



Programmed digital computers important to safety for nuclear power stations

Calculateurs programmés importants pour la sûreté des centrales nucléaires

Digitalrechner für sicherheitstechnisch wichtige Systeme in Kernkraftwerken

Tato norma obsahuje IEC 987:1989.

Tato norma je přeložena z anglického znění bez redakčních změn. V případě, že by vznikl spor o výklad, použije se původní anglické znění normy.

This standard is translated from the English version without editorial changes. In all cases of interpretation disputes the English version applies.

Národní předmluva

Citované normy

IEC 50 (191) dosud nezavedena

IEC 557:1987 zavedena částečně v ČSN 35 6580 Přístroje jaderné techniky. Systémy pro kontrolu, řízení a ochranu jaderných reaktorů. Názvy a definice

IEC 639:1979 dosud nezavedena

IEC 780:1984 zavedena v ČSN IEC 780 Ověření způsobilosti elektrických součástí bezpečnostního systému jaderných reaktorů (35 6609)

IEC 801-1:1984 zavedena v ČSN IEC 801-1 Elektromagnetická kompatibilita. Zařízení pro měření a řízení průmyslových procesů (18 0014)

IEC 801-2:1984 dosud nezavedena

IEC 801-3:1984 dosud nezavedena

IEC 801-4:1984 dosud nezavedena

IEC 812:1995 dosud nezavedena

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

IEC 1025 dosud nezavedena

ISO 2382/1:1984 dosud nezavedena

Bezpečnostní příručky MAAE 50-SG-D3, 50-SG-D7 a 50-SG-D8 dosud nezavedeny, jsou uloženy v ÚISJP Praha 5 - Zbraslav

Ó Český normalizační institut, 1993

15943

Strana 2

Obdobné mezinárodní, regionální a zahraniční normy

NEN 10987 Geprogrammeerde digitale computers, van belang voor de veiligheid van kencentrales (Počítačové systémy důležité pro bezpečnost jaderných elektráren)

Vypracování normy

Zpracovatel Bohumil Hájek, K lučinám 21, 130 00 Praha 3, IČO 44368933

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Českého normalizačního institutu: Ing. Jaromír Petřík

Strana 3

**POČÍTAČOVÉ SYSTÉMY DŮLEŽITÉ PRO
BEZPEČNOST JADERNÝCH ELEKTRÁREN**

**IEC 987
První vydání
1989-11**

Obsah	strana
Předmluva	3
Úvod	4
1 Předmět normy a rozsah použití	5
2 Termíny a definice	5
3 Osnova projektu	6
4 Požadavky na technické vybavení	8
5 Návrh a vývoj	11
6 Ověřování a kontrola platnosti (verifikace a validizace)	13
7 Ověření způsobilosti	15
8 Výroba	15
9 Instalace a uvádění do chodu	15
10 Údržba	16
11 Změny	18
12 Provoz	18
13 Dokumentace	19
Přílohy	
A - Schéma životního cyklu počítačového systému	20
B - Vývojový diagram ověření způsobilosti	21
C - Příklad postupu údržby	22

Předmluva

1) Oficiální rozhodnutí nebo dohody IEC týkající se technických otázek zpracovaných technickými komisemi, v nichž jsou zastoupeny všechny zainteresované národní komitěty, vyjadřují v největší možné míře mezinárodní shodu v názoru na předmět, kterého se týkají.

2) Mají formu doporučení pro mezinárodní použití a v tomto smyslu jsou přijímána národními komitěty.

3) Na podporu mezinárodního sjednocení vyjadřuje IEC přání, aby všechny národní komitěty převzaly text doporučení IEC do svých národních předpisů v rozsahu, který národní podmínky dovolují. Jakýkoliv rozdíl mezi doporučením IEC a odpovídajícím národním předpisem by měl být pokud možno v národním předpise jasně vyznačen.

Úvodní údaje

Tuto normu vypracovala subkomise 45A Přístroje pro reaktory technické komise č. 45 Přístroje jaderné techniky.

Text této normy je založen na těchto dokumentech:

Šestiměsíční pravidlo Zpráva o výsledku hlasování

Úplnou informaci o hlasování pro přijetí této normy je možno nalézt ve zprávě o výsledku hlasování ve výše uvedené tabulce.

Strana 4

Odkazy na normy

IEC 50 (191):International Electrotechnical Vocabulary (IEV), Chapter 191:Dependability and quality of service (being printed) [Mezinárodní elektrotechnický slovník (MES), kapitola 191: Spolehlivost funkce a jakost služby (v tisku)]

IEC 557:1982 IEC terminology in the nuclear reactor field (Názvosloví IEC v oboru jaderných reaktorů)

IEC 639:1979 Nuclear reactors. Use of the protection system for non-safety purposes (Jaderné reaktory. Využití ochranného systému k jiným účelům než bezpečnostním)

IEC 780:1984 Qualification of electrical item of the safety system for nuclear power generating stations (Ověření způsobilosti elektrických součástí bezpečnostního systému jaderných reaktorů)

IEC 801-1:1984 Electromagnetic compatibility for industrial-process measurement and control equipment. Part 1: General introduction (Elektromagnetická kompatibilita. Zařízení pro měření a řízení průmyslových procesů. Část 1: Všeobecný úvod)

IEC 801-2:1984 Part 2: Electrostatic discharge requirements (Část 2: Požadavky při elektrostatickém výboji)

IEC 801-3:1984 Part 3: Radiated electromagnetic field requirements (Část 3: Požadavky spojené s vyzařovaným elektromagnetickým polem)

IEC 801-4:1988 Part 4: Electrical fast transient/burst requirements (Část 4: Požadavky spojené s rychlými elektromagnetickými jevy, skupinami impulsů)

IEC 812:1985 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (Postupy analýzy spolehlivosti systému - Postup analýzy druhu a účinku poruchy)

IEC 880:1986 Software for computers in the safety systems of nuclear power stations (Programové prostředky počítačů používaných v bezpečnostních systémech jaderných elektráren)

IEC 1025 (): Fault-treeanalysis - FTA (being printed) (Analýza stromu poruch (v tisku))

Další citované normy:

ISO 2382/1:1984 Data processing - Vocabulary - Part 01: Fundamental terms. (Zpracování údajů - Názvosloví - Část 01: Základní pojmy)

Úvod

Základní zásady pro návrh systémů důležitých pro bezpečnost jaderných elektráren jsou definovány v existujících normách jako např. Bezpečnostní příručky MAAE 50-SG-D3 a D8, které jsou aplikovatelné pro návrh systémů s pevným propojením.

Tato norma rozšiřuje působnost těchto principů na využívání počítačových systémů v systémech důležitých pro bezpečnost. Vztahuje se na multiprocesorové distribuované systémy a na rozsáhlé centralizované počítačové systémy konstruované jednak z komerčně dostupných částí, jednak z nově vyvíjeného technického vybavení.

Tato norma formuluje specifické požadavky na technické vybavení číslicových počítačů (hardware). Specifické požadavky na programové vybavení (software) počítačů a požadavky na společné oblasti technického i programového vybavení uvádí IEC 880.

Tato norma rovněž stanoví požadavky na zálohování, nezávislost a strukturální rozdělení.

Obecné požadavky na ověření způsobilosti uvedené v IEC 780, zejména v 4.2, platí pro počítačové systémy důležité pro bezpečnost jaderných elektráren.

Pro moduly používané při návrhu daných bezpečnostních systémů mohou být přijatelnou metodou ověření způsobilosti relevantní a ověřitelné provozní zkušenosti z jaderných i dalších aplikací, jak je uvedeno v IEC 780, v kombinaci s vysoce spolehlivými programy zajištění jakosti.

Strana 5

1 Předmět normy a rozsah použití

Tato norma platí pro technické vybavení počítačových systémů použitých v systémech důležitých pro bezpečnost jaderných elektráren. Vztahuje se tudíž i na samy bezpečnostní systémy a obecně vzato, i na systémy, které s bezpečností souvisejí (viz Bezpečnostní příručka MAAE 50-SG-D8, obrázek 1). Některé její požadavky na systémy však nemusí být aplikovatelné pro systémy související s bezpečností.

Požadavky této normy tvoří doplněk k požadavkům na třídy bezpečnosti.

Specifikované požadavky se vztahují, kromě jiného, na dále uvedené prvky těchto systémů, až do úrovně jednotlivých součástí:

- a) externí napájecí zdroje počítačového systému;
- b) vnitřní architektura;
- c) vstupní a výstupní zařízení a rozhraní;
- d) prostředky pro přenos dat;
- e) paměti;
- f) zařízení ke kontinuálnímu prověřování správné funkce v takovém rozsahu, aby výpadek tohoto zařízení nevedl k poruše celého počítačového systému.

-- Vynechaný text --