ČESKÁ TECHNICKÁ NORMA

ICS 03.100.40; 03.120.01; 35.080

Červenec

1999

	Management spolehlivosti - Část 3: Návod k použití - Oddíl 6: Softwarová hlediska spolehlivosti	ČSN IEC 60300-3-6 01 0690

Dependability management - Part 3: Application guide - Section 6: Software aspects of dependability

Gestion de la sûreté de fonctionnement - Partie 3: Guide d'application - Section 6: Aspects logiciels de la sûreté de fonctionnement

Zuverlässigkeits-Management - Teil 3: Anwendungsleitfaden - Hauptabschnitt 6: Softwareaspekte der Zuverlässigkeit

Tato norma je českou verzí mezinárodní normy IEC 60300-3-6:1997. Mezinárodní norma IEC 60300--
-6:1997 má status české technické normy.

This standard is the Czech version of the International Standard IEC 60300-3-6:1997. The International Standard IEC 60300-3-6:1997 has the status of a Czech Standard.

56328

Národní předmluva

Citované normy

ISO 8402:1994 zavedena v ČSN ISO 8402 Management jakosti a zabezpečování jakosti - Slovník (01 0300)

ISO 9000-3:1991 nahrazena ISO 9000-3:1997 zavedenou v ČSN ISO 9000-3 Normy pro management jakosti a zabezpečování jakosti - Část 3: Směrnice pro použití ISO 9001:1994 při vývoji, dodávce a údržbě softwaru (ISO 9000-3:1997) (01 0320)

ISO/IEC 9126:1991 zavedena v ČSN ISO/IEC 9126 Informační technika - Hodnocení softwarového produktu - Charakteristiky jakosti a návod pro jejich používání (36 9020)

ISO/IEC 12207:1995 zavedena v ČSN ISO/IEC 12207 Informační technologie - Procesy v životním cyklu softwaru (36 9784)

IEC 60050(191):1990 zavedena v ČSN IEC 50(191) Medzinárodný elektrotechnický slovník. Kapitola 191: Spožahlivosť a akosť služieb (01 0102)

IEC 60300-1/ISO 9000-4:1993 zavedena v ČSN ISO 9000-4/IEC 300-1 Normy pro řízení a zabezpečování jakosti. Část 4: Pokyny pro řízení spolehlivosti/Řízení spolehlivosti. Část 1: Řízení programu spolehlivosti (01 0690)

IEC 60300-2:1995 zavedena v ČSN EN 60300-2 Management spolehlivosti - Část 2: Prvky a úkoly programu spolehlivosti (01 0690)

IEC 60300-3-9:1995 zavedena v ČSN IEC 300-3-9 Management spolehlivosti - Část 3: Návod k použití - Oddíl 9: Analýza rizika technologických systémů (01 0690)

IEC 60812:1985 zavedena v ČSN IEC 812 Metody analýzy spolehlivosti systému - Postup analýzy způsobů a důsledků poruch (FMEA) (01 0675)

IEC 61014:1989 zavedena v ČSN IEC 1014 Programy rastu bezporuchovosti (01 0645)

IEC 61025:1990 zavedena v ČSN IEC 1025 Analýza stromu poruchových stavov (01 0676)

IEC 61160:1992 zavedena v ČSN IEC 1160 Oficiální přezkoumání návrhu (01 0678)

IEC 61160:1992/Amendment 1:1994 zavedena v ČSN IEC 1160/A1 Změna 1 k ČSN IEC 1160 Oficiální přezkoumání návrhu (01 0678)

IEC 61164:1995 zavedena v ČSN IEC 1164 Růst bezporuchovosti. Metody statistických testů a odhadů (01 0647)

Souvisící ČSN

ČSN IEC 300-3-3 Management spolehlivosti - Část 3: Návod k použití - Oddíl 3: Analýza nákladů životního cyklu (01 0690)

ČSN IEC 1163-1 Třídění namáháním pro zlepšení bezporuchovosti - Část 1: Opravitelné objekty

vyráběné v dávkách (01 0648)

ČSN ISO 9127 Informační technika. Uživatelská dokumentace a informace na obalu zákaznických softwarových balíků (36 9806)

ČSN ISO/IEC TR 9294 Informační technika. Směrnice pro řízení tvorby dokumentace softwaru (36 9807)

ČSN ISO/IEC 10746-2 Informační technologie - Otevřené distribuované zpracování - Referenční model: Základy (36 9526)

Vysvětlivky k textu převzaté normy

Definice některých pojmů z oboru spolehlivosti zavedených v normách z oboru informační technologie zpracovávaných v ISO/IEC JTC 1 (viz např. ČSN ISO/IEC 2382-14 a ČSN ISO/IEC 10746-2) se již v anglickém originálu značně liší od definic uvedených v normách pro obor spolehlivosti zpracovávaných v IEC TC 56 (viz ČSN IEC 50(191)).

Zejména anglický termín *fault* podle definice 14.01.10 ČSN ISO/IEC 2382-14 či podle 13.5.3 ČSN ISO/IEC 10746-2 a podle poznámek k tomuto článku nelze přeložit jako „poruchový stav“ (191-05-01 podle ČSN IEC 50(191)). V oboru informační technologie se tento termín běžně překládá termínem „vada“, jehož význam odpovídá definicím 14.01.10 a 13.5.3 v uvedených normách. Český termín „vada“ je však již definován v 2.11 ČSN ISO 8402 a v 1.5.8 ČSN ISO 3534-2 pro anglický termín „defect“.

Anglický termín „test“ se v normách na zkoušky výrobků z oboru informační technologie (normách řady ČSN ISO/IEC 9646) překládá podle souvislosti jako „zkouška“ i jako „test“ a tyto pojmy se považují v podstatě za synonyma. Přitom v oblasti, která se týká především řízení jakosti (pro posuzování shody implementace jako celku) byl přednostně používán termín „zkouška/zkoušení“ a pro dílčí kroky zkoušky byl ponechán termín „test/testování“, tj. byla pokud možno dodržována zásada, že se „zkouška“ shody skládá z jednotlivých „testů“ shody. Tato zásada byla dodržována i v této normě.

Pokud byly při zpracování této normy zjištěny rozdíly v názvosloví používaném v ČSN ISO/IEC 12207 a v normách pro řízení jakosti (ČSN ISO 8402, normy řady ČSN ISO 9000) či v předchozích normách řady ČSN IEC 60300, bylo přednostně dodržováno zavedené a ustálené názvosloví používané v normách pro řízení jakosti a v předchozích normách řady ČSN IEC 60300, do níž náleží i tato norma. Týká se to zejména překladu anglických termínů *acceptance* („přijetí“, nikoliv „akceptace“), *contract* („smlouva“, nikoliv „kontrakt“), *control* („řízení“, nikoliv „kontrola“), *improvement* („zlepšování“, nikoliv „zdokonalování“), *management* („management“, nikoliv „řízení“) a *release* („uvolnění“, nikoliv „vydání).

Je tedy nutné zdůraznit, že do doby, než budou sjednoceny definice základních termínů v oboru spolehlivosti mezi ISO/IEC JTC 1 a IEC TC 56, platí termíny z tohoto oboru uvedené v této normě výhradně pro účely této normy a norem, které se na tuto normu odvolávají.

Anglický termín „product“ je v této normě ve shodě s 1.4 normy ČSN ISO 8402 překládán jako „výrobek“ a může zahrnovat i službu a software. Výraz „software product“ je však v této normě v souladu s 3.26 normy ČSN ISO/IEC 12207 překládán jako „softwarový produkt“.

Upozornění na národní poznámky

Do normy byly ke kapitole 1 a k článkům 6.2.1, 6.5, 6.7.2, 6,7.3 a C.2 a k příloze E doplněny informativní národní poznámky.

Upozornění na národní přílohu

Do této normy byla doplněna informativní národní příloha NA, která obsahuje anglicko-český a česko-anglický slovník použitých termínů.

Vypracování normy

Zpracovatel: RNDr. Jaroslav Matějček, CSc., IČO 41127749

Technická normalizační komise: TNK 5 Spolehlivost

Pracovník Českého normalizačního institutu: Ing. Jaromír Čížek

Prázdná strana

MEZINÁRODNÍ NORMA

Management spolehlivosti - Část 3: Návod k použití - Oddíl 6: Softwarová hlediska spolehlivosti

IEC 60300-3-6

První vydání

1997-11

ICS 03.100.40; 03.120.01; 35.080

Deskriptory: applications, computer software, data processing, electrical engineering, guide books, information processing, management, planning, programmes, quality management, reliability related program, reliability, reliability management, specification (approval), testing, specifications, computer programs.

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 IEC, kromě jiných činností, 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.

Mezinárodní norma IEC 60300-3-6 byla připravena Technickou komisí IEC 56 Spolehlivost.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
56/583/FDIS	56/600/RVD

Úplné informace týkající se hlasování o schválení této normy jsou obsaženy ve zprávě o hlasování uvedené v tabulce.

Přílohy A, B, C, D, E a F jsou pouze pro informaci.

Úvod

Spolehlivost je souhrnný termín popisující pohotovost systému nebo výrobku. Pohotovost výrobku je ovlivňována jeho bezporuchovostí, udržovatelností a zajištěností údržby. V mnoha systémech a výrobcích se bezporuchovost, udržovatelnost a pohotovost řadí mezi dominantní znaky výkonnosti, které mají pro uživatele usilující o ekonomicky efektivní provoz výrobků a systémů zásadní důležitost. Bezporuchovost a udržovatelnost jsou vnitřní vlastnosti dané návrhem výrobku. Zajištěnost údržby je z hlediska výrobku vnější a ovlivňuje jakost služby. Zajištěnost údržby odráží schopnost údržbářské organizace poskytovat zdroje nezbytné k zachování úrovně úsilí vynaloženého na zajištěnost údržby pro dosažení cílů pohotovosti.

Aby bylo možné program spolehlivosti efektivně použít, musí být přizpůsoben výrobku. Program spolehlivosti má tvořit součást celkového programu managementu projektu, aby se dosáhlo řádné koordinace s vývojem, výrobou, ověřováním a využitím výrobku. Prvky a úkoly programu spolehlivosti mají být v souladu s ostatními podpůrnými programy, jako je management jakosti, management konfigurace, sběr dat atd.

Proces managementu spolehlivosti zahrnuje plánování, specifikaci, analýzu návrhu, ověřování a validaci, implementaci a vyhodnocování projektu a zpětnovazební tok dat o výrobku nebo službě. Moderní systémy a výrobky často obsahují software jako funkční entitu pro dosažení cílů v oblasti provozní výkonnosti. Software obsažený v systému nebo vložený do výrobku se podrobuje procesu managementu spolehlivosti. Tento návod k použití je zaměřen na softwarová hlediska spolehlivosti. Poskytují se v něm specifické směrnice pro volbu a použití příslušných činností v programech spolehlivosti sdružených s výrobky obsahujícími software nebo se systémy konfigurovanými pomocí software s hardwarovými prvky.

Na pohotovost výrobků mohou mít vliv hardwarové poruchy, softwarové vady nebo lidské chyby. Chybná funkce výrobku, která je příčinou vzniku nepoužitelných stavů, může být sledovatelná až po zjištění vnitřních anomálií návrhu, nebo může být způsobena vnějším rušením včetně chybného postupu. Poruchy výrobku mohou pocházet od vnitřních vad způsobených návrhem ve vazbě na hardwarové nebo softwarové problémy. Poruchu hardwaru a opotřebené součásti lze identifikovat a izolovat, opravit nebo nahradit, aby se udržela stále stejná úroveň bezporuchovosti výrobku. Software, jakmile byl jednou vytvořen ve tvaru kódu nebo instrukcí, nepodléhá, na rozdíl od většiny fyzického hardwaru, opotřebení nebo znehodnocení. Některé softwarové procesy mohou být proto odlišné od procesů použitelných pro implementaci hardwaru. Záměrem tohoto návodu k použití je uvést do vztahu procesy životního cyklu softwaru s etapami životního cyklu výrobku v rámci managementu spolehlivosti.

Management spolehlivosti je definován v IEC 60300-1. Prvky a úkoly programu spolehlivosti jsou specifikovány v IEC 60300-2. Tento návod k použití doplňuje IEC 60300-2 v podobě implementace programu spolehlivosti systémů nebo výrobků obsahujících software. Klade se důraz na uplatnění příslušných softwarových činností spojených s implementací prvků a úkolů uvedených v IEC 60300-2 v odpovídajícím čase či etapě, jak je znázorněno v příloze A. V příloze B se uvádí volba prvků programu spolehlivosti sdružených s jednotlivými etapami životního cyklu.

Usilovalo se o harmonizaci tohoto návodu k použití s normou ISO/IEC 12207 pro procesy životního cyklu softwaru. Přehled procesů životního cyklu softwaru je uveden v příloze C. Pro usnadnění vztahu mezi procesy životního cyklu softwaru a příslušnými prvky programu spolehlivosti a etapami životního cyklu výrobku jsou v příloze D uvedeny vzájemné odkazy.

Na vztah mezi spolehlivostí (norem řady IEC 60300) a jakostí (norem řady ISO 9000) je zaměřena norma IEC 60300-1/ISO 9000-4 a tento vztah nebude v tomto návodu k použití zpracováván. U těch znaků jakosti, které ovlivňují ukazatele spolehlivosti softwarových prvků, však mají být brány v úvahu směrnice obsažené v ISO 9000-3 pro aplikaci ISO 9001 na software. V příloze E jsou uvedeny vzájemné odkazy mezi IEC 60300-2 a ISO 9000-3.

V příloze F jsou uvedeny dodatečné odkazy na literaturu týkající se softwarových hledisek spolehlivosti.

---

1 Předmět normy

Tento návod k použití doplňuje IEC 60300-2 a jsou v něm uvedeny směrnice pro volbu a použití prvků a úkolů spolehlivosti s ohledem na systémy nebo výrobky obsahující software.

Tento návod k použití je určen pro manažery projektů, administrátory (správce) smluv, návrháře výrobků, projektanty*) (vývojáře) softwaru, specialisty na spolehlivost, specialisty na jakost, zajišťující personál a správce (udržovatele)**) systému, kteří přispívají ke spolehlivosti výrobků nebo systémů.

-- Vynechaný text --