

ČESKÁ TECHNICKÁ NORMA

ICS 25.040.40; 29.020 **Únor 2011**

**Funkční bezpečnost elektrických/elektronických/
programovatelných elektronických systémů souvisejících
s bezpečností -
Část 4: Definice a zkratky**

ČSN
EN 61508- 4
ed. 2
18 0301

idt IEC 61508- 4:2010

Functional safety of electrical/electronic/programmable electronic safety related systems –
Part 4: Definitions and abbreviations

Sécurité fonctionnelle des systemes électriques/électroniques/électroniques programmables relatifs
a la sécurité –
Partie 4: Définitions et abréviations

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer
elektronischer Systeme –
Teil 4: Begriffe und Abkürzungen

Tato norma je českou verzí evropské normy EN 61508- 4:2010. 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 61508- 4:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

S účinností od 2013-05-01 se nahrazuje ČSN EN 61508- 4 (18 0301) ze září 2002, která do uvedeného data platí souběžně s touto normou.

Národní předmluva

Upozornění na používání této normy

Souběžně s touto normou se může do 2013-05-01 používat dosud platná ČSN EN 61508-4 (18 0301) ze září 2002, v souladu s předmluvou k EN 61508- 4:2010.

Změny proti předchozím normám

Toto vydání obsahuje celkovou revizi a obsahuje řadu připomínek získaných v průběhu celého projednávání.

Informace o citovaných normativních dokumentech

IEC Guide 104:1997 nezaveden

ISO/IEC Guide 51:1999 nezaveden

Informativní údaje z IEC 61508- 4:2010

Mezinárodní norma IEC 61508- 4 byla připravena subkomisí SC 65A: Systémová hlediska, technické komise IEC TC 65: Měření a řízení průmyslových procesů.

Toto druhé vydání ruší a nahrazuje první vydání publikované v roce 1998. Toto vydání představuje jeho technickou revizi.

Toto vydání bylo podrobena celkové revizi a obsahuje řadu připomínek přijatých v průběhu celé revize.

Norma má status základní bezpečnostní publikace podle IEC Guide 104.

Text této normy vychází z těchto dokumentů:

FDIS
65A/551/FDIS

Zpráva o hlasování
65A/575/RVD

Úplné informace o hlasování při schvalování této normy je možné nalézt ve zprávě o hlasování uvedené v tabulce.

Tato publikace byla vypracována podle Směrnice ISO/IEC, Část 2.

Seznam všech částí souboru IEC 61508 publikovaných pod společným názvem *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností* je možno nalézt na webových stránkách IEC.

Komise rozhodla, že obsah této publikace se nebude měnit až do konečného data vyznačeného na internetové adrese IEC <http://webstore.iec.ch> v termínu příslušejícímu dané publikaci. Po tomto datu bude publikace buď

- znovu potvrzena;
- zrušena;
- nahrazena revidovaným vydáním nebo
- změněna.

Vypracování normy

Zpracovatel: Ing. Jiří Šplíchal – SEL, IČ 18664075, Ing. Jiří Šplíchal

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Tomáš Pech

EVROPSKÁ NORMA EN 61508- 4

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM Květen 2010

Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností -

Část 4: Definice a zkratky

(IEC 61508- 4:2010)

Functional safety of electrical/electronic/programmable electronic safety related systems -

Part 4: Definitions and abbreviations

(IEC 61508- 4:2010)

Sécurité fonctionnelle des systèmes

électriques/électroniques/électroniques programmables relatifs à la sécurité -

Partie 4: Définitions et abréviations

(CEI 61508- 4:2010)

Funktionale Sicherheit sicherheitsbezogener

elektrischer/elektronischer/programmierbarer elektronischer Systeme -

Teil 4: Begriffe und Abkürzungen

(IEC 61508- 4:2010)

Tato evropská norma byla schválena CENELEC 2010-05-01. Členové CENELEC 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 Ústředním sekretariátu nebo u kteréhokoliv člena CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Ústřednímu sekretariátu, má stejný status jako oficiální verze.

CENELEC

Evropský výbor pro normalizaci v elektrotechnice

European Committee for Electrotechnical Standardization

Comité Européen de Normalisation Electrotechnique

Europäisches Komitee für Elektrotechnische Normung

Řídící centrum: Avenue Marnix 17, B-1000 Brusel

© 2010 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmikoli prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN 61508-4:2010 E

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, 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 a Švýcarska.

Předmluva

Text dokumentu 65A/551/FDIS, budoucí druhé vydání IEC 61508-4 vypracovaný v subkomisi SC 65A, Systémová hlediska, technické komise IEC TC 65 Měření a řízení průmyslových procesů, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 61508-4 dne 2010-05-01.

Tato evropská norma nahrazuje EN 61508-4:2001.

Norma má status základní bezpečnostní publikace podle IEC Guide 104.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN a CENELEC nelze činit odpovědnými za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Byla stanovena tato data:

- nejzazší datum zavedení EN na národní úrovni vydáním identické národní normy nebo vydáním oznámení o schválení EN k přímému používání jako normy národní
- nejzazší datum zrušení národních norem, které jsou s EN v rozporu

(dop) 2011-02-01

(dow) 2013-05-01

Přílohu ZA doplnil CENELEC.

Oznámení o schválení

Text mezinárodní normy IEC 61508-4:2010 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod 6

1 Rozsah platnosti 8

2 Citované normativní dokumenty 10

3 Definice a zkratky 10

3.1 Termíny týkající se bezpečnosti 11

3.2 Zařízení a vybavení 13

3.3 Systémy: všeobecná hlediska 16

3.4 Systémy – hlediska související s bezpečností 18

3.5 Bezpečnostní funkce a integrita bezpečnosti 19

3.6 Vada, porucha a chyba (viz obrázek 4) 22

3.7 Činnosti životního cyklu 27

3.8 Potvrzení míry bezpečnosti 27

Bibliografie 31

Rejstřík 32

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace 35

Obrázek 1 – Celkový rámec souboru norem IEC 61508 9

Obrázek 2 – Programovatelný elektronický systém 16

Obrázek 3 – Elektrický/elektronický/programovatelný elektronický systém E/E/PE – struktura a terminologie 17

Obrázek 4 – Model poruch 23

Tabulka 1 – Zkratky použité v této normě 10

Úvod

Systémy obsahující elektrické a/nebo elektronické prvky se již řadu let používají ve většině aplikačních oblastech pro plnění bezpečnostních funkcí. Systémy založené na využití počítačů (obecně označované jako programovatelné elektronické systémy) se již používají ve všech aplikačních oblastech pro plnění jiných než bezpečnostních funkcí a ve stále větší míře také pro plnění funkcí bezpečnostních. Má-li být technika založená na počítačových systémech efektivně a bezpečně využívána, je nutné, aby osoby odpovědné za rozhodování měly pro rozhodnutí týkající se bezpečnostních hledisek dostatek informací a pokynů.

Tato mezinárodní norma stanovuje obecný přístup pro všechny životní cykly bezpečnosti systémů obsahujících elektrické a/nebo elektronické a/nebo programovatelné elektronické prvky (elektrické/elektronické/ programovatelné elektronické systémy (E/E/PE) a využívané pro zajišťování bezpečnostních funkcí. Tento sjednocený přístup byl přijat proto, aby se u všech elektrických systémů souvisejících s bezpečností používalo racionálního a konzistentního technického přístupu. Hlavním cílem je usnadnit tvorbu dalších aplikačních norem pro jednotlivé dílčí oblasti založenou na souboru IEC 61508.

POZNÁMKA 1 Příklady publikací a aplikační oblasti mezinárodních norem založených na souboru IEC 61508 jsou uvedeny v Bibliografii (viz odkazy [1], [2] a [3]).

Ve většině případů se bezpečnost zajišťuje prostřednictvím několika ochranných systémů založených na různých technických principech (např. mechanických, hydraulických, pneumatických, elektrických, elektronických, programovatelných elektronických). Jakákoliv bezpečnostní strategie proto musí počítat nejen se všemi prvky v rámci daného systému (např. senzory, řídicími zařízeními a akčními členy), ale také se všemi systémy s bezpečností souvisejícími, které dohromady tvoří celkovou sestavu systémů souvisejících s bezpečností. Proto může tato mezinárodní norma, přestože je zaměřena na elektrické/elektronické/programovatelné elektronické systémy (E/E/PE) související s bezpečností, poskytnout také určitý základní rámec, na jehož základě je možné posuzovat i systémy související s bezpečností založené na jiných technických principech.

Počítá se s velkou rozmanitostí aplikací systémů E/E/PE souvisejících s bezpečností v mnoha různých aplikačních oblastech a pokrývajících široký rozsah složitosti, nebezpečí i rizik. Vyžadovaná bezpečnostní opatření budou v každé konkrétní aplikaci záviset na mnoha faktorech, charakteristických pro danou aplikaci. Tato mezinárodní norma umožňuje, vzhledem ke svému obecnému charakteru, formulaci takových opatření v budoucích aplikačních mezinárodních normách a revizích těch, které již v současné době existují.

Tato mezinárodní norma

- počítá se všemi závažnými fázemi životního cyklu celkové bezpečnosti, bezpečnosti systému E/E/PE a bezpečnosti softwaru (např. od počáteční koncepce přes návrh, realizaci, provoz a údržbu až po vyřazení z provozu) při používání systémů E/E/PE pro plnění bezpečnostních funkcí;
- byla zpracována s ohledem na rychlý rozvoj techniky a její struktura je dostatečně pevná a obsažná, aby

umožnila další rozvoj;

- umožňuje tvorbu aplikačních mezinárodních norem týkajících se systémů E/E/PE souvisejících s bezpečností, tvorbu aplikačních mezinárodních norem koncipovaných v rámci této normy znamenající vyšší úroveň konzistence (např. z hlediska základních principů, terminologie atd.), jak v aplikačních oblastech, tak napříč těmito oblastmi. To bude mít jak bezpečnostní, tak ekonomický přínos;
- poskytuje metodu pro zpracování specifikace bezpečnostních požadavků nutných pro dosažení požadované funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností;
- pro stanovení požadavků na úroveň integrity bezpečnosti používá metody založené na riziku;
- zavádí úroveň integrity bezpečnosti pro specifikaci cílové úrovně integrity pro bezpečnostní funkce, které mají být použity v systémech E/E/PE souvisejících s bezpečností;

POZNÁMKA 2 Norma nestanovuje požadavky na úroveň integrity bezpečnosti ani nestanovuje, jak je úroveň integrity bezpečnosti určena. Místo toho poskytuje koncepční rámec založený na riziku a příklady technik.

- stanovuje cílové míry poruch pro bezpečnostní funkce plněné systémy E/E/PE souvisejícími s bezpečností, které jsou zaměřeny na úroveň integrity bezpečnosti;
- nastavuje nižší mez opatření cílových poruch pro bezpečnostní funkce vykonávané jedním systémem E/E/PE souvisejícím s bezpečností. Pro systémy E/E/PE související s bezpečností pracující
- v režimu provozu s nízkým vyžádáním (malou poptávkou) je dolní mez průměrné pravděpodobnosti nebezpečné poruchy na vyžádání stanovena na 10^{-5} ;
- v režimu provozu s vysokým nebo trvalým vyžádáním (poptávkou) je dolní mez stanovena na průměrnou pravděpodobnost nebezpečné poruchy na vyžádání 10^{-9} za hodinu;

POZNÁMKA 3 Jednotlivý systém E/E/PE související s bezpečností neznamena nutně jednokanálovou architekturu.

POZNÁMKA 4 Je možné dosáhnout návrhu systémů souvisejících s bezpečností s nižšími hodnotami cílové integrity bezpečnosti pro nekomplexní systémy, ale tyto meze mají ukázat, co je možné dosáhnout v současné době pro poměrně komplexní systémy (např. programovatelné elektronické systémy související s bezpečností).

- stanovuje požadavky, aby se bylo možno vyvarovat chyb a řídit systematické poruchy, které jsou založeny na zkušenosti a úsudku z praktické zkušenosti v průmyslu. I když pravděpodobnost vzniku systematické poruchy nemůže být obecně kvantifikována, může však norma požadovat, aby pro specifikovanou bezpečnostní funkci mohla být cílová protiporuchová opatření spojená s bezpečnostní funkcí dosažena, jestliže budou splněny všechny požadavky normy;
- zavádí systematickou schopnost, používanou na jakoukoliv součást tak, aby systematická integrita splňovala požadavky stanovené úrovní integrity bezpečnosti;
- přijímá široký rozsah principů, technik a opatření pro dosažení funkční bezpečnosti pro systémy E/E/PE související s bezpečností, ale nepoužívá výslovně koncepci „závady prostý“. Nicméně koncepce „závady prostý“ a „vnitřně bezpečný“ mohou být principiálně použitelné a použití takových principů je akceptovatelné, jestliže splňují požadavky příslušných článků normy.

1 Rozsah platnosti

1.1 Tato část IEC 61508 obsahuje definice a vysvětlení termínů použitých v částech 1 až 7 souboru norem IEC 61508.

1.2 Definice jsou seskupeny pod všeobecným záhlavím tak, aby termíny, které se k sobě vztahují, mohly být srozumitelné v kontextu k ostatním. Je však třeba poznamenat, že tato záhlaví nejsou určena k tomu, aby doplňovala význam těchto definic.

1.3 IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 jsou základní bezpečnostní publikace, ačkoliv se jejich status nepoužívá v kontextu malé komplexnosti k bezpečnostním systémům E/E/PE (viz 3.4.3 v IEC 61508-4). Jako základní bezpečnostní publikace jsou určeny pro používání technickými

komisemi při přípravě norem podle principů obsažených v IEC Guide 104 a ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 jsou také určeny pro používání jako samostatné publikace. Horizontální bezpečnostní funkce těchto mezinárodních norem se neuplatňují na lékařská zařízení, ve shodě se souborem IEC 60601.

1.4 Jedna z povinností technické komise je používat základní bezpečnostní publikace při přípravě svých publikací všude tam, kde je to použitelné. V této souvislosti se požadavky, zkušební metody a zkušební podmínky v základní bezpečnostní publikaci nepoužijí, pokud se specificky uvádějí nebo jsou do těchto publikací zahrnuty.

1.5 Obrázek 1 ukazuje celkový rámec souboru IEC 61508 a ukazuje roli, jakou hraje IEC 61508-4 ve snaze dosáhnout funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností.



Obrázek 1 - Celkový rámec souboru norem IEC 61508

Konec náhledu - text dále pokračuje v placené verzi ČSN.