

2017

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

83 3205

idt ISO 13849-1:2015

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 13849-1:2015. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 13849-1:2015. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazují ČSN EN ISO 13849-1 (83 3205) z července 2016 a ČSN CR 954-100 (83 3205) z února 2000.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 13849-1:2015 do soustavy norem ČSN. Zatímco norma z července 2016 převzala EN ISO 13849-1:2015 schválením k přímému používání jako ČSN, tato norma ji přejímá překladem.

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 (83 3205) Bezpečnost strojních zařízení –

Bezpečnostní části ovládacích systémů – Část 2: Ověřování platnosti

IEC 60050-191:1990 zavedena v ČSN IEC 50(191):1993 (01 0102) Mezinárodní elektrotechnický slovník.

Kapitola 191: Spotřeba a kvalita služeb

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

IEC 61508-4:2010 zavedena v ČSN EN 61508-4 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 4: Definice a zkratky

IEC 62061:2012 zavedena v ČSN EN 62061:2005 (33 2208) Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností

ISO/TR 22100-2:2013 nezavedena

ISO/TR 23849 nezavedena

Upozornění na národní poznámky

Do normy byla ke článku 4.5.2 doplněna národní poznámka.

Vypracování normy

Zpracovatel: Svaz strojírenské technologie, IČ 00548871, Ing. Leoš Mačák

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jaroslav Zajíček

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 13849-1

Prosinec 2015

ICS 13.110
13849-1:2008

Nahrazuje EN ISO

Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů –
Část 1: Obecné zásady pro konstrukci
(ISO 13849-1:2015)

Safety of machinery – Safety-related parts of control systems –
Part 1: General principles for design
(ISO 13849-1:2015)

Sécurité des machines – Parties des systèmes
de commande relatives à la sécurité –
Partie 1: Principes généraux de conception
(ISO 13849-1:2015)

Sicherheit von Maschinen – Sicherheitsbezogene
Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsgrundsätze
(ISO 13849-1:2015)

Tato evropská norma byla schválena CEN dne 2015-06-20.

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, Bývalé jugoslávské republiky Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Maltu, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, 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: Avenue Marnix 17, B-1000 Brusel

© 2015 CEN Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky

Ref.

č. EN ISO 13849-1:2015 E

jsou celosvětově vyhrazena národním členům CEN.

Evropská předmluva

Tento dokument (EN ISO 13849-1:2015) vypracovala technická komise ISO/TC 199 „Bezpečnost strojních zařízení“, ve spolupráci s technickou komisí CEN/TC 114 „Bezpečnost strojních zařízení“, jejíž sekretariát zajišťuje DIN.

Této evropské normě je nutné nejpozději do června 2016 dát 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 června 2016.

Upozorňuje se na možnost, že některé prvky tohoto normativního dokumentu mohou být předmětem patentových práv. CEN [a/nebo CENELEC] nesmí být činěn odpovědným za identifikaci některých nebo všech těchto patentových práv.

Tento dokument nahrazuje EN ISO 13849-1:2008.

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

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

Podle vnitřních předpisů CEN/CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Irsko, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německo, Nizozemska, Norsko, Polsko, Portugalsko, Rakousko, Rumunsko, Řecko, Slovensko, Slovinsko, Spojené království, Španělsko, Švédsko, Švýcarsko a Turecko.

Oznámení o schválení

Text ISO 13849-1:2015 byl schválen CEN jako EN ISO 13849-1:2015 bez jakýchkoliv modifikací.

Evropská předmluva.....	4
Předmluva.....	7
Úvod.....	8
1..... Předmět normy.....	10
2..... Citované dokumenty.....	10
3..... Termíny, definice, značky a zkratky termínů.....	11
3.1..... Termíny a definice.....	11
3.2..... Značky a zkrácené termíny.....	16
4..... Konstrukční úvahy.....	17
4.1..... Bezpečnostní cíle v návrhu.....	17
4.2..... Strategie pro snížení rizika.....	19
4.2.1... Obecně.....	19
4.2.2... Příspěvek ke snížení rizika ovládacím systémem.....	19
4.3..... Určení požadované úrovně vlastností	

(PL _r).....	22
4.4..... Návrh	
SRP/CS.....	
.....	22
4.5..... Hodnocení dosažené úrovně vlastností PL a vztahu se	
SIL.....	23
4.5.1... Úroveň vlastností	
PL.....	
.....	23
4.5.2... Střední doba do nebezpečné poruchy každého kanálu	
(MTTF _D).....	24
4.5.3... Diagnostické pokrytí	
(DC).....	
..	25
4.5.4... Zjednodušený postup pro odhad kvantifikovatelných hledisek	
PL.....	25
4.5.5... Popis výstupní části SRP/CS podle	
kategorie.....	27
4.6..... Bezpečnostní požadavky na	
software.....	28
4.6.1...	
Obecně.....	
.....	28
4.6.2... Bezpečnostní vestavěný software	
(SRESW).....	28
4.6.3... Bezpečnostní aplikační software	
(SRASW).....	29
4.6.4... Parametrizace založená na	
software.....	31
4.7..... Ověřování, že dosažená PL splňuje	
PL _r	32
4.8..... Ergonomická hlediska	
návrhu.....	
32	
5..... Bezpečnostní	
funkce.....	
.....	32

5.1..... Specifikace bezpečnostních funkcí.....	32
5.2..... Detaily bezpečnostních funkcí.....	34
5.2.1... Funkce bezpečného zastavení.....	34
5.2.2... Funkce ručního opětného nastavení.....	34
5.2.3... Funkce spuštění/opětného spuštění.....	35
5.2.4... Funkce místního ovládání.....	35
5.2.5... Funkce vyřazení.....	35
5.2.6... Doba reakce.....	35
5.2.7... Bezpečnostní parametry.....	36
5.2.8... Kolísání, ztráta a opětné obnovení zdrojů energie.....	36
6..... Kategorie a jejich vztah k $MTTF_D$ každého kanálu, DC_{avg} a CCF.....	36
6.1..... Obecně.....	36

6.2..... Specifikace kategorií.....	
.....	36
6.2.1... Obecně.....	
.....	36
6.2.2... Označené architektury.....	
.....	37
6.2.3... Kategorie B.....	
.....	37
6.2.4... Kategorie 1.....	
.....	37
6.2.5... Kategorie 2.....	
.....	38
6.2.6... Kategorie 3.....	
.....	40
6.2.7... Kategorie 4.....	
.....	41
6.3..... Kombinace SRP/CS k dosažení celkové PL.....	42
7..... Uvažování závady, vyloučení závady.....	44
7.1..... Obecně.....	
.....	44
7.2..... Uvažování závady.....	
.....	44
7.3..... Vyloučení závady.....	
.....	44
8.....	

Platnost.....	44
9.....	
Údržba.....	44
10..... Technická dokumentace.....	44
11..... Informace pro používání.....	45
Příloha A (informativní) Určení požadované úrovně vlastností (PL _r).....	46
Příloha B (informativní) Bloková metoda a bezpečnostní blokové schéma.....	49
Příklad C (informativní) Výpočet nebo hodnocení MTTF _p hodnot pro jednotlivé komponenty.....	51
Příloha D (informativní) Zjednodušená metoda odhadu MTTFD pro každý kanál.....	57
Příloha E (informativní) Odhady pro diagnostické pokrytí (DC) pro funkce a moduly.....	59
Příloha F (informativní) Odhady pro poruchu se společnou příčinou (CCF).....	62
Příloha G (informativní) Systematická porucha.....	64
Příloha H (informativní) Příklad kombinace několika bezpečnostních částí ovládacího systému.....	66
Příloha I (informativní) Příklady.....	69
Příloha J (informativní) Software.....	76
Příloha K (informativní) Číselné vyjádření obrázku 5.....	79
Příloha ZA (informativní) Vztah mezi touto mezinárodní normou a základními požadavky směrnice EU 2006/42/ES.....	83

Bibliografie.....	
.....	84

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.

Za tento dokument je odpovědná komise ISO/TC 199 *Bezpečnost strojních zařízení*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO 13849-1:2006), které bylo technicky revidováno. Také obsahuje technickou opravu ISO 13849-1:2006 (Cor.1:2009). Změny oproti předchozímu vydání zahrnují

- vypuštění bývalé tabulky 1 z Úvodu,
- aktualizaci a doplnění citovaných dokumentů,
- modifikaci definic termínů *nebezpečná situace* a *režim s vysokým nebo trvalým vyžádáním*,
- doplnění nového termínu a definice *osvědčený v provozu*,
- ediční, ale ne technickou modifikaci obrázku 1,
- nový článek 4.5.5, stejně jako modifikaci existujících částí, včetně příloh, podstatnou změnu přílohy C a doplnění zcela nové přílohy I.

ISO 13849 sestává z následujících částí se společným názvem *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů*:

- *Část 1: Všeobecné zásady pro konstrukci*

- *Část 2: Ověření*

Úvod

Struktura bezpečnostních norem v oblasti strojních zařízení je následující.

- a) Normy typu A (základní bezpečnostní normy) uvádějí základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být aplikována na všechna strojní zařízení.
- b) Normy typu B (obecné bezpečnostní normy) se zabývají jedním nebo více bezpečnostními hledisky nebo jedním nebo více typy ochranných zařízení, která mohou být použita 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. dvouručního ovládání, blokovacích zařízení, zařízení citlivých na tlak, ochranných krytů).
- c) Normy typu C (bezpečnostní normy pro stroje) určují detailní bezpečnostní požadavky pro jednotlivý stroj nebo skupinu strojů.

Tato část ISO 13849 je norma typu B1, jak je stanoveno v ISO 12100.

Tento dokument je důležitý zejména pro následující zájmové skupiny představující poptávku s ohledem na bezpečnost strojů:

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

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, organizace pro lidi se speciálními potřebami);
- poskytovatelé služeb, např. údržba (malé, střední a velké podniky);
- spotřebitelé (v případě strojního zařízení určeného pro použití spotřebiteli).

Výše uvedeným zájmovým skupinám byla dána možnost se účastnit procesu přípravy tohoto dokumentu.

Kromě toho je tento dokument určen pro normalizační orgány, které zpracovávají normy typu C.

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

Pro stroje, které jsou zahrnuty v předmětu normy typu C a které byly navrženy a vyrobeny v souladu s požadavky této normy, mají přednost požadavky normy typu C.

Pro stroje, které byly navrženy a vyrobeny podle ustanovení této normy typu C platí, že pokud se

ustanovení normy typu C odlišují od ustanovení, která jsou stanovena v normách typu A nebo typu B, mají stanovení této normy typu C přednost před ustanoveními jiných norem.

Tato část ISO 13849 je určena jako návod pro ty, kteří se zabývají návrhem a posuzováním ovládacích systémů a dále pro technické komise připravující normy typu B2 a typu C, které jsou předpokladem pro splnění základních bezpečnostních požadavků přílohy I směrnice 2006/42/ES pro strojní zařízení. Norma neuvádí specifický návod pro shodu s jinými směrnicemi ES.

Jako část strategie celkového snížení rizika u stroje bude konstruktér pro snížení rizika často volit některá opatření pomocí aplikace ochranných zařízení plnících jednu nebo více bezpečnostních funkcí.

Části ovládacích systémů, které jsou určeny k plnění bezpečnostních funkcí jsou nazývány bezpečnostní části ovládacích systémů (SRP/CS) a tyto části mohou obsahovat hardware a software a mohou být buď oddělené od ovládacího systému stroje nebo mohou být jeho integrální částí. Kromě bezpečnostních funkcí mohou SRP/CS poskytovat také provozní funkce (např. dvouruční ovládání jako prostředek iniciace procesu).

Schopnosti bezpečnostních částí ovládacích systémů k vykonávání bezpečnostní funkce při předvídatelných podmínkách je přidělena jedna z pěti úrovní, které se nazývají úrovně vlastností (PL). Tyto úrovně vlastností jsou stanoveny pravděpodobností nebezpečné poruchy za hodinu (viz tabulka 2).

Pravděpodobnost nebezpečné poruchy bezpečnostní funkce závisí na několika faktorech, včetně struktury hardware a software, rozsahu mechanismů detekce závady [diagnostické pokrytí (DC)], spolehlivost komponentů [střední doba do nebezpečné poruchy ($MTTF_D$), poruše se společnou příčinou (CCF)], procesu návrhu, provozním zatížením, podmínkách prostředí a pracovních schopnostech.

Aby pomohl konstruktérovi a usnadnil posouzení dosažené úrovně vlastností PL, používá tento dokument metodologii, která je založena na kategorizaci struktur podle specifických návrhových kritérií a specifikovaného chování v podmínkách závady. Těmto kategoriím je přidělena jedna z pěti úrovní, označených jako kategorie B, 1, 2, 3 a 4.

Úrovně vlastností a kategorie se mohou vztahovat na bezpečnostní části ovládacích systémů, jako jsou:

- ochranná zařízení (např. dvouruční ovládání, blokovací zařízení), elektrická snímací ochranná zařízení (např. fotoelektrické clony), zařízení citlivá na tlak,
- ovládací jednotky (např. logická jednotka pro ovládací funkce, zpracování dat, monitorování, atd.), a
- elementy silového ovládání (např. relé, ventily, atd.).

stejně tak na ovládací systémy, které vykonávají bezpečnostní funkce u všech druhů strojních zařízení - od jednoduchých zařízení (např. malých kuchyňských strojů nebo automatických dveří a vrat) až po výrobní zařízení (např. balicí stroje, tiskové stroje, lisy).

Tato část ISO 13849 je určena k poskytnutí srozumitelných podkladů, na základě kterých může být posouzen návrh a vlastnosti každé aplikace bezpečnostních částí ovládacích systémů SRP/CS (a stroje), například třetí stranou, samotnou firmou nebo nezávislou zkušebnou.

Informace o doporučeném používání IEC 62061 a této části ISO 13849

IEC 62061 a tato část ISO 13849 specifikují požadavky pro návrh a realizaci bezpečnostních částí ovládacích systémů strojního zařízení. Používání těchto mezinárodních norem, v souladu s jejich předmětem, může být předpokladem pro splnění relevantních základních bezpečnostních požadavků. ISO/TR 23849 poskytuje návod na použití této části ISO 13849 a IEC 62061 při návrhu bezpečnostních částí ovládacích systémů pro strojní zařízení.

Stejně jako u ISO/TR 23849, ISO/TR 22100-2 byla přidána do seznamu citovaných dokumentů v kapitole 2 - vzhledem ke svému významu při pochopení vztahu mezi touto částí ISO 13849 a ISO 12100.

1 Předmět normy

Tato část ISO 13849 uvádí bezpečnostní požadavky a pokyny o zásadách návrhu a integrace bezpečnostních částí ovládacích systémů (SRP/CS), včetně návrhu software. Pro tyto části SRP/CS specifikuje norma charakteristiky, které zahrnují úroveň vlastností požadovanou k vykonávání bezpečnostních funkcí. Norma platí i pro SRP/CS pro vysoký požadavek a nepřetržitý režim, bez ohledu na druh používané technologie a energie (elektrické, hydraulické, pneumatické, mechanické, atd.) pro všechny druhy strojních zařízení.

Norma nespecifikuje bezpečnostní funkce nebo úrovně vlastností, které mají být použity v jednotlivém případě.

Tato část ISO 13849 uvádí specifické požadavky pro SRP/CS, které používají programovatelný elektronický systém (systémy).

Norma neuvádí specifické požadavky na návrh produktů, které jsou částí SRP/CS. Přesto však mohou být použity uvedené principy, jako například kategorie nebo úrovně vlastností.

POZNÁMKA 1 Příklady produktů, které jsou částí SRP/CS: relé, elektromagnetické ventily, spínače polohy, programovatelné logické automaty (PLC), ovládací jednotky motoru, dvouruční ovládací zařízení, zařízení citlivá na tlak. Pro návrh těchto produktů je důležitý odkaz na specificky používané mezinárodní normy, např. ISO 13851, ISO 13856-1 a ISO 13856-2.

POZNÁMKA 2 Pro definici *požadované úrovně vlastností* viz 3.1.24.

POZNÁMKA 3 Požadavky uvedené v této části ISO 13849 pro programovatelné elektronické systémy jsou kompatibilní s metodologií pro konstrukci a vývoj bezpečnostních elektrických, elektronických a programovatelných elektronických ovládacích systémů pro strojní zařízení, které jsou uvedeny v IEC 62061.

POZNÁMKA 4 Pro bezpečnostní vestavěný software pro komponenty s $PL_r = e$, viz IEC 61508-3:1998, kapitola 7.

Konec náhledu - text dále pokračuje v placené verzi ČSN.