

Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Požadavky na návrh hardwaru počítačových systémů

ČSN
EN 60987
35 6615

mod IEC 60987:2007

Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme

Tato norma je českou verzí evropské normy EN 60987:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 60987:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

S účinností od 2012-06-01 se nahrazuje ČSN IEC 987 (35 6615) z března 1994, která do uvedeného data platí souběžně s touto normou.

Národní předmluva

Upozornění na používání této normy

Souběžně s touto normou se může do 2012-06-01 používat dosud platná ČSN IEC 987 (35 6615) z března 1994, v souladu s předmluvou k EN 60987:2009.

Změny proti předchozím normám

Toto vydání obsahuje následující hlavní technické změny oproti předchozímu vydání:

- pozornost byla věnována skutečnosti, že technické postupy počítačového projektování se v letech od posledního vydání dále vyvinuly;
- aktualizaci formátu tak, aby vyhověl aktuálním směrnícím IEC/ISO pro úpravu norem;
- sladění této normy s novými revizemi IAEA dokumentů NS-R-1 a NS-G-1.3, což zahrnuje přepracování definic, pokud to bylo možné;

- nahrazení, pokud to bylo možné, požadavků souvisejících s normami vydanými po prvním vydání této normy, zejména IEC 61513, 2. vydání IEC 60880 a IEC 62138;
- revize stávajících požadavků a aktualizace terminologie a definic.

Informace o citovaných normativních dokumentech

IEC 60780 zavedena v ČSN IEC 60780 (35 6609) Jaderné elektrárny – Elektrické zařízení bezpečnostního systému – Ověření způsobilosti

IEC 60812 zavedena v ČSN EN 60812 (01 0675) Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)

IEC 60880 zavedena v ČSN IEC 60880 (35 6587) Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Softwarová hlediska počítačových systémů vykonávajících funkce kategorie A

IEC 61000 (soubor) zaveden v souborech ČSN 33 3431, ČSN IEC 1000 (33 3431), ČSN IEC 61000 (33 3431) a ČSN EN 61000 (33 3432) Elektromagnetická kompatibilita (EMC)

IEC 61025 zavedena v ČSN EN 61025 (01 0676) Analýza stromu poruchových stavů (FTA)

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

IEC 62138 zavedena v ČSN IEC 62138 (35 6665) Jaderné elektrárny – Instrumentace a řízení důležité pro bezpečnost – Softwarová hlediska pro systémy využívající počítače vykonávající funkce kategorie B nebo C

ISO 9001 zavedena v ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

IAEA NS-G 1.3 nezavedena

IAEA 50-C/SG-Q:1996 nezavedena

POZNÁMKA Příručky IAEA jsou k dispozici ve Státním úřadu pro jadernou bezpečnost, Senovážné náměstí 9, Praha 1

Porovnání s mezinárodní normou

Text evropské normy přejímá IEC 60987:2007 s těmito modifikacemi:

V článku 1.1 by nahrazen text poznámky 2.

Informativní údaje z IEC 60987:2007

Mezinárodní norma IEC 60987 byla vypracována subkomisí 45A: Instrumentace a řízení v jaderných zařízeních, technické komise IEC TC 45: Přístroje jaderné techniky.

Toto druhé vydání ruší a nahrazuje první vydání publikované v roce 1989. Toto vydání obsahuje následující hlavní technické změny oproti předchozímu vydání:

- pozornost byla věnována skutečnosti, že technické postupy počítačového projektování se v letech od posledního vydání dále vyvinuly;
- aktualizaci formátu tak, aby vyhověl aktuálním směrnícím IEC/ISO pro úpravu norem;

- sladění této normy s novými revizemi IAEA dokumentů NS-R-1 a NS-G-1.3, což zahrnuje přepracování definic, pokud to bylo možné;
- nahrazení, pokud to bylo možné, požadavků souvisejících s normami vydanými po prvním vydání této normy, zejména IEC 61513, 2. vydání IEC 60880 a IEC 62138;
- revize stávajících požadavků a aktualizace terminologie a definic.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
45A/662/FDIS	45A/666/RVD

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

Tato publikace byla vypracována podle Směrnic ISO/IEC, Část 2.

Komise rozhodla, že obsah této publikace se nebude měnit až do konečného data vyznačeného na internetové adrese IEC „<http://webstore.iec.ch>“ v termínu příslušejícímu dané publikaci. Po tomto termínu bude publikace

- opětně potvrzena;
- zrušena;
- nahrazena revidovaným vydáním, nebo
- změněna.

Vypracování normy

Zpracovatel: ÚJV Řež a.s., divize Energoprojekt Praha, IČ 46356088, Ing. Jaroslav Mezera

Technická normalizační komise: TNK 56 Elektrické měřicí přístroje

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Tomáš Pech

EVROPSKÁ NORMA EN 60987
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Červen 2009

ICS 27.120.20

Jaderné elektrárny - Systémy kontroly a řízení důležité pro bezpečnost - Požadavky na návrh hardwaru počítačových systémů
(IEC 60987:2007, modifikována)

Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems
 (IEC 60987:2007, modified)

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés
 (CEI 60987:2007, modifiée)

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme
 (IEC 60987:2007, modifiziert)

Tato evropská norma byla schválena CENELEC 2009-06-01. 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 komitety Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CENELEC

Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Ústřední sekretariát: Avenue Marnix 17, B-1000 Brusel

© 2009 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky jsou celosvětově vyhrazena členům CENELEC.
Ref. č. EN 60987:2009 E

Předmluva

Text mezinárodní normy IEC 60987:2007 vypracovaný v subkomisi 45A, Instrumentace a řízení v jaderných zařízeních, technické komise IEC TC 45, Přístroje jaderné techniky, společně se společnými modifikacemi zpracovanými technickou komisí CENELEC TC 45AX, Instrumentace a řízení v jaderných zařízeních byl předložen k formálnímu hlasování a byl schválen CENELEC jako EN 60987 dne 2009-06-01.

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
- nejzazší datum zrušení národních norem, které jsou s EN v rozporu

(dop) 2010-06-01

(dow) 2012-06-01

Přílohu ZA doplnil CENELEC.

Oznámení o schválení

Text mezinárodní normy IEC 60987:2007 byl schválen CENELEC jako evropská norma s dohodnutými společnými modifikacemi uvedenými dále.

Obsah

Úvod 9

1 Rozsah platnosti 10

1.1 Všeobecně 10

1.2 Použití této normy pro hodnocení již vyvinutého (například COTS) hardwaru 10

1.3 Použitelnost této normy pro vývoj programovatelných logických modulů 11

2 Citované normativní dokumenty 11

3 Termíny a definice 11

4 Skladba návrhu 13

4.1 Všeobecně 13

4.2 Členění návrhu 14

4.3 Zajištění kvality 14

5 Požadavky na hardware 15

5.1 Všeobecně 15

5.2 Požadavky na funkce a charakteristiky 15

5.3 Požadavky na bezporuchovost/pohotovost 16

5.4 Požadavky na odolnost vůči okolnímu prostředí 17

5.5 Požadavky na dokumentaci 17

6 Návrh a vývoj 17

6.1 Všeobecně 17

6.2 Činnosti při návrhu 18

6.3 Bezporuchovost 18

6.4 Údržba 19

6.5 Rozhraní 19

6.6 Změny 19

6.7 Porucha napájení 19

6.8 Výběr komponent 19

6.9 Dokumentace návrhu 19

7 Ověření (verifikace) a prokázání platnosti (validace) 20

7.1	Všeobecně	20
7.2	Plán ověření	20
7.3	Nezávislost ověření	20
7.4	Metody	21
7.5	Dokumentace	21
7.6	Rozpory	21
7.7	Změny a modifikace	21
7.8	Ověření instalace	21
7.9	Prokázání platnosti	22
7.10	Ověření již existujících platforem vybavení	22
8	Ověření způsobilosti	22
9	Výroba	22
10	Instalace a uvedení do provozu	22

Strana

11	Údržba	23
11.1	Požadavky na údržbu	23
11.2	Údaje o poruchách	23
11.3	Dokumentace o údržbě	24
12	Změny	24
13	Provoz	24
Příloha A	(informativní) Přehled životního cyklu systému	25
Příloha B	(informativní) Hrubé schéma ověření způsobilosti	26
Příloha C	(informativní) Příklad postupu údržby	27

Bibliografie	28
--------------	----

Příloha ZA	(normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace	29
-------------------	--	----

Úvod

- a. Technické důvody vzniku, hlavní problémy a organizace této normy

Základní zásady návrhu jaderné instrumentace, které jsou konkrétně použity pro bezpečnostní systémy jaderných elektráren, byly zprvu interpretovány v jaderných normách s odkazem na pevně zapojené systémy v bezpečnostní příručce IAEA 50-SG-D3, která byla nahrazena IAEA příručkou NS--1.3.

IEC 60987 byla poprvé vydána v 1989, aby zahrnula hardwarová hlediska návrhu číslicových systémů pro systémy důležité pro bezpečnost, tj. bezpečnostní systémy a systémy vážící se k bezpečnosti.

I když mnoho požadavků v původním vydání je stále důležitých, existovaly důležité faktory, které si vyžádaly vypracování tohoto revidovaného vydání IEC 60987, zejména:

- vznikla nová norma, která podrobně určovala obecné požadavky na jaderné systémy důležité pro bezpečnost (IEC 61513);
- výrazně narostlo použití již vyvinutých systémových platforem, oproti vývoji na zakázku.

b. Místo této normy ve struktuře souboru norem IEC SC 45A

Normou IEC SC 45A první úrovně pro počítačové systémy důležité pro bezpečnost v jaderných elektrárnách (NPP) je IEC 61513. IEC 60987 je norma IEC SC 45A druhé úrovně týkající se obecné problematiky navrhování hardwaru automatizovaných systémů.

IEC 60880 a IEC 62138 jsou normy druhé úrovně, které společně zahrnují softwarová hlediska počítačových systémů používaných pro provádění funkcí důležitých pro bezpečnost v NPP. IEC 60880 a IEC 62138 se u navrhování hardwaru přímo odvolávají na IEC 60987.

Na požadavky IEC 60870 na způsobilost zařízení jsou odkazy v IEC 60987. U modulů použitých v návrhu konkrétního systému důležitého pro bezpečnost mohou být přijatelným způsobem hodnocení způsobilosti významné a kontrolovatelné provozní zkušenosti z jaderných či jiných aplikací podle IEC 60780, v kombinaci s použitím precizních programů hodnocení kvality.

Více podrobností o struktuře souboru norem IEC SC 45A viz položka d) tohoto úvodu.

c. Doporučení a omezení týkající se použití této normy

Je důležité poznamenat, že tato norma nestanovuje další funkční požadavky na systémy třídy 1 a třídy 2 (požadavky na klasifikaci systémů viz IEC 61513).

Hlediska, pro něž byla stanovena speciální doporučení (například pro zajištění výroby vysoce spolehlivých systémů), jsou:

- celkový přístup k vývoji výpočetního hardwaru;
- celkový přístup k ověření hardwaru a k hardwarovým hlediskům při prokázání platnosti počítačového systému.

Je zjištěno, že počítačová technika se neustále vyvíjí a že u normy jako je tato není možné, aby zahrnula odkazy na všechny moderní projektové technologie a techniky. Aby se zajistilo, že tato norma bude stále platná i v následujících letech, byl spíše kladen důraz na určení zásad, než na konkrétní technologie pro návrh hardwaru. Pokud se vypracují nové projektové techniky, pak by mělo být možno vyhodnotit účelnost takovýchto technik přizpůsobením a použitím projektových zásad obsažených v této normě.

Rozsah platnosti této normy zahrnuje hardware číslicových systémů pro systémy třídy 1 a třídy 2. Zahrnuje více-

procesorové rozptýlené systémy a jednoprocessorové systémy; zahrnuje zhodnocení a používání již vyvinutých položek, například komerčních standardních položek (COTS) a vývoj nového hardwaru.

d. Popis struktury souboru norem IEC SC 45A a vztahy s dalšími dokumenty IEC, IAEA a ISO

Hlavním dokumentem souboru norem IEC SC 45A je IEC 61513. Poskytuje obecné požadavky na I & C systémy a zařízení, které se používají k provádění funkcí důležitých pro bezpečnost v NPP. IEC 61513 určuje strukturu souboru norem IEC SC 45A.

IEC 61513 přímo odkazuje na další normy IEC SC 45A ohledně obecných hledisek kategorizace funkcí a klasifikace systémů, prokázání způsobilosti, oddělení systémů, ochrany proti poruše způsobené společnou příčinou, softwarových hledisek počítačových systémů, hardwarových hledisek počítačových systémů a návrhu dozorní. Normy odkazované přímo na této druhé úrovni mají být považovány společně s IEC 61513 za konzistentní soubor dokumentů.

Ve třetí úrovni jsou normy IEC SC 45A, na které IEC 61513 přímo neodkazuje, což jsou normy vztahující se na konkrétní zařízení, technické metody nebo konkrétní činnosti. Obvykle mohou být tyto dokumenty, které se z hlediska obecné problematiky odkazují na dokumenty druhé úrovně, používány samostatně.

Čtvrté úrovni rozšiřující soubor norem IEC SC 45A odpovídají technické zprávy, které nejsou normativní.

IEC 61513 přijala formát provedení podobný jako u základní bezpečnostní publikace IEC 61508 pro strukturu souhrnného životního cyklu bezpečnosti a strukturu životního cyklu systému a poskytuje interpretaci obecných požadavků z IEC 61508-1, IEC 61508-2 a IEC 61508-4 pro použití v jaderné oblasti. Soulad s IEC 61513 usnadní shodu s požadavky IEC 61508, které byly analyzovány pro jaderný průmysl. V této struktuře vyhovuje IEC 60880 a IEC 62138 normě IEC 61508-3 pro použití v jaderné oblasti.

Z hlediska problematiky zabezpečování kvality (QA) odkazuje IEC 61513 na ISO 9001 a rovněž na IAEA 50-C-QA (nyní nahrazenou IAEA 50-C/SG-Q).

Soubor norem IEC SC 45A důsledně zavádí a rozpracovává principy a základní bezpečnostní hlediska uvedené v příručce IAEA o bezpečnosti NPP a v bezpečnostní řadě IAEA, především požadavky NS-R-1, stanovující požadavky na bezpečnost u návrhu NPP a bezpečnostní příručka NS-G-1.3 zabývající se systémy kontroly a řízení důležitými pro bezpečnost v NPP. Terminologie a definice používané normami SC 45A odpovídají terminologii a definicím používaným v IAEA.

1 Rozsah platnosti

1.1 Všeobecně

Tato mezinárodní norma platí pro hardware počítačového systému NPP u systémů třídy 1 a 2 (podle IEC 61513).

Struktura této normy se oproti původnímu vydání z roku 1989 výrazně nezměnila; avšak některé problémy jsou nyní zahrnuty v normách, které byly mezitím vydány (například IEC 61513 u návrhu architektury systému) a kde je to vhodné byly provedeny odkazy na tyto nové normy. Text této normy byl rovněž změněn tak, aby zachytil vývojové trendy v navrhování hardwaru počítačových systémů, použití již vyvinutého (například COTS) hardwaru a změny v terminologii.

U počítačových hardwarových prostředků použitých pro zavádění a kontrolování softwaru se neuvažuje, že by tvořily standardní část systému důležitého pro bezpečnost a jako takové nejsou náplní této normy.

POZNÁMKA 1 Hardware počítačového systému třídy 3 není v této normě uvedeno a doporučuje se, aby takovéto systémy byly vyvíjeny na základě komerčních norem.

POZNÁMKA 2 Složitější hardwarové komponenty nejsou náplní EN 60987. IEC/SC 45 A přijala nové pracovní náměty zahrnující případy těchto složitějších hardwarových komponent (např. v době publikování EN 60987 se vypracovávala IEC 62566).

1.2 Použití této normy pro hodnocení již vyvinutého (například COTS) hardwaru

I když prvotním cílem této normy je určit hlediska vývoje nového hardwaru, lze jako návod pro hodnocení a použití již vyvinutého (komerčního) hardwaru, například COTS hardwaru, použít postup definovaný v této normě. Směrnice byla vypracována z hlediska interpretace požadavků této normy, když se použije pro hodnocení takovýchto komponent. Především platí požadavky na vyhodnocení kvality z 4.3 týkající se kontroly konfigurace.

Již vyvinuté (komerční) komponenty mohou obsahovat mikroprogramové vybavení (jak uvádí 3.8) a pokud je software mikroprogramového vybavení promyšleně zabudován, a skutečně „transparentní“ pro uživatele, pak má být IEC 60987 použita jako směrnice pro postup vyhodnocení těchto komponent. Příkladem, kde je tato metoda považována za vhodnou je při hodnocení moderních procesorů obsahujících mikrokód. Tento kód je nedílnou součástí „hardwaru“ a je tudíž u procesoru (obsahujícího tento mikrokód) vhodné jej hodnotit jako nedílnou hardwarovou komponentu s pomocí této normy.

Software, který není mikroprogramovým vybavením uvedeným výše, má být vyvíjen nebo vyhodnocován na základě požadavků příslušných norem pro software (například IEC 60880 pro systémy třídy 1 a IEC 62138 pro systémy třídy 2).

1.3 Použitelnost této normy pro vývoj programovatelných logických modulů

I&C komponenty mohou obsahovat programovatelné logické moduly, které určuje projektant I&C komponent logickým návrhem jejich konkrétního použití, na rozdíl od výrobce čipů. Příkladem takovýchto zařízení jsou složité programovatelné logické moduly (CPLD) a pole logických členů programovatelné uživatelem (FPGA).

I když programovatelnost těchto zařízení určuje vývojové procesy použité u těchto zařízení, jsou některé charakteristiky vývojového procesu softwaru a projektové postupy, použité pro takováto zařízení, velmi podobné postupům, použitým při navrhování logických obvodů realizovaných v diskrétních obvodech a sestav integrovaných obvodů. Proto projektový postup a ověření návrhu, použité pro programovatelné logické moduly, mají splňovat důležité požadavky této normy (tj. brát v úvahu konkrétní charakteristiky projektových postupů u takovýchto zařízení). V rozsahu, v němž jsou softwarové prostředky použity pro zajištění projektových postupů u programovatelných logických modulů, mají tyto softwarové prostředky obvykle splňovat směrnici uvedenou pro softwarové vývojové prostředky v příslušných normách pro software, tj. IEC 60880 (systémy třídy 1) nebo IEC 62138 (systémy třídy 2).

Konec náhledu - text dále pokračuje v placené verzi ČSN.