Progresivní technologie v informatice II

Spolehlivé systémy

Fakulta informačních technologií
České vysoké učení technické v Praze

Financováno Evropskou unií NextGenerationEU
Národní plán obnovy

Obsah

- Co znamená „spolehlivost“ a co ***dependability***
- Poruchy a co s nimi
- Proč a kdy a zda vůbec zabezpečovat
- Ukazatele spolehlivosti
- Modely, výpočty a grafy

zdroje: Dhiraj K. Pradham
M. Kaaniche, K. Kanoun, Jean-Claude Laprie
Algirdas Avizienis, Hlavička

„Spolehlivost“

- Základní úlohy spolehlivosti:
  - Zjišťování ….. měření (něco, co už funguje)
  - Předvídání …. predikce (co chci teprve vyrobit)
  - Řízení …. zlepšování (jak zajistit funkčnost podle aplikace)
- Spolehlivost = 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)
- https://www.csq.cz/fileadmin/user_upload/Spolkova_cinnost/Odborne_skupiny/Spolehlivost/informace/Normy_Spolehlivost_2016_08.pdf
- https://shop.normy.biz/detail/502160

Dependability

- sjednocení všech konceptů
- kvalita služeb poskytovaných systémem (Laprie, 1985)
- další termíny slouží ke kvantifikaci provozní spolehlivosti systému

Dependability = provozní spolehlivost: viz předchozí slide

Terminologie

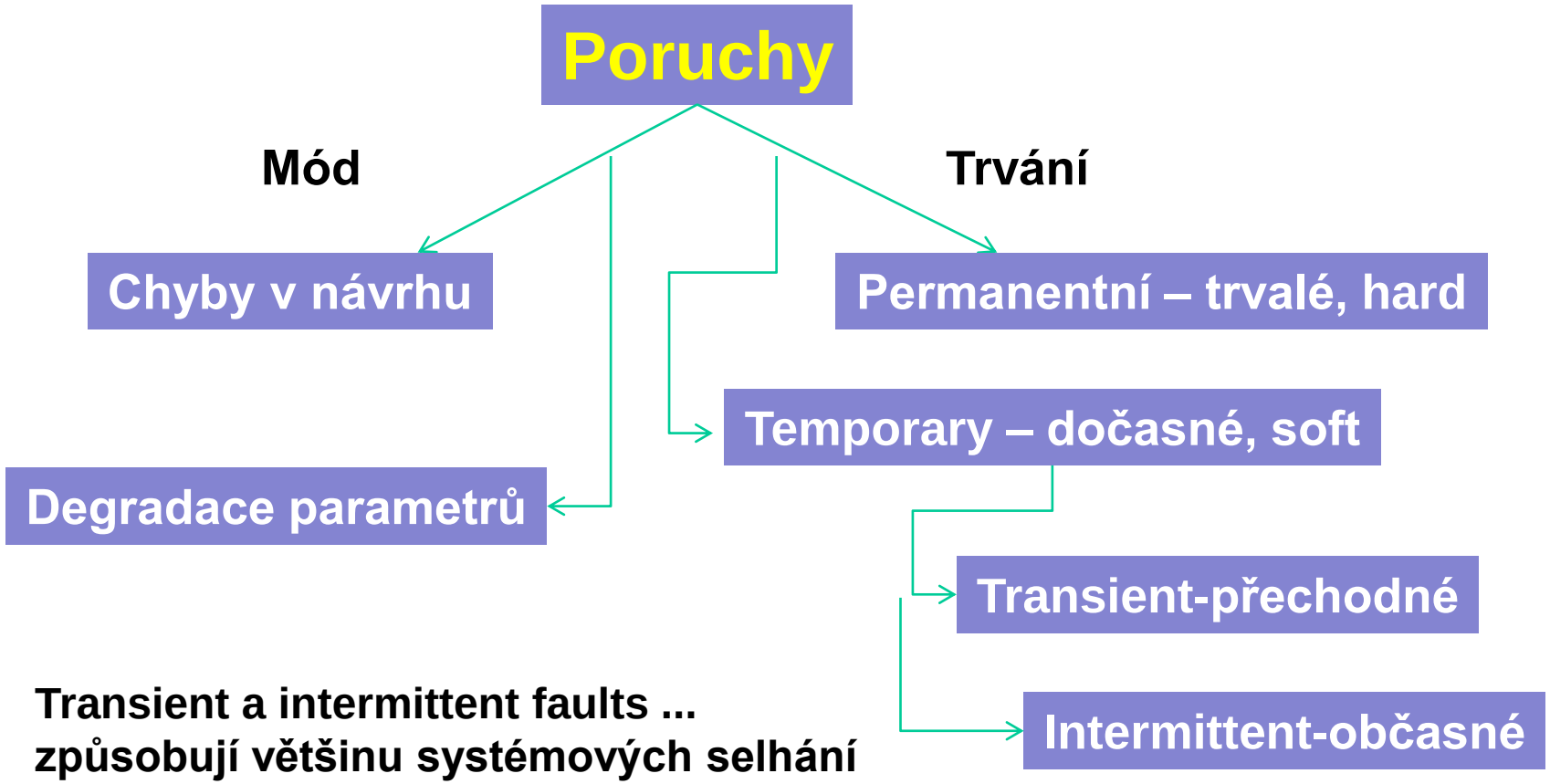
- Dependability - provozní spolehlivost
- **R**eliability – spolehlivost (česky spíš *pravděpodobnost bezporuchového provozu .... bezporuchovost*)
- **A**vailability – pohotovost (součinitel pohotovosti, naopak součinitel prostoje)
- **M**aintanability - udržovatelnost
- **S**afety - bezpečnost
- Security - bezpečnost
- Performability - proveditelnost
- Testability – testovatelnost
- Survaivability ... *schopnost „přežít“*

RAMS parametry

Poruchy, chyby, selhání

- **Defect** (porucha) … fyzický defekt …. fyzický prostor
- **Fault** (porucha) … fyzický prostor, spíš model fyzické poruchy
- **Error** (chyba) … projev poruchy … informační prostor
- **Failure** (selhání) … chyba vede k selhání funkce systému … vnější, uživatelský prostor

Klasifikace poruch



Transient a intermittent faults ...
způsobují většinu systémových selhání

... ctd poruchy, faults

= model defektu na logické úrovni

- Trvalé poruchy (permanent faults)
  - trvalá 1 (stuck-at-one), trvalá 0 (stuck-at-zero)
  - zkrat (bridging fault, shorts)
  - zpoždění (delay fault)
- Přechodné poruchy (transient faults)
  - jednorázové naštvání - SEU (single-event upset)
  - jednorázový pulz - SET (single-event transient)
  - SEL (single-event latch-up) – jednorázové velké zvýšení proudu
  - Překlopení bitu v paměti (bit-flip)
- Občasné poruchy (intermittent faults)
  - způsobené degradací parametrů
  - projeví se po delší době, jen občas
  - často časem přecházejí v trvalé

Fault avoidance, masking, tolerance

- Vyhnutí se poruše → návrh, testování, kontrolní metody (předcházení poruchám využitím ultra spolehlivých komponent)
- Maskování poruchy → zabránění přechodu poruchy jako chyby do informačního prostoru
- Tolerování poruchy → pokračování funkce po nastání poruchy, zabránění selhání systému (návrh systému aby pracoval správně i při výskytu chyby-poruchy)

  lze dosáhnout pomocí redundance*:*

  - Hardwarová redundance
  - Softwarová redundance
  - Redundance v čase

Ukazatele spolehlivosti

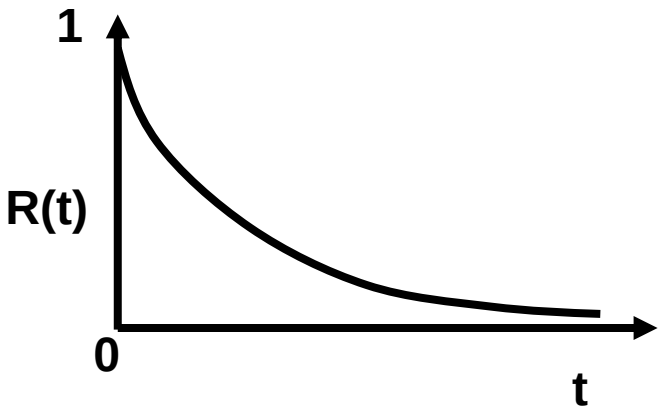
- Jak to kvantifikovat
- Pravděpodobnost
- Záleží na intenzitě poruch a jejím časovém průběhu … zjednodušení
- Obnovované a neobnovované systémy

Reliability - spolehlivost

- Spolehlivost …. pravděpodobnost bezporuchového provozu …. *R(t)*
- pravděpodobnost, že systém pracuje správně v určitém časovém intervalu
- *příklad hodnot: R(t) = 0,9999999 … $0,9_7$*
- *Q(t):* pravděpodobnost poruchy (unreliability) … *někdy F(t)*

R(0) = 1 t = 0 .... funguje na 100%

R(∞) = 0 t = ∞ .... selže



R(t)=průběh pravděpodobnosti, že systém je funkční v závislosti na čase

Availability - pohotovost

- Pravděpodobnost, že systém pracuje správně a provádí své funkce v časovém okamžiku *t* … *A(t)*
- záleží nejen na tom, jak často je nefunkční, ale také jak rychle může být opraven
- př. rezervační systém letenek

Safety - bezpečnost

- Pravděpodobnost, že systém provádí svou funkci správně nebo přestane fungovat tak, že nenaruší funkci jiných systémů, tzn. že selže bezpečným způsobem, nezpůsobí žádnou škodu … *S(t)*

- *Security:* odolnost proti útokům
  - terminologický problém:
    - AJ: security a safety
    - Čj/N/Sw: Bezpečnost/Sicherheit/Säkerhet
    - Norwegian: Security = Sikkerhet, Safety = Trygghet
    - French (francais): securite=safety, surete= security

Performability - proveditelnost

- Pravděpodobnost, že systém bude fungovat na určité úrovni *L* v časovém okamžiku *t* … *P(L,t)*
- *R(t)* … všechny funkce systému se musí provádět správně
- *P* … určitá podmnožina funkcí je prováděna správně

Maintanability - udržovatelnost

- Jde o možnost opravy v případě selhání
- Pravděpodobnost, že porouchaný systém bude uveden do funkčního stavu v čase *t* … *M(t)*
- Zjištění (on line testování !) a nalezení poruchy, fyzická oprava, znovuuvedení do činnosti

Testability - testovatelnost

- Schopnost testovat určité vlastnosti systému
- Zvýšení testovatelnosti - část testů je integrována do systému
- Úzký vztah k udržovatelnosti

Řiditelnost (controllability)

Pozorovatelnost (observability)

Praxe - průmysl

- ***Reliability***
- ***Availability***
- ***Maintanability***
- ***Safety***

…. Tzv. RAMS parametry

Různé typy - třídy systémů

Ultra spolehlivé systémy

Kritické řídící real-time aplikace

Systémová spolehlivost:

Pravděpodobnost, že systém bude pracovat správně přesně specifikovanou dobu.

Př. : Avionické počítače (NASA) ...Pravděpodobnost poruchy menší než 10^{-9} 10 hodin letu

Fault Tolerance:

Maximální počet poruch, které mohou kdekoli v systému nastat aniž způsobí selhání systému.

Long Life systémy

= systémy s dlouhou životností

Aplikace, kde údržba a/nebo oprava není možná

- vesmírná loď bez posádky

Mean time to Failure(MTTF): střední doba do poruchy (bezporuchového provozu)

Předpokládaná doba do selhání systému

Př. : 20 let MTTF pro komunikační satelit

Maximální doba mise: maximální doba operace pro nějakou minimální spolehlivost.

Př.: Spolehlivost 0.90 (pravděpodobnost bezporuchového provozu) pro 10 let provozu výzkumného vozítka na planetách

Vysoce pohotové systémy

Aplikace, kde je výpadek funkce drahý:

- telefonní ústředna
- drahé systémy s vysokým výkonem

Mean time to repair(MTTR – střední doba opravy):

Průměrná doba nutná pro opravu selhání.

Mean time between Failures – střední doba mezi poruchami

(MTBF)=MTTF + MTTR

Availability (pohotovost): Pravděpodobnost, že systém bude pracovat správně v jakémkoli daném čase a podle operačního rozvrhu

MTTF

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

$$= \frac{\text{MTBF} - \text{MTTR}}{\text{MTBF}}$$

Příklady: Cray-1(1975)

MTTF = 4 hodiny

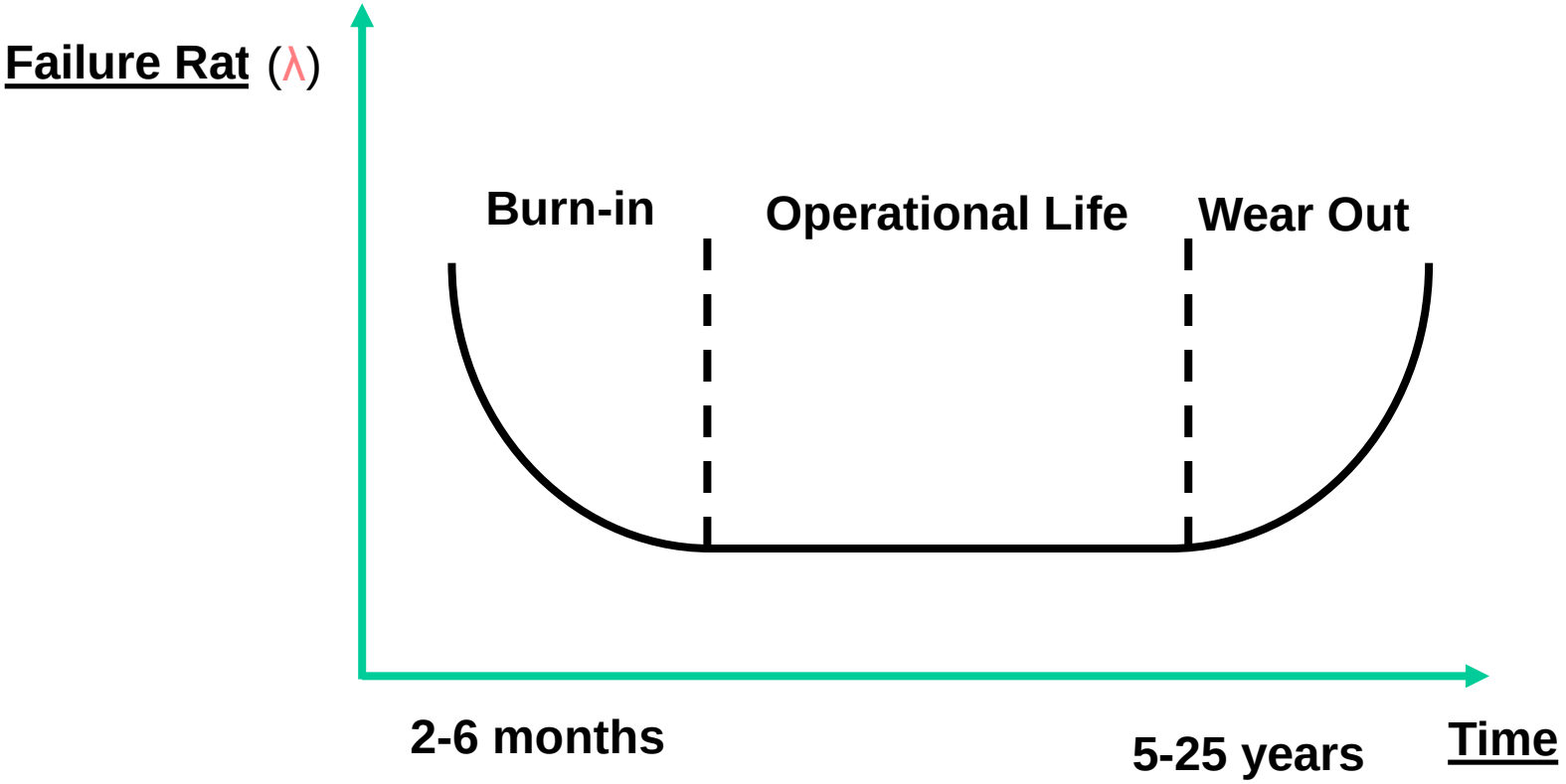
MTTR = 0.1 hodiny

$$\text{Availability} = \frac{4}{4.1} = 0.98$$

BELL ESS
Cíl: 20 minut mimo provoz za 40 let

Vanová křivka

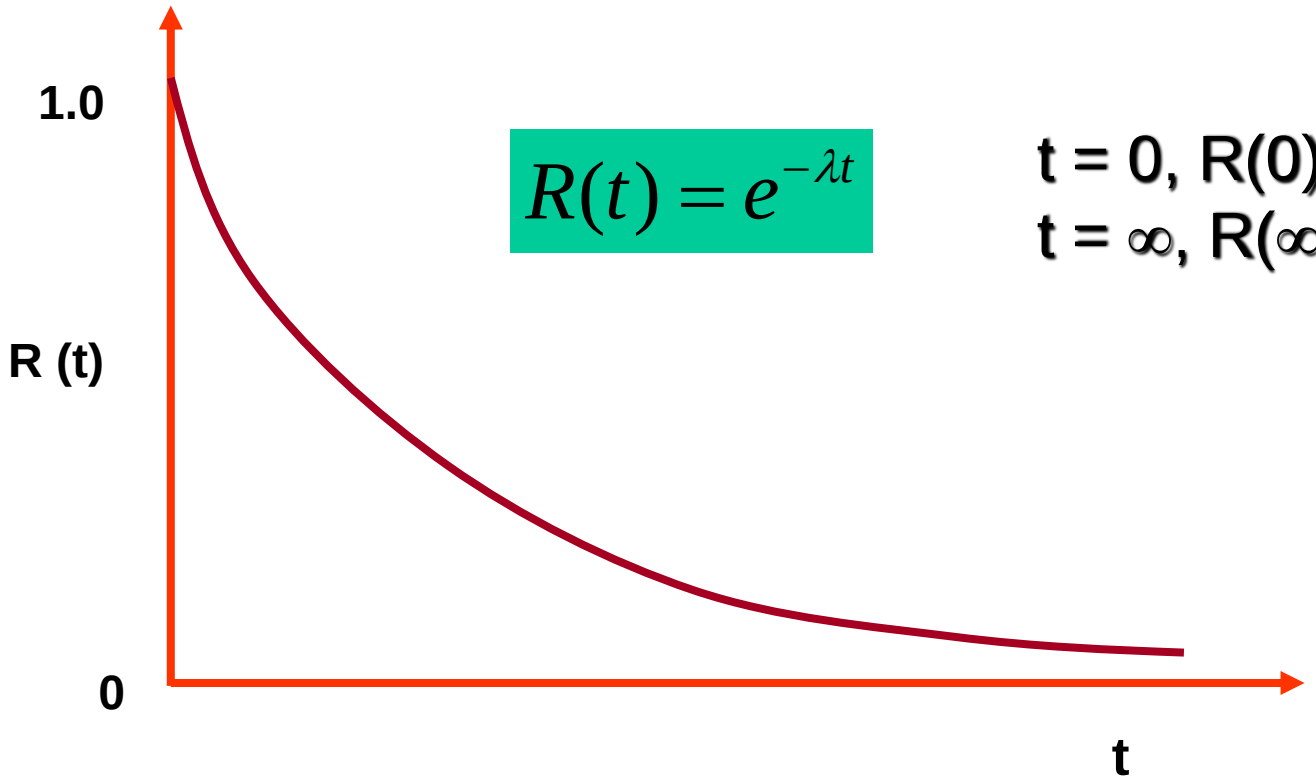
= bath-tube



Předpoklad: Během provozní životnosti („operational life“) vykazují součásti konstantní intenzitu poruch (λ)!!

Konstantní intenzita poruch

- Konstantní intenzita poruch - failure rate (λ) → exponenciální rozložení bezporuchovosti *R*(*t*):



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

t = 0, R(0) = 1
t = ∞, R(∞) =0

Pravděpodobnost, měření a odvození

Náhodný charakter – matematická statistika

Distribuční funkce F(t) …. $0 \leq F(t) \leq 1 \quad \forall\, t$

- Teoretické charakteristiky ukazatelů spolehlivosti – odvozeny na základě teorie pravděpodobnosti
- Empirické charakteristiky ukazatelů spolehlivosti – získané hodnocením statisticky oprávněného náhodného výběru (označujeme ˆ)

Poruchový stav x bezporuchový stav objektu (porucha se nemusí projevit chybou)

Obnovované x neobnovované (opravované x neopravované) objekty

Objekt je neobnovovaný ….. protože je nepřístupný, neopravitelný, oprava je nerentabilní

Neobnovované objekty

Pravděpodobnost poruchy …. Q(t)

Pravděpodobnost, že dojde k poruše do času t

Náhodná veličina: Q(0) = 0, je neklesající,

$$\lim_{t\to\infty} Q(t) = 1$$

Empirická hodnota:

$$\hat{Q}(t) = \frac{\bar{n}(t)}{n}$$

n – počet objektů ve zkušebním souboru

$\bar{n}$ – počet objektů porušených do času t

- **Pravděpodobnost bezporuchového stavu**

R(t) = 1 – Q(t) *(R ... reliability)*

(pravděpodobnost, že nedojde k poruše do času t)

- Empirická hodnota:

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

n – počet objektů ve zkušebním souboru

$\overline{n}(t)$ – počet objektů porušených do času t

- Hustota pravděpodobnosti spojité náhodné veličiny zde **hustota poruch**

$$f(t) = \frac{dQ(t)}{dt}$$

f(t).dt ….s jakou pravděpodobností nastane porucha ve sledovaném objektu v intervalu *dt* následující za okamžikem *t*

Empiricky: počet nově porušených objektů za čas Δt

$$\hat{f}(t) = \frac{\bar{n}(t+\Delta t) - \bar{n}(t)}{n.\Delta t}$$

Podmíněná hustota poruch v čase *t* za předpokladu, že k poruše dosud nedošlo …

- **intenzita poruch**

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

h^{-1}

(Pravděpodobnost, že se objekt neporouchaný v čase *t* porouchá v následujícím *dt*)

Empiricky:

Počet porušených za Δt

$$\hat{\lambda}(t) = \frac{\frac{\bar{n}(t+\Delta t) - \bar{n}(t)}{n.\Delta t}}{\frac{n - \bar{n}(t)}{n}} = \frac{\bar{n}(t+\Delta t) - \bar{n}(t)}{(n - \bar{n}(t)).\Delta t}$$

Počet neporušených krát Δt

odvození vztahu pro *R*

$R(t) = 1 - Q(t)$ →

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

$$\lambda(t) = \frac{f(t)}{R(t)}$$

$$\lambda(t) = -\frac{dR(t)}{dt} \bullet \frac{1}{R(t)}$$

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

integrace

$$-\int_0^t \lambda(\tau)d\tau = \int_1^{R(t)} \frac{d\rho}{\rho} = \left[\ln \rho\right]_1^{R(t)} = \ln R(t)$$

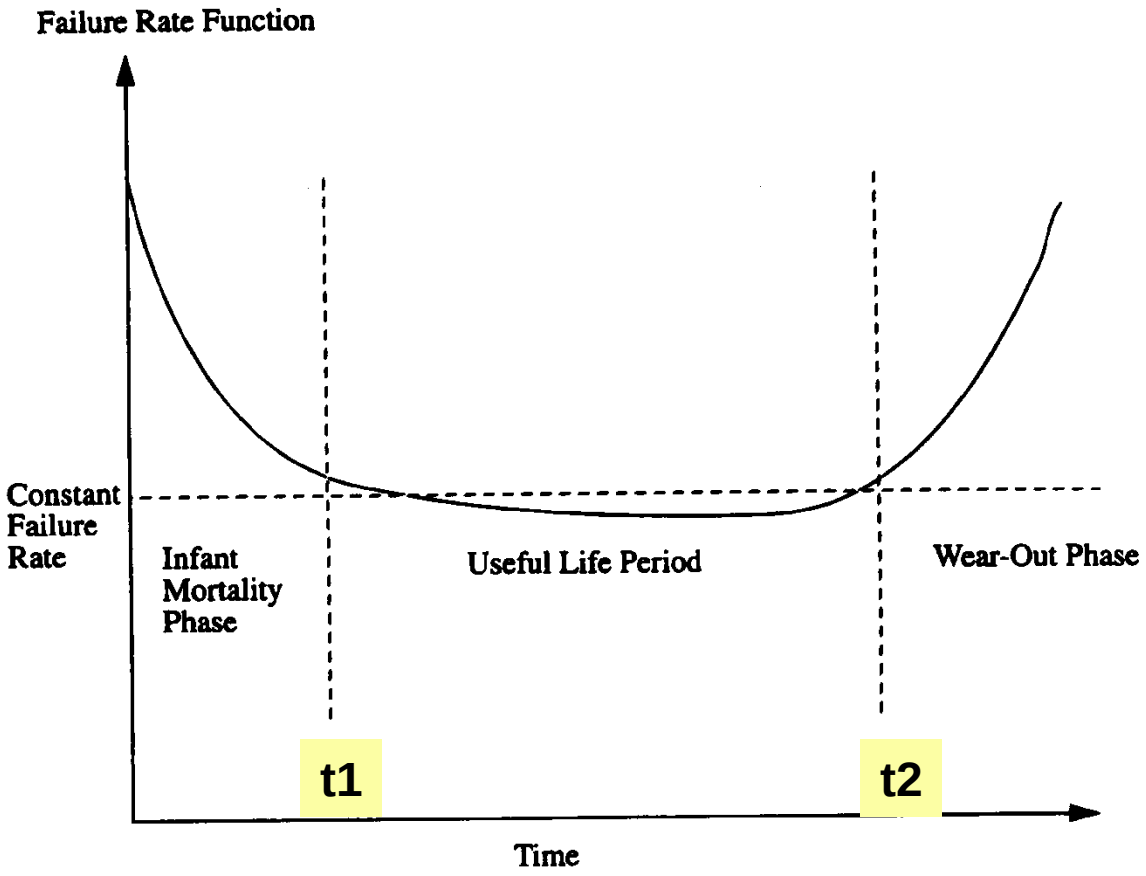
$$\ln(R(t)) = -\int_0^t \lambda(\tau)d\tau$$

řešení: $$R(t) = e^{-\int_0^t \lambda(\tau)d\tau}$$

CO DÁL?

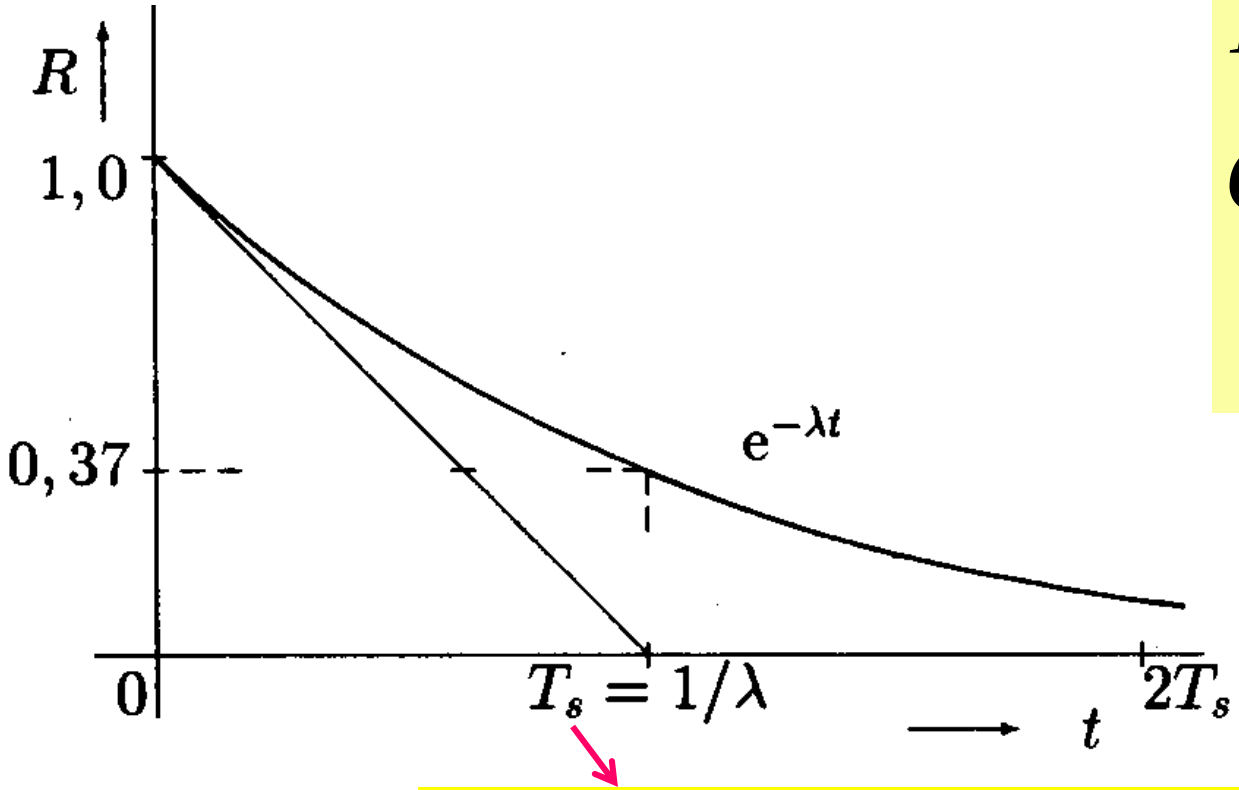
- Pokud neznám průběh intenzity poruch λ v závislosti na čase … *nelze nic … nejde integrovat*
- Empirická zjištění … vanová křivka (bath curve)

V intervalu $t_1 - t_2$ konstantní hodnota v době normálního provozu (10 týdnů – 10 let)



Financováno Evropskou unií NextGenerationEU
Národní plán obnovy

Za předpokladu konstantního λ:



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

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

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

Střední doba bezporuchového provozu MTTF … T_s

Střední doba bezporuchového provozu

T_s ~ MTTF

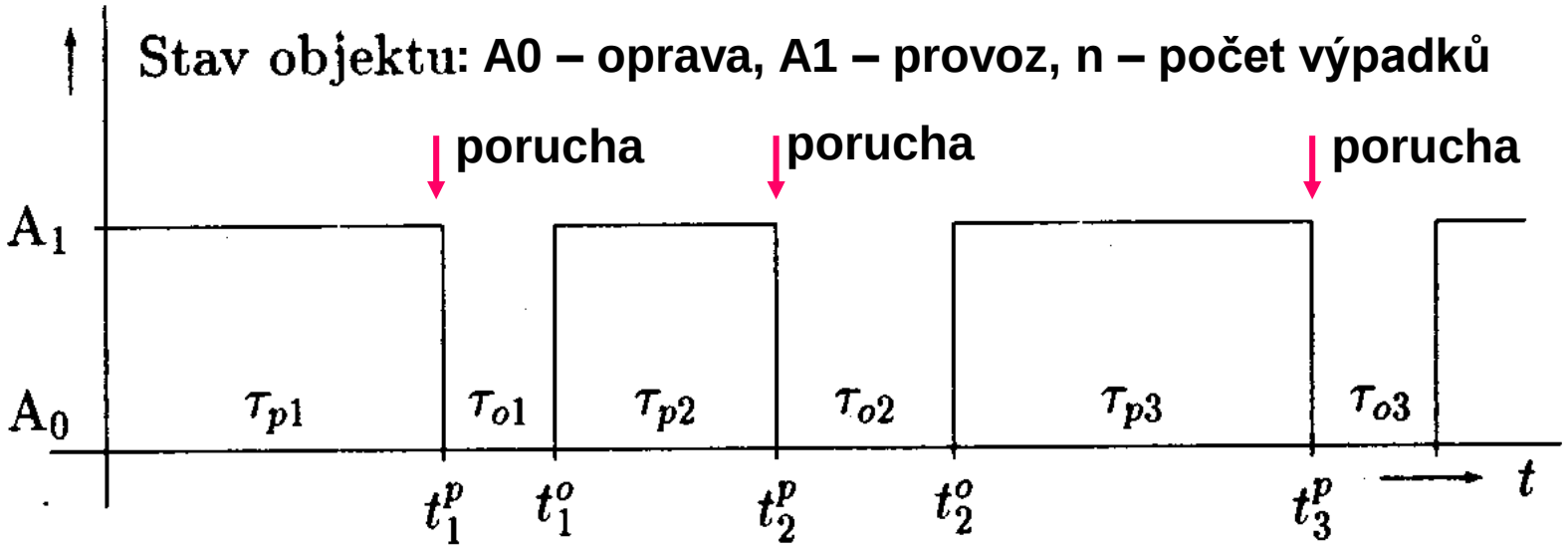
- Střední hodnota sledované náhodné veličiny

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

- MTTF (mean time to failure) – pro neobnovované objekty …. (střední doba do „první“ poruchy)
- Zjednodušení pro konstantní λ (oblíbený vztah – *ale λ je konstantní jen v intervalu t1 – t2 !!!*):

$$T_s = \int_0^\infty e^{-\lambda t}dt = -\frac{1}{\lambda}\left[e^{-\lambda t}\right]_0^\infty = \frac{1}{\lambda}$$

Ukazatele pro obnovované objekty



Střední doba mezi poruchami – MTBF – mean time between failures

Ukazatele pro obnovované objekty

Střední doba opravy – T_O - MTTR - mean time to repair

$$T_o = \frac{\sum_{i=1}^{n} \tau_{oi}}{n}$$

$$\lambda = \frac{1}{T_s}$$

Intenzita poruch – střední počet poruch za jednotku času

Frekvence oprav – střední počet oprav za jednotku času $\tau = \frac{1}{T_o}$

Součinitel pohotovosti a prostoje

Součinitel pohotovosti K_p (... availability A)

Poměr doby provozuschopnosti k celkové sledované době (pravděpodobnost, že v náhodně vybraném okamžiku bude objekt provozuschopný)

t_p - *doba provozu*
t_o - *doba opravy*
T_s - *MTTF*
T_o - *MTTR*
λ - *intenzita poruch, t – intenzita oprav*

$$K_p = \frac{t_p}{t_p + t_o} = \frac{T_s}{T_s + T_o} = \frac{\tau}{\tau + \lambda}$$

Součinitel prostoje – doplněk K_p do 1 (...unavailability)

$$K_n = 1 - K_p = \frac{t_o}{t_p + t_o} = \frac{T_o}{T_s + T_o} = \frac{\lambda}{\tau + \lambda}$$

Spolehlivostní modely

prostředek pro hodnocení/výpočty spolehlivosti

- Kombinatorické modely - blokový model

Spolehlivost systému je odvozena od spolehlivostí jednotlivých komponent:

Sériové spojení – každý prvek musí pracovat správně, aby pracoval správně celý systém – žádná redundance

Paralelní spojení – stačí, aby správně pracoval jeden prvek

Systémy s nezávislými prvky

- Stavový graf, přechodový graf - Markovské modely, Markovské řetězce

Prvky nemusí být nezávislé, ale

intenzity přechodů mezi stavy jsou konstantní

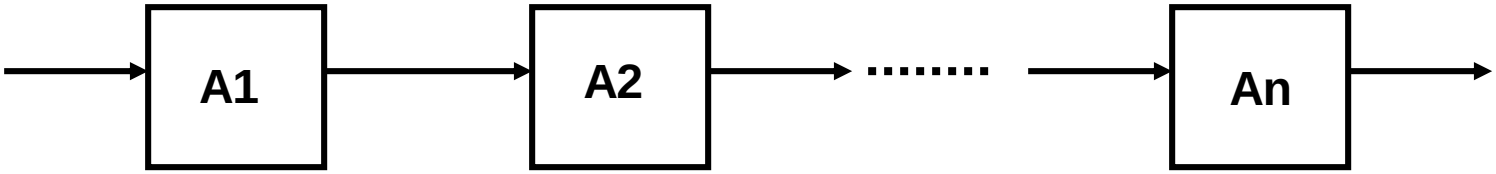
(tzn. intezity oprav a poruch)

Blokové splehlivostní modely

- RBD = „*Reliability Block Diagram*“
- Model vzhledem ke spolehlivosti
- Každý prvek je jeden blok
- Spojnice mezi bloky tvoří cesty mezi vstupem a výstupem
- Každá cesta je jeden provozuschopný stav systému
- Systém je bezporuchový, jestliže jsou všechny bloky aspoň na jedné cestě bezporuchové

…. jen pro nezávislé prvky!!!

Sériový model



$$R_s(t) = \prod_{i=1}^{n} R_i(t)$$

Pro konstantní intenzity poruch pro všechny prvky:

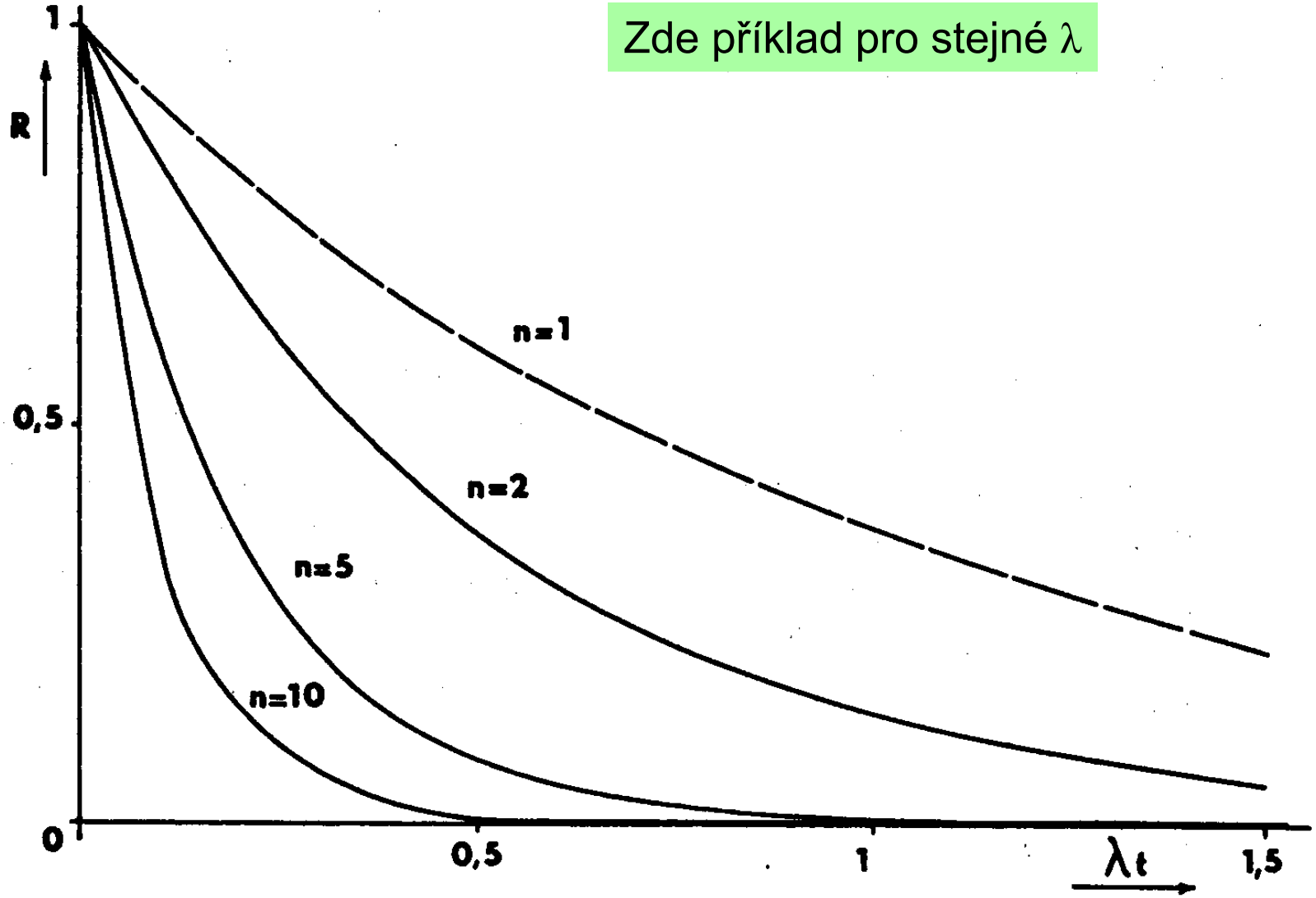
$$R_s(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\lambda t}$$

kde:

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

Co není zálohované je sériové

Zde příklad pro stejné λ



Příklad výpočtu

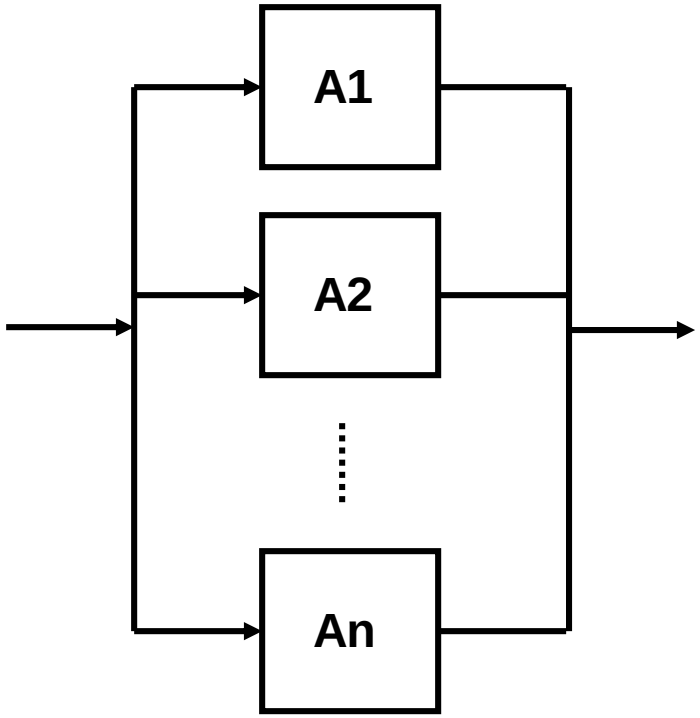
- Systém tvořený 100 IO se stejnou intenzitou poruch $\lambda = 10^{-6}\ h^{-1}$
- $T_s = ?$

$$T_s = \frac{1}{n\lambda} = \frac{1}{100.10^{-6}}\,h = 10^4\,h = 1{,}14\,roku$$

Poznámka: pro reálný výpočet je třeba uvažovat vliv dalších součástek

Jak se změní výsledek, když zohledním další objekty s větší intenzitou poruch, např. jeden sériový objekt: $\lambda = 10^{-4}\ h^{-1}$?

Paralelní model

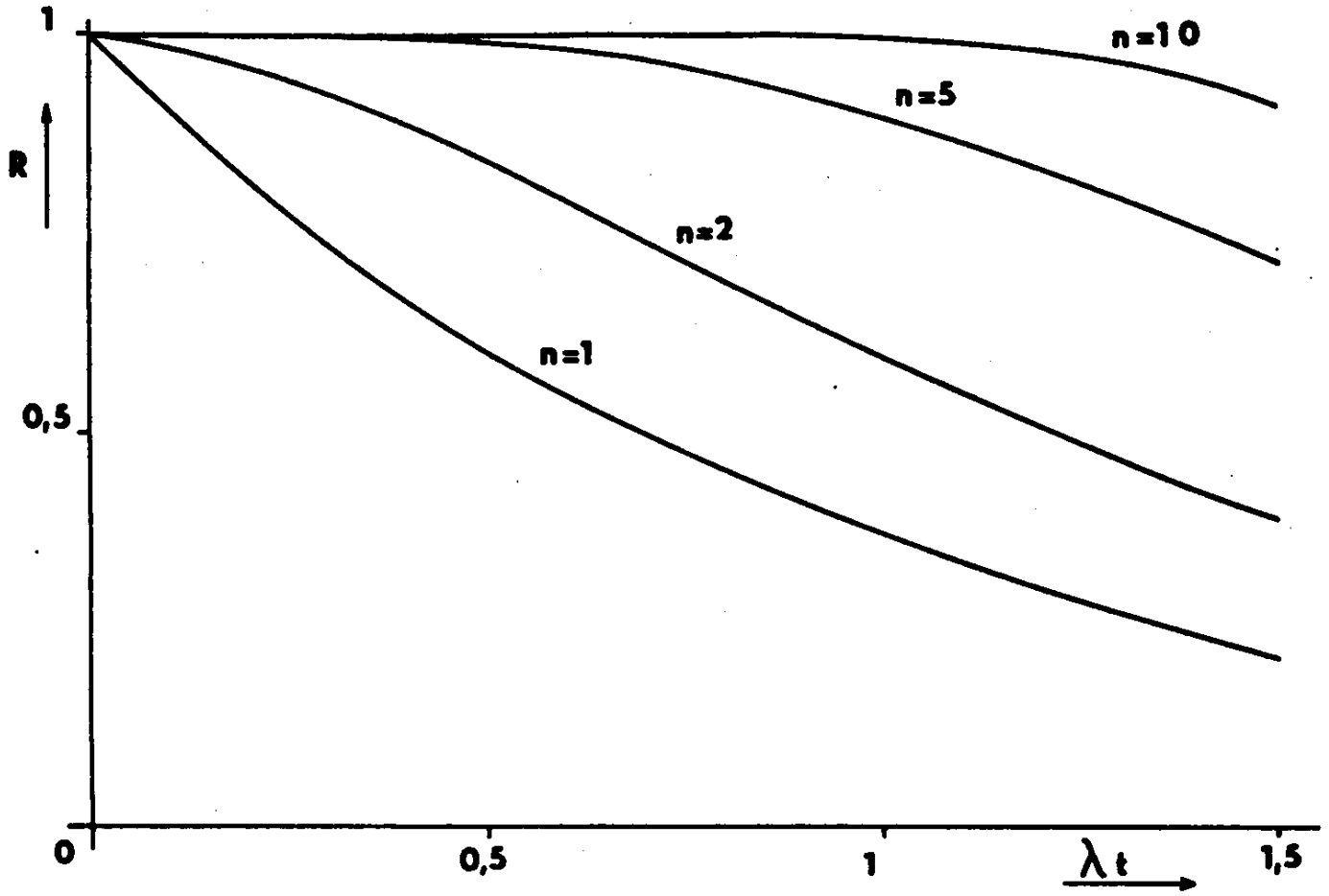


Porucha systému nastane až
při poruše všech prvků současně

$$Q_p(t) = \prod_{i=1}^{n} Q_i(t)$$

$$R_p(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

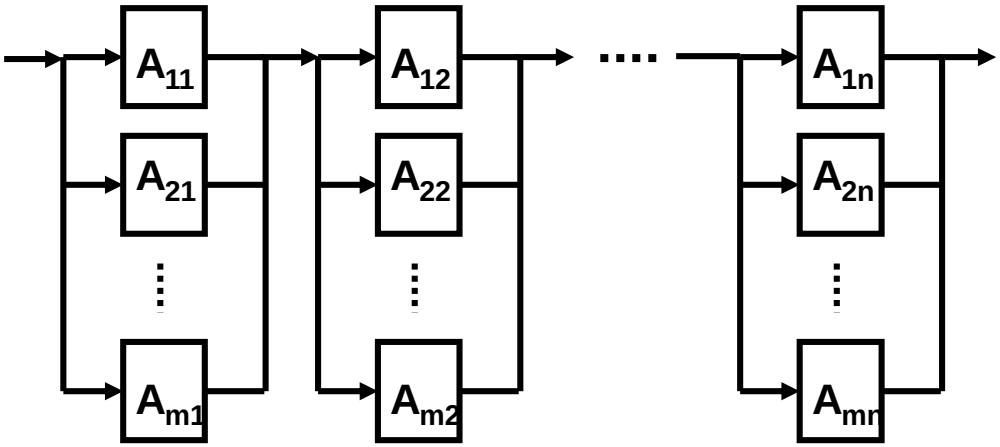
Zde příklad pro stejné λ



Kombinované modely

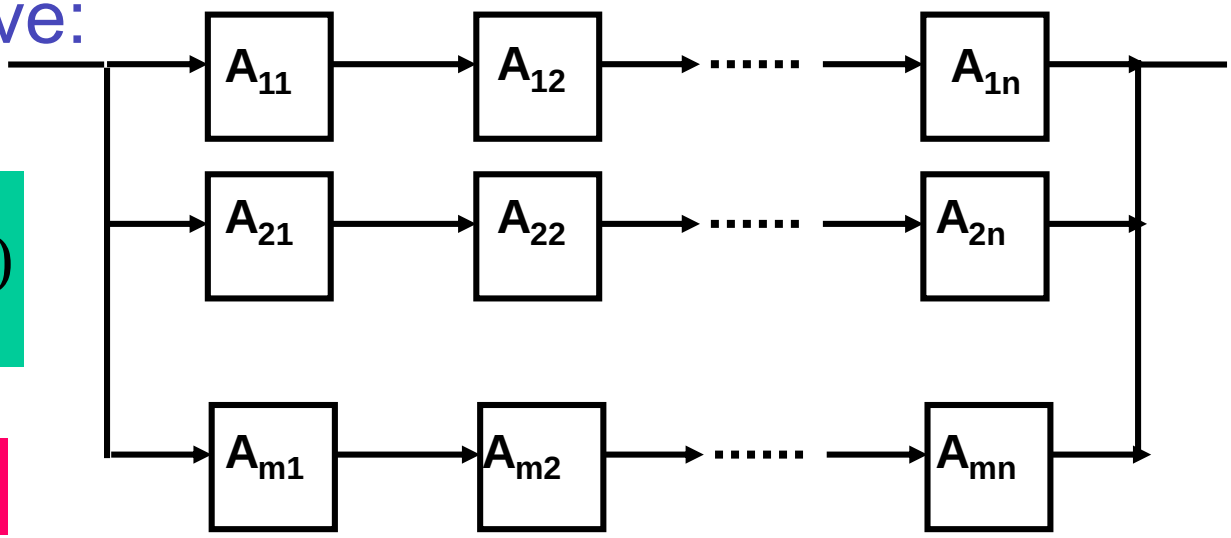
- Sériově-paralelní:

$$R_{sp} = \prod_{j=1}^{n}(1-\prod_{i=1}^{m}1-R_{ij}))$$



- Paralelně-sériové:

$$R_{ps} = 1-\prod_{i=1}^{m}(1-\prod_{j=1}^{n}R_{ij})$$



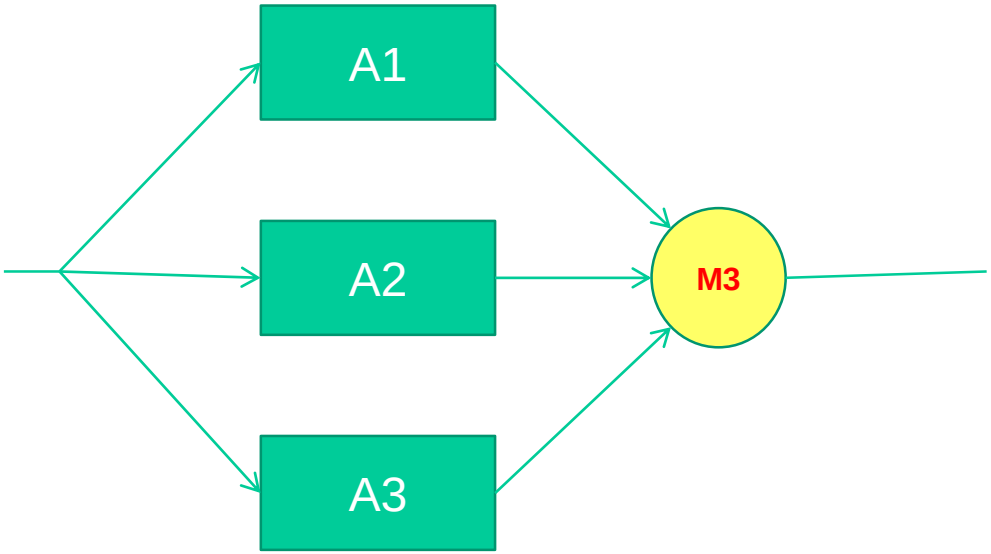
Co je „spolehlivější“??

Zálohování - redundance

- Studená (dynamická) záloha:
  - Záložní prvek není připojen na napájení, vstupy i výstupy jsou odpojeny od systému, data se nezpracovávají
- Teplá (statická) záloha:
  - Záložní prvek je trvale v provozu, je připojen na napájení, zpracovává vstupní hodnoty a výstupy jsou využity pro řízení
- Při studené záloze je třeba řešit náběh bloku
- Každý blok a jeho řízené zapínání nebo vypínání přispívá k celkové (ne)spolehlivosti systému

Jak využít a modelovat redundanci?

- Paralelní model spolehlivosti
- Problém s vyhodnocením (tedy detekce, popř. oprava poruchy)
- Klasické a nejpoužívanější řešení TMR



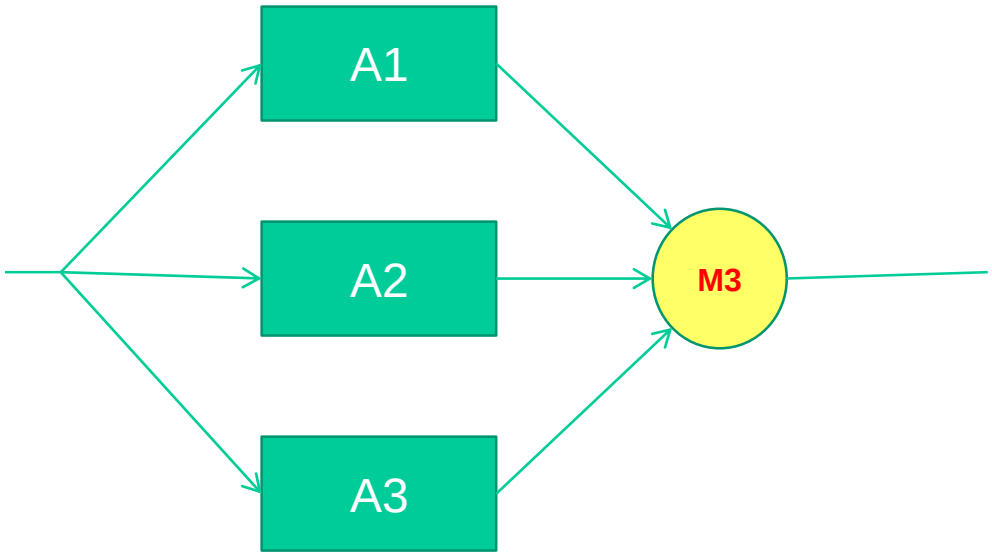
Stavový (přechodový) graf

- Neorientovaný graf, vrcholy .. technické stavy systému
- Hrany spojují vrcholy mezi kterými ex.přechod a jsou ohodnoceny **intenzitou přechodu** mezi stavy
- Pro *n* 2-stavových prvků ex. 2^n vrcholů … zjednodušení: stavy se stejným počtem poruchových prvků jsou reprezentovány jedním vrcholem (proces „faktorizace“)
- Pravděpodobnost bezporuchového stavu v čase *t (R(t))* je součet pravděpodobností bezporuchových stavů

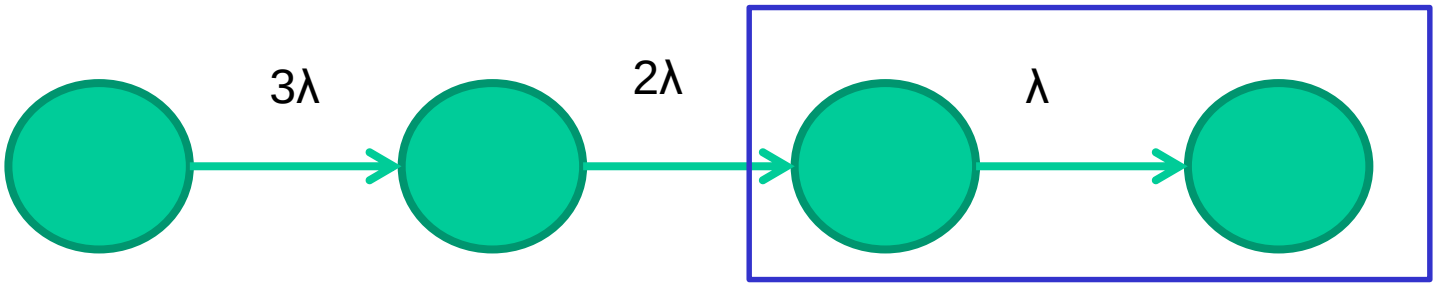
TMR

- Blokový

model struktury



Stavový - Markovký model



Výpočty

$$R_{TMR} = R^3 + 3R^2(1-R) =$$

$$R^3 + 3R^2 - 3R^3 = 3R^2 - 2R^3$$

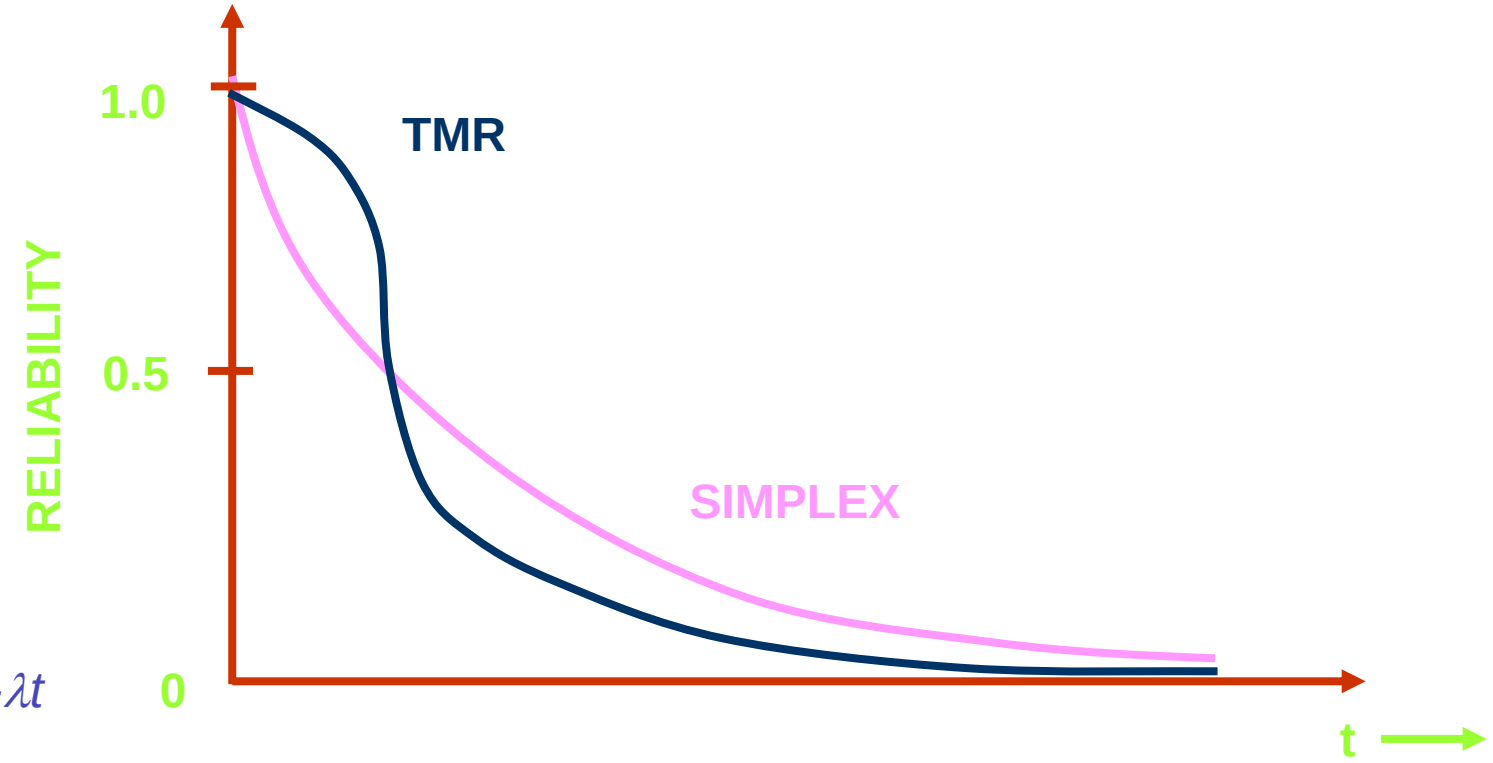
$$T_s = \frac{5}{6\lambda}$$

$$R_{TMR} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

Průběh funkce, derivace, směrnice tečny, …

Program spolehlivost

Srovnání



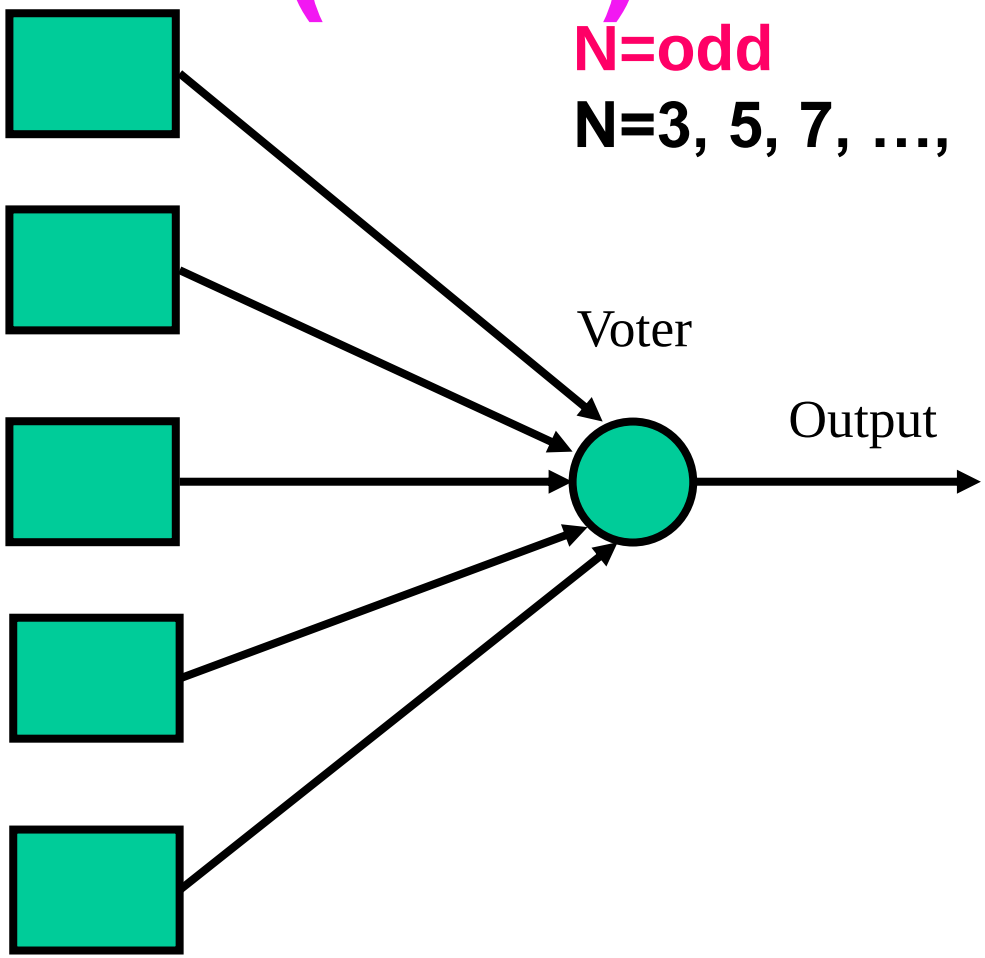
$R_M(t) = e^{-\lambda t}$

$R_{sys}(t) = 3e^{-2\lambda t} - 2\,e^{-3\lambda t}$

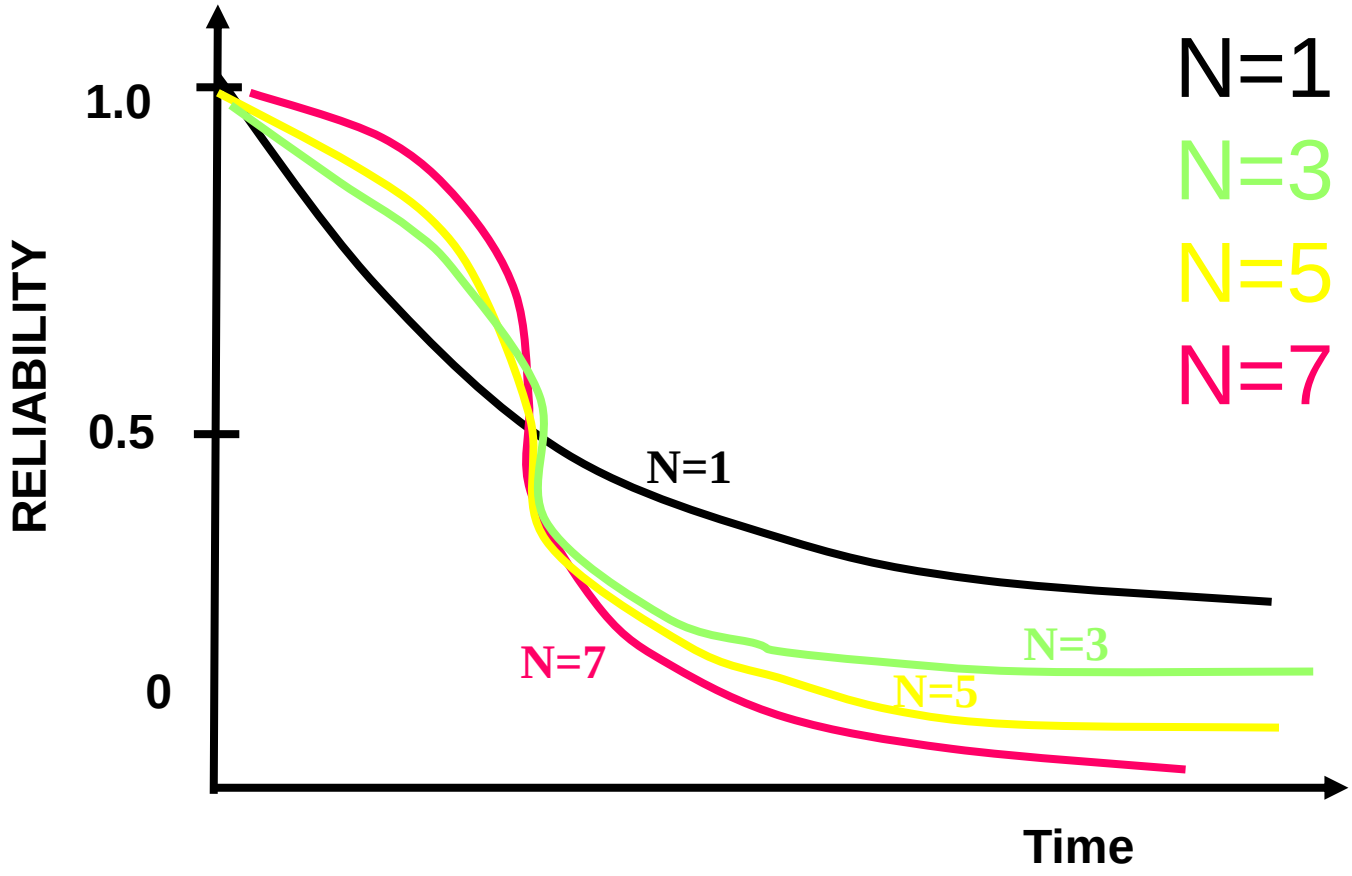
$MTTF_{TMR} = \int_0^{\infty} (3e^{-2\lambda t} - 2e^{-3\lambda t})dt = 5/6\lambda$

tudíž: $MTTF_{TMR} < MTTF_{SIMPLEX}$ ..... vysvětlit proč

N-modulární redundance (NMR)

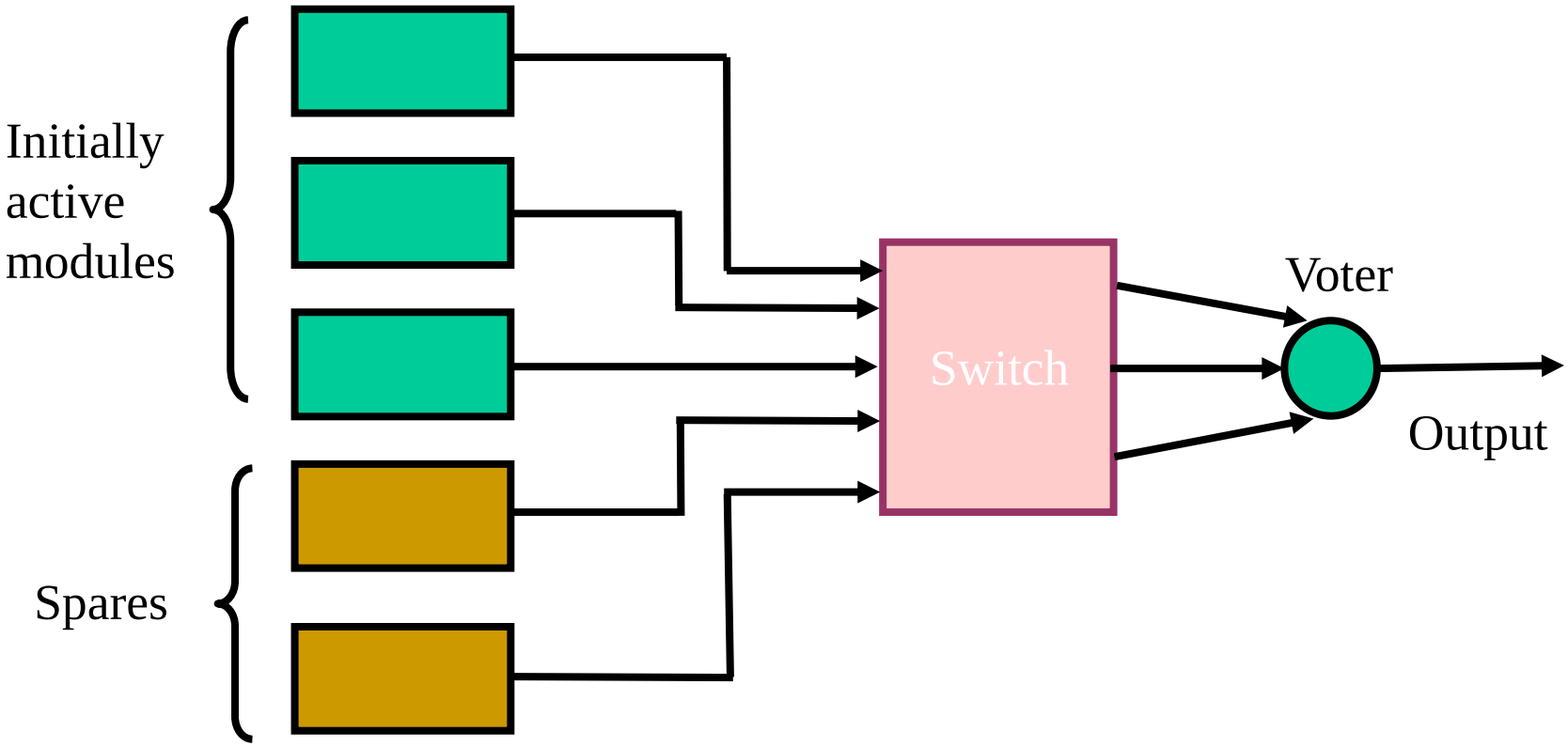


Průběhy R(t)



Hybridní redundance

- kombinace teplé a studené zálohy (GMR)



TMR/SIMPLEX

Systém pracuje jako TMR do selhání prvního modulu, pak pracuje v simplex módu ... vypne se 2. správný modul.

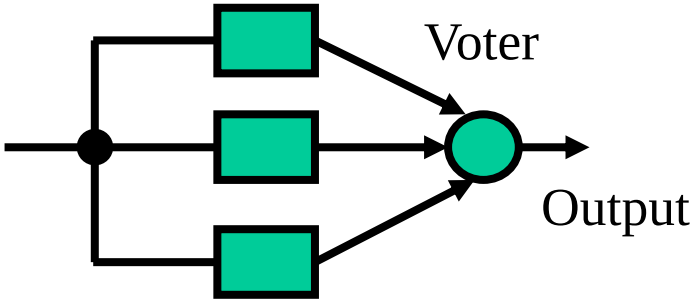
$$R_{sys} = R^3_M + 3R^2_M (1-R_M) + (3/2)R_M(1-R_M)^2$$

$$= 1.5R_M – 0.5\ R^3_M$$

$$> R_M$$

Pro $R_M = e^{-\lambda t}$

$$MTTF = (4/3\lambda)$$



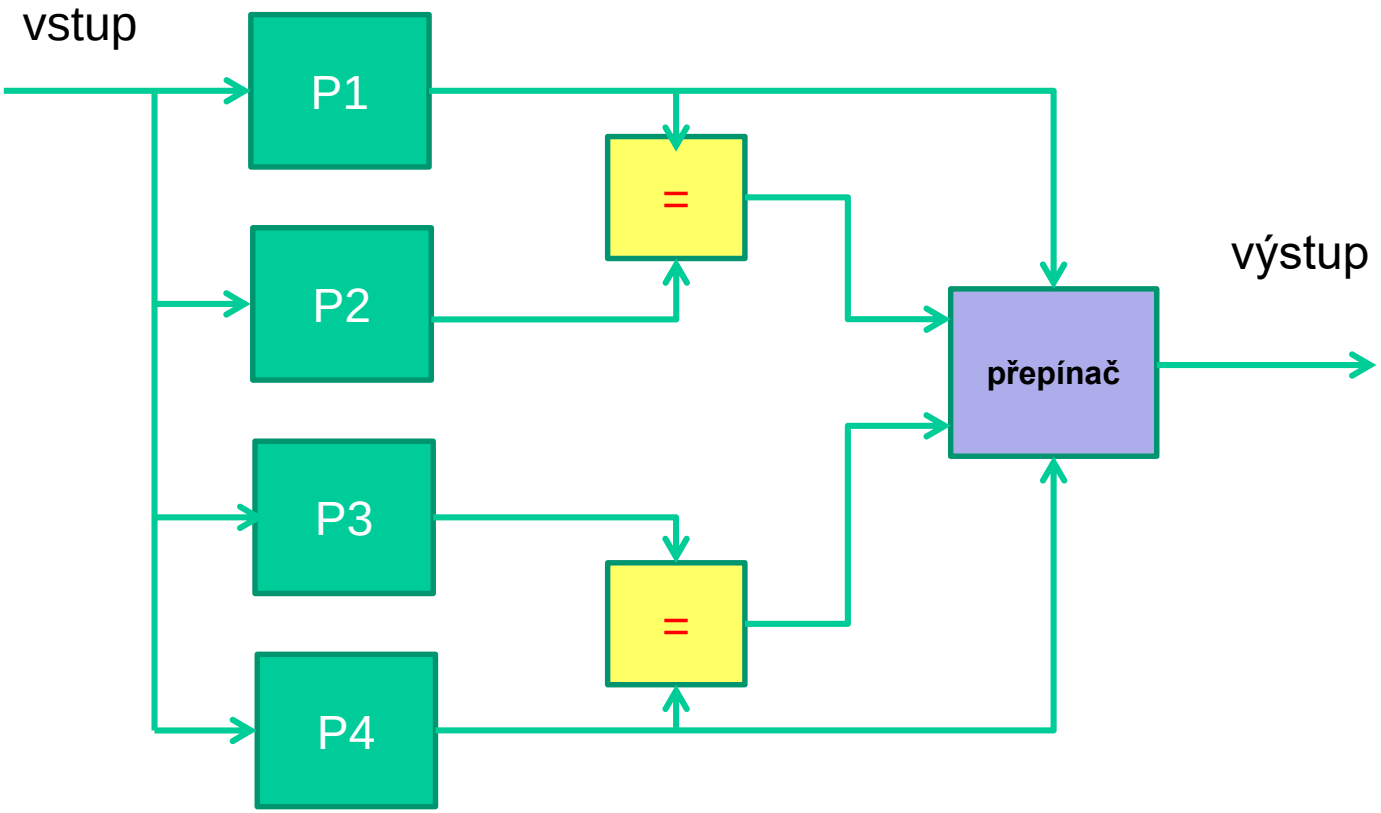
Tedy $MTTF_{TMR/SIMPLEX} > MTTF_{SIMPLEX} > MTTF_{TMR}$

$(4/3\lambda)$ $(1/\lambda)$ $(5/6\lambda)$

Co je nutné doplnit do schématu? Jaký bude overhead?

BiDuplex

- další možnost



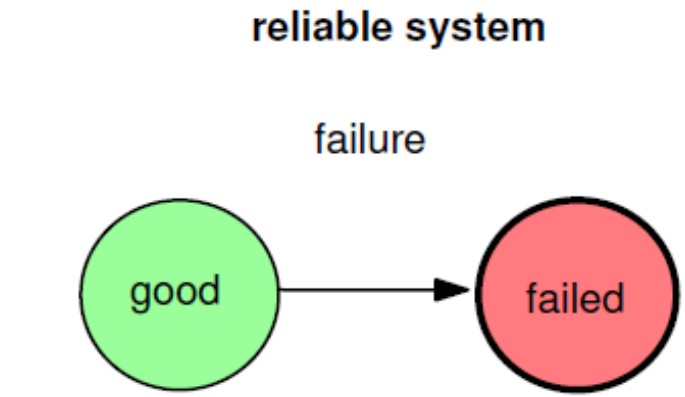
$$R = R^4 + 4(R^3(1-R)) + 2(R^2(1-R)^2) = 2R^2 - R^4$$

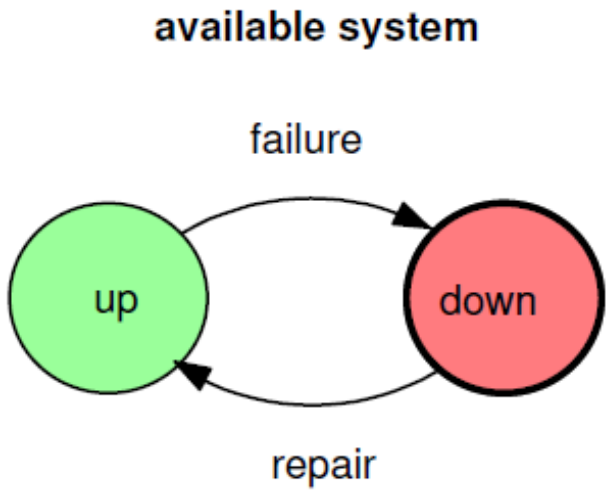
Typy záloh a organizace systému

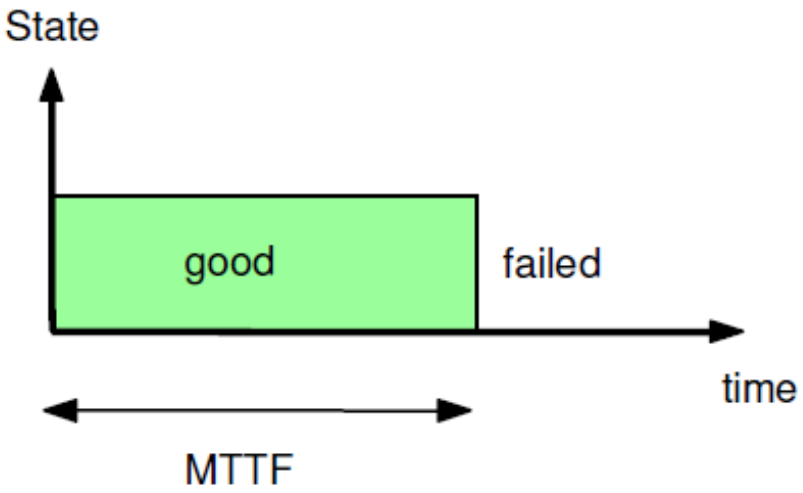
- TMR
- TMR/S
- TMR/S/S
- Duplex
- Biduplex
- GMR, NMR

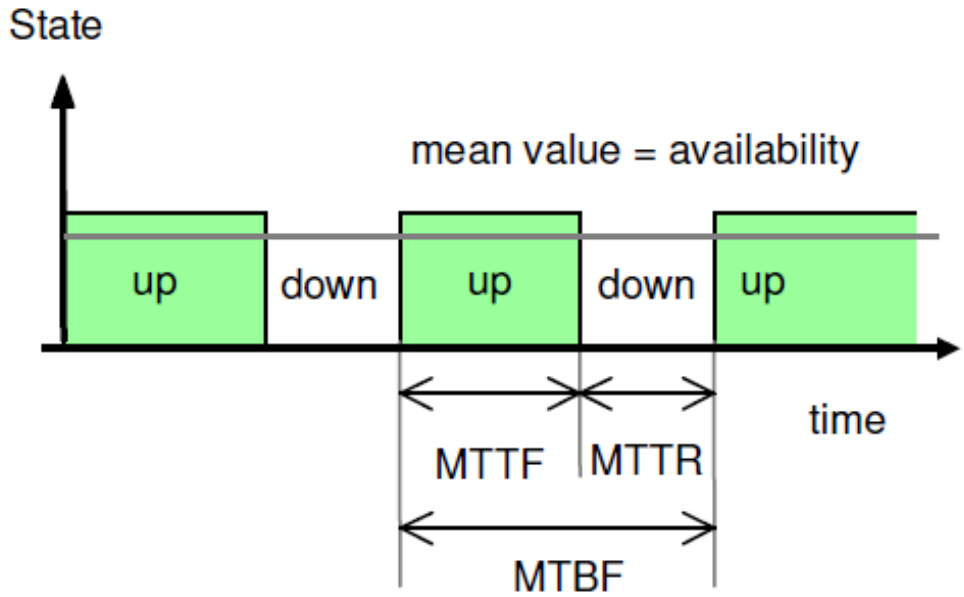
Obnovované x neobnovované systémy

Reliability vs availability



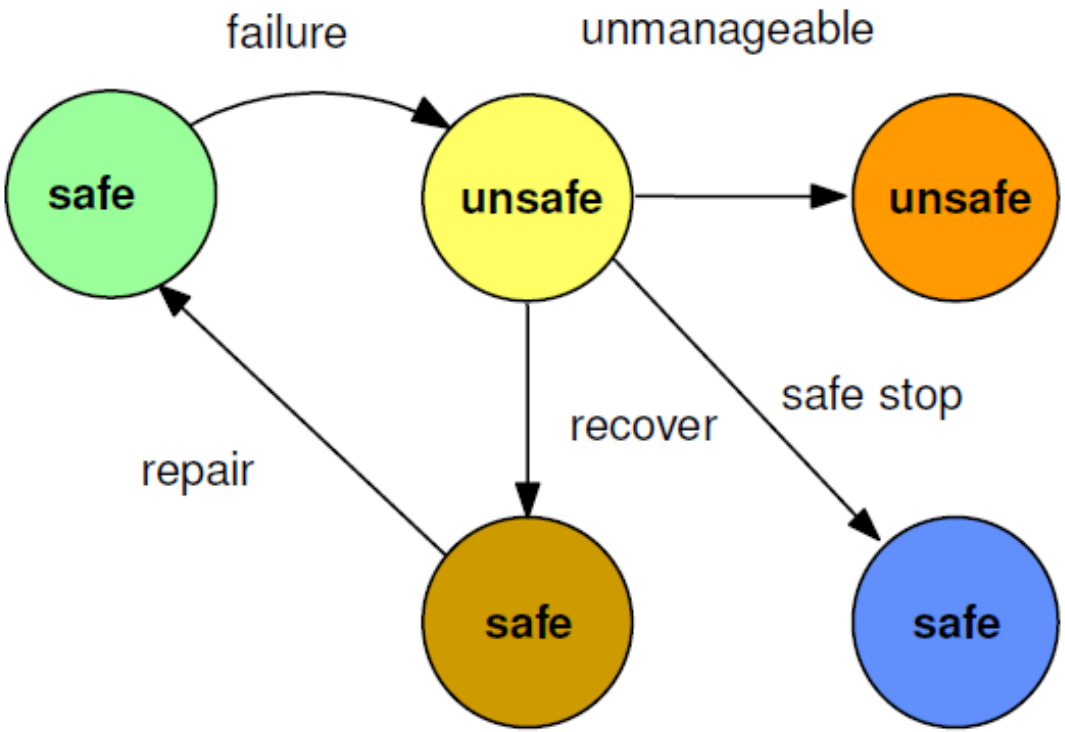




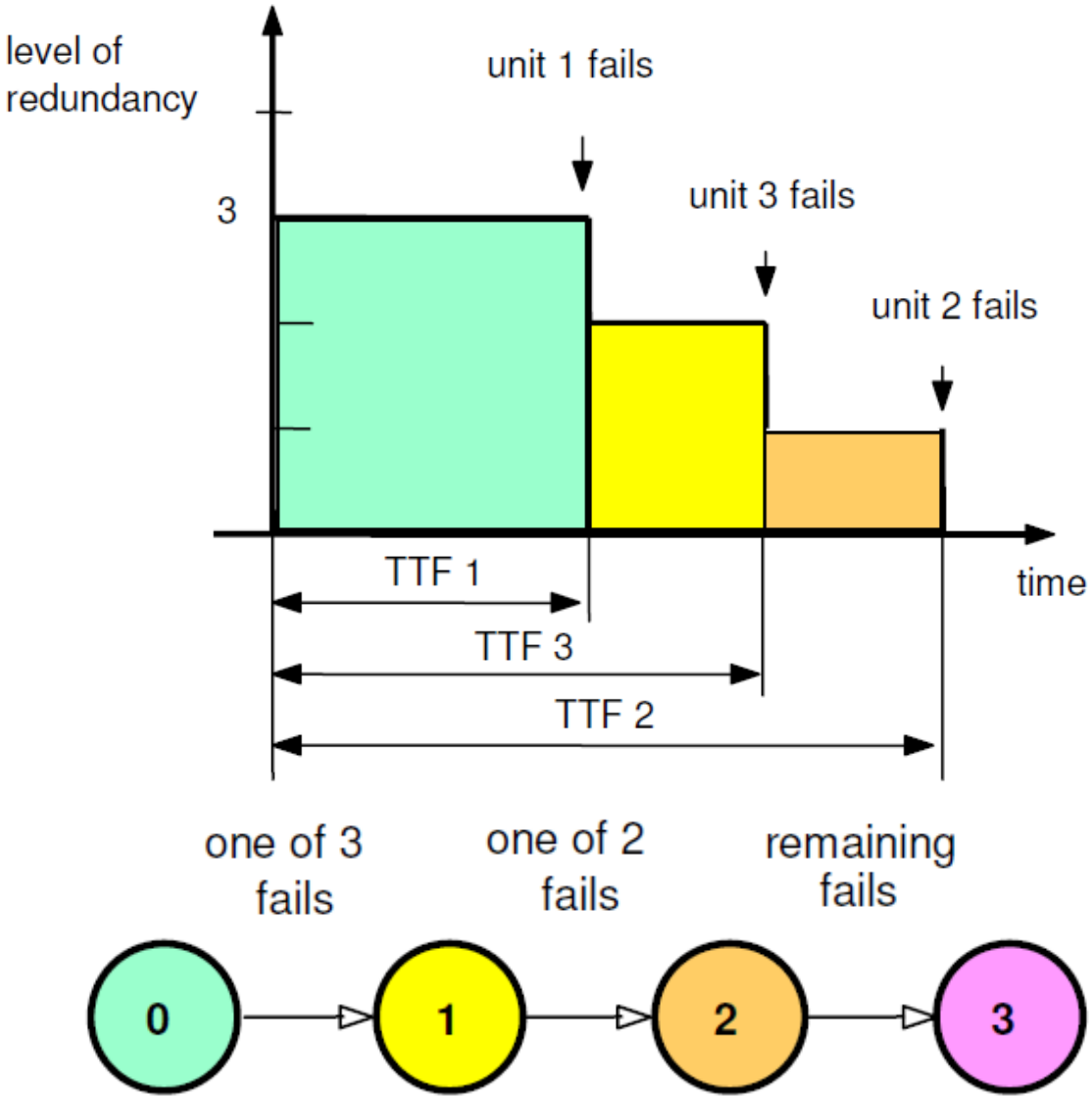


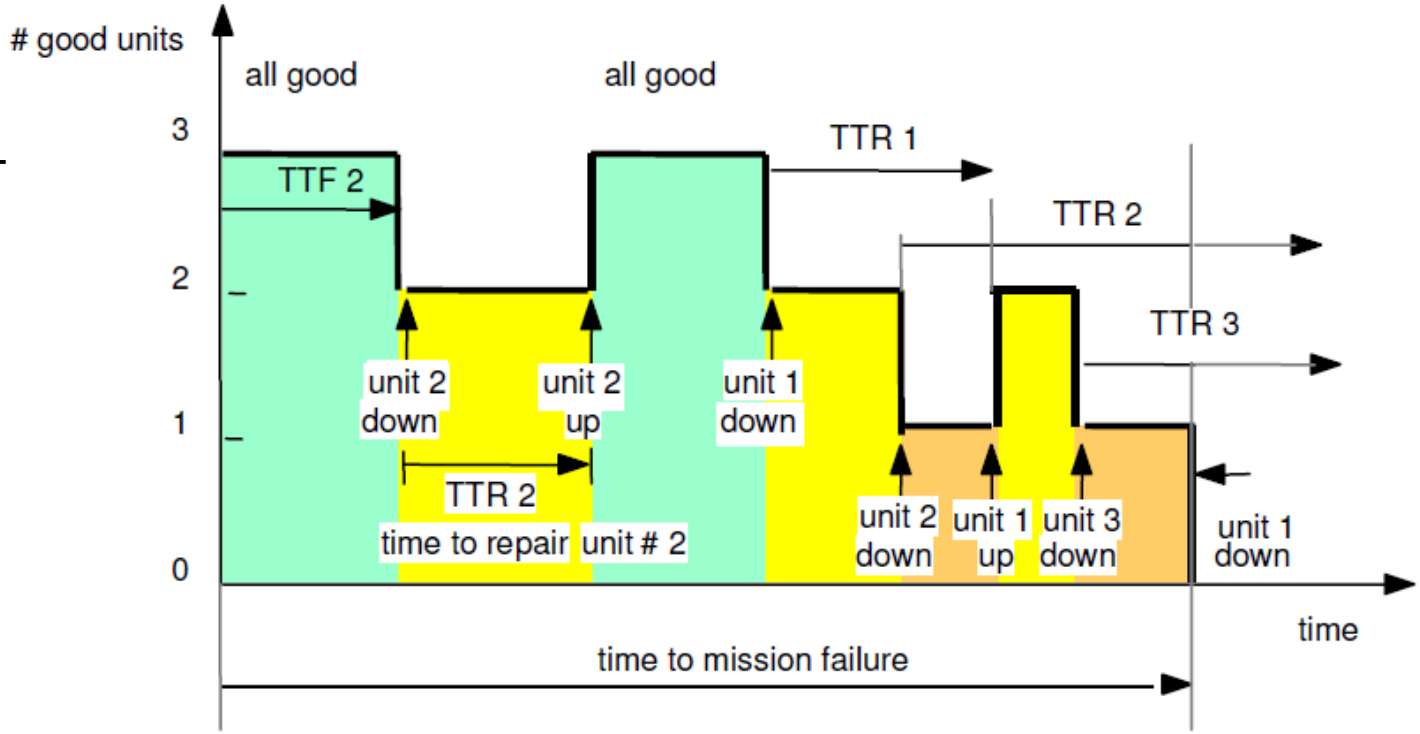
Safety

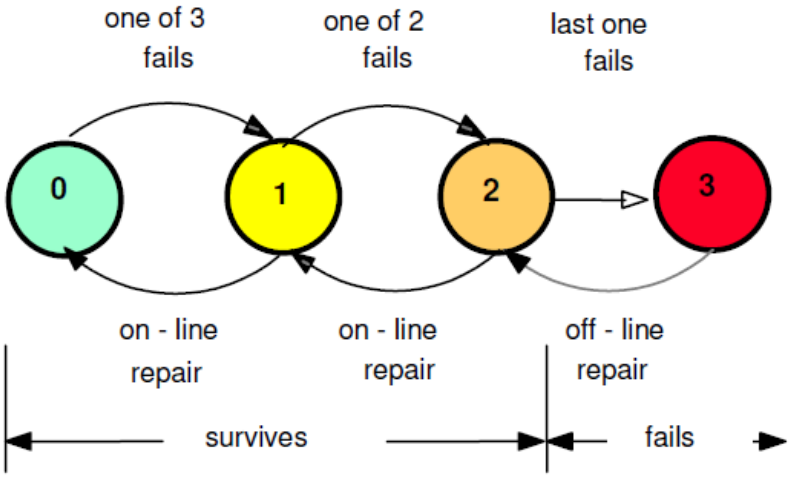
prvek nesmí selhat zakázaným způsobem:



Falt-tolerance - neopravovaný




good units
all good
all good
3
2
1
0
TTF 2
TTR 1
TTR 2
TTR 3
unit 2 down
unit 2 up
unit 1 down
TTR 2
time to repair
unit # 2
unit 2 down
unit 1 up
unit 3 down
unit 1 down
time
time to mission failure


one of 3 fails
one of 2 fails
last one fails
0
1
2
3
on - line repair
on - line repair
off - line repair
survives
fails

Další příklady

The Apollo Guidance Computer: Architecture and Operation (Springer Praxis Books) 2010th Edition by Frank O'Brien

http://www.amazon.com/Apollo-Guidance-Computer-Architecture-Exploration/dp/1441908765/ref=sr_1_1?ie=UTF8&s=books&qid=1297362971&sr=8-1

Číslicové systémy odolné proti poruchám (Hlavička, Racek, Golan, Blažek, ČVUT Praha 1992)