

2024

Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – ČSN
Část 1: Obecné zásady pro konstrukci EN ISO 13849-1
ed. 2
83 3205

idt ISO 13849-1:2023

Safety of machinery – Safety-related parts of control systems –
Part 1: General principles for design

Sécurité des machines – Parties des systemes de commande relatives a la sécurité –
Partie 1: Principes généraux de conception

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze

Tato norma je českou verzí evropské normy EN ISO 13849-1:2023. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 13849-1:2023. 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 13849-1 (83 3205) z října 2023.

S účinností od 2026-05-31 se touto normou nahrazuje ČSN EN ISO 13849-1 (83 3205) z března 2017, která 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 ISO 13849-1:2023 dovoleno do 2026-05-31 používat dosud platnou ČSN EN ISO 13849-1 (83 3205) z března 2017.

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 13849-1:2023 do soustavy norem ČSN.

Zatímco norma z října 2023 převzala EN ISO 13849-1:2023 schválením k přímému používání jako ČSN oznámením ve Věstníku ÚNMZ, tato norma ji přejímá překladem.

Změny proti ČSN EN ISO 13849-1 (83 3205) z března 2017 jsou specifikovány v evropské předmluvě.

Informace o citovaných dokumentech

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 13849-2:2012 zavedena v ČSN EN ISO 13849-2:2013 (83 3205) Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 2: Ověřování platnosti

ISO 13855:2010 zavedena v ČSN EN ISO 13855:2010 (83 3303) Bezpečnost strojních zařízení – Umístění ochranných zařízení s ohledem na rychlosti přiblížení částí lidského těla

ISO 20607:2019 zavedena v ČSN EN ISO 20607:2021 (83 3304) Bezpečnost strojních zařízení – Návod k používání – Obecné principy pro návrh

IEC 61508-3:2010 zavedena v ČSN EN 61508-3 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software

IEC 62046:2018 zavedena v ČSN EN IEC 62046:2019 (33 2207) Bezpečnost strojních zařízení – Použití ochranných zařízení k detekci přítomnosti osob

IEC 62061:2021 zavedena v ČSN EN IEC 62061 ed.2:2022 (33 2208) Bezpečnost strojních zařízení – Funkční bezpečnost řídicích systémů souvisejících s bezpečností

IEC/IEEE 82079-1:2019 zavedena v ČSN EN IEC/IEEE 82079-1 ed.2:2020 (01 3782) Příprava informací pro použití (návodů k použití) produktů – Část 1: Zásady a obecné požadavky

Vysvětlivky k textu převzaté 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 13849-1

Květen 2023

ICS 13.110
13849-1:2015

Nahrazuje EN ISO

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

Safety of machinery – Safety-related parts of control systems –
Part 1: General principles for design
(ISO 13849-1:2023)

Sécurité des machines – Parties des systèmes
de commande relatives à la sécurité –
Partie 1: Principes généraux de conception
(ISO 13849-1:2023)

Sicherheit von Maschinen – Sicherheitsbezogene
Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsgrundsätze
(ISO 13849-1:2023)

Tato evropská norma byla schválena CEN dne 2023-03-03.

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 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, Maltu, Německa,

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



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 jakýmkoliv prostředky

Ref. č. EN ISO 13849-1:2023 E

jsou celosvětově vyhrazena národním členům CEN.

Evropská předmluva

Tento dokument (EN ISO 13849-1:2023) byl vypracován technickou komisí ISO/TC 199 *Bezpečnost strojních zařízení* ve spolupráci s CEN/TC 114 *Bezpečnost strojních zařízení*, jejíž sekretariát zajišťuje DIN.

Této evropské normě je nutno nejpozději do listopadu 2023 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 května 2026.

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.

Tento dokument nahrazuje EN ISO 13849-1:2015.

Tento dokument byl vypracován na základě mandátu uděleného CEN Evropskou komisí a Evropským sdružením volného obchodu a podporuje splnění základních požadavků směrnice (směrnic) EU.

Vztah ke směrnici (směrnicím) EU je uveden v informativní příloze ZA, která je nedílnou součástí tohoto dokumentu.

Jakákoliv zpětná vazba nebo otázky k tomuto dokumentu by měly být směřovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze 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, 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 13849-1:2023 byl schválen CEN jako EN ISO 13849-1:2023 bez jakýchkoliv modifikací.

Evropská předmluva.....	4
Úvod.....	9
1..... Předmět normy.....	12
2..... Citované dokumenty.....	12
3..... Termíny, definice, značky a zkratky termínů.....	13
3.1..... Termíny a definice.....	13
3.2..... Značky a zkratky termínů.....	21
4..... Přehled.....	22
4.1..... Posouzení rizika a proces snižování rizika u stroje.....	22
4.2..... Příspěvek ke snížení rizika..... ..	24
4.3..... Proces návrhu SRP/CS.....	25
4.4..... Metodologie.....	26
4.5..... Požadované informace.....	26

4.6..... Realizace bezpečnostní funkce pomocí subsystémů.....	27
5..... Specifikace bezpečnostních funkcí.....	27
5.1..... Identifikace a obecný popis bezpečnostní funkce.....	27
5.2..... Specifikace bezpečnostních požadavků.....	28
5.2.1... Obecné požadavky.....	28
5.2.2... Požadavky pro specifické bezpečnostní funkce.....	30
5.2.3... Minimalizace motivace k překonání bezpečnostních funkcí.....	33
5.2.4... Vzdálený přístup.....	33
5.3..... Stanovení požadované úrovně vlastností (PL _r) pro každou bezpečnostní funkci.....	33
5.4..... Rvize specifikace požadavků na bezpečnost (SRS).....	33
5.5..... Rozklad SRP/CS na subsystémy.....	34
6..... Úvahy o konstrukci.....	35
6.1..... Vyhodnocení dosažení úrovně vlastností.....	35
6.1.1... Obecný přehled úrovně vlastností.....	35
6.1.2... Korelace mezi úrovní vlastnosti (PL) a úrovní integrity bezpečnosti (SIL).....	36
6.1.3... Architektura – Kategorie a jejich vztah k MTTF _D každého kanálu, průměrné diagnostické pokrytí a porucha se společnou příčinou	

(CCF).....	37
6.1.4... Střední doba do nebezpečné poruchy (MTTF _D).....	44
6.1.5... Diagnostické pokrytí (DC)..... ... 45	
6.1.6... Poruchy se společnou příčinou (CCF).....	45
6.1.7... Systematické poruchy..... 45	
6.1.8... Zjednodušený postup pro odhad úrovně vlastností pro subsystémy.....	46
6.1.9... Alternativní postup pro stanovení úrovně vlastností a PFH bez MTTF _D	47
6.1.10 Uvážení a vyloučení poruchového stavu.....	48
6.1.11 Osvědčená součást..... 49	
6.2..... Kombinace subsystémů pro dosažení celkové úrovně vlastností bezpečnostní funkce.....	50
6.2.1... Obecně..... 50	
6.2.2... Známé hodnoty PFH..... 50	
6.2.3... Neznámé hodnoty PFH..... 50	

6.3..... Ruční parametrizace založená na softwaru.....	51
6.3.1... Obecně.....	51
6.3.2... Vlivy na bezpečnostní parametry.....	51
6.3.3... Požadavky na ruční parametrizaci založenou na softwaru.....	52
6.3.4... Ověření parametrizačního nástroje.....	53
6.3.5... Dokumentace ruční parametrizace založené na softwaru.....	53
7..... Požadavky na bezpečnost softwaru.....	53
7.1..... Obecně.....	53
7.2..... Jazyk s omezenou variabilitou (LVL) a programovací jazyk s plnou variabilitou (FVL).....	55
7.2.1... Jazyk s omezenou variabilitou (LVL).....	55
7.2.2... Programovací jazyk s plnou variabilitou (FVL).....	55
7.2.3... Rozhodnutí pro jazyk s omezenou variabilitou (LVL) nebo programovací jazyk s plnou variabilitou (FVL).....	55
7.3..... Bezpečnostní vestavěný software (SRESW).....	57
7.3.1... Návrh bezpečnostního vestavěného softwaru (SRESW).....	57
7.3.2... Alternativní postupy pro nepřístupný vestavěný software.....	58
7.4..... Bezpečnostní aplikační software (SRASW).....	58

8.....	Ověřování dosažené úrovně vlastností.....	60
9.....	Ergonomické aspekty návrhu.....	60
10.....	Validace.....	60
10.1....	Zásady validace.....	60
10.1.1	Obecně.....	60
10.1.2	Plán validace.....	62
10.1.3	Obecné seznamy poruchových stavů.....	63
10.1.4	Specifické seznamy poruchových stavů.....	63
10.1.5	Informace pro validaci.....	63
10.2....	Validace specifikace požadavků na bezpečnost (SRS).....	64
10.3....	Validace analýzou.....	64
10.3.1	Obecně.....	64
10.3.2	Techniky analýzy.....	65
10.4....	Validace zkoušením.....	65
10.4.1		

Obecně.....	65
10.4.2 Přesnost měření.....	65
10.4.3 Další požadavky na zkoušení.....	66
10.4.4 Počet zkušebních vzorků.....	66
10.4.5 Zkušební metody.....	66
10.5.... Validace bezpečnostních funkcí.....	67
10.6.... Validace bezpečnostní integrity SRP/CS.....	67
10.6.1 Validace subsystému (subsystémů).....	67
10.6.2 Validace opatření proti systematickým poruchám.....	68
10.6.3 Validace bezpečnostního softwaru.....	68
10.6.4 Validace kombinace subsystémů.....	69
10.6.5 Celková validace integrity bezpečnosti.....	69
10.7.... Validace požadavků na prostředí.....	69

10.8.... Záznam o validaci.....	70
10.9.... Validace požadavků na údržbu.....	70
11..... Udržitelnost SRP/CS.....	70
12..... Technická dokumentace.....	71
13..... Informace pro použití.....	71
13.1.... Obecně.....	71
13.2.... Informace pro integraci SRP/CS.....	71
13.3.... Informace pro uživatele.....	72
Příloha A (informativní) Pokyny pro stanovení požadované úrovně vlastností (PL _r).....	73
Příloha B (informativní) Bloková metoda a bezpečnostní blokové schéma.....	77
Příloha C (informativní) Výpočet nebo vyhodnocení MTTF_D hodnot pro jednotlivé součásti.....	79
Příloha D (informativní) Zjednodušená metoda odhadování MTTF_D pro každý kanál.....	85
Příloha E (informativní) Odhady pro diagnostické pokrytí (DC) pro funkce a subsystémy.....	87
Příloha F (informativní) Metoda kvantifikace opatření proti poruchám se společnou příčinou (CCF).....	90
Příloha G (informativní) Systematická	

porucha.....	93
Příloha H (informativní) Příklad kombinace několika subsystémů.....	96
Příloha I (informativní) Příklady pro zjednodušený postup odhadu PL subsystémů.....	99
Příloha J (informativní) Příklad realizace SRESW.....	107
Příloha K (informativní) Číselné vyjádření obrázku 12.....	110
Příloha L (informativní) Odolnost proti elektromagnetickému rušení (EMI).....	113
Příloha M (informativní) Další informace ke specifikaci bezpečnostních požadavků (SRS).....	116
Příloha N (informativní) Předcházení systematickým poruchám při návrhu softwaru.....	118
Příloha O (informativní) Hodnoty bezpečnostních součástí nebo částí ovládacích systémů.....	135
Příloha ZA (informativní) Vztah mezi touto Evropskou normou a základními požadavky směrnice 2006/42/ES, které mají být pokryty.....	137
Bibliografie.....	139

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 obdržených 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 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), jsou uvedeny na tomto odkazu URL: www.iso.org/iso/foreword.html.

Tento dokument byl připraven technickou komisí ISO/TC 199, *Bezpečnost strojních zařízení*, ve spolupráci s technickou komisí Evropského výboru pro normalizaci (CEN) CEN/TC 114 *Bezpečnost strojních zařízení* v souladu s Dohodou o technické spolupráci mezi ISO a CEN (Vídeňská dohoda).

Toto čtvrté vydání zrušuje a nahrazuje třetí vydání (ISO 13849-1:2015), které bylo technicky revidováno.

Hlavní změny jsou následující:

- celý dokument byl reorganizován tak, aby lépe sledoval proces návrhu a vývoje ovládacích systémů;
- nová kapitola 4 o doporučení pro posuzování rizika;
- specifikace bezpečnostních funkcí (aktualizovaná kapitola 5);
- kombinace několika subsystémů (aktualizováno v kapitole 6);
- nová kapitola 7 o požadavcích na bezpečnost softwaru;
- nová kapitola 9 o hlediscích návrhu;
- validace (aktualizovaná kapitola 8 a přesunuto do kapitoly 10);

- nový článek G.5 o managementu funkční bezpečnosti;
- nová příloha L o odolnosti proti elektromagnetickému rušení (EMI);
- nová příloha M s dalšími informacemi ke specifikaci bezpečnostních požadavků (SRS);
- nová příloha N o předcházení systematickým poruchám při návrhu softwaru;
- nová příloha O s hodnotami bezpečnostních součástí nebo částí ovládacích systémů.

Seznam všech částí souboru ISO 13849 lze nalézt na webových stránkách ISO.

Jakákoliv zpětná vazba nebo otázky k tomuto dokumentu by měly být směřovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze najít na www.iso.org/members.html.

Úvod

Struktura bezpečnostních norem v oblasti strojních zařízení je následující:

- a) Normy typu A (základní normy) uvádějí základní pojmy, zásady pro návrh a všeobecné aspekty, které mohou být aplikovány na strojní zařízení.
- b) Normy typu B (obecné bezpečnostní normy) se zabývají jedním nebo více bezpečnostními aspekty nebo jedním nebo více typy ochranných zařízení, která lze použít v širším rozsahu strojních zařízení:
 - normy typu B1 se týkají jednotlivých bezpečnostních aspektů (např. bezpečných vzdáleností, teploty povrchu, hluku);
 - normy typu B2 se týkají ochranných zařízení (např. dvouručního ovládání, blokovacích zařízení, zařízení citlivých na tlak, ochranných krytů).
- c) Normy typu C (bezpečnostní normy pro strojní zařízení) určují detailní bezpečnostní požadavky pro jednotlivý stroj nebo skupinu strojů.

Tento dokument je norma typu B1, jak je stanoveno v ISO 12100:2010.

První vydání tohoto dokumentu bylo vydáno v roce 1999 na základě EN 954-1:1996 (zrušená norma). Druhé vydání bylo revidováno v roce 2006 a třetí vydání bylo revidováno v roce 2015.

Tento dokument je důležitý zejména pro následující zájmové skupiny s ohledem na bezpečnost strojního zařízení:

- výrobce strojů (malé, střední a velké podniky);
- orgány ochrany zdraví a bezpečnosti (regulační organizace, organizace ochrany zdraví, organizace dozorující nad trhem).

Ostatní mohou být ovlivněny úrovní bezpečnosti strojního zařízení dosažené pomocí dokumentu výše uvedených zájmových skupin:

- uživatelé stroje/zaměstnavatelé (malé, střední a velké podniky);
- uživatelé stroje/zaměstnanci (např. obchodní společnosti);
- poskytovatelé služeb, např. údržba (malé, střední a velké podniky);
- spotřebitelé (tj. strojního zařízení určeného pro použití spotřebiteli).

Výše uvedeným zájmovým skupinám byla dána možnost podílet se na přípravě tohoto dokumentu.

Kromě toho je tento dokument určen pro normalizační orgány zpracovávající normy typu C, jak jsou stanoveny v ISO 12100:2010.

Požadavky tohoto dokumentu mohou být doplněny nebo upraveny normou typu C.

U strojů, které spadají do rozsahu předmětu normy typu C a které byly navrženy a vyrobeny v souladu s požadavky této normy, mají požadavky této normy typu C přednost.

POZNÁMKA 1 Příklady a základ pro většinu obsahu jsou založeny na stacionárních strojích v továrních aplikacích. Vyloučeny však nejsou ani další stroje. Tento dokument byl sepsán bez ohledu na to, zda určitá strojní zařízení (např. mobilní stroje) mají specifické požadavky. Tento dokument je však určen k použití v mnoha strojírenských odvětvích a jako základ pro autory norem typu C, pokud je to možné.

Tento dokument je určen jako návod pro ty, kteří se zabývají návrhem a posuzováním ovládacích systémů a dále pro ty, kteří připravují normy typu B2 nebo typu C.

Snížení rizika podle ISO 12100:2010, kapitola 6 je dosaženo aplikací v následujícím pořadí opatření pro inherentně bezpečný návrh, bezpečnostní ochranu a/nebo doplňková opatření na snížení rizika a informace pro použití. Projektant může snížit rizika opatřeními na snížení rizik, která mohou mít bezpečnostní funkce. Části ovládacích systémů strojního zařízení, které jsou přiřazeny k zajištění bezpečnostních funkcí se nazývají bezpečnostní části ovládacích systémů (SRP/CS). Ty se mohou sestávat z hardwaru nebo z kombinace hardwaru a softwaru a mohou být buď oddělené od ovládacího systému stroje nebo jeho nedílnou součástí. Kromě implementace bezpečnostních funkcí může SRP/CS také implementovat provozní funkce.

Pro posouzení rizik stroje se používá ISO 12100:2010. Přílohu A tohoto dokumentu lze použít pro stanovení požadované úrovně vlastností (PL_r) bezpečnostní funkce vykonávané SRP/CS, kde její PL_r není specifikována v příslušné normě typu C. Tento dokument je relevantní pro SRP/CS bezpečnostních funkcí, které se používají k řešení rizik v případech, kdy posouzení rizika provedené podle ISO 12100:2010 stanoví, že je nutné opatření na snížení rizika, které se opírá o bezpečnostní funkci (např. ochranný kryt s blokováním). V těchto případech plní bezpečnostní ovládací systém bezpečnostní funkci. Tento dokument je určen k použití při návrhu a hodnocení SRP/CS. Do rozsahu předmětu tohoto dokumentu spadá pouze ta část ovládacího systému, která souvisí s bezpečností.

Obrázek 1 zobrazuje vztah mezi ISO 12100:2010 a tímto dokumentem. Podrobný přehled viz obrázek 2.

POZNÁMKA 2 Další informace viz také ISO/TR 22100-2:2013.



POZNÁMKA Podle ISO/TR 22100-2:2013, obrázek 2.

Obrázek 1 – Integrace tohoto dokumentu (ISO 13849-1) do procesu snižování rizika podle ISO 12100:2010

POZNÁMKA 3 Obrázek 1 zobrazuje, kde SRP/CS přispívá k procesu snižování rizika podle ISO 12100:2010: Krok 2. SRP/CS podporuje kombinovaná opatření ke snížení rizik implementací bezpečnostních funkcí. Schopnost bezpečnostních částí ovládacího systému vykonávat bezpečnostní funkci za předvídatelných podmínek je přiřazena jedna z pěti úrovní, nazývaných úrovně vlastností (PL). Požadovaná úroveň vlastností (PL_r) pro konkrétní bezpečnostní funkci (v závislosti na požadovaném snížení rizika) bude stanovena odhadem rizika.

Informativní příloha A tohoto dokumentu obsahuje metodu pro odhad rizika a může být použita pro stanovení PL_r bezpečnostní funkce prováděné pomocí SRP/CS. Jakákoli metoda odhadu rizik bude vykazovat odchylky kvůli subjektivní povaze hodnotících kritérií. Ve srovnání s přílohou A mohou mít normy typu C přesnější metody odhadu rizik pro specifické aplikace strojů.

Pravděpodobnost nebezpečné poruchy bezpečnostní funkce závisí na několika faktorech, včetně struktury hardwaru a softwaru, rozsahu mechanismů detekce poruchového stavu [diagnostické pokrytí (DC)], spolehlivosti komponentů [střední doba do nebezpečné poruchy ($MTTF_D$)], poruchy se společnou příčinou (CCF)], procesu návrhu, provozního zatížení, podmínek prostředí a pracovních procesech.

Za účelem usnadnění návrhu SRP/CS a hodnocení dosažených PL, používá tento dokument metodologii založenou na kategorizaci architektur se specifickými kritérii návrhu (např. $MTTF_D$, DC_{avg}) a specifikovaným chováním za podmínek poruchového stavu. Tyto architektury mají přidělenou jednu z pěti úrovní označovaných jako kategorie B, 1, 2, 3 a 4.

Funkční bezpečnost zohledňuje poruchové charakteristiky prvků/komponentů vykovávajících bezpečnostní funkci. Pro každou bezpečnostní funkci je tato poruchová charakteristika vyjádřena jako četnost nebezpečné poruchy za hodinu (PFH).

Úrovně vlastností a kategorie se mohou vztahovat na SRP/CS, např.:

- ovládací jednotky (např. logická jednotka pro ovládací funkce, zpracování dat, monitorování);
- elektrická snímací ochranná zařízení (např. fotoelektrické clony), zařízení citlivá na tlak.

Pro subsystémy SRP/CS používající bezpečnostní části (komponenty) lze stanovit úrovně vlastností a stanovit kategorie, např.:

- ochranná zařízení (např. dvouruční ovládací zařízení, blokovací zařízení);
- prvky silového ovládání (např. relé, ventily);
- senzory a prvky HMI (např. senzory polohy, souhlasné povelové spínače).

Strojní zařízení, na která se vztahuje tento dokument, se mohou pohybovat v rozsahu od jednoduchých (např. malé kuchyňské stroje, nebo automatické dveře a brány) až po složité (např. balicí stroje, tiskařské stroje, lisy a stroje integrované do systému).

Tento dokument a IEC 62061 specifikují metodologii a poskytují související návod pro návrh a implementaci bezpečnostních ovládacích systémů strojního zařízení.

Požadavky kapitoly 10 tohoto dokumentu nahrazují požadavky ISO 13849-2:2012 (s výjimkou informativních příloh).

1 Předmět normy

Tento dokument specifikuje metodiku a poskytuje související požadavky, doporučení a návod pro návrh a integraci bezpečnostních částí ovládacích systémů (SRP/CS), které provádějí bezpečnostní funkce, včetně návrhu softwaru.

Tento dokument platí pro SRP/CS pro režim s vysokým nebo trvalým vyžádáním včetně jejich subsystémů, bez ohledu na typ technologie a energie (např. elektrické, hydraulické, pneumatické a mechanické). Tento dokument se nevztahuje na režim s nízkým vyžádáním.

POZNÁMKA 1 Pro režim s nízkým vyžádáním viz 3.1.44 a soubor IEC 61508.

Tento dokument nespecifikuje bezpečnostní funkce nebo požadované úrovně bezpečnosti (PL_r), které mají být použity v konkrétních aplikacích.

POZNÁMKA 2 Tento dokument specifikuje metodiku návrhu SRP/CS bez ohledu na to, zda určité strojní zařízení (např. mobilní stroje) má specifické požadavky. Tyto specifické požadavky lze vzít v úvahu v normě typu C.

Tento dokument neposkytuje specifické požadavky pro návrh produktů/komponentů, které jsou částí SRP/CS. Specifické požadavky pro návrh některých komponentů SRP/CS jsou pokryty platnými normami ISO a IEC.

Tento dokument neposkytuje specifická opatření pro bezpečnostní aspekty (např. fyzická bezpečnost, IT bezpečnost, kybernetická bezpečnost).

POZNÁMKA 3 Bezpečnostní problémy mohou mít vliv na bezpečnostní funkce. Další informace viz ISO/TR 22100-4 a IEC/TR 63074.

Konec náhledu - text dále pokračuje v placené verzi ČSN.