ČESKÁ TECHNICKÁ NORMA

ICS 27.120.20 **Duben 2011**

Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Požadavky na zvládnutí poruchy se společnou příčinou (CCF)

ČSN
EN 62340
35 6673

idt IEC 62340:2007

Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with Common Cause Failure (CCF)

Centrales nucléaires de puissance – Systemes d,instrumentation et de contrôle commande importants pour la sureté – Exigences permettant de faire face aux Défaillances de Cause Commune (DCC)

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung
von Versagen aufgrund gemeinsamer Ursache

Tato norma je českou verzí evropské normy EN 62340:2010. 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 62340:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

IEC 60671 dosud nezavedena

IEC 60709 zavedena v ČSN IEC 60709 (35 6586) Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Oddělování (idt IEC 60709:2004)

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

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 (idt IEC 60880:2006)

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

IEC 61000-4 soubor zaveden v souboru ČSN EN 61000-4 (33 3432) Elektromagnetická kompatibilita

(EMC) – Část 4: Zkušební a měřicí technika

IEC 61226 zavedena v ČSN EN 61226 (35 6643) Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Klasifikace kontrolních a řídicích funkcí (idt IEC 61226:2009)

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

IAEA Safety Guide NS-G-1.3 nezavedena

IAEA Safety Guide SG-D11 nezavedena

IAEA Safety Glossary:2007 nezaveden

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

Informativní údaje z IEC 62340:2007

Mezinárodní norma IEC 62340 byla vypracována subkomisí 45A: Instrumentace a řízení v jaderných zařízeních, technické komise IEC TC 45: Přístroje jaderné techniky.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
45A/668/FDIS	45A/676/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

- znovu 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 Elektrická měřicí zařízení

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

EVROPSKÁ NORMA EN 62340
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Květen 2010

ICS 27.120.20

Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Požadavky na zvládnutí poruchy se společnou příčinou (CCF) (IEC 62340:2007)

Nuclear power plants – nstrumentation and control systems important to safety – Requirements for coping with Common Cause Failure (CCF) (IEC 62340:2007)

Centrales nucléaires de puissance – Systemes d, instrumentation et de contrôle commande importants pour la sureté – Exigences permettant de faire face aux Défaillances de Cause Commune (DCC) (CEI 62340:2007)

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007)

Tato evropská norma byla schválena CENELEC 2010-05-01. 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 komitéty Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, 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

Řídicí centrum: Avenue Marnix 17, B-1000 Brusel

Ref. č. EN 62340:2010 E

Předmluva

Text mezinárodní normy IEC 62340:2007 vypracovaný SC 45A: Instrumentace a řízení v jaderných zařízeních, IEC TC 45: Přístroje jaderné techniky, byl předložen k formálnímu hlasování CENELEC pro přijetí jako evropská norma a byl schválen CENELEC jako EN 62340 dne 2010-05-01.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN a CENELEC nelze činit odpovědnými za identifikaci libovolného patentového práva nebo všech takových patentových práv.

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	(dop)	2011-05-01
• nejzazší datum zrušení národních norem, které jsou s EN v rozporu	(dow)	2013-05-01

Přílohu ZA doplnil CENELEC.

Jak je stanoveno ve Směrnici pro jadernou bezpečnost 2009/71/EURATOM, kapitola 1, článek 2, bod 2, nebrání se členským státům přijmout přísnější bezpečnostní opatření týkající se témat obsažených v této Směrnici v souladu s národními zákony. Obdobně tato evropské norma nebrání členským státům přijmout přísnější opatření týkající se jaderné bezpečnosti v rámci témat obsažených v této evropské normě.

Oznámení o schválení

Text mezinárodní normy IEC 62340:2007 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod

a. **Technické důvody vzniku, hlavní problémy a organizace normy**

Pro dosažení vysoké úrovně bezpečnosti se jako jedno ze základních opatření pro navrhování systémů kontroly a řízení (systémů I&C) důležitých pro bezpečnost používá zálohování. Protože by porucha se společnou příčinou (CCF – Common Cause Failure) mohla ohrozit efektivnost zálohování, je nezbytné vůči tomu přijmout odpovídající opatření. Jaderný průmysl má zavedené systémy zkonstruované a vyprojektované pro postižení CCF. Během posledních třiceti let byla realizována řada opatření a dosaženo konsensu u řady opatření pro zvládnutí a překo-nání následků CCF.

Záměrem této normy je určit celkový rozsah aspektů týkajících se zvládnutí poruch se společnou příčinou (CCF) a poskytnout přehled důležitých požadavků na systémy I&C použité k provádění funkcí důležitých pro bezpečnost (podle IEC 61226) v jaderných elektrárnách.

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

IEC 62340 je dokument druhé úrovně IEC SC 45A řešící problematiku CCF.

Tato mezinárodní norma doplňuje IEC 61513 a k ní se vážící normy o požadavky na omezení a překonání případné CCF u funkcí I&C kategorie A. Požadavky uvedené v této normě platí pro funkce kategorie A (IEC 61226), pokud by jejich porucha mohla být nepřípustná z hlediska návrhu bezpečnosti provozu.

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

c. **Doporučení a omezení týkající se použití této normy**

Tato norma platí pro systémy I&C důležité pro bezpečnost u nových JE a rovněž pro nahrazení

systémů I&C
ve stávajících elektrárnách. Funkce I&C může být nezbytné udržet nebo aktualizovat, pokud je systém I&C vymě-ňován. Požadavky této normy rovněž uvažují nahrazení I&C jež způsobí změny ve struktuře systémů I&C.

U stávajících elektráren lze použít pouze dílčí soubor požadavků z této normy a tento dílčí soubor má být určen na začátku každého projektu. Požadavky a doporučení, které se v projektu rekonstrukce nebo nahrazení I&C nerealizovaly, mají být případ od případu zdůvodněny na základě komplexního hodnocení bezpečnosti. Případné následky způsobené nedodržením některých aspektů této normy následkem omezení provozu dané elektrárny mají být zváženy jako celek z hlediska zvýšené bezpečnosti získané rekonstrukcí.

Aby nedošlo k překrývání požadavků, využívá tato norma ostatní existující normy pomocí odkazů na příslušné kapitoly (články), především u norem z jaderné oblasti IEC 61513, IEC 60709, IEC 60780 a IEC 60880. Nové požadavky jsou uvedeny tehdy, když je tyto normy neobsahují.

d. **Popis struktury souboru norem IECSC 45A a vztahů s dalšími dokumenty IEC a dokumenty dalších organizací (IAEA, ISO)**

Dokumentem nejvyšší úrovně souboru norem IEC SC 45A je IEC 61513. Uvádí obecné požadavky na systémy a zařízení I&C, které se používají k vykonávání funkcí důležitých pro bezpečnost v JE. IEC 61513 určuje strukturu souboru norem IEC SC 45A.

IEC 61513 přímo odkazuje na další normy IEC SC 45A týkající se obecných hledisek kategorizace funkcí a klasifikace systémů, prokázání způsobilosti, oddělení systémů, ochrany proti poruše se společnou příčinou, softwarových hledisek počítačových systémů, hardwarových hledisek počítačových systémů a návrhu dozorny. Normy zde přímo odkazované jsou normami druhé úrovně, které mají být uvažovány společně s IEC 61513 jako konzistentní soubor dokumentů.

Ve třetí úrovni jsou normy IEC SC 45A, na které IEC 61513 neodkazuje přímo, což jsou normy vztahující se na konkrétní zařízení, technické metody nebo konkrétní činnosti. Tyto dokumenty, které se, pokud jde o obecné záležitosti, odkazují na dokumenty druhé úrovně, mohou být obvykle používány samostatně.

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

IEC 61513 má strukturu podobnou jako mají základní bezpečnostní publikace souboru IEC 61508, tj. obsahuje souhrnnou osnovu životního cyklu bezpečnosti a osnovu životního cyklu systému a interpretuje obecné požadavky IEC 61508-1, IEC 61508-2 a IEC 61508-4 pro použití v jaderné oblasti. Shoda s IEC 61513 umožní shodu s požadavky IEC 61508 v tom smyslu, jak se tyto interpretují pro jaderný průmysl. Pro použití v jaderné oblasti pak IEC 61508-3 odpovídají normy IEC 60880 a IEC 62138.

Pro problematiku zabezpečování kvality (QA), odkazuje IEC 61513 na ISO a rovněž na IAEA 50-C-QA (nově nahrazenou IAEA GS-R-3).

Soubor norem IEC SC 45A důsledně zavádí a rozpracovává zásady a základní bezpečnostní hlediska uvedené ve Směrnici IAEA o bezpečnosti jaderných elektráren a v bezpečnostní řadě IAEA a to především požadavky NS-R-1 stanovující bezpečnostní požadavky týkající se projektu jaderných elektráren a bezpečnostní příručky NS-G-1.3 zabývající se systémy kontroly a řízení důležitými pro bezpečnost v jaderných elektrárnách. Termíny a definice používané normami SC 45A odpovídají termínům a definicím používaným v IAEA.

1 Rozsah platnosti

Systémy I&C důležité pro bezpečnost mohou být navrženy s užitím konvenčních pevně zapojených zařízení, počítačového vybavení nebo zkombinováním obou typů zařízení. Tato mezinárodní norma uvádí požadavky a doporučení[1)] pro celkovou architekturu systémů I&C, která může obsahovat jednu z těchto technologií či obě.

Předmětem této normy je:

a. poskytnout požadavky týkající se vyloučení CCF u systémů I&C provádějících funkce kategorie A;
b. vyžadovat navíc realizaci nezávislých systémů I&C pro zvládnutí CCF, i když pravděpodobnost CCF je snížena striktním použitím zásad celkové bezpečnosti z IEC SC 45A (zejména IEC 61226, IEC 61513, IEC 60880 a IEC 60709);
c. poskytnout přehled kompletního rozsahu požadavků týkajících se CCF, který se však nepřekrývá s oblastmi již určenými v jiných normách. U těch jsou provedeny odkazy.

Tato norma zdůrazňuje potřebu úplné a přesné specifikace bezpečnostních funkcí na základě analýzy projektových havárií a zvážení hlavních bezpečnostních cílů elektrárny. Tato specifikace je předpokladem pro vytvoření úplného souboru podrobných požadavků pro navrhování systémů I&C pro zvládnutí CCF.

Tato norma uvádí zásady a požadavky pro zvládnutí CCF, jimiž se zaručí nezávislost[2)]:

a. mezi systémy I&C plnícími diverzní bezpečnostní funkce kategorie A, které se podílejí na zajištění téhož bezpečnostního cíle;
b. mezi systémy I&C plnícími různé funkce různých kategorií, tj. když je funkce kategorie B deklarována jako záložní k funkci kategorie A; a
c. mezi zálohovanými (redundantními) kanály téhož systému I&C.

Realizace těchto požadavků vede k různým typům ochrany proti vyvolání CCF událostí.

Prostředky pro dosažení ochrany proti CCF jsou uvedeny v této normě z hlediska:

a. náchylnosti k vnitřním rizikům v elektrárně a vnějším rizikům;
b. šíření fyzikálních jevů v hardwaru (např. vysoká napětí); a
c. vyloučení konkrétních poruch a náchylnosti systémů I&C k poruchám, zejména:
    1. šíření funkční poruchy v systémech I&C nebo mezi jednotlivými systémy I&C (např. prostřednictvím komunikace, poruchy nebo chyby sdílených prostředků),
    2. existence společných poruch zavedených v rámci návrhu nebo během provozu systému (např. poruchy způsobené údržbou),
    3. nedostatečné prokázání platnosti systému, takže chování systému v reakci na změny stavu vstupních signálů dostatečně neodpovídá určeným bezpečnostním funkcím,
    4. nedostatečná kvalifikace požadovaných vlastností hardwaru, nedostatečné ověření softwarových komponent, nebo nedostatečné ověření kompatibility mezi nahrazenými a stávajícími komponentami systému.