

2005

Jaderné elektrárny - Instrumentace a řízení
důležité pro bezpečnost - Softwarová hlediska
pro systémy využívající počítače vykonávající
funkce kategorie B nebo C

ČSN
IEC 62138
35 6665

Nuclear power plants - Instrumentation and control important to safety - Software aspects for
computer-based systems
performing category B or C functions

Centrales nucléaires - Instrumentation et contrôle-commande importants pour la sûreté - Aspects
logiciels des systèmes
informatisés réalisant des fonctions de catégorie B ou C

Tato norma je českou verzí mezinárodní normy IEC 62138:2004. Mezinárodní norma IEC 62138:2004
má status české technické normy.

This standard is the Czech version of the International Standard IEC 62138:2004. The International
Standard IEC 62138:2004 has the status of a Czech Standard.



© Český normalizační institut, 2005

72060

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

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

IEC 61513:2001 zavedena v ČSN IEC 61513:2003 (35 6654) Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Všeobecné požadavky na systémy (idt IEC 61513:2001)

Související směrnice

Zákon o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů (č. 18/1997 Sb.)

Vyhláška Státního úřadu pro jadernou bezpečnost o zabezpečování jakosti při činnostech souvisejících s využíváním jaderné energie a činnostech vedoucích k ozáření a o stanovení kritérií pro zařazení a rozdělení vybraných zařízení do bezpečnostních tříd (č. 214/1997 Sb.)

Upozornění na národní poznámku

Do této normy byla ke kapitole 1 doplněna informativní národní poznámka.

Vypracování normy

Zpracovatel: Bohumil Hájek, IČ 44368933

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Tomáš Pech

Strana 3

MEZINÁRODNÍ NORMA

Jaderné elektrárny - Instrumentace a řízení důležité pro bezpečnost -
Softwarová hlediska pro systémy využívající počítače vykonávající
funkce kategorie B nebo C

IEC 62138
První vydání
2004-01

Obsah

Strana

Predmluva

.....
..... 5

Úvod

.....
..... 6

1 Rozsah platnosti

.....

.....	7
2 Normativní odkazy	
.....	7
3 Termíny, definice a zkratky	
.....	7
4 Základní pojetí a předpoklady	12
4.1 Typy softwaru	
.....	12
4.2 Typy dat	
.....	13
4.3 Životní cyklus bezpečnosti systému a softwaru.....	14
4.4 Principy stupňování	
.....	17
5 Požadavky na software systémů I&C vykonávající funkce kategorie C.....	18
5.1 Všeobecné požadavky	
.....	18
5.2 Výběr již vyvinutého softwaru	21
5.3 Specifikace požadavků na software.....	22
5.4 Návrh softwaru	
.....	23

5.5	Realizace nového softwaru	24
5.6	Softwarová hlediska integrace systému.....	25
5.7	Softwarová hlediska validace systému.....	25
5.8	Instalace softwaru na místě určení.....	26
5.9	Záznamy o odchylkách	26
5.10	Modifikace softwaru	26
6	Požadavky na software systémů I&C vykonávající funkce kategorie B.....	27
6.1	Všeobecné požadavky	27
6.2	Výběr již vyvinutého softwaru	30
6.3	Specifikace požadavků na software.....	34
6.4	Návrh softwaru	35
6.5	Realizace nového softwaru	37
6.6	Softwarová hlediska integrace systému.....	39
6.7	Softwarová hlediska validace	

systému.....	39
6.8 Instalace softwaru na místě určení.....	40
6.9 Záznamy o odchylných	40
6.10 Modifikace softwaru	40
Bibliografie	42

Strana 4

Strana

Obrázek 1 - Typické části softwaru v systémech I&C využívajících počítač.....	12
Obrázek 2 - Činnosti životního cyklu bezpečnosti systému (podle definice v IEC 61513).....	13
Obrázek 3 - Činnosti související se softwarem v životním cyklu bezpečnosti systému.....	14
Obrázek 4 - Činnosti vývoje životního cyklu bezpečnosti systému v IEC 62138.....	15
Obrázek 5 - Postup zajištění ověření správnosti pro již vyvinutý software systému I&C bezpečnostní třídy 2.....	16

Strana 5

Předmluva

- 1) IEC (Mezinárodní elektrotechnická komise) je celosvětovou normalizační organizací, zahrnující všechny národní elektrotechnické komitáty (národní komitáty 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 komitát IEC, který se zajímá o projednávání 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. I když je věnováno velké úsilí na to, aby byl technický obsah publikací IEC přesný, IEC nemůže být odpovědná za způsob, jakým jsou používány nebo za jakoukoliv chybnou interpretaci uživatelem..
- 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) Uživatelé by si měli zajistit poslední vydání této normy.
- 7) IEC ani její řídicí pracovníci, zaměstnanci, pomocné síly nebo zástupci včetně samostatných expertů a členů technických komisí a národních komisí IEC neodpovídají za jakékoliv zranění osob, poškození majetku nebo poškození čehokoliv, a» už přímé nebo nepřímé, nebo za náklady (včetně právních poplatků) a výdaje spojené s publikací, používáním a spoléháním se na tuto normu IEC nebo jiné publikace IEC.
- 8) Je věnována pozornost normativním odkazům citovaným v této normě. Používání citovaných publikací je nezbytné ke správnému používání této normy.
- 9) Upozorňuje se na možnost, že některé prvky této mezinárodní normy mohou být předmětem patentových práv. IEC nelze činit odpovědnou za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Mezinárodní norma IEC 62138 byla připravena subkomisí 45A: Instrumentace a řízení v jaderných zařízeních, která je součástí technické komise IEC TC 45: Přístroje jaderné techniky.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
45A/507/FDIS	45A/521/RVD

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

Tato norma byla připravena podle Směrnice ISO/IEC, Část 2.

Komise rozhodla, že obsah této normy zůstane nezměněn do roku 2009. V tomto termínu bude norma

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

Úvod

Struktura souboru norem SC 45A - Vztahy mezi dokumenty IEC, IAEA a ISO

Vstupním bodem souboru norem SC 45A je IEC 61513. Tato norma se zabývá všeobecnými požadavky na systémy a zařízení kontroly a řízení (systémy I&C), které se používají k provádění funkcí důležitých pro bezpečnost v jaderných elektrárnách (JE), a dále se zabývá strukturou souboru norem SC 45A.

IEC 61513 se odkazuje přímo na jiné normy SC 45A v souvislosti se všeobecnými pojmy vztahujícími se ke kategorizaci funkcí a klasifikaci systémů, prokázání způsobilosti, oddělení systémů, softwarovým a hardwarovým hlediskům systémů využívajícím počítače, návrhu dozoren a multiplexnímu provozu. Normy odkazované přímo se považují společně s IEC 61513 za konzistentní soubor dokumentů.

Další normy SC 45A, na které IEC 61513 přímo neodkazuje, jsou normy související s jednotlivými zařízeními, technickými metodami nebo specifickými činnostmi. Tyto dokumenty nižší úrovně, které se odkazují na dříve popsané dokumenty vyšší úrovně pro všeobecné pojmy, mohou být obvykle používány samostatně.

IEC 61513 přijala strukturu provedení podobnou jako základní bezpečnostní normy IEC 61508, s rámcem celkového životního cyklu bezpečnosti a rámcem životního cyklu bezpečnosti systému a poskytuje výklad všeobecných požadavků IEC 61508, části 1, 2 a 4 pro oblast jaderných aplikací. Shoda s IEC 61513 usnadní shodu s požadavky IEC 61508, protože ty byly interpretovány pro jaderný průmysl. V tomto rámci IEC 60880 a IEC 62138 odpovídá IEC 61508, část 3 pro oblast jaderných aplikací.

IEC 61513 odkazuje na ISO jakož i na IAEA 50-C-QA (nyní nahrazeno IAEA 50-C/SG-Q) pro pojmy souvisejícími se zajištěním jakosti.

Soubor norem SC 45A zavádí důsledně a podrobně zásady a základní hlediska bezpečnosti uvedené v kódu IAEA o bezpečnosti jaderných elektráren a v bezpečnostní řadě IAEA, především požadavky NS-R-1, „Bezpečnost jaderných elektráren: Návrh“ a Bezpečnostní příručka NS-G-1.3, „Systémy kontroly a řízení důležité pro bezpečnost v jaderných elektrárnách“. Terminologie a definice používané normami SC 45A jsou ve shodě terminologií a definicemi používanými IAEA.

Strana 7

1 Rozsah platnosti

Tato mezinárodní norma stanoví požadavky pro systémy využívající počítače vykonávající funkce kategorie B nebo C, jak je definováno v IEC 61226. Doplnjuje IEC 60880 a IEC 60880-2, které určují požadavky na systémy využívající počítače vykonávající funkce kategorie A.

Je také ve shodě a doplňuje IEC 61513. Činnosti, které jsou převážně činnostmi na úrovni systému (například integrace, validace a instalace), se norma nezabývá podrobně: požadavky, které se netýkají specificky softwaru, jsou přenechány normě IEC 61513.

IEC 61513 definuje bezpečnostní třídy systémů I&C důležitých pro bezpečnost takto:

- systémy I&C bezpečnostní třídy 1 jsou určeny k provádění bezpečnostních funkcí kategorie A, ale

mohou také plnit bezpečnostní funkce kategorie B a/nebo C a z bezpečnostního hlediska neklasifikované funkce;

- systémy I&C bezpečnostní třídy 2 jsou určeny k provádění bezpečnostních funkcí kategorie B, ale mohou také plnit bezpečnostní funkce kategorie C a z bezpečnostního hlediska neklasifikované funkce;
- systémy I&C bezpečnostní třídy 3 jsou určeny k provádění bezpečnostních funkcí kategorie C, ale mohou také plnit z bezpečnostního hlediska neklasifikované funkce.

Protože daný klasifikovaný systém I&C může z bezpečnostního hlediska provádět funkce různých bezpečnostních kategorií a dokonce neklasifikovaných funkcí, požadavky této normy jsou zaměřeny na bezpečnostní třídu systému I&C.

Tato norma bere v úvahu současné metody vývoje softwaru pro systémy I&C, především:

- použití předem vyvinutého softwaru, zařízení a třídy zařízení, které nebylo nutně navrženo pro oblast jaderného průmyslu;
- použití speciálních zařízení „černých skříněk“ * se zabudovaným softwarem;
- použití aplikačně zaměřených jazyků.

Tato norma není určena k použití jako univerzální příručka pro softwarové inženýrství. Stanoví požadavky, které musí software systémů I&C bezpečnostních tříd 2 a 3 splňovat, aby bylo dosaženo bezpečnostních cílů jaderných systémů.

2 Normativní odkazy

Pro použití této normy jsou nezbytné následující dokumenty. Pro datované odkazy platí pouze citované vydání. Pro nedatované odkazy platí poslední vydání citovaného dokumentu (včetně jakýchkoliv změn).

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

IEC 61513:2001 Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Všeobecné požadavky na systémy
(*Nuclear power plants - Instrumentation and control for system important to safety - General requirements for systems*)

-- Vynechaný text --