

ČESKÁ TECHNICKÁ NORMA

ICS 13.110; 25.040; 29.020 **Leden 2011**

**Funkční bezpečnost elektrických/elektronických/
programovatelných elektronických systémů souvisejících
s bezpečností -
Část 1: Všeobecné požadavky**

ČSN
EN 61508-1
ed. 2
18 0301

idt IEC 61508-1:2010

Functional safety of electrical/electronic/programmable electronic safety-related systems -
Part 1: General requirements

Sécurité fonctionnelle des systemes électriques/électroniques/électroniques programmables relatifs
a la sécurité -
Part 1: Prescriptions générales

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer
elektronischer Systeme -
Teil 1: Allgemeine Anforderungen

Tato norma je českou verzí evropské normy EN 61508-1:2010. 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 61508-1:2010. 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 61508-1 (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 61508-1 (18 0301)
ze září 2002, v souladu s předmluvou k EN 61508-1:2010.

Změny proti předchozím normám

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

Informace o citovaných normativních dokumentech

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

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 Guide 104:1997 nezaveden

ISO/IEC Guide 51:1999 nezaveden

Informativní údaje z IEC 61508-1:2010

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

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

Toto vydání bylo podrobena 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	Zpráva o hlasování
65A/548/FDIS	65A/572/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 61508-1
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Květen 2010

ICS 13.110; 25.040; 29.020 Nahrazuje EN 61508-1:2001

Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností -
Část 1: Všeobecné požadavky
(IEC 61508-1:2010)

Functional safety of electrical/electronic/programmable electronic safety-related systems -
Part 1: General requirements
(IEC 61508-1:2010)

Sécurité fonctionnelle des systèmes

électriques/électroniques/électroniques programmables relatifs à la sécurité -

Partie 1: Exigences générales
(CEI 61508-1:2010)

Funktionale Sicherheit sicherheitsbezogener

elektrischer/elektronischer/programmierbarer elektronischer Systeme -

Teil 1: Allgemeine Anforderungen
(IEC 61508-1:2010)

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.

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

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

Předmluva

Text dokumentu 65A/548/FDIS, budoucí vydání 2 IEC 61508-1, 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 61508-1 dne 2010-05-01.

Tato evropská norma nahrazuje EN 61508-1:2001.

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 (dop) 2011-02-01
- nejzazší datum zrušení národních norem, které jsou s EN v rozporu (dow) 2013-05-01

Přílohu ZA doplnil CENELEC.

Oznámení o schválení

Text mezinárodní normy IEC 61508-1:2010 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod	8
1 Rozsah platnosti	9
2 Citované normativní dokumenty	12
3 Definice a zkratky	12
4 Shoda s touto normou	12
5 Dokumentace	12
5.1 Cíle	12
5.2 Požadavky	13
6 Management funkční bezpečnosti	14

6.1	Cíle	14
6.2	Požadavky	14
7	Požadavky životního cyklu celkové bezpečnosti	16
7.1	Všeobecně	16
7.1.1	Úvod	16
7.1.2	Cíle a požadavky – všeobecně	20
7.1.3	Cíle	24
7.1.4	Požadavky	25
7.2	Koncept	25
7.2.1	Cíl	25
7.2.2	Požadavky	25
7.3	Definice celkového předmětu	25
7.3.1	Cíle	26
7.3.2	Požadavky	26
7.4	Analýzy nebezpečí a rizik	26
7.4.1	Cíle	26
7.4.2	Požadavky	26
7.5	Požadavky celkové bezpečnosti	28
7.5.1	Cíle	28
7.5.2	Požadavky	28
7.6	Přiřazení požadavků celkové bezpečnosti	29
7.6.1	Cíle	29
7.6.2	Požadavky	30
7.7	Plánování celkového provozu a údržby	33
7.7.1	Cíl	34
7.7.2	Požadavky	34
7.8	Plánování potvrzení platnosti celkové bezpečnosti	35
7.8.1	Cíl	35

7.8.2	Požadavky	35
7.9	Plánování celkové instalace a uvedení do provozu	36
7.9.1	Cíle	36
7.9.2	Požadavky	36
7.10	Specifikace požadavků bezpečnosti systému E/E/PE	37
7.10.1	Cíle	37
7.10.2	Požadavky	37
7.11	Systémy E/E/PE související s bezpečností - realizace	39
7.11.1	Cíl	39
7.11.2	Požadavky	39
7.12	Jiné prostředky pro snížení rizika - specifikace a realizace	39
7.12.1	Cíl	39
7.12.2	Požadavky	39
7.13	Celková instalace a uvedení do provozu	39
7.13.1	Cíle	39
7.13.2	Požadavky	39
7.14	Potvrzení platnosti celkové bezpečnosti	40
7.14.1	Cíl	40
7.14.2	Požadavky	40
7.15	Celkový provoz, údržba a opravy	40
7.15.1	Cíl	41
7.15.2	Požadavky	41
7.16	Celková modifikace a zdokonalování	43
7.16.1	Cíl	43
7.16.2	Požadavky	43
7.17	Vyřazení z provozu nebo likvidace	45
7.17.1	Cíl	45

7.17.2 Požadavky 45

7.18 Ověření 46

7.18.1 Cíl 46

7.18.2 Požadavky 46

8 Odhad funkční bezpečnosti 47

8.1 Cíl 47

8.2 Požadavky 47

Příloha A (informativní) Příklad struktury dokumentace 51

Bibliografie 56

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace 58

Obrázek 1 – Celkový rámec souboru norem IEC 61508 11

Obrázek 2 – Životní cyklus celkové bezpečnosti 18

Obrázek 3 – Vývoj životního cyklu ASIC (Model-V) 19

Obrázek 4 – Životní cyklus bezpečnosti softwaru (v realizační fázi) 19

Obrázek 5 – Vztah mezi životním cyklem celkové bezpečnosti a životními cykly bezpečnosti systému E/E/PE a softwaru 20

Obrázek 6 – Přiřazení bezpečnostních požadavků systémům E/E/PE souvisejícím s bezpečností a jiným opatřením pro snížení rizika 31

Obrázek 7 – Příklad modelu provozních a údržbových činností 42

Obrázek 8 – Příklad modelu managementu provozu a údržby 43

Obrázek 9 – Příklad modelu postupu pro modifikaci 45

Obrázek A.1 – Strukturování informací do dokumentových souborů pro skupiny uživatelů 55

Strana

Tabulka 1 – Životní cyklus celkové bezpečnosti – přehled 21

Tabulka 2 – Úrovně integrity bezpečnosti – cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s nízkým vyžádáním 32

Tabulka 3 – Úrovně integrity bezpečnosti: cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s vysokým nebo nepřetržitým vyžádáním 32

- Tabulka 4 – Minimální úrovně nezávislosti osob provádějících odhad funkční bezpečnosti (fáze 1 až 8 a 12 až 16 celkového životního cyklu bezpečnosti (viz obrázek 2)) 49
- Tabulka 5 – Minimální úrovně nezávislosti osob provádějících odhad funkční bezpečnosti (fáze 9 a 10 celkového životního cyklu bezpečnosti včetně všech fází systémů E/E/PE souvisejících s bezpečností a softwaru (viz obrázky 2, 3 a 4)) 50
- Tabulka A.1 – Příklad struktury dokumentace pro informace týkající se životního cyklu celkové bezpečnosti 52
- Tabulka A.2 – Příklad struktury dokumentace pro informace týkající se životního cyklu bezpečnosti systému E/E/PE 53
- Tabulka A.3 – Příklad struktury dokumentace pro informace týkající se životního cyklu bezpečnosti softwaru 54

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 revizích, 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 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 limit 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
- 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 jednobanálnou 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 se bylo možno vyvarovat a řídit systematické chyby, které jsou založeny na zkušenosti a úsudku z praktické zkušenosti v průmyslu. I když pravděpodobnost vzniku systematické poruchy nemůže být obecně kvantifikována, norma dovoluje, aby se to udělalo pro určité specifikované funkce tak, 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, jestliže se použijí požadavky příslušných článků normy.

1 Rozsah platnosti

1.1 Tato mezinárodní norma obsahuje hlediska, která se mají zvážit při použití elektrických/elektronických/programovatelných elektronických systémů (E/E/PE) pro zajišťování bezpečnostních funkcí. Hlavním cílem této normy je usnadnit tvorbu aplikačních mezinárodních norem příslušným technickým komisím, které jsou za příslušné aplikační oblasti zodpovědné. To umožní zvážit všechny činitele spojené s danou aplikací a tím vyhovět všem specifickým potřebám uživatelů a příslušné aplikační oblasti. Dalším cílem této normy je umožnit vývoj systémů E/E/PE souvisejících s bezpečností i v oblastech, kde nejsou příslušné aplikační mezinárodní normy k dispozici.

1.2 Tato norma zejména

- a. platí pro systémy související s bezpečností v případě, že jeden nebo několik takových systémů obsahuje elektrická/elektronická/programovatelná elektronická zařízení;

POZNÁMKA 1 V souvislosti s jednoduchými systémy E/E/PE souvisejícími s bezpečností mohou být některé požadavky uvedené v této normě zbytečné a je možné nepožadovat jejich splnění (viz 4.2 a definice jednoduchého systému E/E/PE souvisejícího s bezpečností v IEC 61508-4, 3.3.4).

POZNÁMKA 2 Přestože částí systému souvisejícího s bezpečností může být i člověk (viz IEC 61508-4, 3.4.1), nejsou v této normě podrobněji zohledněny požadavky spojené s lidským faktorem týkající se návrhu systému E/E/PE souvisejícího s bezpečností.

- b. obecně vychází a je použitelná pro všechny systémy E/E/PE související s bezpečností bez ohledu na konkrétní aplikaci;
 - c. pokrývá dosažení tolerovatelného rizika použitím systémů E/E/PE souvisejících s bezpečností, ale nepokrývá nebezpečí vznikajícího ze zařízení E/E/PE samotného (např. úraz elektrickým proudem);
 - d. vztahuje se na všechny typy systémů E/E/PE souvisejících s bezpečností, včetně ochranných systémů a řídicích systémů;
 - e. nezahrnuje systémy E/E/PE, kde
- jednotlivý systém E/E/PE je schopen zajistit nutné snížení rizika, a
 - požadovaná integrita bezpečnosti systému E/E/PE je nižší než integrita stanovená pro úroveň integrity bezpečnosti 1 (v této normě nejnížší úroveň integrity bezpečnosti);
- f. zaměřuje se hlavně na systémy E/E/PE související s bezpečností, jejichž porucha by mohla mít dopad na bezpečnost osob a/nebo okolního prostředí; současně se však uznává, že následky poruchy by mohly mít také vážné ekonomické následky a v takových případech by mohla být použita pro specifikaci jakéhokoliv systému E/E/PE použitého pro ochranu zařízení nebo výrobku.

POZNÁMKA 3 Viz IEC 61508-4, 3.1.1.

- g. posuzuje systémy E/E/PE související s bezpečností a jiná opatření pro snížení rizika tak, aby bylo možné stanovit specifikaci bezpečnostních požadavků pro systémy E/E/PE související s bezpečností systematickým a na riziku založeným způsobem;
- h. používá model životního cyklu celkové bezpečnosti jako technického rámce pro systematické provádění všech činností, které jsou pro zajištění funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností nezbytné;

POZNÁMKA 4 Ačkoliv se celkový bezpečnostní životní cyklus týká především systémů E/E/PE souvisejících s bezpečností, může také poskytovat technický rámec pro úvahu o libovolném bezpečnostním systému souvisejícím s bezpečností, bez ohledu na technologii tohoto systému (např. mechanický, hydraulický nebo pneumatický).

- i. nestanovuje úroveň integrity bezpečnosti požadované pro různé aplikační oblasti (ty musí vycházet

z podrobných informací a znalostí těchto oblastí). Technická komise odpovědná za konkrétní aplikační oblast musí, tam, kde to je vhodné, pro tyto oblasti stanovit v příslušných normách příslušné úrovně integrity bezpečnosti;

- j. stanovuje všeobecné požadavky na systémy E/E/PE související s bezpečností pro případy, kde žádné aplikační normy nejsou k dispozici;
- k. během analýzy nebezpečí a rizika je třeba zvážit škodlivé požadavky a neoprávněné akce; předmět analýzy zahrnuje všechny fáze bezpečnostního životního cyklu;

POZNÁMKA 5 Jiné normy IEC/ISO oslovují tento předmět do hloubky, viz ISO/IEC/TR 19791 a soubor IEC 62443.

- l. neobsahuje bezpečnostní opatření, která mohou být nutná k tomu, aby zabránila neoprávněným osobám v poškození a/nebo jinému nepříznivém ovlivnění funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností (viz k) výše);
- m. nespecifikuje požadavky na vývoj a realizaci, údržbu a/nebo provoz bezpečnostního úřadu nebo bezpečnostní služby pro zajištění politiky bezpečnosti, která může být systémem E/E/PE souvisejícím s bezpečností vyžadována;
- n. nevztahuje se na lékařská zařízení vyhovující souboru IEC 60601.

1.3 Tato část souboru norem IEC 61508 stanovuje všeobecné požadavky, které jsou použitelné ve všech jejích částech. Ostatní části IEC 61508 jsou zaměřeny na tato konkrétnější témata:

- části 2 a 3 obsahují doplňující a specifické požadavky na systémy E/E/PE související s bezpečností (na hardware i software);
- část 4 obsahuje definice a zkratky používané v celé této normě;
- část 5 obsahuje metodické pokyny pro použití části 1 pro určování úrovní integrity bezpečnosti a to formou uvedení vzorových metod;
- část 6 obsahuje metodické pokyny pro používání částí 2 a 3;
- část 7 obsahuje přehled technik a opatření.

1.4 Části 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 částí IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 se počítá také s jejich použitím jako samostatných norem. Horizontální bezpečnostní funkce těchto mezinárodních norem neplatí pro lékařská zařízení vyhovující souboru norem IEC 60601.

POZNÁMKA Jedna z odpovědností technické komise je, používat při přípravě svých publikací, základní bezpečnostní publikace všude, kde je to možné. V této souvislosti se požadavky, zkušební metody nebo zkušební podmínky těchto základních bezpečnostních publikací nepoužijí pouze tehdy, jsou-li specifikovány v odkazech publikací těchto technických komisí nebo jsou-li do připravovaných publikací přímo začleněny.

1.5 Obrázek 1 ukazuje celkovou strukturu souboru IEC 61508 a vyznačuje úlohu, kterou má IEC 61508-1 pro dosažení 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.