

**Funkční bezpečnost elektrických/elektronických/
programovatelných elektronických systémů souvisejících
s bezpečností -
Část 2: Požadavky na elektrické/elektronické/ programovatelné
elektronické systémy související s bezpečností**

**ČSN
EN 61508-2**
ed. 2
18 0301

idt IEC 61508-2:2010

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Sécurité fonctionnelle des systemes électriques/électroniques/électroniques programmables relatifs
a la sécurité –
Part 2: Exigences pour les systemes électriques/électroniques/électroniques programmables relatifs
a la sécurité

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer
elektronischer Systeme –
Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare
elektronische Systeme

Tato norma je českou verzí evropské normy EN 61508-2:2010. 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 61508-2:2010. 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 61508-2 (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 61508-2 (18 0301)
ze září 2002, v souladu s předmluvou k EN 61508-2:2010.

Změny proti předchozím normám

Toto vydání bylo podrobeno důkladné revizi a zahrnuje množství připomínek přijatých v předešlých
stadiích revize.

Informace o citovaných normativních dokumentech

IEC 60947-5-1 zavedena v ČSN EN 60947-5-1 ed. 2 (35 4101) Spínací a řídicí přístroje nízkého napětí – Část 5-1: Přístroje a spínací ústrojí řídicích obvodů – Elektromechanické přístroje řídicích obvodů

[IEC/TS 61000-1-2](#) zavedena v ČSN IEC 61000-1-2 (33 3431) Elektromagnetická kompatibilita (EMC) – Část 1-2: Všeobecně – Metodika pro dosažení funkční bezpečnosti elektrického a elektronického zařízení s ohledem na elektromagnetické jevy

IEC 61326-3-1 zavedena v ČSN EN 61326-3-1 (35 6508) Elektrická měřicí, řídicí a laboratorní zařízení – Požadavky na EMC – Část 3-1: Požadavky na odolnost zařízení zajišťujících nebo určených k zajištění bezpečnosti příbuzných funkcí (funkční bezpečnost) – Všeobecné průmyslové aplikace

IEC 61508-1:2010 zavedena v ČSN EN 61508-1 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektro-nických/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky

IEC 61508-3:2010 zavedena v ČSN EN 61508-3 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektro-nických/programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software

IEC 61508-4:2010 zavedena v ČSN EN 61508-4 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektro-nických/programovatelných elektronických systémů souvisejících s bezpečností – Část 4: Definice a zkratky

IEC 61508-7:2010 zavedena v ČSN EN 61508-7 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektro-nických/programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření

IEC 61784-3 zavedena v ČSN EN 61784-3 (18 4001) Průmyslové komunikační sítě – Profily – Část 3: Funkční bezpečnost sběrnic pole

IEC 62280-1 nezavedena

IEC 62280-2 nezavedena

IEC Guide 104:1997 nezaveden

ISO/IEC Guide 51:1999 nezaveden

Informativní údaje z IEC 61508-2:2010

Mezinárodní norma byla vypracována subkomisí SC 65A Systémové aspekty, technické komise IEC TC 65 Měření, řízení a automatizace průmyslových procesů.

Toto druhé vydání zrušuje a nahrazuje první vydání vydané v roce 1998. Toto vydání je technickou revizí.

Toto vydání bylo podrobeno důkladné revizi a zahrnuje množství připomínek přijatých v předešlých

stadiích revize.

Má status základní bezpečnostní normy podle IEC Guide 104.

Text této normy vychází z těchto dokumentů:

FDIS
65A/549/FDIS

Zpráva o hlasování
65A/573/RVD

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

Tato publikace byla navržena v souladu se Směrnicemi ISO/IEC, Část 2.

Seznam všech částí souboru IEC 61508, vydaných pod všeobecným názvem *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností*, lze nalézt na internetové adrese IEC.

Komise rozhodla, že obsah základní publikace a jejích změn se nebude měnit až do výsledného data aktualizace uvedeného na internetové adrese IEC <http://webstore.iec.ch> v údajích o této publikaci. K tomuto datu bude publikace

- 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 61508-2
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Květen 2010

ICS 25.040 Nahrazuje EN 61508-2:2001

Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností –
Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností
(IEC 61508-2:2010)

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

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
(IEC 61508-2:2010)

Sécurité fonctionnelle des systèmes

électriques/électroniques/électroniques programmables relatifs à la sécurité –

Partie 2: Exigences pour les systèmes

électriques/électroniques/électroniques programmables relatifs à la sécurité

(CEI 61508-2:2010)

Funktionale Sicherheit sicherheitsbezogener

elektrischer/elektronischer/programmierbarer elektronischer Systeme –

Teil 2: Anforderungen an sicherheitsbezogene

elektrische/elektronische/programmierbare elektronische Systeme
(IEC 61508-2:2010)

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 kteréhokoli 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 jakýmkoli prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN 61508-2:2010 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/549/FDIS, budoucí vydání 2 IEC 61508-2, vypracovaný v subkomisi SC 65A Systémové aspekty, technické komise IEC TC 65 Měření, řízení a automatizace průmyslových procesů, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 61508-2 dne 2010-05-01.

Tato evropská norma nahrazuje EN 61508-2:2001.

Má status základní bezpečnostní normy podle IEC Guide 104.

Je třeba věnovat pozornost možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN a CENELEC nemohou být odpovědné za určení jakýchkoliv 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 61508-2:2010 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod 10

1 Rozsah platnosti 12

2 Citované normativní dokumenty 14

3 Definice a zkratky 15

4 Shoda s touto normou 15

5 Dokumentace 15

6 Management funkční bezpečnosti 15

7 Požadavky životního cyklu bezpečnosti systému E/E/PE 15

7.1 Všeobecně 15

7.1.1 Cíle a požadavky – všeobecně 15

7.1.2 Cíle 15

7.1.3 Požadavky 15

7.2 Specifikace požadavků návrhu systému E/E/PE 19

7.2.1 Cíl 19

7.2.2 Všeobecné požadavky 19

7.2.3 Specifikace požadavků návrhu systému E/E/PE 20

7.3 Plánování potvrzení platnosti bezpečnosti systému E/E/PE 21

7.3.1 Cíl 21

7.3.2 Požadavky 21

7.4 Návrh a vývoj systému E/E/PE 21

7.4.1	Cíl 22
7.4.2	Všeobecné požadavky 22
7.4.3	Syntéza prvků pro dosažení požadované systematické schopnosti 24
7.4.4	Architektonická omezení integrity bezpečnosti hardwaru 24
7.4.5	Požadavky na kvantifikaci vlivu náhodných hardwarových poruch 32
7.4.6	Požadavky pro předcházení systematickým chybám 34
7.4.7	Požadavky pro řízení systematických vad 34
7.4.8	Požadavky na chování systému při zjištění vady 35
7.4.9	Požadavky na realizaci systému E/E/PE 36
7.4.10	Požadavky pro prvky osvědčené v provozu 37
7.4.11	Doplňkové požadavky pro datové komunikace 38
7.5	Začlenění systému E/E/PE 39
7.5.1	Cíl 39
7.5.2	Požadavky 39
7.6	Postupy pro provoz a údržbu systému E/E/PE 40
7.6.1	Cíl 40
7.6.2	Požadavky 40
7.7	Ověření bezpečnosti systému E/E/PE 41
7.7.1	Cíl 41
7.7.2	Požadavky 41
7.8	Modifikace systému E/E/PE 42
7.8.1	Cíl 42
7.8.2	Požadavky 42
7.9	Ověření systému E/E/PE 43
7.9.1	Cíl 43
7.9.2	Požadavky 43
8	Odhad funkční bezpečnosti 44

Příloha A (normativní) Techniky a opatření pro systémy E/E/PE související s bezpečností – řízení poruch během provozu 45

Příloha B (normativní) Techniky a opatření pro systémy E/E/PE související s bezpečností – předcházení systematickým poruchám během různých fází životního cyklu 60

Příloha C (normativní) Diagnostické pokrytí a poměr bezpečných poruch 69

Příloha D (normativní) Příručka bezpečnosti pro vyhovující položky 71

Příloha E (normativní) Požadavky na speciální architekturu integrovaných obvodů (IO) s čipovou redundancí 73

Příloha F (informativní) Techniky a opatření pro ASIC – předcházení systematickým poruchám 78
Bibliografie 85

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace 86

Obrázek 1 – Celkový rámec souboru norem IEC 61508 13

Obrázek 2 – Životní cyklus bezpečnosti systému E/E/PE (ve fázi realizace) 16

Obrázek 3 – Vývoj životního cyklu ASIC (Model-V) 17

Obrázek 4 – Vztah mezi předmětem IEC 61508-2 a IEC 61508-3 17

Obrázek 5 – Určení maximální SIL pro specifikovanou architekturu (subsystém E/E/PE související s bezpečností složený z několika prvků v sérii , viz 7.4.4.2.3) 28

Obrázek 6 – Určení maximální SIL pro specifikovanou architekturu (subsystém E/E/PE související s bezpečností složený ze dvou subsystémů X a Y 30

Obrázek 7 – Architektura pro datovou komunikaci 39

Tabulka 1 – Fáze realizace životního cyklu bezpečnosti systému E/E/PE – Přehled 18

Tabulka 2 – Maximální dovolená úroveň integrity bezpečnosti pro bezpečnostní funkci prováděnou prvkem nebo subsystémem typu A souvisejícím s bezpečností 27

Tabulka 3 - Maximální dovolená úroveň integrity bezpečnosti pro bezpečnostní funkci prováděnou prvkem nebo subsystémem typu B souvisejícím s bezpečností 27

Tabulka A.1 – Vady nebo poruchy, které se mají předpokládat při kvantifikaci vlivu náhodných poruch hardwaru nebo se mají vzít v úvahu při odvozování poměru bezpečných poruch 47

Tabulka A.2 – Elektrické součásti 49

Tabulka A.3 – Elektrické součásti 49

Tabulka A.4 – Základní jednotky 50

Tabulka A.5 – Rozsah permanentní paměti 50

Tabulka A.6 – Rozsah proměnné paměti 51

Tabulka A.7 – Jednotky I/O (vstupů/výstupů) a rozhraní (vnější komunikace) 51

Tabulka A.8 – Datové cesty (vnitřní komunikace) 52

Tabulka A.9 – Napájení 52

Tabulka A.10 – Sekvence programů (hlídání) 53

Tabulka A.11 – Hodiny 53

Tabulka A.12 – Komunikace a velkokapacitní paměť 54

Tabulka A.13 – Senzory 54

Strana

Tabulka A.14 – Koncové prvky (akční členy) 55

Tabulka A.15 – Techniky a opatření pro řízení systematických poruch způsobených návrhem hardwaru 56

Tabulka A.16 – Techniky a opatření pro řízení systematických poruch způsobených namáháním nebo vlivy prostředí 57

Tabulka A.17 – Techniky a opatření pro řízení systematických provozních poruch 58

Tabulka A.18 – Účinnost technik a opatření pro řízení systematických poruch 59

Tabulka B.1 – Techniky a opatření pro předcházení chybám při specifikaci požadavků na návrh systému E/E/PE 61

Tabulka B.2 – Techniky a opatření pro předcházení chybám během návrhu a vývoje systému E/E/PE 62

Tabulka B.3 – Techniky a opatření pro předcházení chybám během začleňování systému E/E/PE 63

Tabulka B.4 – Techniky a opatření pro předcházení chybám a poruchám během provozních a údržbových postupů systému E/E/P 64

Tabulka B.5 – Techniky a opatření pro předcházení chybám během potvrzování platnosti bezpečnosti systému E/E/PE 65

Tabulka B.6 – Účinnost technik a opatření pro předcházení systematickým poruchám 66

Tabulka E.1 – Techniky a opatření zvyšující b_{B-IC} 76

Úvod

Systémy obsahující elektrické a/nebo elektronické součásti se již řadu let používají ve většině aplikačních oblastí pro plnění bezpečnostních funkcí. Systémy založené na využití počítačů (obecně nazývané 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 podrobně stanovuje obecný přístup pro všechny aktivity životního cyklu bezpečnosti systémů obsahujících elektrické a/nebo elektronické a/nebo programovatelné elektronické součásti (E/E/PE) 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) souvisejícími 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 v revizích norem, které již v současné době existují.

Tato mezinárodní norma

- počítá se všemi důležitými fázemi životního cyklu celkové 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 úrovně 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 úrovně 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 úrovně integrity bezpečnosti;
- v režimu provozu s nízkým vyžádáním (malou poptávkou) je dolní mez pro plnění projektované funkce na vyžádání stanovena na střední pravděpodobnost nebezpečné poruchy 10^{-5} ,
- v režimu provozu s vysokým nebo trvalým vyžádáním (poptávkou) je dolní mez stanovena na střední pravděpodobnost nebezpečné poruchy 10^{-9} za hodinu;

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

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

- stanovuje požadavky, aby bylo možno předcházet a řídit systematické chyby, které jsou založeny na zkušenosti a úsudku z praktických zkušeností v průmyslu. I když pravděpodobnost vzniku systematické poruchy nemůže být obecně kvantifikována, norma dovoluje, aby se tak stalo pro určité specifikované funkce, aby cílová protiporuchová opatření spojená s bezpečnostní funkcí mohla být dosažena, jestliže budou splněny požadavky normy;
- zavádí systematickou schopnost, používanou na jakoukoliv součást, s přesvědčením, že systematická integrita bezpečnosti splňuje požadavky stanovené úrovně integrity bezpečnosti;
- přijímá široký rozsah principů, technik a opatření pro dosažení funkční bezpečnosti pro systémy E/E/PE související s bezpečností, ale nepoužívá výslovně koncept „závady prostý“. Nicméně koncepty „závady prostý“ a „vnitřně bezpečný“ mohou být principiálně použitelné a použití takových principů je akceptovatelné, pokud odpovídají požadavkům příslušných článků normy.

1 Rozsah platnosti

1.1 Tato část souboru IEC 61508

- a. je určena k použití teprve po důkladném porozumění IEC 61508-1, která vymezuje celkový pracovní rámec pro dosažení funkční bezpečnosti;
- b. platí pro jakýkoliv systém související s bezpečností, podle definice v IEC 61508-1, obsahující alespoň jednu jeho součást založenou na elektrickém, elektronickém nebo programovatelném elektronickém prvku;
- c. platí pro všechny prvky systému E/E/PE související s bezpečností (včetně senzorů, akčních členů a rozhraní operátora);
- d. stanovuje způsob, jak zpřesnit specifikaci požadavků vytvořených podle IEC 61508-1 (obsahující specifikaci požadavků bezpečnostních funkcí systému E/E/PE a specifikaci požadavků systému E/E/PE souvisejícího s bezpečností a specifikuje požadavky integrity bezpečnosti systému E/E/PE) do specifikace požadavků návrhu systému E/E/PE;
- e. stanovuje požadavky na činnosti, které se musí realizovat během návrhu a výroby systémů E/E/PE souvisejících s bezpečností (tj. stanovuje model životního cyklu bezpečnosti systému E/E/PE) s výjimkou

softwaru, který je předmětem IEC 61508-3 (viz obrázky 2 až 4). Tyto požadavky zahrnují použití technik a opatření klasifikovaných z hlediska úrovně integrity bezpečnosti a zabraňujících a umožňujících řízení vad a poruch;

- f. stanovuje informace nezbytné pro provedení instalace, uvedení do provozu a konečné potvrzení platnosti bezpečnosti systémů E/E/PE souvisejících s bezpečností;
- g. neplatí pro fázi provozu a údržby systémů E/E/PE souvisejících s bezpečností – tato fáze je předmětem IEC 61508-1 – IEC 61508-2 však stanovuje požadavky týkající se přípravy informací a postupů, které uživatel potřebuje pro provoz a údržbu systémů E/E/PE souvisejících s bezpečností;
- h. stanovuje požadavky, které má plnit organizace provádějící jakékoliv modifikace systémů E/E/PE souvisejících s bezpečností.

POZNÁMKA 1 Tato část IEC 61508 se zaměřuje hlavně na dodavatele a/nebo příslušná technická oddělení uvnitř společností, proto jsou zařazeny požadavky na modifikaci.

POZNÁMKA 2 Vztah mezi IEC 61508-2 a IEC 61508-3 je ukázán na obrázku 4.

- i. není určena pro lékařská zařízení, která odpovídají souboru IEC 60601.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 jsou základní bezpečnostní normy, přestože tento status neplatí v kontextu jednoduchých systémů E/E/PE souvisejících s bezpečností (viz IEC 61508-4, 3.4.3). Jako základní normy bezpečnosti jsou určeny pro použití technickými komisemi při tvorbě norem podle zásad uvedených v pokynu IEC Guide 104 a pokynu ISO/IEC Guide 51. U IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 se také počítá s jejím použitím jako samostatných norem. Horizontální bezpečnostní funkce této mezinárodní normy se nevztahuje na lékařská zařízení, shodná se souborem IEC 60601.

1.3 Jedna z povinností technické komise je používat základní bezpečnostní hlediska bezpečnosti publikace při přípravě svých publikací všude tam, kde je to použitelné. V této souvislosti se základní bezpečnostní publikace nepoužívají, pokud se specificky uvádějí nebo jsou do těchto publikací zahrnuty.

POZNÁMKA Funkční bezpečnost systému E/E/PE souvisejícího s bezpečností lze dosáhnout pouze v případě, že jsou splněny všechny požadavky s ní spojené. Proto je důležité posouzení všech požadavků a jejich dostatečné uvádění.

1.4 Na obrázku 1 je uveden celkový rámec souboru IEC 61508 a vyznačena úloha, kterou má IEC 61508-2 z hlediska dosažení funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností. V IEC 61508-6, příloze A je popsáno použití IEC 61508-2 a IEC 61508-3.



Obrázek 1 - Celkový rámec souboru norem IEC 61508

Konec náhledu - text dále pokračuje v placené verzi ČSN.