

2024

Zemědělské a lesnické strojní zařízení a traktory -
Bezpečnostní části ovládacích systémů -
Část 2: Etapa návrhu

ČSN
EN ISO 25119-2

47 0068

idt ISO 25119-2:2019

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems -
Part 2: Concept phase

Tracteurs et matériels agricoles et forestiers - Parties des systemes de commande relatives a la
sécurité -
Partie 2: Phase de projet

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von
Steuerungen -
Teil 2: Konzeptphase

Tato norma je českou verzí evropské normy EN ISO 25119-2:2023. Překlad byl zajištěn Českou
agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 25119-2:2023. It was translated
by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO 25119-1:2018 zavedena v ČSN EN ISO 25119-1:2024 (47 0068) Zemědělské a lesnické strojní
zařízení a traktory - Bezpečnostní části ovládacích systémů - Část 1: Obecné zásady pro konstrukci
a vývoj

ISO 25119-3:2018 zavedena v ČSN EN ISO 25119-3:2024 (47 0068) Zemědělské a lesnické strojní
zařízení a traktory - Bezpečnostní části ovládacích systémů - Část 3: Sériový vývoj, hardware
a software

ISO 25119-4:2018 zavedena v ČSN EN ISO 25119-4:2024 (47 0068) Zemědělské a lesnické strojní
zařízení a traktory - Bezpečnostní části ovládacích systémů - Část 4: Výroba, provoz, úpravy
a podpůrné procesy

Souvisící ČSN

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

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

ČSN EN IEC 61496-1 (33 2206) Bezpečnost strojních zařízení - Elektrická snímací ochranná zařízení - Část 1: Obecné požadavky a zkoušky

ČSN EN IEC 62061 (33 2208) Bezpečnost strojních zařízení - Funkční bezpečnost řídicích systémů souvisejících s bezpečností

ČSN EN ISO 13849-1:2023 (83 3205) Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Obecné zásady pro konstrukci

ČSN EN ISO 13849-2:2013 (83 3205) Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 2: Ověřování platnosti

ČSN EN 61508-6 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3

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 25119-2

Září 2023

ICS 35.240.99;
65.060.01

Zemědělské a lesnické strojní zařízení a traktory - Bezpečnostní části ovládacích systémů - Část 2: Etapa návrhu (ISO 25119-2:2019)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2: Concept phase (ISO 25119-2:2019)

Tracteurs et matériels agricoles et forestiers - Traktoren und Maschinen für die Land-Parties des systèmes de commande relatives a la und Forstwirtschaft - Sicherheitsbezogene Teile sécurité - von Steuerungen -
Partie 2: Phase de projet Teil 2: Konzeptphase
(ISO 25119-2:2019) (ISO 25119-2:2019)

Tato evropská norma byla schválena CEN dne 2023-01-09.

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 bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoliv 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, Malty, Německa,

Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédsko, 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

© 2023 CEN Veškerá práva pro využití v jakékoliv formě a jakýmikoliv prostředky

Ref. č. EN ISO 25119-2:2023 E

jsou celosvětově vyhrazena národním členům CEN.

Evropská předmluva.....	6
.....	
Předmluva.....	7
.....	
Úvod.....	9
.....	
1..... Předmět normy.....	10
.....	
2..... Citované dokumenty.....	10
.....	
3..... Termíny a definice.....	11
.....	
4..... Zkratky termínů.....	11
.....	
5..... Návrh - UoO.....	12
.....	
5.1..... Cíle.....	12
.....	
5.2..... Předpoklady.....	12
.....	
5.3..... Požadavky.....	12
.....	
5.3.1... Základní požadavky a podmínky prostředí.....	12
5.3.2... Omezení UoO a její rozhraní s jinou UoO.....	12
5.3.3... Mapování a přidělování odpovídajících funkcí ovlivňujících UoO, zdroje	

napětí.....	12
5.3.4... Další určení.....	12
5.4..... Výstupy práce.....	13
6..... HARA - Určení AgPL _r	13
6.1..... Cíle.....	13
6.2..... Předpoklady.....	13
6.3..... Požadavky.....	13
6.3.1... Postupy přípravy HARA.....	13
6.3.2... Úkoly HARA.....	13
6.3.3... Účastníci HARA.....	13
6.3.4... Klasifikace potenciálního úrazu.....	13
6.3.5... Klasifikace vystavení ve sledované situaci.....	14
6.3.6... Klasifikace možného zabránění úrazu.....	14
6.3.7... Výběr AgPL _r	15
6.4..... Výstupy práce.....	

.....	16
7..... Návrh funkční bezpečnosti.....	16
7.1..... Cíle.....	16
7.2..... Předpoklady.....	16
7.3..... Požadavky.....	16
7.3.1... Bezpečnostní cíle.....	16
7.3.2... Požadavky na funkční bezpečnost.....	16
7.3.3... Hodnota MTTF_D.....	16
7.3.4... Hodnota DC.....	17
7.3.5... Výběr kategorií, MTTF_{DC}, DC a SRL.....	17
7.3.6... Dosažení AgPL_r.....	18
7.3.7... Kompatibilita s jinými normami na funkční bezpečnost.....	19
7.3.8... Spojování E/E/PES.....	19
7.3.9... Alternativní kombinace SRP/CS k dosažení celkové AgPL.....	19
7.4..... Výstupy práce.....	

Příloha A (normativní) Navrhované architektury pro SRP/CS.....	20
Příloha B (informativní) Zjednodušená metoda odhadu $MTTF_{DC}$ kanálu.....	26
Příloha C (informativní) Určení diagnostického pokrytí (DC).....	29
Příloha D (informativní) Odhad poruchy se společnou příčinou (CCF).....	34
Příloha E (informativní) Systematická porucha.....	35
Příloha F (informativní) Vlastnosti funkcí souvisejících s bezpečností, které jsou základní pro snížení rizika.....	37
Příloha G (informativní) Příklad analýzy rizika.....	39
Příloha H (normativní) Kompatibilita s jinými normami na funkční bezpečnost.....	43
Příloha I (informativní) Alternativní metoda posouzení spojených systémů.....	45
Příloha J (normativní) Alternativní kombinace SRP/CS k dosažení celkové AgPL.....	46
Příloha ZA (informativní) Vztah mezi touto evropskou normou a základními požadavky směrnice 2006/42/ES, které mají být pokryty.....	50
Bibliografie.....	52

Evropská předmluva

Text ISO 25119-2:2019 vypracovala technická komise ISO/TC 23 *Zemědělské a lesnické strojní zařízení a traktory* Mezinárodní komise pro normalizaci (ISO) a byla přijata technickou komisí CEN/TC 144 *Zemědělské a lesnické strojní zařízení a traktory*, jejíž sekretariát zajišťuje AFNOR.

Této evropské normě je nutné nejpozději do března 2024 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 března 2024.

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

Tento dokument byl vypracován na základě mandátu uděleného CEN Evropskou komisí a Evropským sdružením volného obchodu (European Free Trade Association; EFTA) a podporuje základní požadavky směrnice (směrníc)/nařízení EU.

Vztah ke směrnici (směrnícím)/nařízení (nařízením) EU je uveden v informativní příloze ZA, která je nedílnou součástí tohoto dokumentu.

Jakákoliv zpětná vazba a otázky k tomuto dokumentu by měly být směřované na národní normalizační orgán. Úplný seznam těchto orgánů je možné najít na webových stránkách CEN.

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, Irsko, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německo, Nizozemska, Norsko, Polsko, Portugalsko, Rakousko, Republiky Severní Makedonie, Rumunsko, Řecko, Slovensko, Slovinsko, Spojeného království, Srbsko, Španělsko, Švédsko, Švýcarsko a Turecko.

Oznámení o schválení

Text ISO 25119-2:2019 byl schválen CEN jako EN ISO 25119-2:2023 bez jakýchkoli 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 23 *Zemědělské a lesnické strojní zařízení a traktory*, subkomise SC 19 *Elektronika zemědělských strojů*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO 25119-2:2018), to představuje malou revizi. Změny v porovnání s předchozím vydáním jsou následující:

- byla provedena malá revize přílohy H, aby se zlepšila srozumitelnost a význam požadavků, které musí koncový uživatel dodržovat, pokud jde o subsystémy, prvky nebo součásti navržené podle ISO 26262.

Seznam všech částí souboru ISO 25119 je k dispozici 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

ISO 25119 (všechny části) stanovují přístup k posuzování, navrhování a ověřování všech činností životního cyklu bezpečnosti bezpečnostních částí obsahujících elektrické a/nebo elektronické a/nebo programovatelné elektronické systémy (E/E/PES) traktorů používaných v zemědělství a lesnictví a samojízdných strojů s vezoucí se obsluhou a nesených, návěsných a přívěsných strojů používaných v zemědělství. Platí také pro mobilní komunální zařízení.

Předpokladem pro použití ISO 25119 (všechny části) je zpracování vhodné identifikace nebezpečí a analýzy rizika (např. ISO 12100) pro celý stroj. Výsledkem je, že E/E/PES je často určeno pro poskytování funkcí souvisejících s bezpečností, které tvoří části bezpečnostních ovládacích systémů (SRP/CS). Mohou sestávat z hardwaru nebo softwaru, mohou být samostatnými nebo integrovanými částmi ovládacího systému a mohou buď vykonávat výhradně funkce související s bezpečností, nebo mohou být částí provozní funkce.

Obecně platí, že projektant (a do jisté míry uživatel) kombinuje návrh a ověřování těchto SRP/CS v rámci posouzení rizika. Cílem je snížit riziko spojené s daným nebezpečím (nebo nebezpečnou situací) za všech podmínek používání stroje. Toho lze dosáhnout použitím různých opatření (s SRP/CS i bez SRP/CS) s konečným výsledkem dosažení bezpečného stavu.

ISO 25119 (všechny části) rozděluje schopnost bezpečnostních částí vykonávat funkci související s bezpečností za předem předvídatelných podmínek do pěti úrovní vlastností. Úroveň vlastností ovládaného kanálu závisí na několika faktorech, jako je struktura systému (kategorie), rozsah mechanismů detekce poruch (diagnostické pokrytí), spolehlivost součástí (střední doba do nebezpečné poruchy, porucha se společnou příčinou), návrh postupů, provozní napětí, podmínky prostředí a provozní postupy. Jsou zvažovány tři typy poruch, které mohou způsobit selhání E/E/PES vedoucí k potenciálním nebezpečným situacím: systematická, se společnou příčinou a náhodná.

S cílem vést projektanta při navrhování, ověřování a usnadňovat posuzování dosažené úrovně vlastností stanovují ISO 25119 (všechny části) přístup založený na klasifikaci architektury s různými konstrukčními charakteristikami a specifickým chováním v případě poruchového stavu.

Úrovně vlastností a kategorie lze použít na ovládací systémy všech druhů mobilních strojů: od jednoduchých systémů (např. přepouštěcích ventilů) po složité systémy (např. řízení kabelem), jakož i na ovládací systémy ochranných zařízení (např. blokovací zařízení, zařízení citlivá na tlak).

ISO 25119 (všechny části) přijímají přístup ke stanovení rizika na základě stanovení rizik a zároveň poskytují prostředky ke stanovení požadované úrovně vlastností pro funkce související s bezpečností, které mají být implementovány bezpečnostními kanály E/E/PES. Stanoví požadavky na celý životní cyklus bezpečnosti E/E/PES (návrh, ověřování, výrobu, provoz, údržbu, vyřazení z provozu), které jsou nezbytné pro dosažení požadované funkční bezpečnosti pro E/E/PES, které jsou spojeny s úrovněmi vlastností.

Struktura bezpečnostních norem pro strojní zařízení je následující.

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

b) 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).

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

Tento dokument je normou typu B1, 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);
- spotřebitelé (v případě strojního zařízení určeného spotřebitelům).

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

Kromě toho je tento dokument určen pro normalizační orgány tvořící normy typu C.

požadavky tohoto dokumentu mohou být doplněny nebo modifikovány normou typu C.

Pro stroje, které jsou pokryty předmětem normy typu C a které jsou navrženy a vyrobeny podle požadavků takové normy, mají požadavky normy typu C přednost.

1 Předmět normy

Tento dokument specifikuje etapu návrhu vývoje bezpečnostních částí ovládacích systémů (SRP/CS) traktorů používaných v zemědělství a lesnictví a samojízdných strojů s vezoucí se obsluhou a nesených, návěsných a přívěsných strojů používaných v zemědělství. Platí také pro mobilní komunální zařízení (např. zametací stroje).

Tento dokument neplatí pro:

- letadla a vznášedla používaná v zemědělství;
- žací a zahradní vybavení.

Tento dokument specifikuje vlastnosti a kategorie požadované pro SRP/CS pro provádění jejich funkcí souvisejících s bezpečností. Neidentifikuje úrovně vlastností pro konkrétní použití.

POZNÁMKA 1 Normy typu C specifické pro stroj mohou specifikovat úrovně vlastností (AgPL) pro funkce souvisejí s bezpečností u strojů v rámci jejich předmětu. V opačném případě je specifikace AgPL odpovědností výrobce.

Tento dokument platí pro bezpečnostní části elektrických/elektronických/programovatelných elektronických systémů (E/E/PES), protože souvisí s mechatronickými systémy. Pokrývá možná nebezpečí způsobená nesprávným fungováním bezpečnostních systémů E/E/PES, včetně vzájemného působení těchto systémů. Nezabývá se nebezpečími souvisejícími s elektrickým proudem, ohněm, kouřem, teplem, zářením, toxicitou, hořlavostí, reaktivitou, korozi, uvolněním energie a podobnými nebezpečími, pokud nejsou přímo způsobena nesprávným fungováním bezpečnostních systémů E/E/PES. Pokrývá také nesprávné fungování bezpečnostních systémů E/E/PES zapojených do ochranných opatření, bezpečnostních ochran nebo funkcí souvisejících s bezpečností v reakci na nebezpečí, která nejsou součástí E/E/PES.

Příklady zahrnuté do předmětu tohoto dokumentu:

- SRP/CS omezující elektrický proud v elektrických hybridech, aby se předešlo nebezpečím poruchy izolace/úrazu elektrickým proudem;
- elektromagnetické rušení s SRP/CS;
- SRP/CS určené k zabránění požáru.

Příklady nezahrnuté do předmětu tohoto dokumentu:

- porucha izolace kvůli tření, která vede k nebezpečím úrazu elektrickým proudem;
- jmenovité elektromagnetické záření ovlivňující blízké ovládací systémy stroje;
- koroze způsobující přehřátí elektrických kabelů.

Tento dokument neplatí pro jiné systémy než E/E/PES (např. hydraulické, mechanické nebo pneumatické).

POZNÁMKA 2 Viz také ISO 12100 pro zásady navrhování týkající se bezpečnosti strojního zařízení.

Tento dokument neplatí pro bezpečnostní části ovládacích systémů vyrobené před datem tohoto vydání.

Konec náhledu - text dále pokračuje v placené verzi ČSN.