Spolehlivost elektronických systémů

studijní text frekventantů předmětu PV171

OBSAH

1 Úvod do problematiky řízení spolehlivosti

S problémem spolehlivosti nerůznějších přístrojů a zařízení se dostává do styku (a často též do konfliktu) téměř každý z nás ve svém denním životě. Uživatel většinou hodnotí spolehlivost podle toho, zda s ní je nebo není spokojen. Konstruktéři a výrobci jsou nuceni se spolehlivostí zabývat podstatně důkladněji, protože na jejich práci v převážné míře závisí, zda výrobek bude spolehlivý nebo ne. S pasivním přístupem ke spolehlivosti by se však ve skutečnosti neměl spokojovat ani uživatel, protože i on může svými znalostmi významně ovlivnit výslednou spolehlivost zařízení které používá. Měl by proto být schopen především kvalifikovaně ohodnotit spolehlivost, umět se rozhodnout, jakou spolehlivost skutečně potřebuje, měl by vědět, jak jí dosáhne a také co za ni zaplatí.

Některé základní úvahy, použitelné jako východisko při studiu spolehlivosti číslicových systémů, budou uvedeny v tomto skriptu. Pro potřeby exaktního popisu zavedeme několik pojmů, na které se v dalším textu budeme odvolávat, a popíšeme jejich vzájemné vztahy. Z dnes již velmi rozsáhlé teorie spolehlivosti tím samozřejmě pokryjeme jen nepatrný zlomek. Pro podrobnější studium teorie spolehlivosti je třeba obrátit se na některou ze specializovaných publikací, jichž je ve světové i naší technické literatuře dostatek, viz např. [*Bedn90*], [*Bill83*], [*Maix84*], [*Schn81*], [*Star82*], nebo [*Usak89*]

V průběhu rozpracování teorie spolehlivosti se postupně konstituovaly tři základní úlohy, jimiž se teorie spolehlivosti zabývá. Jedná se o následující disciplíny:

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

1.1 Definice spolehlivosti

Chceme-li mít možnost hodnotit a srovnávat spolehlivost systémů, musíme především definovat veličiny, v nich hodnotu spolehlivosti budeme udávat a v níž ji budeme měřit, protože spolehlivost jako taková není sama o sobě kvantifikovatelná i když ji téměř každý uživatel dokáže intuitivně popsat. 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“***.

Tato definice je doplněna několika vysvětlujícími poznámkami:

- Spolehlivost je komplexní vlastnost, která může zahrnovat např. bezporuchovost, životnost, udržovatelnost a skladovatelnost, buď jednotlivě nebo v kombinaci.
- Technickými podmínkami se rozumí souhrn specifikací technických vlastností, předepsaných pro požadovanou funkci objektu, dále způsoby jeho provozu, skladování, přepravy, údržby a opravy.
- Provozní ukazatele jsou ukazatele produktivity, rychlosti, spotřeby elektrické energie, paliva, apod.

Pro jednoznačnost diskuse by bylo vhodné upřesnit, co rozumíme pod pojmem ***objekt***. Je to zjevně velmi obecný pojem, jehož význam je možno chápat vždy podle toho, co právě zkoumáme. Do uvedené definice spolehlivosti lze za objekt dosadit libovolně malý nebo libovolně velký celek, který jsme schopni zkoumat současně. V číslicové technice to tedy může být součástka, obvod, funkční blok, jednotka, systém, apod.

Z citované definice lze vyvodit několik závěrů použitelných při studiu možností kvantitativního vyjádření spolehlivosti. Jako „***komplexní vlastnost***“ (zahrnující několik

různých hledisek) lze spolehlivost zřejmě stěží vyjádřit jednou číselnou hodnotou, která by nám umožnila uspořádat všechny objekty podle spolehlivosti. Přístup tvůrce normy je odlišný, namísto komplexní vlastnosti norma zavádí tzv. ukazatele spolehlivosti, což jsou veličiny, které lze jednotlivě vyhodnocovat. Ty jsou pak kvantitativním vyjádřením dílčích vlastností tvořících ve svém souhrnu spolehlivost.

Při studiu spolehlivosti se často budeme setkávat s pojmy ***porucha*** a ***chyba***. I když je jejich smysl intuitivně zřejmý, bude vhodné uvést jejich definice, protože mají pro další výklad klíčový význam. Ve smyslu citované názvoslovné normy:

Porucha je (angl. ***fault***) ***jev spočívající v ukončení schopnosti objektu plnit požadovanou funkci podle technických podmínek.***

Naproti tomu chyba je normou definována takto:

Chyba je (angl. ***error***) ***rozdíl mezi správnou a skutečnou hodnotou nějaké veličiny, zjištěný měřením nebo pozorováním***.

Z uvedených dvou definic vyplývá, že chyba je obvykle důsledkem nějaké poruchy, avšak každá porucha se nemusí nutně projevit jako chyba (např. nepoužívá-li se při provádění funkce žádná z poruchových součástek).

Velký počet různých typů poruch, které v číslicových systémech mohou nastat, vedl k vytvoření zjednodušené reprezentace poruch, k tzv. ***modelům poruch***. Nejběžnějším modelem jsou poruchy ***trvalé nula*** ($\mathbf{t_0}$) a ***trvalá jednička*** ($\mathbf{t_1}$), které symbolizují trvalou přítomnost konstantního napětí odpovídajícího jedné ze dvou logických úrovní. Tímto způsobem lze modelovat převážnou většinu fyzikálních poruch vznikajících v kontaktních (reléových) obvodech, pro něž byl původně vytvořen, a v polovodičových číslicových obvodech (především v obvodech typu TTL). Výjimku tvoří zkraty signálních vodičů , které je třeba modelovat jinak, viz např. [*Hlav82*]. Samostatný model vyžadují též poruchy ***trvale sepnuto*** a ***trvale přerušeno***, které jsou charakteristické pro obvody vyrobené technologií CMOS.

Při dalších úvahách budeme rozlišovat dva stavy objektu, a to ***poruchový*** (tj. stav, kdy porucha nastala) a ***bezporuchový*** (tj. stav kdy porucha nenastala). V nejednodušším 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 nesmírně 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, speciální vojenská zařízení, přístroje umístěné na odlehlých místech Země), nebo proto, že není opravován z organizačních důvodů (např. oprava není rentabilní). Tato hlediska hrají významnou roli zejména při specifikaci vlastností systémů odolných proti poruchám, a proto se k nim ještě vrátíme.

Se spolehlivostí velmi úzce souvisí i bezpečnost provozu systému. Obvykle bývá definována jako pravděpodobnost, že se na výstupu systému neobjeví nedetekovaná chyba

[*Cour76*], což nelze vyjádřit žádným spolehlivostním ukazatelem. Kromě vlastní pravděpodobnosti výskytu chyby tu totiž hraje významnou roli i pravděpodobnost její detekce. Zvýšené bezpečnosti systému se dosahuje použitím průběžných kontrol správnosti funkce systému. Metody kontroly lze rozdělit na:

- obvodové,
- programové,
- mikroprogramové,
- smíšené (hybridní, kdy se používají kombinace předchozích metod).

Nejběžnější jsou kontroly obvodové procující s pomocí:

- redundance (informační = bezpečnostní kódy, obvodová = zdvojování atd.),
- predikce následujícího stavu,
- kontrola časových sousledností.

Výstupem hlídačů průběžných kontrol lze ovlivnit činnost systému. Systém lze zastavit, lze modifikovat jeho činnost, rekonfigurovat používané prostředky a zdroje, degradovat výkonnost nebo funkce systému, případně zajistit vhodným způsobem zotavení po chybě.

Pokud výstupem hlídačů těchto kódů ovlivníme činnost systému, můžeme zabránit škodlivým důsledkům, které by v řízené soustavě měla nesprávná činnost elektronického systému.

Aplikace, při nichž na správné činnosti systému závisejí velké materiální hodnoty, případně lidské životy, obvykle vyžadují velkou bezpečnost i spolehlivost.

1.1.1 Číselné charakteristiky 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 (τ>0)**, pak její distribuční funkci **F(t)** lze vyjádřit vztahem **F(t)=P(τ>0)**, kde **P(A)** je pravděpodobnost jevu **A** a **t** je nezáporné reálné číslo. Distribuční funkce **F(t)** je neklesající a platí pro ni $\mathbf{0 \geq F(t) \geq 1}$ pro všechna **t**.

1.1.1.1 Pravděpodobnost poruchy

V teorii spolehlivosti je základní sledovanou náhodnou veličinou 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)**. Pravděpodobnost poruchy neobnovovaných objektů lze v základních úlohách vyčíslit na základě spolehlivostního experimentuje statistickým vztahem:

$$\overline{\mathbf{Q}}(\mathbf{t}) = \frac{\mathbf{n(t)}}{\mathbf{N_0}}$$

Legenda:

N_0 počet objektů na začátku spolehlivostního experimentu,
n(t) počet objektů s poruchou za dobu **t.**

1.1.1.2 Pravděpodobnost bezporuchového provozu

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 provozu*** (bezporuchového stavu) objektu v čase **t**. Platí následující vztah:

$$\mathbf{R(t) = 1 - Q(t)} \qquad 1.1$$

Pro určení pravděpodobnosti bezporuchového provozu neobnovovaného objektu na základě experimentů platí statistický vztah:

$$\overline{\mathbf{R}}\mathbf{(t)} = \frac{\mathbf{N_0 - n(t)}}{\mathbf{N_0}}$$

Legenda:

$\mathbf{N_0}$	počet objektů na začátku spolehlivostního experimentu,
n(t)	počet objektů s poruchou za dobu **t.**

V této souvislosti je třeba upozornit na jedno zjednodušení, které stále ještě přežívá z dřívější terminologie spolehlivosti a vyskytuje se především v překladech z anglosaské literatury. Je to ztotožnění spolehlivosti s pravděpodobností bezporuchového provozu. Pokud se v nějakém textu bez dalšího upřesnění vyskytne číselný údaj o spolehlivosti, jedná se zpravidla o hodnotu pravděpodobnosti bezporuchového provozu. V této knize však budeme oba uvedené pojmy rozlišovat.

1.1.1.3 Hustota pravděpodobnosti poruchy

Je-li náhodná veličina spojitá, lze odvodit další důležitou charakteristiku spolehlivosti, která se nazývá ***hustota pravděpodobnosti poruch*** - **a(t)** náhodné veličiny **t**. Je definována derivací distribuční funkce podle času, tedy pokud tato derivace existuje.

$$\mathbf{a(t)} = \frac{\mathbf{dQ(t)}}{\mathbf{dt}} \qquad 1.2$$

Veličina **a(t)** se v teorii spolehlivosti nazývá hustota poruch. Součin **a(t)dt** udává, s jakou pravděpodobností nastane ve sledovaném objektu porucha ve velmi krátkém intervalu **dt** následujícím za okamžikem **t**.

Pro určení hustoty pravděpodobnosti poruch neobnovovaného objektu na základě experimentů platí statistický vztah:

$$\overline{\mathbf{a}}\mathbf{(t)} = \frac{\mathbf{n(\Delta t)}}{\mathbf{N_0 * \Delta t}}$$

Legenda:

$\mathbf{N_0}$	počet objektů na začátku spolehlivostního experimentu,
$\mathbf{n(\Delta t)}$	počet objektů s poruchou za dobu **t**,
$\mathbf{\Delta t}$	časový interval měření.

1.1.1.4 Intenzita poruch

Další charakteristikou je ***intenzita poruch*** (intenzita pravděpodobnosti náhodné veličiny) definovaná vztahem:

$$\lambda\mathbf{(t)} = \frac{\mathbf{a(t)}}{\mathbf{R(t)}} = \frac{\mathbf{a(t)}}{\mathbf{1 - Q(t)}} \qquad 1.3$$

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 **dt** následujícím za časem **t**, je **λ(t)d(t)**.

Pro určení intenzity poruch neobnovovaného objektu na základě experimentů platí statistický vztah:

$$\bar{\lambda}(t) = \frac{n(\Delta t)}{N_{stř} \bullet \Delta t}$$

Legenda:

$N_{stř}$ střední hodnota počtu správně pracujících experimentálních objektů,

$$N_{stř} = \frac{N_i + N_{i+1}}{2}$$

$n(\Delta t)$ počet objektů s poruchou za dobu **t**,

Δt časový interval měření.

Ze vztahů (1.1) až (1.3) vyplývá, že dosud zavedené ukazatele spolu těsně souvisejí. Chceme-li tuto závislost explicitně vyjádřit, musíme postupně dosadit (1.1) do (1.2) a odtud do (1.3)

$$a(t) = -\frac{dR(t)}{dt}$$

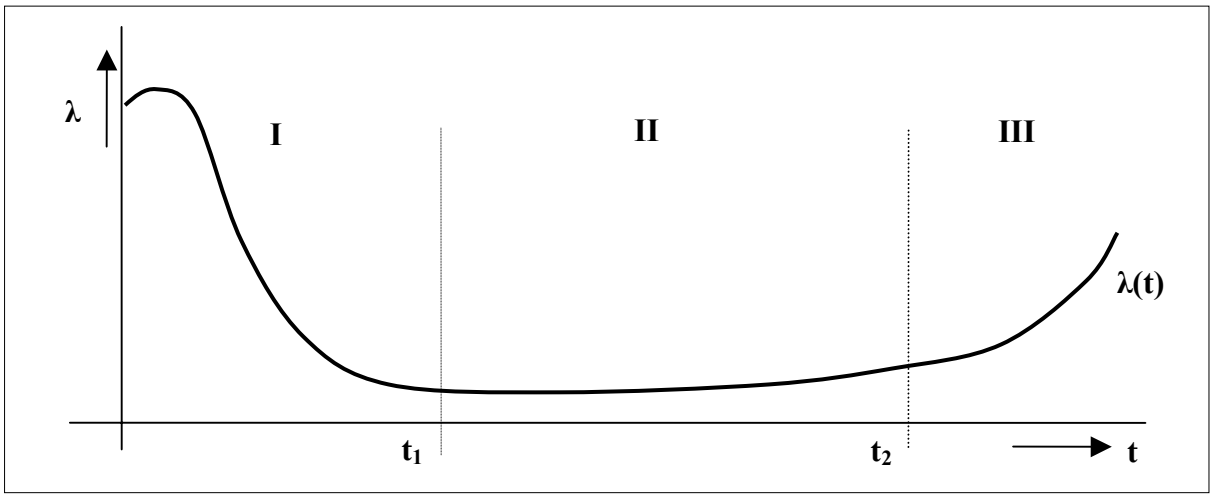
$$\lambda(t) = -\frac{dR(t)}{dt} * \frac{1}{R(t)} \qquad 1.4$$

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

Odvozenou diferenciální rovnici 1.4 můžeme upravit a řešit integrací:

$$R(t) = \exp(-\int_0^t \lambda(t)dt) \qquad 1.4$$

Pokud neznáme průběh intenzity poruch **λ(t)** v závislosti na čase, nemůžeme výraz (1.5) dále zjednodušit. Empiricky však bylo zjištěno, že průběh **λ(t)** obvykle odpovídá tzv. vanové křivce znázorněné na obr. 1.1.



Obr. 1.1 Průběh intenzity poruch v závislosti na čase

Pro elektronické součástky platí $t_1 \cong$ **6 až 10 týdnů** a $t_2 \cong$ **10 let**. V intervalu $\langle t_1, t_2 \rangle$, který označujeme jako období normálního provozu, platí, že **λ** má přibližně konstantní

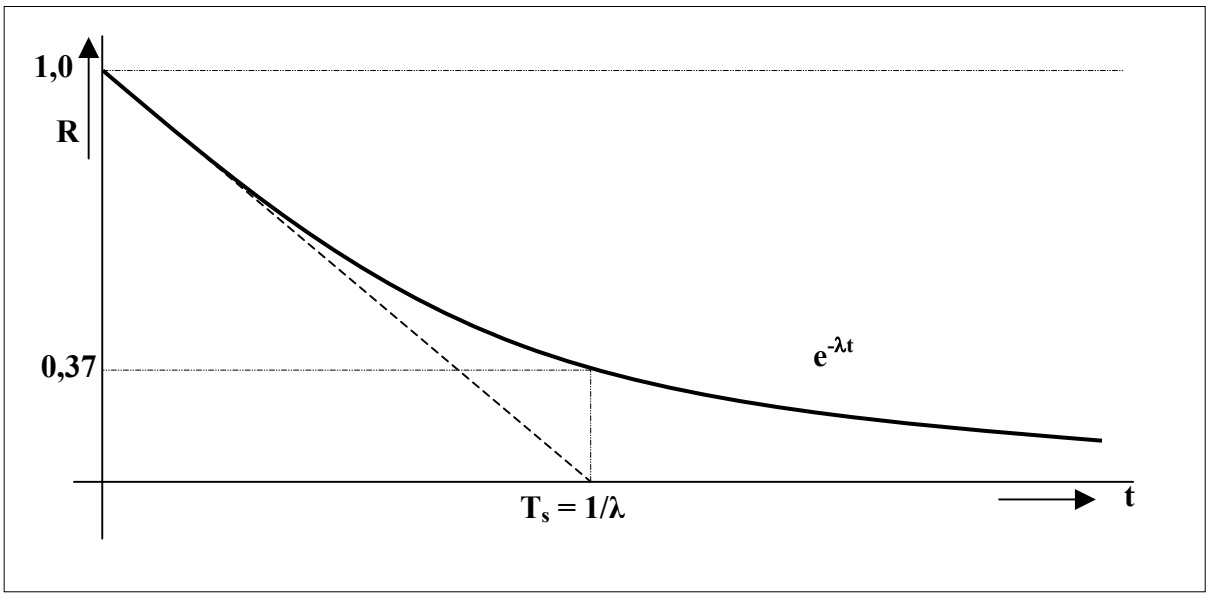
hodnotu. V takovém případě dokážeme integrál v (1.5) jednoduše vypočítat a po nahrazení funkce času konstantou dostaneme následující vztahy

$$\mathbf{R(t) = e^{-\lambda t}} \qquad 1.6$$

$$\mathbf{Q(t) = 1 - e^{-\lambda t}} \qquad 1.7$$

$$\mathbf{a(t) = \lambda \cdot e^{-\lambda t}} \qquad 1.8$$

Výrazy (1.6) až (1.8) popisují tzv. exponenciální rozdělení nebo exponenciální zákon poruch. Jeho grafickým vyjádřením je exponenciála (viz obr. 1.2), která pro **t = 0** má hodnotu **R(0) = 1.** Průběh 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.



Obr. 1.2. Průběh R(t) pro konstantní intenzitu poruch

Exponenciálu na obr. 1.2 lze interpretovat ještě jinak:
jestliže uvedeme v čase **t = 0** do provozu **n** objektů s konstantní intenzitou poruch **λ**, počet $\mathbf{n_b(t)}$ bezporuchových objektů se vlivem poruch bude v závislosti na čase zmenšovat po exponenciální křivce $\mathbf{n_b(t) = n^* e^{-\lambda t}}$.

Konstantní hodnota a exponenciální průběh R(t) budeme nadále předpokládat u všech prvků a podsystémů, jimiž se budeme zabývat. Skutečna hodnota, na níž se 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 na trhu standardní číslicové integrované obvody se pravděpodobnost bezporuchového provozu 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 (blíže viz odst. 1.2).

1.1.1.5 Střední doba bezporuchového provozu

Dalším důležitým ukazatelem je ***střední doba bezporuchového provozu*** - $\mathbf{T_s}$ (tj. střední hodnota sledované náhodné veličiny). 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:

$$\mathbf{Ts} = \int_0^\infty \mathbf{R(t)dt} \qquad 1.9$$

Pro neobnovované objekty se $\mathbf{T_s}$ nazývá také ***střední doba do*** (první) ***poruchy***. V anglosaské literatuře a jejích překladech se pro ni používá zkratka **MTTF** (*mean time to failure*).

Známe-li průběh **R(t)**, můžeme odvodit hodnotu $\mathbf{T_s}$ integrací podle (1.9). Pro exponenciální rozdělení tak dostaneme:

$$\mathbf{Ts} = \int_0^\infty \mathbf{e^{-\lambda t}dt} = \frac{\mathbf{1}}{\boldsymbol{\lambda}} \qquad 1.10$$

Tento jednoduchý vztah se často používá, avšak musíme si být stále vědomi jeho omezené platnosti. Kdybychom totiž do (1.10) mechanicky dosadili např. intenzitu poruch integrovaného obvodu $\boldsymbol{\lambda} = \mathbf{10^{-6}}$ 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 intenzita poruch má konstantní hodnotu (viz obr. 1.1, kde **t** mívá velikost řádově deset let), takže takový výpočet ztrácí reálný smysl. Musíme tedy počítat s tím, že jednotlivé elektronické součástky selhávají podstatně dříve, než po době $\mathbf{T_s}$ vypočtené podle (1.10).

1.1.2 Ukazatele spolehlivosti obnovovaných objektů

Obnovovaný objekt prochází během svého technického života posloupností stavů, která je schematicky znázorněna na obr. 1.3. Na vodorovné (časové) ose jsou vyznačeny okamžiky $\mathbf{t_i^p}$, kdy nastala index **i** znamená označení **i-té** poruchy a **t** okamžiky, kdy byla uskutečněná **i-tá** obnova bezporuchového stavu. Na svislé ose je naznačen stav objektu, přičemž $\mathbf{A_1}$ označuje bezporuchový a $\mathbf{A_0}$ poruchový stav. Předpokládáme, že na počátku provozu je objekt v bezporuchovém stavu. Délka trvání **i-tého** úseku bezporuchového provozu je označena $\boldsymbol{\tau_{pi}}$ a doba trvání **i-té** opravy $\boldsymbol{\tau_{oi}}$.

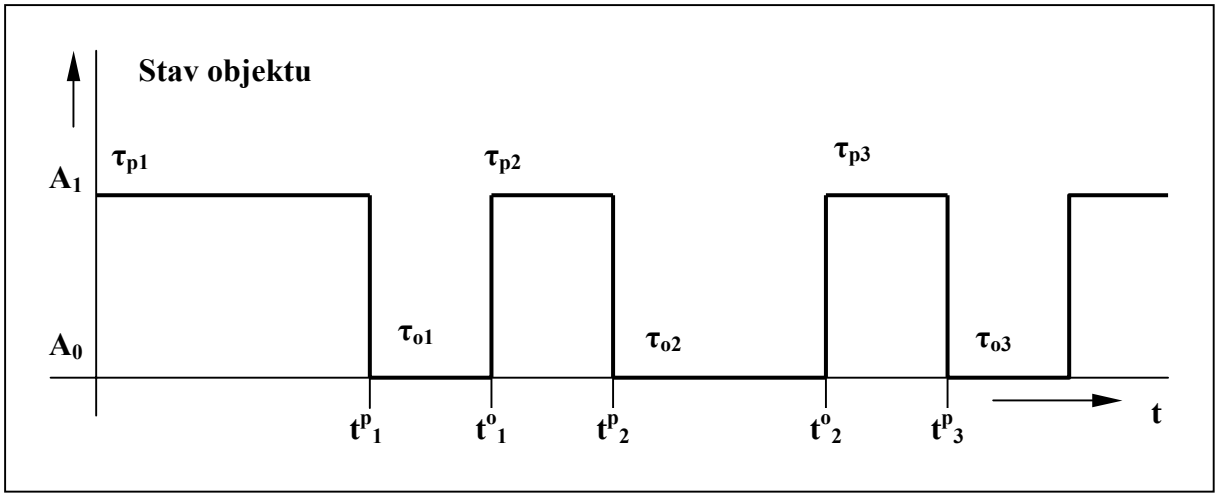
Pro obnovované objekty se místo parametru ***střední doby do poruchy*** používá číselná charakteristika ***střední doba mezi poruchami***. Stanoví se jako "aritmetický průměr všech naměřených dob bezporuchového provozu od skončení opravy do výskytu následující poruchy".

Tuto hodnotu získáme tak, že kumulativní dobu provozu **t**, vypočtenou jako součet všech dob provozu za sledované období dělíme počtem **n** výpadků způsobených poruchami. Platí:

$$\mathbf{T_s} = \frac{\mathbf{tp}}{\mathbf{n}} = \frac{\mathbf{1}}{\mathbf{n}} \sum_{\mathbf{i-1}}^{\mathbf{n}} \boldsymbol{\tau_{pi}} \qquad 1.11$$

Pro úplnost poznamenejme, že v anglosaské literatuře, např. [Bill83], se zavádí ukazatel ***MTBF*** (*mean time between failures*), který se počítá jako střední doba od jednoho výskytu poruchy do dalšího výskytu poruchy (od $\mathbf{t^0_i}$ do $\mathbf{t^0_{i+1}}$ na obr. 1.3.). Do této doby je pak zahrnuta i doba trvání opravy $\boldsymbol{\tau_{oi}}$, takže hodnota ***MTBF*** je větší, než hodnota $\mathbf{T_s}$, vypočtená podle vztahu (1.11). V tomto textu budeme střední hodnotu intervalu mezi dvěma po sobě následujícími poruchami označovat jako střední dobu cyklu $\mathbf{T_c}$.

Jako charakteristiky, vyjadřující okamžitou nebo dlouhodobou použitelnost opravovaného výpočetního systému, se používají **součinitel pohotovosti** (též koeficienty) a **součinitel prostoje** (v anglicky psané literatuře jsou označovány jako ***availability***).



Obr. 1.3. Sled stavů obnovovaného systému

Okamžitý součinitel pohotovosti - $\mathbf{K_p(t)}$ udává pravděpodobnost, že v čase **t** bude systém v provozuschopném stavu. Zpravidla existuje limita $\mathbf{K_p = \lim_{t\to\infty} K(t)}$, 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

$$\mathbf{K_p = \frac{t_p}{t_p + t_o}} \qquad 1.12$$

kde $\mathbf{t_p}$ je kumulativní doba provozu a $\mathbf{t_o}$ je kumulativní doba opravy během sledovaného období. Podobně jako v (1.11) můžeme zavést střední dobu opravy vztahem

$$\mathbf{T_o = \frac{t_o}{n}} \qquad 1.13$$

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 $\boldsymbol{\mu}$, označovaným jako intenzita oprav, platí

$$\mathbf{T_o = \frac{1}{\mu}} \qquad 1.14$$

Dosadíme-li do (1.12) postupně (1.11), (1.13) a (1.14), dostaneme

$$\mathbf{K_p = \frac{T_s}{T_s + T_o} = \frac{\mu}{\mu + \lambda}} \qquad 1.15$$

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

I když definice pravděpodobnosti bezporuchového provozu a součinitele pohotovosti vykazují určitou podobnost, nesmíme tyto dva pojmy zaměňovat. Pravděpodobnost bezporuchového provozu udává, s jakou pravděpodobností nedošlo k poruše po celý interval

<0,t>, zatímco pohotovost buď hodnotí stav v jednom náhodně zvoleném okamžiku (to platí pro okamžitý součinitel pohotovosti) nebo statisticky srovnává počet případů, kdy systém je a kdy není provozuschopný během celého sledovaného intervalu (stacionární součinitel pohotovosti). Požadavky vyjádřené hodnotou pravděpodobnosti bezporuchového provozu je tedy možno hodnotit jako podstatně přísnější než požadavky vyjádřené součinitelem pohotovosti.

Kromě součinitele pohotovosti se při hodnocení spolehlivosti obnovovaných systémů používá též ***součinitel technického využití*** - $\mathbf{K_{tv}}$ definovaný vztahem

$$\mathbf{K_{tv} = \frac{t_p}{t_p + t_o + t_u}} \qquad 1.16$$

Veličiny $\mathbf{t_p}$ a $\mathbf{t_o}$ zde mají stejný význam jako dříve a $\mathbf{t_u}$ je kumulativní doba plánované údržby.

1.1.3 Hodnoty ukazatelů spolehlivosti

Každý ukazatel spolehlivosti mění svou hodnotu v závislosti na velkém počtu vlivů. Řada těchto vlivů již byla empiricky zjištěna, avšak jejich analytické vyjádření není snadné. Na obr.1.1 je znázorněna např. závislost intenzity poruch na čase. Pro období normálního provozu se předpokládá její konstantní hodnota, avšak tento předpoklad je velmi zjednodušený. Na intenzitu poruch má vliv především zatížení, teplota, mechanické namáhání, pracovní prostředí, atd. Navíc je třeba počítat i s tím, že se hodnoty naměřené pro několik součástek stejného typu mohou značně lišit. Ještě významnější rozdíly zjistíme, začneme-li porovnávat výrobky vyrobené v různé době, případně pocházející od různých výrobců, protože zde hraje významnou roli úroveň technologie, kvalita surovin, úroveň vstupních, mezioperačních a výstupních kontrol, apod.

Je tedy velmi obtížné udávat „typické“ hodnoty platné pro určitý typ nebo dokonce skupinu typů výrobků. Zde musí přijít ke slovu matematická statistika, která nám dá k dispozici nejen prostředky pro odvození reprezentativních hodnot pro určitou skupinu objektů, ale hlavně poučení, jaké závěry můžeme z těchto hodnot vyvozovat. V úvodu jsme se však zmínili o tom, že tímto směrem se náš výklad nebude ubírat. Uvedeme zde jen stručný přehled typických hodnot intenzity poruch několika důležitých součástek, s nimiž se často setkáváme v číslicových systémech. Přehled by nám měl sloužit především jako základ pro odhady spolehlivostních ukazatelů nezálohovaných systémů a jejich částí. Pro práci s ním připomínáme, že uvedené hodnoty jsou pouze orientační a v každém konkrétním případě je musíme nahradit přesnějšími hodnotami dodanými výrobcem nebo získanými vlastním měřením.

V tab. 1.1, 1.2 a 1.3 jsou uvedeny střední hodnoty intenzity poruch podle [Mate85]. Jsou to hodnoty platné pro běžné provozní podmínky charakterizované teplotou okolí 50^{o}C, zatížením na 50% jmenovité hodnoty a pozemním neklimatizovaným prostředím. Při předběžném odhadu ukazatelů spolehlivosti můžeme tyto hodnoty dosadit např. do vzorců uvedených v kapitole 2.

1.2 Metody řízení spolehlivosti

Každý uživatel přirozeně požaduje co nejvyšší spolehlivost zařízení, které používá. Požadavek zvyšování spolehlivosti přitom obvykle implicitně zahrnuje současné zlepšení všech ukazatelů spolehlivosti, které je však většinou nerealizovatelné nebo realizovatelné jen v omezené míře. Výhodné je, když se nám podaří snížit hodnotu intenzity poruch **λ**, protože tím automaticky zlepšíme hodnoty všech důležitých ukazatelů spolehlivosti. To má za

následek zvýšení pravděpodobnost bezporuchového provozu, prodloužení střední doby bezporuchového provozu, zvýšení hodnoty součinitele pohotovosti, atd.). Takovýto zásah, který lze jednoznačně označit jako zvýšení spolehlivosti, je však nesmírně obtížný, protože metody snižování intenzity poruch jsou velmi složité a především nákladné.

TYP SOUČÁSTKY	INTENZITA PORUCH $\lambda[10^{-6}h^{-1}]$
bipolární číslicové SSI,MSI	
1 - 2 hradla	0,2
3 - 11 hradel	0,25
12 - 99 hradel	0,28 - 0,8
MOS číslicové	
1 - 2 hradla	0,3
3 - 11 hradel	0,4
12 - 99 hradel	0,5 - 2,3
lineární (hermetické)	
3 - 10 tranzistorů	0,3 - 0,55
11 - 100 tranzistorů	0,6 - 5,5
bipolární číslicové	
100 hradel	0,8
500 hradel	1,4
1000 hradel	2,3
2000 hradel	5,0
MOS číslicové LSI	
100 hradel	1,7
500 hradel	8,0
1000 hradel	35
2000 hradel	100

Tab. 1.1. Orientační hodnoty intenzity poruch integrovaných obvodů

INTENZITA PORUCH $\lambda[\ 10^{-6}\ h^{-1}]$	ROM bipol.	ROM MOS	RAM bipol.	RAM MOS
64 bitů	0,5	0,9	0,15	0,15
256 bitů	0,75	2,0	0,45	0,3
2k bity	1,7	7	4,0	2,0
16k bitů	5,5	50	30	12
64k bitů	20	250		50

Tab. 1.2. Orientační hodnoty intenzity poruch polovodičových pamětí

TYP SOUČÁSTKY	INTENZITA PORUCH λ [$10^{-6}h^{-1}$]
Tranzistory SI	
nízkovýkonové	0,02 - 0,75
výkonové	1,2 - 7,8
Diody SI	
nízkovýkonové	0,016 - 0,27
výkonové	0,16 - 0,5
Odpory	
vrstvové uhlíkové	0,02 - 0,05
Kondenzátory	
papírové	0,07
polystyrénové	0,35
polyesterové	0,05
slídové	0,02
keramické	0,005 - 0,04
elektrolytické	0,03 - 0,4
hliníkové	0,13 - 0,7
Relé	0,4 - 1,3
Konektory (50 kontaktních párů)	0,05 - 0,6
Spoje (1 spoj)	
ovíjené	0,000 005
pájené vlnou	0,0012 - 0,1
pájené ručně	0,01
Optické kabely (1 km)	
jednovláknové	0,1

Tab. 1.3. Orientační hodnoty intenzity poruch diskrétních součástek

Pro metody a opatření vedoucí ke snižování intenzity poruch se vžilo souhrnné označení ***předcházení poruchám*** (angl. *fault avoidance*). Použitelnost těchto metod je omezená proto, že od jisté úrovně rostou náklady spojené s dalším snižováním intenzity poruch neúměrně rychle a také proto, že se vyskytují objektivní fyzikální překážky, jejichž překonání se vymyká našim možnostem, resp. znalostem.

V takové situaci je třeba hledat jiné možnosti zlepšování hodnot ukazatelů spolehlivosti. Jednou z nich je možnost vzít výskyt poruch v úvahu a respektovat ho při návrhu a realizaci systému. Smíříme se tedy s tím, že k poruchám součástek bude docházet i nadále, ale dosáhneme toho, že se tyto poruchy nebudou projevovat na chování systému, případně se budou projevovat jen minimálně. Tento způsob reakce na poruchy se nazývá ***odolnost proti poruchám*** nebo ***tolerance poruch*** (angl. *fault tolerance*) a systém, který je takové reakce schopen, je ***systém odolný proti poruchám*** (angl. *fault-tolerant system*). Při hodnocení spolehlivosti systému odolného proti poruchám pak musíme rozlišovat mezi poruchou součástky a poruchou systému, označovanou též jako ***selhání systému*** (angl. *failure*). Za poruchu systému považujeme pouze takovou poruchu jeho součástek, která způsobí nepřijatelnou změnu chování, takže je ve smyslu definice poruchy z ods. 1.1 ukončena schopnost systému jako celku plnit požadovanou funkci. Odpovídajícím způsobem pak musíme upravit i metodu výpočtu hodnot jednotlivých ukazatelů spolehlivosti (např.

střední doba mezi poruchami bude měřena výlučně na základě poruch systému jako celku, apod.).

Společnou vlastností všech metod tolerance poruch je nerovnoměrnost jejich vlivu na jednotlivé ukazatele spolehlivosti. To znamená, že pro zlepšení hodnoty jednoho ukazatele máme k dispozici určité metody, které mohou hodnotu jiného ukazatele buď zlepšit jen v omezené míře, nebo ponechat beze změny, či dokonce zhoršit. Vhodná metoda se pak volí jako kompromis mezi požadavky kladenými na hodnoty různých ukazatelů spolehlivosti a je ovlivněna ještě dalšími omezujícími podmínkami, jako je cena, hmotnost, rozměry, spotřeba energie, apod. V takovém případě tedy nemůžeme zaručit zlepšení všech ukazatelů spolehlivosti současně, takže by nebylo správné mluvit zjednodušeně o zvyšování spolehlivosti. Budeme proto používat obecnější výraz řízení spolehlivosti.

1.2.1 Předcházení poruchám

Metody předcházení poruchám byly již teoreticky podrobně rozpracovány, avšak s jejich uplatněním v praxi stále nemůžeme být spokojeni. je to způsobeno především překážkami organizační povahy, případně ekonomickými hledisky. Navíc stojí v cestě i zmíněné fyzikální překážky. Víme, že pro projekty, v nichž jsou na spolehlivost kladeny extrémní požadavky, jsou výrobci schopni zajistit - za příslušnou cenu - spolehlivostní ukazatele o několik řádů lepší, než je běžný standard. S takovou extrémní spolehlivostí však konstruktér nemůže při běžných projektech počítat. Přesto existuje řada metod, jak u sériově vyráběných součástek zaručit co nejvyšší *„rozumně“* dosažitelnou spolehlivost. Tyto metody nelze přehlížet jako překonané nebo dokonce nepotřebné, protože můžeme velmi snadno dokázat, že tolerovat lze vždy jen omezený počet poruch. Nejprve tedy musíme využít všech dosažitelných prostředků předcházení poruchám, a pouze na zbývající poruchy uplatnit metody tolerance. S nejdůležitějšími metodami předcházení poruchám se proto musí seznámit každý odborník bez ohledu na to, jaké metody řízení spolehlivosti bude používat.

Poruchám lze předcházet při návrhu, výrobě i provozu systému. Při návrhu je třeba především volit spolehlivou součástkovou základnu a spolehlivou technologii. V obou případech musíme brát v úvahu podmínky, v nichž bude výsledný systém pracovat. Kromě toho je třeba volit optimální pracovní bod všech součástek z hlediska výkonu (nevyčerpávat povolené zatížení výstupů), tepelného režimu (zajistit dostatečné chlazení), napájení, odrušení, pracovní frekvence, apod.

Při výrobě hraje klíčovou roli vstupní kontrola součástek, polotovarů a použitých materiálů. Důležitost vstupní kontroly vyplývá z výsledků řady prováděných rozborů a statistických výzkumů. Např. podle (Siew82) vyřazovala firma DEC (v současné době sloučená do firmy COMPAQ) při vstupní kontrole 2,5 % všech součástek, které pocházejí od subdodavatelů. Mezi převzatými součástkami pak zůstává jen 0,04 % vadných. Cenu, kterou za takto dokonalou vstupní kontrolu zaplatí uživatel, je možné chápat též jako cenu za zvyšování spolehlivosti. Sami výrobci se snaží zajišťovat spolehlivost především velkou technologickou kázní, sledovat průběžnými (mezioperačními) kontrolami. Výsledné výrobky se navíc podrobují tzv. spolehlivostním testům, při nichž se zkoušejí při zvýšené, případně snížené teplotě, při zvýšeném napětí, při vibracích, apod.

Z hlediska předcházení poruchám jsou velmi účinné různé teplotní cykly, protože při nich se projeví skryté poruchy, které by jinak mohly ovlivnit funkci výrobku až během jeho použití. Z hlediska průběhu intenzity poruch podle obr. 1.1 to znamená, že se snažíme podstatně zkrátit první úsek křivky (období časných poruch) a při montáži pak používat již jen součástky s konstantní intenzitou poruch. Při tom je však třeba podrobně znát fyzikální děje, které probíhají v testovaných součástkách, a pečlivě jim přizpůsobit teplotní režim.

Neodborně a především nedbale prováděné teplotní cykly (např. bez možnosti přesně nastavovat a měřit pracovní teploty) mohou naopak snížit spolehlivost, protože způsobí vznik nových degradačních mechanismů, které se projeví až při použití součástky.

K významným metodám předcházení poruchám patří i zvyšování stupně integrace polovodičových součástek. Vývody pouzdra patří k nejporuchovějším částem integrovaných obvodů, takže snížením počtu pouzder ubývá nespolehlivých míst. Navíc odpadá i poruchové propojování plošnými spoji a zmenšuje se tepelné vyzařování (ubývá výstupních budičů).

Z hlediska provozu je pro předcházení poruchám nejdůležitější dodržování technických podmínek. Mezi ně patří požadavky na:

- klimatizaci (teplota, vlhkost a prašnost vzduchu),
- intenzitu rušení (ze sítě i přímým vyzařováním ze zdrojů),
- stabilitu napájení, apod.

Navíc je třeba zajistit pravidelnou profylaxi a opravy v souhlase s předpisy výrobce. Vzhledem k tomu, že se na výpadcích systému významnou měrou podílí i vliv lidského činitele, je třeba omezit možnosti jeho chybných zásahů. Toho se dosahuje čitelným a srozumitelným označením ovládacích prvků, vytvořením kvalitní dokumentace a převedením komunikace člověka s počítačem do takové formy, která je člověku blízká a srozumitelná (přirozený jazyk, grafické symboly, apod.).

1.2.2 Odolnost proti poruchám

Systém se označuje jako odolný proti poruchám, jestliže je schopen správně vykonávat svou funkci i v přítomnosti poruch technického vybavení nebo chyb v programech. Protože však termín „správně vykonávat funkci“ lze chápat různě, je třeba upřesnit, kdy je funkce považována za správně vykonanou. Obvykle se vyžaduje splnění těchto tří podmínek:

- zpracování dat nebylo zastaveno ani zaměněno v důsledku poruchy,
- výsledek je správný,
- výsledek byl získán v předepsané době.

Jsou-li splněny pouze některé z uvedených tří požadavků (např. výsledek je správný, ale byl dodán opožděně), označuje se systém jako ***částečně odolný proti poruchám***. První požadavek, tedy zachování funkceschopnosti programu, se ovšem považuje za dominantní, takže musí být splněn i v systémech, které jsou odolné jen částečně.

Během práce na projektech systémů odolných proti poruchám, z nichž mnohé byly realizovány a vyzkoušeny v praxi , se vyvinula poměrně dobře propracovaná metodika návrhu [Aviz86]. Je to ovšem heuristický postup založený na postupných aproximacích výsledku, takže jeho aplikace vyžaduje značnou míru zručnosti a zkušeností. Navíc nikdy nelze předem rozhodnout, zda dosáhneme cíle, který jsme si zvolili. V současné době však tento postup představuje nejlepší metodu, která byla na základě dosavadních znalostí zformována.

Návrh systému odolného proti poruchám vychází obvykle z tzv. neodolného systému, tedy systému navrženého s minimálními prostředky, které splňují dané požadavky na funkci. Tento prvotní tvar systému se pak dále zdokonaluje postupnými obměnami a doplňky tak, aby se co nejvíce přiblížil ideálnímu stavu splňujícímu všechny požadavky na spolehlivost při dodržení omezujících podmínek.

Hlavní fáze, kterými návrh systému odolného proti poruchám prochází, jsou tyto:

1) stanovení cílů,
2) volba metod detekce poruch,
3) návrh algoritmů zotavení po poruše,

4) vyhodnocení odolnosti proti poruchám.

V první fázi je třeba vytvořit především jasně formulované ***zadání projektu***. Vzhledem k tomu, že žádný systém nemůže být odolný proti „všemu, co může selhat“, je třeba přesně specifikovat všechny situace, v nichž si systém má zachovat funkceschopnost. Prakticky to znamená sestavit co nejúplnější seznam poruch, které při provozu systému mohou nastat, a roztřídit je podle pravděpodobnosti výskytu, případně podle toho, jak na ně systém má reagovat. Pokud v některých případech připustíme, aby jeho funkceschopnost byla omezená, musíme dostatečně přesně charakterizovat všechny přípustné změny, např. pokles výkonnosti, prodloužení doby reakce, omezení repertoáru funkcí, které systém dokáže vykonávat, apod.

Dále musíme stanovit mezní hodnoty ukazatelů spolehlivosti pro výsledný systém. Tyto hodnoty se často vztahují k určitým specifickým typům poruch (např. omezujeme střední dobu do poruchy opravitelné za provozu), nebo k jednotlivým dílčím funkcím systému. Proto je třeba hned na začátku projektu stanovit metodiku, podle níž se bude hodnotit dosažený stupeň odolnosti výsledného systému proti poruchám. K této otázce se podrobněji vrátíme při upřesnění čtvrté fáze popisované metody návrhu.

Detekce poruch má při zajišťování odolnosti klíčový význam, protože systém je schopen správně reagovat pouze na ty poruchy, o nichž je dostatečně přesně informován. Při volbě metod detekce poruch je třeba vzít v úvahu, jaké typy poruch se v systému mohou vyskytnout (při tom můžeme použít seznam sestavený během první fáze návrhu), jak rychle má systém na jednotlivé typy poruch reagovat, jaké prostředky jsou již v systému k dispozici, atd. Metodami a prostředky detekce poruch se zabývá diagnostika číslicových systémů, jíž byla věnována řada specializovaných publikací, mimo jiné též kniha [Hlav82]. Zde se proto omezíme jen na stručnou rekapitulaci nejdůležitějších poznatků.

Diagnostika, používaná v číslicových systémech odolných proti poruchám, můžeme mít jednu z těchto čtyř forem:

- spouštěcí diagnostika,
- periodická diagnostika,
- průběžná diagnostika,
- diagnostika redundantních částí.

Spouštěcí diagnostika je soubor diagnostických testů spouštěných automaticky při zapnutí napájecího napětí. Jejich úkolem je prověřit v co nejkratší době všechny důležité funkce systému a signalizovat případnou poruchu obsluze. Jsou to tedy pouze detekční testy, které navíc často nebývají úplné, především tehdy, když aplikace nedovoluje příliš odkládat okamžik zahájení provozu systému.

Periodická diagnostika se provádí v přestávkách mezi aplikačními programy. Po dobu testu tedy musí být výpočet na určitou dobu přerušen, aby systém mohl být podroben testu. Výsledkem takového testu je úplná informace o technickém stavu testované jednotky v okamžiku provedení testu. Není však zaručeno, že se tento stav nezmění ani během následujícího výpočtu až do okamžiku příštího testu. Proto je třeba volit periodicitu testů tak, aby pravděpodobnost vzniku poruchy mezi dvěma po sobě následujícími provedeními testů byla dostatečně malá.

Průběžná diagnostika představuje nepřetržitý zdroj informací o správnosti operací prováděných v systému a je v podstatě totožná se zabezpečením systému proti poruchám. Obvykle je založena na kontrole správnosti bezpečnostního kódu. Hlavní výhodou průběžné diagnostiky realizované tímto způsobem je její časová nenáročnost (výpočet se nepřerušuje

ani nezpomaluje) a velmi jednoduché řízení. Průběžná diagnostika však může být realizována i jinou formou kontroly správnosti výsledku, např. kontrolním výpočtem probíhajícím v jiném procesu, opakovaným výpočtem ve stejném procesu , jednoduchou kontrolou důležitých vlastností získaného výsledku (např. porovnáním s mezními hodnotami), apod.

Velmi oblíbeným prostředkem kontroly správné funkce číslicových systémů, zejména pokud jsou použity při řízení v reálném čase, je tzv. hlídací časovač (angl. *watchdog timer*), někdy nazývány také diagnostické hodiny [Hude85]. Je to v podstatě čítač, který v předem stanovených intervalech pravidelně přerušuje činnost procesoru a vyžaduje obsluhu (nulování nebo nastavení výchozí hodnoty). Jestliže procesor nezareaguje správně a předepsaném čase, signalizuje hlídací časovač poruchu, případně přímo vyvolá zotavení po poruše.

Určitou nevýhodou průběžné diagnostiky je závislost rozsahu získané informace o technickém stavu objektu na řešeném problému, protože průběžná diagnostika signalizuje jen takové poruchy na které je navržena (které byly vybrány jako pravděpodobné, že by mohly nepříznivě ovlivnit výpočet).

Obvod pracující s bezpečnostně kódovanými informacemi, jejichž správnost se kontroluje hlídačem kódu, se nazývá samočinně kontrolovaný (*self - checking*). Z hlediska kvality diagnostiky je však účelné, aby obvod byl schopen ovlivnit jeho funkci. Takový obvod se nazývá úplně samočinně kontrolovaný (*totally self - checking*, zkratka ***TSC***). Formálně se úplně samočinně kontrolovaný obvod definuje jako samočinně testovaný a současně bezpečný proti poruchám. Obvod je samočinně testovaný, jestliže vektory převedené na jeho vstupy během normálního provozu tvoří úplný diagnostický test. Bezpečný proti poruchám je obvod, v němž lze poruchu, která způsobí chybu výstupního signálu, zjistit na základě kontroly správnosti kódu výstupu.

Redundantní části se diagnostikují proto, že bez informací o technickém stavu záložních prvků bychom riskovali, že některý z těchto prvků bude nepoužitelný ve chvíli, kdy bychom na něj potřebovali přenést funkci. Záložní prvky jsou většinou vystaveny stejným podmínkám jako prvky provádějící vlastní řízení (i když většinou jsou bez zátěže nebo jejich pracovní zátěž je menší), takže u nich *nemůžeme* předpokládat nulovou intenzitu poruch.

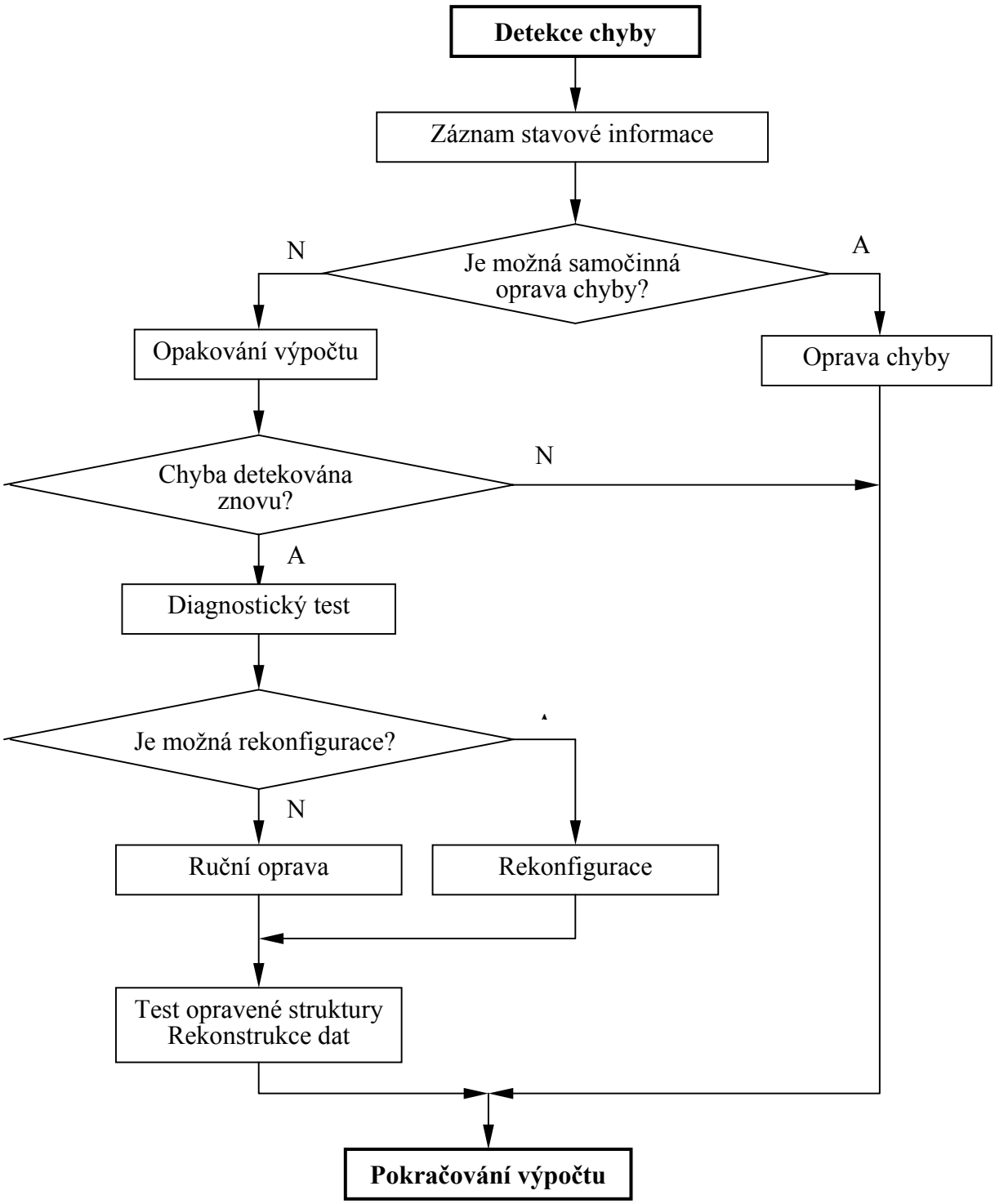
Zotavení po poruše zahrnuje všechny úkony, které je třeba provést od okamžiku zjištění poruchy do obnovení funkce systému. Zotavení je vlastně hlavním nástrojem odolnosti proti poruchám, a proto má určující význam pro kvalitu výsledného systému. Průběh zotavení po poruše určuje, jak bude systém reagovat na poruchu. Podle výsledků můžeme rozlišovat tři úrovně zotavení:

- zotavení do původní úrovně funkceschopnosti,
- zotavení do degradovaného stavu,
- bezpečné ukončení funkce.

Obecný tvar vývojového diagramu zotavení po poruše je znázorněn na obr. 1.4. Pro úplnost je třeba připomenout, že k zotavovacím mechanismům v obecném slova smyslu patří i obvodové maskování chyby, i když při něm k detekci poruch nedochází. Tato nejdokonalejší, nejrychlejší, ale též nejnákladnější forma zotavení je výhodná tím, že porucha se neprojeví chybou na výstupu systému.

Vyhodnocení odolnosti proti poruchám je kontrolou, do jaké míry se nám podařilo splnit zadání. Protože s formulací požadavků na odolnost i s jejich ověřováním jsou zatím poměrně malé zkušenosti, je třeba dbát na to, aby při hodnocení byla použita stejná kritéria jako při formulaci zadání. Používají se analytické metody hodnocení, tj. výpočet, dále simulační metody a ověřování na funkčním vzoru. Kromě číselných hodnot vybraných

ukazatelů spolehlivosti se hodnotí též některé další vlastnosti, které se spolehlivostními ukazateli souvisejí jen nepřímo (úspěšnost zotavení, pokrytí poruch, schopnost reakce na změněné pracovní podmínky, apod.). Používá-li systém též zotavení do degradovaného stavu, vyhodnocuje se i pravděpodobnost přechodu na různé úrovně výkonnosti.



Obr. 1.4. Vývojový diagram zotavení po chybě

1.2.2.1 Součinitel zvýšení spolehlivosti

Pro názornost je účelné určit také relativní změny hodnot některých důležitých ukazatelů. K tomu se zavádějí různé pomocné součinitele, jako např. ***součinitel zvýšení spolehlivosti*** nebo ***součinitel prodloužení mise***. Součinitel zvýšení spolehlivosti $\mathbf{K_R(t)}$ je definován vztahem

$$\mathbf{K_R(t) = \frac{R_z(t)}{R(t)}} \qquad 1.17$$

tedy jako podíl pravděpodobnostní bezporuchového provozu zálohovaného a nezálohovaného systému v době **t**.

1.2.2.2 Součinitel prodloužení mise

Součinitel prodloužení mise udává, kolikrát se prodlouží doba, během níž pravděpodobnost bezporuchového provozu poklesne pod stanovenou mezní hodnotu $\mathbf{R_{min}}$. Je-li $\mathbf{T(R_{min})}$ doba poklesu pravděpodobnosti nezálohovaného systému na $\mathbf{R_{min}}$ a $\mathbf{T_z(R_{min})}$ doba stejného poklesu pravděpodobnosti pro zálohovaný systém, je součinitel prodloužení mise $\mathbf{K_T(R_{min})}$ definován vztahem

$$\mathbf{K_T(R_{min}) = \frac{T_z(R_{min})}{T(R_{min})}} \qquad 1.18$$

Po vyhodnocení odolnosti výsledného systému musí následovat zdokonalování a upřesňování projektu, protože zjištěné hodnoty většinou nevyhovují zadání. Projekt se zdokonaluje použitím jiného typu nebo rozsahu zálohy, jiného způsobu jejího řízení, apod. Každé zdokonalení je třeba znovu vyhodnotit a porovnat se zadáním. Pokud dosažené vlastnosti stále nevyhovují požadavkům, následuje další zdokonalení , atd. Tento iterativní postup končí buď tím, že se dostatečně přiblížíme zadání, nebo zjištěním, že za daných podmínek a pomocí prostředků, které máme k dispozici, nelze požadovaných vlastností dosáhnout. V takovém případě musíme zadání upravit a přizpůsobit tak požadavky reálným možnostem.

1.3 Oblasti využití systémů odolných proti poruchám

Odolnost proti poruchám byla donedávna výsadní vlastností systémů používaných v několika privilegovaných oborech, např. v kosmonautice, letectví nebo ve vojenské technice. S poklesem ceny, rozměrů a energetické náročnosti elektronických systémů však odolnost proti poruchám postupně proniká do řady dalších aplikačních oblastí, takže již zdaleka není ničím výjimečným. Za všechny příklady, dokumentující její potřebnost , uveďme alespoň jeden, který je velmi přesvědčivý.

Dne 22. listopadu 1985 utrpěla Bank of New York během půl druhé hodiny ztrátu 5 miliónů dolarů jen proto, že v jejím ústředním počítači se vyskytla porucha, které si nikdo nevšiml [Anal86]. Počítač totiž začal vyzvedávat peníze z konta u centrální banky a během uvedené doby si stačil „vypůjčit“ 32 miliardy dolarů. I když dlužná částka byla při nejbližší příležitosti vrácena, musela Bank of New York zaplatit za tuto neobvyklou výpůjčku úroky, které představovaly vzniklou ztrátu. Kdyby počítač použitý ve zmíněné bance byl odolný proti poruchám, k takovému omylu by s největší pravděpodobností nemohlo dojít.

Uvedený příklad, stejně jako mnoho podobných, které můžeme najít v tisku, dokazuje, jak je každodenní život v hospodářsky vyspělých zemích závislý na počítačích. Z toho, jak velké škody může jejich případné selhání způsobit, lze odvodit, jak velkou částku se vyplatí investovat do zajištění jejich odolnosti proti poruchám. Při aplikacích v oblasti financí je

takový výpočet poměrně jednoduchý, protože potenciální ztráty jsou přímo vyjádřeny v měnových jednotkách a lze je tedy velmi snadno srovnat s pořizovacími, případně udržovacími náklady na výpočetní techniku. Poměrně přehledné jsou i vztahy ve výrobní sféře a ve službách, protože i zde můžeme porovnávat měnové jednotky. Složitější situace ale nastává tam, kde je v sázce zdraví, nebo politické důsledky, apod. Zde jsme obvykle nuceni vzdát se přesných kalkulací, protože uvedené hodnoty lze těžko vyčíslit (i když pojišťovny mají sazebník i pro tyto kategorie). Klesající cena a snadná dostupnost systémů odolných proti poruchám však usnadňují rozhodování, protože díky jim lze tyto systémy použít i v případech, které by donedávna byly považovány za sporné.

Podle povahy řešeného problému lze úlohy vyžadující použití počítačů odolných proti poruchám rozdělit do několika aplikačních oblastí. Mezi nejrozsáhlejší patří *řízení v reálném čase* a *zpracování transakcí ve spřaženém režimu*. Kromě toho existuje velké množství speciálních oblastí, pro které se většinou používají systémy odvozené z uvedených hlavních kategorií.

Řízení v reálném čase se využívá především ve výrobní sféře (při řízení technologických procesů), v dopravě (včetně kosmických letů), v lékařství, apod. Tyto aplikace kladou vysoké nároky na hodnotu pravděpodobnosti bezporuchového provozu, zatímco hodnoty ostatních ukazatelů spolehlivosti (včetně střední doby bezporuchového provozu) většinou nejsou považovány za kritické. Systémy používané pro tento typ aplikací se někdy zjednodušeně označují jako ***vysoce spolehlivé***.

Zpracování transakcí ve spřaženém režimu se využívá především v bankách, spořitelnách, pojišťovnách, na poštách , ve zdravotnické službě, při rezervaci místenek na nejrůznější dopravní prostředky a v mnoha dalších aplikacích vyžadujících styk s bázemi dat. Do této kategorie patří též systémy používané v telekomunikacích, zejména pro číslicové řízení telefonních ústředen. Většina těchto úloh vyžaduje především velkou pohotovost. Naproti tomu krátkodobý výpadek systému není považován za kritický, takže pro pravděpodobnost bezporuchového provozu většinou nejsou vyžádány extrémní hodnoty. Systémy této kategorie se zjednodušeně nazývají ***vysoce pohotové***.

Další důležitou kategorii systémů odolných proti poruchám představují systémy, u nichž jsou kladeny značné nároky na hodnotu střední doby bezporuchového provozu. Patří sem například tzv. ***systémy s odloženou údržbou***, u nichž je pevně stanovena doba, během níž nelze provádět údržbu. Typickým reprezentantem této kategorie jsou palubní počítače letadel. Další speciální aplikační oblast představují systémy s dlouhou životností, u nichž se s údržbou nepočítá vůbec. Jsou to např. počítače pro nepilotované kosmické lety, nepřístupné pozemní nebo podmořské stanice, apod.

Závěrem je třeba zdůraznit, že uvedený výčet je provizorní, protože počet oblastí, v nichž se uplatňují systémy odolné proti poruchám, se neustále zvětšuje. Každý úspěch totiž vyvolává snahu vyzkoušet výhody odolnosti proti poruchám i v dalších oblastech, což je značně usnadňováno celkovým rozvojem výpočetní techniky.

2 Hodnocení spolehlivosti číslicových systémů

Základní úlohu při predikci spolehlivosti systému je určení hodnot jeho celkových spolehlivostních ukazatelů ze známých hodnot spolehlivostních ukazatelů prvků a ze způsobu jejich spojení. Uvedená úloha se řeší s využitím spolehlivostních modelů. Existuje velké množství různých spolehlivostních modelů. Účelem této kapitoly není podat jejich vyčerpávající přehled, ale spíše seznámit čtenáře s nejdůležitějšími typy modelů a dále s metodikou jejich konstrukce a řešení. Podrobněji je probírána teorie a využití Markovských modelů, které jsou základem moderních modelovacích technik v oblasti spolehlivosti výpočetních systémů.

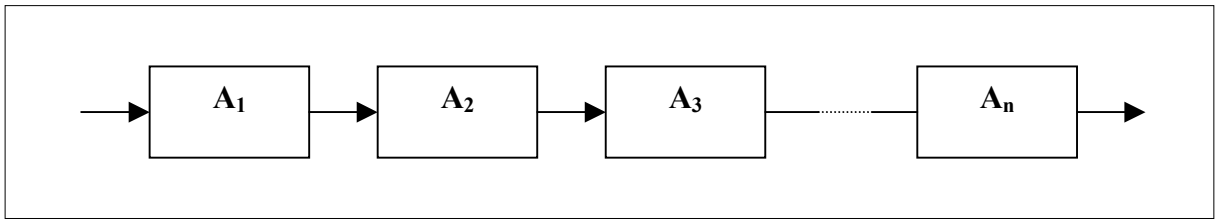
Vytvoření modelu je vždy spojeno se zjednodušením modelované skutečnosti, protože abstrahuje od vlastností objektu, které nejsou pro sledovaný účel podstatné. Ve spolehlivostních modelech proto zpravidla rozlišujeme pouze stavy systému důležité z hlediska jeho spolehlivosti (provozuschopný nebo porouchaný). V některých případech se dále uvažují stavy se sníženou bezpečností provozu nebo se sníženým výkonem.

2.1 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 dáme 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 modely využívané zejména pro neobnovované systémy.

2.1.1 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. 2.1.



Obr. 2.1. Sériový spolehlivostní model

Jestliže známe pravděpodobnosti bezporuchového provozu $\mathbf{R_i(t)}$ pro každý prvek $\mathbf{A_i}$, je výsledná pravděpodobnost bezporuchového provozu **R(t)** dána jejich součinem.

$$\mathbf{R(t)} = \prod_{i=1}^{n} \mathbf{R_i(t)} \tag{2.1}$$

Pro konstantní intenzitu poruch λ_i každého prvku dostaneme

$$\mathbf{R(t)} = \prod_{i=1}^{n} \mathbf{e}^{-\lambda_i t} = \mathbf{e}^{-\lambda t} \tag{2.2}$$

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

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{2.3}$$

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 $\mathbf{T_s}$ získáme z (2.2) integrací podle (1.9). Pro konstantní intenzity poruch λ_i dostaneme

$$\mathbf{T_s} = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\lambda} \tag{2.4}$$

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

$$\mathbf{T_s} = \frac{1}{\mathbf{n}\lambda_p} \tag{2.5}$$

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. Stručný výtah z této normy (verze MIL-HDBK-217D) je uveden dále v dodatku na konci knihy. 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.

2.1.2 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. 2.2.

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

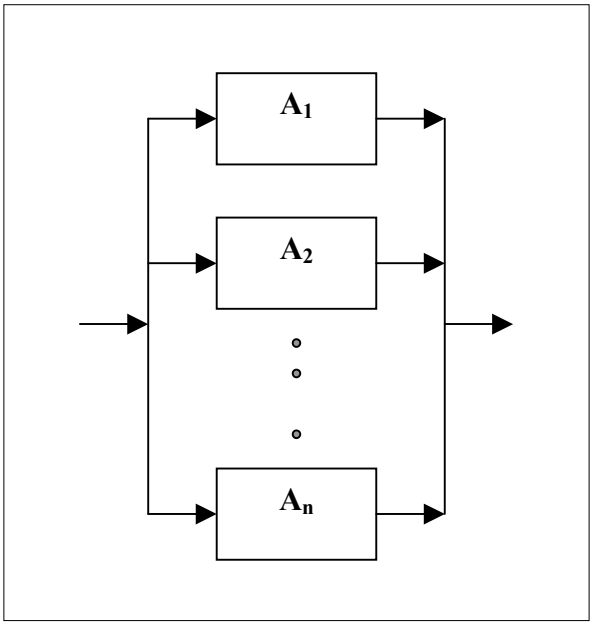
$$\mathbf{Q(t)} = \prod_{i=1}^{n} \mathbf{Q_i(t)} \tag{2.6}$$

Pro pravděpodobnost bezporuchového provozu lze vztah upravit do tvaru

$$\mathbf{R\,(t)} = \mathbf{1} - \prod_{i=1}^{n} \mathbf{(1 - R_i(t))} \tag{2.7}$$

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

$$T_s = \frac{1}{\lambda(t)} \sum_{i=1}^{n} \frac{1}{i} \qquad (2.8)$$



Obr. 2.2. Paralelní spolehlivostní model

2.1.3 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 (2.1) a (2.6) nebo (2.7).

Postup řešení kombinovaného modelu ukážeme na příkladu modelu neobnovovaného systému podle obr. 2.3.

Jsou dány konstantní intenzity poruch λ_1, λ_2, λ_3 a chce 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}

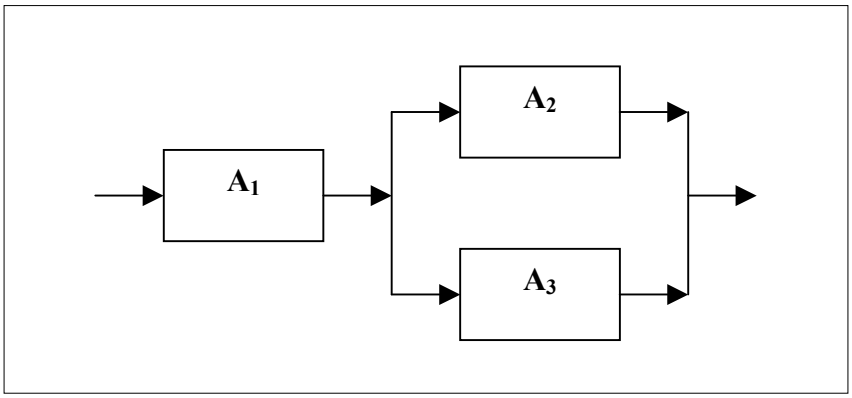
$$R_{23} = 1 - Q_{23} = R_2 + R_3 - R_2 R_3$$

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

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

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

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 (2.1), (2.6), (2.7) a jsou uvedeny například v [Bill83], [Usak89], [Star82].



Obr. 2.3. Příklad kombinovaného modelu

V této souvislosti je vhodné připomenout důležitou interpretaci blokového spolehlivostního schéma. Modelovaný systém je schopný provozu, jestliže existuje alespoň jedna cesta ze vstupu na výstup schématu.

2.1.4 Modely využívající stavový graf

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

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 kódu stavu) – nepředpokládáme tedy současnou poruchu několika prvků systému. V tomto případě představuje stavový graf krychli v **n**-rozměrném prostoru.

Stavových 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 $\mathbf{p_i(t)}$, můžeme určit **R(t)** s využitím stavového grafu podle vztahu pro součet pravděpodobností vzájemně se vylučujících náhodných jevů.

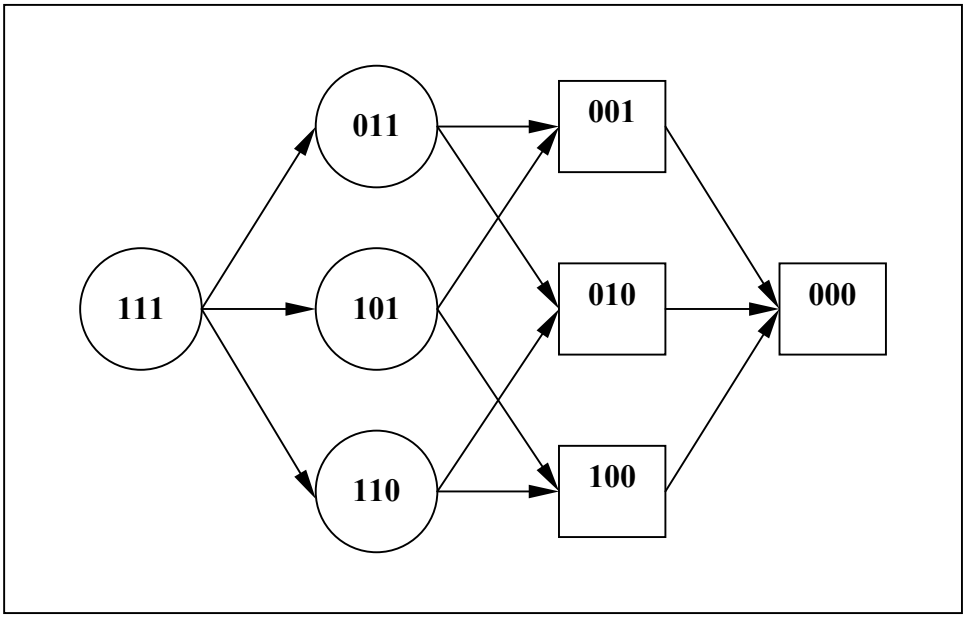
$$\mathbf{R(t)} = \sum_{\mathbf{i}} \mathbf{p_i(t)} \tag{2.9}$$

Index ***i*** probíhá přes všechny stavy, ve kterých je systém jako celek provozuschopný. Použití stavového grafu předvedeme na příkladu.

Příklad 2.1

Uvažujeme 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. 2.4.

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



Obr. 2.4. Příklad stavového grafu

$$R = R_1R_2R_3 + Q_1R_2R_3 + R_1Q_2R_3 + R_1R_2Q_3 =$$
$$= R_1R_2R_3 + (1-R_1)R_2R_3 + R_1(1-R_2)R_3 + R_1R_2(1-R_3) =$$
$$= R_1R_2 + R_1R_3 + R_2R_3 - 2\,R_1R_2R_3$$

Použití různých typů spolehlivostních modelů demonstruje následující příklad výpočtu spolehlivostních ukazatelů paměti zabezpečené proti poruchám samoopravným kódem (viz dále kap. 4).

Příklad 2.2

Uvažujme paměť složenou z k *slov o rozměru* n *bitů. Použitý samoopravný kód umožňuje tolerovat jeden chybný bit ve slově. 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. Uvažujme 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*

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

Všechny slova paměti a řídící logika jsou ve spolehlivostním smyslu spojený 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

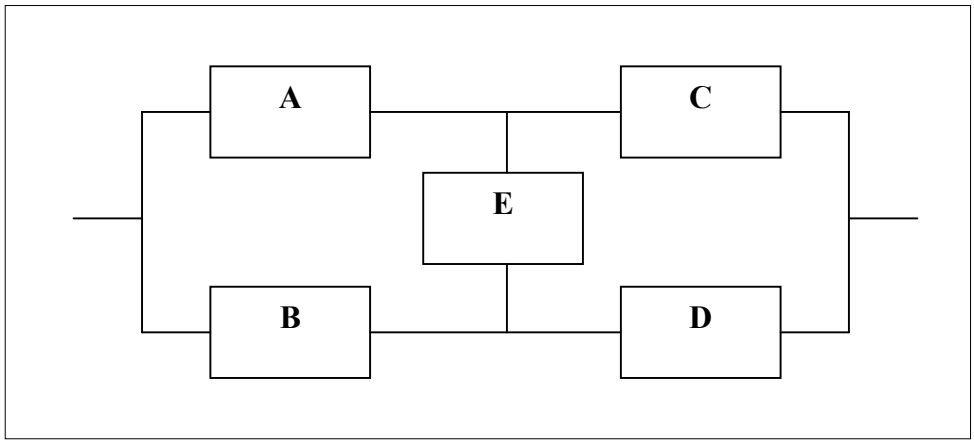
$$R_{(t)} = e^{-\lambda_c t}\,(ne^{-(n-1)\lambda_b t} - (n-1)e^{-r\lambda_b t})^k$$

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). Výpočtu spolehlivosti paměti se samoopravným kódem je dále věnována pozornost v jiném příkladu (odst. 4.2.3.).

2.1.5 Metoda řezů

Omezením praktické použitelnosti metod založených na stavovém grafu (resp. výčtu stavů s určitou vlastností) je exponenciální nárůst počtu stavů s počtem prvků systému. Jednu z možností, jak tento problém překonat, poskytuje metoda řezů. Řezem rozumíme množinu prvků uvažovaného systému, jejichž současná porucha způsobí poruchu celku. Z minimálního řezu nelze vypustit žádný prvek bez ztráty vlastnosti řezu. Další úvahy provedeme pro systém, jehož spolehlivostní model je na obrázku 2.5. Model není možné přímo převést na nějakou kombinací sériového a paralelního spojení.

Množina minimálních řezů - {AB, CD, AED, BEC}



Obr. 2.5. Minimální řezy

Úvaha, že výskyt kteréhokoliv z možných minimálních řezů znamená poruchu celého systému, vede k následujícímu vztahu pro pravděpodobnost poruchy uvažovaného systému

$$\mathbf{Q_\Sigma = Q_A\,Q_B + Q_C\,Q_D + Q_A\,Q_E\,Q_D + Q_B\,Q_E\,Q_C}$$

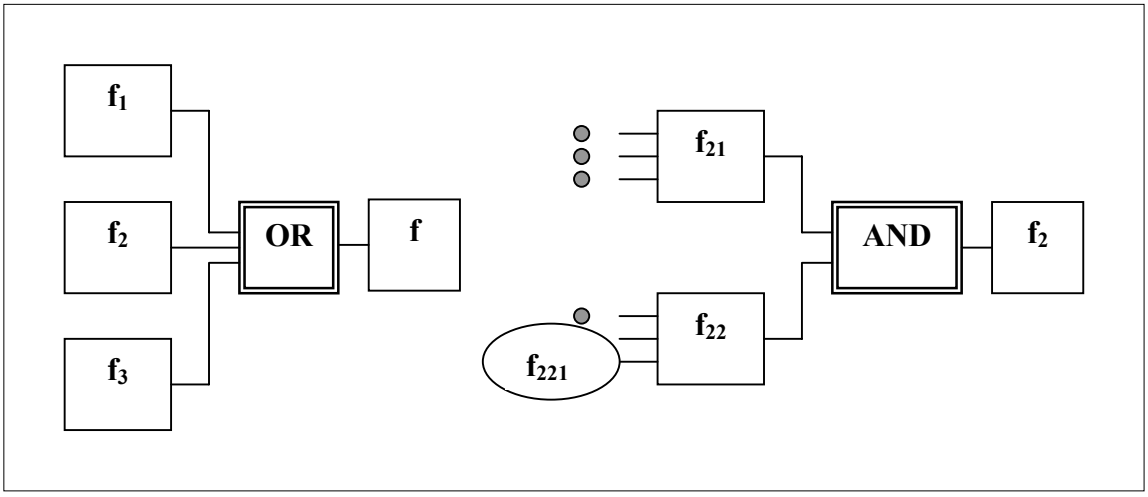
Tento vztah není korektní, protože pravděpodobnost některých stavů (řezů) je v součtu obsažena více než jednou. Například pravděpodobnost $\mathbf{Q_A\,Q_B\,Q_C\,Q_D\,Q_E}$ výskytu řezu **ABCDE** je obsažena ve všech prvcích uvedeného součtu a měla by se tedy třikrát odečíst.

Uvedený vzorec zřejmě poskytuje odhad $\mathbf{Q_\Sigma}$ pravděpodobnosti poruchy **Q** s vlastností $\mathbf{Q_\Sigma \geq Q}$. Pro případy technické praxe jsou hodnoty pravděpodobnosti poruchy prvků (např. $\mathbf{Q_A}$) malé hodnoty součinů typu $\mathbf{Q_A\,Q_B\,Q_C\,Q_D\,Q_E}$ jsou zanedbatelné. Numerická přesnost odhadu $\mathbf{Q_\Sigma}$ provedeného naznačeným postupem je pak velmi dobrá. Získáme tedy konzervativní odhad s dobrou přesností ($\mathbf{Q_\Sigma = Q,\ Q_\Sigma \geq Q}$). Vyhledání množiny všech minimálních řezů v zadaném spolehlivostním schématu je možné algoritmizovat ([Bill83], [Star91]).

2.1.6 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 událostí **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 2.6.



Obr. 2.6. Příklad stromu poruch

Význam označení bloků může být například:

f - porucha počítače
f1 - porucha procesoru
f2 - ztráta napájecího napětí
f3 - porucha paměti
f21 - porucha záložní baterie
f22 - ztráta napětí síťového zdroje
f221 - někdo omylem vypnul síťový vypínač, základní událost, pravděpodobnost události 0,00002

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. 2.6.)
- Výpočet spolehlivostních ukazatelů typu ***R***, ***Q*** z pravděpodobností základních událostí je jednoduchý.
- U složitých systémů může strom poruch sloužit jako podklad pro rozhodování operátora v průběhu rekonfigurace.
- 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.
- Strom poruch lze použít jako model pokrytí poruchy ve víceúrovňovém spolehlivostním modelu výpočetního systému (viz dále čl. 2.3).

Poznámka

Pro detailnější studium všech uvedených postupů odkážeme na literaturu (např.[Bill83], [Usak89], [Star82]). Dále existují přístupy, které jsou založeny na tzv. logické teorii spolehlivosti [Levi85], [Schn81].

Prozatím jsme uvažovali modely neobnovovaných systémů. Všechny 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 (2.1) a (2.6) 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 pohotovostí postoje 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 postoje u obnovovaných systémů je složitější záležitostí a bude popsán dále v odst. 2.2.3.