

Návod pro specifikace spolehlivosti systémů	ČSN EN 62347 01 0696
---	--------------------------------

idt IEC 62347:2006

Guidance on system dependability specifications

Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes

Anleitung zur Spezifikation der Zuverlässigkeit von Systemen

Tato norma je českou verzí evropské normy EN 62347:2007. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 62347:2007. It was translated by Czech Standards Institute. It has the same status as the official version.



© Český normalizační institut, 2007
Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

79665

-
Kapitola 191: Spožehlivost a akost sluzieb

IEC 60300-1 zavedena v ČSN EN 60300-1 (01 0690) Management spolehlivosti - Část 1: Systémy managementu spolehlivosti

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

IEC 60300-3-4 zavedena v ČSN IEC 300-3-4 (01 0690) Management spolehlivosti - Část 3: Návod k použití - Oddíl 4: Pokyny ke specifikaci požadavků na spolehlivost

IEC 60300-3-15 dosud nezavedena

IEC 61069 (všechny části) zavedeny v souboru norem ČSN EN 61069 (18 0451) Měření a řízení průmyslových procesů - Hodnocení vlastností systému pro odhad systému

IEC 61069-1 zavedena v ČSN EN 61069-1 (18 0451) Měření a řízení průmyslových procesů - Hodnocení vlastností systému pro odhad systému - Část 1: Všeobecné úvahy a metodologie

ISO/IEC 15288 zavedena v ČSN ISO/IEC 15288 (36 9042) Systémové inženýrství - Procesy životního cyklu systému

ISO 9000:2005 zavedena v ČSN EN ISO 9000:2006 (01 0300) Systémy managementu kvality - Základní principy a slovník

Informativní údaje z IEC 62347:2006

Mezinárodní norma IEC 62347 byla připravena Technickou komisí IEC 56: Spolehlivost.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
56/1138/FDIS	56/1161/RVD

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

Tato publikace byla navržena v souladu s Částí 2 Směrnice ISO/IEC.

Komise rozhodla, že se obsah této publikace nebude měnit až do výsledného data udržování této normy vyznačeného na webové stránce IEC s adresou <http://webstore.iec.ch> v údajích týkajících se této publikace. Po tomto datu bude tato publikace buď

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

Upozornění na národní poznámku

Do normy byla k článku 4.1.2 doplněna informativní národní poznámka.

Vypracování normy

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

Technická normalizační komise: TNK 5 Spolehlivost

Pracovník Českého normalizačního institutu: Ing. Pavel Voráček

Strana 3

EVROPSKÁ NORMA	EN 62347
EUROPEAN STANDARD	
NORME EUROPÉENNE	
EUROPÄISCHE NORM	Březen 2007

ICS 03.120.01

Návod pro specifikace spolehlivosti systémů
(IEC 62347:2006)

Guidance on system dependability specifications
(IEC 62347:2006)

Lignes directrices pour les spécifications
de sûreté de fonctionnement des systèmes
(CEI 62347:2006)

Anleitung zur Spezifikation der Zuverlässigkeit
von Systemen
(IEC 62347:2006)

Tato evropská norma byla schválena CENELEC 2007-03-01. 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 jakémkoliv 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: rue de Stassart 35, B-1050 Brusel

© 2007 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmikoli prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN

62347:2007 E

Strana 4

Předmluva

Text dokumentu 56/1138/FDIS, budoucího 1. vydání normy IEC 62347, vypracovaný v technické komisi IEC TC 56 „Spolehlivost“, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 62347 dne 2007-03-01.

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 (dop) 2007-12-01
- nejzazší datum zrušení národních norem,
které jsou s EN v rozporu (dow) 2010-03-01

Přílohu ZA doplnil CENELEC.

Oznámení o schválení

Text mezinárodní normy IEC 62347:2006 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Strana 5

Obsah

Strana

Úvod

.....

..... 6

1 Předmět normy

.....

..	7
2 Citované normativní dokumenty.....	7
3 Termíny a definice.....	7
4 Pojmy týkající se spolehlivosti systému.....	8
4.1 Pochopení systému.....	8
4.2 Životní cyklus systému.....	9
4.3 Provoz systému.....	10
4.4 Provozní profil systému.....	11
4.5 Požadavky na spolehlivost.....	11
5 Postup při specifikování spolehlivosti systému.....	13
5.1 Proces specifikace systému.....	13
5.2 Proces specifikace spolehlivosti systému.....	13
5.3 Stanovení hodnot ukazatelů spolehlivosti.....	14
5.4 Kroky postupu při stanovení požadavků na spolehlivost systému.....	15
Příloha A (informativní) Hodnocení znaků spolehlivosti.....	18
Příloha B (informativní) Příklad vypracování specifikace spolehlivosti systému - Domácí bezpečnostní systém.....	23

Bibliografie

..... 29

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace..... 30

Obrázek 1 - Příklad vlastností systému a souvisejících znaků..... 8

Obrázek 2 - Přehled etap životního cyklu systému..... 10

Obrázek 3 - Vztah provozního profilu systému a scénáře při provozu systému..... 11

Obrázek 4 - Přehled procesu specifikace systému..... 14

Obrázek 5 - Kroky pro stanovení požadavků na spolehlivost systému..... 16

Obrázek B.1 - Konfigurace systému pro běžný provozní režim..... 26

Obrázek B.2 - Konfigurace systému pro nouzový provozní režim..... 26

Obrázek B.3 - Konfigurace systému pro provozní režim s bezpečnostní službou..... 27

Tabulka A.1 - Příklady ovlivňujících faktorů při jednotlivých ovlivňujících podmínkách..... 21

Tabulka A.2 - Vztah vlastností systému k ovlivňujícím podmínkám..... 22

Strana 6

Úvod

Systém je fyzická a/nebo virtuální entita. Někdy je nutné vymezit hranice systému tak, aby jej bylo možné odlišit nebo oddělit od jiných systémů. Aby systém splnil specifickou potřebu nebo účel, nebo aby dosáhl určitého cíle, vzájemně reaguje se svým okolním prostředím. To se uskutečňuje prostřednictvím interakce prvků systému představujících nezbytné funkce navržené tak, aby byl splněn zamýšlený cíl. Proces vývoje specifikace systému představuje stanovení funkcí potřebných ke splnění specifického cíle. Podrobný návrh systému začíná teprve poté, co byly zjištěny tyto funkce.

Systémy se mohou lišit svou konstrukční i funkční složitostí. Systém se může skládat z hardwarových, softwarových a lidských prvků nebo může být kombinací jakýchkoliv z těchto prvků, aby vykonával nezbytné funkce. Systém plnící jedinou funkci může být produkt, jako je televizní přijímač nebo

softwarový program pro regulaci osvětlení. Systém vykonávající více funkcí může být domácí kino nebo letadlo. Jednotlivé systémy s vymezenými hranicemi mohou být spolu pospojovány, aby vytvořily složitou soustavu vzájemně na sebe působících systémů, jako je elektrická rozvodná síť nebo služba internetového protokolu.

Ve specifikaci systému se stanovuje obálka a hranice systému. Struktura systému je často hierarchickým propojením subsystémů a vzájemně na sebe působících systémů. Specifikace systému je použitelná u všech systémů, které mají stejné obecně použitelné vymezení systému, bez ohledu na jejich hierarchii. Specifikace systému nezaměňuje ani nenahrazuje při používání specifikaci produktu, kde jsou uvedeny specifické podrobnosti o požadavcích na produkt.

Ze spolehlivosti systému se usuzuje, že je systém chápán jako důvěryhodný a že je schopen na požádání poskytovat službu ve formě kýžených atributů výkonnosti. Takových atributů výkonnosti lze dosáhnout začleněním spolehlivosti do funkcí. Ze spolehlivosti logicky vyplývá povědomí o důvěře uživatele získané z předchozích zkušeností se systémem, který při plnění očekávání uživatele funguje bez poruch.

V této mezinárodní normě je uvedeno zdůvodnění důležitosti uvádění spolehlivosti ve specifikaci systému pomocí funkcí. Je v ní uveden postup stanovení požadavků na spolehlivost systémů. Pro provoz generického systému je popsán proces stanovení funkcí potřebných ke splnění cíle spolehlivosti systému. Pro provoz specifického systému je zaveden pojem provozní profil, aby se stanovily požadavky na funkce vykonávané v určitém prostředí, které se vztahuje k provozu specifického systému. Tato mezinárodní norma je založena na modelu systému a kategorizaci funkcí stanovených v souboru norem IEC 61069. Příslušné technické procesy pro stanovení a analýzu požadavků na systém jsou převzaty z ISO/IEC 15288. Kroky postupu a procesy stanovení požadavků na spolehlivost systémů jsou uvedeny s použitelnými příklady. Jako vodítko pro management spolehlivosti se používají normy IEC 60300-1 a IEC 60300-2. V této mezinárodní normě je proces specifikace spolehlivosti rozšířen v tom smyslu, že se norma zabývá funkcemi jako nezbytným předpokladem pro návrh systému. Tato norma doplňuje normu IEC 60300-3-4 o specifikaci požadavků na spolehlivost produktů a zařízení. Technický proces začlenění spolehlivosti do návrhu systémů je popsán v IEC 60300-3-15.

Strana 7

1 Předmět normy

V této mezinárodní normě je uveden návod na vypracování specifikací spolehlivosti systémů. Je v ní uveden proces hodnocení systému a postup stanovení požadavků na spolehlivost systémů.

Tato mezinárodní norma není určena k certifikaci nebo posuzování shody pro smluvní účely. Jejím záměrem není měnit jakákoliv práva nebo povinnosti vyplývající z příslušných požadavků uvedených v zákonech, předpisech a nařízeních.

-- Vynechaný text --