

	Software pro počítače důležitý pro bezpečnost jaderných elektráren - Část 2: Aspekty softwaru týkající se ochrany před poruchami se společnou příčinou, použití softwarových nástrojů a již vyvinutého softwaru	ČSN IEC 60880-2 35 6587
---	---	-----------------------------------

Software for computers important to safety for nuclear power plants -

Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software

Logiciel pour les calculateurs de sûreté des centrales nucléaires -

Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés

Software für Rechner in Sicherheitssystemen von Kernkraftwerken -

Teil 2: Vorkehrungen gegen Versagen aufgrund von Software-Fehlern, Verwendung von Software-Werkzeugen und vorgefertigter Software

Tato norma je českou verzí mezinárodní normy IEC 60880-2:2000. Mezinárodní norma IEC 60880-2:2000 má status české technické normy.

This standard is the Czech version of the International Standard IEC 60880-2:2000. The International Standard IEC 60880-2:2000 has the status of a Czech Standard.

Národní předmluva

Citované normy

IEC 60780:1998 zavedena v ČSN IEC 60780:2001 (35 6609) Jaderné elektrárny - Elektrické zařízení bezpečnostního systému - Ověření způsobilosti (idt IEC 60780:1998)

IEC 60848:1988 nahrazena IEC 60848:2002 dosud nezavedenou

IEC 60880:1986 zavedena v ČSN IEC 880:1993 (35 6587) Programové prostředky počítačů bezpečnostních systémů jaderných elektráren (idt IEC 880:1986)

IEC 60987:1989 zavedena v ČSN IEC 987:1994 (35 6615) Počítačové systémy důležité pro bezpečnost jaderných elektráren (idt IEC 987:1989)

IEC 61069-2:1993 dosud nezavedena

IEC 61226:1993 zavedena v ČSN IEC 1226:2000 (35 6643) Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Klasifikace (idt IEC 1226:1993)

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 61513 dosud nezavedena

IEC/TR3 61940:1998 dosud nezavedena

ISO 9001:1994 zavedena v ČSN EN ISO:1997 (01 0321) Systémy jakosti. Model zabezpečování při návrhu, vývoji, výrobě. Instalaci a servisu

ISO/IEC 9126:1991 nahrazena ISO/IEC 9126-1:2001 dosud nezavedenou

MAAE 50-C-D (revize 1):1988 nezavedena

MAAE 50-SG-D3:1980 nezavedena

MAAE 50-SG-D8:1986 nezavedena

MAAE 50-SG-D11:1986 nezavedena

MAAE 50-C-QA6:1981 nezavedena

POZNÁMKA Příručky MAAE jsou k dispozici v Ústavu jaderných informací, Elišky Přemyslovny 1335, Praha 5 - Zbraslav

IEEE 610:1990 nezavedena

Související ČSN

ČSN IEC 880:1993 (35 6587) Programové prostředky počítačů bezpečnostních systémů jaderných elektráren

Vypracování normy

Zpracovatel: Bohumil Hájek, IČO 44368933

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Tomáš Pech

Strana 3

MEZINÁRODNÍ NORMA

Software pro počítače důležitý pro bezpečnost
jaderných elektráren -

Část 2: Aspekty softwaru týkající se ochrany před poruchami
se společnou příčinou, použití softwarových nástrojů
a již vyvinutého softwaru

IEC 60880-2

První vydání

2000-12

Obsah

Strana

Předmluva

..... 5

Úvod

..... 6

1 Rozsah platnosti a předmět

normy..... 7

2 Normativní

odkazy

..... 7

3 Definice a

zkratky

..... 7

4 Požadavky a

doporučení

..... 9

4.1	Ochrana před poruchami se společnou příčinou vlivem softwaru.....	9
4.1.1	Úvod.....	9
4.1.2	Návrh softwaru proti CCF.....	10
4.1.3	Zdroje a účinky CCF způsobené softwarem.....	11
4.1.4	Implementace diverzity.....	11
4.1.5	Srovnání nevýhod a výhod spojených s použitím diverzity.....	12
4.2	Softwarové nástroje k vývoji softwaru.....	12
4.2.1	Úvod.....	12
4.2.2	Výběr nástrojů.....	12
4.2.3	Požadavky na nástroje.....	13
4.3	Prokázání způsobilosti již vyvinutého softwaru.....	16
4.3.1	Úvod.....	16
4.3.2	Všeobecné požadavky.....	17
4.3.3	Proces vyhodnocení a posouzení.....	17

4.3.4 Požadavky na integraci do systému a údržbu PDS.....	22
Příloha A Úvahy o CCF a diverzitě.....	25
A.1 CCF způsobené softwarem.....	25
A.2 Potenciální příčiny a důsledky CCF.....	25
A.3 Ochrana před CCF	26
A.4 Prokázání správnosti	26
A.5 Rysy diverzity	26
A.6 Nevýhody, výhody a zdůvodnění diverzity.....	27
Příloha B Požadavky IEC 60880 na používání a prokázání způsobilosti softwarových nástrojů.....	29
Příloha C Nástroje k vytváření a kontrole specifikace, návrhu a kódu.....	30
C.1 Konstruktivní nástroje	30
C.2 Analytické nástroje	30
Strana 4	
Strana	
Příloha D Požadavky IEC 60880 týkající se PDS	32
D.1 Souhrn požadavků IEC 60880 týkajících se PDS.....	32

D.2	Dokumentace k vyhodnocení	
PDS.....		32
D.3	Návod na výběr použitelných požadavků IEC	
60880.....		33
D.4	Návod na rozdělení nesouladů a kompenzační	
činitelé.....		33
D.5	Sběr a validace dat o provozní	
historii.....		34
Literatura		
.....		35
Obrázek 1 - Diagram prokázání způsobilosti již vyvinutého		
softwaru.....		23
Obrázek 2 - Vztah vyhodnocení a posouzení PDS s plánem prokázání způsobilosti systému, do kterého		
je		
integrován		
.....		24

Předmluva

- 1) IEC (Mezinárodní elektrotechnická komise) je celosvětovou normalizační organizací, zahrnující všechny národní elektrotechnické komitety (národní komitety IEC). Cílem IEC je podporovat mezinárodní spolupráci ve všech otázkách, které se týkají normalizace v oblasti elektrotechniky a elektroniky. Za tím účelem, kromě jiných činností, IEC vydává mezinárodní normy. Jejich příprava je svěřena technickým komisím, každý národní komitét IEC, který se zajímá o projednávaný předmět, se může těchto přípravných prací zúčastnit. Mezinárodní vládní i nevládní organizace, s nimiž IEC navázala pracovní styk se této přípravy rovněž zúčastňují. IEC úzce spolupracuje s Mezinárodní organizací pro normalizaci (ISO) v souladu s podmínkami dohodnutými mezi těmito dvěma organizacemi.
- 2) Oficiální rozhodnutí nebo dohody IEC týkající se technických otázek vyjadřují v největší možné míře mezinárodní shodu v názoru na předmět, kterého se týkají, jelikož jsou v každé technické komisi zastoupeny všechny zainteresované národní komitety.
- 3) Vypracované dokumenty mají formu doporučení pro mezinárodní použití publikovaných formou norem, technických zpráv nebo pokynů a v tomto smyslu jsou přijímány národními komitety.
- 4) Na podporu mezinárodního sjednocení národní komitety IEC přebírají mezinárodní normy IEC transparentně v maximální možné míře do svých národních a regionálních norem. Každý rozdíl mezi normou IEC a odpovídající národní nebo regionální normou se v těchto normách jasně vyznačí.
- 5) IEC nemá žádný postup týkající se vyznačování schválení a nenese žádnou odpovědnost za prohlášení o shodě předmětu s některou jeho normou.
- 6) Upozorňuje se na možnost, že některé prvky této mezinárodní normy mohou být předmětem patentových práv. IEC

není možné činit odpovědnou za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Mezinárodní norma IEC 60880-2 byla připravena subkomisí 45A: Přístroje pro reaktory, která je součástí technické komise IEC TC 45: Přístroje jaderné techniky.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
45A/402/FDIS	45A/406/RVD

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

Tato norma byla navržena ve shodě se směrnicemi ISO/IEC, Část 3.

Přílohy A, B, C a D jsou pouze informativní.

Když bude IEC 60880 (1986) revidována, bude publikována jako IEC 60880-1.

Komise rozhodla, že obsah této normy zůstane nezměněn do roku 2006. V tomto termínu bude norma

- potvrzena;
- stažena;
- nahrazena novým vydáním nebo
- změněna.

Strana 6

Úvod

Tato část IEC 60880 obsahuje požadavky na software pro bezpečnostní systémy využívající počítače v jaderných elektrárnách a měla by být používána společně s IEC 60880. Tato část obsahuje požadavky v několika oblastech souvisejících s pokrokem a zkušenostmi se systémy softwaru používanými v oboru bezpečnosti v období od vydání IEC 60880.

Ochrana před závadami softwaru, které mohou vést k poruše se společnou příčinou (CCF) (CCF - Common Cause Failure) systémů využívajících počítače, musí být ve shodě s bezpečnostní řadou MAAE č. 50-C-D a jsou uvedeny technické požadavky vyplývající z těchto opatření. Také rychle vzrostlo použití počítačových nástrojů a jsou uvedeny požadavky na jejich používání. Praktické použití softwaru pro bezpečnostní systémy využívající počítače často závisí na použití již vyvinutého softwaru a s tímto jsou uvedeny související požadavky a doporučení.

Tato část IEC 60880 se odkazuje na základní bezpečnostní normu IEC 61513.

Tato část platí pro kategorii A funkcí systému I&C a přidružené systémy a zařízení (FSE) v IEC 61226.

POZNAMKA Podle klasifikace IEC 61513 jsou funkce kategorie A použity v systémech třídy 1, které odpovídají bezpečnostním systémům MAAE.

1 Rozsah platnosti a předmět normy

Tato část IEC 60880 platí pro software bezpečnostních systémů využívajících počítače v jaderných elektrárnách. Uvádí požadavky pro software funkcí kategorie A, systémů a přidružených zařízení (FSE). Vztahuje se na:

- ochranu před poruchami se společnou příčinou, způsobených softwarem;
- automatizované nástroje k vývoji softwaru důležitého pro bezpečnost; a
- použití již vyvinutého softwaru.

O přípravě a schválení údajů se pojednává v příslušných třech tématech.

2 Normativní odkazy

Součástí této části IEC 60880 jsou i ustanovení dále uvedených norem, na něž jsou odkazy v textu této části IEC 60880. V době uveřejnění této části IEC 60880 byla platná uvedená vydání. Všechny normy podléhají revizím a účastníci, kteří uzavírají dohody na podkladě této části IEC 60880, by měli využít nejnovějšího vydání dále uvedených norem. Členové IEC a ISO udržují seznamy platných mezinárodních norem.

IEC 60880:1986 Programové prostředky počítačů bezpečnostních systémů jaderných elektráren
(*Software for computers in the safety systems of nuclear power stations*)

IEC 61226:1993 Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Klasifikace
(*Nuclear power plants - Instrumentation and control systems important for safety - Classification*)

IEC 61508-4:1998 Funkční bezpečnost elektrických/elektronických/programových elektronických systémů vztahených k bezpečnosti - Část 4: Definice a zkratky
(*Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations*)

IEC 61513 Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Všeobecné požadavky na systémy
(*Nuclear power plants - Instrumentation and control systems important for safety - General requirements for systems*)¹⁾

ISO/IEC 9126:1991 Informační technika - Ověření softwaru - Charakteristiky jakosti a návod na jejich použití
(*Information technology - Software product evaluation - Quality characteristics and guidelines for their use*)

MAAE 50-C-D (1. vydání):1988 Kód o bezpečnosti jaderných elektráren: Projekt
(*IAEA 50-C-D (rev. 1):1988, Code of the safety of Nuclear Power Plants: Design*)

MAAE 50-SG-D11:1986 Obecné bezpečnostní zásady pro projektování jaderných elektráren

(IAEA 50-SG-D11:1986, General design safety principles for nuclear power plants - A safety guide)

IEEE 610:1990 Normalizovaný slovník terminologie softwarového inženýrství
(Standard glossary of software engineering terminology)

-- Vynechaný text --