

# Spolehlivost

INP 2019

FIT VUT v Brně



- Definice spolehlivosti
- Ukazatele spolehlivosti
- Modelování spolehlivosti
  - Kombinatorické modely
  - Markovské modely
- Systémy odolné proti poruchám

*Pozn.: Bude prezentován jen velmi základní přehled problematiky, podrobněji v (magisterském) kurzu Systémy odolné proti poruchám.*

1

2

## Spolehlivost

- **Spolehlivost byla** definována 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* (ČSN 01 0102 „Názvosloví spolehlivosti v technice“).
  - *Objekt* – součástka, obvod, funkční jednotka, nebo systém
  - *Provozní ukazatele* – produktivita, rychlost, výkonnost, spotřeba energie, ...
  - *Technické podmínky* – souhrn specifikací technických vlastností, předepsaných pro požadovanou funkci objektu, způsob jeho provozu, skladování, přepravy, údržby a oprav
- **Spolehlivost je** souhrnný termín používaný pro popis pohotovosti a činitelů, které ji ovlivňují: bezporuchovost, udržovatelnost a zajištěnost údržby (platná terminologická norma ČSN IEC 50 (191))
- Spolehlivost je komplexní vlastnost objektu, která je číselně nekvantifikovatelná – v angličtině *dependability*.

3

## Porucha, chyba, selhání

- **Porucha** – např. poškození obvodu v důsledku přehřátí, což může a nemusí způsobit chybu.
- **Chyba** – odchýlení od korektního stavu systému – např. dojde v důsledku poruchy k chybnému sečtení, což může a nemusí způsobit selhání.
- **Selhání** – systém nepracuje podle specifikace.

**Fault (porucha) → Error (chyba) → Failure (selhání)**

4

## Příčiny selhání

- chyba software
- návrhová chyba hardware
- náhodná chyba (v datech)
- vnější rušení – např. chyba v datech, uložených v paměti, např. částicí alfa
- porucha hardware
  - destrukcí – průraz statickou elektřinou, aj.
  - korozi
  - mechanickým poškozením
  - atd.

5

## Klasifikace poruch a chyb

- **časově stálé** – permanentní, trvalý defekt (hard defect)
- **přechodné** – objeví se chyba v datech a zase zmizí (soft error, transient error)
- **občasné** – opakovaně se občas objeví a zase zmizí - intermittent error, např. zlomený drát, nebo vadný mechanický kontakt („vakl“ kontakt)

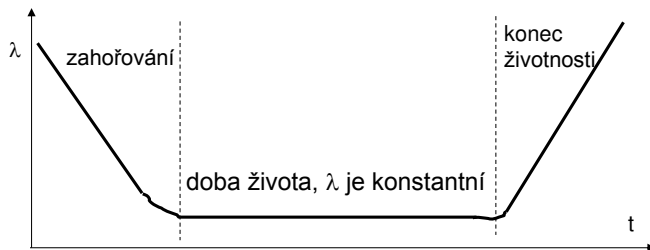
## Klasifikace objektů (systémů)

- **neopravované** – neopravují se, protože to není ekonomické (např. žárovka)
- **opravované** – obsahují mechanismy umožňující opravit určité poruchy

6

## Intenzita poruch

- **Intenzita poruch**  $\lambda$  – četnost, s jakou se systém porouchá. Vyjadřuje se jako počet poruch za jednotku času.
- Časový průběh funkce  $\lambda(t)$  je popsán **vanovou křivkou**.



- V praxi je často intenzita poruch zjednodušeně modelována konstantou, např.  $\lambda = 0,001$  porucha/hod.

7

## Ukazatele spolehlivosti

$R(t)$  – **pravděpodobnost bezporuchové činnosti** v intervalu  $<0, t>$ , v angl. reliability. Je to podmíněná pravděpodobnost, a to tím, že v čase 0 je objekt bez poruchy.

$R(t)$  se chová podle exponenciálního zákona  $R(t) = e^{-\lambda t}$

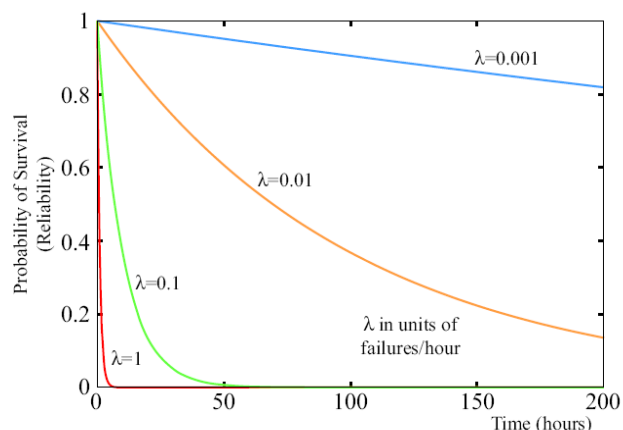
Komplementární veličina je **pravděpodobnost výskytu poruchy**  $Q(t) = 1 - R(t)$ .

Sledovaný časový interval činnosti (doba mise – mission time) je zásadní:

- u počítače v kosmických aplikacích je např. 10 let (let kosmické sondy na hranici sluneční soustavy)
- u počítače pro letadla je např. 15 hod., tj. asi max. doba letu

8

## Funkce $R(t)$ při různých hodnotách $\lambda$



**Odolnost proti poruchám** – schopnost systému pracovat bezchybně i za přítomnosti poruch. Je to něco jiného, než pravděpodobnost bezporuchové činnosti!

Jak? – díky použití opravných kódů, a maskováním chyb/poruch systémem TMR – viz dále.

Ani velmi spolehlivý systém, postavený z velmi spolehlivých součástí, nemusí být odolný proti poruchám.

**Pohotovost** (availability) je pravděpodobnost, že v okamžiku  $t$  bude systém funkční.

Koeficient pohotovosti  $K_p(t)$ , v angl.  $a(t)$ .

Př. Počítač v bance může mít občas poruchu, ale musí se rychle opravit tak, aby to klienti nepoznali. Takže nemusí být odolný proti poruchám.

9

10

## Střední doba bezporuchové činnosti $T_S$

$$T_S = \int_0^{\infty} R(t) dt$$

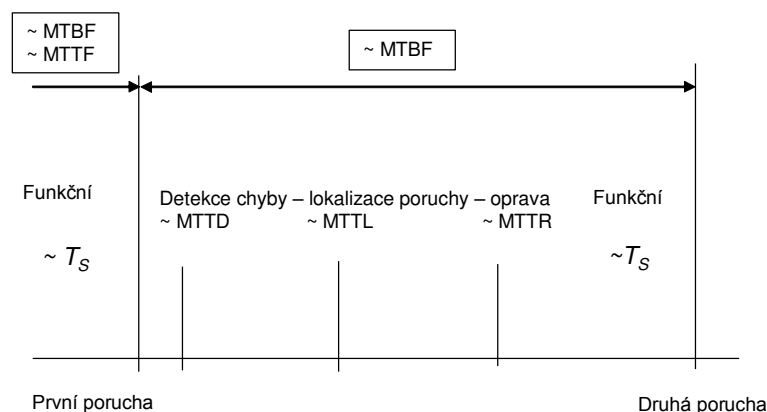
- Pro exponenciální zákon platí  $T_S = 1/\lambda$ .

$$T_S = \int_0^{\infty} e^{-\lambda t} dt = \frac{1}{\lambda} \quad \text{pokud } R(t) = e^{-\lambda t}$$

- $T_S$  nemá stejný význam jako další veličina, používaná pro **opravované systémy**, tzv. **střední doba mezi poruchami** – Mean Time Between Failures (MTBF)

- Pro **neopravované systémy** lze  $T_S$  lze ztotožnit se střední dobou do (první) poruchy Mean Time To a Failure (MTTF)

## Vztahy mezi středními ukazateli spolehlivosti



MTDD – Mean Time To Detect  
MTTL – Mean Time To Locate  
MTTR – Mean Time To Repair

11

12

Pro **opravované systémy** je analogicky zavedena **intenzita oprav**  $\mu$  jako převrácená hodnota střední doby opravy  $T_O = 1/\mu$

Pohotovost  $a = T_S / (T_S + T_O) = \mu / (\mu + \lambda)$

**Bezpečnost** (safety)  $S(t)$  je pravděpodobnost, že systém buďto pracuje správně, nebo hlásí poruchu, případně chybu v datech. Hodnota  $S(t)$  je tedy větší než  $R(t)$ .

Příklady:

- Systém pro řízení dopravní křižovatky nebo železničního přejezdu se konstruuje jako bezpečný. Když selže, nesmí nikdy nastavit v obou směrech zelenou, resp. nesmí blikat bílé světlo. Bezpečný stav je: nesvíťí nic, všude je červená, nebo oranžová, atd.
- Když se porouchá hydraulika letadla, lze je řídit ručně.
- Když se porouchá ventil, tak nejde otevřít.

13

14

## Modelování spolehlivosti: Kombinatorický výpočet $R(t)$

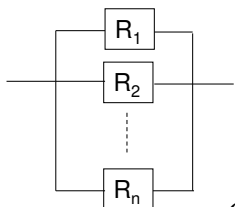
## Sériové spoehlivostní zapojení



$$R(t) = \prod_{i=1}^n R_i(t) \quad \text{za dobu } t$$

Výčet provozuschopných stavů:  
111 ... 1

## Paralelní spolehlivostní zapojení



$$Q(t) = \prod_{i=1}^n Q_i(t) \Rightarrow R(t) = 1 - \prod_{i=1}^n (1 - R_i(t))$$

Výčet provozuschopných stavů:

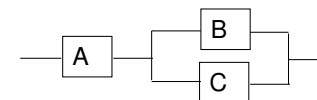
111 ... 1	
011 ... 1	
101 ... 1	
...	
000 ... 1	
000 ... 0	Ne!

**Sériově-paralelní** spolehlivostní zapojení se řeší modifikovanou Karnaughovou mapou.

Postup výpočtu:

1. Vytvořit spolehlivostní model analyzovaného systému.
2. Nakreslit spolehlivostní Karnaughovu mapu – 1 odpovídá bezporuchovému modulu, 0 modulu s poruchou. Počet proměnných je roven počtu modulů v systému. U složitých systémů sdružujeme moduly do modulů vyšší úrovně, a ty pak řešíme postupně.
3. Provozuschopné stavy systému vyznačíme v mapě jedničkami.
4. Najdeme disjunktivní pokrytí mapy, tj. každá jednička je pokryta pouze jedenkrát. Formálně zaměňujeme logické operace AND, OR, NOT za součin, součet a jedničkový komplement.

Příklad:



A, B, C jsou pravděpodobnosti  
bezporuchové činnosti

A	1	1	1

Výčet  
provozních  
stavů:

Disjunktní pokrytí a úprava:

$$R = A.B + A.(1-B).C$$

15

16

## Další metody kombinatorického modelování

### Zálohování „m z n“

$$R(t)_{m \text{ z } n} = \sum_{i=0}^{n-m} \binom{n}{i} R^{n-i}(t) [1 - R(t)]^i$$

kde  $n$  je počet všech modulů  
 $m$  je počet požadovaných fungujících modulů  
 $i$  je počet přijatelných poruch

Př. viz dále - TMR

## Další metody kombinatorického modelování

**Binomický zákon** – vyjadřuje pravděpodobnost  $P$ , že nastane  $r$  nezávislých událostí na  $n$  místech. Předpokládá, že pravděpodobnost výskytu události  $p$  (vadný výrobek, průraz izolace) je stejná.

$$P = \binom{n}{r} p^r (1-p)^{n-r} = \frac{n! p^r (1-p)^{n-r}}{r! (n-r)!}$$

17

18

## Markovské spolehlivostní modely

- Kombinatorické modelování často selhává, protože
  - blokové modely se obtížně sestavují
  - spolehlivostní modely jsou složité
  - proces oprav se popisuje obtížně
- Proto se nejčastěji používají **Markovské spolehlivostní modely**
  - Spolehlivostní model je vytvářen pomocí teorie stochastických procesů s diskrétními stavy a spojitým časem.
  - Markovský proces – náhodná posloupnost hodnot, kde  $k$ -tá hodnota závisí pouze na hodnotě  $k-1$ .
  - Spolehlivostní model lze vyjádřit grafem, maticí nebo soustavou rovnic. Model popisuje pravděpodobnosti přechodů mezi důležitými stavy systému. Z modelu lze vypočítat klíčové spolehlivostní ukazatele (příklady uvidíme při popisu TMR, NMR atd).
  - mimo možnosti INP

## Zvyšování spolehlivosti systému

Základní princip zvyšování spolehlivosti je **zálohování** součástí, funkčních jednotek, nebo celých systémů (redundance).

### Typy záloh:

- **technické vybavení** (zálohy zdvojení, ztrojení, ...)
- **programové vybavení** (alternativní programy, testovací a diagnostické programy)
- **informační** (detekční a opravné kódy – např. parita, Hammingův kód)
- **časové** (opakování operace)

### Typy substitučních záloh:

- **zatížená** – intenzita poruch je stejná jako u funkční jednotky – stejný pracovní režim
- **odlehčená** – intenzita poruch je snižena, např. snížením napájecího napětí
- **nezatížená** – intenzita poruch je (teoreticky) nulová

### Typy záloh podle využití v čase:

- **statická** – pracuje nepřetržitě po celou dobu funkce systému, je trvale připojená, nebo jako záloha bez přepínání
- **dynamická** – neboli s přepínáním podle potřeby

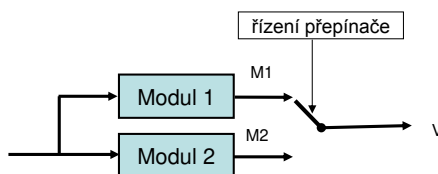
19

100% spolehlivost nelze u reálných systémů zajistit nikdy!!!

20

## Techniky zajištění odolnosti proti poruchám: Duplexní systém

- Jednoduchá metoda, která využívá dvě stejně pracující (nicméně ne nutně stejně implementované) verze modulu M.
- Pokud jsou výstupy M1 a M2 různé, není zřejmé na základě jejich pozorování, který výsledek je správný.
- Nelze dosáhnout **maskování chyby** a řízená soustava je ohrožena chybou nebo výpadkem řídicího signálu během přepínání na záložní prvek.
- Cena navíc oproti nezabezpečené verzi: 1 x modul, přepínač, řídicí logika



## Techniky zajištění odolnosti proti poruchám

- Statická redundance
  - třimodulová redundance (TMR)
  - NMR – zobecnění TMR
    - N – celkový počet modulů
    - n – počet modulů, jejichž porucha je tolerována

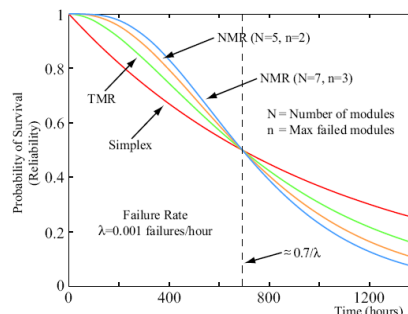
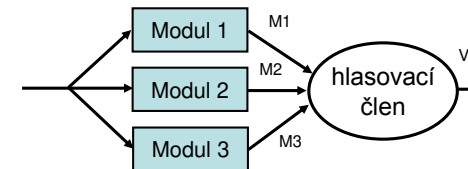


Figure 2.15: The TMR architecture only provides improved dependability over its simplex alternative up to a specific point in the systems lifetime. This point is determined by the failure rate of the simplex system.

Pozn: Simplex = 1 modul



Příklad realizace hlasovacího členu pro 1b výstup (majoritní funkce)

M1	M2	M3	V
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$$R(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

## Techniky zajištění odolnosti proti poruchám

- Dynamická redundance
  - Při poruše aktivního modulu se systém přepne na záložní modul. Musí existovat detektor poruchy.
- Hybridní redundance
  - TMR + náhrada poškozených modulů záložními moduly

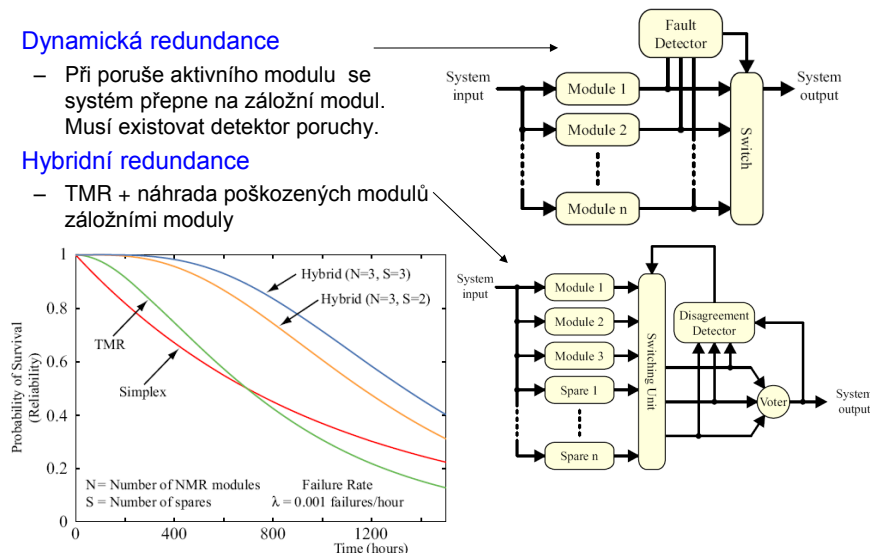


Figure 2.18: This graph shows the change in reliability with time of two hybrid redundancy systems compared to that of simplex and TMR systems. One hybrid system has two spares,  $S = 2$ , the other three,  $S = 3$ , both use TMR for masking. The voter, switch and disagreement detector are assumed to never fail.

## Spolehlivost z pohledu návrhu

- Pasivní přístup:** volba spolehlivějších součástek, řízení kvality, stínění, chlazení, bezpečná návrhová pravidla, verifikace návrhu, důsledná dokumentace, testování a diagnostika, nepoužívá se redundance – jde o předcházení poruchám (**fault avoidance**)
- Aktivní přístup:** použití hw i sw (i časové) redundance, návrh bezpečných a odolných obvodů, detekce chyb v datech, oprava chyb v datech pomocí opravných kódů, hlavně jde o tolerování (maskování) poruch, izolaci poruch a rekonfiguraci s cílem vyřadit vadné součásti (**fault tolerance**).
- Praxe: kombinace pasivního i aktivního přístupu

## Literatura

- Drábek V.: Systémy odolné proti poruchám. Přednášky FIT VUT 2009
- Hlavička J. et al.: Číslicové systémy odolné proti poruchám. Vydavatelství ČVUT Praha 1992
- Polsterová H.: Spolehlivost v elektrotechnice, skriptum FEKT VUT v Brně, 2003
- Greensted A.: A reliability Engineered Multicellular Architecture Inspired by Endocrinology: The BioNode System. PhD Thesis, The University o York, 2004, 184 s.