Kapitola 7

Základy teorie spolehlivosti počítačových systémů

Tři základní úlohy, jimiž se teorie spolehlivosti zabývá, jsou:

- zjišťování (měření) spolehlivosti,
- předvídání (predikce) spolehlivosti,
- řízení (zlepšování) spolehlivosti.

Zde se budeme zabývat zejména druhým uvedeným bodem. Nejprve zavedeme veličiny (tzv. spolehlivostní ukazatele), které umožňují číselně kvantifikovat spolehlivost. Dále se budeme zabývat předvídáním (odhadem) hodnot spolehlivostních ukazatelů počítačového systému (ze známých hodnot spol. ukazatelů součástek) prostřednictvím matematických a simulačních spolehlivostních modelů.

7.1 Spolehlivost a její kvantifikace

7.1.1 Co je to "spolehlivost"

Chceme-li mít možnost hodnotit a srovnávat spolehlivost systémů, musíme především definovat veličiny, které budeme měřit, protože spolehlivost jako taková není sama o sobě kvantifikovatelná. V ČSN 010102* je spolehlivost charakterizována jako "obecná vlastnost objektu spočívající ve schopnosti plnit požadované funkce při zachování hodnot stanovených provozních ukazatelů v daných mezích a v čase podle stanovených technických podmínek".

Z citované definice lze vyvodit několik závěrů použitelných při studiu možností kvantitativního vyjádření spolehlivosti. Jako "komplexní vlastnost", zahrnující několik různorodých hledisek, lze spolehlivost zřejmě stěží vyjádřit jednou číselnou hodnotou, která by nám umožnila uspořádat všechny objekty podle spolehlivosti. Namísto toho zavádí norma tzv. ukazatele spolehlivosti , což jsou veličiny, které lze jednotlivě vyhodnocovat. Ty jsou pak kvantitativním vyjádřením dílčích vlastností tvořících ve svém souhrnu spolehlivost.

Při dalších úvahách budeme rozlišovat dva stavy objektu, jehož spolehlivost hodnotíme, a to *poruchový* (tj. stav, kdy porucha nastala) a *bezporuchový* (tj. stav, kdy porucha nenastala). V nejjednodušším případě systém po výskytu poruchy setrvá v poruchovém stavu až do okamžiku, kdy je porucha opravena, nebo kdy je systém vyřazen z provozu. Takovou poruchu označujeme jako stálou. V praxi se však často setkáváme s tím, že porucha zcela neočekávaně mizí a znovu se objevuje v okamžicích, které nikdo nedokáže předvídat. Takovou poruchu označujeme jako nestálou nebo občasnou.

Pro výslednou spolehlivost objektu je důležité, zda během jeho provozu provádíme obnovu bezporuchového stavu nebo ne. Podle toho budeme rozlišovat objekty *obnovované* a *neobnovované*. Obnova je přitom chápána jako vlastní přechod z poruchového do bezporuchového stavu, zatímco činnost, která k tomu vedla, se označuje jako oprava. Tyto termíny odpovídají ČSN 010102*, a proto je zde budeme používat, i když v praxi se častěji ve stejném významu používá označení opravovaný nebo neopravovaný objekt. Objekt může být neobnovovaný proto, že je neopravitelný (např. integrovaný obvod), nepřístupný (kosmické sondy, přístroje umístěné na odlehlých místech Země), nebo proto, že není opravován z organizačních důvodů (např. oprava není rentabilní).

7.1.2 Ukazatele spolehlivosti neobnovovaných objektů

Všechny důležité veličiny používané při studiu a hodnocení spolehlivosti mají náhodný charakter, a proto se při práci s nimi používá počet pravděpodobnosti. Při určování hodnot ukazatelů spolehlivosti se pak využívají metody matematické statistiky.

Náhodná veličina je charakterizována svou distribuční funkcí, čili pravděpodobností, že bude nabývat hodnoty menší než je určitá zadaná hodnota. Jestliže označíme náhodnou veličinu τ ($\tau > 0$), pak její distribuční

funkci $F(t)$ lze vyjádřit vztahem $F(t) = \mathcal{P}(\tau < t)$ kde $\mathcal{P}(A)$ je pravděpodobnost jevu A a t je nezáporné reálné číslo. Distribuční funkce $F(t)$ je neklesající a platí pro ni $0 \leq F(t) \leq 1$ pro všechna t.

V teorii spolehlivosti je základní sledovanou náhodnou veličinou τ velikost časového intervalu od uvedení do provozu do poruchy objektu. Je-li t čas měřený od uvedení do provozu, má distribuční funkce význam *pravděpodobnosti poruchy* objektu do času t a značí se $Q(t)$.

Další důležitou charakteristikou spolehlivosti je tzv. doplňková funkce, čili doplněk distribuční funkce do jedničky. V teorii spolehlivosti se značí $R(t)$ a interpretuje se jako *pravděpodobnost bezporuchového stavu* (bezporuchového provozu) objektu v čase t. Platí

$$R(t) = 1 - Q(t) \tag{7.1}$$

Je-li náhodná veličina spojitá, lze odvodit další důležitou charakteristiku spolehlivosti, která se nazývá hustota pravděpodobnosti $f(t)$ náhodné veličiny t. Je definována derivací distribuční funkce podle času, tedy

$$f(t) = \frac{\mathrm{d}Q(t)}{\mathrm{d}t} \tag{7.2}$$

pokud tato derivace existuje.

Veličina $f(t)$ se v teorii spolehlivosti nazývá *hustota poruch* . Součin $f(t)\mathrm{d}t$ udává, s jakou pravděpodobností nastane ve sledovaném objektu porucha ve velmi krátkém intervalu $\mathrm{d}t$ následujícím za okamžikem t.

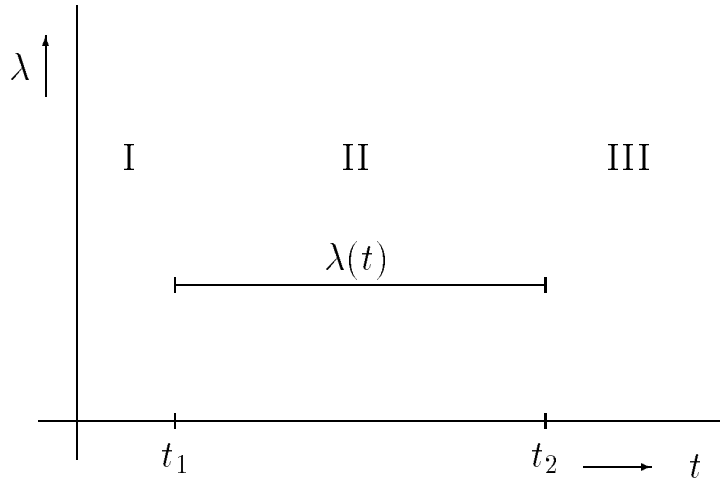
Další charakteristikou je intenzita pravděpodobnosti náhodné veličiny (zkráceně intenzita pravděpodobnosti) definovaná vztahem

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - Q(t)} \tag{7.3}$$

V teorii spolehlivosti se tato veličina nazývá *intenzita poruch* a patří k nejdůležitějším spolehlivostním ukazatelům používaným v praxi. Udává podmíněnou hustotu poruch v čase t za předpokladu, že k poruše dosud nedošlo. Pravděpodobnost, že se objekt neporouchaný v čase t porouchá v malém časovém intervalu $\mathrm{d}t$ následujícím za t, je $\lambda(t)\mathrm{d}t$.

Ze vztahů (7.1) až (7.3) vyplývá, že dosud zavedené ukazatele spolu těsně souvisejí. Chceme-li tuto závislost explicitně vyjádřit, musíme postupně dosadit (7.1) do (7.2) a odtud do (7.3)

$$f(t) = -\frac{\mathrm{d}R(t)}{\mathrm{d}t}$$



Obr. 7.1: Průběh intenzity poruch v závislosti na čase

$$\lambda(t) = -\frac{\mathrm{d}R(t)}{\mathrm{d}t}\frac{1}{R(t)} \tag{7.4}$$

Odvozenou diferenciální rovnici můžeme upravit na tvar

$$-\lambda(t)\mathrm{d}t = \frac{\mathrm{d}R(t)}{R(t)}$$

a řešit integrací

$$R(t) = \exp\left(-\int_0^t \lambda(\tau)\mathrm{d}\tau\right) \tag{7.5}$$

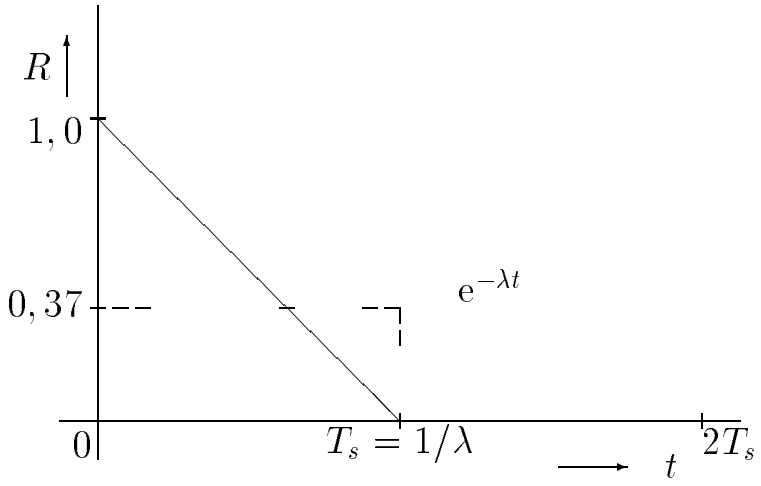
Pokud neznáme průběh intenzity poruch $\lambda(t)$ v závislosti na čase, nemůžeme výraz (7.5) dále zjednodušit. Empiricky však bylo zjištěno, že průběh $\lambda(t)$ obvykle odpovídá tzv. *vanové křivce* znázorněné na obr. 7.1.

Pro elektronické součástky platí $t_1 \doteq 6$ až 10 týdnů a $t_2 \doteq 10$ let. V intervalu $< t_1, t_2 >$, který označujeme jako období normálního provozu, platí, že λ má přibližně konstantní hodnotu. V takovém případě dokážeme integrál v (7.5) vypočítat a dostaneme

$$R(t) = \mathrm{e}^{-\lambda t} \tag{7.6}$$

$$Q(t) = 1 - \mathrm{e}^{-\lambda t} \tag{7.7}$$

$$f(t) = \lambda \mathrm{e}^{-\lambda t} \tag{7.8}$$



Obr. 7.2: Průběh $R(t)$ pro konstantní intenzitu poruch

Výrazy (7.6) až (7.8) popisují tzv. *exponenciální rozdělení* nebo *exponenciální zákon poruch.* Jeho grafickým vyjádřením je exponenciála na obr. 7.2. Pro $t = 0$ má hodnotu $R(0) = 1$, což odpovídá předpokladu, že na počátku měření je objekt v bezporuchovém stavu. Naproti tomu pro t rostoucí nade všechny meze klesá hodnota pravděpodobnosti $R(t)$ k nule. Exponenciálu na obr. 7.2 lze interpretovat ještě jinak: jestliže uvedeme v čase $t = 0$ do provozu n objektů s konstantní intenzitou poruch λ, počet $n_b(t)$ bezporuchových objektů se vlivem poruch bude v závislosti na čase zmenšovat po exponenciální křivce $n_b(t) = n\mathrm{e}^{-\lambda t}$.

Konstantní hodnotu λ a exponenciální průběh $R(t)$ budeme nadále předpokládat u všech prvků a podsystémů, jimiž se budeme zabývat. Skutečná hodnota, na níž se λ pro určitou součástku nebo podsystém ustálí, závisí na mnoha okolnostech, především na technologické úrovni výroby, na provozních podmínkách a v neposlední řadě i na velikosti a složitosti sledovaného objektu. Pro číslicové integrované obvody se pohybuje v rozmezí $10^{-8}h^{-1}$ až $10^{-5}h^{-1}$, přičemž pro paměťové obvody je obvykle o něco nižší než pro obecné logické obvody srovnatelné složitosti.

Dalším důležitým ukazatelem je *střední doba bezporuchového provozu* T_s (tj. střední hodnota sledované náhodné veličiny τ). Jak název naznačuje, je to střední hodnota provozní doby objektu, během níž nenastala žádná porucha. Pro její výpočet platí vztah odvozený z výrazu pro střední

hodnotu spojité náhodné veličiny

$$T_s = \int_0^\infty R(t)\mathrm{d}t \tag{7.9}$$

Pro neobnovované objekty se T_s nazývá také *střední doba do* (první) *poruchy*, v anglosaské literatuře se pro ni používá zkratka MTTF (mean time to failure).

Známe-li průběh $R(t)$, můžeme odvodit hodnotu T_s integrací podle (7.9). Pro exponenciální rozdělení tak dostaneme

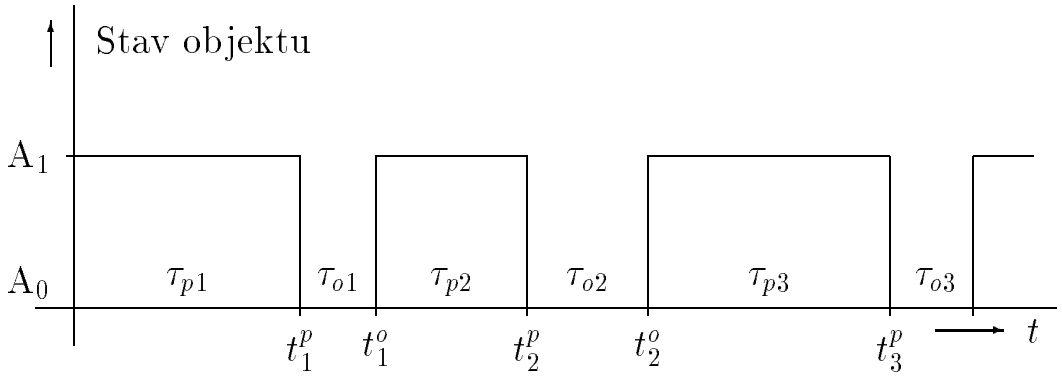
$$T_s = \int_0^\infty \mathrm{e}^{-\lambda t}\mathrm{d}t = \frac{1}{\lambda} \tag{7.10}$$

Tento jednoduchý vztah se často používá, avšak musíme si být stále vědomi jeho omezené platnosti. Kdybychom totiž do (7.10) mechanicky dosadili např. intenzitu poruch integrovaného obvodu $\lambda = 10^{-6}h^{-1}$, dostali bychom střední dobu do poruchy jeden milión hodin, tj. asi 114 let. Po tak dlouhé době však již zdaleka nemáme právo předpokládat, že λ má konstantní hodnotu (viz obr. 7.1, kde t_2 mívá velikost řádově deset let), takže takový výpočet ztrácí reálný smysl. Musíme tedy počítat s tím, že elektronické součástky selhávají podstatně dříve, než po době T_s vypočtené podle (7.10).

7.1.3 Ukazatele spolehlivosti obnovovaných objektů

Obnovovaný objekt prochází během svého technického života posloupností stavů, která je schematicky znázorněna na obr. 7.3. Na vodorovné (časové) ose jsou vyznačeny okamžiky t_i^p, kdy nastala i-tá porucha a okamžiky t_i^o, kdy byla uskutečněna i-tá obnova bezporuchového stavu. Na svislé ose je naznačen stav objektu, přičemž A_1 označuje bezporuchový a A_0 poruchový stav. Předpokládáme, že na počátku provozu je objekt v bezporuchovém stavu. Délka trvání i-tého úseku bezporuchového provozu je označena τ_{pi} a doba trvání i-té opravy τ_{oi}.

Pro obnovované objekty se místo střední doby do poruchy používá *střední doba mezi poruchami* . Stanoví se jako aritmetický průměr všech naměřených dob bezporuchového provozu od skončení opravy do výskytu následující poruchy. Tuto hodnotu získáme tak, že kumulativní dobu provozu t_p, vypočtenou jako součet všech dob provozu za sledované období,



Obr. 7.3: Sled stavů obnovovaného systému

dělíme počtem n výpadků způsobených poruchami. Platí

$$T_s = \frac{t_p}{n} = \frac{1}{n}\sum_{i=1}^{n} \tau_{pi} \tag{7.11}$$

Pro úplnost poznamenejme, že v anglosaské literatuře, např. [?], se zavádí ukazatel MTBF (mean time between failures), který se počítá jako střední doba od jednoho výskytu poruchy do dalšího výskytu poruchy (od t_i^0 do t_{i+1}^0 na obr. 7.3.). Do této doby je pak zahrnuta i doba trvání opravy τ_{oi}, takže hodnota MTBF je větší, než hodnota T_s, vypočtená podle vztahu (7.11). V tomto textu budeme střední hodnotu intervalu mezi dvěma po sobě následujícími poruchami označovat jako střední dobu cyklu T_c.

Jako charakteristiky, vyjadřující okamžitou nebo dlouhodobou použitelnost opravovaného výpočetního systému, se používají součinitele (též koeficienty) pohotovosti a prostoje (v anglicky psané literatuře jsou označovány jako availability a unavailability). *Okamžitý součinitel pohotovosti* $K_p(t)$ udává pravděpodobnost, že v čase t bude systém v provozuschopném stavu. Zpravidla existuje limita $K_p = \lim_{t\to\infty} K_p(t)$, označovaná jako stacionární součinitel pohotovosti. Hodnota tohoto ukazatele udává pravděpodobnost, že systém, který je v ustáleném provozním režimu, bude provozuschopný v libovolně zvoleném okamžiku. Prakticky můžeme tuto hodnotu interpretovat jako poměrnou část provozuschopné doby z celkové sledované doby. Platí

$$K_p = \frac{t_p}{t_p + t_o} \tag{7.12}$$

kde t_p je kumulativní doba provozu a t_o je kumulativní doba opravy během sledovaného období. Podobně jako v (7.11) můžeme zavést střední dobu opravy vztahem

$$T_o = \frac{t_o}{n} \tag{7.13}$$

V anglosaské odborné literatuře se tato veličina označuje zkratkou MTTR (mean time to repair).

Považujeme-li dobu trvání opravy za náhodnou veličinu, která má exponenciální rozdělení s konstantním parametrem μ, označovaným jako intenzita oprav, platí

$$T_o = \frac{1}{\mu} \tag{7.14}$$

Dosadíme-li do (7.12) postupně (7.11), (7.13) a (7.14), dostaneme

$$K_p = \frac{T_s}{T_s + T_o} = \frac{\mu}{\mu + \lambda} \tag{7.15}$$

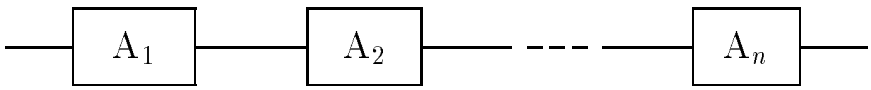
Součinitel prostoje je doplňkem součinitele pohotovosti do jedné. I pro něj můžeme určit okamžitou a ustálenou hodnotu. Okamžitý součinitel prostoje $K_n(t) = 1 - K_p(t)$ udává pravděpodobnost, že v čase t nebude systém provozuschopný. Stacionární součinitel prostoje $K_n = \lim_{t\to\infty} K_n(t)$ je roven pravděpodobnosti, že v libovolně zvoleném okamžiku systém nebude provozuschopný.

7.2 Modely systémů s nezávislými prvky

U mnoha reálných systémů lze předpokládat nezávislost poruch a popřípadě i oprav jednotlivých prvků. V takovém případě jsou doby do poruchy u jednotlivých prvků nezávislé náhodné veličiny. Spolehlivostní modely systémů s nezávislými prvky jsou relativně jednoduché, a proto v případě, kdy máme možnost volby, jim dáváme přednost před jinými typy modelů. Po matematické stránce jsou tyto modely založeny na vztazích pro násobení pravděpodobností nezávislých náhodných jevů (tj. pravděpodobností bezporuchového provozu *R(t)* a poruch *Q(t)* jednotlivých prvků) a pro sčítání pravděpodobností vzájemně se vylučujících jevů (tj. možných stavů systému). Dále uvedeme základní modely využívané zejména pro neobnovované systémy.

7.2.1 Sériový model

Tento model používáme v případě, kdy porucha kteréhokoliv prvku způsobí poruchu celku a časové intervaly do poruchy jednotlivých prvků jsou navzájem nezávislé náhodné veličiny. Sériový spolehlivostní model systému složeného z prvků A_1 až A_n je na obr. 7.4.



Obr. 7.4: Sériový spolehlivostní model

Jestliže známe pravděpodobnosti bezporuchového provozu $R_i(t)$ pro každý prvek A_i, je výsledná pravděpodobnost bezporuchového provozu $R(t)$ dána jejich součinem

$$R(t) = \prod_{i=1}^{n} R_i(t) \tag{7.16}$$

Pro konstantní intenzitu poruch λ_i každého prvku dostaneme

$$R(t) = \prod_{i=1}^{n} \mathrm{e}^{\lambda_i t} = \mathrm{e}^{\lambda t} \tag{7.17}$$

kde λ je výsledná intenzita poruch systému, získaná jako součet intenzit poruch prvků λ_i

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{7.18}$$

Sériové spojení prvků se zadanými konstantními intenzitami poruch lze tedy nahradit jedním prvkem s celkovou intenzitou poruch získanou součtem intenzit poruch všech prvků.

Střední dobu bezporuchového provozu T_s získáme z (7.17) integrací podle (1.9). Pro konstantní intenzity poruch λ_i dostaneme

$$T_s = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\lambda} \tag{7.19}$$

Pro sériové spojení n shodných prvků s konstantní intenzitou poruch λ_p dostaneme střední dobu bezporuchového provozu

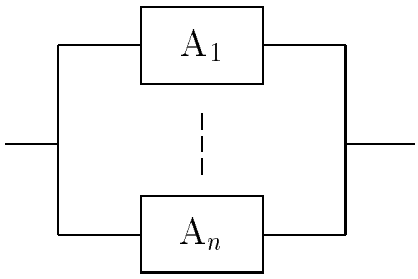
$$T_s = \frac{1}{n\lambda_p} \tag{7.20}$$

Je třeba poznamenat, že skutečné (např. elektrické) zapojení systému nemusí být sériové. Sériovost ve spolehlivostním modelu vyjadřuje pouze vlastnost systému z hlediska spolehlivosti.

Sériový spolehlivostní model se v souvislosti s výpočetními systémy odolnými proti poruchám velmi často využívá jako základní model číslicového modulu, kterým je typicky deska s plošným spojem, osazená integrovanými obvody. Předpokládáme-li, že porucha kterékoliv součástky způsobí poruchu desky, je spolehlivostním modelem sériové spojení součástek. Obvykle se předpokládají konstantní intenzity poruch součástek, získané například z údajů výrobce nebo výpočtem podle nějakého poruchového modelu součástky. Jednou z nejvyužívanějších výpočetních metodik je americká vojenská norma s označením MIL-HDBK-217. Získané intenzity poruch součástek je na základě odvozených vlastností sériového modelu možné sečíst na výslednou konstantní intenzitu poruch, která charakterizuje spolehlivostní chování modulu jako celku.

7.2.2 Paralelní model

Paralelní model používáme tehdy, dochází-li k poruše systému pouze při poruše všech jeho prvků. Paralelní spolehlivostní model pro n prvků je znázorněn graficky na obr. 7.5.



Obr. 7.5: Paralelní spolehlivostní model

Jestliže známe pravděpodobnost poruchy $Q_i(t)$ pro každý prvek A_i a jsou-li poruchy prvků nezávislé, můžeme výslednou pravděpodobnost poruchy $Q(t)$ vyjádřit vztahem

$$Q(t) = \prod_{i=1}^{n} Q_i(t) \tag{7.21}$$

Pro pravděpodobnost bezporuchového provozu lze vztah upravit do tvaru

$$R(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) \tag{7.22}$$

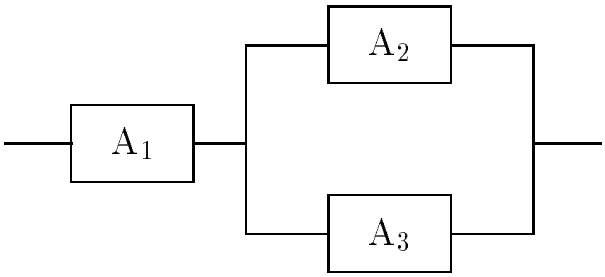
Použijeme-li n shodných prvků s konstantní intenzitou poruch λ_p, je možné podle [?] vyjádřit střední dobu bezporuchového provozu jako

$$T_s = \frac{1}{\lambda_p} \sum_{i=1}^{n} \frac{1}{i} \tag{7.23}$$

7.2.3 Kombinované modely

Ve složitějších případech může být spolehlivostní model systému s nezávislými prvky vytvořen nějakou kombinací sériového a paralelního spojení prvků. Pravděpodobnost bezporuchového provozu lze pro kombinovaný systém určit postupnou aplikací vzorců (7.16) a (7.21) nebo (7.22).

Postup řešení kombinovaného modelu ukážeme na příkladu modelu neobnovovaného systému podle obr. 7.6.



Obr. 7.6: Příklad kombinovaného modelu

Jsou dány konstantní intenzity poruch $\lambda_1, \lambda_2, \lambda_3$ a chceme určit například střední dobu bezporuchového provozu T_s. Nejprve určíme pravděpodobnost poruchy paralelního spojení prvků A_2 a A_3

$$Q_{23} = Q_2 Q_3 = (1 - R_2)(1 - R_3) = 1 - R_2 - R_3 + R_2 R_3$$

Dále určíme výsledné R ze sériového spojení R_1 a R_{23}

$$R_{23} = 1 - Q_{23} = R_2 + R_3 - R_2 R_3$$

$$R = R_1 R_{23} = R_1 R_2 + R_1 R_3 - R_1 R_2 R_3$$

Po dosazení časových závislostí $R_i(t) = \exp(-\lambda_i t)$ dostaneme

$$R(t) = \mathrm{e}^{-(\lambda_1+\lambda_2)t} + \mathrm{e}^{-(\lambda_1+\lambda_3)t} - \mathrm{e}^{-(\lambda_1+\lambda_2+\lambda_3)t}$$

Nakonec určíme střední dobu bezporuchového provozu

$$T_s = \int_0^\infty R(t)\mathrm{dt} = \frac{1}{\lambda_1+\lambda_2} + \frac{1}{\lambda_1+\lambda_3} - \frac{1}{\lambda_1+\lambda_2+\lambda_3}$$

Speciálním případem kombinovaných modelů je sériově-paralelní model (sériové spojení n bloků, z nichž každý obsahuje paralelní spojení m prvků) a paralelně-sériový model (paralelní spojení m větví o n prvcích). Příslušné vzorce pro R a Q lze jednoduše získat z (7.16) a (7.21) nebo (7.22).

V této souvislosti je vhodné připomenout důležitou interpretaci blokového spolehlivostního schématu. Porucha prvku představuje přerušení příslušné větve ve schématu. Modelovaný systém je schopný provozu, jestliže existuje alespoň jedna cesta ze vstupu na výstup schématu.

7.2.4 Modely využívající stavový graf

Uvažujme systém složený z n prvků A_1 až A_n. Každý z prvků může být buď ve stavu 1 (schopný provozu) nebo ve stavu 0 (porouchaný). Stav celého systému lze zřejmě kódovat n-bitovým binárním číslem, jehož jednotlivé pozice odpovídají stavu prvků A_1 až A_n. Počet stavů spolehlivostního modelu systému je potom dán mocninou 2^n.

Spolehlivostní model je možné konstruovat jako tzv. stavový graf. Uzly grafu odpovídají stavům modelu a hrany odpovídají možným přechodům mezi stavy. V modelu je možné rozlišit stavy, ve kterých je systém jako celek schopný provozu (označujeme kolečkem) a stavy, ve kterých je systém porouchaný (označujeme čtverečkem). Zpravidla uvažujeme pouze přechody mezi sousedními stavy (tj. stavy lišícími se pouze v jedné pozici kódu stavu) - nepředpokládáme tedy současnou poruchu několika prvků systému. V tomto případě představuje stavový graf krychli v n-rozměrném prostoru.

Stavovým grafem lze vyjádřit i sériové, paralelní nebo kombinované modely. Hlavní oblastí jeho využití jsou však případy, které nelze převést na kombinaci sériového nebo paralelního spolehlivostního spojení. Označíme-li pravděpodobnost výskytu i-tého stavu v čase t jako $p_i(t)$, můžeme určit

$R(t)$ s využitím stavového grafu podle vztahu pro součet pravděpodobností vzájemně se vylučujících náhodných jevů

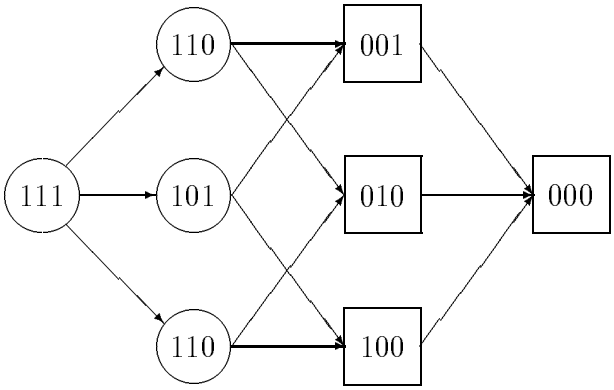
$$R(t) = \sum_i p_i(t) \tag{7.24}$$

Index i probíhá přes všechny stavy, ve kterých je systém jako celek provozuschopný.

Použití stavového grafu předvedeme na příkladu.

Příklad 7.1.

Uvažujme systém složený ze tří prvků A_1, A_2 a A_3. Systém jako celek je schopný provozu, jestliže alespoň dva prvky jsou schopné provozu. Zřejmě nelze použít žádnou kombinaci sériového nebo paralelního spojení prvků. Stavový graf je pro uvedený příklad znázorněn na obr. 7.7.



Obr. 7.7: Příklad stavového grafu

U jednotlivých stavů jsou uvedeny kódy stavu (např. 101 je stav, ve kterém prvky A_1 a A_3 jsou v provozu, kdežto prvek A_2 je porouchaný).

Pravděpodobnost bezporuchového provozu získáme součtem pravděpodobností stavů 111, 011, 101 a 110:

$$R = R_1R_2R_3 + Q_1R_2R_3 + R_1Q_2R_3 + R_1R_2Q_3 =$$

$$= R_1R_2R_3 + (1 - R_1)R_2R_3 + R_1(1 - R_2)R_3 + R_1R_2(1 - R_3) =$$

$$= R_1R_2 + R_1R_3 + R_2R_3 - 2R_1R_2R_3 \qquad \square$$

Příklad 7.2

Uvažujme paměť složenou z k slov o rozměru n bitů. Použitý samoopravný kód umožňuje tolerovat jeden chybný bit ve slově (tj. musí fungovat $n-1$ z n bitů). Předpokládáme, že poruchy jednotlivých bitů ve slově (a v různých slovech) jsou nezávislé. Dále předpokládáme, že porucha v řídící logice paměti způsobí poruchu celé paměti. Uvažujeme konstantní intenzitu poruch paměťové buňky (jednoho bitu) λ_b a konstantní intenzitu poruch řídící logiky λ_c. Označíme pravděpodobnost bezporuchového provozu paměťové buňky $R_b(t) = \exp(-\lambda_b t)$ a řídící logiky $R_c(t) = \exp(-\lambda_c t)$. Pravděpodobnost bezporuchového provozu pro jedno slovo paměti je

$$R_w = R_b^n + nQ_bR_b^{n-1} = R_b^n + n(1-R_b)R_b^{n-1} = nR_b^{n-1} - (n-1)R_b^n$$

Všechna slova paměti a řídící logika jsou ve spolehlivostním smyslu spojeny sériově a tedy pravděpodobnost bezporuchového provozu pro celou paměť je dána vztahem

$$R = R_c(nR_b^{n-1} - (n-1)R_b^n)^k$$

Po dosazení časových funkcí dostaneme výsledný vztah

$$R(t) = \mathrm{e}^{-\lambda_c t}(n\mathrm{e}^{-(n-1)\lambda_b t} - (n-1)\mathrm{e}^{-n\lambda_b t})^k$$

Je třeba podotknout, že uvažujeme pouze trvalé poruchy paměťových buněk. Přechodná porucha v některé paměťové buňce (např. samovolná změna zapsané informace v dynamické RAM paměti vlivem radioaktivního záření) je řídící logikou paměti obvykle tolerována (chyba při čtení, oprava a zápis opravené informace).

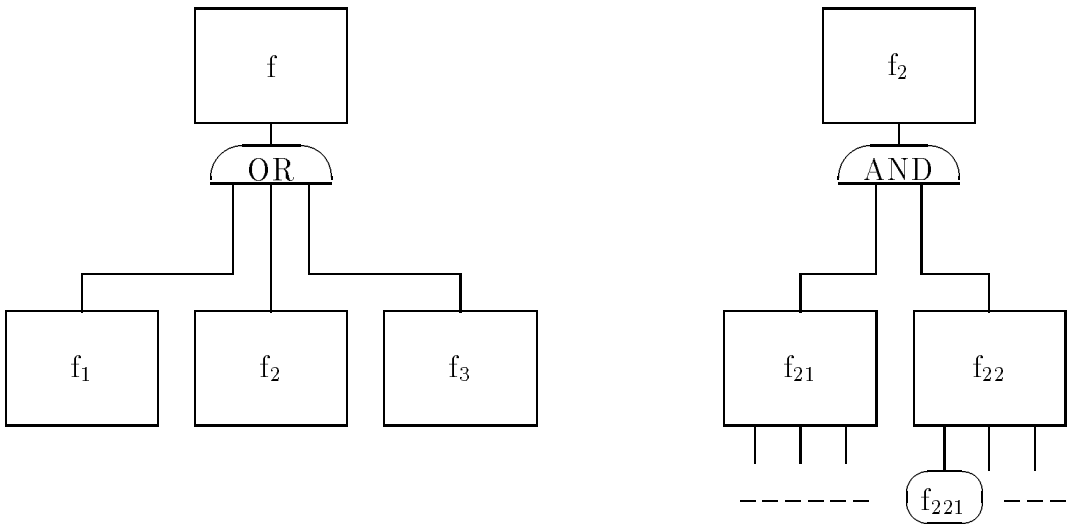
7.2.5 Stromy poruch

Stromy poruch představují klasickou a v praxi často využívanou formu spolehlivostního modelu. Je dána množina základních událostí (zpravidla poruch) a pravděpodobnosti těchto událostí - buď jako funkce času nebo jako konstanty vztažené například k uvažované době života zařízení. Dále je dána množina operátorů (označovaných jako hradla - gates). Operátory jsou charakterizovány jednak svojí logickou funkcí (vytváří z booleovských hodnot událostí i-té úrovně booleovskou hodnotu události $i-1$ úrovně) a dále aritmetickou funkcí (z pravděpodobností událostí i-té úrovně se počítá pravděpodobnost události $i-1$ úrovně). Popis spolehlivostního chování

systému uvedeným způsobem pak vede k hierarchické (stromové) struktuře událostí, ve které jsou jednotlivé úrovně událostí vázány různými typy hradel. Nejobvyklejšími typy hradel jsou OR (odpovídá sériovému spolehlivostnímu spojení) a AND (odpovídá paralelnímu spojení). Příklad stromu poruch je na obrázku 7.8.

Význam označení bloků může být například:

f	porucha počítače
f_1	porucha procesoru
f_2	ztráta napájecího napětí
f_3	porucha paměti
f_{21}	porucha záložní baterie
f_{22}	ztráta napětí síťového zdroje
f_{221}	někdo omylem vypnul síťový vypínač, základní událost, pravděpodobnost události 0,00002



Obr. 7.8: Příklad stromu poruch

Oblíbenost stromů poruch při spolehlivostní analýze je způsobena zejména jejich následujícími výhodami.

- Umožňují přehledné grafické znázornění spolehlivostního chování systému.
- Umožňují postupné zjemňování spolehlivostního modelu do libovolné úrovně detailů.

- Je možné rozdělit strom na podstromy, které se vyhodnocují samostatně (viz obr. 7.8).
- Výpočet spolehlivostních ukazatelů typu R, Q z pravděpodobností základních událostí je jednoduchý.
- Strom poruch lze pro zadané konstantní intenzity základních událostí relativně jednoduše převést na markovský model. Každé kombinaci základních událostí, která ponechává systém provozuschopný, patří jeden stav v odpovídajícím markovském modelu.

Poznámka

Prozatím jsme uvažovali modely neobnovovaných systémů. Všechny dosud uvedené modely však lze využít i pro výpočet součinitelů pohotovosti a prostoje obnovovaných systémů za předpokladu, že doby poruch i oprav jednotlivých prvků jsou navzájem nezávislé (prvky se neovlivňují). Ve vztazích (7.16) a (7.21) se nahradí pravděpodobnosti bezporuchového provozu $R(t)$ součinitelem pohotovosti $K_p(t)$ nebo K_p a pravděpodobnosti poruchy $Q(t)$ součinitelem prostoje $K_n(t)$ nebo K_n. Vztahy pro výpočet součinitelů pohotovosti a prostoje pro prvek se známými konstantními hodnotami intenzity poruch λ a intenzity oprav μ byly uvedeny v předchozí kapitole. Výpočet střední doby bezporuchového provozu a střední doby prostoje u obnovovaných systémů je složitější záležitostí a bude popsán dále.

7.3 Markovské modely

7.3.1 Markovské modely neobnovovaných systémů

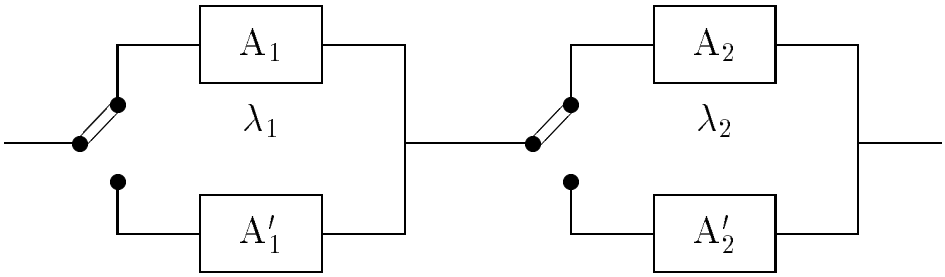
Markovské modely se využívají v případě, že spolehlivostní chování prvků systému *není nezávislé*. Typicky se jedná o případ, kdy jsou některé prvky využité jako tzv. *studená záloha* - tj. jsou na počátku vypnuté (nezatížené - jejich intenzita poruch je nízká) a zapínají se až po poruše dosud aktivního prvku. Neobnovovaný systém se časem porouchá, pročež jeho "život" je třeba popsat markovským modelem *s absorpčními stavy*. Absorpční stavy modelu představují stavy, ve kterých je systém porouchaný jako celek. Graf přechodů markovského modelu neobnovovaného systému je *acyklický* (po poruše neexistuje obnova - tj. není možný návrat do stavu před poruchou).

Použití markovských modelů ve spolehlivostních aplikacích je omezeno předpokladem, že intenzity poruch a oprav jsou konstantní pro všechny prvky systému. Náhodné doby do poruchy prvků a náhodné doby oprav prvků mají v tomto případě exponenciální pravděpodobnostní rozdělení.

Příklad markovského modelu neobnovovaného systému již byl uveden v kap.2 (příklad 2.1). Zde ještě uvedeme příklad využití modelu, kdy není nutné formulovat a řešit soustavu diferenciálních rovnic.

Příklad 7.3.

Uvažujme systém znázorněný blokovým spolehlivostním schématem na obrázku 2.9.



Obr. 7.9: Spolehlivostní schéma pro příklad 7.3

Moduly A'_1,A'_2 představují nezatíženou dynamickou zálohu. Graf přechodů pro uvažovaný systém je uveden na obr.7.10. Ve stavu 2 je porouchaný modul A_1,ostatní jsou v pořádku. Ve stavu 3 je porouchaný modul A_2,ostatní jsou v pořádku. Ve stavu 4 jsou porouchané A_1 a A_2. Určíme přímo střední dobu bezporuchového provozu T_s. V grafu neexistuje žádný cykl a můžeme tedy s výhodou použít postup podle 5b.

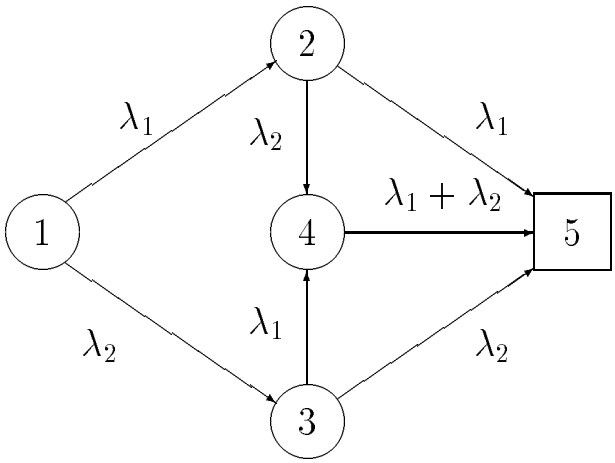
Existují 4 možné cesty z výchozího stavu 1 do absorpčního stavu 5. Například pro první cestu 1-2-4-5 odvodíme celkovou dobu trvání cesty a pravděpodobnost realizace cesty

$$T_{c1} = \frac{1}{\lambda_1+\lambda_2} + \frac{1}{\lambda_1+\lambda_2} + \frac{1}{\lambda_1+\lambda_2} = \frac{3}{\lambda_1+\lambda_2}$$

$$p_{c1} = \frac{\lambda_1}{\lambda_1+\lambda_2}\frac{\lambda_2}{\lambda_1+\lambda_2} = \frac{\lambda_1\lambda_2}{(\lambda_1+\lambda_2)^2}$$

Podobně dostaneme pro další cesty 1-2-5, 1-3-5 a 1-3-4-5 :

$$T_{c2} = \frac{2}{\lambda_1+\lambda_2} \ , \qquad p_{c2} = \frac{\lambda_1^2}{(\lambda_1+\lambda_2)^2}$$



Obr. 7.10: Graf přechodů pro příklad 7.3

$$T_{c3} = \frac{2}{\lambda_1 + \lambda_2} \ , \qquad p_{c3} = \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2}$$

$$T_{c4} = \frac{3}{\lambda_1 + \lambda_2} \ , \qquad p_{c4} = \frac{\lambda_1 \lambda_2}{(\lambda_1 + \lambda_2)^2}$$

Výraz pro T_s lze již pak snadno odvodit

$$T_s = \sum_{i=1}^{4} T_{ci} p_{ci} = \frac{2\lambda_1^2 + 6\lambda_1\lambda_2 + 2\lambda_2^2}{(\lambda_1 + \lambda_2)^2}$$

7.3.2 Markovské modely obnovovaných systémů

V obnovovaném systému je možné některé poruchy opravit a vrátit se do výchozího stavu. Graf přechodů markovského procesu, kterým modelujeme chování systému pak ztrácí acyklický charakter. Přechody odpovídající opravě prvku mají jako intenzitu přechodu příslušnou intenzitu oprav μ. Tato se typicky určí jako převrácená hodnota střední doby opravy. Zde je třeba poznamenat, že předpoklad exponenciálního pravděpodobnostního rozdělení doby opravy (potřebný pro regulérní využití markovského modelu) není příliš reálný (na rozdíl od rozdělení doby do poruchy).

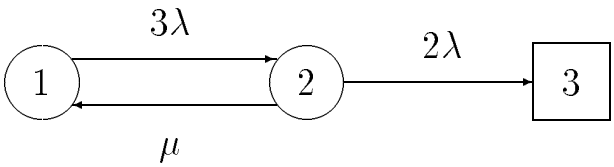
Pokud není možné opravit všechny poruchy, dostaneme markovský model s absorpčními stavy, které odpovídají neopravitelným poruchám. Příklady modelů této kategorie jsou dále 7.4 a 7.5. Předpokládáme–li, že

po každé poruše následuje oprava vadného prvku a opětné uvedení systému do provozu, pak v grafu přechodů markovského náhodného procesu, kterým modelujeme chování takového systému, nejsou absorpční stavy. Z každého stavu grafu lze pak v konečném počtu kroků přejít do kteréhokoliv jiného stavu. Markovské modely bez absorbčních stavů tedy budeme využívat pro obnovované systémy, u kterých neuvažujeme neopravitelné poruchy. V idealizovaném modelu budeme uvažovat nekonečně dlouhou dobu života systému. V anglosaské literatuře se modely bez absorpčních stavů označují jako *availability models* na rozdíl od modelů s absorpčními stavy, pro které je používán název *reliability models*. Příklad markovského spolehlivostního modelu bez absorbčních stavů je dále 7.6.

Příklad 7.4

Uvažujme systém složený ze tří shodných výpočetních modulů, které obsahují procesor, paměť a I/O modul. Výsledky výpočtu všech tří modulů se před výstupem porovnávají hlasovacím mechanismem realizovaným buď elektronicky nebo programově, popřípadě kombinací obou způsobů. Výsledek hlasování umožní odhalit případný vadný modul. Budeme předpokládat, že vadný modul se může opravit za provozu zbývajících dvou a po opravě se opět připojí k výpočtu. Jedná se o tzv. *opravovaný systém TMR* .

Dále předpokládejme konstantní intenzitu poruch jednoho modulu λ a konstantní intenzitu jeho oprav μ. V takovém případě dostáváme jednoduchý markovský model s absorpčním stavem. Graf přechodů je na obr. 7.11.



Obr. 7.11: Graf přechodů pro příklad 7.4

Ve stavu 1 jsou všechny moduly bezporuchové, ve stavu 2 se jeden modul opravuje a dva pracují. Stav 3 představuje poruchu, kterou považujeme za neopravitelnou, stav je tedy absorpční. Známe-li hodnoty λ a μ, lze určit pravděpodobnosti stavů $p_1(t)$, $p_2(t)$, a $p_3(t)$ řešením soustavy rovnic

$$\begin{aligned} p_1'(t) &= -3\lambda p_1(t) + \mu p_2(t) \\ p_2'(t) &= 3\lambda p_1(t) - (\mu + 2\lambda) p_2(t) \\ p_3'(t) &= 2\lambda p_2(t) \end{aligned}$$

Počáteční podmínky jsou $p_1(0) = 1$, $p_2(0) = 0$, $p_3(0) = 0$. Po vyřešení soustavy lze určit střední dobu bezporuchového provozu T_s:

$$T_s = \frac{5}{6\lambda} + \frac{\mu}{6\lambda^2}$$

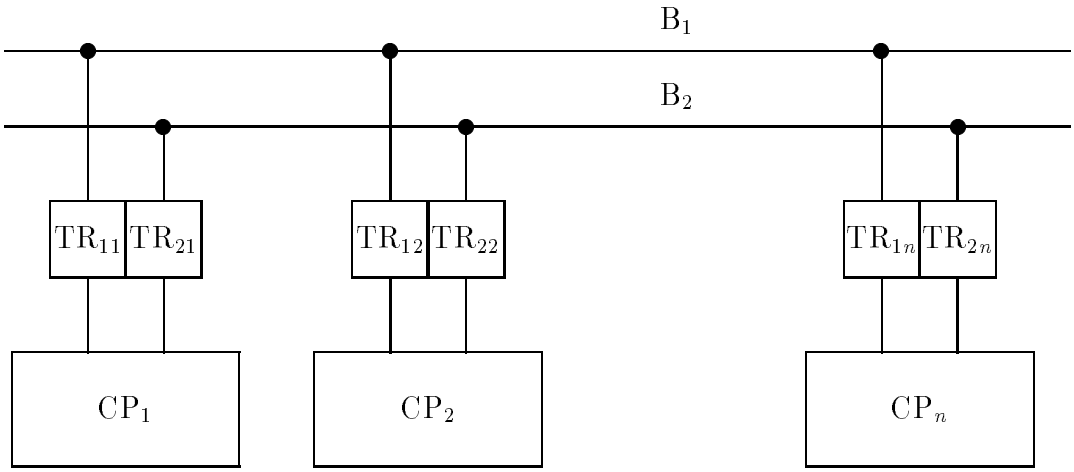
Uvedený model odpovídá výpočetnímu systému August 300, který uvedla již v roce 1981 na trh americká firma August Systems jako superspolehlivý počítač pro řízení průmyslových (zejména chemických) procesů. Pokud uvažujeme $\mu = 0,041h^{-1}$ (odpovídající střední doba opravy 24 hodin) a $\lambda = 1,8.10^{-4}h^{-1}$, dostaneme $T_s = 24$ let, což je údaj uváděný ve firemních materiálech. Při stejné intenzitě poruch je střední doba do poruchy samostatně pracujícího modulu $1/\lambda = 5550\ h = 0,63$ roku. Střední doba do poruchy neopravovaného TMR systému je $5/6\lambda = 4630h$, tj. menší než pro samostatně pracující (spolehlivostně neřešený) modul.

Příklad 7.5

Distribuované řídicí systémy na bázi lokálních počítačových sítí (LAN - Local Area Networks) nacházejí stále širší uplatnění v průmyslové praxi. Zvýšené nároky na spolehlivostní parametry vedou k využití takových architektur, které umožňují toleranci určitých tříd poruch. Často se využívá lokální síť s jednou sériovou sběrnicí. Sběrnice představuje ze spolehlivostního hlediska "úzký profil". Zajímalo by nás prodloužení střední doby bezporuchového provozu T_s dvousběrnicové sítě proti síti s jednou sběrnicí. Dále uvedeme markovský model podle [?].

Komunikační subsystém LAN tvoří stanice připojené na sběrnice, přičemž i-tá stanice zahrnuje jeden komunikační procesor CP_i a dvě jednotky vysílačů a přijímačů TR_{1i}, TR_{2i}. Sběrnice B_j obsahuje vlastní přenosová média a prvky nutné pro připojení jednotlivých stanic (obr.7.12). Při normální činnosti je vždy jedna sběrnice ve funkci nezatížené zálohy. Jestliže nějaká porucha znemožní správnou činnost aktivní sběrnice, stanice aktivují (pokud je to možné) záložní sběrnici a pokračují dále v normální činnosti. Model založíme na dále uvedených předpokladech.

- Porucha komunikačního procesoru CP ovlivní obě sběrnice se známou pravděpodobností $1 - r_{CP}$ a porucha modulu TR ovlivní sběrnici,



Obr. 7.12: Komunikační subsystém LAN

na kterou je připojen, s pravděpodobností $1 - r_{TR}$. Parametry r_{CP} a r_{TR} budeme nazývat pravděpodobnosti separace poruch příslušných prvků.

- Uvažujeme zmenšení intenzity poruch nezatížených záložních prvků s koeficientem ν_B pro sběrnici a ν_{TR} pro modul TR ($0 \leq \nu_B \leq 1, \quad 0 \leq \nu_{TR} \leq 1$).

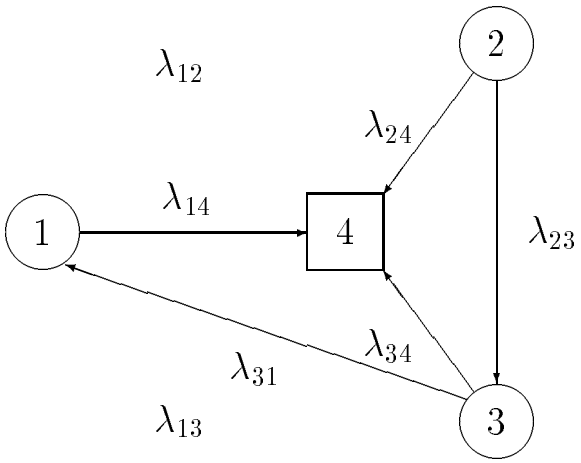
- Vznik poruch komunikačních procesorů, modulů TR a sběrnic je reprezentován konstantními intenzitami poruch λ_{CP}, λ_{TR} a λ_B. Intenzita poruch sběrnice B je úměrná počtu připojených stanic n, tedy $\lambda_B = n\lambda_u$, kde λ_u je intenzita poruch sběrnice s jednou stanicí.

- Vadné sběrnice nebo stanice jsou opravovány nezávisle (za činnosti systému) s konstantní intenzitou oprav μ. Předpokládáme, že po dobu opravy vadné sběrnice nevznikne její další porucha, ať už vlivem připojených modulů TR nebo sběrnice samotné.

- Nezatížené záložní komponenty jsou náhodně a nezávisle testovány s konstantní intenzitou v a případná chyba je zjištěna s pravděpodobností rovnou jedné. Oprava je zahájena okamžitě po zjištění poruchy.

Matematickým modelem použitým k výpočtu T_s je markovský proces, jehož graf přechodů je na obr. 7.13.

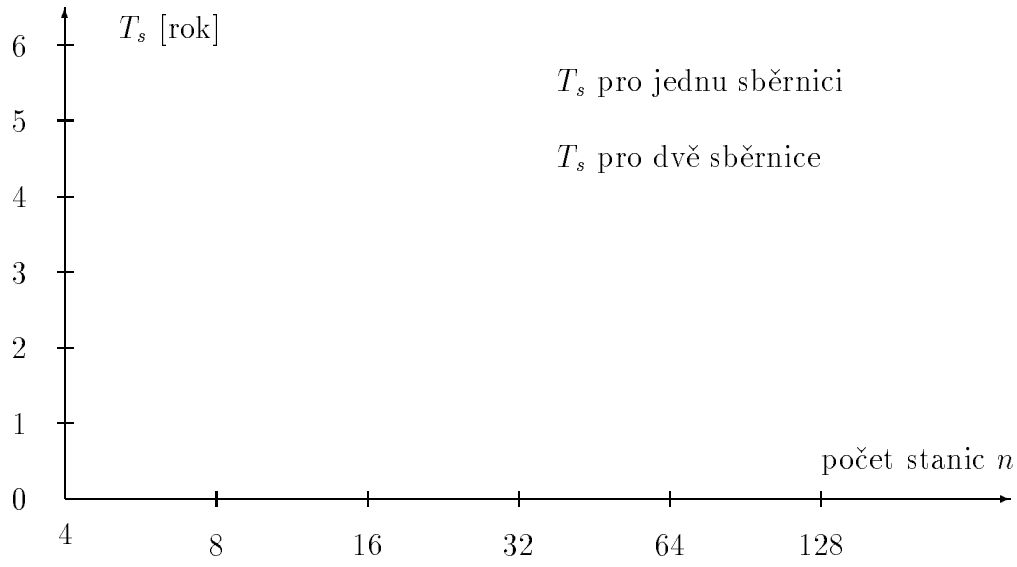
Stav **1** - obě sběrnice jsou v provozuschopném stavu



Obr. 7.13: Graf přechodů spolehlivostního modelu LAN

Stav **2** - skrytá porucha nezatížené záložní sběrnice
(dosud nebyla zjištěna testem)
Stav **3** - probíhá oprava vadné záložní sběrnice
Stav **4** - celková porucha komunikačního subsystému
(obě sběrnice neprovozuschopné)
Přechod **12** - porucha záložní sběrnice způsobená modulem typu
TR nebo B
$\lambda_{12} = n[(1 - r_{TR})\nu_{TR}\lambda_{TR} + \nu_B\lambda_u]$
Přechod **13** - porucha aktivní sběrnice způsobená modulem typu
TR nebo B
$\lambda_{13} = n[(1 - r_{TR})\lambda_{TR} + \lambda_u]$
Přechod **14** - porucha obou sběrnic způsobená modulem typu CP
$\lambda_{14} = n[(1 - r_{CP})\lambda_{CP}]$
Přechod **23** - preventivní test záložní sběrnice
$\lambda_{23} = v$
Přechod **24** - porucha aktivní sběrnice způsobená TR, B nebo CP
$\lambda_{24} = n[(1 - r_{CP})\lambda_{CP} + (1 - r_{TR})\lambda_{TR} + \lambda_u]$
Přechod **31** - oprava záložní sběrnice
$\lambda_{31} = \mu$
Přechod **34** - porucha aktivní sběrnice způsobená TR, B nebo CP
$\lambda_{34} = n[(1 - r_{CP})\lambda_{CP} + (1 - r_{TR})\lambda_{TR} + \lambda_u]$

Střední doba bezporuchového provozu T_s byla určena numericky pro



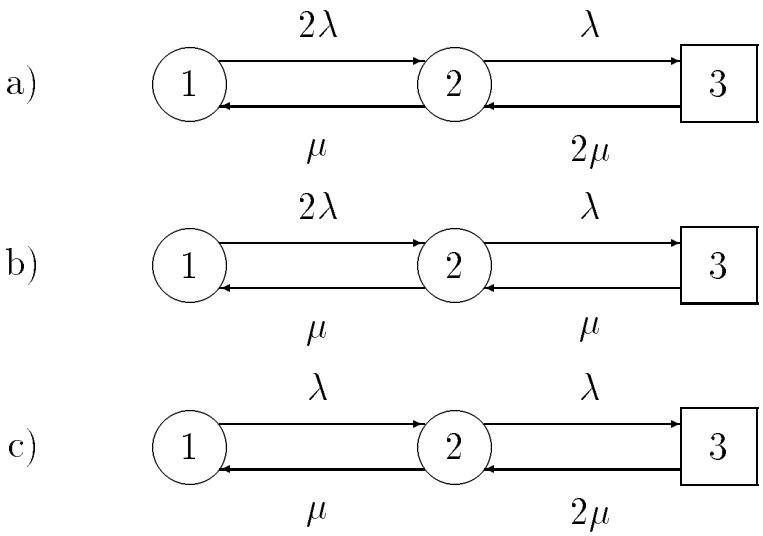
Obr. 7.14: Porovnání T_s pro různé verze LAN

následující číselné hodnoty: $\lambda_{CP} = 0,95$ rok^{-1}, $\lambda_{TR} = 0,05$ rok^{-1}, $\lambda_u = 0,1$ rok^{-1}, $\mu = 1000$ rok^{-1}. Z analýzy modelu mimo jiné vyplynulo, že pro hodnoty ν_B větší než 0,2 lze při intenzitě testování $v = 100$ rok^{-1} dosáhnout znatelného zvýšení T_s proti netestovanému systému v rozmezí od 40 do 85 procent. Jako klíčový parametr ovlivňující hodnotu T_s se jeví r_{CP}, tj. pravděpodobnost, že porucha komunikačního procesoru neovlivní správnou funkci obou sběrnic.

Na závěr uvedeme v obr. 7.14 porovnání zjištěné závislosti T_s na počtu stanic n pro případ s jednou a se dvěma sběrnicemi pro výše uvedené číselné hodnoty intenzit událostí a pro hodnoty dalších parametrů $r_{TR} = 0,90$, $\nu_B = 0,80$, $\nu_{TR} = 0,50$, $r_{CP} = 0,95$, $v = 100$ rok^{-1}. Pro síť s jednou sběrnicí je porucha aktivní sběrnice poruchou celkovou, a proto je T_s dána převrácenou hodnotou intenzity λ_{34}.

Příklad 7.6

Uvažujme opravovaný systém složený ze dvou modulů. Pro správnou funkci celku je nutná správná funkce alespoň jednoho modulu. Použité dva moduly mají stejnou intenzitu oprav μ a stejnou intenzitu poruch λ. Porouchaný modul se opravuje za provozu zbývajícího modulu. Pokud se porouchají oba moduly, opravují se současně (předpokládáme neomezenou opravářskou kapacitu). Chceme určit stacionární součinitel pohotovosti K_p. Nejprve nakreslíme graf přechodů (obr.7.15a).



Obr. 7.15: Graf přechodů duplexního obnovovaného systému

Ve stavu 1 fungují oba moduly, ve stavu 2 je porouchaný jeden modul a ve stavu 3 jsou porouchané oba moduly. Dále napíšeme přímo soustavu rovnic pro ustálené pravděpodobnosti stavů s využitím frekvenční rovnováhy a doplníme normalizační podmínku

$$\begin{aligned} 2\lambda p_1 &= \mu p_2 \\ 2\lambda p_1 + 2\mu p_3 &= (\lambda + \mu) p_2 \\ \lambda p_2 &= 2\mu p_3 \\ p_1 + p_2 + p_3 &= 1 \end{aligned}$$

Soustava je relativně lehce řešitelná. Z první a třetí rovnice postupně dostaneme

$$p_2 = \frac{2\lambda}{\mu} p_1 \,, \qquad p_3 = \frac{\lambda}{2\mu} p_2 = \frac{\lambda^2}{\mu^2} p_1$$

Získané p_2, p_3 dosadíme do normalizační podmínky a určíme p_1

$$p_1 = \frac{1}{1 + \frac{2\lambda}{\mu} + \frac{\lambda^2}{\mu^2}}$$

Nakonec získáme hledaný stacionární koeficient pohotovosti K_p součtem pravděpodobností p_1 a p_2

$$K_p = p_1 + p_2 = \frac{\mu(\mu + 2\lambda)}{(\mu + \lambda)^2}$$

Je třeba si uvědomit, že v tomto příkladu můžeme pro určení K_p použít jednodušší model - paralelní spolehlivostní spojení dvou nezávislých modulů. Koeficienty pohotovosti jednotlivých modulů jsou

$$K_{p1} = K_{p2} = \frac{\mu}{\mu + \lambda}$$

Výsledný koeficient pohotovosti získáme ze vztahu pro pravděpodobnost bezporuchového provozu paralelního spojení dvou nezávislých modulů

$$K_p = K_{p1} + K_{p2} - K_{p1}K_{p2} = 2\frac{\mu}{\mu + \lambda} - \frac{\mu^2}{(\mu + \lambda)^2} = \frac{\mu(\mu + 2\lambda)}{(\mu + \lambda)^2}$$

Dále určíme střední dobu bezporuchového provozu T_s. Graf z obrázku 7.15a zjednodušíme na 2 stavy zavedením makrostavů S_p a S_o. Přitom bude $S_p = \{1, 2\}$ a $S_o = \{3\}$. Střední frekvence průchodů makrostavem S_p je $f_p = \lambda p_2$. Střední dobu bezporuchového provozu potom stanovíme s využitím dříve odvozených vzorců pro p_1 a p_2

$$T_s = \frac{p_p}{f_p} = \frac{p_1 + p_2}{\lambda p_2} = \frac{1}{\lambda} + \frac{\mu}{2\lambda^2}$$

Pokud by byla opravářská kapacita omezena na jednoho opraváře, dostaneme graf přechodů podle obrázku 7.15b. Děje probíhající v jednotlivých modulech už nejsou nezávislé, protože při souběhu poruch obou modulů jeden z nich čeká na zahájení opravy. Pokud je jeden ze dvou uvažovaných modulů použit jako nezatížená záloha, dostaneme graf přechodů podle obr. 7.15c. V žádné z obou uvedených modifikací příkladu 7.6 (obr. 7.15b a 7.15c) už ale nelze použít paralelní spolehlivostní spojení (chování modulů není nezávislé).

7.4 Simulační spolehlivostní modely

Pro určení spolehlivostních ukazatelů lze též použít metodu pravděpodobnostního modelování. V jednotlivých pokusech se sledují hodnoty realizací vybraných náhodných veličin (ukazatelů spolehlivosti), které se po provedení dostatečného počtu pokusů statisticky vyhodnotí. Postup pravděpodobnostního modelování předvedeme na příkladu.

Příklad 7.7

Uvažujme neobnovovaný systém se spolehlivostním schématem podle obr. 7.9. Jedná se o moduly A_1 a A_2 zapojené sériově. Záložní moduly A'_1 a A'_2 jsou stejného typu jako A_1 a A_2, nejsou zatížené a připojují se až po poruše svého hlavního modulu. Pro oba typy modulů známe pravděpodobnostní rozdělení času do poruchy modulu - tedy hustoty pravděpodobnosti poruch $f_1(t)$ a $f_2(t)$. Předpokládáme dále, že uvedená rozdělení nejsou exponenciální a tudíž intenzity poruch obou uvažovaných typů modulů nejsou konstantní. Zajímá nás střední doba bezporuchového provozu T_s a pravděpodobnost, s jakou nastane porucha dříve než v čase, který označíme t_1.

Takto zadanou úlohu neumíme jednoduše řešit s využitím dosud uvedených matematických modelů. Markovský model nejde přímo použít, protože intenzity poruch nejsou konstantní. Sériově-paralelní spolehlivostní spojení rovněž nejde použít, protože chování prvků není nezávislé (záložní moduly jsou nezatížené a připojí se až po poruše hlavního prvku).

Postup pravděpodobnostního modelování uvažovaného problému je velmi jednoduchý. Provedeme celkem N pokusů, číslo N bude řádu nejméně tisíců. V každém pokusu zjistíme konkrétní dobu τ_{si} do poruchy systému. Zavedeme proměnnou S, ke které budeme průběžně přičítat výsledky pokusů. Dále zavedeme čítač K, který budeme inkrementovat, pokud při pokusu vyjde $\tau_{si} < t_1$. Obě proměnné musí být před zahájením pokusů vynulovány. Při výpočtu výsledku i-tého pokusu budeme postupovat takto:

1. Pomocí generátoru náhodných čísel s rozdělením $f_1(t)$ vygenerujeme náhodná čísla τ_1 a τ'_1. Tato čísla mají význam doby do poruchy modulů A_1 a A'_1.

2. Pomocí generátoru s rozdělením $f_2(t)$ určíme náhodná čísla τ_2 a τ'_2.

3. Určíme dobu do poruchy systému τ_{si} podle vztahu

$$\tau_{si} = \min\{\tau_1 + \tau'_1,\ \tau_2 + \tau'_2\}$$

4. Výsledek pokusu přičteme k výsledkům předchozích pokusů, tedy $S \leftarrow S + \tau_{si}$.

5. Pokud platí $\tau_{si} < t_1$, inkrementujeme čítač K.

Po provedení všech N pokusů můžeme určit hledané výsledky. Hodnotu T_s určíme na základě vztahu (2.39) jako $T_s \doteq S/N$. Pravděpodobnost, že se

systém porouchá dříve než za čas t_1, určíme podle vzorce

$$\mathcal{P}\{\tau_{si} < t_1\} \doteq \frac{K}{N} \qquad \square$$

Uvedený příklad mimo jiné demonstruje hlavní výhodu simulačních spolehlivostních modelů. Jde o možnost poměrně jednoduchého použití jiného než exponenciálního rozdělení pravděpodobnosti doby do poruchy prvků i pro systémy se závislým chováním prvků. Dále i pro složité systémy nevzrůstá nadměrně složitost modelu (výpočetní složitost je úměrná počtu prvků a nikoliv počtu stavů). V případě potřeby můžeme model upřesnit zahrnutím dalších aspektů chování systému.

Na uvedeném příkladu lze rovněž ukázat, že některé spolehlivostní ukazatele nejde pomocí simulačního modelu efektivně určit. Chceme například ověřit, že uvažovaný systém se porouchá během použití (mise) v době trvání $t_1 = 10$ hodin (počítač v letadle) s pravděpodobností menší než 10^{-5} (což není nejpřísnější - na sto tisíc letů se připouští jedno selhání počítače - a v letadle není kritický jen počítač). Tato pravděpodobnost je v použitém příkladu dána poměrem K/N. Aby měl výsledek statistický význam, musí být K řádu alespoň desítky. Celkový počet pokusů N pak vychází řádově miliony. Kromě neúnosného nárůstu doby výpočtu se setkáme v podobných případech také s problémem, že výstupní množina generátorů náhodných čísel není ve skutečnosti spojitá a například testovaná podmínka $\tau_{si} < 10$) nemusí být (s ohledem na nespojitou výstupní množinu čísel použitých generátorů) splněna ani pro neomezený počet pokusů.