ČESKÁ TECHNICKÁ NORMA

ICS 13.110 **Prosinec**
2008

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

idt ISO 13849-1:2006

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

Sécurité des machines - Partie 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 13849-1:2008. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 13849-1:2006. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 13849-1 (83 3205) z června 2007.

Národní předmluva

Změny proti předchozím normám

Tato norma obsahuje aktuální informace o citovaných normativních dokumentech a upravené články týkající se přílohy ZA a přílohy ZB.

Informace o citovaných normativních dokumentech

ISO 12100-1:2003 zavedena v ČSN EN ISO 12100-1:2004 (83 3001) Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 1: Základní terminologie, metodologie (idt ISO 12100-1:2003)

ISO 12100-2:2003 zavedena v ČSN EN ISO 12100-2:2004 (83 3001) Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 2: Technické zásady (idt ISO 12100-2:2003)

ISO 13849-2:2003 zavedena v ČSN EN ISO 13489-2:2008 (83 3205) Bezpečnost strojních zařízení - Bezpečnostní části řídicích systémů - Část 2: Ověřování (idt ISO 1349-2:2003)

ISO 14121-1 zavedena v ČSN EN ISO 14121-1 (83 3010) Bezpečnost strojních zařízení - Posouzení rizika -
Část 1: Zásady (idt ISO 14121-1)

IEC 60050-191:1990 zavedena v ČSN IEC 50(191):1993 (01 0102) Mezinárodný elektrotechnický slovník -
Kapitola 191: Spolahlivosť a akosť služieb

IEC 61508-3:1998 zavedena v ČSN EN 61508-3:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 3: Požadavky na software

IEC 61508-4:1998 zavedena v ČSN EN 61508-4:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 4: Definice a zkratky

Citované předpisy

Směrnice Evropského parlamentu a Rady 98/37/ES z 22. června 1998, o sbližování právních předpisů členských států týkajících se strojních zařízení, ve znění směrnice 98/79/ES. V České republice je tato směrnice zavedena nařízením vlády č. 24/2003 Sb., kterým se stanoví technické požadavky na strojní zařízení, v platném znění.

Směrnice Evropského parlamentu a Rady 2006/42/ES ze 17. května 2006, o sbližování právních předpisů členských států týkajících se strojních zařízení. V České republice je tato směrnice zavedena nařízením vlády č. 176/2008 Sb. z 27. května 2008, kterým se stanoví technické požadavky na strojní zařízení, v platném znění (toto nařízení vlády platí od 29.12.2009).

Upozornění na národní poznámky

Do normy byla v příloze F doplněna informativní národní poznámka.

Vypracování normy

Zpracovatel: Václav Svoboda, IČ 15296296

Pracovník Českého normalizačního institutu: Ing. Ján Chorvát

EVROPSKÁ NORMA EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM	EN ISO 13849-1 Červen 2008

ICS 13.110 Nahrazuje EN ISO 13849-1:2006

Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Všeobecné zásady pro konstrukci
(ISO 13849-1:2006)
Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
(ISO 13849-1:2003)

Sécurité des machines - Partie des systemes de commande relatives a la sécurité
Partie 1: Principes généraux de conception
(ISO 13849-1:2006)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen -
Teil 1: Allgemeine Gestaltungsleitsätze
(ISO 13849-1:2006)

Tato evropská norma byla schválena CEN 2008-05-18.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řidicím centru 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 Řidicímu centru, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CEN
Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
Řidicí centrum: rue de Stassart 36, B-1050 Brusel

Ref. č. EN ISO 13849-1:2008 E

Obsah

Předmluva

Text ISO 13849-1:2006 byl vypracován technickou komisí ISO/TC 199 „Bezpečnost strojních zařízení“ mezinárodní organizace pro normalizaci (ISO) a byl převzat jako EN ISO 13849-2:2008 technickou komisí CEN/TC 114 „Bezpečnost strojních zařízení“, která má sekretariát v DIN.

Této evropské normě je nutno nejpozději do listopadu 2008 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 prosince 2009.

Pozornost by měla být věnována možnosti, že některé z prvků tohoto dokumentu mohou být předmětem patentových práv. CEN (a/nebo CENELEC) nesmí být činěna odpovědna za identifikování některých nebo veškerých takových patentových práv.

Tento dokument nahrazuje EN ISO 13849-1:2006.

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

Vztah ke směrnici (směrnicím) EU je uveden v informativních přílohách ZA a ZB, které jsou nedílnou součástí tohoto dokumentu.

Podle Vnitřních předpisů CEN/CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojené království, Španělska, Švédska a Švýcarska.

Oznámení o schválení

Text normy ISO 13849-1:2006 byl schválen CEN jako EN ISO 13849-1:2008 bez jakýchkoliv modifikací.

Úvod

Struktura bezpečnostních norem v oblasti strojních zařízení je následující.

a) Normy typu A (základní normy) uvádějí základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být aplikována na všechna strojních zařízení.

b) Normy typu B (skupinové 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 příslušných 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, jako je stanoveno v ISO 12100-1.

Pro stroje, které byly konstruovány 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 B, mají ustanovení této normy typu C přednost před ustanoveními jiných norem.

Tato část ISO 13849 je určena jako návod pro ty, kteří se zabývají konstrukcí a posuzováním ovládacích systémů a dále pro technické komise připravující normy typu B2 a C, které jsou předpokladem pro splnění základních bezpečnostních požadavků přílohy I směrnice Rady 98/37/EC pro strojní zařízení. Norma neuvádí specifický návod pro shodu s jinými směrnicemi EC.

Jako součást 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 součástí. 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 definovány pravděpodobností nebezpečné poruchy za hodinu (viz tabulku 3).

Pravděpodobnost nebezpečné poruchy bezpečnostní funkce závisí na několika faktorech, včetně struktury hardware a software, rozsahu mechanismů detekce závady [diagnostické pokrytí (DC)], spolehlivosti součástí [střední doba do nebezpečné poruchy ($MTTF_d$)], poruše se společnou příčinou

(CCF), procesu konstrukce, provozním zatížení, podmínkách prostředí a pracovních postupech.

Aby pomohl konstruktérovi a usnadnil posouzení dosažené úrovně vlastností (PL), používá tento dokument metodologii, která je založena na kategorizaci struktur podle specifických konstrukčních 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

– prvky silového ovládání (např. relé, ventily, atd.),

a stejně tak na ovládací systémy, které vykonávají bezpečnostní funkce u všech druhů strojních zařízení - od jednoduchých zařízení (např. malých kuchyňských strojků 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 posouzena konstrukce 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 konstrukci a realizaci bezpečnostních částí ovládacích systémů strojních zařízení. Používání těchto mezinárodních norem, podle jejich předmětu, může být předpokladem pro splnění relevantních základních bezpečnostních požadavků. Následující tabulka sumarizuje předměty normy IEC 62061 a této části ISO 13849.

Tabulka 1 - Doporučené použití IEC 62061 a ISO 13849-1

	Technologie realizující bezpečnostní ovládací funkci (funkce)	**ISO 13849-1**	**IEC 62061**
A	Neelektrická, např. hydraulika	X	Nezahrnuje
B	Elektromechanická, např. relé a/nebo neúplná elektronika	Omezená na stanovenou architekturu [a)] a až do PL = e	Všechny architektury a až do SIL 3
C	Úplná elektronika, např. programovatelná	Omezená na stanovenou architekturu [a)] a až do PL = d	Všechny architektury a až do SIL 3
D	A kombinovaná s B	Omezená na stanovenou architekturu [a)] a až do PL = e	X[c)]

E	C kombinovaná s B	Omezená na stanovenou architekturu (viz poznámku 1) a až do PL = d	Všechny architektury a až do SIL 3
F	C kombinovaná s A, nebo C kombinovaná s A a B	X[b)]	X[c)]
X udává, že tímto předmětem se zabývá mezinárodní norma, která je uvedena v záhlaví sloupce.			
[a)] Stanovené architektury jsou definovány v 6.2, aby byl zjednodušen způsob pro kvantifikaci úrovně vlastností. [b)] Pro úplnou elektroniku: používání stanovených architektur podle této části ISO 13849 až do PL = d nebo jakékoliv architektury podle IEC 62061. [c)] Pro neelektrické technologie, používání částí podle této části ISO 13849 jako subsystémů.			

1 Předmět normy

Tato část ISO 13849 uvádí bezpečnostní požadavky a pokyny pro zásady konstrukce a integrace bezpečnostních částí ovládacích systémů (SRP/CS), včetně návrhu software. Pro tyto části SRP/CS specifikuje norma vlastnosti, které zahrnují úroveň vlastností požadovanou k vykonávání bezpečnostních funkcí. Norma platí pro bezpečnostní části ovládacích systémů (SRP/CS) 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 bezpečnostní části ovládacích systémů (SRP/CS), které používají programovatelný elektronický systém (systémy).

Norma neuvádí specifické požadavky na konstrukci výrobků, které jsou součástí bezpečnostních částí ovládacích systémů (SRP/CS). Přesto však uvedené zásady, jako např. kategorie nebo úrovně vlastností, mohou být použity.

POZNÁMKA 1 Příklady výrobků, které jsou součástí bezpečnostních částí ovládacích systémů: relé, elektromagnetické ventily, spínače polohy, programovatelné logické řadiče (PLCs), ovládací jednotky motoru, dvouruční ovládací zařízení, zařízení citlivá na tlak. Pro konstrukci těchto výrobků je důležitý odkaz na specificky používané mezinárodní normy, např. ISO 13851, ISO 13856-1 a ISO 13856-2.

POZNÁMKA 2 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 navrhování 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 součásti s PL_r = e viz kapitolu 7 v IEC 61508-3:1998.

-- Vynechaný text --