

2025

Bezpečnost strojních zařízení – Směrnice
pro funkční bezpečnost řídicích systémů souvisejících s bezpečností

ČSN
CLC IEC/TS 63394

33 2203

idt IEC/TS 63394:2023

Safety of machinery – Guidelines on functional safety of safety-related control system

Sécurité des machines – Lignes directrices sur la sécurité fonctionnelle des systèmes de commande relatifs à la sécurité

Sicherheit von Maschinen – Leitlinien zur funktionalen Sicherheit sicherheitsbezogener Steuerungssysteme

Tato norma je českou verzí technické specifikace CLC IEC/TS 63394:2024. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the Technical Specification CLC IEC/TS 63394:2024. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Upozornění na používání této normy

Tato norma přejímá technickou specifikaci CLC IEC/TS 63394:2024 vydanou v souladu s vnitřními předpisy CEN/CENELEC, část 2.

Informace o citovaných dokumentech

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 TR 63074:2019 nezavedena

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 13849-1:2015 zavedena v ČSN EN ISO 13849-1:2017 (83 3205) Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Obecné zásady pro konstrukci

ISO 13850:2015 zavedena v ČSN EN ISO 13850:2017 (83 3311) Bezpečnost strojních zařízení – Funkce nouzového zastavení – Zásady pro konstrukci

ISO 13851:2019 zavedena v ČSN EN ISO 13851:2020 (83 3325) Bezpečnost strojních zařízení – Dvouruční ovládací zařízení – Zásady pro konstrukci a výběr

ISO 14118:2017 zavedena v ČSN EN ISO 14118:2018 (83 3220) Bezpečnost strojních zařízení – Zamezení neočekávanému spuštění

ISO 14119:2013 zavedena v ČSN EN ISO 14119:2014 (83 3315) Bezpečnost strojních zařízení – Blokovací zařízení spojená s ochrannými kryty – Zásady pro konstrukci a volbu

Souvisící ČSN

ČSN EN 60204-1 ed. 3:2019 (33 2200) Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Obecné požadavky

ČSN EN 60947-5-3 ed. 2:2014 (35 4101) Spínací a řídicí přístroje nízkého napětí – Část 5-3: Přístroje a spínací prvky řídicích obvodů – Požadavky na bezdotykové přístroje s definovaným chováním při poruše (PDDB)

ČSN EN IEC 60947-5-8 ed. 2:2021 (35 4101) Spínací a řídicí přístroje nízkého napětí – Část 5-8: Přístroje a spínací prvky řídicích obvodů – Trojpolohové ovládací spínače

ČSN EN 60947-7-1 ed. 3 (35 4101) Spínací a řídicí přístroje nízkého napětí – Část 7-1: Pomocná zařízení – Svorkovnice pro měděné vodiče

ČSN EN 60947-7-2 ed. 3 (35 4101) Spínací a řídicí přístroje nízkého napětí – Část 7-2: Pomocná zařízení – Svorkovnice pro ochranné měděné vodiče

ČSN EN 61000-6-7 (33 3432) Elektromagnetická kompatibilita (EMC) – Část 6-7: Kmenové normy – Požadavky na odolnost pro zařízení určené k provádění funkcí v systémech vztahujících se k bezpečnosti (funkční bezpečnost) na průmyslových stanovištích

ČSN EN 61025:2007 (01 0676) Analýza stromu poruchových stavů (FTA)

ČSN EN IEC 61496-1 ed. 4 (33 2206) Bezpečnost strojních zařízení – Elektrická snímací ochranná zařízení – Část 1: Obecné požadavky a zkoušky

ČSN EN 61508-1 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky

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

ČSN EN 61508-5 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovně integrity bezpečnosti

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

ČSN EN 61508-7 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření

ČSN EN 61800-5-2 ed. 2:2018 (35 1720) Systémy elektrických výkonových pohonů s nastavitelnou rychlostí – Část 5-2: Bezpečnostní požadavky – Funkční

ČSN EN 61511 (soubor) (18 0303) Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů

ČSN EN 61649:2009 (01 0653) Weibullova analýza

ČSN EN ISO 11161:2007 (83 3210) Bezpečnost strojních zařízení – Integrované výrobní systémy – Základní požadavky

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

ČSN EN ISO 13856-1:2013 (83 3301) Bezpečnost strojních zařízení – Ochranná zařízení citlivá na tlak – Část 1: Všeobecné zásady pro konstrukci a zkoušení rohoží citlivých na tlak a podlah citlivých na tlak

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).

Informativní údaje z IEC/TS 63394:2023

Tuto technickou specifikaci vypracovala technická komise IEC/TC 44 *Bezpečnost strojních zařízení – Elektrotechnické aspekty*.

Text této technické specifikace se zakládá na těchto dokumentech:

Návrh k vyjádření	Zpráva o hlasování
44/980/DTS	44/989/RVDTS

Úplnou informaci o hlasování při schvalování této technické specifikace lze najít ve zprávě o hlasování ve výše uvedené tabulce.

Jazyk použitý při vypracování této technické specifikace je angličtina.

Tento dokument byl navržen v souladu se směrnicemi ISO/IEC, část 2, a byl vypracován v souladu se směrnicemi ISO/IEC, část 1, a se směrnicemi ISO/IEC, dodatkem IEC, dostupnými na www.iec.ch/members_experts/refdocs. Hlavní typy dokumentů vypracované v IEC jsou podrobněji popsány na www.iec.ch/standardsdev/publications.

Komise rozhodla, že obsah tohoto dokumentu zůstane nezměněn až do data příští prověrky (stability date) uvedeného na webových stránkách IEC (webstore.iec.ch) v údajích o tomto dokumentu. K tomuto datu bude dokument buď

- znovu potvrzen,
- zrušen,
- nahrazen revidovaným vydáním, nebo
- změněn.

Upozornění na národní poznámky

Do této normy byla k článku 4.1.2 doplněna národní poznámka.

UPOZORNĚNÍ – Publikace obsahuje barevný tisk, který je považován za potřebný k porozumění jejímu obsahu. Uživatelé by proto měli pro tisk tohoto dokumentu použít barevnou tiskárnu.

Vypracování normy

Zpracovatel odborného překladu: Ing. František Valenta, ELVAM, IČO 66051649

Technická normalizační komise: TNK 153 Bezpečnost elektrických zařízení a funkční bezpečnost strojních zařízení

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat na e-shopu.

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.

TECHNICKÁ SPECIFIKACE
TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CLC IEC/TS 63394

Únor 2024

ICS 13.110; 29.020;
25.040.99

Bezpečnost strojních zařízení – Směrnice pro funkční bezpečnost řídicích systémů souvisejících s bezpečností
(IEC/TS 63394:2023)

Safety of machinery – Guidelines on functional safety of safety-related control system
(IEC/TS 63394:2023)

Sécurité des machines – Lignes directrices
sur la sécurité fonctionnelle des systèmes
de commande relatifs à la sécurité
(IEC/TS 63394:2023)

Sicherheit von Maschinen – Leitlinien zur
funktionalen Sicherheit sicherheitsbezogener
Steuerungssysteme
(IEC/TS 63394:2023)

Tato technická specifikace byla schválena CENELEC dne 2024-01-22.

Členové CENELEC jsou povinni oznámit existenci této TS stejným způsobem jako u EN a umožnit, aby TS byla v příslušné formě okamžitě dostupná na národní úrovni. Je dovoleno, aby zůstaly v platnosti národní normy, které jsou s TS v rozporu.



Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Řídící centrum CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

© 2024 CENELEC Veškerá práva pro využití v jakékoliv formě a jakýmkoliv prostředky
jsou celosvětově vyhrazena členům CENELEC.

Ref. č. CLC IEC/TS 63394:2024 E

Členy CENELEC jsou národní elektrotechnické komitáty 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.

Evropská předmluva

Tento dokument (CLC IEC/TS 63394:2024) sestává z textu IEC/TS 63394:2023, který vypracovala technická komise IEC/TC 44 *Bezpečnost strojních zařízení – Elektrotechnické aspekty*.

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

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CENELEC.

Oznámení o schválení

Text mezinárodní technické specifikace IEC/TS 63394:2023 byl schválen CENELEC jako evropská technická specifikace bez jakýchkoliv modifikací.

Úvod.....	15
1..... Rozsah platnosti.....	16
2..... Citované dokumenty.....	16
3..... Termíny a definice.....	17
3.1..... Termíny a definice.....	17
3.2..... Abecední seznam termínů, definic a zkratk.....	28
4..... Typická klasifikace bezpečnostních funkcí v bezpečnosti strojních zařízení.....	30
4.1..... Obecně.....	30
4.1.1... Přehled.....	30
4.1.2... Posouzení rizika a snižování rizika podle ISO 12100.....	30
4.1.3... Snižování rizika a propojení s SCS a SRP/CS.....	31
4.1.4... Základní předpoklady pro snižování rizika v strojních zařízeních.....	32
4.2..... Základní bezpečnostní předpoklady pro návrh a integraci SCS nebo SRP/CS.....	32
4.3..... Bezpečnostní funkce.....	32
4.3.1...	

Obecně.....	32
4.3.2... Proces snižování rizika bezpečnostními funkcemi.....	32
4.3.3... Typická klasifikace bezpečnostních funkcí.....	33
4.4..... Vzájemný vztah mezi ISO 12100 a IEC 62061 nebo ISO 13849-1.....	34
4.4.1... Obecně.....	34
4.4.2... Vstupní informace v souladu s IEC 62061 nebo ISO 13849-1.....	34
4.4.3... Výstupní informace z IEC 62061 nebo ISO 13849-1.....	35
4.5..... Bezpečnostní funkce pro ochranu osob.....	35
4.5.1... Obecně.....	35
4.5.2... Bezpečnostní funkce pro ochranu osob založené na ochranných krytech a ochranných zařízeních.....	36
4.6..... Jiné bezpečnostní funkce pro zabránění nebezpečným situacím.....	36
4.6.1... Obecně.....	36
4.6.2... Jiné bezpečnostní funkce.....	36
4.7..... Bezpečnostní funkce pro ochranu integrity bezpečnosti stroje.....	37
4.7.1... Obecně.....	37
4.7.2... Bezpečnostní funkce pro ochranu integrity bezpečnosti stroje.....	38

4.8.....	Bezpečnostní funkce a normy typu C.....	38
5.....	Režim provozu na vyžádání související s bezpečnostními funkcemi.....	38
5.1.....	Obecně.....	38
5.2.....	Režim provozu s vysokým vyžádáním bezpečnostní funkce nebo s nepřetržitým provozem.....	39
5.2.1...	Obecně.....	39
5.2.2...	Přístup IEC 62061 a ISO 13849-1.....	39
5.2.3...	Zřídka aktivované bezpečnostní funkce.....	39
5.3.....	Režim provozu s nízkým vyžádáním bezpečnostní funkce.....	41
5.3.1...	Obecně.....	41
5.3.2...	Přístup IEC 62061 a ISO 13849-1.....	41
6.....	Proces návrhu bezpečnostních funkcí.....	41

6.1.....	
Obyecně.....	
.....	41
6.2.....	Postup
návrhu.....	
.....	42
6.3.....	Hodnocení požadované integrity
bezpečnosti.....	42
6.4.....	Rozklad bezpečnostní
funkce.....	
42	
6.5.....	Návrh
subsystému.....	
.....	42
6.5.1...	Omezení
architektury.....	
.....	42
6.5.2...	Nahromadění poruchových stavů a nedetekovaného poruchového
stavu.....	44
6.5.3...	Hodnocení
PFH.....	
.....	44
6.6.....	Příklady bezpečnostních
funkcí.....	45
7.....	Verifikační postupy pro bezpečnostní
funkce.....	46
7.1.....	
Obyecně.....	
.....	46
7.2.....	Verifikace zkušebního intervalu bezpečnostní
funkce.....	46
7.3.....	Verifikační
postupy.....	
.....	46
7.4.....	Počáteční
verifikace.....	
.....	46

7.5..... Periodická	
verifikace.....	
.....	47

7.5.1...	
Obecně.....	
.....	47

7.5.2... Frekvence periodické	
verifikace.....	
48	

7.6..... Vykazování	
verifikace.....	
.....	49

Příloha A (informativní) Posouzení rizika a snižování rizika podle ISO	
12100.....	50

A.1.....	
Obecně.....	
.....	50

A.2..... Zásady posouzení	
rizika.....	
.....	50

A.2.1..	
Obecně.....	
.....	50

A.2.2.. Základní informace, které mají být dostupné (jako vstup pro posouzení	
rizika).....	50

A.2.3.. Analýza	
rizika.....	
.....	51

A.3..... Snižování rizika pomocí bezpečnostní ochrany a doplňkových ochranných	
opatření.....	54

A.3.1..	
Obecně.....	
.....	54

A.3.2.. Z podstaty bezpečná konstrukční	
opatření.....	55

A.3.3.. Volba bezpečnostní ochrany a doplňkových ochranných	
opatření.....	55

A.4..... Jiná ochranná opatření (založená na	
postupu).....	57

A.4.1..	
Obecně.....	
.....	57
A.4.2..	
Postupy pro	
údržbu.....	
.....	57
A.4.3..	
Organizační pracovní	
postupy.....	
57	
A.5.....	
Ochranné kryty a ochranná zařízení podle ISO	
12100.....	57
A.5.1..	
Obecně.....	
.....	57
A.5.2..	
Ochranný kryt s blokováním se spouštěcí funkcí, s funkcí ručního	
restartu.....	58
A.5.3..	
Ochranné zařízení podle ISO	
12100.....	58
A.5.4..	
Ruční místní řídicí zařízení	
(a postup).....	59
A.5.5..	
Zařízení pro ruční volbu parametrů	
(a postup).....	60
A.5.6..	
Zařízení pro ruční volbu provozního režimu	
(a postup).....	60
A.5.7..	
Zařízení pro řízení energie	
(a postup).....	60
A.6.....	
Přístup maticového	
přiřazení.....	
....	60
A.6.1..	
Přehled.....	
.....	60

A.6.2..	
Obecně.....	
.....	60
A.6.3.. Metodika IEC 62061:2021, příloha	
A.....	61
A.7..... Přístup grafu	
rizika.....	
.....	61
A.7.1..	
Obecně.....	
.....	61
A.7.2.. Metodika ISO 13849-1:2015, příloha A s přiřazenou	
SIL.....	61
Příloha B (informativní) Metodika návrhu SCS nebo	
SRP/CS.....	63
B.1.....	
Obecně.....	
.....	63
B.2..... Plán funkční	
bezpečnosti.....	
.....	63
B.3..... Specifikace bezpečnostních	
požadavků.....	63
B.3.1..	
Obecně.....	
.....	63
B.3.2.. Funkční	
požadavky.....	
.....	64
B.3.3.. Požadavky na integritu	
bezpečnosti.....	
64	
B.4..... Ochrana před neočekávaným	
spuštěním.....	65
B.5..... Rozklad bezpečnostní	
funkce.....	
65	

B.5.1..	
Obečně.....	
.....	65
B.5.2..	
Architektura subsystému založená na rozkladu shora	
dolů.....	65
B.6.....	
Návrh SCS s použitím	
subsystémů.....	
65	
B.7.....	
Požadavky na systematickou integritu	
bezpečnosti.....	66
B.7.1..	
Obečně.....	
.....	66
B.7.2..	
Úroveň	
SCS.....	
.....	66
B.7.3..	
Úroveň	
subsystému.....	
.....	67
B.8.....	
Elektromagnetická	
odolnost.....	
.....	69
B.9.....	
Ruční parametrizace založená na	
softwaru.....	69
B.10...	
Aspekty	
zabezpečení.....	
.....	70
B.11...	
Aspekty	
zkoušení.....	
.....	71
B.12...	
Návrh a vývoj	
subsystému.....	
.....	71
B.12.1	
Obečně.....	
.....	71
B.12.2	
Návrh architektury	
subsystému.....	
....	72

B.12.3 Uvažování poruchových stavů a vyloučení poruchových stavů.....	74
B.12.4 Omezení architektury subsystému.....	74
B.12.5 Architektury návrhu subsystému.....	.. 75
B.12.6 Hodnota PFH subsystémů.....	76
B.13... Validace.....	76
B.14... Dokumentace.....	78
Příloha C (informativní) Příklady hodnot MTTFD pro jednotlivé součásti.....	81
Příloha D (informativní) Příklady pro diagnostické pokrytí (DC).....	82
D.1..... Obecně.....	82
D.2..... Vliv kabeláže, zapojení a propojení.....	82
D.2.1.. Obecně.....	82
D.2.2.. „Sériové zapojení“	83
D.3..... Použití informací z výrobního procesu.....	84
D.3.1.. Obecně.....	84

D.3.2.. Použití očekávaného časování nebo čekání na stav signálu.....	84
--	-----------

D.4..... Typická opatření

DC.....	84
---------	----

Příloha E (informativní) Opatření k dosažení funkční bezpečnosti s ohledem na elektromagnetické jevy.....	86
--	-----------

E.1.....

Obecně.....	86
-------------	----

E.2.....

Opatření.....	86
---------------	----

E.2.1..

Obecně.....	86
-------------	----

E.2.2.. Doporučení pro elektrické/elektronické položky zařízení (prostředky nebo přístroje).....	86
---	-----------

E.2.3.. Doporučení pro integraci SCS nebo SRP/CS do elektrických zařízení stroje.....	86
--	-----------

Příloha F (informativní) Pokyny pro software.....	88
--	-----------

F.1.....

Obecně.....	88
-------------	----

F.2.....

Dokumentace.....	88
------------------	----

F.3.....

Činnosti.....	90
---------------	----

Příloha G (informativní) Příklady bezpečnostních funkcí.....	95
---	-----------

G.1.....

Obecně.....	95
-------------	----

G.2..... Bezpečnostní

funkce.....	95
G.2.1.. Základní informace.....	95
G.2.2.. Podrobný popis bezpečnostních požadavků.....	95
G.2.3.. Příklad ochranného krytu s blokováním.....	97
Příloha H (informativní) Hodnocení hodnoty PFH subsystému.....	100
H.1.....	
Obecně.....	100
H.2..... Tabulkový přístup (IEC 62061).....	100
H.3..... Zjednodušené vzorce pro odhad hodnoty PFH (IEC 62061).....	100
H.4..... Přístupy IEC 61508, IEC 62061 a ISO 13849-1.....	100
H.4.1..	
Obecně.....	100
H.4.2.. Přístup IEC 61508.....	100
H.4.3.. Přístup IEC 62061.....	101
H.4.4.. Přístup ISO 13849-1:2015, příloha K.....	102
H.5..... Základní úvahy ohledně exponenciálního a Weibullova rozdělení.....	104
H.5.1.. Exponenciální rozdělení.....	104
H.5.2.. Weibullovo	

rozdělení.....	105
H.6..... T10 a B10.....	106
H.6.1.. Obecně.....	106
H.6.2.. T10 s exponenciálním rozdělením.....	106
H.6.3.. T10 s Weibullovým rozdělením.....	107
H.7..... Přehled vzorců PFH.....	108
H.7.1.. Definice.....	108
H.7.2.. Vzorce.....	108
H.7.3.. Příklady.....	111
H.8..... Metodika pro odhad CCF.....	112
H.9..... Základní architektura subsystému A (1001).....	113
H.9.1.. Obecně.....	113
H.9.2.. PFH.....	113
H.9.3.. Zjednodušený Weibullův přístup.....	114

H.10... Základní architektura subsystému C (10o1D).....	114
H.10.1 Obecně.....	114
H.10.2 Reakce na poruchový stav prováděná jiným subsystémem.....	114
H.10.3 Reakce na poruchový stav, kterou je třeba vzít v úvahu v subsystému.....	115
H.10.4 PFH.....	117
H.10.5 Vliv CCF.....	118
H.11... Základní architektura subsystému B (10o2).....	118
H.11.1 Obecně.....	118
H.11.2 PFH.....	119
H.11.3 Vliv CCF.....	119
H.12... Základní architektura subsystému D (10o2D).....	119
H.12.1 Obecně.....	119
H.12.2 Hodnocení PFH Term A.....	120
H.12.3 Hodnocení PFH Term B.....	120

H.12.4 Hodnocení PFH Term C a Term

D..... 121

H.12.5

PFH.....
..... 121

H.12.6 Vliv

CCF.....
..... 121

H.13... Základní architektura subsystému D (1oo2D) se dvěma časovými
obdobími..... 121

H.13.1

Obecně.....
..... 121

H.13.2 Hodnocení PFH Term

A.....
122

H.13.3 Hodnocení PFH Term

A.....
122

H.13.4 Hodnocení PFH Term C a Term

D..... 122

H.13.5

PFH.....
..... 122

H.13.6 Vliv

CCF.....
..... 122

Příloha I (informativní) Komentované příklady stávajících
předpisů..... 123

I.1.....

Obecně.....
..... 123

I.2..... Evropská

unie.....
..... 123

I.2.1.... Obecná evropská

legislativa.....
.... 123

I.2.2.... Nově navržený předpis pro strojní zařízení (ve fázi

přípravy)..... 123

I.2.3.... Relevantní

legislativa.....
..... 124

I.2.4.... Povinnosti výrobce

stroje.....
... 124

I.3..... Severní Amerika -

USA.....
... 124

I.4..... Severní Amerika -

Kanada.....
.. 125

I.5..... Jižní Amerika -

Brazílie.....
..... 125

I.6.....

Čína.....
..... 125

I.7.....

Japonsko.....
..... 125

Příloha J (informativní) Kombinace režimů

provozu..... 126

J.1.....

Obecně.....
..... 126

J.2..... Základní přístupy k různým režimům

provozu..... 126

J.2.1...

Obecně.....
..... 126

J.2.2... Opatření pro snižování rizika v režimu provozu s nízkým vyžádáním bezpečnostní

funkce..... 127

J.3..... Použití subsystémů s různými režimy

provozu..... 127

J.3.1...

Obecně.....
..... 127

J.3.2... Příklad s různými režimy provozu.....	128
J.3.3... Subsystem (subsystemy) používaný pro různé druhy provozu.....	129
Bibliografie.....	132
Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a jim odpovídající evropské publikace.....	134
 Obrázek 1 – Integrace v procesu snižování rizika v ISO 12100.....	 31
Obrázek 2 – Rozklad SCS nebo SRP/CS.....	32
Obrázek 3 – Proces snižování rizika bezpečnostními funkcemi.....	33
Obrázek 4 – Režim provozu s vysokým vyžádáním.....	39
Obrázek 5 – Proces pro určení režimu provozu s vysokým vyžádáním.....	40
Obrázek 6 – Režim provozu s nízkým vyžádáním.....	41
Obrázek A.1 – Přístup přiřazení SIL.....	61
Obrázek A.2 – Přístup grafu rizika v ISO 13849-1:2015, obrázek A.1 s přiřazenou SIL.....	62
Obrázek B.1 – Příklad rozkladu bezpečnostní funkce.....	66
Obrázek B.2 – Možné účinky rizika (rizik) zabezpečení na SCS (IEC TR 63064:2019, obrázek 2).....	71
Obrázek B.3 – Zřídka aktivované bezpečnostní funkce a režim provozu subsystémů.....	74
Obrázek H.1 – Kumulativní distribuční funkce (CDF).....	108
Obrázek H.2 – Porucha se společnou	

příčinou.....	113
Obrázek H.3 – Blokové schéma spolehlivosti základní architektury subsystému A (1oo1).....	113
Obrázek H.4 – Funkce nedostupnosti základní architektury subsystému A (1oo1).....	113
Obrázek H.5 – Blokové schéma spolehlivosti 1oo1, zjednodušený Weibullův přístup.....	114
Obrázek H.6 – Logický pohled na základní architekturu subsystému C (1oo1D) s iniciací bezpečného stavu pomocí jiného subsystému.....	115
Obrázek H.7- Blokové schéma spolehlivosti základní architektury subsystému C (1oo1D) s iniciací bezpečného stavu pomocí jiného subsystému.....	115
Obrázek H.8 – Funkce nedostupnosti základní architektury subsystému C (1oo1D).....	115
Obrázek H.9 – Logický pohled na základní architekturu subsystému C (1oo1D) s reakcí na poruchový stav.....	116
Obrázek H.10 – Blokové schéma spolehlivosti základní architektury subsystému C (1oo1D) s reakcí na poruchový stav...	116
Obrázek H.11 – Funkce nedostupnosti základní architektury subsystému C (1oo1D).....	117
Obrázek H.12 – Blokové schéma spolehlivosti základní architektury subsystému B (1oo2).....	118
Obrázek H.13 – Funkce nedostupnosti základní architektury subsystému B (1oo2).....	118
Obrázek H.14 – Blokové schéma spolehlivosti základní architektury subsystému D (1oo2D).....	119
Obrázek H.15 – Funkce nedostupnosti základní architektury subsystému D (1oo2D).....	120
Obrázek J.1 – Základní přístup v režimu provozu s vysokým vyžádáním nebo nepřetržitým provozu na základě IEC 61508 (a IEC 62061).....	126
Obrázek J.2 – Základní přístup v režimu provozu s nízkým vyžádáním na základě IEC 61508 (a IEC 61511).....	127

Obrázek J.3 – Funkční

pohled.....
..... 128

Obrázek J.4 – Logický

pohled.....
..... 129

Obrázek J.5 – Rozkladový

pohled.....
.. 129

Obrázek J.6 – Kvantitativní hodnocení SIL pomocí přístupu poměru pravděpodobnosti poruch
každého subsystému..... 130

Obrázek J.7 – Příklad kvantitativního hodnocení SIL pomocí přístupu poměru pravděpodobnosti
poruch každého

subsystému.....
..... 131

Tabulka 1 – Termíny použité v tomto dokumentu.....	28
Tabulka 2 – Vstupní informace pro specifikaci bezpečnostních požadavků (SRS).....	34
Tabulka 3 – Výstupní informace z návrhu SCS nebo SRP/CS na celkové posouzení rizika.....	35
Tabulka 4 – Bezpečnostní funkce pro ochranu osob.....	36
Tabulka 5 – Jiné bezpečnostní funkce.....	37
Tabulka 6 – Bezpečnostní funkce pro ochranu integrity.....	38
Tabulka 7 – Omezení architektury pro režim provozu s vysokým vyžádáním.....	43
Tabulka A.1 – Základní informace pro posouzení rizika podle ISO 12100.....	50
Tabulka A.2 – Určení omezení strojního zařízení podle ISO 12100.....	51
Tabulka A.3 – Zásady identifikace nebezpečí podle ISO 12100.....	52
Tabulka A.4 – Odhad rizika podle ISO 12100.....	53
Tabulka A.5 – Dodatečné uvažované aspekty během odhadu rizika podle ISO 12100.....	54
Tabulka A.6 – Ochranné kryty podle ISO 12100.....	58
Tabulka A.7 – Příklady ochranných zařízení podle ISO 12100.....	59
Tabulka B.1 – Přehledový plán funkční bezpečnosti.....	63
Tabulka B.2 – Přehled základních funkčních požadavků.....	64
Tabulka B.3 – SIL a mezní hodnota PFH.....	64

Tabulka B.4 – Vyvarování se systematických poruch (úroveň SCS nebo SRP/CS).....	66
Tabulka B.5 – Řízení systematických poruch (úroveň SCS nebo SRP/CS).....	67
Tabulka B.6 – Vyvarování se systematických poruch (úroveň subsystému).....	68
Tabulka B.7 – Řízení systematických poruch (úroveň subsystému).....	68
Tabulka B.8 – Ruční parametrizace založená na softwaru.....	70
Tabulka B.9 – Příčina a účinky zřídka aktivovaných bezpečnostních funkcí.....	73
Tabulka B.10 – Omezení architektury a základní požadavky na subsystém.....	75
Tabulka B.11 – Přehled validačního procesu s požadovanými informacemi.....	77
Tabulka B.12 – Technická dokumentace založená na procesu návrhu (tabulka 9 v IEC 62061.2021, modifikovaná).....	79
Tabulka B.13 – Přehled dokumentace.....	80
Tabulka C.1 – Hodnoty $MTTF_D$ nebo B_{10D} pro součásti (odvozené z ISO 13849-1:2015).....	81
Tabulka C.2 – Vztah λ_D , $MTTF_D$ a B_{10D}	81
Tabulka D.1 – Opatření k zabránění zkratu.....	83
Tabulka D.2 – Hodnoty DC a doporučená opatření.....	85
Tabulka E.1 – Nevyčerpávající seznam doporučení týkajících se opatření EMI pro integraci prostředků nebo zařízení do elektrických zařízení stroje.....	87
Tabulka F.1 – Dokumenty pro SW úroveň 1 a SW úroveň 2.....	88
Tabulka F.2 – Pokyny pro	

kódování.....	89
Tabulka F.3 – Přehled protokolů.....	90
Tabulka F.4 – SW úrovně 1 – Přehled základních činností.....	91
Tabulka F.5 – SW úrovně 2 – Přehled základních činností.....	92
Tabulka F.6 – SW úrovně 2 – Přehled základních činností.....	94
Tabulka G.1 – Příklady bezpečnostních funkcí a přidružených zařízení souvisejících s bezpečností.....	95
Tabulka G.2 – Základní informace související se specifikací bezpečnostních požadavků.....	96
Tabulka G.3 – Příklad parametrů souvisejících s bezpečností pro bezpečnostní funkci s požadovanou SIL 1.....	98
Tabulka G.4 – Příklad parametrů souvisejících s bezpečností pro bezpečnostní funkci s požadovanou SIL 3.....	99

Tabulka H.1 – Vzorce pro základní architekturu subsystému A (1001).....	109
Tabulka H.2 – Vzorce pro základní architekturu subsystému C (1001D).....	109
Tabulka H.3 – Vzorce pro základní architekturu subsystému B (1002).....	110
Tabulka H.4 – Vzorce pro základní architekturu subsystému D (1002D).....	110
Tabulka H.5 – Příklady hodnot PFH založených na B_{10D}	111
Tabulka H.6 – Příklady hodnot PFH založených na T_{10D} a B_{10D}	112
Tabulka J.1 – $PFD_{avg\ max}$ a PFH_{max} pro příslušnou cílovou SIL.....	131

Úvod

V kontextu bezpečnosti strojních zařízení poskytuje sektorová norma IEC 62061 spolu s ISO 13849-1 požadavky a návod pro výrobce strojů na návrh, vývoj a integraci řídicího systému souvisejícího s bezpečností (SCS) nebo popřípadě s bezpečností souvisejících částí řídicích systémů (SRP/CS) včetně vstupních zařízení a koncových prvků bez ohledu na technologii (mechanická, pneumatická, hydraulická a elektrická technologie).

Důležité jsou tyto aspekty:

- klasifikace bezpečnostních funkcí,
- architektura realizace bezpečnostních funkcí,
- režimy provozu bezpečnostních funkcí,
- výpočet založený na použité technologii.

Bezpečnostní funkce mohou být tedy klasifikovány takto:

- Bezpečnostní funkce, které zastavují nebezpečný pohyb (pohyby) stroje a které jsou hlavně prováděny SCS nebo SRP/CS strojů pro ochranu osob. Typické příklady jsou ochranné kryty s blokováním, snímací ochranná zařízení, dvouruční ovládací zařízení a nouzové zastavení.
- Bezpečnostní funkce, které chrání integritu bezpečnosti stroje před destrukcí a které mohou v druhém kroku mít vliv na ochranu osob. Typické příklady jsou ochranné přístroje, přístroje pro omezení tlaku nebo teploty (rovněž definovaných jako „parametry související s bezpečností“, například poloha, rychlost, teplota nebo tlak, odlišujících se od mezních hodnot stanovených v řídicím systému).
- Jiné bezpečnostní funkce, které nejsou pokryty dvěma předcházejícími případy.

POZNÁMKA 1 Jsou definovány různé druhy bezpečnostních funkcí v souladu s klasifikacemi a definicemi v ISO 12100 a ISO 13849-1.

Uvažují se architektury subsystémů pro provádění bezpečnostní funkce (funkcí).

POZNÁMKA 2 V IEC 62061:2021 jsou zavedeny informace pro mapování klasifikace SIL (úroveň integrity bezpečnosti) v IEC 62061/IEC 61508 a klasifikace v ISO 13849-1 z hlediska kategorií, architektur, určených architektur a PL (úroveň vlastností). Pro umožnění zpětné kompatibility se v tomto dokumentu uvažují tato různá kritéria.

V závislosti na režimu provozu bezpečnostní funkce se budou uvažovat kritéria a výpočty pro splnění požadavků tohoto dokumentu a pro dosažení souladu s existujícími předpisy (jako jsou například doporučení pro použití v Evropě) a pro splnění jiných požadavků již stanovených v existujících normách, například na periodicitu zkoušek.

Pro zohlednění mechanických, pneumatických, hydraulických a elektrických technologií, aplikací pro bezpečnostní funkce, architektury a režim provozu, jsou hodnoceny přidružené výpočty.

POZNÁMKA 3 Například většina výpočtů v normách je založena na exponenciálním zákonu, který je typicky použitelný pro elektronickou technologii. Pro mechanickou technologii nebo jiné technologie

se aplikuje Weibullovo rozdělení a exponenciální rozdělení se s výjimkou omezení nepoužívá.

1 Rozsah platnosti

V kontextu bezpečnosti strojních zařízení poskytuje sektorová norma IEC 62061 spolu s ISO 13849-1 požadavky pro výrobce strojů na návrh, vývoj a integraci řídicích systémů souvisejících s bezpečností (SCS) nebo s bezpečností souvisejících částí řídicích systémů (SRP/CS) v závislosti na použité technologii (mechanická, pneumatická, hydraulická a elektrická technologie) k provádění bezpečnostních funkcí. Tento dokument nenahrazuje ISO 13849-1 a IEC 62061. Tento dokument uvádí doplňkový návod na aplikaci IEC 62061 nebo ISO 13849-1. Tento dokument:

- uvádí pokyny a specifikuje doplňkové požadavky na konkrétní bezpečnostní funkce založené na metodice ISO 12100, které jsou důležité ve strojních zařízeních a respektují typické mezní podmínky strojních zařízení;
- uvažuje bezpečnostní funkce, které jsou navrženy pro režim provozu s vysokým vyžádáním, které jsou však provozovány jen zřídka, nazývané zřídka aktivovanými bezpečnostními funkcemi;

POZNÁMKA 1 IEC 62061:2021 zcela pokrývá vysoké vyžádání. V tomto dokumentu se však podrobněji uvažují i jiné bezpečnostní funkce související s ochranou samotného stroje a nepřímo osob.

- uvádí doplňkové informace pro výpočet měr poruch za použití jiných (neelektronických) technologií založených například na Weibullově rozdělení, neboť všechny vzorce definované v IEC 62061 a ISO 13849-1 jsou založeny na exponenciálním rozdělení.

Základem pro tyto pokyny a doplňkové požadavky je tedy

- typická klasifikace bezpečnostních funkcí;
- uvážení typických architektur používaných pro navrhování bezpečnostních funkcí;
- uvážení režimů provozu bezpečnostních funkcí;
- odvození a hodnocení vzorců PFH pro subsystémy uvažující použitou technologii.

POZNÁMKA 2 Tyto pokyny se mohou rovněž použít pro aplikaci ISO 13849-1 na proces návrhu SRP/CS.

Tento dokument se nezabývá režimem provozu s nízkým vyžádáním podle IEC 61508.

Tento dokument nebere v úvahu analýzu vrstev ochrany (LOPA) ani základní systém řízení procesů (BPCS) podle IEC 61511 jako opatření pro snížení rizika.

Tento dokument uvažuje všechny fáze životního cyklu stroje týkající se funkční bezpečnosti a SCS nebo SRP/CS.

POZNÁMKA 3 Uživatel stroje potřebuje informace od výrobce stroje pro bezpečný provoz stroje, například užitečnou životnost součástí, informace o údržbě a zkoušení bezpečnostních funkcí, pokud jsou potřeba.

Konec náhledu - text dále pokračuje v placené verzi ČSN.