ICS 13.110 SLOVENSKÁ TECHNICKÁ NORMA Október 2024

STN	**Bezpečnosť strojov Bezpečnostné časti riadiacich systémov Časť 1: Všeobecné zásady navrhovania (ISO 13849-1: 2023)**	**STN EN ISO 13849-1** 83 3313

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

Sécurité des machines
Parties des systèmes de commande relatives à la sécurité
Partie 1: Principes généraux de conception

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

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO 13849-1: 2023.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO 13849-1 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO 13849-1: 2023.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO 13849-1 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO 13849-1 z augusta 2023, ktorá od 1. 8. 2023 nahradila STN EN ISO 13849-1 z mája 2016 v celom rozsahu.

STN EN ISO 13849-1 z mája 2016 sa môže súbežne s touto STN používať do **31. 5. 2026**.

obsahuje farebné strany

138069

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO, © 2023 ISO, ref. č. ISO 13849-1: 2023 E.

Informácie pre používateľa STN

Hlavné zmeny oproti predchádzajúcemu vydaniu sú nasledovné:

- celý dokument bol reorganizovaný tak, aby lepšie sledoval proces návrhu a vývoja riadiacich systémov;
- nová kapitola 4 o odporúčaní na posúdenie rizika;
- špecifikácia bezpečnostných funkcií (aktualizovaná kapitola 5);
- kombinácia viacerých podsystémov (aktualizovaná kapitola 6);
- nová kapitola 7 o požiadavkách na bezpečnosť softvéru;
- nová kapitola 9 o ergonomických aspektoch návrhu;
- validácia (aktualizovaná kapitola 8 a presunuté do kapitoly 10);
- nová kapitola G.5 o riadení funkčnej bezpečnosti;
- nová príloha L o odolnosti voči elektromagnetickému rušeniu (EMI);
- nová príloha M s dodatočnými informáciami pre špecifikáciu bezpečnostných požiadaviek;
- nová príloha N o opatreniach na zabránenie chybám pri návrhu softvéru súvisiaceho s bezpečnosťou;
- nová príloha O s bezpečnostnými hodnotami komponentov alebo častí riadiacich systémov.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO 12100: 2010 prijatá ako STN EN ISO 12100: 2011 Bezpečnosť strojov. Všeobecné zásady konštruovania strojov. Posudzovanie a znižovanie rizika (ISO 12100: 2010) (83 3001)

ISO 13849-2: 2012 prijatá ako STN EN ISO 13849-2: 2013 Bezpečnosť strojov. Bezpečnostné časti riadiacich systémov. Časť 2: Hodnotenie (ISO 13849-2: 2012) (83 3313)

ISO 13855: 2010 prijatá ako STN EN ISO 13855: 2010 Bezpečnosť strojov. Umiestnenie ochranných zariadení so zreteľom na rýchlosť približujúcich sa častí ľudského tela (ISO 13855: 2010) (83 3303)

ISO 20607: 2019 prijatá ako STN EN ISO 20607: 2021 Bezpečnosť strojov. Návod na používanie. Všeobecné zásady tvorby (ISO 20607: 2019) (83 3004)

IEC 61508-3: 2010 prijatá ako STN EN 61508-3: 2010 Funkčná bezpečnosť elektrických/elektronických/programovateľných elektronických bezpečnostných systémov. Časť 3: Požiadavky na programové vybavenie (18 4020)

IEC 62046: 2018 prijatá ako STN EN IEC 62046: 2019 Bezpečnosť strojových zariadení. Aplikácia ochranných zariadení na detekciu prítomnosti osôb (33 2206)

IEC 62061: 2021 prijatá ako STN EN IEC 62061: 2021 Bezpečnosť strojov. Funkčná bezpečnosť bezpečnostných riadiacich systémov (35 2220)

IEC/IEEE 82079-1: 2019 prijatá ako STN EN IEC/IEEE 82079-1: 2020 Príprava informácií na používanie (návodu na používanie) výrobkov. Časť 1: Zásady a všeobecné požiadavky (01 3783)

Súvisiace právne predpisy

smernica Európskeho parlamentu a Rady 2006/42/ES zo 17. mája 2006 (OJ L 157 z 9. 6. 2006) o strojových zariadeniach a o zmene a doplnení smernice 95/16/ES

nariadenie vlády SR č. 436/2008 Z. z., ktorým sa ustanovujú podrobnosti o technických požiadavkách a postupoch posudzovania zhody na strojové zariadenia

Vypracovanie

Spracovateľ: Ing. Daniela Onofrejová, PhD., Košice

Technická komisia: TK 29 Bezpečnosť strojov a ergonómia

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 13849-1

Máj 2023

ICS 13.110

Nahrádza EN ISO 13849-1: 2015

Bezpečnosť strojov
Bezpečnostné časti riadiacich systémov
Časť 1: Všeobecné zásady navrhovania
(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 Gestaltungsleitsätze
(ISO 13849-1: 2023)

Túto európsku normu schválil CEN 3. marca 2023.

Členovia CEN sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO 13849-1: 2023 SK

Obsah

strana

Európsky predhovor ... 11

Úvod ... 12

1 Predmet ... 16

2 Normatívne odkazy ... 16

3 Termíny, definície, symboly a skrátené termíny ... 17
3.1 Termíny a definície ... 17
3.2 Symboly a skrátené termíny ... 24

4 Prehľad ... 26
4.1 Proces posudzovania a znižovania rizík na stroji ... 26
4.2 Príspevok k znižovaniu rizika ... 28
4.3 Proces navrhovania SRP/CS ... 29
4.4 Metodika ... 30
4.5 Požadované informácie ... 30
4.6 Realizácia bezpečnostnej funkcie pomocou podsystémov ... 31

5 Špecifikácia bezpečnostných funkcií ... 31
5.1 Identifikácia a všeobecný opis bezpečnostnej funkcie ... 31
5.2 Špecifikácia bezpečnostných požiadaviek ... 32
5.2.1 Všeobecné požiadavky ... 32
5.2.2 Požiadavky na špecifické bezpečnostné funkcie ... 34
5.2.3 Minimalizácia motivácie vyradiť bezpečnostné funkcie ... 38
5.2.4 Vzdialený prístup ... 39
5.3 Stanovenie požadovanej úrovne výkonnosti (PLr) pre každú bezpečnostnú funkciu ... 39
5.4 Preskúmanie špecifikácie bezpečnostných požiadaviek (SRS) ... 39
5.5 Rozklad SRP/CS na podsystémy ... 40

6 Úvahy o návrhu ... 41
6.1 Hodnotenie dosiahnutej úrovne výkonnosti ... 41
6.1.1 Všeobecný prehľad úrovne výkonnosti ... 41
6.1.2 Korelácia medzi úrovňou výkonnosti (PL) a úrovňou integrity bezpečnosti (SIL) ... 43
6.1.3 Architektúra – Kategórie a ich vzťah k $MTTF_D$ každého kanála, priemerné diagnostické pokrytie a porucha so spoločnou príčinou (CCF) ... 43
6.1.4 Stredný čas do nebezpečnej poruchy ($MTTF_D$) ... 51
6.1.5 Diagnostické pokrytie (DC) ... 52
6.1.6 Poruchy so spoločnou príčinou (CCF) ... 52
6.1.7 Systematické poruchy ... 53
6.1.8 Zjednodušený postup odhadu úrovne výkonnosti pre podsystémy ... 53

6.1.9 Alternatívny postup na určenie úrovne výkonnosti a PFH bez $MTTF_D$ ... 55
6.1.10 Posúdenie poruchového stavu a jeho vylúčenie ... 56
6.1.11 Osvedčený komponent ... 57
6.2 Kombinácia podsystémov na dosiahnutie celkovej úrovne výkonnosti bezpečnostnej funkcie ... 58
6.2.1 Všeobecne ... 58
6.2.2 Známe hodnoty PFH ... 58
6.2.3 Neznáme hodnoty PFH ... 59
6.3 Manuálna parametrizácia založená na softvéri ... 59
6.3.1 Všeobecne ... 59
6.3.2 Vplyvy na parametre súvisiace s bezpečnosťou ... 60
6.3.3 Požiadavky na manuálnu parametrizáciu založenú na softvéri ... 60
6.3.4 Overenie parametrizačného nástroja ... 61
6.3.5 Dokumentácia manuálnej parametrizácie založenej na softvéri ... 62
7 Požiadavky na bezpečnosť softvéru ... 62
7.1 Všeobecne ... 62
7.2 Jazyk obmedzenej variability (LVL) a jazyk úplnej variability (FVL) ... 64
7.2.1 Jazyk obmedzenej variability (LVL) ... 64
7.2.2 Jazyk úplnej variability (FVL) ... 64
7.2.3 Rozhodnutie pre jazyk obmedzenej variability (LVL) alebo jazyk úplnej variability (FVL) ... 64
7.3 Vstavaný softvér súvisiaci s bezpečnosťou (SRESW) ... 66
7.3.1 Návrh vstavaného softvéru súvisiaceho s bezpečnosťou (SRESW) ... 66
7.3.2 Alternatívne postupy pre neprístupný vstavaný softvér ... 67
7.4 Aplikačný softvér súvisiaci s bezpečnosťou (SRASW) ... 68
8 Overenie dosiahnutej úrovne výkonnosti ... 70
9 Ergonomické aspekty návrhu ... 70
10 Validácia ... 71
10.1 Princípy validácie ... 71
10.1.1 Všeobecne ... 71
10.1.2 Plán validácie ... 73
10.1.3 Všeobecné zoznamy poruchových stavov ... 73
10.1.4 Špecifické zoznamy poruchových stavov ... 73
10.1.5 Informácie pre validáciu ... 74
10.2 Validácia špecifikácie bezpečnostných požiadaviek (SRS) ... 75
10.3 Validácia analýzou ... 75
10.3.1 Všeobecne ... 75
10.3.2 Techniky analýzy ... 75
10.4 Validácia testovaním ... 76

10.4.1 Všeobecne ... 76
10.4.2 Presnosť merania ... 76
10.4.3 Dodatočné požiadavky na skúšanie ... 77
10.4.4 Počet skúšobných vzoriek ... 77
10.4.5 Skúšobné metódy ... 77
10.5 Validácia bezpečnostných funkcií ... 78
10.6 Validácia integrity bezpečnosti SRP/CS ... 78
10.6.1 Validácia podsystému(-ov) ... 78
10.6.2 Validácia opatrení proti systematickým poruchám ... 80
10.6.3 Validácia softvéru súvisiaceho s bezpečnosťou ... 80
10.6.4 Validácia kombinácie podsystémov ... 81
10.6.5 Celková validácia integrity bezpečnosti ... 81
10.7 Validácia požiadaviek prostredia ... 82
10.8 Validačný záznam ... 82
10.9 Validácia požiadaviek na údržbu ... 82
11 Udržateľnosť SRP/CS ... 83
12 Technická dokumentácia ... 83
13 Informácie pre použitie ... 84
13.1 Všeobecne ... 84
13.2 Informácie pre integráciu SRP/CS ... 84
13.3 Informácie pre používateľa ... 84
Príloha A (informatívna) – Návod na určenie požadovanej úrovne výkonnosti (PL_r) ... 86
A.1 Všeobecne ... 86
A.2 Výber požadovanej úrovne výkonnosti (PL_r) ... 87
A.3 Návod na výber parametrov S, F a P na odhad rizika ... 87
A.3.1 Závažnosť zranenia, S1 a S2 ... 87
A.3.2 Frekvencia a/alebo časy vystavenia nebezpečenstvu, F1 a F2 ... 87
A.3.3 Možnosť vyhnúť sa poškodeniu alebo ho obmedziť, P1 a P2 ... 88
A.4 Prekrývajúce sa nebezpečenstvá ... 90
Príloha B (informatívna) – Bloková metóda a bloková schéma súvisiaca s bezpečnosťou ... 91
B.1 Bloková metóda ... 91
B.2 Bloková schéma súvisiaca s bezpečnosťou ... 91
Príloha C (informatívna) – Výpočet alebo vyhodnotenie hodnôt $MTTF_D$ pre jednotlivé komponenty ... 93
C.1 Všeobecne ... 93
C.2 Metóda osvedčených technických postupov ... 93
C.3 Hydraulické komponenty ... 95
C.4 $MTTF_D$ pneumatických, mechanických a elektro-mechanických komponentov ... 95

C.4.1 Všeobecne ... 95
C.4.2 Výpočet $MTTF_D$ pre komponenty z B_{10D} ... 96
C.4.3 Vysvetlenie vzorcov ... 96
C.4.4 Príklad ... 97
C.5 Údaje $MTTF_D$ elektronických komponentov ... 97
C.5.1 Všeobecne ... 97
C.5.2 Polovodiče ... 98
C.5.3 Pasívne komponenty ... 99

Príloha D (informatívna) – Zjednodušená metóda na odhad $MTTF_D$ pre každý kanál ... 101
D.1 Metóda počítania dielov ... 101
D.2 $MTTF_D$ pre rôzne kanály, symetrizácia $MTTF_D$ pre každý kanál ... 102

Príloha E (informatívna) – Odhady pre diagnostické pokrytie (DC) pre funkcie a podsystémy ... 103
E.1 Príklady diagnostického pokrytia (DC) ... 103
E.2 Odhad priemerného diagnostického pokrytia ... 106

Príloha F (informatívna) – Metóda kvantifikácie opatrení proti poruchám so spoločnou príčinou (CCF) ... 107
F.1 Všeobecne ... 107
F.2 Odhad účinku opatrení proti CCF ... 107
F.3 Opis opatrení proti poruche so spoločnou príčinou (CCF) v tabuľke F.1 ... 108
F.3.1 Separácia/segregácia ... 108
F.3.2 Rozmanitosť ... 108
F.3.3 Návrh/aplikácia/skúsenosti ... 109
F.3.4 Posudzovanie/analýza ... 109
F.3.5 Školenie ... 109
F.3.6 Životné prostredie ... 109
F.4 Opatrenia proti poruche so spoločnou príčinou (CCF) a iné príslušné normy ... 110

Príloha G (informatívna) – Systematická porucha ... 111
G.1 Všeobecne ... 111
G.2 Opatrenia na riadenie systematických porúch ... 111
G.3 Opatrenia na zabránenie systematickým poruchám počas návrhu SRP/CS ... 112
G.4 Opatrenia na predchádzanie systematickým poruchám počas integrácie SRP/CS ... 112
G.5 Manažérstvo funkčnej bezpečnosti ... 113

Príloha H (informatívna) – Príklad kombinácie viacerých podsystémov ... 114

Príloha I (informatívna) – Príklady pre zjednodušený postup odhadu PL podsystémov ... 117
I.1 Všeobecne ... 117
I.2 Bezpečnostná funkcia a požadovaná úroveň výkonnosti (PL_r) ... 117
I.3 Príklad A – Jednokanálový systém ... 118
I.3.1 Identifikácia bezpečnostných častí ... 118

I.3.2 Kvantifikácia $MTTF_D$, DC_{avg}, opatrenia proti CCF, kategórie a úrovne výkonnosti 119
I.4 Príklad B – Redundantný systém 120
I.4.1 Identifikácia bezpečnostných častí 120
I.4.2 Kvantifikácia $MTTF_D$ pre každý kanál, priemerné diagnostické pokrytie, opatrenia proti CCF, kategória a úroveň výkonnosti 122

Príloha J (informatívna) – Príklad realizácie SRESW 126
J.1 Popis príkladu 126
J.2 Aplikácia V-modelu životného cyklu bezpečnosti softvéru 126
J.3 Overenie špecifikácie softvéru na rôznych úrovniach (t. j. SDS, SSDS, MDS) 128
J.4 Príklad pravidiel programovania 129

Príloha K (informatívna) – Číselné znázornenie na obrázku 12 130

Príloha L (informatívna) – Odolnosť proti elektromagnetickému rušeniu (EMI) 134

Príloha M (informatívna) – Ďalšie informácie pre špecifikáciu bezpečnostných požiadaviek (SRS) 138

Príloha N (informatívna) – Vyhýbanie sa systematickej poruche pri návrhu softvéru 141
N.1 Výber opatrení na predchádzanie poruchových stavov pri návrhu softvéru súvisiaceho s bezpečnosťou 141
N.2 Príklad na validáciu softvéru 148
N.2.1 Všeobecne 148
N.2.2 Pokyny pre kódovanie 148
N.2.3 Špecifikácia bezpečnostných funkcií 148
N.2.4 Vstupné informácie zo špecifikácie hardvérového návrhu 149
N.2.5 Aplikačný program 151
N.2.6 Validácia implementovaného SRASW 152

Príloha O (informatívna) – Hodnoty súvisiace s bezpečnosťou komponentov alebo častí riadiacich systémov 162
O.1 Definícia typov zariadení 162
O.1.1 Všeobecne 162
O.1.2 Typ zariadenia 1 163
O.1.3 Typ zariadenia 2 163
O.1.4 Typ zariadenia 3 163
O.1.5 Typ zariadenia 4 163
O.2 Ďalšie informácie 164
O.2.1 Softvér 164
O.2.2 Základné bezpečnostné princípy 164
O.2.3 Osvedčené bezpečnostné princípy 164

Príloha ZA (informatívna) – Vzťah medzi touto európskou normou a základnými požiadavkami smernice EÚ 2006/42/ES, na ktoré sa má vzťahovať 165

Literatúra 168

Európsky predhovor

Tento dokument (EN ISO 13849-1: 2023) vypracovala technická komisia ISO/TC 199 *Bezpečnosť strojov* v spolupráci s technickou komisiou CEN/TC 114 *Bezpečnosť strojov,* ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskôr do novembra 2023 a národné normy, ktoré sú s ňou v rozpore, sa musia zrušiť najneskôr do mája 2026.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN nezodpovedá za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Tento dokument nahrádza EN ISO 13849-1: 2015.

Tento dokument sa vypracoval na základe žiadosti o normalizačnú prácu, ktorú CEN predložila Európska komisia a Európske združenie voľného obchodu, aby sa podporili základné požiadavky smernice (smerníc).

Vzťah k smernici (smerniciam) EÚ sa uvádza v informatívnej prílohe ZA, ktorá je neoddeliteľnou súčasťou tohto dokumentu.

Akákoľvek spätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu/národnej technickej komisii používateľov. Kompletný zoznam týchto orgánov je na webovom sídle CEN.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text ISO 13849-1: 2023 schválil CEN ako EN ISO 13849-1: 2023 bez akýchkoľvek modifikácií.

Úvod

Štruktúra bezpečnostných noriem v oblasti strojových zariadení je nasledovná:

a) Normy typu A (základné normy) uvádzajú základné pojmy, zásady navrhovania a všeobecné aspekty, ktoré možno uplatniť na strojové zariadenia.

b) Normy typu B (všeobecné bezpečnostné normy) sa zaoberajú jedným alebo viacerými bezpečnostnými aspektmi alebo jedným alebo viacerými typmi bezpečnostných zariadení, ktoré možno použiť v širokom rozsahu strojových zariadení:

   – normy typu B1 týkajúce sa konkrétnych bezpečnostných aspektov (napr. bezpečnostné vzdialenosti, povrchová teplota, hluk);

   – normy typu B2 týkajúce sa bezpečnostných zariadení (napr. dvojručné ovládanie, blokovacie zariadenia, zariadenia citlivé na tlak, ochranné kryty).

c) Normy typu C (bezpečnostné normy pre strojové zariadenia) sa zaoberajú podrobnými bezpečnostnými požiadavkami pre konkrétny stroj alebo skupinu strojov.

Tento dokument je normou typu B1 podľa definície v norme ISO 12100: 2010.

Prvé vydanie tohto dokumentu bolo uverejnené v roku 1999 na základe normy EN 954-1: 1996 (zrušená norma). Druhé vydanie bolo revidované v roku 2006 a tretie vydanie bolo revidované v roku 2015.

Tento dokument má význam najmä pre nasledujúce skupiny zainteresovaných strán, pokiaľ ide o bezpečnosť strojových zariadení:

– výrobcov strojov (malé, stredné a veľké podniky);

– orgány na ochranu zdravia a bezpečnosti (regulačné orgány, organizácie na prevenciu nehôd, trhový dohľad).

Ostatné subjekty môžu byť ovplyvnené úrovňou bezpečnosti strojových zariadení dosiahnutou pomocou tohto dokumentu:

– používatelia strojov/zamestnávatelia (malé, stredné a veľké podniky);

– používatelia strojov/zamestnanci (napr. odbory);

– poskytovatelia služieb, napr. v oblasti údržby (malé, stredné a veľké podniky);

– spotrebitelia (t. j. stroje určené na používanie spotrebiteľmi).

Vyššie uvedené skupiny zainteresovaných strán mali možnosť zúčastniť sa na procese vypracovania tohto dokumentu.

Okrem toho je tento dokument určený pre normalizačné orgány, ktoré vypracúvajú normy typu C, ako sú definované v norme ISO 12100: 2010.

Požiadavky tohto dokumentu môžu byť doplnené alebo upravené normou typu C.

V prípade strojov, na ktoré sa vzťahuje rozsah pôsobnosti normy typu C a ktoré boli navrhnuté a vyrobené podľa požiadaviek tejto normy, majú požiadavky tejto normy typu C prednosť.

POZNÁMKA 1. – Príklady a základ väčšiny obsahu sú založené na stacionárnych strojoch v továrenských aplikáciách. Nie sú však vylúčené ani iné stroje. Tento dokument bol napísaný bez toho, aby sa zohľadnilo, či určité strojové zariadenia (napr. mobilné strojové zariadenia) majú špecifické požiadavky. Tento dokument je však určený na použitie v mnohých odvetviach strojárstva a ako základ pre tvorcov noriem typu C, pokiaľ je to uplatniteľné.

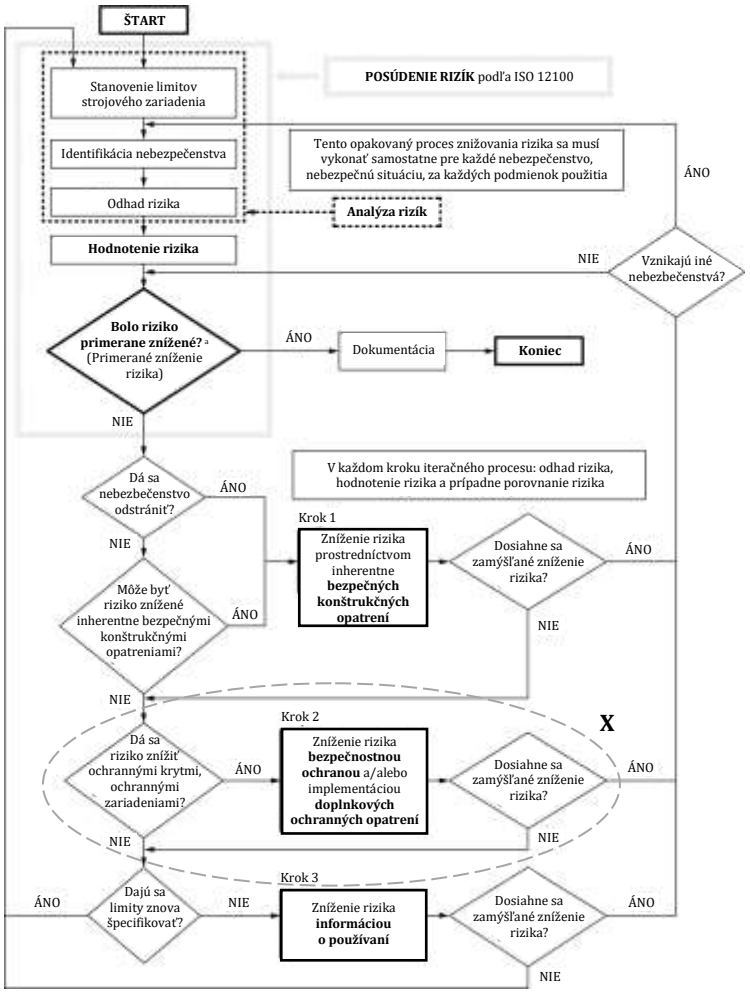
Tento dokument má poskytnúť usmernenie tým, ktorí sa podieľajú na návrhu a posudzovaní riadiacich systémov, a tým, ktorí pripravujú normy typu B2 alebo typu C.

Zníženie rizika podľa normy ISO 12100: 2010, kapitola 6, sa dosahuje uplatnením v nasledujúcom poradí inherentne bezpečných konštrukčných opatrení, ochranných a/alebo doplnkových opatrení na zníženie rizika a informácií na použitie. Projektant môže znížiť riziká pomocou opatrení na zníženie rizika, ktoré môžu mať bezpečnostné funkcie. Časti riadiacich systémov strojových zariadení, ktoré sú určené na poskytovanie bezpečnostných funkcií, sa nazývajú bezpečnostné časti riadiacich systémov (SRP/CS). Môžu pozostávať z hardvéru alebo kombinácie hardvéru a softvéru a môžu byť buď oddelené od riadiaceho systému stroja, alebo jeho neoddeliteľnou súčasťou. Okrem realizácie bezpečnostných funkcií môžu SRP/CS realizovať aj prevádzkové funkcie.

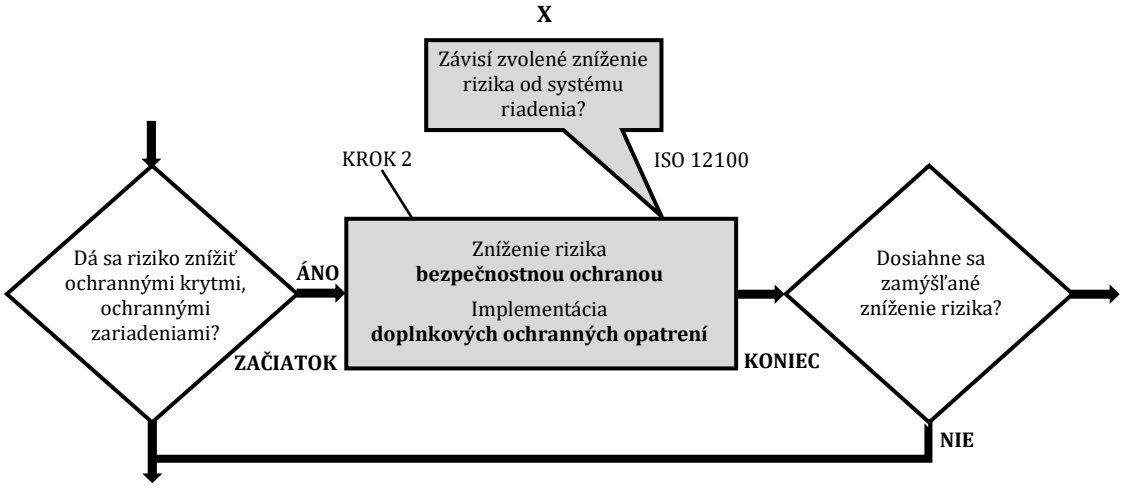
Na posúdenie rizika stroja sa používa norma ISO 12100: 2010. Príloha A tohto dokumentu sa môže použiť na určenie požadovanej úrovne výkonnosti (PL_r) bezpečnostnej funkcie vykonávanej SRP/CS, ak jej PL_r nie je špecifikovaná v platnej norme typu C. Tento dokument je relevantný pre bezpečnostné funkcie SRP/CS, ktoré sa používajú na riešenie rizík pre prípady, keď sa na základe posúdenia rizika vykonaného podľa normy ISO 12100: 2010 zistí, že je potrebné opatrenie na zníženie rizika, ktoré sa opiera o bezpečnostnú funkciu (napr. ochranný kryt s blokovaním). V týchto prípadoch riadiaci systém súvisiaci s bezpečnosťou vykonáva bezpečnostnú funkciu. Tento dokument je určený na použitie pri navrhovaní a hodnotení SRP/CS. Do predmetu tohto dokumentu patrí len tá časť riadiaceho systému, ktorá súvisí s bezpečnosťou.

Obrázok 1 znázorňuje vzťah medzi normou ISO 12100: 2010 a týmto dokumentom. Podrobný prehľad je uvedený na obrázku 2.

POZNÁMKA 2. – Ďalšie informácie sa nachádzajú aj v ISO/TR 22100-2: 2013.



[a] Prvýkrát je otázka zodpovedaná prvotným posúdením rizika. Pre ďalšie informácie pozri obrázok A.1.



POZNÁMKA. – Na základe ISO/TR 22100-2: 2013, obrázok 2.

Obrázok 1 – Integrácia tohto dokumentu (ISO 13849-1) do procesu znižovania rizík podľa normy ISO 12100: 2010

POZNÁMKA 3. – Na obrázku 1 je znázornené, kde SRP/CS prispieva k procesu znižovania rizík podľa normy ISO 12100: 2010: Krok 2. SRP/CS podporuje kombinované opatrenia na znižovanie rizík prostredníctvom implementácie bezpečnostných funkcií. Schopnosti bezpečnostných častí riadiacich systémov vykonávať bezpečnostnú funkciu za predvídateľných podmienok je pridelená jedna z piatich úrovní, ktoré sa nazývajú úrovne výkonnosti (PL). Požadovaná úroveň výkonnosti (PL_r) pre konkrétnu bezpečnostnú funkciu (v závislosti od požadovaného zníženia rizika) sa určí odhadom rizika.

Informatívna príloha A tohto dokumentu obsahuje metódu odhadu rizika a môže sa použiť na určenie PL_r bezpečnostnej funkcie vykonávanej SRP/CS. Každá metóda odhadu rizika bude vykazovať odchýlku z dôvodu subjektívnej povahy hodnotiacich kritérií. V porovnaní s prílohou A môžu mať normy typu C špecifickejšie metódy odhadu rizika pre konkrétne strojové aplikácie.

Frekvencia nebezpečnej poruchy bezpečnostnej funkcie závisí od viacerých faktorov, okrem iného od hardvérovej a softvérovej štruktúry, rozsahu mechanizmov na zisťovanie porúch [diagnostické pokrytie (DC)], spoľahlivosti komponentov [stredný čas do nebezpečnej poruchy ($MTTF_D$), poruchy so spoločnou príčinou (CCF)], procesu návrhu, prevádzkového zaťaženia, podmienok prostredia a prevádzkových postupov.

S cieľom uľahčiť návrh SRP/CS a posúdenie dosiahnutej PL, sa v tomto dokumente používa metodika založená na kategorizácii architektúr so špecifickými kritériami návrhu (napr. $MTTF_D$, DC_{avg}) a špecifikovaným správaním v podmienkach poruchy. Týmto architektúram je pridelená jedna z piatich úrovní označovaných ako kategórie B, 1, 2, 3 a 4.

Funkčná bezpečnosť zohľadňuje charakteristiky porúch prvkov/komponentov vykonávajúcich bezpečnostnú funkciu. Pre každú bezpečnostnú funkciu je táto charakteristika porúch vyjadrená ako frekvencia výskytu nebezpečnej poruchy za hodinu (PFH).

Úrovne a kategórie výkonnosti sa môžu uplatniť na SRP/CS, napr.:

- riadiace jednotky (napr. logická jednotka pre riadiace funkcie, spracovanie údajov, monitorovanie);
- elektrocitlivé ochranné zariadenia (napr. fotoelektrické bariéry), zariadenia citlivé na tlak.

Úrovne výkonnosti možno definovať a kategórie určiť pre podsystémy SRP/CS s použitím bezpečnostných častí (komponentov), napr.:

- ochranné zariadenia (napr. dvojručné ovládacie zariadenia, blokovacie zariadenia);
- riadiace prvky výkonu (napr. relé, ventily);
- snímače a prvky HMI (napr. snímače polohy, aktivačný snímač).

Strojové zariadenia, na ktoré sa vzťahuje tento dokument, môžu byť od jednoduchých (napr. malé kuchynské stroje alebo automatické dvere a brány) až po zložité (napr. baliace stroje, tlačiarenské stroje, lisy a stroje integrované do systému).

Tento dokument aj norma IEC 62061 špecifikujú metodiku a poskytujú súvisiace pokyny na návrh a realizáciu riadiacich systémov strojových zariadení súvisiacich s bezpečnosťou.

Požiadavky uvedené v kapitole 10 tohto dokumentu nahrádzajú požiadavky normy ISO 13849-2: 2012 (okrem informatívnych príloh).

1 Predmet

Tento dokument špecifikuje metodiku a poskytuje súvisiace požiadavky, odporúčania a usmernenia na návrh a integráciu bezpečnostných častí riadiacich systémov (SRP/CS), ktoré vykonávajú bezpečnostné funkcie, vrátane návrhu softvéru.

Tento dokument sa vzťahuje na SRP/CS pre režimy s vysokým dopytom a nepretržité prevádzkové režimy vrátane ich podsystémov bez ohľadu na typ technológie a energie (napr. elektrickej, hydraulickej, pneumatickej a mechanickej). Tento dokument sa nevzťahuje na režim prevádzky s nízkym dopytom.

POZNÁMKA 1. – Pre režim prevádzky s nízkym dopytom pozri 3.1.44 a súbor IEC 61508.

Tento dokument nešpecifikuje bezpečnostné funkcie alebo požadované úrovne výkonnosti (PL_r), ktoré sa majú používať v konkrétnych aplikáciách.

POZNÁMKA 2. – Tento dokument špecifikuje metodiku návrhu SRP/CS bez toho, aby sa zohľadnilo, či určité strojové zariadenia (napr. mobilné strojové zariadenia) majú špecifické požiadavky. Tieto špecifické požiadavky možno zohľadniť v norme typu C.

Tento dokument neuvádza špecifické požiadavky na návrh výrobkov/komponentov, ktoré sú súčasťou SRP/CS. Špecifické požiadavky na konštrukciu niektorých komponentov SRP/CS sú zahrnuté v platných normách ISO a IEC.

Tento dokument neposkytuje špecifické opatrenia pre bezpečnostné aspekty (napr. fyzická bezpečnosť, bezpečnosť IT, kybernetická bezpečnosť).

POZNÁMKA 3. – Bezpečnostné otázky môžu mať vplyv na bezpečnostné funkcie. Ďalšie informácie sú uvedené v ISO/TR 22100-4 a IEC/TR 63074.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO 12100: 2010 *Safety of machinery – General principles for design – Risk assessment and risk reduction.* [Bezpečnosť strojov. Všeobecné zásady konštruovania strojov. Posudzovanie a znižovanie rizika.]

ISO 13849-2: 2012 *Safety of machinery – Safety-related parts of control systems – Part 2: Validation.* [Bezpečnosť strojov. Bezpečnostné časti riadiacich systémov. Časť 2: Validácia.]

ISO 13855: 2010 *Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body.* [Bezpečnosť strojov. Umiestnenie ochranných zariadení so zreteľom na rýchlosť približujúcich sa častí ľudského tela.]

ISO 20607: 2019 *Safety of machinery – Instruction handbook – General drafting principles.* [Bezpečnosť strojov. Návod na používanie. Všeobecné zásady tvorby.]

IEC 61508-3: 2010 *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements.* [Funkčná bezpečnosť elektrických/elektronických/programovateľných elektronických bezpečnostných systémov. Časť 3: Požiadavky na programové vybavenie.]

IEC 62046: 2018 *Safety of machinery – Application of protective equipment to detect the presence of persons.* [Bezpečnosť strojových zariadení. Aplikácia ochranných zariadení na detekciu prítomnosti osôb.]

IEC 62061: 2021 *Safety of machinery – Functional safety of safety-related control systems.* [Bezpečnosť strojov. Funkčná bezpečnosť bezpečnostných riadiacich systémov.]

IEC/IEEE 82079-1: 2019 *Preparation of information for use (instructions for use) of products – Part 1: Principles and general requirements.* [Príprava informácií na používanie (návodu na používanie) výrobkov. Časť 1: Zásady a všeobecné požiadavky.]