

2005

Funkční bezpečnost - Bezpečnostní přístrojové
systémy pro sektor průmyslových procesů -
Část 2: Metodický pokyn pro používání IEC 61511-1

ČSN
EN 61511-2

18 0303

idt IEC 61511-2:2003

Functional safety - Safety instrumented systems for the process industry sector -
Part 2: Guidelines for the application of IEC 61511-1

Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de
transformation -
Partie 2: Lignes directrices pour l'application de la CEI 61511-1

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie -
Teil 2: Anleitungen zur Anwendung des Teils 1

Tato norma je českou verzí evropské normy EN 61511-2:2004. Evropská norma EN 61511-2:2004 má
status
české technické normy.

This standard is the Czech version of the European Standard EN 61511-2:2004. The European
Standard
EN 61511-2:2004 has the status of the Czech Standard.



© Český normalizační institut, 2005

74297

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

Národní předmluva

Obdobné mezinárodní normy

IEC 61511-2:2003 Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1

(Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů - Část 2: Metodický pokyn pro používání IEC 61511-1)

Informativní údaje z IEC 61511-2:2003

Tato mezinárodní norma IEC 61511-2 byla připravena subkomisí 65A: Systémové aspekty, technické komise IEC 65: Měření a řízení průmyslových procesů.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
65A/387A/FDIS	65A/390/RVD

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

Upozornění na národní přílohy

Do normy byly doplněny informativní národní přílohy NA Rejstřík použitých zkratk a NB Rejstřík citovaných norem.

Vypracování normy

Zpracovatel: TENOR Praha, IČ 64924327, Lucie Krausová

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Ing. Jaromír Petřík

Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů -
Část 2: Metodický pokyn pro používání IEC 61511-1
Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1
(IEC 61511-2:2003)

Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation -
Partie 2: Lignes directrices pour l'application de la
CEI 61511-1
(CEI 61511-2:2003)

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie -
Teil 2: Anleitungen zur Anwendung des Teils 1
(IEC 61511-2:2003)

Tato evropská norma byla schválena CENELEC 2004-10-01. 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.

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

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

© 2004 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN 61511-

2:2004 E

Text mezinárodní normy IEC 61511-2:2004 vypracovaný SC 65A „Systémové aspekty“ technické komise IEC TC 65 „Měření a řízení průmyslových procesů“ byl předložen k Jednotnému schvalovacímu procesu a byl schválen CENELEC jako EN 61511-2 dne 2004-10-01 bez jakýchkoli změn.

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) 2005-10-01
- nejzazší datum zrušení národních norem,
které jsou s EN v rozporu (dow) 2007-10-01

Oznámení o schválení

Text mezinárodní normy IEC 61511-2:2003 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Strana 5

Obsah

Strana

Úvod

..... 7

1 Rozsah
platnosti

..... 9

2 Normativní
odkazy

..... 9

3 Termíny, definice a
zkratky

..... 9

4 Shoda s touto
normou

..... 9

5 Management funkční
bezpečnosti

..... 9

5.1
Cíl

..... 9

5.2

Požadavky

.....	9
6 Požadavky na životní cyklus bezpečnosti.....	14
6.1 Cíle.....	14
6.2 Požadavky.....	15
7 Verifikace.....	15
7.1 Cíl.....	15
8 Posouzení nebezpečí a rizik procesu.....	15
8.1 Cíle.....	15
8.2 Požadavky.....	15
9 Přiřazení bezpečnostních funkcí k ochranným vrstvám.....	18
9.1 Cíl.....	18
9.2 Požadavky na proces přiřazení.....	18
9.3 Přídavné požadavky pro úroveň integrity bezpečnosti 4.....	19

9.4	Požadavky na základní systém řízení procesů tvořící ochrannou vrstvu.....	19
9.5	Požadavky na prevenci poruch se společnou příčinou, společného režimu a závislých poruch.....	20
10	Specifikace bezpečnostních požadavků na SIS.....	21
10.1	Cíl.....	21
10.2	Všeobecné požadavky.....	21
10.3	Bezpečnostní požadavky na SIS.....	21
11	Návrh a konstrukce SIS.....	22
11.1	Cíl.....	22
11.2	Všeobecné požadavky.....	22
11.3	Požadavky na chování systému při detekci poruchy.....	26
11.4	Požadavky na toleranci k poruchám hardwaru.....	26
11.5	Požadavky na výběr součástí a subsystémů.....	27
11.6	Provozní zařízení.....	29
11.7	Rozhraní.....	29
11.9	Pravděpodobnost poruchy	

SIF.....	32
12 Požadavky na aplikační software včetně výběrových kritérií pro software obslužný.....	33
12.1 Požadavky na životní cyklus bezpečnosti aplikačního softwaru.....	33
12.2 Specifikace požadavků na bezpečnost aplikačního softwaru.....	36
12.3 Plánování validace bezpečnosti aplikačního softwaru.....	38
12.4 Návrh a vývoj aplikačního softwaru.....	38
12.5 Integrace aplikačního softwaru se subsystémem SIS.....	44

Strana 6

	Strana
12.6 Postupy modifikace softwaru FPL a LVL.....	44
12.7 Verifikace aplikačního softwaru.....	45
13 Tovární přijímací zkoušení (FAT).....	46
13.1 Cíle	46
13.2 Doporučení	46
14 Instalace SIS a jeho zařazení do výroby.....	46
14.1 Cíle	46
14.2	

Požadavky

..... 46

15 Validace bezpečnosti

SIS..... 46

15.1

Cíl

..... 46

15.2

Požadavky

..... 46

16 Provoz a údržba

SIS.....

47

16.1

Cíle

..... 47

16.2

Požadavky

..... 47

16.3 Kontrolní zkoušení a

inspekce..... 47

17 Modifikace

SIS

.. 48

17.1

Cíl

..... 48

17.2

Požadavky

..... 49

18 Vyřazení SIS z

provozu

..... 49

18.1

Cíle

..... 49

18.2

Požadavky

..... 49

19 Požadavky na informace a dokumentaci.....

49

19.1

Cíle

..... 49

19.2

Požadavky

..... 49

Příloha A (informativní) Příklad způsobu výpočtu pravděpodobnosti poruchy na vyžádání pro bezpečnostní
přístrojovou
funkci

51

Příloha B (informativní) Charakteristický vývoj architektury

SIS..... 52

Příloha C (informativní) Aplikační vlastnosti bezpečnostního

PLC..... 56

Příloha D (informativní) Příklad metodiky vývoje aplikačního softwaru logického automatu

SIS..... 58

Příloha E (informativní) Příklad vývoje externě konfigurované diagnostiky pro bezpečnostně konfigurovaný

logický automat

PE.....
62

Národní příloha NA (informativní) Rejstřík použitých

zkratk..... 64

Národní příloha NB (informativní) Rejstřík citovaných

norem..... 65

Obrázek 1 - Celková struktura této

normy..... 8

Obrázek 2 - Funkce BPCS a zobrazení nezávislosti působící příčiny.....	20
Obrázek 3 - Životní cyklus vývoje softwaru (model V).....	34
Obrázek C.1 - Logický automat.....	56
Obrázek E.1 - Časovací schéma EWDT.....	62
Tabulka 1 - Charakteristická struktura a obsah příručky bezpečnosti.....	42

Strana 7

Úvod

Bezpečnostní přístrojové systémy se používají již mnoho let k plnění bezpečnostních přístrojových funkcí v průmyslových procesech. Aby mohly být přístroje efektivně využívány v bezpečnostních přístrojových funkcích, je nezbytné dosáhnout určitých minimálních úrovní jejich normalizace.

Tato mezinárodní norma se vztahuje na používání bezpečnostních přístrojových systémů v průmyslových procesech. Též se týká rozhraní mezi bezpečnostními přístrojovými systémy a jinými bezpečnostními systémy tím, že požaduje provést posouzení nebezpečí a procesních rizik. Bezpečný přístrojový systém zahrnuje senzory, logické automaty a koncové členy.

Tato norma má vzhledem k svému použití dvě základní koncepce: životní cyklus bezpečnosti a úroveň integrity bezpečnosti. Životní cyklus bezpečnosti tvoří ústřední rámec spojující většinu koncepcí v této mezinárodní normě.

Logické automaty bezpečných přístrojových systémů jsou založeny na elektrické (E), elektronické (E) a programovatelné elektronické (PE) technice. Používají-li se pro logické automaty jiné techniky, mohou se základní zásady této normy využít. Tato norma rovněž platí pro senzory a koncové členy bezpečnostních přístrojových systémů bez ohledu na použitou techniku. Tato norma je pro průmyslové procesy charakteristická v rámci norem řady IEC 61508.

Tato norma ukazuje přístup k činnosti životního cyklu bezpečnosti s použitím minimálního počtu norem. Tento přístup byl přijat jako technická metoda racionální a konzistentní. Cílem této normy je poskytnout návod jak vyhovět IEC 61511-1.

Aby se používání této normy usnadnilo, jsou kapitoly a články očíslovány shodně s odpovídajícím normativním textem v 61511-1 (s výjimkou příloh).

Ve většině případů se bezpečnosti dosáhne nejlépe vnitřně bezpečným návrhem procesu, vždy kdykoli je to praktické, a pokud je to nutné, kombinováním s řadou ochranných systémů spoléhajících se na jiné technické systémy (např. chemické, mechanické, hydraulické, pneumatické, elektrické,

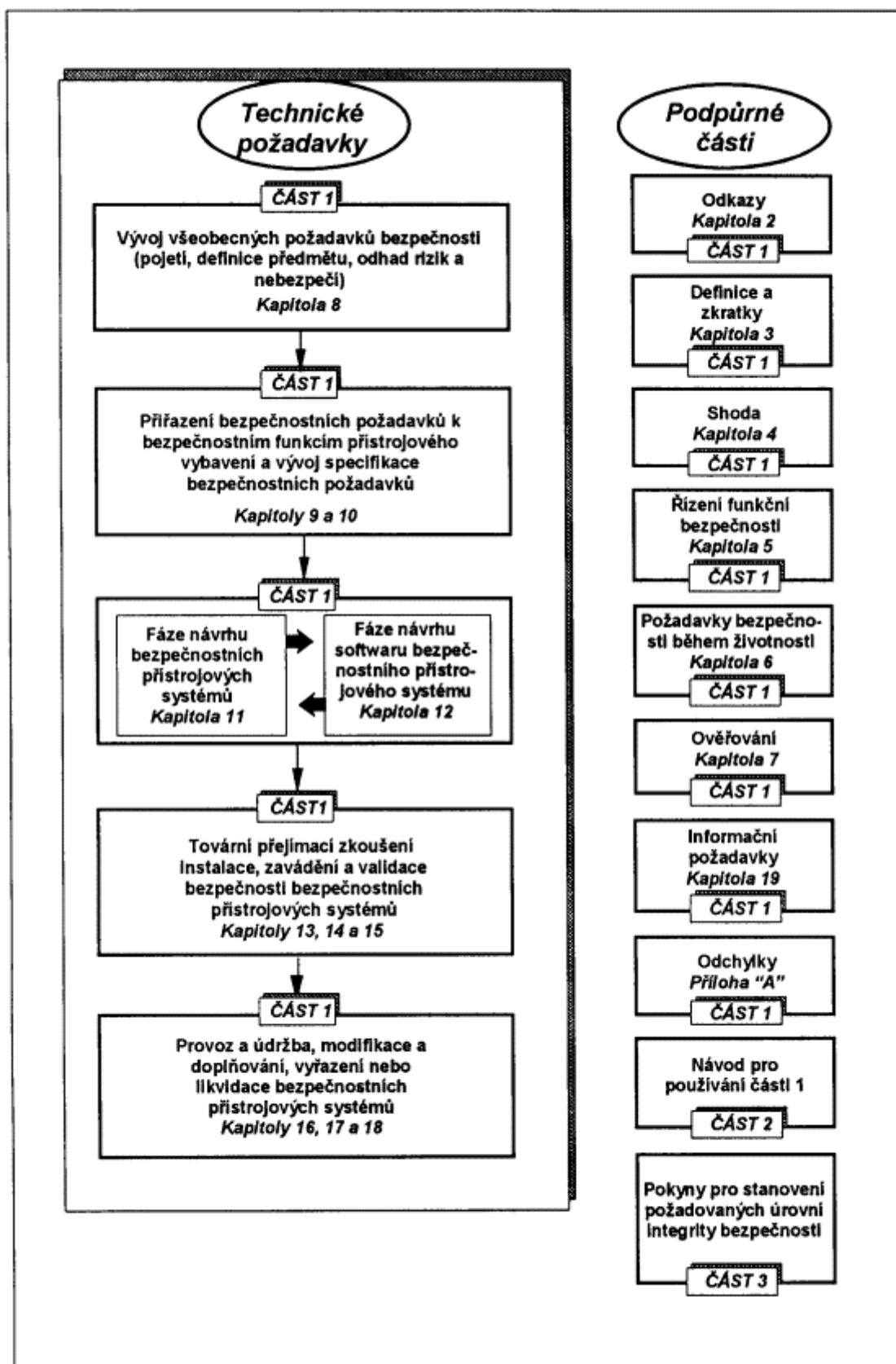
elektronické, termodynamické (např. omezovače plamene), programovatelné elektronické) určené k odstranění každého zbytkového identifikovaného rizika. Aby se tento přístup zjednodušil, tato norma:

- vyžaduje k zjištění celkových bezpečnostních požadavků, aby byla posouzena nebezpečí a rizika;
- vyžaduje, aby k bezpečnostním přístrojovým systémům bylo provedeno přidělení bezpečnostních požadavků;
- pracuje v rámci použitelném pro všechny přístrojové metody dosahování funkční bezpečnosti;
- uvádí podrobně používání některých činností, jako jsou řízení bezpečnosti, které se mohou použít ve všech metodách dosahování funkční bezpečnosti.

Tato mezinárodní norma na bezpečnostní přístrojové systémy pro průmyslové procesy:

- platí pro všechny fáze životního cyklu bezpečnosti od počátečního pojetí, návrhu, zavádění, provozu a údržby, až k vyřazení z provozu;
- umožňuje, aby existující nebo nové národní normy specifické pro průmyslové procesy byly s touto normou harmonizovány.

Tato norma je určena k zavádění vysoké úrovně konzistence (např. zásadními principy, terminologií, informacemi) v průmyslových procesech. To by mělo přinést jak bezpečnostní, tak ekonomické výhody.



Obrázek 1 - Celková struktura této normy

IEC 61511-2 poskytuje návody pro specifikaci, návrh, instalaci, provoz a údržbu bezpečnostních přístrojových funkcí a souvisejícího bezpečnostního přístrojového systému definovaného v IEC 61511-1. Tato norma je upravena tak, aby každá kapitola a každý článek odpovídaly stejným číslům v IEC 61511-1 (s výjimkou příloh).

2 Normativní odkazy

Další návody se neposkytují.

-- Vynechaný text --