

2007

Analýza stromu poruchových stavů (FTA)

ČSN
EN 61025

01 0676

idt IEC 61025:2006

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)

Fehlzustandsbaumanalyse

Tato norma je českou verzí evropské normy EN 61025:2007. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 61025:2007. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN IEC 1025 (01 0676) z ledna 1994.



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

79666

Změny proti předchozí normě

Změny proti předchozí normě jsou uvedeny v článku Informativní údaje z IEC 61025:2006 v této Národní předmluvě.

Informace o citovaných normativních dokumentech

IEC 60050(191) zavedena v ČSN IEC 50(191) (01 0102) Mezinárodní elektrotechnický slovník - Kapitola 191: Spožahlivost a akost služieb

IEC 61165 zavedena v ČSN EN 61165 (01 0691) Použití Markovových technik

Související normy

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

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

IEC 61078 zavedena v ČSN EN 61078 (01 0677) Techniky analýzy spolehlivosti - Blokový diagram bezporuchovosti a booleovské metody

Informativní údaje z IEC 61025:2006

Mezinárodní norma IEC 61025 byla připravena Technickou komisí IEC 56: Spolehlivost.

Text této normy vychází z těchto dokumentů:

FDIS	Zpráva o hlasování
56/1142/FDIS	56/1162/RVD

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

Toto druhé vydání ruší a nahrazuje první vydání publikované v roce 1990 a je jeho technickou revizí.

Hlavní změny vzhledem k předchozímu vydání jsou tyto:

- bylo doplněno podrobné vysvětlení metodiky stromu poruchových stavů;
- byla doplněna kvantitativní hlediska a hlediska bezporuchovosti u analýzy stromu poruchových stavů (FTA);
- byl přesněji vymezen vztah analýzy stromu poruchových stavů k jiným technikám spolehlivosti;
- byly doplněny příklady analýz a užití metod vysvětlených v této normě;
- byly aktualizovány značky používané v současné době.

Kapitola 7, která se zabývá analýzou, byla revidována tak, že je zaměřena na tradiční analýzu logického stromu poruchových stavů odděleně od kvantitativní analýzy, která se již po mnoho let používá pro zlepšování bezporuchovosti produktů v jejich etapě vývoje.

Některé materiály zahrnuté dříve do hlavní části této normy byly přeneseny do příloh A a B.

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

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

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

Strana 3

Vysvětlivky k textu převzaté normy

Název metody FTA (Fault Tree Analysis) se v české odborné literatuře překládá různým způsobem:

- analýza stromu chyb;
- analýza stromu vad;
- analýza stromu poruch;
- analýza stromů poruch;
- analýza stromem poruch;
- analýza stromu poruchových stavů;
- a jiné.

Většina těchto názvů vychází z nesprávného překladu anglického termínu „fault“.

Pro tento překlad nelze použít český termín „chyba“, který je definován v 191-05-24 ČSN IEC 50(191) pro anglický termín „error“ jako „nesoulad mezi počítanou, pozorovanou nebo měřenou hodnotou nebo podmínkou a skutečnou definovanou nebo teoreticky správnou hodnotou nebo podmínkou“.

Termín „vada“ je definovaný termín z oboru managementu kvality („nesplnění požadavku ve vztahu k zamýšlenému nebo specifikovanému použití“ - viz 3.6.3 ČSN EN ISO 9000:2001), který je vyhrazen pro překlad anglického termínu „defect“ a má právní dopady. V důsledku toho se má termín „vada“ používat s krajní opatrností.

Termín „porucha“ je definován v 191-04-01 ČSN IEC 50(191) pro anglický termín „failure“ jako „ukončení schopnosti objektu plnit požadovanou funkci“. Porucha je jev (událost) přechodu mezi stavem, kdy je objekt schopen plnit požadovanou funkci a stavem, kdy není schopen plnit tuto funkci.

Termín „fault“ je definován v 191-05-01 ČSN IEC 50(191) jako „poruchový stav“ („stav objektu charakterizovaný neschopností plnit požadovanou funkci kromě neschopnosti během preventivní údržby jiných plánovaných činností nebo způsobený nedostatkem vnějších zdrojů“).

Jediným správným překladem termínu „fault“ je tudíž jeho český ekvivalent „poruchový stav“.

Jak vyplývá z popisu FTA (viz 5.1), sestavuje se příslušný strom vždy pro *jednu* vrcholovou událost (poruchový

stav), takže správný překlad názvu normy „Fault tree analysis“ by měl být „Analýza stromu poruchového stavu“, jak to odpovídá též francouzskému názvu „Analyse par arbre de panne“ i německému názvu „Fehlzustandsbaumanalyse“. Vzhledem k tomu, že se název „Analýza stromu poruchových stavů“ používá pro FTA ve všech normách zabývajících se spolehlivostí a v mnoha dalších člancích v odborné literatuře, byl v této normě ponechán uvedený tradiční název odpovídající názvu předchozí normy ČSN IEC 1025:1994.

Upozornění na národní poznámky

Do normy byly ke kapitole 8 a k tabulce A.1 v příloze A doplněny informativní národní poznámky.

Vypracování normy

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

Technická normalizační komise: TNK 5 Spolehlivost

Pracovník Českého normalizačního institutu: Ing. Pavel Voráček

Strana 4

Prázdna strana

Strana 5

EVROPSKÁ NORMA	EN 61025
EUROPEAN STANDARD	
NORME EUROPÉENNE	
EUROPÄISCHE NORM	Duben 2007

ICS 03.120.01; 03.120.99
S1:1992

Nahrazuje HD 617

Analýza stromu poruchových stavů (FTA)
(IEC 61025:2006)
Fault tree analysis (FTA)
(IEC 61025:2006)

Analyse par arbre de panne (AAP)
(CEI 61025:2006)

Fehlzustandsbaumanalyse
(IEC 61025:2006)

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

61025:2007 E

Strana 6

Předmluva

Text dokumentu 56/1142/FDIS, budoucího 2. vydání normy IEC 61025, vypracovaný v technické komisi IEC TC 56 „Spolehlivost“, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 61025 dne 2007-03-01.

Tato evropská norma nahrazuje HD 617 S1:1992.

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 61025:2006 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod

..... 8

1 Předmět
normy

..... 9

2 Citované normativní
dokumenty..... 9

3 Termíny a
definice

..... 9

4
Značky

..... 12

5
Všeobecně

..... 12

5.1 Popis a struktura stromu poruchových
stavů..... 12

5.2
Cíle

..... 13

5.3
Použití

..... 13

5.4 Kombinace s jinými technikami analýzy
bezporuchovosti..... 14

6 Rozvoj a
vyhodnocení

..... 15

6.1 Všeobecné

úvahy	
.....	
15	
6.2 Požadované informace o systému.....	17
6.3 Grafický popis a struktura stromu poruchových stavů.....	18
7 Rozvoj a vyhodnocení stromu poruchových stavů.....	19
7.1 Všeobecně	
.....	
..... 19	
7.2 Předmět analýzy	
.....	
19	
7.3 Seznámení se se systémem.....	19
7.4 Rozvoj stromu poruchových stavů.....	19
7.5 Sestavení stromu poruchových stavů.....	20
7.6 Intenzity poruch při analýze stromu poruchových stavů.....	32
8 Identifikace a označování ve stromu poruchových stavů.....	33
9 Zpráva	
.....	
..... 33	
Příloha A (informativní) Značky.....	
35	
Příloha B (informativní) Podrobný postup vytváření disjunkcí.....	41
Bibliografie	
.....	
..... 44	

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace..... 45

Obrázek 1 - Vysvětlení termínů používaných v analýze stromu poruchových stavů..... 11

Obrázek 2 - Reprezentace sériové struktury pomocí stromu poruchových stavů..... 21

Obrázek 3 - Reprezentace paralelní aktivní zálohy pomocí stromu poruchových stavů..... 22

Obrázek 4 - Příklad stromu poruchových stavů, ve kterém jsou znázorněny různé typy hradel..... 23

Obrázek 5 - Obdélníková reprezentace hradel a událostí..... 24

Obrázek 6 - Příklad stromu poruchových stavů obsahujícího opakovanou událost a hradlo pro transfer..... 25

Obrázek 7 - Příklad, na kterém jsou ukázány události se společnou příčinou při obdélníkové reprezentaci hradel.. 25

Obrázek 8 - Příklad můstkového obvodu, který má být analyzován pomocí stromu poruchových stavů..... 28

Obrázek 9 - Reprezentace stromu poruchových stavů můstkového obvodu..... 29

Obrázek 10 - FTA můstkového systému - Esaryho-Proschanova metoda, bez vytváření disjunkcí..... 30

Obrázek 11 - Pravděpodobnost poruchy můstkového systému vypočtená s aproximací vzácné události..... 31

Obrázek 12 - Pravděpodobnost výskytu vrcholové události s vytvářením disjunkcí..... 32

Obrázek A.1 - Příklad hradla PAND..... 38

Tabulka A.1 - Často používané značky pro strom poruchových stavů..... 35

Tabulka A.2 - Obecné značky pro události a popis událostí..... 38

Tabulka A.3 - Statická hradla..... 39

Tabulka A.4 - Dynamická hradla..... 40

Úvod

Analýza stromu poruchových stavů (FTA - Fault tree analysis) se zabývá identifikací a analýzou podmínek a faktorů, které způsobují nebo mohou potenciálně způsobit výskyt nebo přispívat k výskytu specifikované vrcholové události. Při analýze FTA je touto událostí obvykle „zadření“ nebo zhoršené fungování systému, snížení bezpečnosti nebo zhoršení jiných důležitých provozních atributů, zatímco při analýze STA (Success Tree Analysis - analýze stromu úspěchů) je touto událostí atribut popisující úspěch (bezporuchový stav).

FTA se často uplatňuje při analýze bezpečnosti systémů (jako jsou dopravní systémy, elektrárny nebo jakékoliv jiné systémy, u kterých se vyžaduje vyhodnocení bezpečnosti jejich provozu). Analýzu stromu poruchových stavů lze též použít pro analýzu pohotovosti a udržovatelnosti. Pro jednoduchost se však bude ve zbývajících částech této normy používat k reprezentaci i těchto hledisek fungování systému termín „bezporuchovost“.

Tato norma se zabývá dvěma přístupy k analýze FTA. Prvním z nich je kvalitativní přístup, při kterém se pravděpodobnost události a faktorů, které k ní přispívají, (vstupních událostí) nebo jejich četnost výskytu nesleduje. Při tomto přístupu se provádí podrobná kvalitativní analýza událostí/poruchových stavů a přístup je znám jako kvalitativní či tradiční FTA. Široce se používá v aplikacích v jaderném průmyslu a v mnoha jiných případech, kdy se hledají potenciální příčiny poruchových stavů, přičemž pravděpodobnost jejich výskytu není předmětem zájmu. Občas se při tradiční analýze FTA některé události zkoumají kvantitativně, ale tyto výpočty se odlučují od jakýchkoliv pojmů celkové bezporuchovosti a v tomto případě se nikdo nepokouší vypočítat celkovou bezporuchovost s použitím analýzy FTA. Druhý přístup, který se přejímá v mnoha průmyslových odvětvích, je převážně kvantitativní přístup, při kterém se pomocí podrobné analýzy FTA modeluje celý produkt, proces nebo systém, a velká většina základních událostí, ať již poruchových stavů, nebo událostí, má v modelu nějakou pravděpodobnost výskytu stanovenou pomocí analýzy nebo zkoušky. V tomto případě je konečným výsledkem pravděpodobnost výskytu vrcholové události reprezentující pravděpodobnost bezporuchového provozu nebo pravděpodobnost poruchového stavu či poruchy.

1 Předmět normy

V této mezinárodní normě je popsána analýza stromu poruchových stavů a je v ní uveden návod na její použití v podobě:

- vymezení základních principů;
 - popisu a vysvětlení příslušného matematického modelování;
 - vysvětlení vztahů analýzy FTA k jiným technikám modelování bezporuchovosti;
- popisu kroků použitých při provádění analýzy FTA;
- identifikace vhodných předpokladů, událostí a způsobů poruch;
- identifikace a popisu obecně používaných značek.

-- Vynechaný text --