

Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností

**ČSN
EN 62061
OPRAVA 1
33 2208**

idt IEC 62061:2005/Cor.2:2008-04

Corrigendum

Tato oprava ČSN EN 62061:2005 je českou verzí opravy IEC 62061:2005/Cor.2:2008-04. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This Corrigendum to ČSN EN 62061:2005 is the Czech version of the Corrigendum IEC 62061:2005/Cor.2:2008-04. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

ČSN EN 62061 (33 2208) Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností z listopadu 2005 se opravuje takto:

3.2 Termíny a definice

Vypouští se poznámka k definici 3.2.41: bezpečná porucha.

Nahrazuje se tabulka 5 takto:

Tabulka 5 – Omezení architektury na subsystemy: maximální SIL, kterou lze uplatňovat pro SRCF využívající tento subsystem

Podíl bezpečných poruch	Odolnost proti vadám hardwaru (viz poznámka 1)		
	0	1	2
< 60 %	není dovoleno (výjimky viz poznámka 3)	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (viz poznámka 2)
≥ 99 %	SIL3	SIL3 (viz poznámka 2)	SIL3 (viz poznámka 2)

POZNÁMKA 1 Odolnost proti vadám hardwaru N znamená, že $N + 1$ poruchových stavů způsobí ztrátu řídicí funkce související s bezpečností.

POZNÁMKA 2 V této normě se s úrovní SIL 4 neuvažuje. SIL 4 – viz IEC 61508-1.

POZNÁMKA 3 Viz 6.7.6.4 nebo subsystemy, kde nebyly uvažovány poruchové stavy, které by mohly způsobit nebezpečnou poruchu, viz 6.7.7.

V kapitole 6 se doplňuje nový článek 6.7.6.4 takto:

6.7.6.4 Elektromechanické subsystémy, které mají podíl bezpečných poruch menší než 60 % a nulovou odolnost proti vadám hardwaru, které používají osvědčené součásti (viz poznámka) v souladu s PLC kategorie 1 podle ISO 13849-1:2006, se pokládají za dosahující SILCL SIL1.

POZNÁMKA Osvědčenou součástí pro bezpečnostní použití je součást, která byla:

- a) v minulosti značnou měrou úspěšně používána v podobných aplikacích, nebo
- b) vyrobena a ověřena podle zásad, které prokazují její vhodnost a spolehlivost pro bezpečnostní aplikace.

Přečíslovává se 6.7.6.4 takto:

6.7.6.5 Tam, kde je subsystém navržen podle ISO 13849-1:1999 a potvrzena jeho platnost (validace) podle ISO 13849-2:2003, může být uplatněn následující vztah v kontextu se samotným omezením architektury podle tabulky 6. Předpokládá se, že subsystém určité kategorie odpovídající ISO 13849-1 má odpovídající odolnost proti vadám hardwaru a podíl bezpečných poruch, jak je uvedeno v tabulce 6.

POZNÁMKA Pro dosažení požadované SIL je také nutné splnit požadavky týkající se pravděpodobnosti nebezpečné poruchy a systematické integrity bezpečnosti.

Nahrazuje se tabulka 6 takto:

Tabulka 6 – Omezení architektury: SILCL ve vztahu ke kategoriím

Kategorie	Odolnost proti vadám hardwaru	SFF	Maximální dosažitelná mez SIL podle omezení architektury
	Předpokládá se, že subsystémy se stanovenou kategorií mají níže uvedené charakteristiky		
1	0	< 60 %	Viz poznámka 1
2	0	60 % – 90 %	SIL 1 (viz poznámka 2)
3	1	< 60 %	SIL 1
	1	60 % – 90 %	SIL 2
4	> 1	60 % – 90 %	SIL 3 (viz poznámka 3)
	1	> 90 %	SIL 3 (viz poznámka 4)

POZNÁMKA 1 Předpokládá se, že subsystémy, které mají SFF < 60 %, ale jsou navrženy v souladu s kategorií 1 podle ISO 13849-1:1999 a je potvrzena jejich platnost (validace) podle ISO 13849-2:2003, budou dosahovat SILCL SIL 1.

POZNÁMKA 2 Předpokládá se, že případ kategorie 2, kde SFF je > 90 %, nebude dosažen konstrukčními požadavky z ISO 13849-1:1999.

POZNÁMKA 3 Předpokládá se, že diagnostické pokrytí je pro subsystémy kategorie 4, u nichž se uvažuje s větší odolností než proti jednotlivé vadě hardwaru (tzn. akumulovaným vadám), menší než 90 %.

POZNÁMKA 4 U kategorie 4 se v případě odolnosti proti jednotlivé vadě hardwaru požaduje SFF větší než 90 %, ale menší než 99 %.

POZNÁMKA 5 Kategorie B podle ISO 13849-1:1999 se nepovažuje za postačující pro dosažení SIL 1.

Mění se poznámka k 6.7.7.3 takto:

POZNÁMKA Je dovoleno neuvažovat poruchové stavy v souladu s 3.3 a D.5 z ISO 13849-2:2003.

Mění se 6.7.8.1.6 a tabulka 7 takto:

6.7.8.1.6 Tam, kde je navržen jednoduchý subsystém podle ISO 13849-1:1999 a potvrzena platnost (validace) podle ISO 13849-2:2003 a také splňuje požadavky omezení architektury (viz 6.7.6) a systematické integrity bezpečnosti (viz 6.7.9), je možné pro odhad integrity bezpečnosti hardwaru (viz 6.6.3.2) použít prahové hodnoty pravděpodobnosti nebezpečné poruchy (PFH_D) uvedené v tabulce 7.

Tabulka 7 – Pravděpodobnosti nebezpečné poruchy

Kategorie	Odolnost proti vadám hardwaru	DC	Prahové hodnoty PFH_D (za hodinu), které je pro subsystém možné vyžadovat
	Předpokládá se, že subsystémy se stanovenou kategorií mají dále uvedené charakteristiky		PFH_D ($MTTF_{\text{subsystém}}, T_{\text{test}}, DC$) (viz poznámka 1)
1	0	0 %	Poskytuje dodavatel nebo se použijí obecně dostupná data (viz příloha D)
2	0	60 % – 90 %	$\geq 10^{-6}$
3	1	60 % – 90 %	$\geq 2 \times 10^{-7}$
4	> 1	60 % – 90 %	$\geq 3 \times 10^{-8}$
	1	> 90 %	$\geq 3 \times 10^{-8}$

POZNÁMKA 1 Prahová hodnota PFH_D je funkcí MTTF subsystému (odvozenou výrobcem subsystému nebo z příslušných manuálů součástí), doby zkušebního cyklu předepsaného ve specifikaci bezpečnostních požadavků (tato informace je také požadovaná pro potvrzení platnosti (validace) subsystému podle ISO 13849-2:2003, 3.5) a diagnostického pokrytí uvedeného v této tabulce (tyto hodnoty jsou založeny na požadavcích pro kategorie popsané v ISO 13849-1:1999).

POZNÁMKA 2 Kategorie B podle ISO 13849-1:1999 se nepovažuje za postačující pro dosažení SIL 1.

Mění se poznámka k 6.7.8.2.1 takto:

POZNÁMKA 2 V rovnicích (A) až (D) uvedených v 6.7.8.2 se předpokládají konstantní a dostatečně malé ($1 \gg \lambda \times T$) intenzity poruch (λ) prvků subsystému (to znamená, že střední doba do nebezpečné poruchy musí být mnohem větší než interval kontrolní zkoušky nebo doba života subsystému). Proto mohou být použity následující základní rovnice:

- $\lambda = 1/MTTF$, kde MTTF je vyjádřena v hodinách.

Pro elektromechanické přístroje je intenzita poruch určena pomocí hodnoty B_{10} a počtu provozních cyklů C (vyjádřeného jako počet provozních cyklů za hodinu) dané aplikace podle specifikace (viz 5.2.3).

- $\lambda = 0,1 \times C/B_{10}$

Příloha A: Určení SIL

Mění se třetí odstavec v A.2.4.1 takto:

Mělo by také být možné předvídat dobu trvání ohrožení, např. pokud bude delší než 10 min. Tam, kde je doba trvání ohrožení kratší než 10 min, může být hodnota snížena na číslo v daném řádku v tabulce A.2 uvedené níže. To neplatí pro četnost ohrožení ≤ 1 h, která by neměla být nikdy snížena.

Mění se tabulka A.2 takto:

Tabulka A.2 – Třídy četnosti a doby trvání ohrožení (Fr)

Četnost a doba trvání ohrožení (Fr)	
Četnost ohrožení	Četnost Fr (viz A.2.4.1)
≤ 1 za h	5
< 1 za h až ≥ 1 za den	5
< 1 za den až ≥ 1 za 2 týdny	4
< 1 za 2 týdny až ≥ 1 za rok	3
< 1 za rok	2

Mění se tabulka A.6 takto:

Tabulka A.6 – Matice určení SIL

Závažnost (Se)	Třída (Cl)				
	4	5–7	8–10	11–13	14–15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Mění se obrázek A.3 takto:

Příloha F: Metodika pro odhad citlivosti na rušení společnou poruchou (CCF)

Mění se tabulka F.2 takto:

Tabulka F.2 – Odhad součinitele CFF (β)

Celkové bodové hodnocení	Součinitel společné poruchy (β)
≤ 35	10 % (0,1)
36 – 65	5 % (0,05)
66 – 85	2 % (0,02)
86 – 100	1 % (0,01)

Mění se vzorec (D.2)

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_{De}$$

Vypracování opravy normy

Zpracovatel: Ing. František Valenta, ELVAM, IČ 66051649

Technická normalizační komise: TNK 22 Elektrotechnické předpisy

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Viera Borošová

U p o z o r n ě n í : Změny a doplňky, jakož i zprávy o nově vydaných normách jsou uveřejňovány ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 62061 OPRAVA 1

Vydal Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, Praha
Rok vydání 2009, 8 stran

84188 Cenová skupina 998

