Reliability of Digital Systems

Redundancy, Spares, and Repairs (1)

Václav Přenosil

Design and Architecture of Digital Systems Laboratory

prenosil@fi.muni.cz

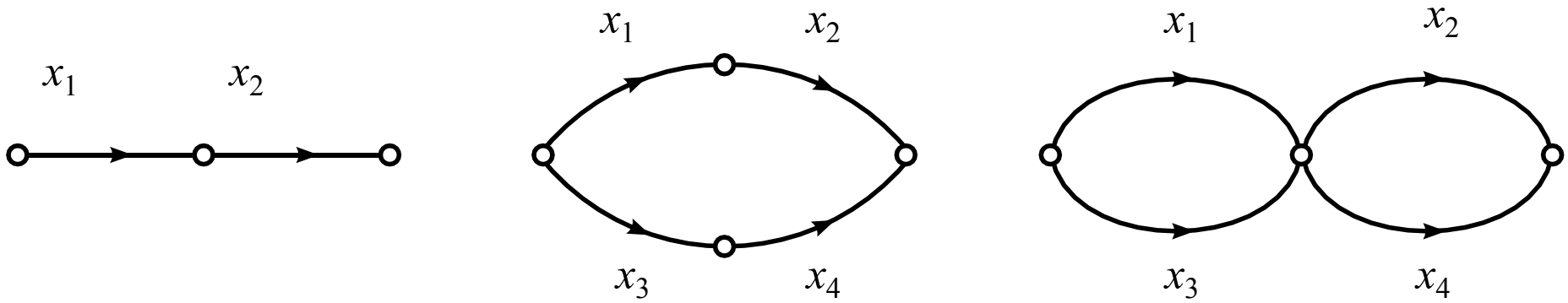
Fall, 2020

Úvod

- Nástrojem pro zvýšení spolehlivosti a dostupnosti systému při limitované spolehlivosti prvků systému je redundance.
  - Redundance znamená poskytnout spolehlivostnímu modelu systému alternativní cesty, které umožní systému pokračovat v provozu, i když některé komponenty selžou,
- Alternativní cesty spolehlivostním modelem lze realizovat paralelní instalací prvků nebo systémů, což lze zajistit několika postupy:
  - **paralelní redundancí** v **pohotovostním režimu** (*hot standby*) – všechny redundantní prvky jsou nepřetržitě napájeny a provozovány
  - **pohotovostní redundancí** (*cold redundancy*) – je napájen jenom funkční zálohovaný prvek (pracuje on-line). Zálohovací prvky nejsou napájeny a do provozu jsou zapínány automaticky nebo ručně v okamžiku selhání zálohovaného prvku
- Jednou z metod pohotovostní redundance je použití náhradních dílů nebo oprav k obnovení systému

Redundance prvků systému

- Předpokládejme tři spolehlivostní modely systému, viz níže



Obrázek 1: Porovnání tří různých systémů: (a) nezálohovaný systém, (b) celková redundance systému, (c) redundance na úrovni prvků systému.

- Pro nezálohovaný systém (a)

$$R_a(p) = P(x_1)P(x_2) = p^2$$

kde oba prvky x_1 a x_2 jsou nezávislé a totožné

$$P(x_1) = P(x_2) = p$$

Redundance prvků systému

- Pro model (b) platí

$$R_b(p) = P(x_1x_2 + x_3x_4)$$

Pokud jsou systémy nezávislé a identické (*independent identical units - IIU*) se spolehlivostí *p,* pak platí:

$$R_b(t) = 2R_a - R_a^2 = p^2(2 - p^2)$$

- Pro model (c) platí

$$R_c(p) = P(x_1 + x_3)P(x_2 + x_4)$$

Za předpokladu *IIU*

$$R_c(p) = p^2(2 - p)^2$$

- Pokud porovnáme spolehlivosti modelu (b) a (c) tak získáme vztah

$$\frac{R_c(p)}{R_b(p)} = \frac{p^2(2-p)^2}{p^2(2-p^2)} = \frac{(2-p)^2}{(2-p^2)} = \frac{4-4p+p^2}{(2-p^2)} = \frac{(2-p^2)+2(1-p)^2}{(2-p^2)}$$
$$= 1 + \frac{2(1-p)^2}{(2-p^2)} \qquad (1)$$

Redundance prvků systému

- V rovnici 1)

$$0 < p < 1 \rightarrow 2 - p^2 > 0 \rightarrow R_c(p)/R_b(p) \geq 1$$

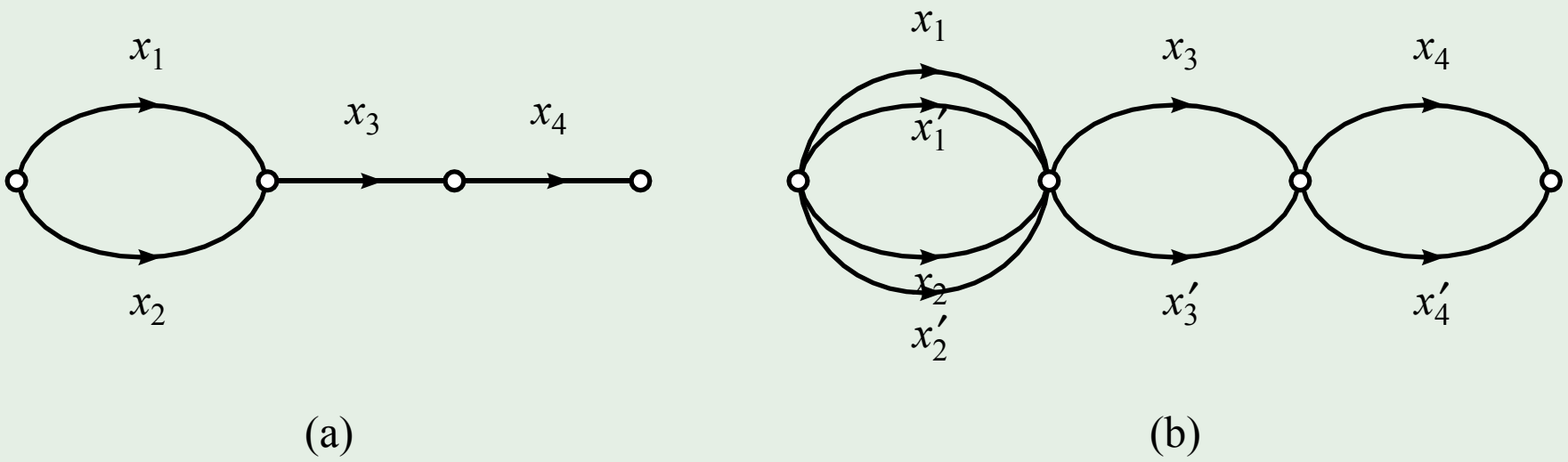
  - Redundance prvků je lepší než celková redundance systému
- Rozšíření podle obrázku 1 pro:
  a) sériový model *n*-prvků
  b) model celkové redundance – dva paralelní systémy s *n* prvky
  c) sériový model *n* po dvou paralelních prvcích

$$\frac{R_c(p)}{R_b(p)} \approx \frac{(1-p)^n}{(2-p^n)}$$

- Jednodušším důkazem výše uvedeného vztahu je hledat sady cest
  - Na obr. 1(b) sadu cest reprezentují cesty x_1x_2 and x_3x_4
  - Na obr. 1(c) sada cest obsahuje cesty x_1x_2, x_3x_4, x_1x_4 a x_3x_2
  - Spolehlivost systému je dána součtem pravděpodobností sad cest, systém na obr. 1 (c) má jednak stejné dvě sady cest jako obr. 1 (b), ale navíc má další dvě další cesty, proto redundance prvků vykazuje vyšší spolehlivost než celková redundance
- Vyšší spolehlivost redundance prvků než celková redundance platí také pro prvky, které nejsou identické.

Redundance prvků systému

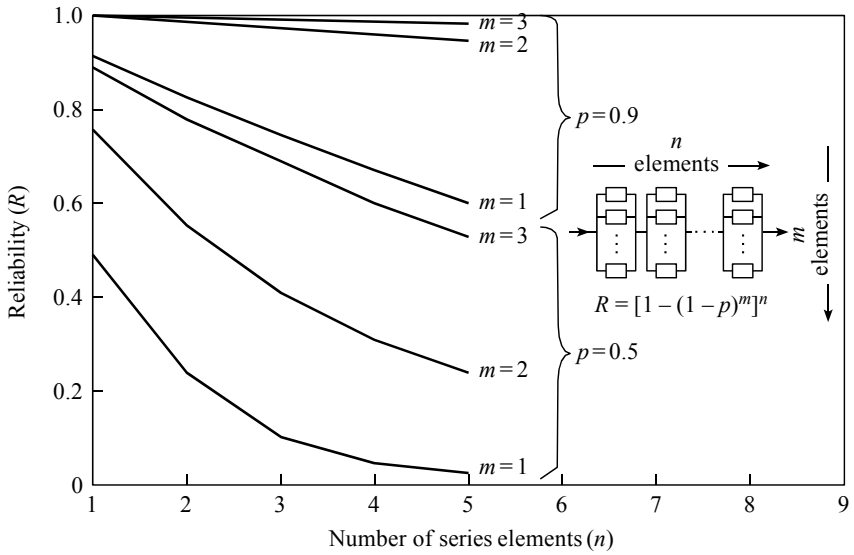
Příklad



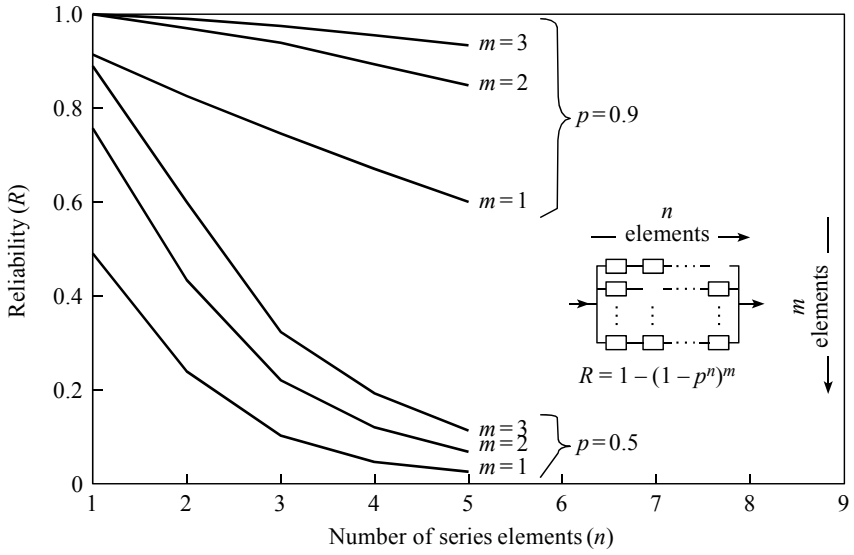
Obrázek 2: Redundance prvků: (a) originální systém (b) redundantní systém.

- Redundance prvků systému (a) je zobrazena v části (b) obr. 2
  - Redundance prvků vykazuje vyšší spolehlivost než celková redundance systému

Redundance prvků systému



(a)



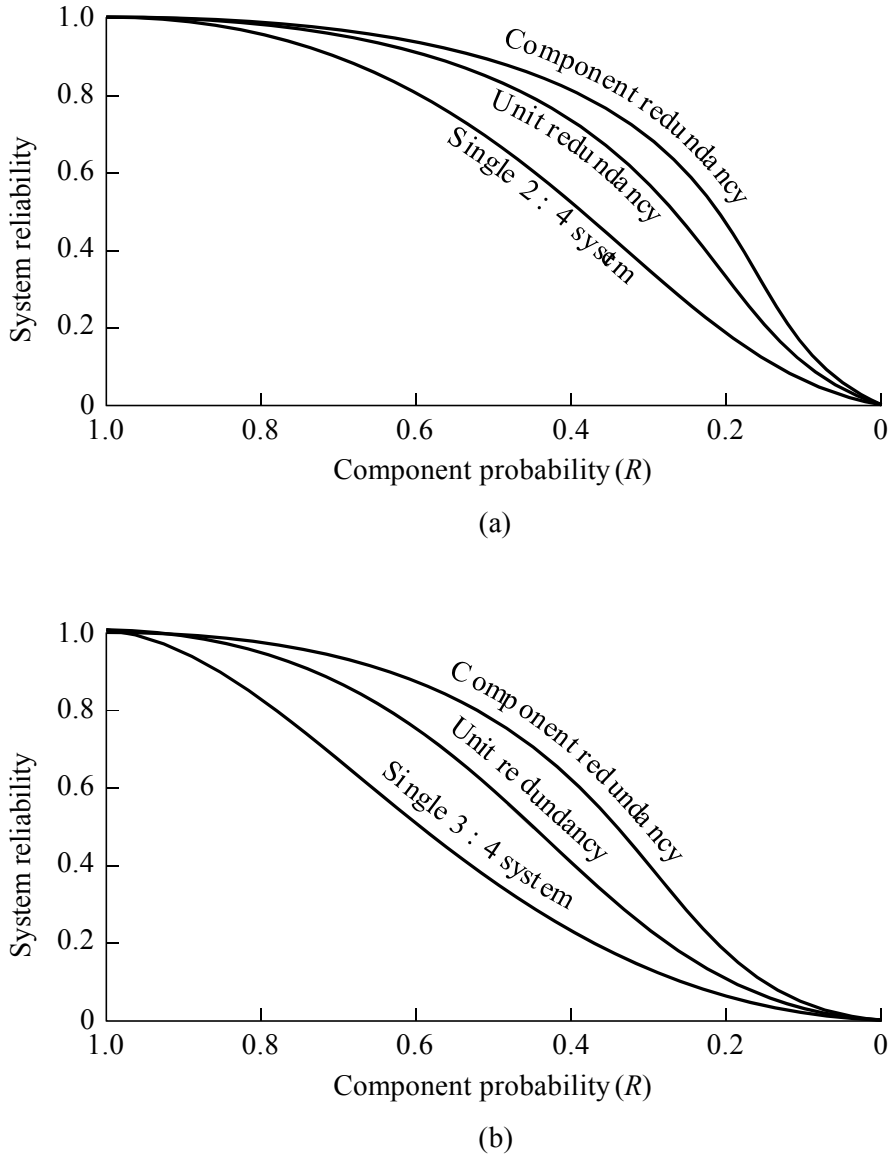
(b)

Obrázek 3: Porovnání: (a) redundance prvků(b) celková redundance.

Redundance prvků systému

- Porovnání redundance prvků a celkové redundance v systému *r* z *n*
  - Pro $r = n$ je se jedná o sériový spolehlivostní model a platí předchozí výsledek
  - Pro $r = 1$ se struktura redukuje na n paralelních prvků a redundance komponent a celková redundance jsou identické
  - U $2 \leq r < n$ je redundance komponent opět lepší
    - To lze doložit součtem spolehlivosti všech možných sad cest

Redundance prvků systému



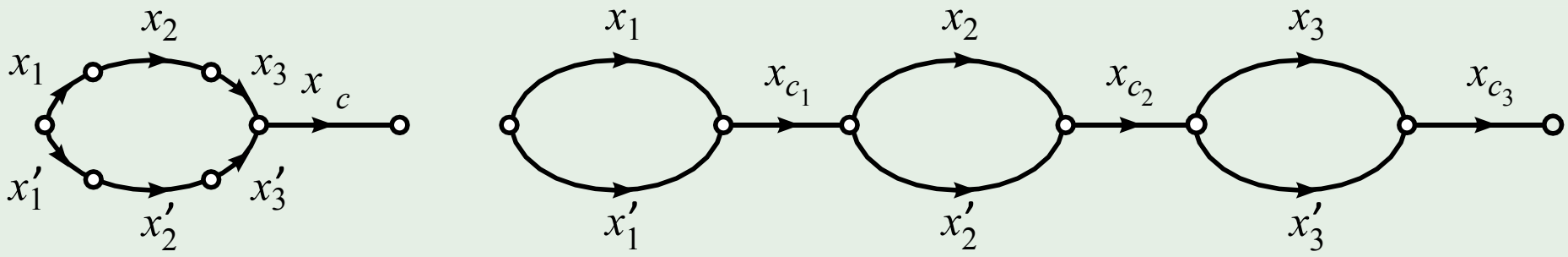
Obrázek 4: Porovnání redundance prvků a celkové redundance spolehlivostního systému *r* z *n*: (a) 2 z 4 systém a (b) 3 z 4 systém.

Redundance prvků systému

- Redundanci lze realizovat přidáním dalších pomocných obvodů
  - Takové obvody nebo součásti se nazývají vazební členy nebo přepínače
  - Přepínače rekonfigurují systém (propojují různé paralelní prvky systému) po zjištěné chybě
  - Přepínače komplikují spolehlivostní analýzu redundantního systému
  - V některých případech mohou přepínače zhoršovat spolehlivost redundantní konfigurace

Redundance prvků systému

Example



(a) Celková redundance (jeden přepínač)

(b) Redundance prvků (tři přepínače)

Obrázek 5: Systém s celkovou redundancí (a) a systém redundancí prvků včetně přepínačů.

- Pro variantu (a) platí:

$$R_a = P(x_1 x_2 x_3 + x_1' x_2' x_3')P(x_c)$$

Pokud systém tvoří IIU a spolehlivost přepínače vztahem $P(x_c) = K * p$

$$R_a = (2p^3 - p^6)Kp$$

Redundance prvků systému

Příklad (pokračování)

- Pro model (b)

$$R_b = P(x_1 + x_1')P(x_2 + x_2')P(x_3 + x_3')P(x_{c_1})P(x_{c_2})P(x_{c_3})$$

Pokud systém tvoří IIU se spolehlivostí $P(x_{c_1}) = P(x_{c_2}) = P(x_{c_3}) = Kp$

$$R_b = (2p - p^2)^3(Kp)^3$$

- Pro porovnání vlivu spolehlivosti přepínače Kp, položme $R_a = R_b$

$$(2p^3 - p^6)Kp = (2p - p^2)^3K^3p^3 \rightarrow K^2 = \frac{(2p^3 - p^6)}{(2p - p^2)^3p^2}$$

Pokud $p = 0{,}9$ a $K = 1{,}085778501 \rightarrow P(x_c) = Kp = 0{,}9772006509$
tj. pokud $P_f(x_i) = 1 - p = 0{,}1 \rightarrow R_a = R_b$ *pak* $P_f(x_c) = 0{,}0228$

- Jestliže pravděpodobnost poruchy přepínače bude menší než 22.8% ($\frac{0{,}0228}{0{,}1} \times 100$) pravděpodobnosti poruchy prvku, pak spolehlivost systému s redundancí prvků bude lepší

Přibližné funkce spolehlivosti

- Většina výrazů spolehlivosti systému se zjednodušuje na součty a rozdíly různých exponenciálních funkcí
  - Může být obtížné tyto funkce interpretovat
  - Často je výhodné mít techniky, které poskytují přibližné analytické výrazy

Přibližné spolehlivostní funkce: Exponenciální rozvoj

- Ve spolehlivostních výpočtech se často pracuje s exponenciální funkcí ve tvaru e^{-Z}
  - Maclaurinův rozvoj funkce e^{-Z} v okolí Z = 0

$$e^{Z} = 1 - Z + \frac{Z^2}{2!} - \frac{Z^3}{3!} + \cdots + \frac{(-Z)^n}{n!} + \cdots$$

$$e^{-Z} = 1 - Z + \frac{Z^2}{2!} - \frac{Z^3}{3!} + \cdots + \frac{(-Z)^n}{n!} + R_n(Z)$$

kde

$$R_n(Z) = (-1)^{n+1} \int_0^Z \frac{(Z-\xi)^n}{n!} e^{-\xi} d\xi$$

  - Můžeme aproximovat e^{-Z} pomocí n členů řady a funkci $R_n(Z)$ použít k aproximaci zbytku
  - Často se používají pouze dva nebo tři členy rozvoje
    - V případě vysoce spolehlivých systémů je hodnota funkce $e^{-Z} \sim 1$, z čehož plyne že exponent Z je malý, a tudíž jeho vyšší mocniny Z^n u členů rozvoje jsou postupně o několik dekadických řádů rozvoje menší a lze je bez újmy na přesnosti zanedbat

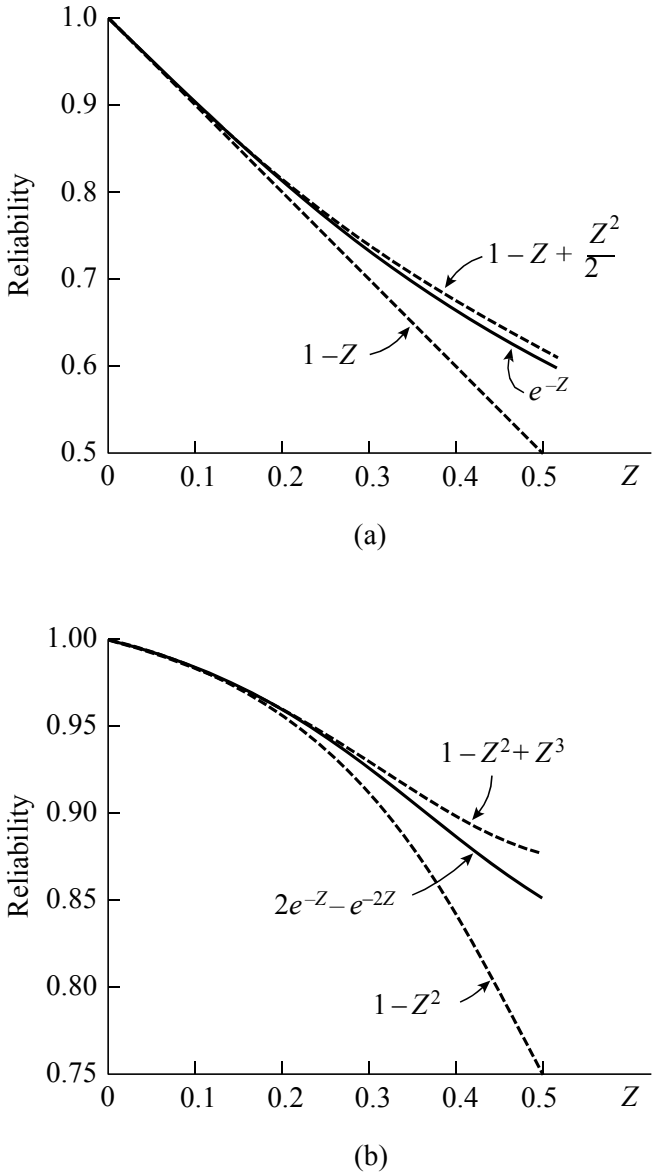
Přibližné spolehlivostní funkce: Exponenciální rozvoj

Příklad

- Spolehlivost dvou paralelních prvků je dána vztahem

$$
\begin{aligned}
(2e^{-Z}) + (-e^{-2Z}) &= \left(2 - 2Z + \frac{2Z^2}{2!} - \frac{2Z^3}{3!} + \cdots + \frac{2(-Z)^n}{n!} + \cdots\right) \\
&\quad + \left(-1 + 2Z - \frac{(2Z)^2}{2!} + \frac{(2Z)^3}{3!} - \cdots - \frac{(2Z)^n}{n!} + \cdots\right) \\
&= 1 - Z^2 + Z^3 - \frac{7}{12}Z^4 + \frac{1}{4}Z^5 - \cdots
\end{aligned}
$$

Přibližné spolehlivostní funkce: Exponenciální rozvoj



Obrázek 6: Porovnání přesných a přibližných spolehlivostních funkcí: (a) modely jednoho prvku a (b) modely dvou paralelních prvků

Přibližné spolehlivostní funkce: Míra intenzity poruch

Příklad

- Spolehlivostní model systému tvoří dva sériově zapojené prvky x_2x_3 a paralelně zapojený prvek x_1
  - Jestliže všechny prvky mají stejnou konstantní intenzitu λ, pak platí

$$R(t) = P(x_1 + x_2x_3) = e^{-\lambda t} + e^{-2\lambda t} - e^{-3\lambda t}$$

$$z(t) = \frac{f(t)}{R(t)} = -\frac{\acute{R}(t)}{R(t)} = \frac{\lambda(1 + 2e^{-\lambda t} - 3e^{-2\lambda t})}{1 + e^{-\lambda t} - e^{-2\lambda t}}$$

- Úprava funkce $z(t)$ pomocí Taylorova rozvoje:

$$z(t) = 1 + \lambda t - 3\lambda^2 t^2/2 + \cdots$$

Přibližné spolehlivostní funkce: MTTF

- Číselná charakteristika MTTF obsahuje méně podrobné informace o systému než výrazy spolehlivosti, a proto se s ním lépe pracuje

$$MTTF = \int_0^\infty R(t)dt$$

- Pro sériový model spolehlivosti systému s n prvky z nichž každý míru poruchy $z_i(t)$ a pravděpodobnost poruchy $Z(t) = \int z(t)dy$

$$R(t) = exp\left[-\sum_{i=1}^{n} Z_i(t)\right]$$

$$MTTF = \int_0^\infty \left\{exp\left[-\sum_{i=1}^{n} Z_i(t)\right]\right\} dt$$

Přibližné spolehlivostní funkce: MTTF

- Pro spolehlivostní model dvou paralelních prvků

$$R(t) = e^{-Z_1(t)} + e^{-Z_2(t)} - e^{-[Z_1(t)+Z_2(t)]}$$

Pokud oba prvky mají konstantní intenzitu poruch

$$MFFT = \int_0^\infty R(t)dt = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

- Zobecněno pro model s *n* paralelně spojených prvků s konstantní intenzitou poruch

$$MFFT = \left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \cdots + \frac{1}{\lambda_n}\right) - \left(\frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \cdots + \frac{1}{\lambda_i + \lambda_j}\right) + \left(\frac{1}{\lambda_1 + \lambda_2 + \lambda_3} + \frac{1}{\lambda_1 + \lambda_2 + \lambda_4} + \cdots + \frac{1}{\lambda_i + \lambda_j + \lambda_k}\right) - \ldots + (-1)^{n+1}\frac{1}{\sum_{i=1}^{n} \lambda_i}$$

Přibližné spolehlivostní funkce: MTTF

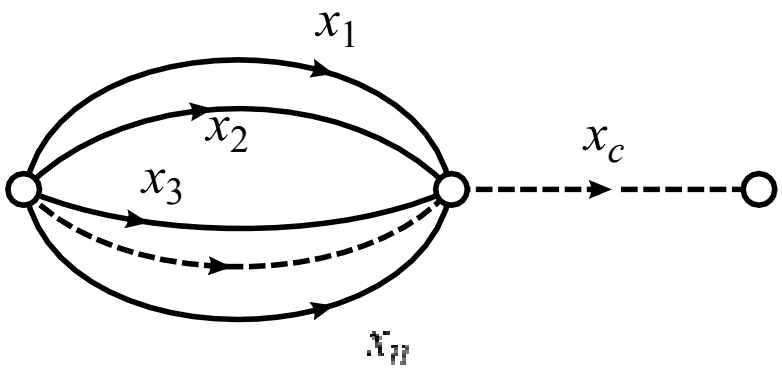
- Pokud všechny prvky mají stejnou intenzitu poruch $\lambda_1 = \lambda_2 = \cdots = \lambda_n = \lambda$

$$MTTF = \frac{1}{\lambda}\left[\frac{\binom{n}{1}}{1} - \frac{\binom{n}{2}}{2} + \frac{\binom{n}{3}}{3} - \cdots + (-1)^{n+1}\frac{\binom{n}{n}}{n}\right] = \frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i}$$

- Toto je harmonická řada
- Rozvojem pomocí Eulerovy řady dostaneme:

$$\frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i} = \frac{1}{\lambda}\left[0{,}577 + \ln(n) + \frac{1}{2n} - \frac{1}{12n(n+1)} + \cdots\right]$$

Model paralelní redundance: Nezávislé poruchy



Obrázek 7: Model spolehlivostního systémy s n prvky a spínačem x_c

- Pokud neuvažujeme spínač, pak

$$R(t) = P(x_1 + x_2 + \ldots + x_n) = 1 - P(\overline{x_1}\,\overline{x_2}\ldots\overline{x_n})$$

- In case of constant-hazard components

$$P_f = P(\overline{x_i}) = 1 - e^{-\lambda_i t} \longrightarrow R(t) = 1 - \left[\prod_{i=1}^{n}\left(1 - e^{-\lambda_i t}\right)\right]$$

Model paralelní redundance: Nezávislé poruchy

- Pro lineárně rostoucí intenzitu poruch

$$R(t) = 1 - \left[\prod_{i=1}^{n}\left(1 - e^{-K_i t^2/2}\right)\right]$$

- Pokud uvažujeme i spínač

$$R(t) = \left\{1 - \left[\prod_{i=1}^{n}\left(1 - e^{-\frac{K_i t^2}{2}}\right)\right]\right\} P(x_c)$$

Pro IIU s konstantní intenzitou poruch

$$R(t) = [1 - (1 - e^{-\lambda t})^n]\, e^{-\lambda_c t}$$

Pokud je $\lambda_c t < \lambda t \ll 1$ (Maclaurin rozvoj dává $e^{-Z} \approx 1 - Z$ v okolí $Z = 0$):
$(1 - e^{-\lambda t}) \approx \lambda t$ a $e^{-\lambda_c t} \approx 1 - \lambda_c t \rightarrow R(t) \approx [1 - (\lambda t)^n](1 - \lambda_c t)$

Zanedbáním posledního členu dostaneme

$$R(t) \approx 1 - \lambda_c t - (\lambda t)^n$$

Model paralelní redundance: Nezávislé poruchy

- V rovnici

$$R(t) \approx 1 - \lambda_c t - (\lambda t)^n$$

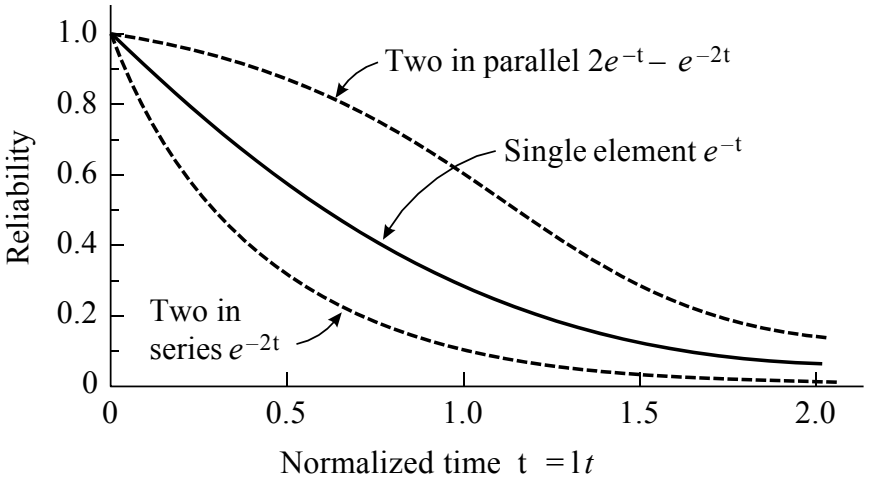
intenzita poruch spínače musí být malá, jinak se stane dominantní částí pravděpodobnosti poruchy

- Horní limit pro intenzitu spínače λ_c

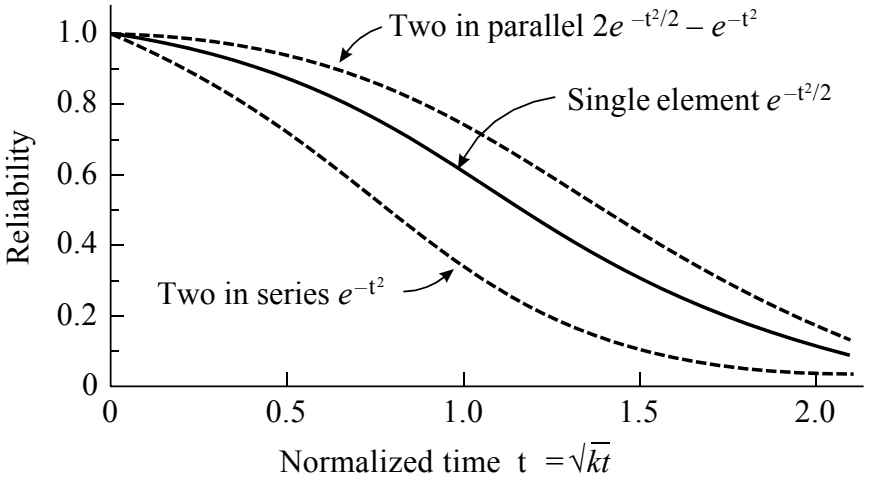
$$\lambda_c t < (\lambda t)^n \longrightarrow \frac{\lambda_c}{\lambda} < (\lambda t)^{n-1}$$

- Pokud $n = 3$ a $\lambda t = 0.1 \rightarrow \lambda_c < 0{,}01\lambda$
  Pokud $\lambda_c = 0{,}01\lambda$, pravděpodobnost poruchy spojovacího systému se rovná pravděpodobnosti poruchy paralelního systému
- Toto je limitující faktor pro realizace paralelních modelů spolehlivosti

Model paralelní redundance: Nezávislé poruchy



(a)



(b)

Obrázek 8: Porovnání funkcí spolehlivosti prvků: (a) s konstantní intenzitou poruch, (b) s lineárně rostoucí intenzitou poruch.

Paralelní redundance: Závislé a společné efekty

- Režim společné poruchy ovlivní funkci všech prvků v paralelním modelu
  - Příkladem může být porucha spínače

Příklad (vliv závislých poruch)

- Pro zvýšení spolehlivosti komunikace se používají dva satelitní kanály. Pravděpodobnost poruchy kanálu $Z = 0{,}01 \rightarrow R = 0{,}99$
- Spolehlivost dvou paralelních kanálů c_1 a c_2

$$R = P(c_1 + c_2) = 1 - P(\overline{c_1}\,\overline{c_2}) = 1 - P(\overline{c_1})P(\overline{c_2}|\overline{c_1})$$

- Pokud jsou poruchy kanálů c_1 a c_2 nezávislé, pak

$$R = 1 - 0{,}01 * 0{,}01 = 0{,}9999$$

- Předpokládejme, že čtvrtina poruch satelitního přenosu je vlivem atmosférického rušení, které ovlivňuje oba kanály

$$P(\overline{c_2}|\overline{c_1}) = 0{,}25 \longrightarrow R = 1 - P(\overline{c_1})P(\overline{c_2}|\overline{c_1}) = 1 - 0{,}01 * 0{,}25 = 0{,}9975$$

- Závislost způsobila zvýšení pravděpodobnosti poruchy přenosu z hodnoty 0,0001 na 0,0025

Spolehlivostní model *r*-z-*n*

- Struktura *r*-z-*n* představuje systém *n* prvků, ve kterém musí pracovat *r* prvků, aby systém mohl pracovat
- Pokud se prvky liší nebo jsou závislé, musí se použít přístup strukturálního modelu
- Pokud je *n* prvků nezávislých a identických, pak platí

$$B(r:n) = \binom{n}{r} p^r (1-p)^{n-r}$$

$$P_s = \sum_{k=r}^{n} B(k:n)$$

- Pro prvky s konstantní intenzitou poruch předchozí rovnice má tvar

$$R(t) = \sum_{k=r}^{n} \binom{n}{r} e^{-k\lambda t} \left(1 - e^{-\lambda t}\right)^{n-k}$$

Spolehlivostní model *r*-z-*n*

- Pro prvky s lineárně rostoucí intenzitou poruch

$$R(t) = \sum_{k=r}^{n} \binom{n}{r} e^{-kKt^2/2} \left(1 - e^{-Kt^2/2}\right)^{n-k}$$

- Pro prvky s intenzitou poruch podle Weibullova rozdělení

$$R(t) = \sum_{k=r}^{n} \binom{n}{r} e^{-kKt^{m+1}/(m+1)} \left(1 - e^{-Kt^{m+1}/(m+1)}\right)^{n-k}$$

Spolehlivostní model *r*-z-*n*

- Poissonovo rozdělení
  - Pokud je *p* velmi malé a *n* je velmi velké, binomická hustota nabývá speciální omezující formy, což je Poissonův zákon pravděpodobnosti
  - V binomické distribuci

$$B(r;n,p) = \binom{n}{r} p^r (1-p)^{n-r}$$

nejpravděpodobnější počet výskytů $np = \mu \rightarrow p = \frac{\mu}{n}$

  - Limitní tvar je nazýván Poissonova distribuce

$$\lim_{n\to\infty} B\left(r;n,\frac{\mu}{n}\right) = \lim_{n\to\infty} \underbrace{\frac{n!}{r!\,(n-r)!}}_{1} \underbrace{\left(\frac{\mu}{n}\right)^r}_{\mu^r/r!} \underbrace{\left(1-\frac{\mu}{n}\right)^n}_{\exp(-\mu)} \underbrace{\left(1-\frac{\mu}{n}\right)^{-r}}_{1}$$

$$f(r;\mu) = \frac{\mu^r e^{-\mu}}{r!}$$

Spolehlivostní model *r*-z-*n*

- Binomické rozdělení můžeme aproximovat Poissonovým nebo normálním rozdělením, v závislosti na hodnotách *n* a *p*
  - Lze také vyvinout podobné aproximace pro případ, kdy *n* parametry nejsou totožné
- Poissonova aproximace pro binomické hodnoty platí pro $p \leq 0{,}05$ a $n>20$, což představuje oblast s nízkou spolehlivostí
  - V oblasti s vysokou spolehlivostí se počítá s pravděpodobností poruchy, což vyžaduje $q=1-p \leq 0{,}05$ a $n \geq 20$
- Za předpokladu odlišných prvků definujeme průměrné pravděpodobnosti spolehlivosti a poruchy $\overline{p}$ a $\overline{q}$ jako:

$$\overline{p} = \frac{1}{n}\sum_{i=1}^{n} p_i = 1 - \overline{q} = 1 - \frac{1}{n}\sum_{i=1}^{n}(1 - q_i)$$

Spolehlivostní model *r*-z-*n*

- Pro oblast s vysokou pravděpodobností spolehlivosti

$$R(t) = \sum_{k=r}^{n} \frac{(n\overline{q}\,)^k e^{-n\overline{q}}}{k!}$$

- Pro oblast s nízkou pravděpodobností spolehlivosti

$$R(t) = \sum_{k=r}^{n} \frac{(n\overline{p}\,)^k e^{-n\overline{p}}}{k!}$$

- Tyto dvě rovnice platí i pro IIU, kde $\overline{p} = p$ a $\overline{q} = q$

Spolehlivostní model *r*-z-*n*

Příklad

- Pro přenos dat je určen optický kabel s 20 kanály a systém, který pro správnou funkci potřebuje funkčních všech 20 kanálů

  P_f každého kanálu $q = 0{,}0005$ a $p = 0{,}9995$

- Pravděpodobnost správné funkce (všech 20 kanálu je funkčních)

  $$R_{20} = (0{,}9995)^{20} = 0{,}990047$$

- Při použití dvou kabelů s 20 kanály a přepínáním mezi nimi činí

  $$R_{2/20} = 2(0{,}990047) - (0{,}990047)^2 = 0{,}9999009$$

- Pokud v jednom kabelu bude vyčleněn další kanál, výsledkem bude systém *r*-z-*n*, kde $n=21$

  $$R_{21} = B(21 : 21) + B(20 : 21) = p^{21}q^0 + 21p^{20}q^1$$

  $$= (0{,}9995)^{21} + 21(0{,}9995)^{20}(0{,}0005) = 0{,}98755223 + 0{,}010395497$$

  $$= 0{,}999947831 > R_{2/20}$$

Spolehlivostní model *r*-z-*n*

Příklad (pokračování)

- Pro kontrolu hodnoty R_{21} lze použít odvozenou aproximační rovnici

$$R(t) = \sum_{k=r}^{n} \frac{(n\bar{q})^k e^{-n\bar{q}}}{k!} = (1+nq)e^{-nq} = [1+21(0{,}0005)]e^{-22*0{,}0005}$$
$$= 0{,}999831687$$

- Systém *r*-z-*n* je efektivnější, protože redundance je aplikována na nižší úrovni

References

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