ČESKÁ TECHNICKÁ NORMA

ICS 03.120.01 **Květen 2013**

Návod pro softwarová hlediska spolehlivosti

ČSN
EN 62628
01 0692

idt IEC 62628:2012

Guidance on software aspects of dependability

Lignes directrices concernant la sureté de fonctionnement du logiciel

Leitlinien zu Softwareaspekten der Zuverlässigkeit

Tato norma je českou verzí evropské normy EN 62628:2012. 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 62628:2012. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

IEC 60300-3-15 zavedena v ČSN EN 60300-3-15 (01 0690) Management spolehlivosti – Část 3-15: Pokyn k použití – Inženýrství spolehlivosti systémů

Souvisící ČSN

ČSN EN 62508 (01 0681) Návod pro lidská hlediska spolehlivosti

ČSN EN 60300-1 (01 0690) Management spolehlivosti – Část 1: Systémy managementu spolehlivosti

ČSN EN 60300-2 (01 0690) Management spolehlivosti – Část 2: Směrnice pro management spolehlivosti

ČSN EN 60300-3-3 (01 0690) Management spolehlivosti – Část 3-3: Pokyn k použití – Analýza nákladů životního cyklu

ČSN EN 62347 (01 0696) Návod pro specifikace spolehlivosti systémů

ČSN EN 61160 (01 0678) Přezkoumání návrhu

ČSN EN 61078 (01 0677) Techniky analýzy spolehlivosti – Blokový diagram bezporuchovosti a booleovské metody

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

ČSN EN 61165 (01 0691) Použití Markovových technik

ČSN EN 62551 (01 0677) Techniky analýzy spolehlivosti – Techniky Petriho sítí

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

ČSN IEC 60300-3-1 (01 0690) Management spolehlivosti – Část 3-1: Pokyn k použití – Techniky analýzy spolehlivosti – Metodický pokyn)

ČSN EN 61508-3 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software

ČSN EN 62429 (01 0647) Růst bezporuchovosti – Zkoušení namáháním pro zjišťování časných poruch v jedinečných složitých systémech)

ČSN EN 61014 (01 0645) Programy růstu bezporuchovosti

ČSN EN 61164 (01 0647) Růst bezporuchovosti – Metody statistických testů a odhadů

Informativní údaje z IEC 62628:2012

Mezinárodní normu IEC 62628 vypracovala technická komise IEC/TC 56 *Spolehlivost*.

Text této normy se zakládá na těchto dokumentech:

FDIS	Zpráva o hlasování
56/1469/FDIS	56/1480/RVD

Úplnou informaci o hlasování při schvalování této normy lze najít ve zprávě o hlasování ve výše uvedené tabulce.

Tato publikace byla vypracována v souladu se směrnicemi ISO/IEC, část 2.

Komise rozhodla, že obsah této publikace se nebude měnit až do výsledného data aktualizace uvedeného na webových stránkách IEC (http://webstore.iec.ch) v údajích o této publikaci. K tomuto datu bude publikace buď

- znovu potvrzena,
- zrušena,
- nahrazena revidovaným vydáním, nebo
- změněna.

Vysvětlivky k textu převzaté normy

Vypracování normy

Zpracovatel: Alopex, s.r.o., IČ 27266982, doc. Ing. David Vališ, Ph.D.

Technická normalizační komise: TNK 5 Spolehlivost

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jindřich Šesták

EVROPSKÁ NORMA EN 62628
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Září 2012

ICS 03.120.01

Pokyn pro softwarová hlediska softwaru
(IEC 62628:2012)

Guidance on software aspects of dependability
(IEC 62628:2012)

Lignes directrices concernant la sureté
de fonctionnement du logiciel
(CEI 62628:2012)

Leitlinien zu Softwareaspekten der Zuverlässigkeit
(IEC 62628:2012)

Tato evropská norma byla schválena CENELEC dne 2012-09-12. Členové CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC 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 Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Členy CENELEC jsou národní elektrotechnické komitéty Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, 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, Švýcarska a Turecka.

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 62628:2012 E

Předmluva

Text dokumentu 56/1469/FDIS, budoucího prvního vydání IEC 62628, vypracovaný technickou komisí IEC/TC 56 *Spolehlivost* byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 62628:2012.

Jsou stanovena tato data:

• nejzazší datum zavedení dokumentu na národní úrovni vydáním identické národní normy nebo vydáním oznámení o schválení k přímému používání jako normy národní	(dop)	2013-06-12
• nejzazší datum zrušení národních norem, které jsou s dokumentem v rozporu	(dow)	2015-09-12

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CENELEC [a/nebo CEN] nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv.

Přílohu ZA doplnil CENELEC.

Oznámení o schválení

Text mezinárodní normy IEC 62628:2012 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Strana

Úvod

Software má v současných produktech a systémech široké použití. Jedná se například o použití softwaru v programovatelném řídícím zařízení, počítačových systémech a komunikačních sítích. Během let vzniklo mnoho norem pro softwarové inženýrství, pro management softwarových procesů, pro zajištění kvality a bezporuchovosti softwaru, ale pouze několik z nich se zaměřilo na problémy softwaru z hlediska spolehlivosti.

Spolehlivost je schopnost systému fungovat tak, jak je to požadováno a tehdy, když je to požadováno, za účelem splnění specifických cílů za daných podmínek použití. Ze spolehlivosti systému se usuzuje, že je systém důvěryhodný a je schopen vykonávat požadovanou službu na vyžádání s cílem uspokojit potřeby uživatele. Vzrůstající trendy v používání softwaru v odvětví služeb rychle pronikl do internetových služeb a vývoje webu. Normalizovaná rozhraní a protokoly umožnily použití funkčnosti softwaru třetí stranou v rámci celého internetu, čímž povolily používání křížových platforem, křížových poskytovatelů a křížových domén. Software se stal hnacím mechanismem k tomu, aby se realizovaly složité systémové operace a aby bylo možné dosáhnout proveditelného elektronického obchodování pro bezproblémovou integraci a management podnikových procesů. Návrh softwaru předpokládá, že jeho hlavní funkcí bude zpracovávání dat, sledování bezpečnosti, bezpečnostní ochrana a komunikační spoje v síťových službách. Tento posun v paradigmatu dává globálním obchodním společnostem důvěru v situaci, ve které se pro udržení obchodních operací silně spoléhají na softwarové systémy. Spolehlivost systémů hraje rozhodující úlohu při ovlivňování úspěšné funkčnosti systému a integrity dat.

Tato mezinárodní norma poskytuje nejlepší současné průmyslové praktiky a představuje platnou metodiku usnadňující dosažení spolehlivosti softwaru. Určuje vliv managementu na softwarová hlediska spolehlivosti a poskytuje příslušné technické procesy s cílem vkonstruovat spolehlivost softwaru do systémů. Rozvoj technologií softwaru a rychlé přizpůsobení aplikací softwaru v průmyslových praktikách vyvolalo potřebu vytvořit praktickou normu pro spolehlivost softwaru pro globální obchodní prostředí. V návodu k použití této normy byl použit strukturovaný přístup.

V této normě jsou uvedeny procesy a požadavky na generickou spolehlivost softwaru. Tvoří základ pro použití spolehlivosti při vývoji většiny softwarových produktů a implementaci softwarových systémů. Pro životně důležité, bezpečnostní a zabezpečovací aplikace jsou nutné další požadavky. Tato norma se nezaměřuje na kvalifikační záležitosti softwaru specifické pro nějaké průmyslové odvětví týkající se bezporuchovosti a shody kvality.

Tato norma může také sloužit jako návod k návrhu spolehlivosti firmware. Nezaměřuje se však na hlediska implementace firmwaru, jehož software je obsažen nebo zabudován do hardwarových čipů, s cílem realizovat vyhrazené funkce. Jedná se například o čipy zákaznických integrovaných obvodů (ASIC) a řadičů řízených mikroprocesorem. Tyto produkty jsou často navrženy a začleněny jako součást fyzických schopností hardwaru s cílem minimalizovat jejich velikost a hmotnost a usnadnit jejich použití v reálném čase, jako například produkty, které jsou používány v mobilních telefonech. Ačkoli mohou být obecné principy a praktiky spolehlivosti popsané v této normě použity jako pokyny k návrhu a použití firmwaru, k jejich fyzické konstrukci, výrobě zařízení a implementaci zabudovaného softwarového produktu jsou nezbytné specifické požadavky. Ve srovnání s poruchami softwarových systémů se fyzika poruch zákaznických zařízení chová odlišně.

Tato mezinárodní norma není určena k posuzování shody nebo k účelům certifikace.

1 Předmět normy

Tato mezinárodní norma se zaměřuje na problémy týkající se softwarových hledisek spolehlivosti a poskytuje návod, jak dosáhnout spolehlivosti fungování softwaru, která je ovlivňována disciplínami managementu, procesy návrhu a prostředím použití. Ustanovuje se v ní všeobecný rámec pro požadavky na spolehlivost softwaru, je v ní uveden proces spolehlivosti softwaru pro aplikace životního cyklu systému, jsou prezentována kritéria zajišťování a metodika pro návrh a implementaci spolehlivosti softwaru a jsou poskytovány praktické přístupy pro hodnocení výkonnosti a měření charakteristik spolehlivosti v softwarových systémech.

Tato norma je použitelná jako návod pro projektanty a dodavatele softwarových systémů, pracovníky zajišťující integraci systému, provozní obsluhu a údržbáře a pro uživatele softwarových systémů, kteří se zabývají praktickými přístupy a aplikačním inženýrství s cílem dosáhnout spolehlivosti produktů a softwarových systémů.