

**2002**

	Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky	ČSN EN 61508-1  18 0301
--	--	----------------------------------

idt IEC 61508-1:1998 + IEC 61508-1:1998/Cor.:1999-05

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à  
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 61508-1:2001. Evropská norma EN 61508-1:2001 má  
status české technické normy.

This standard is the Czech version of the European Standard EN 61508-1:2001. The European  
Standard EN 61508-1:2001 has the status of the Czech Standard.

© Český normalizační institut,  
2002

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány  
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

**65005**

## Citované normy

ISO/IEC Guide 51:1990 nezaveden, nahrazen ISO/IEC Guide 51:1999 nezavedeným

IEC Guide 104:1997 nezaveden

IEC 61508-2:2000 zavedena v ČSN EN 61508-2:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností (idt IEC 61508-2:2000, idt EN 61508-2:2001)

IEC 61508-3:1998 zavedena v ČSN EN 61508-3:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 3: Požadavky na software (idt IEC 61508-3:1998 + Cor. 1999-04, idt EN 61508-3:2001)

IEC 61508-4:1998 zavedena v ČSN EN 61508-4:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 4: Definice a zkratky (idt IEC 61508-4:1998 + Cor. 1999-04, idt EN 61508-4:2001)

IEC 61508-5:1998 zavedena v ČSN EN 61508-6:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 5: Příklady metod určování úrovně integrity bezpečnosti (idt IEC 61508-5:1998 + Cor. 1999, idt EN 61508-5:2001)

IEC 61508-6:2000 zavedena v ČSN EN 61508-6:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3 (idt IEC 61508-6:2000, idt EN 61508-6:2001)

IEC 61508-7:2000 zavedena v ČSN EN 61508-7:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 7: Přehled technik a opatření (idt IEC 61508-7:2000, idt EN 61508-7:2001)

## Porovnání s mezinárodní normou

ČSN EN 61508-1 je identická s IEC 61508-1:1998 včetně její opravy IEC 61508-1:1998/Cor.:1999-05, navíc však obsahuje normativní přílohu ZA „Normativní odkazy na mezinárodní publikace s jejich příslušnými evropskými publikacemi, kterou doplnil CENELEC.

## Informativní údaje z IEC 61508-1:1998

Tuto mezinárodní normu IEC 61508-1 připravila subkomise 65A: „Systémové aspekty“ technické komise IEC TC 65 „Měření a řízení průmyslových procesů“

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
65A/264/FDIS	65A/274/RVD

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

Přílohy A, B a C jsou pouze informativní.

IEC 61508 se skládá z těchto částí uváděných pod společným názvem Funkční bezpečnost

elektrických/ elektronických/programovatelných elektronických systémů souvisejících s bezpečností:

- Část 1: Všeobecné požadavky
- Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností
- Část 3: Požadavky na software
- Část 4: Definice a zkratky
- Část 5: Příklady metod určování úrovně integrity bezpečnosti
- Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3
- Část 7: Přehled technik a opatření

Strana 3

---

Vypracování normy

Zpracovatel: PRO\*MAN CS, Praha, IČO 16458443, Ing. Petr Římský

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Ing. Jaromír Petřík

Strana 4

---

Prázdná strana

Strana 5

---

EVROPSKÁ NORMA EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM	EN 61508-1 Prosinec 2001
---	-----------------------------

ICS 13.110;25.040;29.020;35.240.50

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

Část 1: Všeobecné požadavky

(IEC 61508-1:1998 + corrigendum 1999)

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

Part 1: General requirements

(IEC 61508-1:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Part 1: Prescriptions générales (CEI 61508-1:1998 + corrigendum)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999)

Tato evropská norma byla schválena CENELEC 2001-07-03. 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, České republiky, Dánska, Finska, Francie, Irsko, Islandu, Itálie, Lucemburska, Malty, Německa, Nizozemska, Norska, Portugalska, Rakouska, Řecka, Spojeného království, Španělska, Švédsko a Švýcarska.

## **CENELEC**

**Evropský výbor pro normalizaci v elektrotechnice**

**European Committee for Electrotechnical Standardization**

**Comité Européen de Normalisation Electrotechnique**

**Europäisches Komitee für Elektrotechnische Normung**

**Ústřední sekretariát: rue de Stassart 35, B-1050 Brusel**

© 2001 CENELEC. Veškerá práva pro využití v jakékoli formě a v jakémkoli

Ref. č. EN 61508-1:2001 E

množství jsou vyhrazena národním členům CENELEC.

### Předmluva

Text mezinárodní normy IEC 61508-1:1998 včetně její opravy IEC 61508:1998/Cor.:1999-05 připravila subkomise 65A: „Systémové aspekty“ technické komise IEC TC 65 „Měření a řízení průmyslových procesů“ a byl předložen CENELEC k jednotnému schvalovacímu postupu a byl schválen CENELEC jako EN 61508-1 dne 2001-07-03 bez jakýchkoliv modifikací.

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) 2002-08-01
- nejzazší datum zrušení národních norem, které jsou s EN v rozporu (dow) 2004-08-01

Přílohy označené jako „normativní“ jsou součástí této normy.

Přílohy označené jako „informativní“ jsou uvedeny pouze pro informaci.

V této normě je normativní příloha ZA a přílohy A, B a jsou informativní.

Přílohu ZA doplnil CENELEC.

IEC 61508 je základní bezpečnostní norma platná pro funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností. Předmět normy uvádí:

„Tato mezinárodní norma zahrnuje hlediska, která se doporučuje vzít v úvahu při použití elektrických/elektronických/programovatelných elektronických systémů (E/E/PES - electrical/electronic/programmable electronic system) pro plnění bezpečnostních funkcí. Hlavním cílem této normy je usnadnit technickým komisím odpovědným za jednotlivé aplikační oblasti tvorbu aplikačních oborových mezinárodních norem. To umožní plné respektování všech relevantních faktorů s danou aplikací spojených a tím splnění charakteristických potřeb dané aplikační oblasti. Dalším cílem této normy je umožnění vývoje elektrických/elektronických/programovatelných elektronických (E/E/PE - electrical/electronic/programmable electronic) systémů souvisejících s bezpečností tam, kde příslušné aplikační oborové mezinárodní normy neexistují.“

Zpráva CENELEC ROBT-004 schválená na 103. zasedání technického výboru (březen 2000) uznává, že některé normy IEC, které se v současné době buď vydávají nebo připravují, jsou oborovými implementacemi IEC 61508. Např.:

- IEC 61511, Funkční bezpečnost - Bezpečnostní přístrojové systémy pro oblast průmyslových procesů;
- IEC 62061, Bezpečnost strojního zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů řízení;
- IEC 61513, Jaderné elektrárny - Přístrojová technika a řízení systémů důležitých pro bezpečnost - Všeobecné požadavky na systémy.

Oblast železnic také zpracovala soubor evropských norem (EN 50126; EN 50128 a prEN 50129).

POZNÁMKA EN 50126 a EN 50128 vycházejí z dřívějších návrhů IEC 61508. prEN 50129 vychází z poslední verze IEC 61508.

Tento seznam předem nevyklučuje další oborové implementace IEC 61508, které mohou být v současné době vydávány nebo zpracovávány v rámci IEC nebo CENELEC.

## Oznámení o schválení

Text mezinárodní normy IEC 61508-1:1998 včetně její oprav z května 1999 schválil CENELEC jako evropskou normu bez jakýchkoliv modifikací.

Strana 7

---

### Obsah

Strana

#### Úvod

.....  
..... 9

#### **1** Rozsah platnosti

.....  
11

#### **2** Normativní odkazy

..... 14

#### **3** Definice a zkratky

.....  
14

#### **4** Shoda s touto normou

..... 14

#### **5** Dokumentace

.....  
... 15

##### **5.1** Cíle

.....  
..... 15

##### **5.2** Požadavky

.....  
..... 15

#### **6** Management funkční bezpečnosti

..... 16

## **6.1**

Cíle

..... 16

## **6.2**

Požadavky

..... 17

## **7 Požadavky životního cyklu celkové**

bezpečnosti..... 18

### **7.1**

Všeobecně

..... 18

### **7.2**

Koncept

..... 27

### **7.3 Definice celkového předmětu (oblasti**

použití)..... 28

### **7.4 Analýza nebezpečí a**

rizik..... 28

### **7.5 Požadavky celkové**

bezpečnosti..... 30

### **7.6 Přiřazení bezpečnostních**

požadavků..... 31

### **7.7 Plánování celkového provozu a**

údržby..... 36

### **7.8 Plánování potvrzení platnosti**

bezpečnosti..... 38

### **7.9 Plánování celkové instalace a uvedení do**

provozu..... 39

### **7.10 Realizace:**

E/E/PES

..... 39

### **7.11 Realizace: systémy založené na jiných technických**

principech..... 39

### **7.12 Realizace: vnější prostředky pro snížení**

rizika..... 40

<b>7.13</b>	Celková instalace a uvedení do provozu.....	40
<b>7.14</b>	Potvrzení platnosti celkové bezpečnosti.....	41
<b>7.15</b>	Celkový provoz, údržba a opravy.....	41
<b>7.16</b>	Celková modifikace a zdokonalování.....	44
<b>7.17</b>	Vyřazení z provozu nebo likvidace.....	46
<b>7.18</b>	Ověření ..... .....	47
<b>8</b>	Odhad funkční bezpečnosti..... 47	
<b>8.1</b>	Cíl ..... .....	47
<b>8.2</b>	Požadavky ..... .....	48
<b>Přílohy</b>		
<b>Příloha A</b>	(informativní) Příklad struktury dokumentace.....	51
<b>A.1</b>	Všeobecně ..... .....	51
<b>A.2</b>	Struktura dokumentu životního cyklu bezpečnosti.....	52
<b>A.3</b>	Fyzické uspořádání dokumentů.....	54
<b>A.4</b>	Seznam dokumentů .....	56



**Příloha B** (informativní) Kvalifikace

osob..... 57

**B.1**

Cíl

..... 57

**B.2** Všeobecné

úvahy

..... 57

**Příloha C** (informativní)

Bibliografie.....

58

**Příloha ZA** (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace..... 59**Tabulky****1** Životní cyklus celkové bezpečnosti:

přehled..... 23

**2** Úrovně integrity bezpečnosti: cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s nízkým vyžádáním

..... 35

**3** Úrovně integrity bezpečnosti: cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s vysokým nebo nepřetržitým vyžádáním..... 35**4** Minimální úrovně nezávislosti osob provádějících odhad funkční bezpečnosti (fáze 1 až 8 a 12 až 16 (viz obrázek 2) životního cyklu celkové bezpečnosti))..... 50**5** Minimální úrovně nezávislosti osob provádějících odhad funkční bezpečnosti (fáze 9 životního cyklu celkové bezpečnosti včetně všech fází životního cyklu bezpečnosti E/E/PES a bezpečnosti softwaru (viz obrázky 2, 3 a 4))..... 50

**A.1** Příklad struktury dokumentace pro informace týkající se životního cyklu celkové bezpečnosti..... 52

**A.2** Příklad struktury dokumentace pro informace týkající se životního cyklu bezpečnosti E/E/PES..... 53

**A.3** Příklad struktury dokumentace pro informace týkající se životního cyklu bezpečnosti softwaru..... 54

## **Obrázky**

**1** Celková struktura této normy..... 13

**2** Životní cyklus celkové bezpečnosti..... 20

**3** Životní cyklus bezpečnosti E/E/PES (v realizační fázi)..... 21

**4** Životní cyklus bezpečnosti softwaru (v realizační fázi)..... 21

**5** Vztah mezi životním cyklem celkové bezpečnosti a životními cykly bezpečnosti E/E/PES a softwaru  
.....  
..... 22

**6** Přiřazení bezpečnostních požadavků E/E/PE systémům souvisejícím s bezpečností, systémům souvisejícím s bezpečností založených na jiných technických principech a vnějším prostředkům pro snížení rizika..... 34

**7** Příklad modelu provozních a údržbových činností..... 43

**8** Příklad modelu managementu provozu a údržby..... 44

**9** Příklad modelu postupu pro modifikaci..... 46

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

**A.2** Strukturování informací u velkých složitých systémů a u malých jednoduchých systémů..... 55

---

# Úvod

Systémy obsahující elektrické a/nebo elektronické součásti se již řadu let používají ve většině aplikačních oblastech pro plnění bezpečnostních funkcí. Systémy založené na využití počítačů (obecně zařazované jako programovatelné elektronické systémy (PES - programmable electronic systems)) se již ve všech aplikačních oblastech používají 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 životní cykly bezpečnosti systémů obsahujících elektrické a/nebo elektronické a/nebo programovatelné elektronické součásti (elektrické/elektronické/programovatelné elektronické systémy (E/E/PES - electrical/electronic/programmable electronic systems)) a využívané pro zajištění bezpečnostních funkcí. Tento sjednocený přístup byl přijat proto, aby se u všech elektrických systémů související s bezpečností používalo racionálního a konzistentního technického přístupu. Hlavním cílem je usnadnění tvorby dalších aplikačních norem pro jednotlivé dílčí oblasti.

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 (E/E/PE - electrical/electronic/programmable electronic) systémy 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 E/E/PES v mnoha různých aplikačních oblastech a pokrývajících široký rozsah složitosti, nebezpečí i rizik. Vyžadovaná bezpečnostní opatření budou v každé konkrétní aplikaci záviset na mnoha pro danou aplikaci charakteristických faktorech. Tato mezinárodní norma umožňuje, vzhledem ke svému obecnému charakteru, formulaci takových opatření v budoucích aplikačních mezinárodních normách.

Tato mezinárodní norma

- počítá se všemi důležitými fázemi životního cyklu celkové bezpečnosti, bezpečnosti E/E/PES a bezpečnosti softwaru (např. od počáteční koncepce přes návrh, realizaci, provoz a údržbu až po vyřazení z provozu) při používání E/E/PE systémů pro plnění bezpečnostních funkcí;
- byla zpracována s ohledem na rychlý rozvoj techniky; její struktura je dostatečně pevná a obsažná, aby umožnila další rozvoj;
- umožňuje tvorbu aplikačních mezinárodních norem týkajících se E/E/PE systémů 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 E/E/PE systémů souvisejících s bezpečností;

- pro stanovení cílové úrovně integrity bezpečnosti pro bezpečnostní funkce realizované E/E/PE systémy souvisejícími s bezpečností používá úrovní integrity bezpečnosti;
- pro stanovení požadavků na úroveň integrity bezpečnosti používá metody založené na riziku;
- stanovuje číselné hodnoty cílové míry poruch pro E/E/PE systémy související s bezpečností vázané na jednotlivé úrovně integrity bezpečnosti;
- stanovuje dolní mez pro cílové míry poruch, v režimu nebezpečné poruchy, které lze požadovat u jednotlivého E/E/PE systému souvisejícího s bezpečností; u E/E/PE systémů souvisejících s bezpečností pracujících
  - v režimu provozu s malým vyžádáním (malou poptávkou) je dolní mez pro plnění projektované funkce na vyžádání stanovena na střední pravděpodobnost poruchy  $10^{-5}$ ,

Strana 10

---

- v režimu provozu s velkým nebo trvalým vyžádáním (poptávkou) je dolní mez stanovena na střední pravděpodobnost poruchy  $10^{-9}$  za hodinu;

POZNÁMKA Jednotlivý E/E/PE systém související s bezpečností neznámá nutně jednobáňovou architekturu.

- pro dosažení funkční bezpečnosti E/E/PE systémů souvisejících s bezpečností přejímá široký rozsah principů, technik a opatření, ale nepočítá s koncepcí založenou na zabezpečení proti poruchám (výpadku), která může mít své opodstatnění v případech, kdy jsou dobře definovány režimy poruchy a při relativně nízké úrovni složitosti. Koncepce zabezpečení proti poruchám byla, vzhledem k celkovému rozsahu složitosti E/E/PE systémů souvisejících s bezpečností, které jsou předmětem této normy, uznána jako nevhodná.

Strana 11

---

## 1 Rozsah platnosti

**1.1** Tato mezinárodní norma obsahuje hlediska, která se doporučuje zvážit při použití elektrických/elektronických/programovatelných elektronických systémů (E/E/PES - electrical/electronic/programmable electronic system) pro zajištění bezpečnostních funkcí. Hlavním cílem této normy je usnadnit tvorbu aplikačních mezinárodních norem příslušným technickým komisím za příslušné aplikační oblasti odpovědným. To umožní zvážit všechny činitele s danou aplikací spojené a tím vyhovět všem specifickým potřebám příslušné aplikační oblasti. Dalším cílem této normy je možnost využití elektrických/elektronických /programovatelných elektronických (E/E/PE - electrical/electronic/programmable electronic) systémů 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 E/E/PE systémy souvisejícími s bezpečností mohou být některé požadavky uvedené v této normě zbytečné a je možné nepožadovat jejich splnění (viz 4.2 a definice jednoduchého E/E/PE systému souvisejícího s bezpečností 3.3.4 v IEC 61508-4).

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

- b) obecně vychází a je použitelná pro všechny E/E/PE systémy související s bezpečností bez ohledu na konkrétní aplikaci;\*
- c) zahrnuje možná nebezpečí vyvolaná poruchami (selháním) bezpečnostních funkcí prováděných E/E/PE systémy souvisejícími s bezpečností, na rozdíl od nebezpečí způsobených vlastním E/E/PE zařízením (např. úder elektrickým proudem atd.);
- d) nezahrnuje E/E/PE systémy, kde
  - jednotlivý E/E/PE systém je schopen zajistit nutné snížení rizika, a
  - požadovaná integrita bezpečnosti E/E/PE systému je nižší než integrita stanovená pro úroveň integrity bezpečnosti 1 (v této normě nejnižší úroveň integrity bezpečnosti);
- e) se zaměřuje hlavně na E/E/PE systémy 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 E/E/PE systému použitého pro ochranu zařízení nebo produktu.

POZNÁMKA Viz 3.1.1 a 7.3.1.2 v IEC 61508-4. \*

- f) posuzuje E/E/PE systémy související s bezpečností, systémy související s bezpečností založené na jiných technických principech a prostředky 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;
- g) používá model životního cyklu celkové bezpečnosti jako technického rámce pro systematické provádění všech činností, které jsou pro zajištění funkční bezpečnosti E/E/PE systémů souvisejících s bezpečností nezbytné;

POZNÁMKA 3 Mezi počáteční fáze životního cyklu celkové bezpečnosti patří i nutné úvahy o jiných technických principech (stejně jako o E/E/PE systémech souvisejících s bezpečností), vnějších prostředcích pro snížení rizika umožňujících zpracování specifikace bezpečnostních požadavků pro systémy E/E/PE související s bezpečností systematickým a na riziku založeným způsobem.

POZNÁMKA 4 Přestože se životní cyklus celkové bezpečnosti týká především E/E/PE systémů souvisejících s bezpečností, může poskytnout také určitý technický rámec i pro úvahy týkající se jakéhokoliv systému souvisejícího s bezpečností bez ohledu na technický princip u něj použitý (např. mechanický, hydraulický nebo pneumatický).

\* Oprava podle originálu opravenky z května 1999.

- h) nestanovuje úrovně 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 příslušné úrovně integrity bezpečnosti stanovit v příslušných normách;
- i) stanovuje všeobecné požadavky na E/E/PE systémy související s bezpečností pro případy, kde žádné aplikační normy nejsou k dispozici;
- j) neobsahuje bezpečnostní opatření, která mohou být nutná k tomu, aby zabránily neoprávněným osobám v poškození a/nebo jiném nepříznivém ovlivnění funkční bezpečnosti E/E/PE systémů souvisejících s bezpečností.

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

- část 2 a 3 obsahují doplňující a konkrétnější požadavky na E/E/PE systémy 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 použití částí 2 a 3;
- část 7 obsahuje přehled technik a opatření.

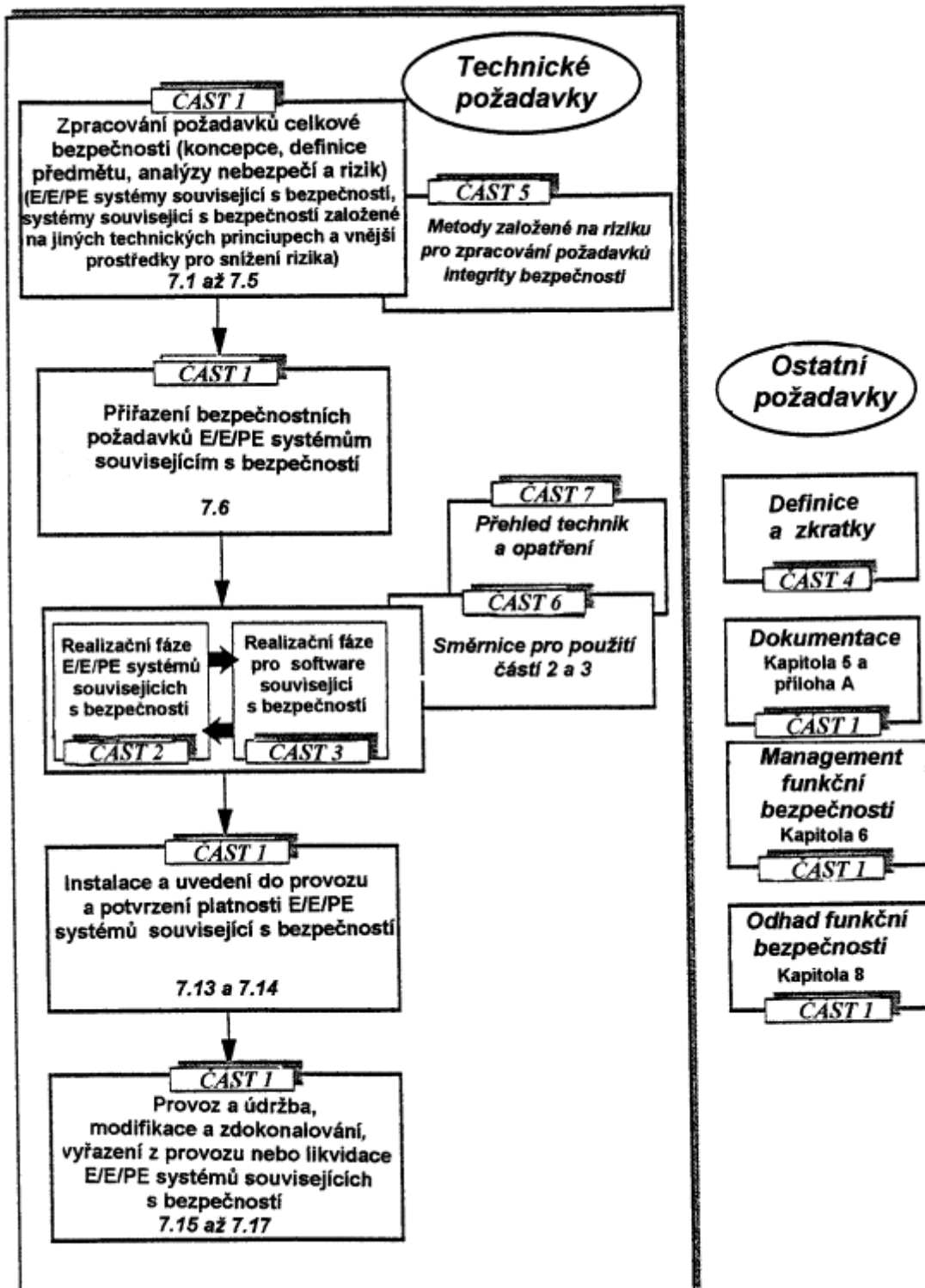
1.4 Části 1, 2, 3 a 4 jsou základní bezpečnostní normy, přestože tento status neplatí v kontextu jednoduchých systémů E/E/PE souvisejících s bezpečností (viz 3.4.4 části 4). Jako základní normy bezpečnosti jsou určeny pro použití technickými komisemi při tvorbě norem podle zásad uvedených v pokynu *IEC Guide 104* a pokynu *ISO/IEC Guide 51*. U částí 1, 2, 3 a 4 se počítá také s jejich použitím jako samostatných norem. \*

Jednou z odborných povinností technické komise je používat, všude, kde je to vhodné, základních norem bezpečnosti při tvorbě komisí připravovaných norem. V tomto kontextu příslušné požadavky, zkušební metody nebo zkušební podmínky z této základní bezpečnostní normy neplatí, nejsou-li v normách připravených technickými komisemi konkrétně zmíněny nebo uvedeny.

**POZNÁMKA** V USA a Kanadě lze až do vydání navržené oborové implementace IEC 61508 jako mezinárodní normy pro oblast procesů (tj. IEC 61511) používat v oblasti průmyslových procesů místo IEC 61508 existující národní normy bezpečnosti procesů založené na IEC 61508 (tj. ANSI/ISA S84.01-1996) (viz odkaz [8] v příloze C).

**1.5** Na obrázku 1 je ukázána celková struktura částí 1 až 7 IEC 61508 a vyznačena úloha, kterou má IEC 61508-1 pro dosažení funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností.

\* Oprava podle originálu opravenky z května 1999.



Obrázek 1 - Celková struktura této normy

## 2 Normativní odkazy

Součástí této normy jsou i ustanovení dále uvedených norem, na něž jsou odkazy v textu této části mezinárodní normy IEC 61508. U datovaných odkazů se pozdější změny nebo revize kterékoli z těchto publikací u této normy neaplikují. Avšak účastníci, kteří uzavírají dohody na podkladě této části mezinárodní normy, by měli využít nejnovějšího vydání dále uvedených norem. U nedatovaných odkazů platí nejnovější vydání citovaných norem. Členové IEC a ISO udržují seznamy platných mezinárodních norem.

ISO/IEC Guide 51:1990 Metodické pokyny pro začleňování bezpečnostních hledisek do norem

*(Guidelines for the inclusion of safety aspects in standards)*

IEC Guide 104:1997 Pokyn pro tvorbu bezpečnostních norem a úlohu komisí při použití základních a skupinových bezpečnostních norem

*(Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions)*

IEC 61508-2:2000 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností

*(Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems)*

IEC 61508-3:1998 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 3: Požadavky na software

*(Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements)*

IEC 61508-4:1998 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 4: Definice a zkratky

*(Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations)*

IEC 61508-5:1998 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 5: Příklady metod určování úrovně integrity bezpečnosti

*(Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels)*

IEC 61508-6:2000 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 6: Metodické pokyny pro použití IEC 61508-2 a 61508-3

*(Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 a IEC 61508-3)*

IEC 61508-7:2000 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických



systemů souvisejících z bezpečností - Část 7: Přehled technik a opatření

*(Functional safety of electrical/electrical/programmable electronic safety-related systems - Part 7: Overview of techniques and measures)*

---

**-- Vynechaný text --**