ČESKÁ TECHNICKÁ NORMA

ICS 25.040.40 **Září**
2002

	Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností- Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3	ČSN EN 61508-6 18 0301

idt IEC 61508-6:2000

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

Sécurité fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Part 6: Lignes directrices pour l’application de la CEI 61508-2 et de la CEI 61508-3

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie fűr IEC 61508-2 und IEC 61508-3

Tato norma je českou verzí evropské normy EN 61508-6:2001. Evropská norma EN 61508-6:2001 má status české technické normy.

This standard implements the original version of the European Standard EN 61508-6:2001. The European Standard EN 61508-6:2001 has the status of the Czech Standard.

65445

Národní předmluva

Citované normy

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 61508-2:2000 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)

IEC 61508-3:1998 zavedena jako 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 + 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 61508-5:2000 zavedena v ČSN EN 61508-5:2002 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 5: Příklady metod určování úrovní integrity bezpečnosti (idt IEC 61508-5:1998 + IEC 61508-5:1998/Cor.:1999)

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)

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

IEC Guide 104:1997 nezaveden

Porovnání s mezinárodní normou

ČSN EN 61508-6 je identická s IEC 61508-6:2000, navíc však obsahuje normativní přílohu ZA „Normativní odkazy na mezinárodní publikace s jejich příslušnými evropskými publikacemi“, kterou doplnil CENELEC.

Informativní údaje z IEC 61508-6:2000

Tuto mezinárodní normu IEC 61508-6 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/295/FDIS	65A/304/RVD

Úplné informace o hlasování při schvalování této normy je možné nalézt ve zprávě o hlasování

uvedené v tabulce.

Tato norma byla navržena v souladu se Směrnicemi ISO/IEC, Část 3.

Přílohy A, B, C, D a E 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 úrovní integrity bezpečnosti

– Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3

– Část 7: Přehled technik a opatření

Komise rozhodla, že obsah zůstane nezměněn až do roku 2005. Potom bude tato norma

- potvrzena
- zrušena
- nahrazena přepracovaným vydáním nebo
- změněna.

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

Prázdná strana

EVROPSKÁ NORMA EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM	EN 61508-6 Prosinec 2001

ICS 25.040.40

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

Functional safety of electrical/electronic/programmable electronic safety-related system
Part 6: Guidelines for application of IEC 61508-2 and IEC 61508-3
(IEC 61508-6:2000)

Sécurité fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité -
Part 6: Lignes directrices pour l’application de la CEI 61508-2 et de la CEI 61508-3
(CEI 61508-6:2000)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme -
Teil 6: Anwendungsrichtlinie fűr IEC 61508-2 und IEC 61508-3
(IEC 61508-6:2000)

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 komitéty Belgie, České republiky, Dánska, Finska, Francie, Irska, Islandu, Itálie, Lucemburska, Malty, Německa, Nizozemska, Norska, Portugalska, Rakouska, Řecka, Spojeného království, ©panělska, ©védska a ©výcarska.

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

Ref. č. EN 61508-6:2001 E

Předmluva

Text této mezinárodní normy IEC 61508-6:2000 připravila subkomise 65A: „Systémové aspekty“ technické komise IEC TC 65 „Měření a řízení průmyslových procesů“ a byl předložen CENELEC k Jednotnému schvalovacími postupu a byl schválen CENELEC jako EN 61508-6 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 až E 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. 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 61508-6:2000 schválil CENELEC jako evropskou normu bez jakýchkoliv modifikací.

Obsah

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 zajiš»ování 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 zajiš»uje 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) 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 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 nízkým vyžádáním (malou poptávkou) je dolní mez pro plnění projektované funkce na vyžádání stanovena na střední pravděpodobnost poruchy 10^{-5},

  – v režimu provozu s vysokým 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 neznamená nutně jednokanálovou 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.

1 Rozsah platnosti

1.1 Tato část IEC 61508 obsahuje informace a metodické pokyny týkající se IEC 61508-2 a IEC 61508-3.

– Příloha A uvádí stručný přehled požadavků IEC 61508-2 a IEC 61508-3 a stanovuje funkční kroky pro jejich použití.

– Příloha B uvádí příklad techniky výpočetu pravděpodobností poruchy hardwaru a tuto přílohu se doporučuje číst spolu s přílohou D a v IEC 61508-2 uvedenou přílohou C a 7.4.3.

– Příloha C uvádí zpracovaný příklad výpočtu diagnostického pokrytí a tuto přílohu se doporučuje číst spolu s přílohou C v IEC 61508-2.

– Příloha D uvádí metodologii kvantifikace účinku společných poruch (poruch se společnou příčinou) souvisejících s hardwarem na pravděpodobnost poruchy.

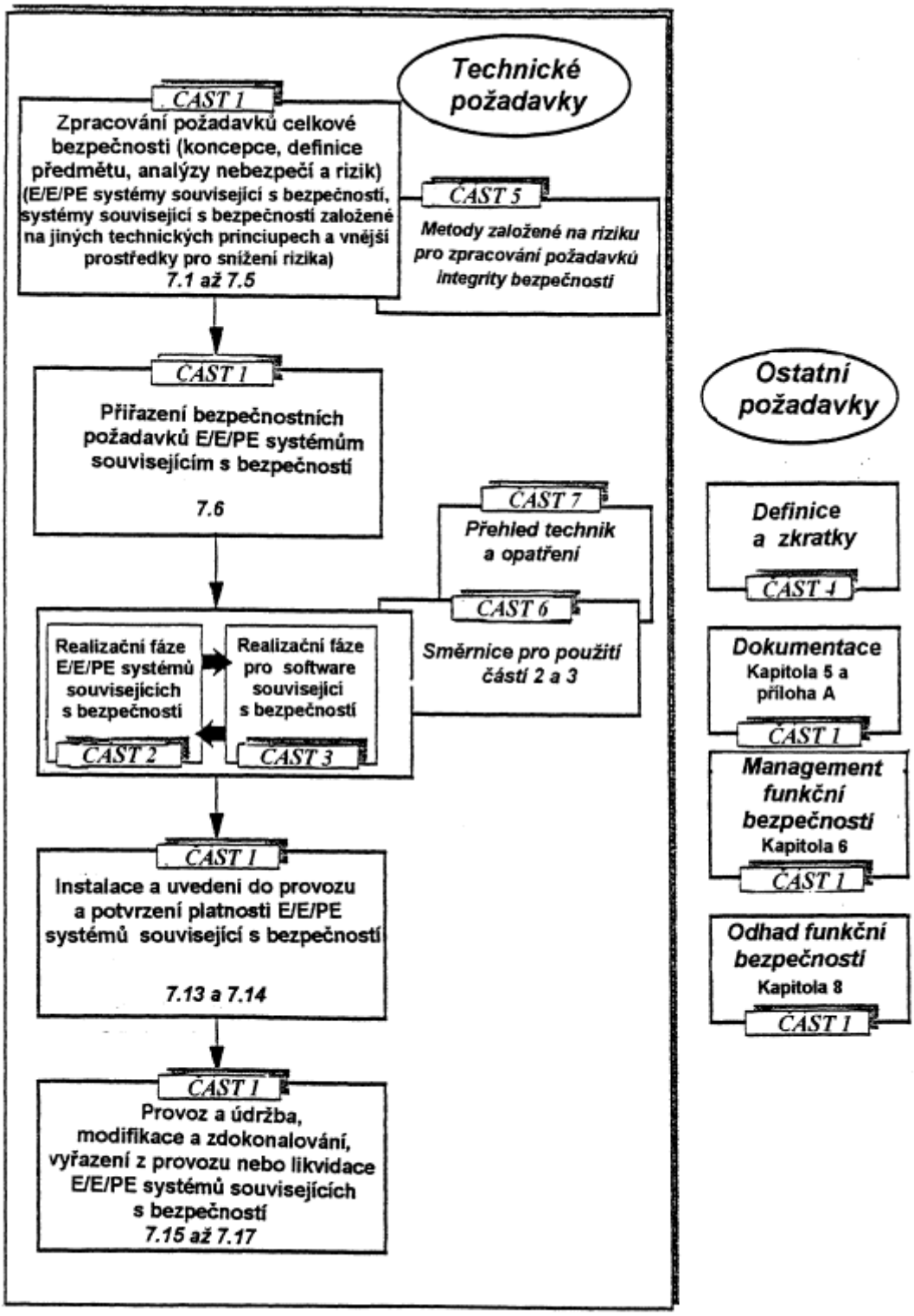
– Příloha E uvádí zpracované příklady použití tabulek integrity bezpečnosti softwaru stanovené v příloze A v IEC 61508-3 pro úrovně integrity bezpečnosti 2 a 3.

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 systémů E/E/PE souvisejících s bezpečností (viz 3.4.4 IEC 51808-4). 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 počítá také s jejím použitím jako samostatné normy.

1.3 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).

1.4 Na obrázku 1 je ukázána celková struktura částí 1 až 7 IEC 61508 a naznačena úloha, kterou má IEC 61508-6 na dosažení funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností.



Obrázek 1 - Celková struktura IEC 61508

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 61508 (všechny části) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících z bezpečností

(Functional safety of electrical/electronical/programmable electronic safety-related systems)

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

(Guide to the drafting standards and the role of committees with safety pilot functions and safety group functions)

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

(Guidelines for the inclusion of safety aspects in standards)

-- Vynechaný text --