

ČESKÁ TECHNICKÁ NORMA

ICS 21.020 **Srpen 2013**

Techniky analýzy spolehlivosti –
Techniky Petriho sítí

ČSN
EN 62551
01 0677

idt IEC 62551:2012

Analysis techniques for dependability – Petri net techniques

Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Petri

Analysemethoden für Zuverlässigkeit – Petrinetze

Tato norma je českou verzí evropské normy EN 62551:2012. 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 62551:2012. 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 60050-191:1990 zavedena v ČSN IEC 50(191):1993 (01 0102) Mezinárodní elektrotechnický slovník –

Kapitola 191: Spožahlivost a akost' služieb

Souvisící ČSN

ČSN IEC 60050-151:2004 (33 0050) Mezinárodní elektrotechnický slovník – Část 151: Elektrická a magnetická zařízení

ČSN IEC 50(111):1998 (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 111: Fyzika a chemie

ČSN IEC 60050-351:2007 (33 0050) Mezinárodní elektrotechnický slovník – Část 351: Technologie řízení

ČSN EN 61508 (18 0301) (soubor) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností

ČSN EN 61508-1 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky

ČSN EN 61508-4 ed. 2:2011 (18 0301) Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 4: Definice a zkratky

ČSN EN 61165:2007 (01 0691) Použití Markovových technik

ČSN EN 50126-1:2001 (33 3502) Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces

ČSN EN 60812:2007 (01 0675) Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)

ČSN EN 61025:2007 (01 0676) Analýza stromu poruchových stavů (FTA)

ČSN EN 61078:2007 (01 0677) Techniky analýzy spolehlivosti – Blokový diagram bezporuchovosti a booleovské metody

ČSN EN 61511-3:2005 (18 0303) Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů – Část 3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti

ČSN EN 61703:2002 (01 0607) Matematické výrazy pro ukazatele bezporuchovosti, pohotovosti, udržovatelnosti a zajištěnosti údržby

Informativní údaje z IEC 62551:2012

Mezinárodní normu IEC 62551 vypracovala technická komise IEC/TC 56 *Spolehlivost*.

Text této normy se zakládá na těchto dokumentech:

FDIS	Zpráva o hlasování
56/1476/FDIS	56/1484/RVD

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

Názvosloví Petriho sítí uváděné v české odborné literatuře je dosud neustálené a pro stejné anglické termíny se používají jejich různé české ekvivalenty. Týká se to především následujících termínů:

fire/firing/fired

Pro tento anglický termín se používají české termíny „provést“/„provedení“/„proveden“,

„spustit“/„spuštění“/„spuštěný“, „uskutečnit“/„uskutečnění“/„uskutečněn“, „aktivovat“/„aktivace“/„aktivovaný“ nebo „realizovat“/„realizace“/„realizovaný“; v poslední době se též používá termín „odpálit“/„odpal“/„odpálený“, který nejvíce odpovídá příslušnému anglickému termínu, a tento překlad byl použit v této normě.

token

V české literatuře se pro tento anglický termín používají termíny „žeton“, „tečka“, „značka“, „značení“ nebo „označení“ a v poslední době se nejčastěji používá český odborný termín „token“, který byl použit v této normě.

enabled

V české literatuře se pro tento anglický termín používají termíny „umožněn“, „uschopněn“ „aktivní“/„aktivován“/ „aktivovaný“, „povolen“/„povolený“ nebo „dovolen“/„dovolený“ a v poslední době se nejčastěji používá český termín „proveditelný“, který byl použit v této normě.

reward / reward function / rate reward / impulse reward

Tyto pojmy se používají hlavně v příbuzném oboru „Markov Reward Model“, který se obvykle (nesprávně) překládá jako „Markovův model s oceněním“ nebo „Markovův model s hodnocením“. Samotný termín „reward“ se v článcích zabývajících se tímto modelem překládá jako „výnos“ nebo „užitek“ a je definován jako „bonus, zisk nebo duálně (též) jako náklady“. Této definici nejlépe odpovídá význam pojmu „užitek“ a proto byl tento termín použit pro překlad termínu „reward“ v celé normě i pro odvozené termíny „funkce užitku“ (*reward function*), „souhrnný užitek“ (*rate reward*) a „impulzní užitek“ (*impulse reward*) popsané v článku A.3.3.4.

Vypracování normy

Zpracovatel: RNDr. Jaroslav Matějček, CSc., IČ 41127749 ve spolupráci s Centrem pro jakost a spolehlivost výroby – www.cqr.cz

Technická normalizační komise: TNK 5 Spolehlivost

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

EVROPSKÁ NORMA EN 62551

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM Listopad 2012

ICS 21.020

Techniky analýzy spolehlivosti – Techniky Petriho sítí (IEC 62551:2012)

Analysis techniques for dependability –
Petri net techniques
(IEC 62551:2012)

Tato evropská norma byla schválena CENELEC dne 2012-11-06. 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.

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

© 2012 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky jsou celosvětově vyhrazena členům CENELEC.
Ref. č. EN 62551:2012 E

Členy CENELEC jsou národní elektrotechnické komitety 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 a Švýcarska.

Předmluva

Text dokumentu 56/1476/FDIS, budoucího 1. vydání normy IEC 62551, vypracovaný technickou komisí IEC/TC 56 *Spolehlivost*, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 62551:2012.

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) 2013-08-06

nejzazší datum zrušení národních norem, které jsou s dokumentem v rozporu

(dow) 2015-11-06

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

Oznámení o schválení

Text mezinárodní normy IEC 62551:2012 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

Obsah

Strana

Úvod 10

1 Rozsah platnosti 11

2 Citované dokumenty 11

3 Termíny, definice, značky a zkratky 11

3.1 Termíny a definice 11

3.2 Značky a zkratky 13

4 Obecný popis Petriho sítí 14

4.1 Nečasované Petriho sítě nízké úrovně 14

4.2 Časované Petriho sítě nízké úrovně 14

4.3 Petriho sítě vysoké úrovně 15

4.4 Rozšíření Petriho sítí a modelování s Petriho sítěmi 15

4.4.1 Další reprezentace prvků Petriho sítí 15

4.4.2 Vztah k pojmům spolehlivosti 16

5 Modelování a analýza spolehlivosti pomocí Petriho sítí 16

5.1 Kroky, které se obecně mají provádět 16

5.2 Podrobný popis kroků, které se mají vykonat 17

5.2.1 Obecně 17

5.2.2 Popis hlavních částí a funkcí systému (krok 1) 18

5.2.3 Modelování struktury systému na základě dílčích modelů Petriho sítě a jejich vztahů (krok 2) 18

5.2.4 Zpřesňování modelů z kroku 2, dokud se nedosáhne požadované úrovně podrobnosti (krok 3) 19

5.2.5 Analýza modelu k dosažení výsledků, které jsou předmětem zájmu (krok 4) 20

5.2.6 Reprezentace a interpretace výsledků analýz (krok 5) 21

5.2.7 Souhrn dokumentace (krok 6) 21

6 Vztah k jiným modelům spolehlivosti 21

Příloha A (informativní) Struktura a dynamika Petriho sítí 22

Příloha B (informativní) Pohotovost se zálohováním m z n 31

Příloha C (informativní) Abstraktní příklad 36

Příloha D (informativní) Modelování typických pojmů spolehlivosti 39

Příloha E (informativní) Příklad železničního přejezdu 40

Bibliografie 57

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a na jim příslušející evropské publikace 59

Obrázek 1 - Vážená inhibiční hrana 15

Obrázek 2 - Místo p je vícenásobné místo 15

Obrázek 3 - Značení na místě p po odpalu přechodu t 16

Obrázek 4 - Aktivace přechodu t závisí na hodnotě V 16

Obrázek 5 - Metodika skládající se hlavně z kroků ‚modelování‘, ‚analýza‘ a ‚reprezentace‘ 17

Obrázek 6 - Proces modelování a analýzy pomocí Petriho sítí 17

Obrázek 7 - Struktura modelování zabývající se dvěma hlavními částmi ‚regulovaná soustava‘ a ‚řídící zařízení‘
s modely pro jejich funkce a spolehlivost 19

Obrázek 8 - Určování metody analýzy jako funkce PN modelu 20

Obrázek A.1 - Cyklus stav-přechod pro pohotovost součásti 22

Obrázek A.2 - Přechod ‚porucha‘ je proveditelný 23

Strana

Obrázek A.3 - Místo ‚je porouchaná‘ bylo označeno v důsledku odpalu ‚poruchy‘ 23

Obrázek A.4 - Přechod ‚oprava součásti₁‘ je proveditelný 23

Obrázek A.5 - Token na místě ‚údržbářská četa je k dispozici‘ není použit 24



Obrázek A.6 - Přechod není proveditelný 24

Obrázek A.7 - Značení před odpalem 24

Obrázek A.8 - Značení po odpalu 24

Obrázek A.9 - PN s počátečním značením 25

Obrázek A.10 - Příslušný RG 25

- Obrázek A.11 – Přejchody ,oprava součásti_{nizká priorita} ‘ a ,porucha součásti_{vysoká priorita} ‘ jsou proveditelné 26
- Obrázek A.12 – Značení po odpalu přechodu ,oprava součásti_{nizká priorita} ‘ 26
- Obrázek A.13 – Časovaná síť PN se dvěma časovanými přechody s exponenciálním rozdělením 27
- Obrázek A.14 – Odpovídající stochastický graf dosažitelnosti 27
- Obrázek A.15 – Petriho síť s časovanými přechody 28
- Obrázek B.1 – Dvě sítě pro pohotovost jednotlivých objektů se specifickými intenzitami poruch a oprav 31
- Obrázek B.2 – Stochastický graf dosažitelnosti odpovídající obrázku B.1 s globálními stavy (pro ,součást₁ je porouchaná‘ se používá zkratka ) 31
- Obrázek B.3 – Tři sítě pro pohotovost jednotlivých objektů se specifickými intenzitami poruch a oprav 31
- Obrázek B.4 – Stochastický graf dosažitelnosti odpovídající obrázku B.3 s globálními stavy (pro ,součást₁ je porouchaná‘ se používá zkratka ) 32
- Obrázek B.5 – Specificky propojená síť pohotovosti 1 ze 3 32
- Obrázek B.6 – Specificky propojená síť pohotovosti 2 ze 3 33
- Obrázek B.7 – Specificky propojená síť pohotovosti 3 ze 3 33
- Obrázek B.8 – Stochastický graf dosažitelnosti s provozními stavy specifickými pro systém 34
- Obrázek B.9 – Specificky propojená síť bezporuchovosti 1 ze 3 34
- Obrázek B.10 – Graf dosažitelnosti pro síť uvedenou na obrázku B.9 34
- Obrázek B.11 – Specificky propojená síť bezporuchovosti 2 ze 3 35
- Obrázek B.12 – Graf dosažitelnosti pro síť uvedenou na obrázku B.11 35
- Obrázek B.13 – Specificky propojená síť bezporuchovosti 3 ze 3 35
- Obrázek B.14 – Graf dosažitelnosti pro síť uvedenou na obrázku B.13 35
- Obrázek C.1 – Typická síť pohotovosti 36
- Obrázek C.2 – Stochastický graf pohotovosti sítě uvedené na obrázku C.1 se svými globálními stavy a agregovanými globálními stavy v souladu s pohotovostí a bezpečností 36
- Obrázek C.3 – Základní pojetí modelování bezporuchovosti a funkce 37
- Obrázek C.4 – Obecná hierarchická síť se superpřechody pro modelování bezporuchovosti 37
- Obrázek C.5 – Obecná hierarchická síť se superpřechody a supermísty 37

Obrázek C.6 – Obecná hierarchická síť se superpřechody pro modelování pohotovosti 38

Obrázek C.7 – Obecná hierarchická síť se superpřechody a supermísty 38

Obrázek E.1 – Použitý příklad železničního přejezdu a jeho zabezpečovacího zařízení 40

Obrázek E.2 – Hlavní části příkladu modelu železničního přejezdu 41

Obrázek E.3 – Dílčí modely příkladu modelu železničního přejezdu 42

Obrázek E.4 – PN model procesů automobilového a vlakového provozu 44

Obrázek E.5 – PN model procesů dopravního provozu a spolehlivosti dopravního provozu 45

Obrázek E.6 – PN model procesu dopravního provozu s ideální řídicí funkcí 46

Obrázek E.7 – PN model příkladu modelu železničního přejezdu 47

Strana

Obrázek E.8 – Sebrané naměřené hodnoty toku silničního provozu konkrétního železničního přejezdu: Časové intervaly mezi dvěma automobily přijíždějícími k železničnímu přejezdu 48

Obrázek E.9 – Přibližná distribuční funkce založená na naměřených hodnotách uvedených na obrázku E.5 49

Obrázek E.10 – Sebrané naměřené hodnoty doby strávené silničním vozidlem v nebezpečné zóně železničního přejezdu 49

Obrázek E.11 – Přibližná distribuční funkce založená na naměřených hodnotách uvedených na obrázku E.10 50

Obrázek E.12 – Agregovaný graf RG a informace o příslušných stavech 54

Obrázek E.13 – Výsledky kvantitativní analýzy ukazující průměrnou pohotovost železničního přejezdu pro uživatele silničního provozu jako funkci intenzity nebezpečí (nebezpečných poruch) zabezpečovacího zařízení pro různé použité doby aktivace a přiblížení T_{AC} 55

Obrázek E.14 – Výsledky kvantitativní analýzy ukazující individuální riziko uživatelů železničního přejezdu jako funkci intenzity nebezpečí (nebezpečných poruch) zabezpečovacího zařízení pro různé použité doby přiblížení a aktivace T_{AC} 56

Obrázek E.15 – Diagram pohotovosti/bezpečnosti založený na kvantitativních výsledcích analýzy modelu ukázaných na obrázcích E.13 a E.14 56

Tabulka 1 – Značky v nečasovaných Petriho sítích 13

Tabulka 2 – Doplnkové značky v časovaných Petriho sítích 13

Tabulka 3 – Značky pro hierarchické modelování 13

Tabulka 4 – Odpovídající si pojmy v systémech, Petriho sítích a ve spolehlivosti 16

Tabulka 5 – Povinné a doporučené části dokumentace 21

Tabulka A.1 – Odpovídající si pojmy v systémech, Petriho sítích, grafech dosažitelnosti a ve spolehlivosti 25

Tabulka A.2 – Místo a přechod s užítky 30

Tabulka D.1 – Pojmy spolehlivosti modelované PN strukturami 39

Tabulka D.2 – Modelování nákladů na stavy a události 39

Tabulka E.1 – Místa týkající se automobilů v dílčím modelu ‚Proces dopravního provozu‘ (viz obrázek E.4) 48

Tabulka E.2 – Přechody týkající se automobilového provozu v dílčích modelech ‚Proces dopravního provozu‘
a ‚Spolehlivost dopravního provozu‘ (viz obrázek E.7) 51

Tabulka E.3 – Místa týkající se vlakového provozu v dílčím modelu ‚Proces dopravního provozu‘ (viz obrázek E.7) 51

Tabulka E.4 – Přechody týkající se vlakového provozu v dílčím modelu ‚Proces dopravního provozu‘ (viz obrázek E.7) 52

Tabulka E.5 – Místa v dílčím modelu ‚Spolehlivost dopravního provozu‘ (viz obrázek E.7) 52

Tabulka E.6 – Přechody v dílčím modelu ‚Spolehlivost dopravního provozu‘ (viz obrázek E.7) 52

Tabulka E.7 – Místa v dílčím modelu ‚Řídící funkce‘ (viz obrázek E.7) 53

Tabulka E.8 – Přechody v dílčím modelu ‚Řídící funkce‘ (viz obrázek E.7) 53

Tabulka E.9 – Místa v dílčím modelu ‚Spolehlivost řídicího zařízení‘ (viz obrázek E.7) 53

Tabulka E.10 – Přechody v dílčím modelu ‚Spolehlivost řídicího zařízení‘ (viz obrázek E.7) 53

Tabulka E.11 – Specifikace booleovských podmínek pro stavy, které mají být začleněny do agregovaného stavu 55

Úvod

V této mezinárodní normě je uvedena základní metodika pro reprezentaci základních prvků Petriho sítí (PN – *Petri nets*) [1]¹ a návod pro používání technik v oblasti spolehlivosti.

Vnitřní síla modelování s použitím Petriho sítí spočívá v jeho schopnosti popsat chování systému pomocí modelování vztahu mezi lokálními stavy a lokálními událostmi. Na základě těchto skutečností dosáhly Petriho sítě širokého přijetí v mnoha průmyslových oblastech použití (např. v informační, komunikační, dopravní, výrobní a zpracovatelské oblasti a v energetice).

Konvenční metody jsou při zacházení se skutečnými průmyslovými systémy velmi omezené, protože nejsou schopny zvládnout zacházení s vícestavovými systémy, ani nejsou schopny modelovat dynamické chování systému (např. u stromu poruchových stavů nebo blokových diagramů bezporuchovosti) a mohou být náchylné k prudkému vzrůstu kombinací stavů, se kterými se má zacházet (např. u Markovova procesu). Tudíž je zapotřebí mít alternativní metody modelování

a výpočtu.

Výpočty spolehlivosti průmyslového systému jsou určeny k modelování různých stavů systému a procesu, jak se systém vyvíjí z jednoho stavu do jiného, když dojde k nějakým událostem (poruchám, opravám, periodickým testům, nastane noc, den atd.).

Technici zabývající se bezporuchovostí potřebují k dosažení svých modelů uživatelsky přívětivou grafickou podporu. Petriho sítě jsou zásluhou své grafické prezentace velmi slibnou technikou pro modelování a výpočty spolehlivosti.

Analytické výpočty jsou omezeny na malé systémy a/nebo tím, že musí být splněna přísná hypotéza (např. exponenciální zákon, nízká pravděpodobnost). Pro zacházení se systémy průmyslového rozsahu je nutné je kvalitativně rozšířit. To lze provést tak, že se vyjde z analytického výpočtu a přejde se k simulaci Monte Carlo.

Cílem této normy je vymežit sjednocené základní principy sítí PN v kontextu spolehlivosti a aktuálního používání PN modelování a analyzování Petriho sítě jako prostředku ke kvalitativnímu i kvantitativnímu posuzování spolehlivosti a ukazatelů systému vztahujících se k riziku.

1 Rozsah platnosti

V této mezinárodní normě je uveden návod pro metodiku založenou na Petriho sítích pro účely spolehlivosti. Napomáhá při modelování systému, analyzování modelu a prezentaci výsledků analýzy. Tato metodika je zaměřena na ukazatele vztahující se ke spolehlivosti se všemi příbuznými vlastnostmi, jako je bezporuchovost, pohotovost, pohotovost výroby, udržovatelnost a bezpečnost (např. ukazatele vztahující se k úrovni integrity bezpečnosti (SIL) [2]).

V normě se pojednává o následujících tématech vztahujících se k Petriho sítím:

- a. jsou definovány zásadní termíny a značky a popisuje se jejich užití a metody grafické reprezentace;
- b. je navržena terminologie a její vztah ke spolehlivosti;
- c. je prezentován přístup krok po kroku pro
 1. modelování spolehlivosti pomocí Petriho sítí,
 2. vedení při používání technik založených na Petriho sítích pro kvalitativní i kvantitativní analýzy spolehlivosti,
 3. prezentování a interpretaci výsledků analýz;
- d. je naznačen vztah Petriho sítí k jiným technikám modelování;
- e. jsou uvedeny praktické příklady.

V této normě není uveden návod, jak řešit matematické problémy, které vzniknou při analyzování sítě PN; takový návod lze nalézt v [3] a [4].

Tato norma je použitelná ve všech průmyslových odvětvích, kde se provádějí kvalitativní a kvantitativní analýzy spolehlivosti.

Konec náhledu - text dále pokračuje v placené verzi ČSN.