Reliability of Digital Systems

Redundancy, Spares, and Repairs (2)

Václav Přenosil

Design and Architecture of Digital Systems Laboratory

prenosil@fi.muni.cz

Fall, 2020

Pohotovostní systémy: Úvod

- Pohotovostní systém předpokládá, že některé prvky jsou zdvojeny tak, že jeden prvek je např. x_1 je primární a druhý prvek x_1' je záložní a tvoří paralelní spolehlivostní model
  - V běžném paralelním systému prvky x_1 a x_1' zahájí provoz v čase t = 0 a oba mohou mít poruchu
  - Vylepšení spočívá v zapnutí pouze primárního systému x_1 a systém x_1' necháme bez napájení (bez zatížení), čímž snížíme pravděpodobnost jeho poruchy
  - Pokud je možnost detekovat poruchu prvku x_1, pak lze aktivovat záložní prvek x_1' a tento se stane aktivním
  - Taková konfigurace systému se nazývá pohotovostní
  - Prvek x_1 se nazývá primárním prvkem a prvek x_1' pohotovostním prvkem
  - Jestliže je interval t_1 časem selhání prvku x_1 a interval t_2 časem selhání x_1' pak
    - pak v paralelním systému je časem selhání hodnota $max(t_1, t_2)$
    - v pohotovostním systému je doba poruchy rovna $t_1 + t_2$
- Běžný paralelní systém se nazývá systém s „horkou" zálohou a pohotovostní systém se nazývá systémem se „studenou" zálohou

Pohotovostní systémy: Pravděpodobnost bezp. činnosti

Tabulka 1: Stavy paralelního systému

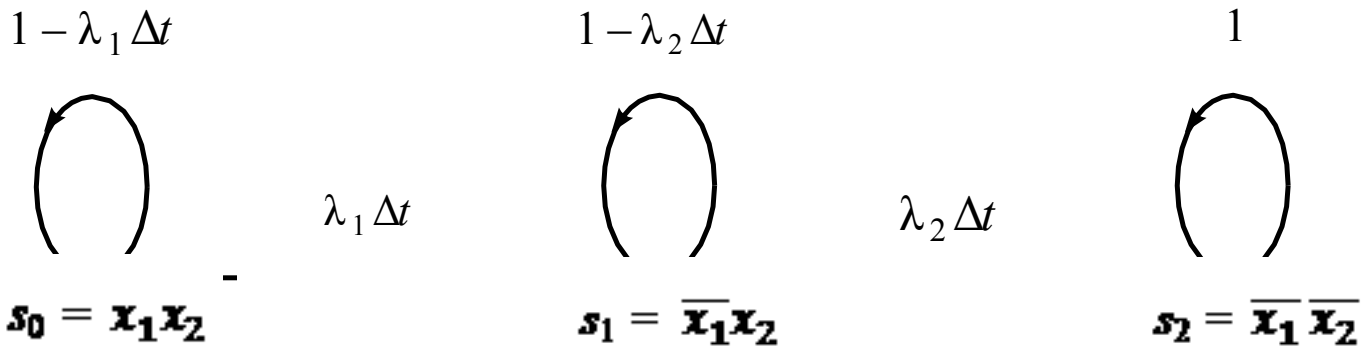
$s_0 = x_1 x_2$	oba prvky funkční
$s_1 = x_1 \overline{x_2}$	x_1 funkční; x_2 v poruše
$s_2 = \overline{x_1} x_2$	x_2 funkční; x_1 v poruše
$s_3 = \overline{x_1}\,\overline{x_2}$	oba prvky v poruše

- Předpokládejme, že záložní prvek bez napájení je bezporuchový

Tabulka 2: Stavy pohotovostního systému

$s_0 = x_1 x_2$	on-line a záložní prvky jsou funkční
$s_1 = \overline{x_1} x_2$	on-line prvek je v poruše, záložní prvek je funkční
$s_2 = \overline{x_1}\,\overline{x_2}$	on-line prvek i záložní prvek jsou v poruše

Pohotovostní systémy: Pravděpodobnost bezp. činnosti



Obrázek 1: Pravděpodobnostní stavový model pro pohotovostní systém

$$\frac{df(t)}{dt} \leftrightarrow sF(s) - f(0) \qquad e^{-at} \leftrightarrow \frac{1}{s+a}$$

$$\frac{dP_{s0}(t)}{dt} = -\lambda_1 P_{s0}(t) \longrightarrow sP_{s0}(s) - 1 = -\lambda_1 P_{s0}(s) \longrightarrow$$

$P_{s0}(t=0)=1$

$$\longrightarrow P_{s0}(s) = \frac{1}{s+\lambda_1} \longrightarrow P_{s0}(t) = e^{-\lambda_1 t}$$

Pohotovostní systémy: Pravděpodobnost bezp. činnosti

$$\frac{dP_{s1}(t)}{dt} = -\lambda_2 P_{s1}(t) + \lambda_1 P_{s0}(t) \longrightarrow sP_{s1}(s) - 0 = -\lambda_2 P_{s1}(s) + \lambda_1 P_{s0}(s) \longrightarrow$$

$P_{s1}(t=0)=0$

$$\longrightarrow P_{s1}(s)(s+\lambda_2) = \lambda_1(s+\lambda_1) \longrightarrow P_{s1}(s) = \lambda_1\left(\frac{1}{(s+\lambda_1)(s+\lambda_2)}\right) =$$

$$= \lambda_1\left(\frac{A_1}{(s+\lambda_1)} + \frac{A_2}{(s+\lambda_2)}\right)$$

$$A_1 = \left[\frac{1}{(s+\lambda_1)(s+\lambda_2)}(s+\lambda_1)\right]_{s=-\lambda_1} = \frac{1}{-\lambda_1+\lambda_2}$$

$$A_2 = \left[\frac{1}{(s+\lambda_1)(s+\lambda_2)}(s+\lambda_2)\right]_{s=-\lambda_2} = \frac{1}{-\lambda_2+\lambda_1}$$

$$P_{s1}(s) = \frac{\lambda_1}{\lambda_2-\lambda_1}\left(\frac{1}{(s+\lambda_1)} - \frac{1}{(s+\lambda_2)}\right) \longrightarrow P_{s1}(t) = \frac{\lambda_1}{\lambda_2-\lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)$$

$$R(t) = P_{s0}(t) + P_{s1}(t)$$

Pohotovostní systémy: Pravděpodobnost bezp. činnosti

- Pokud mají jak online, tak pohotovostní prvky stejnou intenzitu poruch, pak předchozí vzorce mají tvar

$$P_{s1}(t) = \frac{\lambda_1}{\lambda_2 - \lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right) = \lambda_1 \frac{0}{0}$$

  - Standardní možností v podobných případech je nutno použít l'Hopitalova pravidlo

$$\textbf{pokud } \lim_{x \to c} f(x) = \lim_{x \to c} g(x) = 0 \textbf{ nebo } \infty \textbf{ a existuje } \lim_{x \to c} \frac{f'(x)}{g'(x)}$$

$$\textbf{pak } \lim_{x \to c} \frac{f(x)}{g(x)} = \lim_{x \to c} \frac{f'(x)}{g'(x)}$$

- Vezmeme-li derivaci čitatele a jmenovatele samostatně s ohledem na λ_2 a poté vezmeme limit $\lambda_2 \rightarrow \lambda_1$, tak výsledkem je

$$P_{s1}(t) = \lambda t e^{-\lambda t} \longrightarrow R(t) = e^{-\lambda t} + \lambda\, e^{-\lambda t}$$

Pohotovostní systémy: Pravděpodobnost bezp. činnosti

- Spolehlivost pohotovostního systému se dvěma stejnými on-line a pohotovostními komponentami

$$R(t) = e^{-\lambda t} + \lambda\, e^{-\lambda t}$$

  - Toto řešení lze pozorovat jako první dva členy v Poissonově rozdělení
  - Pravděpodobnost poruchy je rovna $q = \lambda t$
  - Počet událostí typu zapnutí zálohy je $\mu = nq$, ale protože start zálohy nezačíná před vznikem závady na primárním prvku, pak časy výskytu obou událostí (poruchy a přepnutí) představují posloupnost v čase (jeden po druhém) → μ = 1q = q

Pohotovostní systémy: Pravděpodobnost bezp. činnosti

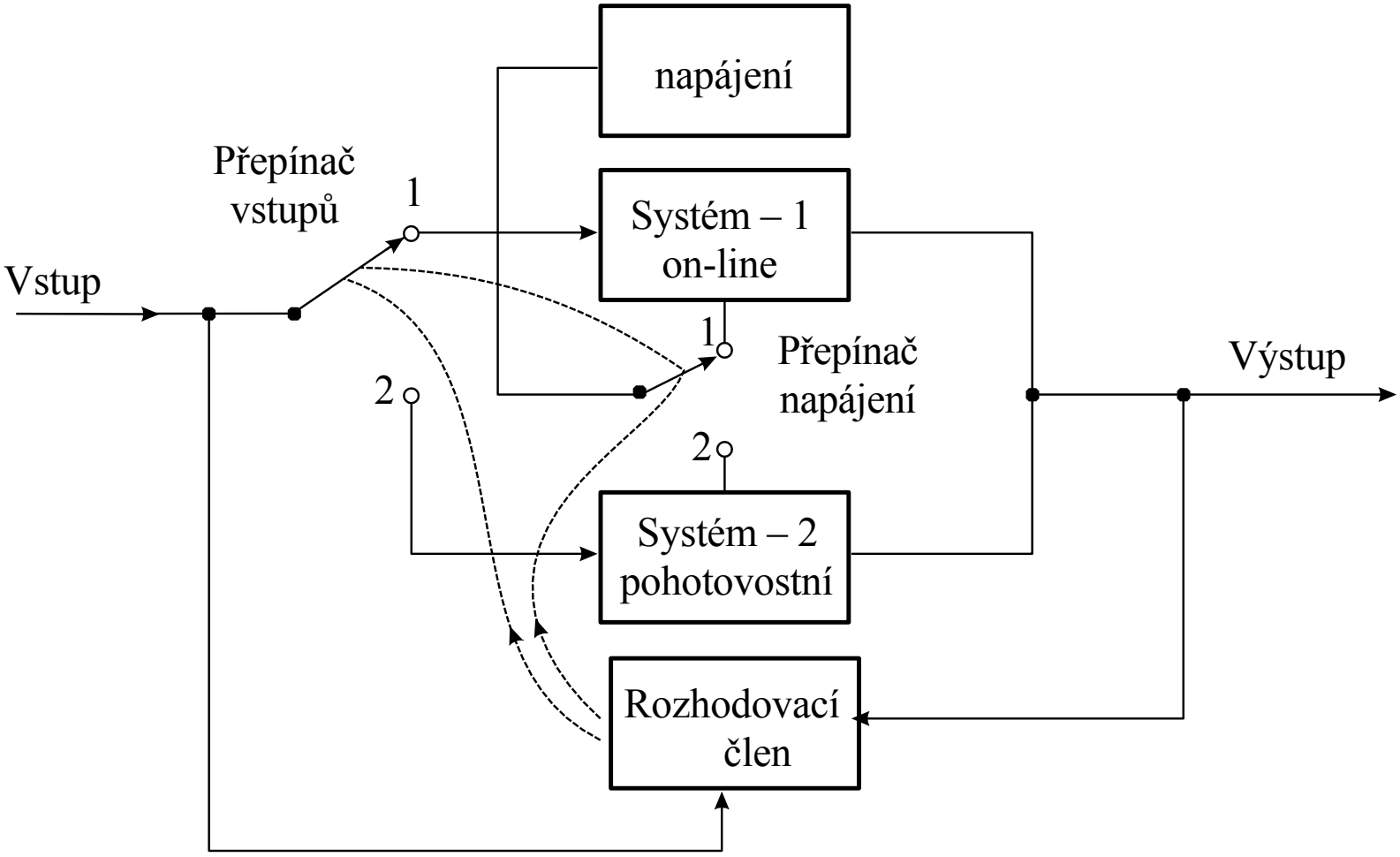
- Pokud se model z obr. 1 lze rozšíří o velké množství prvků a stavů, tak i pro tento případ Poissonovo rozdělení poskytuje řešení
- Pro *n* identických pohotovostních prvků je systém funkční, pokud dojde maximálně k *n-1* poruchám
  - Poissonovo rozdělení

$$R(t) = e^{-\lambda t} \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!}$$

Porovnání paralelního a pohotovostního systému

- Pohotovostní systémy jsou výhodnější než systémy paralelní
  - Funkčnost a výhodnost závisí na spolehlivosti pohotovostního přepínače
  - Ve srovnání je také třeba vzít v úvahu spolehlivost vazebního členu v paralelním systému
- Přepnutí do pohotovostního systému musí vykonávat tři funkce
  1) Musí mít nějaký rozhodovací prvek nebo algoritmus, který je schopen detekovat nesprávnou činnost
  2) Přepínač poté musí přepnout výstup z on-line prvku na pohotovostní prvek a případně přepnout vstupy
  3) Přepnout napájení z on-line do pohotovostního prvku

Porovnání paralelního a pohotovostního systému



Obrázek 2: Pohotovostní systém, ve kterém je zobrazeno přepínání vstupu a napájení.

Porovnání paralelního a pohotovostního systému

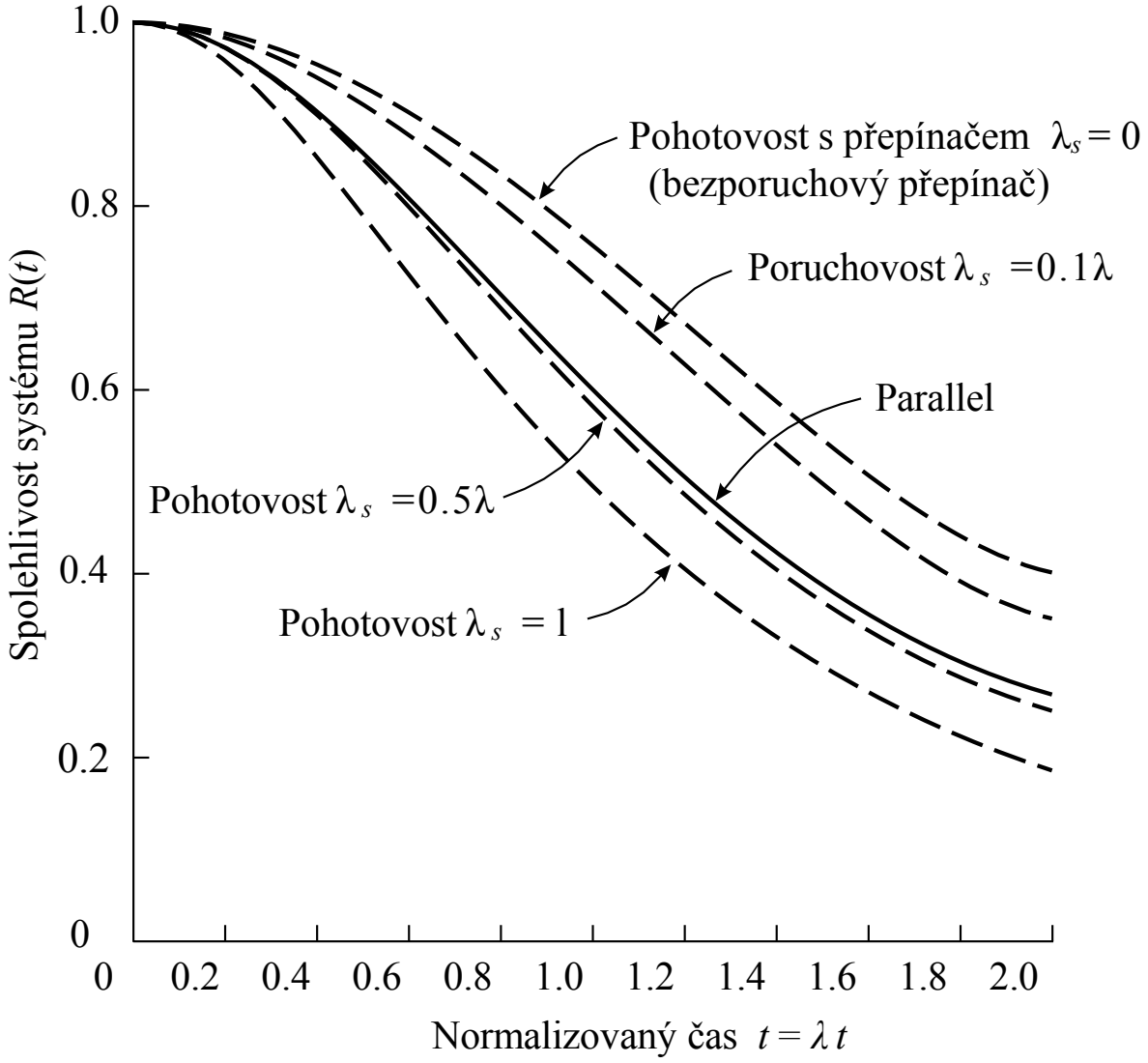
- Pokud přepínače nejsou bezporuchové
  - Za předpokladu:
    - Jakákoli porucha přepínače je poruchou systému
    - Poruchy spínače jsou nezávislé na poruše online a pohotovostního systému
    - Přepínače mají konstantní poruchovost λ_s
  - poté pro oba identické online a pohotovostní systémy platí:

$$R(t) = e^{-\lambda_s t}(e^{-\lambda t} + \lambda t e^{-\lambda t})$$

- Spolehlivost běžného paralelního systém (viz obr. 3)

$$R(t) = 1 - (1 - e^{-\lambda t})^2$$

Porovnání paralelního a pohotovostního systému



Obrázek 3: Porovnání paralelního systému a pohotovostního systému s poruchovým přepínačem

Porovnání paralelního a pohotovostního systému

- Jednoduchý způsob, jak vylepšit model spolehlivosti přepínače, je předpokládat, že přepínač selže pouze při přepnutí z on-line do pohotovostního režimu, po selhání on-line prvku
  - Když je on-line prvek bezchybný, nemůže se porucha přepínače projevit,
  - V takovém případě je pravděpodobnost bezporuchové činnosti přepínače součtem pravděpodobnosti jeho správné funkce a pravděpodobnost jedné poruchy a bezchybnost přepínače je také jeho správná funkce
  - Spolehlivost přepínače v následující rovnici představuje pouze druhý člen

$$R(t) = e^{-\lambda t} + \lambda t e^{-\lambda t} \rightarrow R(t) = e^{-\lambda t} + \lambda t e^{-\lambda t} e^{-\lambda_s t}$$

  - Toto je realističtější model přepínače než ten předchozí

Opravitelné systémy: Úvod

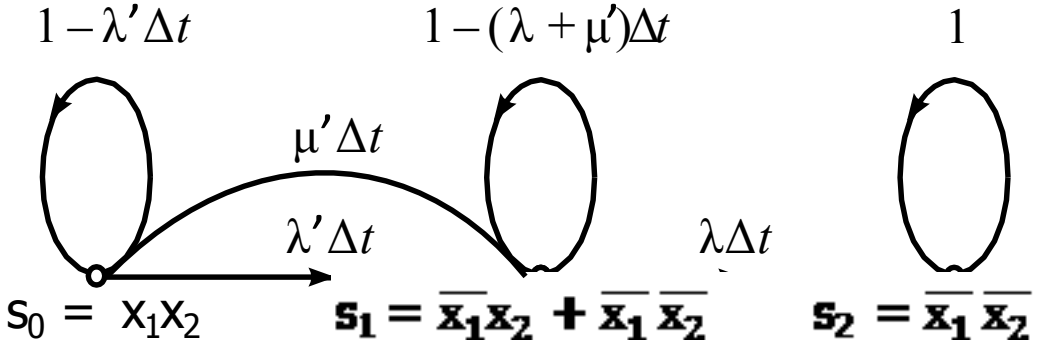
- Na opravu a výměnu lze pohlížet jako na stejný proces
  - Výměna vadné součásti za náhradní je jen rychlá oprava

- Proces opravy
  1) Detekce, že došlo k selhání
  2) Diagnostika nebo lokalizace příčiny selhání
  3) Zpoždění výměny nebo opravy (včetně logistického zpoždění)
  4) Test a kalibrace systému

- Oprava obecně zlepšuje spolehlivost a dostupnost
  - V případě jediného prvku oprava neovlivní spolehlivost, ale zlepší dostupnost
  - V případě redundance, oprava zlepší spolehlivost i dostupnost
    - Spolehlivost se zlepší, pokud lze selhávající prvek opravit a obnovit před selháním zbývajícího prvku

Opravitelné systémy: Spolehlivost dvou prvků

- Oprava vylepšuje paralelní i pohotovostní systém
- Markovův model pro dvouprvkový paralelní nebo pohotovostní systém s opravou je uveden na obr.4
  - V případě běžného paralelního systému
    - Pravděpodobnost přechodu ze stavu s_0 do s_1 je 2λ, protože každý prvek může selhat
  - V případě pohotovostního systému
    - Pravděpodobnost přechodu ze stavu s_0 do s_1 je λ, může selhat jen jeden prvek
  - Pokud je možno opravovat více prvků zároveň (více spolupracujících opravářů), je intenzita opravy > μ (μ je intenzita opravy pro jeden prvek)



$\lambda' = 2\lambda$	pro paralelní systém
$\lambda' = \lambda$	pro pohotovostní systém
$\mu' = \mu$	s možností jedné opravy
$\mu' = k\mu$	s možností k oprav paralelně

Figure 4: Markovův model spolehlivosti pro dva identické paralelní prvky s možností k paralelních oprav

Opravitelné systémy: Spolehlivost dvou prvků

- Z obr. 4 vyplývá:

$$\frac{dP_{s_0}t}{dt} = -\lambda' P_{s_0}(t) + \mu' P_{s_1}(t)$$

$$\frac{dP_{s_1}t}{dt} = \lambda' + P_{s_0}(t) - (\lambda + \mu') P_{s_1}(t)$$

$$\frac{dP_{s_2}t}{dt} = \lambda P_{s_1}(t)$$

- Za předpokladu, že oba systémy jsou zpočátku funkční:

$$P_{s_0}(0) = 1 \quad P_{s_1}(0) = P_{s_2}(0) = 0$$

$$\frac{df(t)}{dt} \longleftrightarrow sF(s) - f(0)$$

$$sP_{s_0}(s) - 1 = -\lambda' P_{s_0}(s) + \mu' P_{s_1}(s)$$

$$sP_{s_1}(s) - 0 = \lambda' P_{s_0}(s) - (\lambda + \mu') P_{s_1}(s)$$

$$sP_{s_2}(s) - 0 = \lambda P_{s_1}(s)$$

Opravitelné systémy: Spolehlivost dvou prvků

- Pokračování předešlého výpočtu:

$$P_{s_0}(s) = \frac{(s + \lambda + \mu')}{[s^2 + (\lambda + \lambda' + \mu')s + \lambda\lambda']}$$

$$P_{s_1}(s) = \frac{\lambda'}{[s^2 + (\lambda + \lambda' + \mu')s + \lambda\lambda']}$$

$$P_{s_2}(s) = \frac{\lambda\lambda'}{s[s^2 + (\lambda + \lambda' + \mu')s + \lambda\lambda']}$$

- Dalším krokem je expanze částečných zlomků (pro tento tvar rovnic je obtížné)
- Nakonec je transformujte z frekvenční domény do časové domény

$$e^{-at} \xleftrightarrow[\text{transformation}]{\text{Laplace}} \frac{1}{s + a}$$

- Zjednodušení výpočtu přináší výpočet MTTF

Opravitelné systémy: MTTF

- Snadnější porovnání vlastností několika systémů je porovnání jejich MTTF (není třeba vyčíslovat pravděpodobnost bezporuchové činnosti):

$$MTTF = \lim_{s \to \infty} R^*(s)$$

- Z obr. 4 vyplývá:

$$R(t) = P_{s_0}(t) + P_{s_1}(t) \longrightarrow MTTF = \lim_{s \to \infty} R^*(s) = \lim_{s \to \infty} (P_{s_0}(s) + P_{s_1}(s))$$

$$MTTF = \frac{\lambda + \lambda' + \mu'}{(\lambda\lambda')}$$

Opravitelné systémy: MTTF

- Výsledky substituce různých hodnot intenzit poruch λ' uvedených na obr. 4 ve vyjádření v MTTF pro jednu opravu s $\mu' = \mu$ (v daném čase lze provádět pouze jednu opravu) jsou uvedeny v Tab. 3
  - Oprava silně zvyšuje MTTF

Tabulka 3: Porovnání MTTF pro několik systémů

Typ prvku	vzorec	Pro $\lambda = 1$, $\mu = 10$
Jednoduchý prvek	$1/\lambda$	1.0
Dva paralelní prvky – bez opravy	$1{,}5/\lambda$	1.5
Dva zálohované prvky – bez opravy	$2/\lambda$	2.0
Dva paralelní prvky – s opravou	$(3\lambda+\mu)/2\lambda^2$	6.5
Dva zálohované prvky – s opravou	$(2\lambda+\mu)/\lambda^2$	12.0

Reference

Martin L. Shooman, *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, Wiley-Interscience, 2001.