ČESKÁ TECHNICKÁ NORMA

ICS 35.240.99; 65.060.01 **Červenec 2021**

Zemědělské a lesnické stroje a traktory – Bezpečnostní části ovládacích systémů – Část 3: Sériový vývoj, hardware a software

ČSN ISO 25119-3

47 0068

Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 3: Series development, hardware and software

Tracteurs et matériels agricoles et forestiers – Parties des systemes de commande relatives a la sécurité – Partie 3: Développement en série, matériels et logiciels

Tato norma je českou verzí mezinárodní normy ISO 25119-3:2018. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 25119-3:2018. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 25119-3 (47 0068) ze září 2019.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně přejímané normy i způsobu převzetí. ČSN EN ISO 25119-3 z října 2019 převzala EN ISO 25119-3:2018 (která převzala ISO 25119-3:2018) schválením k přímému používání jako ČSN oznámením ve Věstníku ÚNMZ. Tato norma přejímá překladem pouze ISO 25119-3:2018, protože rozhodnutím Technického výboru CEN byla EN ISO 25119-3:2018 zrušena.

Informace o citovaných dokumentech

ISO 25119-1 zavedena v ČSN ISO 25119-1 (47 0068) Zemědělské a lesnické stroje a traktory – Bezpečnostní části ovládacích systémů – Část 1: Obecné zásady pro konstrukci a vývoj

ISO 25119-2:2018 nezavedena

ISO 25119-4:2018 zavedena v ČSN ISO 25119-4:2021 (47 0068) Zemědělské a lesnické stroje

a traktory – Bezpečnostní části ovládacích systémů – Část 4: Výroba, provoz, úpravy a podpůrné procesy

Souvisící ČSN

ČSN EN ISO 9001 Systémy managementu kvality – Požadavky

ČSN EN ISO 12100 Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižo-
vání rizika

ČSN EN 61496-1 Bezpečnost strojních zařízení – Elektrická snímací ochranná zařízení – Část 1: Obecné poža-
davky a zkoušky

Vypracování normy

Zpracovatel: CTN, Státní zkušebna strojů a.s., Praha 6, IČO 27146235, Ing. Miloslav Vomočil

Pracovník České agentury pro standardizaci: Ing. Ludmila Fuxová

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.

MEZINÁRODNÍ NORMA

Zemědělské a lesnické stroje a traktory – Bezpečnostní části ovládacích systémů – Část 3: Sériový vývoj, hardware a software

ISO 25119-3
Druhé vydání
2018-10

ICS 35.240.99; 65.060.01

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
Fax: + 41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org
Publikováno ve Švýcarsku

Obsah

Strana

Předmluva..... 6

Úvod..... 7

1..... Předmět normy..... 9

2..... Citované dokumenty..... 9

3..... Termíny a definice..... 10

4..... Zkratky termínů..... 10

5..... Návrh systému..... 11

5.1.....

Cíle..... 11

5.2.....
Obecně..... 11

5.3.....
Předpoklady..... 11

5.4.....
Požadavky..... 12

5.4.1... Bezpečnostní požadavky na
strukturu..... 12

5.4.2... Návrh technické
bezpečnosti..... 12

5.5..... Výstupy
práce..... 13

6.....
Hardware..... 13

6.1.....
Cíle..... 13

6.2.....
Obecně..... 13

6.3.....
Předpoklady..... 14

6.4.....
Požadavky..... 14

6.5..... Kategorie
hardwaru..... 15

6.6..... Výstupy
práce..... 15

7.....
Software.....
..... 16

7.1..... Plánování vývoje
softwaru.....
..... 16

7.1.1...
Cíle.....
..... 16

7.1.2...
Obecně.....
..... 16

7.1.3...
Předpoklady.....
..... 16

7.1.4...
Požadavky.....
..... 16

7.1.5... Výstupy
práce.....
..... 18

7.2..... Specifikace požadavků na bezpečnost
softwaru..... 18

7.2.1...
Cíle.....
..... 18

7.2.2...
Obecně.....
..... 18

7.2.3...
Předpoklady.....
..... 18

7.2.4...
Požadavky.....
..... 18

7.2.5... Výstupy
práce.....
..... 21

7.3..... Návrh architektury
softwaru.....

..... 21

7.3.1...
Cíle.....
..... 21

7.3.2...
Obecně.....
..... 21

7.3.3...
Předpoklady.....
..... 21

7.3.4...
Požadavky.....
..... 21

7.3.5... Výstupy
práce.....
..... 23

7.4..... Navrhování a implementace součásti
softwaru..... 23

7.4.1...
Cíle.....
..... 23

7.4.2…
Obecně…… 23

7.4.3…
Předpoklady…… 23

7.4.4…
Požadavky…… 23

7.4.5… Výstupy
práce…… 31

7.5…… Testování softwarové
součásti…… 31

7.5.1…
Cíle…… 31

7.5.2…
Obecně…… 31

7.5.3…
Předpoklady…… 31

7.5.4…
Požadavky…… 31

7.5.5… Výstupy
práce…… 38

7.6…… Integrace a testování
softwaru…… 38

7.6.1…
Cíle…… 38

7.6.2…
Obecně…… 38

7.6.3…
Předpoklady…… 38

7.6.4…
Požadavky…… 38

7.6.5… Výstupy
práce…… 40

7.7…… Testování bezpečnosti
softwaru…… 40

7.7.1…
Cíle…… 40

7.7.2…
Obecně…… 40

7.7.3…
Předpoklady…… 40

7.7.4…
Požadavky…… 40

7.7.5… Výstupy
práce…… 43

7.8…… Softwarová
parametrizace…… 43

7.8.1…
Cíl…… 43

7.8.2…
Obecně…… 43

7.8.3…
Předpoklady…… 43

7.8.4…

Požadavky..... 44

7.8.5... Výstupy
práce..... 44

Příloha A (informativní) Příklad programu pro hodnocení funkční bezpečnosti na AgPL
= e..... 45

Příloha B (normativní) Nezávislost pomocí rozdělení
softwaru..... 47

Bibliografie..... 55

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 směrnicích 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 směrnicích 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 obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená 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 stroje a traktory*, subkomise SC 19 *Elektronika zemědělských strojů*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO 25119-3:2010), které bylo technicky

revidováno. Hlavní změny ve srovnání s předchozím vydáním jsou následující:

- byl změněn úvod přidáním specifických informací o bezpečnostních normách;
- byly stanoveny předpoklady funkční bezpečnosti;
- kapitola 5 byla změněna takto:
  - byly stanoveny předpoklady funkční bezpečnosti a
  - zjednodušily se obecné požadavky na návrhy technické bezpečnosti;
- do dokumentu byly přidány další pokyny k ověření stejnoměrnosti specifikací zkoušek a protokolů;
- příloha B byla změněna na normativní přílohu;
- dokument byl edičně upraven.

Seznam všech částí souboru ISO 25119 je k dispozici na webových stránkách ISO.

Jakákoliv zpětná vazba nebo otázka na tento dokument by měla být směrována na národní normalizační orgán. Úplný seznam těchto orgánů je dostupný na 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 nebo 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 bezpečnostní části 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) rozdělují schopnost bezpečnostních částí vykonávat funkci související s bezpečností za předem předvídatelných podmínek do pěti úrovní provedení. Úroveň provedení 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 provedení stanovují ISO 25119 (všechny části) přístup založený na klasifikaci architektury s různými konstrukčními charakteristikami a specifickým chováním v případě poruchového stavu.

Úrovně provedení 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 rizik na základě stanovení rizika a zároveň poskytují prostředky ke stanovení požadované úrovně provedení 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 provedení.

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 (řídicí 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 obecné zásady pro navrhování a vývoj bezpečnostních částí ovládacích systémů (SRP/CS) traktorů používaných v zemědělství a lesnictví a samojízdných strojů s vezoucí se obsluhou a nesených, návěsných nebo 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 související 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, korozí, 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 systémy jiné 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.