ČESKÁ TECHNICKÁ NORMA

ICS 27.120.20 **Únor 2003**

	Jaderné elektrárny - Kontrolní a řídicí funkce důležité pro bezpečnost - Použití pravděpodobnostního hodnocení bezpečnosti ke klasifikaci	ČSN IEC 61838 35 6652

idt IEC TR 61838:2001

Nuclear power plants - Instrumentation and control functions important for safety - Use of probabilistic safety assessment
for the classification

Centrales nucléaires - Fonctions d'instrumentation et de contrôle-commande importants pour la sûreté - Utilisation des
évaluations probabilistes de sûreté pour le classesment

Kernkraftwerke - Für die Sicherheit wichtige Leittechnik-Funktionen - Anwendung der probabilistischen
Sicherheitsbeurteilung für die Klassifizierung

Tato norma je českou verzí technické zprávy IEC 61838:2001. Technická zpráva IEC 61838:2001 má status české technické normy.

This standard is the Czech version of the Technical Report IEC 61838:2001. The Technical Report IEC 61838:2001 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 60812:1985 zavedena v ČSN IEC 812:1991 (01 0675) Metody analýzy spolehlivosti systému - Postup analýzy způsobů a důsledků poruch (FMEA) (idt HD 485 S1:1987, idt IEC 812:1985)

IEC 60863:1986 zavedena v ČSN IEC 863:1991 (01 0621) Prezentace předpovědí bezporuchovosti, udržovatelnosti a pohotovosti (idt IEC 863:1986)

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

IEC 60964:1989 zavedena v ČSN IEC 964:1994 (35 6618) Navrhování dozoren pro jaderné elektrárny (idt IEC 964:1989)

IEC 60980:1989 zavedena v ČSN IEC 980:1993 (35 6614) Doporučené způsoby ověřování seizmické způsobilosti elektrického zařízení bezpečnostního systému jaderných elektráren (idt IEC 980:1989)

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

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 soubor zaváděn v souboru ČSN EN 61508 (18 0301) Funkční bezpečnost elektrických/-elektronických/programovatelných elektronických systémů souvisejících s bezpečností

Bezpečnostní příručka MAAE 50-SG-D8:1984 Systémy kontroly a řízení související s bezpečností jaderných elektráren

INSAG 3: Základní bezpečnostní zásady pro jaderné elektrárny

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

Souvisící normy

ČSN IEC 50(191):1993 (01 0102) Medzinárodný elektrotechnický slovník - Kapitola 191: Spoµahlivos» a akos» služieb

ČSN ISO 3534-2:1994 (01 0216) Statistika - Slovník a značky - Část 2: Statistické řízení jakosti

ČSN EN ISO 9000:2001 (01 0300) Systémy managementu jakosti - Základy, zásady a slovník (idt ISO 9000:2000)

ČSN IEC 1025:1994 (01 0676) Analýza stromu poruchových stavov

ČSN IEC 300-3-9:1997 (01 0690) Management spolehlivosti - Část 3: Návod k použití - Oddíl 9: Analýza rizika technologických systémů

ČSN EN 60300-2:1997 (01 0690) Management spolehlivosti - Část 2: Prvky a úkoly programu spolehlivosti

Upozornění na národní poznámky

Do normy byly k článkům 3.1.7, 3.1.16, 5.2.1, 5.2.2.1, 5.2.3, 6.4.2, 6.4.3, 6.5.1 a A.3.2 doplněny informativní národní poznámky.

Vypracování normy

Zpracovatel: Bohumil Hájek, IČO 44368933

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Tomáš Pech

TECHNICKÁ ZPRÁVA
Jaderné elektrárny - Kontrolní a řídicí funkce důležité pro bezpečnost - Použití pravděpodobnostního hodnocení bezpečnosti ke klasifikaci

IEC TR 61838
První vydání
2001-02

Obsah

Strana

Předmluva

1) IEC (Mezinárodní elektrotechnická komise) je celosvětovou normalizační organizací, zahrnující všechny národní elektrotechnické komitéty (národní komitéty 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 komitéty.

3) Vypracované dokumenty mají formu doporučení pro mezinárodní použití publikovaných formou norem, technických zpráv nebo pokynů a v tomto smyslu jsou přijímány národními komitéty.

4) Na podporu mezinárodního sjednocení národní komitéty 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 nelze činit odpovědnou za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Hlavní úlohou technických komisí IEC je příprava mezinárodních norem. Technická komise však může navrhnout publikování technické zprávy, když tato zpráva zahrnuje údaje odlišné od údajů běžně publikovaných jako mezinárodní norma, například „stav znalostí“.

IEC 61838, jež je technickou zprávou, byla připravena subkomisí 45A: Přístroje pro reaktory, která je součástí technické komise IEC TC 45: Přístroje jaderné techniky.

Text této technické zprávy vychází z těchto dokumentů:

Dotazovací návrh	Zpráva o hlasování
45A/363/CDV	45A/388/RVC

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

Tato publikace byla připravena podle směrnice ISO/IEC, Část 3.

Tento dokument, který je čistě informativní, není možné považovat za mezinárodní normu.

Přílohy A a B jsou pouze informativní.

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

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

Úvod

IEC 61226 Jaderné elektrárny - Systémy kontroly a řízení importantní pro bezpečnost - Klasifikace byla vydána v roce 1993. Potřeba klasifikovat kontrolní a řídicí funkce v jaderných elektrárnách vychází z doporučení Mezinárodní agentury pro atomovou energii (MAAE), (International Atomic Energy Agency (IAEA)). IEC 61226 zdůrazňuje, že to jsou **funkce**, které musí být klasifikovány na počátku etapy projektování, takže je stanoven stupeň importance pro bezpečnost každé funkce. V etapě projektu jsou funkce systému I&C rozděleny do jednotlivých systémů kontroly a řízení, z nichž každý obvykle obsahuje několik typů zařízení. Tyto systémy a zařízení jsou obvykle zařazeny do bezpečnostních kategorií, ale jsou to funkce, které určují základní kategorizaci.

K zajištění spojení systémů a zařízení s funkcemi byl v IEC 61226 zaveden pojem FSE. FSE je definován jako:

> Funkce a přidružené systémy a zařízení. Funkce se vykonávají pro nějaký účel nebo k dosažení nějakého cíle. Přidružené systémy a zařízení jsou soubory komponent a samostatných části, které

se používají k vykonání těchto funkcí.

IEC 61226 poskytuje metodu kategorizace pro FSE založenou na kvalitativních kritériích. Většina kritérií je jadernému průmyslu dobře srozumitelná, protože vyjadřují, že jediná a nejdůležitější jaderná bezpečnostní funkce je zabránění haváriím a zmírnění úniků štěpných produktů. Proto je klasifikace FSE v IEC 61226 deterministický proces a neuvažuje postupy s kvantitativním hodnocením rizika.

V posledních deseti letech metody hodnocením rizika dozrály, zvláště k použití v jaderných elektrárnách, i když je jejich použití v projektu JE (a povolování) ve světě značně rozdílné. V některých zemích se pravděpodobnostní hodnocení rizika jeví jako podstatná součást procesu projektu a konečného hodnocení bezpečnosti; v jiných zemích tomu tak není.

Několik let se diskutuje o tom, jak by mohlo být klasifikační schéma založené na riziku začleněno do IEC 61226. Jak je naznačeno výše, ve světě existují významné rozdíly v použití hodnocení rizika, což při návrhu mezinárodní normy vede k několika problémům, především:

a) Měly by být přijatelné klasifikační schéma založené na riziku místo na deterministickém přístupu? Pokud ano, jaké jsou požadavky (především pokud jde o normy modelování a validace dat), které musí být použity?

b) Pokud klasifikace založená na riziku vede k jiným klasifikacím FSE v porovnání s deterministickým přístupem, které klasifikaci by se mělo dát přednost?

c) Měly by se k dosažení maximálního prospěchu použít oba tyto přístupy současně? Deterministický přístup je založen na rozumných dobře ověřených jaderných bezpečnostních principech. Výsledky hodnocení rizika mohou vést k podcenění při klasifikaci specifických funkcí I&C (vzhledem ke specifickým prvkům projektu elektrárny). Mělo by toto podcenění být nějakým způsobem omezeno?

d) Mělo by být použití hodnocení rizika oficiálně ustanoveno, když se uvažuje o efektivnosti elektrárny a úpravách I&C během její existence? Podobně, měly by být zahrnuty požadavky na použití hodnocení rizika do rozhodování o preventivní údržbě?

Po obsáhlé diskusi o těchto otázkách bylo konstatováno, že dodatek k IEC 61226 je nyní předčasný. Avšak aby se pokročilo v diskusi, uvádí tato technická zpráva několik různých přístupů k používání pravděpodobnostního hodnocení rizika při klasifikaci FSE.

1 Rozsah platnosti

Tato technická zpráva podává přehled některých metod, s jejichž pomocí mohou být výsledky pravděpodobnostního hodnocení rizika používány ke stanovení klasifikačních kritérií „založených na riziku“ tak, že umožňují zařazení FSE do čtyř kategorií uvedených v IEC 61226.

Použití postupů založených na riziku, ve spojení s přístupem ke klasifikaci založeným na důsledcích uvedených v IEC 61226, je obvykle stanoveno podle užitečnosti a/nebo nařízení v členských zemích. Při absenci mezinárodně dohodnutého přístupu by tento stav měl pokračovat, ale tato technická zpráva se snaží podporovat diskusi na toto téma a přispívat ke sbližování stanovisek tak, aby mohla být dohodnuta mezinárodní norma IEC.

Jsou diskutovány bezpečnostní zásady a užitečnost přístupu založeného na riziku ke klasifikaci a jsou uvedeny čtyři různé přístupy.

Dále jsou v této zprávě uvedeny odkazy na dokumenty IEC a MAAE, které se k tomuto tématu vztahují.

Tato zpráva také pojednává o omezeních spojených s použitím postupů pravděpodobnostního hodnocení bezpečnosti (probabilistic safety assessment (PSA)).

V příloze A je uveden návod na modelování kontrolních a řídicích funkcí pro pravděpodobnostní hodnocení rizika.

2 Normativní odkazy

Publikace MAAE

50-SG-D8:1984 Systémy kontroly a řízení související s bezpečností jaderných elektráren
(Safety related instrumentation and control systems for nuclear power plants)

INSAG 3: Základní bezpečnostní zásady pro jaderné elektrárny
(Basic safety principles for nuclear power plants)

Publikace IEC

IEC 60964:1989 Navrhování dozoren pro jaderné elektrárny
(Design for control rooms of nuclear power plants)

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

-- Vynechaný text --