, blokovacích zařízení, zařízení citlivých na tlak, ochranných krytů).

Normy typu C (bezpečnostní normy pro strojní zařízení) se zabývají detailními bezpečnostními požadavky pro jednotlivý stroj nebo skupinu strojů.

Tento dokument je normou typu C, jak je stanoveno v ISO 12100.

Tento dokument je důležitý zejména pro následující skupiny investorů představující hráče na trhu s ohledem na bezpečnost strojních zařízení:

- výrobci strojů (malé, střední a velké podniky);
- zdravotnické a bezpečnostní orgány (řídící orgány, organizace pro prevenci úrazů, dozor nad trhem atd.).

I další mohou být ovlivněni úrovní bezpečnosti strojního zařízení dosaženou prostředky dokumentu pro výše uvedené skupiny investorů:

- uživatelé strojů/zaměstnavatelé (malé, střední a velké podniky);
- uživatelé strojů/zaměstnanci (např. odbory, organizace pro osoby se zvláštními potřebami);
- poskytovatelé servisu, např. pro údržbu (malé, střední a velké podniky).

Výše uvedené skupiny investorů měly možnost spolupracovat na návrhu tohoto dokumentu.

Dotčené strojní zařízení a rozsah, v němž jsou zahrnuta nebezpečí, nebezpečné situace nebo nebezpečné události, jsou uvedeny v předmětu tohoto dokumentu.

Pokud se požadavky této normy typu C liší od požadavků uvedených v normách typu A nebo typu B, mají požadavky této normy typu C přednost před požadavky jiných norem pro stroje, které byly navrženy a vyrobeny podle požadavků této normy typu C.

1 Předmět normy

Tento dokument specifikuje obecné zásady pro vývoj softwaru a požadavky na přenos signálu bezpečnostních částí ovládacích systémů strojů (safety-related parts machine-control systems; MCS) ve strojních zařízeních pro zemní práce (earth-moving machinery; EMM) a jejich vybavení, jak je uvedeno v ISO 6165. Kromě toho se tento dokument zabývá významnými nebezpečími stanovenými v ISO 12100 souvisejícími se softwarem zabudovaným do ovládacího systému stroje. Významná nebezpečí, která jsou řešena, jsou nesprávné reakce výstupů ovládacího systému stroje na vstupy ovládacího systému stroje.

Kybernetická bezpečnost je mimo rozsah tohoto dokumentu.

POZNÁMKA Pro návod na kybernetickou bezpečnost viz příslušné bezpečnostní normy.

Tento dokument neplatí pro EMM vyrobené před datem jeho vydání.

Konec náhledu - text dále pokračuje v placené verzi ČSN.