

2002

	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 18 0301
---	--	--

idt IEC 61508-2:2000

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité -

Part 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à 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 61508-2:2001. Evropská norma EN 61508-2:2001 má status české technické normy.

This standard implements the original version of the European Standard EN 61508-2:2001. The European Standard EN 61508-2:2001 has the status of the Czech Standard.

Národní předmluva

Citované normy

IEC 60050(371):1984 zavedena v ČSN IEC 50(371):1997 (33 0050) Mezinárodní elektrotechnický slovník. Kapitola 371: Dálkové ovládání (idt IEC 50(371):1984)

IEC 60300-3-2:1993 zavedena v ČSN IEC 300-3-2:1995 (01 0690) Řízení spolehlivosti. Část 3: Návod k použití. Oddíl 2: Sběr dat o spolehlivosti z provozu (idt IEC 300-3-2:1993)

IEC 61000-1-1:1992 zavedena v ČSN IEC 1000-1-1:1995 (33 3431) Elektromagnetická kompatibilita (EMC). Část 1: Všeobecně. Díl 1: Použití a interpretace základních definice a pojmů (idt IEC 1000-1-1:1992)

IEC 61000-2-5:1995 nezavedena

IEC 61508-1:1998 zavedena v ČSN EN 61508-1:1998 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 1: Všeobecné požadavky (idt IEC 61508-1:1998 + IEC 61508-1:1998/Cor.:1999)

IEC 61508-3:1998 zavedena v ČSN EN 61508-3:1998 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 2: Požadavky na software) (idt IEC 61508-3:1998 + IEC 61508-3:1998/Cor.:1999)

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 + IEC 61508-4:1998/Cor.:1999)

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 + IEC 61508-5:1998/Cor.:1999)

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)

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)

IEC Guide 104:1997 nezaveden

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

IEEE 352:1987 nezavedena

Porovnání s mezinárodní normou

ČSN EN 61508-2 je identická s IEC 61508-2:2000, obsahuje však navíc normativní přílohu ZA „Normativní odkazy na mezinárodní publikace s jejich příslušnými evropskými publikacemi, kterou

doplnil CENELEC.

Informativní údaje z IEC 61508-2:2000

Tuto mezinárodní normu IEC 61508-2:2000 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/294/FDIS	65A/303/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 3.

Přílohy A, B a C jsou nedílnou částí této normy.

Strana 3

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

Komise rozhodla, že se obsah této normy zůstane nezměněn až roku 2006. Potom bude norma

- potvrzena;
- zrušena;
- nahrazena revidovaným vydáním, nebo
- formou změn upravena.

Vypracování normy

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

Prázdná strana

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61508-2
Prosinec 2001

ICS 25.040.40

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

Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností
(IEC 61508-2:2000)

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

Part 2: Requirements for electrical/electronic/programmable electronic safety-related
systems
(IEC 61508-2:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité -
Part 2: Prescriptions pour les systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
(CEI 61508-2:2000)

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer
elektronischer Systeme -
Teil 2: Anforderungen an
sicherheitsbezogene
elektrische/elektronische/programmierbare
elektronische Systeme
(IEC 61508-2:2000)

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, Irska, Islandu, Itálie, Lucemburska, Maltý, Německa, Nizozemska, Norska, Portugalska, Rakouska, Řecka, 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

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

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

Ref. č. EN 61508-2:2001 E

množství jsou vyhrazena národním členům CENELEC.

Strana 6

Předmluva

Text této mezinárodní normy IEC 61508-2:2000 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 61508-2 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.

V této normě jsou normativní přílohy A, B, C a ZA.

Přílohu ZA doplnil CENELEC.

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

„Tato mezinárodní norma zahrnuje hlediska, která se doporučuje vzít v úvahu při použití elektrických/elektronických/programovatelných elektronických systémů (E/E/PES - electrical/electronic/program-mable 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 nevylučuje 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 61508-2:2000 schválil CENELEC jako evropskou normu bez jakýchkoliv modifikací.

Strana 7

Obsah

Strana

Úvod

..... 9

1 Rozsah
platnosti

.....
11

2 Normativní
odkazy

..... 13

3	Definice a zkratky	
		13
4	Shoda s touto normou	
		14
5	Dokumentace	
		14
6	Management funkční bezpečnosti	
		14
7	Požadavky životního cyklu bezpečnosti E/E/PES	
		14
7.1	Všeobecně	
		14
7.2	Specifikace požadavků bezpečnosti E/E/PES	
		18
7.3	Plánování potvrzení platnosti bezpečnosti E/E/PES	
		21
7.4	Návrh a vývoj E/E/PES	
		21
7.5	Začlenění E/E/PES	
		37
7.6	Postupy pro provoz a údržbu E/E/PES	
		38
7.7	Potvrzení platnosti bezpečnosti E/E/PES	
		40
7.8	Modifikace E/E/PES	
		41
7.9	Ověření E/E/PES	
		41

8	Odhad funkční bezpečnosti.....	42
Příloha A	(normativní) Techniky a opatření pro E/E/PE systémy související s bezpečností: řízení poruch během provozu	43
A.1	Všeobecně	43
A.2	Integrita bezpečnosti hardwaru.....	44
A.3	Systematická integrita bezpečnosti.....	53
Příloha B	(normativní) Techniky a opatření pro E/E/PE systémy související s bezpečností: předcházení systematickým poruchám během různých fází životního cyklu.....	60
Příloha C	(normativní) Diagnostické pokrytí a podíl bezpečných poruch.....	70
C.1	Výpočet diagnostického pokrytí a podílu bezpečných poruch subsystému.....	70
C.2	Určení činitelů diagnostického pokrytí.....	71
Příloha ZA	(normativní) Normativní odkazy na mezinárodní publikace a jim příslušející evropské publikace.....	73
Bibliografie		72
Obrázek 1	Celková struktura této normy.....	12
Obrázek 2	Životní cyklus bezpečnosti E/E/PES (během fáze realizace).....	15
Obrázek 3	Vztah a aplikační oblast IEC 61508-2 a IEC 61508-3.....	16
Obrázek 4	Vztah mezi architekturami hardwaru a softwaru u programovatelné elektroniky.....	22

Obrázek 5	Příklad omezení integrity bezpečnosti hardwaru pro jednobanárovou bezpečnostní funkci.....	27
-----------	--	----

Obrázek 6	Příklad omezení integrity bezpečnosti hardwaru pro vícebanárovou bezpečnostní funkci.....	29
-----------	---	----

Tabulka 1	Přehled - Fáze realizace životního cyklu bezpečnosti E/E/PES.....	17
-----------	---	----

Tabulka 2	Integrita bezpečnosti hardwaru: omezení architektury na subsystémy související s bezpečností typu A.....	26
-----------	--	----

Tabulka 3	Integrita bezpečnosti hardwaru: omezení architektury na subsystémy související s bezpečností typu B.....	26
-----------	--	----

Tabulka A.1	Vady nebo poruchy, které se mají během provozu zjišťovat nebo analyzovat při odvozování podílu bezpečných poruch	45
-------------	--	----

Strana 8

Strana

Tabulka A.2	Elektrické subsystémy.....	46
-------------	----------------------------	----

Tabulka A.3	Elektronické subsystémy.....	47
-------------	------------------------------	----

Tabulka A.4	Základní jednotky.....	48
-------------	------------------------	----

Tabulka A.5	Skupiny permanentních pamětí.....	48
-------------	-----------------------------------	----

Tabulka A.6	Skupiny měnitelných pamětí.....	49
-------------	---------------------------------	----

Tabulka A.7	Jednotky I/O (vstupů/výstupů) a rozhraní (vnější komunikace).....	50
-------------	---	----

Tabulka A.8	Datové cesty (vnitřní komunikace).....	50
-------------	--	----

Tabulka A.9	Napájecí zdroje.....	51
-------------	----------------------	----

Tabulka A.10	Pořadí programů	
--------------	-----------------	--

(hlídač).....	51
Tabulka A.11 Systém větrání a vytápění (je-li nutný).....	52
Tabulka A.12 Hodiny	52
Tabulka A.13 Komunikace a velkokapacitní paměť».....	53
Tabulka A.14 Senzory	53
Tabulka A.15 Koncové prvky (akční členy).....	54
Tabulka A.16 Techniky a opatření pro řízení systematických poruch způsobených návrhem hardwaru a softwaru.....	56
Tabulka A.17 Techniky a opatření pro řízení systematických poruch způsobených namáháním nebo vlivy prostředí	57
Tabulka A.18 Techniky a opatření pro řízení systematických provozních poruch.....	58
Tabulka A.19 Účinnost technik a opatření pro řízení systematických poruch.....	59
Tabulka B.1 Doporučení pro předcházení chybám a omylům při specifikaci požadavků E/E/PES (viz 7.2).....	62
Tabulka B.2 Doporučení pro předcházení chybám během návrhu a vývoje E/E/PES (viz 7.4).....	63
Tabulka B.3 Doporučení pro předcházení vadám během začleňování E/E/PES (viz 7.5).....	64
Tabulka B.4 Doporučení pro předcházení vadám a poruchám během provozních a údržbových postupů E/E/PES (viz 7.6)	65
Tabulka B.5 Doporučení pro předcházení vadám během potvrzování platnosti bezpečnosti E/E/PES	

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 system)) 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 system)) a využívané pro zajišťování 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/PE systémů 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 oborových 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 požadavků bezpečnosti 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 úrovně 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} ,
 - 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 neznamena nutně jednokanálovou architekturu.

Strana 10

- 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 část 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 principu;
- c) platí pro všechny dílčí systémy a jejich součásti v E/E/PE systému souvisejícím s bezpečností (včetně senzorů, akčních členů a rozhraní operátora);
- d) stanovuje způsob zpřesňování informací týkajících se požadavků celkové bezpečnosti získaných podle IEC 61508-1 a jejich přiřazování E/E/PE systémům souvisejícím s bezpečností, a stanovuje způsob dalšího zpřesňování požadavků celkové bezpečnosti prostřednictvím požadavků funkční bezpečnosti a integrity bezpečnosti E/E/PE systémů;
- e) stanovuje požadavky na činnosti, které se musí realizovat během návrhu a výroby E/E/PE systémů souvisejících s bezpečností (tj. stanovuje model životního cyklu bezpečnosti E/E/PES) s výjimkou softwaru, který je předmětem IEC 61508-3 (viz obrázky 2 a 3) - tyto požadavky zahrnují použití technik a opatření klasifikovaných z hlediska úrovně integrity bezpečnosti a zabráňujících a umožňujících řízení vad a poruch;
- f) stanovuje informace nezbytné pro instalaci, uvedení do provozu a konečné potvrzení platnosti bezpečnosti E/E/PE systémů souvisejících s bezpečností;
- g) neplatí pro fázi provozu a údržby E/E/PE systémů 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 E/E/PE systémů souvisejících s bezpečností;
- h) stanovuje požadavky, které má plnit organizace provádějící jakékoliv modifikace E/E/PE systémů souvisejících s bezpečností.

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

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

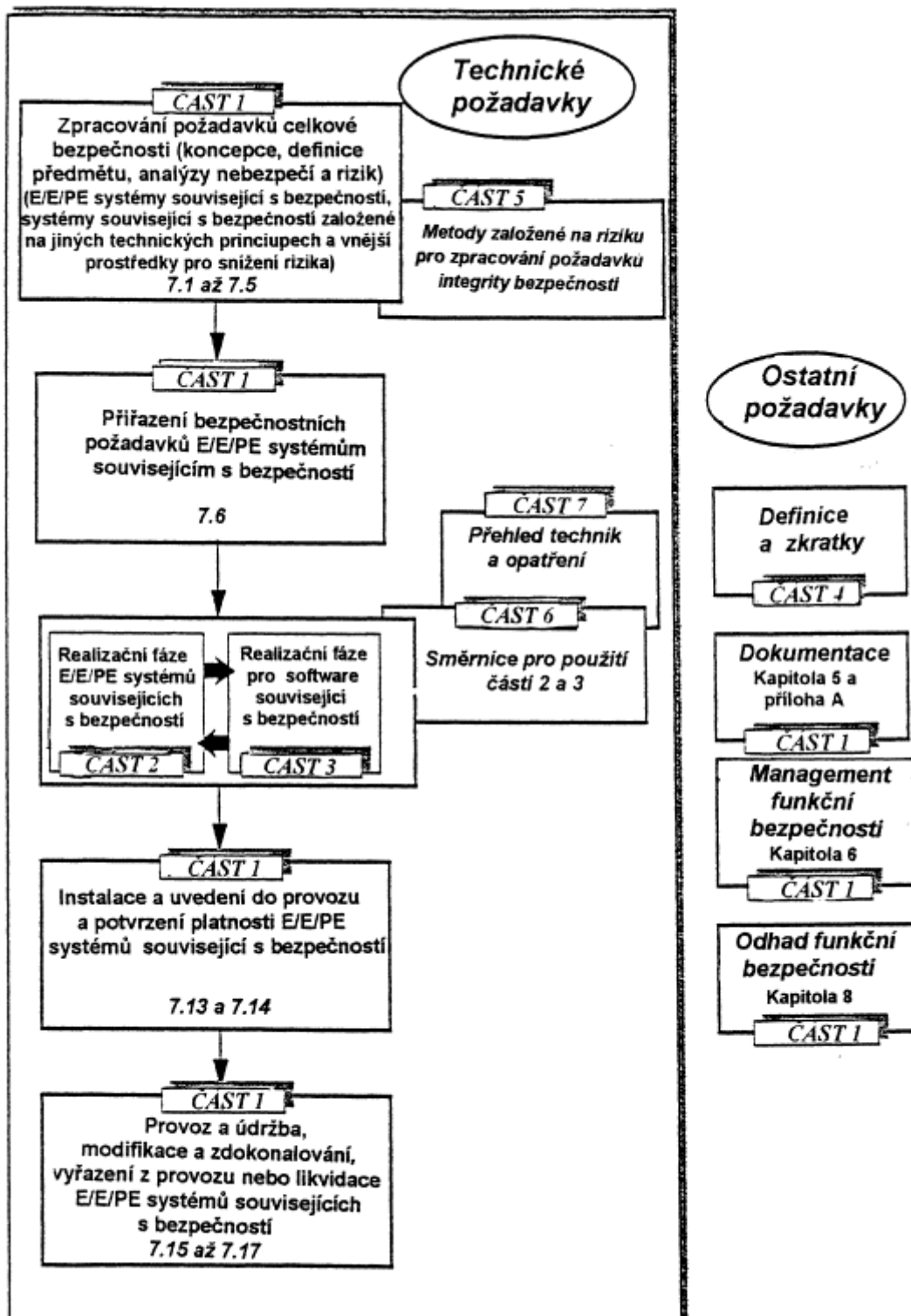
1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 a IEC 61508-4 jsou základní bezpečnostní normy, přestože tento status neplatí v kontextu jednoduchých E/E/PE systémů souvisejících s bezpečností (viz 3.4.4 IEC 61508-4). Jako základní normy bezpečnosti jsou určeny pro použití technickými komisemi při tvorbě norem podle zásad uvedených v pokynu IEC Guide 104 a pokynu ISO/IEC Guide 51. U IEC 61508 se také počítá s jejím použitím jako samostatné normy.

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 1 Funkční bezpečnost E/E/PE systému 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 zdokumentování.

POZNÁMKA 2 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).

1.3 Na obrázku 1 je ukázána celková struktura částí 1 až 7 IEC 61508 a vyznačena úloha, kterou má IEC 61508-2 z hlediska dosažení funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností. V příloze A v IEC 61508-6 je popsáno použití IEC 61508-2 a IEC 61508-3.



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 kterékoliv 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.

IEC 60050(371):1984 Mezinárodní elektrotechnický slovník - Kapitola 371: Dálkové ovládání

(International Electrotechnical Vocabulary - Chapter 371: Telecontrol)

IEC 60300-3-2:1993 Řízení spolehlivosti - Část 3: Návod k použití - Oddíl 2: Sběr dat o spolehlivosti z provozu

(Dependability management - Part 3: Application guide - Section 2: Collection of dependability data from the field)

IEC 61000-1-1:1992 Elektromagnetická kompatibilita (EMC) - Část 1: Všeobecně - Díl 1: Použití a interpretace základních definic a pojmů

(Electromagnetic compatibility (EMC) - Part 1: General - Section 1: Application and interpretation of fundamental definitions and terms)

IEC 61000-2-5:1995 Elektromagnetická kompatibilita (EMC) - Část 2: Prostředí - Díl 5: Klasifikace elektromagnetických prostředí - Základní norma EMC

(Electromagnetic compatibility (EMC) - Part 2: Environment - Section 5: Classification of electromagnetic environments - Basic EMC publication)

IEC 61508-1:1998 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností - Část 1: Všeobecné požadavky

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

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/electrical/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 systémů 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)

IEC Guide 104:1997 Tvorba bezpečnostních norem a použití základních a skupinových bezpečnostních norem

(The preparation of safety publications and the use of basic safety publications and group safety publications)

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

(Guidelines for the inclusion of safety aspects in standards)

IEEE 352:1987 Pokyn IEEE týkající se všeobecných principů analýzy bezporuchovosti bezpečnostních systémů jaderných elektráren)

(IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems)

-- Vynechaný text --