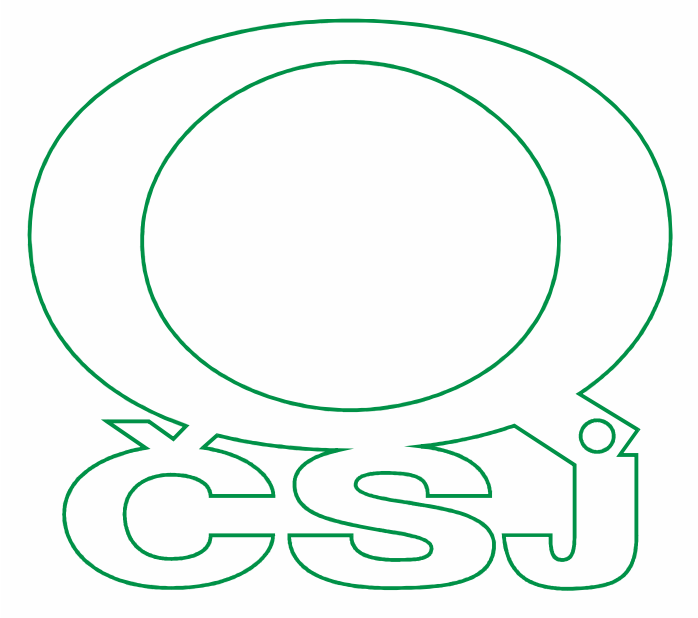
ČESKÁ
SPOLEČNOST
PRO JAKOST



Bezporuchovost a pohotovost

Materiály z 59. semináře odborné skupiny pro spolehlivost
Konaného dne 24. 2. 2015

Česká společnost pro jakost, Novotného lávka 5, 116 68 Praha 1, www.csq.cz

Obsah:

Blokové diagramy - bezporuchovost sériových a paralelních systémů

Ing. Jan Kamenický, Ph.D.
Technická univerzita v Liberci, Studentská 2, 461 17 Liberec
jan.kamenicky@tul.cz

1 Struktura systémů

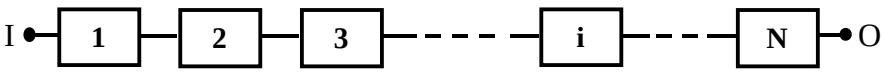
Blokové diagramy bezporuchovosti (RBD z angl. Reliability Block Diagram) jsou podmnožinou logických blokových diagramů. Obecně lze říct, že pomocí blokových diagramů jsou modelovány struktury systémů, kdy každý blok představuje prvek systému, liniemi jsou pak modelovány vazby mezi těmito prvky. Struktury systémů mohou být v zásadě čtyři:

- sériová
- paralelní
- výběrová
- smíšená

Pomocí blokových diagramů bezporuchovosti je možné modelovat všechny struktury systému, nicméně primární určení RBD je pro modelování sériových, paralelních a z nich složených smíšených systémů. Problém nastává také při modelování systémů se zpětnou vazbou. Stručně si ukažme způsob grafického záznamu a výpočtu spolehlivostních parametrů pro sériovou a paralelní strukturu systému.

1.1 Sériový systém

Nejjednodušším typem uspořádání struktury systému je sériové zapojení jeho prvků. Pozor, nejedná se o konstrukční a technologické provedení konkrétního systému! Sériovou strukturu ze spolehlivostního hlediska mé systém tehdy, jestliže platí, že při poruše kteréhokoliv jednotlivého prvku dojde k poruše celého systému (ukončení jeho schopnosti plnit požadované funkce). Příklad modelu blokového diagramu bezporuchovosti sériového zapojení systému je na Obrázek 1.



Obrázek 1: Blokové schéma sériového systému

Sériový systém se nachází v bezporuchovém stavu, jsou-li v daném okamžiku současně v bezporuchovém stavu všechny jeho prvky a naopak v poruchovém stavu se sériový systém nachází tehdy, je-li v poruchovém stavu alespoň jeden jeho prvek. Označíme-li bezporuchový stav i-tého prvku jako jev A_i a jeho poruchový stav jako jev $\overline{A}_i$ a obdobně pro systém bezporuchový stav A_S a poruchový stav $\overline{A}_S$. Pravděpodobnost toho, že se i-tý prvek systému nachází v bezporuchovém stavu označme $P(A_i) = R_i$ a pravděpodobnost poruchového stavu $P(\overline{A}_i) = Q_i$. Pro systém označme $P(A_S) = R_S$ a $P(\overline{A}_S) = Q_S$. Sériový systém, který je složen z N prvků, lze charakterizovat následujícími rovnicemi:

$$A_S = A_1 \cap A_2 \cap \ldots\ldots\ldots \cap A_i \cap \ldots\ldots\ldots \cap A_{N-1} \cap A_N = \bigcap_{i=1}^{i=N} A_i \qquad (1)$$

$$\overline{A_S} = \overline{A_1} \cap \overline{A_2} \cap \ldots\ldots\ldots \cap \overline{A_i} \cap \ldots\ldots\ldots \cap \overline{A_{N-1}} \cap \overline{A_N} = \bigcup_{i=1}^{i=N} \overline{A_i} \qquad (2)$$

Pravděpodobnost bezporuchového stavu sériového systému je:

$$R_S = P(A_S) = P(A_1 \cap A_2 \cap \ldots\ldots\ldots \ldots \cap A_i \cap \ldots\ldots\ldots \ldots \cap A_N) = P\left(\bigcap_{i=1}^{i=N} A_i\right) \qquad (3)$$

Za předpokladu vzájemné nezávislosti jednotlivých poruch prvků lze tuto rovnici přepsat do tvaru:

$$R_S = P(A_S) = P(A_1) \cdot P(A_2) \cdot \ldots\ldots\ldots \cdot P(A_i) \cdot \ldots\ldots\ldots \cdot P(A_N) = \prod_{i=1}^{i=N} R_i \qquad (4)$$

Jsou-li poruchy vzájemně závislé, je třeba pracovat s výrazem pro úplnou pravděpodobnost a rovnice má tvar:

$$R_S = P(A_1) \cdot P(A_2 \mid A_1) \cdot P(A_3 \mid A_1 \cap A_2) \cdot \ldots\ldots \cdot P(A_N \mid A_1 \cap A_2 \cap \ldots\ldots \cap A_{N-1})$$

Vzhledem k tomu, že poruchový a bezporuchový stav jsou vzájemně se vylučující stavy, platí pro pravděpodobnost poruchového stavu systému rovnice:

$$Q_S = 1 - R_S \qquad (5)$$

Přičemž pro exponenciální rozdělení platí vztah:

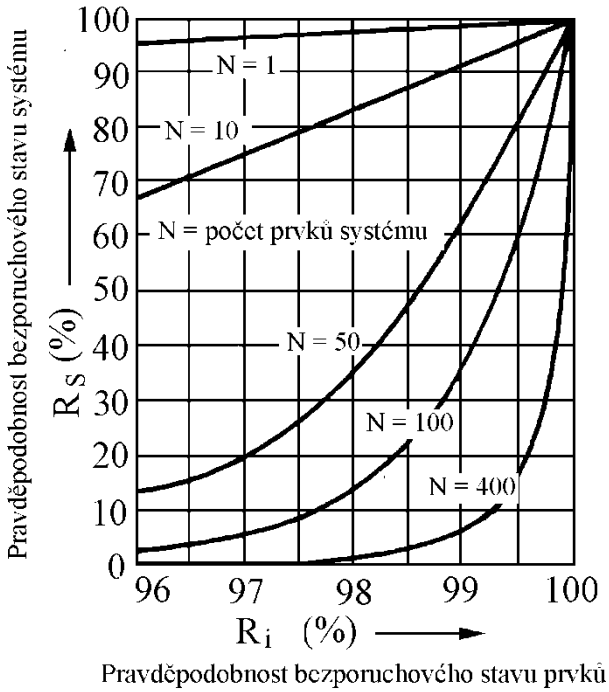
$$R_S(t) = \exp(-\lambda_S \cdot t) = \prod_{i=1}^{i=N} \exp(-\lambda_i \cdot t) = \exp\left[-\sum_{i=1}^{i=N} \lambda_i \cdot t\right] \qquad (6)$$

Z uvedené rovnice vyplývá, že:

$$\lambda_S = \sum_{i=1}^{i=N} \lambda_i \qquad (7)$$

To znamená, že rozdělení pravděpodobnosti poruch sériového systému, jehož prvky mají exponenciální rozdělení pravděpodobnosti poruch je opět exponenciální s výslednou intenzitou poruch systému rovnou součtu intenzit poruch jeho prvků.

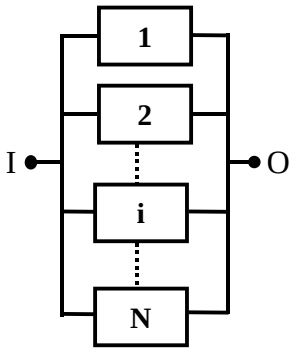
Z uvedených vztahů je zřejmé, že výsledná bezporuchovost systému se sériovým zapojením prvků je závislá na počtu prvků systému a zároveň na úrovni bezporuchovosti jednotlivých prvků. Tato skutečnost je znázorněna na Obrázek 2.



Obrázek 2: Závislost pravděpodobnosti bezporuchového provozu sériového systému na počtu a pravděpodobnosti bezporuchového provozu jeho (totožných) prvků

1.2 Paralelní systém

Druhým velmi často se vyskytujícím typem uspořádání struktury systému je paralelní zapojení jeho prvků. Opět je zde myšleno paralelní zapojení z hlediska spolehlivosti, nikoliv funkčně. Paralelní strukturou nazýváme takové uspořádání systému, pro které platí, že k poruše systému dojde až při současné poruše všech jeho prvků. Příklad blokového schématu paralelního systému je na Obrázek 3.



Obrázek 3: Blokové schéma paralelního systému

Paralelní systém se nachází v provozuschopném stavu tehdy, je-li v provozuschopném stavu alespoň jeden jeho prvek. Analogicky se paralelní systém nachází v poruchovém stavu tehdy a jen tehdy, jsou-li v poruchovém stavu současně všechny jeho prvky. Paralelní systém složený z N prvků tak můžeme charakterizovat následujícími rovnicemi:

$$A_S = A_1 \cup A_2 \cup ..... \cup A_i \cup ..... \cup A_{N-1} \cup A_N = \bigcup_{i=1}^{i=N} A_i \qquad (8)$$

$$\overline{A}_S = \overline{A}_1 \cap \overline{A}_2 \cap ..... \cap \overline{A}_i \cap ..... \cap \overline{A}_{N-1} \cap \overline{A}_N = \bigcap_{i=1}^{i=N} \overline{A}_i \qquad (9)$$

Při dalším popisu bezporuchovosti paralelního systému budeme vycházet z rovnice (6), která popisuje poruchový stav systému $\overline{A}_S$. Pravděpodobnost toho, že se paralelně uspořádaný systém

nachází v poruchovém stavu lze s využitím pravidel pro výpočet pravděpodobnosti jevů vyjádřit rovnicí:

$$Q_S = P(\overline{A}_S) = P(\overline{A}_1 \cap \overline{A}_2 \cap ..... \cap \overline{A}_i \cap ..... \cap \overline{A}_{N-1} \cap \overline{A}_N) = P\left(\bigcap_{i=1}^{i=N} \overline{A}_i\right) \quad (10)$$

Je-li vznik poruch jednotlivých prvků vzájemně nezávislý, lze tuto rovnici přepsat do tvaru:

$$Q_S = P(\overline{A}_S) = P(\overline{A}_1) \cdot P(\overline{A}_2) \cdot ..... \cdot P(\overline{A}_i) \cdot ..... \cdot P(\overline{A}_N) = \prod_{i=1}^{i=N} Q_i \quad (11)$$

Jsou-li poruchy vzájemně závislé, je třeba pracovat s výrazem pro úplnou pravděpodobnost a rovnice má tvar:

$$Q_S = P(\overline{A}_1) \cdot P(\overline{A}_2 \mid \overline{A}_1) \cdot P(\overline{A}_3 \mid \overline{A}_1 \cap \overline{A}_2) \cdot ..... \cdot P(\overline{A}_N \mid \overline{A}_1 \cap \overline{A}_2 \cap .... \cap \overline{A}_{N-1})$$

S využitím platnosti rovnice $Q_S = 1 - R_S$ (5) je možné vztah mezi pravděpodobností bezporuchového a poruchového stavu zapsat jako:

$$R_S = 1 - Q_S = 1 - \prod_{i=1}^{i=N} Q_i \quad (12)$$

Tento vztah je možné opět s využitím (5) vyjádřit jako:

$$R_S(t) = 1 - \prod_{i=1}^{i=N} [1 - R_i(t)] \quad (13)$$

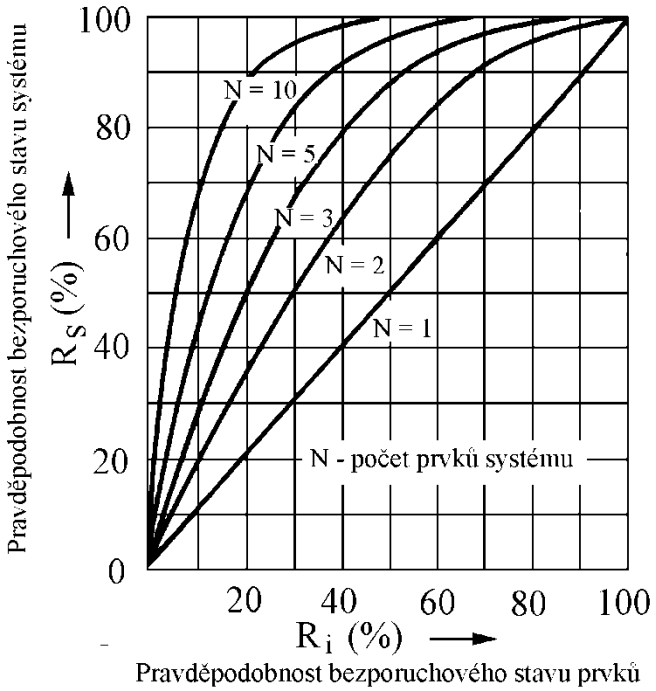
Přičemž pro exponenciální rozdělení platí vztah:

$$R_S(t) = 1 - \prod_{i=1}^{i=N} [1 - \exp(-\lambda_i \cdot t)] \quad (14)$$

Z rovnice (14) vyplývá i vztah pro intenzitu poruch paralelního systému:

$$\lambda_S = \prod_{i=1}^{i=N} \lambda_i \quad (15)$$

Stejně jako v případě sériového zapojení prvků do systému, i v případě paralelního zapojení je výsledná pravděpodobnost bezporuchového provozu, resp. pohotovost, závislá na počtu prvků sytému a jejich individuální pravděpodobnosti bezporuchového provozu. Grafické vyjádření této závislosti je uvedeno na Obrázek 4.



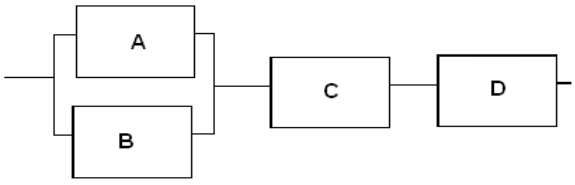
Obrázek 4: Závislost pravděpodobnosti bezporuchového provozu paralelního systému na počtu a pravděpodobnosti bezporuchového provozu jeho (totožných) prvků

2 Blokové diagramy bezporuchovosti

Blokové diagramy bezporuchovosti jsou podmnožinou logických blokových diagramů. Z toho lze odvodit, že existují i blokové diagramy poruchy, které pracují s negativní logikou, tzn., že jednotlivé bloky znázorňují poruchu prvku. Zůstaňme však u blokových diagramů bezporuchovosti. U systémů, zobrazených pomocí RBD, hledáme tzv. *úspěšnou cestu* mezi vstupní a výstupní branou diagramu. Úspěšnou cestou je množina prvků, které musí být v provozuschopném stavu, aby byla splněna funkce systému. Dalším pojmem z oblasti RBD je *minimální úspěšná cesta*, což je taková úspěšná cesta, ze které není možné odebrat žádný blok, aniž by došlo k ukončení funkce systému. Příklady grafického záznamu průběhu analýzy pomocí blokového diagramu bezporuchovosti a příklady numerického výpočtu ukazatelů spolehlivosti, jako je pravděpodobnost bezporuchového provozu a pohotovost systému budou obsahem následujících kapitol.

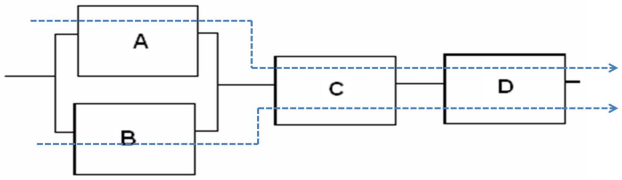
2.1 Grafická podoba RBD

Blokový diagram bezporuchovosti se skládá z bloků a čar, které symbolizují prvky systému a jejich vzájemné vazby. Vazby mohou být oboustranné i jednosměrné, v tom případě je čára nahrazena šipkou. Příklad jednoduchého blokového diagramu bezporuchovosti, znázorňujícího sério-paralelní sytém, je uveden na Obrázek 5.



Obrázek 5: Příklad sério-paralelního blokového diagramu bezporuchovosti

Graficky lze nalézt minimální úspěšné cesty tohoto modelu intuitivně, jak je zřejmé z Obrázek 6.



Obrázek 6: Znázornění úspěšných cest

Pro kontrolu grafického řešení bude uvedena časově náročná, nicméně detailní a pravdivá analýza modelové situace pravdivostní tabulkou, viz tabulku 1.

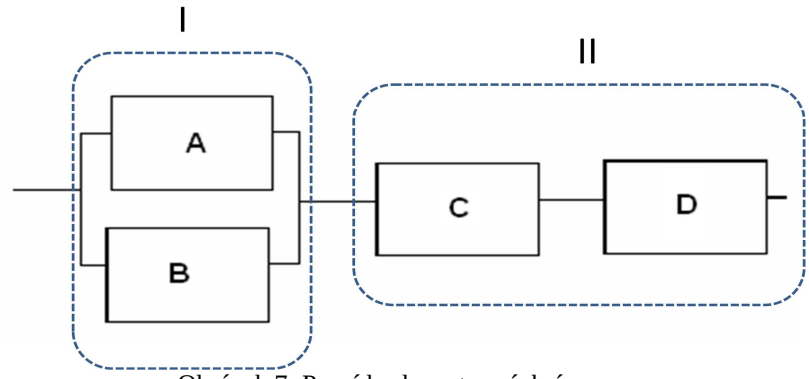
Tabulka 1: Pravdivostní tabulka řešení modelové situace RBD

Komp A.	Komp. B	Komp. C	Komp.D	Systém	Logický výraz
0	**0**	**0**	**0**	**0**	$A \cap B \cap C \cap D$
0	**0**	**0**	**1**	**1**	$A \cap B \cap C \cap \overline{D}$
0	**0**	**1**	**0**	**1**	$A \cap B \cap \overline{C} \cap D$
0	**0**	**1**	**1**	**1**	$A \cap B \cap \overline{C} \cap \overline{D}$
0	**1**	**0**	**0**	**0**	$A \cap \overline{B} \cap C \cap D$
0	**1**	**0**	**1**	**1**	$A \cap \overline{B} \cap C \cap \overline{D}$
0	**1**	**1**	**0**	**1**	$A \cap \overline{B} \cap \overline{C} \cap D$
0	**1**	**1**	**1**	**1**	$A \cap \overline{B} \cap \overline{C} \cap \overline{D}$
1	**0**	**0**	**0**	**0**	$\overline{A} \cap B \cap C \cap D$
1	**0**	**0**	**1**	**1**	$\overline{A} \cap B \cap C \cap \overline{D}$
1	**0**	**1**	**0**	**1**	$\overline{A} \cap B \cap \overline{C} \cap D$
1	**0**	**1**	**1**	**1**	$\overline{A} \cap B \cap \overline{C} \cap \overline{D}$
1	**1**	**0**	**0**	**1**	$\overline{A} \cap \overline{B} \cap C \cap D$
1	**1**	**0**	**1**	**1**	$\overline{A} \cap \overline{B} \cap C \cap \overline{D}$
1	**1**	**1**	**0**	**1**	$\overline{A} \cap \overline{B} \cap \overline{C} \cap D$
1	**1**	**1**	**1**	**1**	$\overline{A} \cap \overline{B} \cap \overline{C} \cap \overline{D}$

Z pravdivostní tabulky je zřejmé, že výsledkem jsou tři úspěšné cesty, přičemž pouze dvě z nich jsou minimální úspěšnou cestou. Jedná se o stavy systému, kdy jsou v provozuschopném stavu tyto množiny prvků: {A, B, C, D}, {A, C, D} a {B, C, D}. Je zřejmé, že první množina není minimální úspěšnou cestou, protože lze nalézt prvek, po jehož odebrání zůstane množina stále úspěšnou cestou. V následující kapitole bude představen další způsob výpočtu RBD.

2.2 Příklady výpočtu RBD

I v této kapitole budeme pracovat s jednoduchým modelem systému dle obrázku 5. Pro výpočet použijeme metodu postupných úprav. V prvním kroku výpočtu provedeme dvě operace naráz, upravíme oblasti I a II, viz obrázek 7.



Obrázek 7: První krok postupných úprav

V případě paralelního systému, tvořeného prvky A a B dostaneme zastupující prvek „I“, jehož pravděpodobnost bezporuchového provozu, vypočtená ze znalosti pravděpodobností =1−1− ·1− = + − ( )· ( ) (16).

(16)

Analogicky vztah pro výpočet pravděpodobnosti bezporuchového provozu zastupujícího prvku „II“ lze vyjádřit dle (17):

(17)

Po provedení těchto úprav dostaneme zjednodušený RBD, skládající se de facto pouze ze dvou komponent, I a II v sériovém zapojení. Pravděpodobnost bezporuchového provozu takto strukturovaného systému je možno vypočítat dle (18).

(18)

Po zpětném dosazení je možné vyjádřit výslednou pravděpodobnost bezporuchového provozu systému pomocí pravděpodobností bezporuchového provozu jednotlivých prvků systému, viz (19).

(19)

Výraz (19) lze dále zjednodušit na (20):

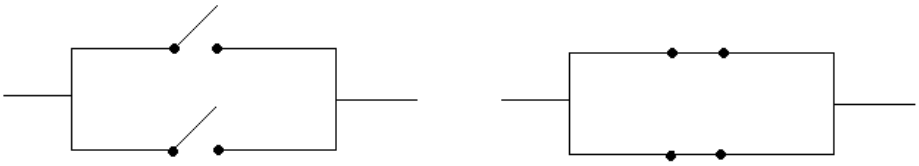
(20)

Z tohoto výrazu jsou dobře vidět minimální úspěšné cesty RBD: {A, C, D} a {B, C, D}. V případě takto jednoduchého modelu, resp. modelovaného systému, lze minimální úspěšné cesty nalézt i bez pomoci matematického aparátu, ovšem pro složitější systémy je nezbytné používat pravidla Booleovské algebry.

3 Logika RBD

Jak bylo uvedeno již v kapitole 1.1, může v praxi existovat rozpor mezi funkčním a spolehlivostním uspořádáním systému. Pro ukázku budou popsány dva případy, kdy se funkční uspořádání liší od toho spolehlivostního.

Prvním příkladem, uvedeným na Obrázek 8, je dvojice paralelně zapojených spínačů. V prvním případě se jedná o spínací kontakty, kdy požadovanou funkcí je sepnutí obvodu. Z toho vyplývá, že funkce bude splněna již při funkčnosti jednoho spínače, tedy zapojení je i ze spolehlivostního hlediska paralelní. V druhém případě máme technologicky paralelně zapojené rozpínací kontakty, jejichž funkcí je rozepnutí obvodu. Tady je zřejmé, že funkce bude splněna pouze při současné funkčnosti obou spínačů, a proto se ze spolehlivostního hlediska jde o sériové uspořádání.



Obrázek 8: Příklad technologického paralelního zapojení

Jako druhý příklad rozdílnosti chápání struktury systému budiž uvedeno potrubí na pitnou vodu. Na trase dopravy pitné vody je nainstalována chemická úpravna vody, chemická analýza vody a nádrž se pstruhy. Toto všechno je z pohledu odběratele na linii, tedy sériově. Ovšem pokud se podíváme na funkci zásobování pitnou nezávadnou vodou, resp. obyvatelstvo nebude ohroženo kvalitou vody, zjistíme, že stačí, aby jediné z vyjmenovaných zařízení bylo v provozu, a voda o snížené kvalitě se nedostane ke koncovému odběrateli - buď bude chemicky upravena, nebo bude její snížená kvalita odhalena při chemickém rozboru, resp. biologicky pomocí živých pstruhů. Ze spolehlivostního pohledu jsou tato tři místa na linii v paralelním uspořádání.

4 Závěr

Metoda blokových diagramů bezporuchovosti je relativně snadná na zpracování, nevyžaduje softwarovou podporu (pro méně složité systémy), a proto je poměrně široce používána. Na základě analýzy minimálních úspěšných cest je možné získat seznam prvků, jejichž porucha by způsobila poruchu celého systému, čehož se hojně využívá např. v petrochemickém nebo plynárenském průmyslu pro určení těch zařízení, kam je vhodné alokovat zvýšené finanční prostředky na údržbu, včetně monitoringu stavu těchto zařízení. Tento text může sloužit jako návod k základnímu použití metody blokových diagramů bezporuchovosti a jako inspirace, které oblasti lidské činnosti je možné pomocí RBD modelovat.

Literatura

[1] ČSN EN 61078:2006 Techniky analýzy spolehlivosti - Blokový diagram bezporuchovosti a booleovské metody

[2] Fuchs, P.: Využití spolehlivosti v provozní praxi, Liberec, 2002

Pohotovost výběrových systému podle návrhu konfigurace K z N a způsobu provozování

Ing. Jaroslav Zajíček, Ph.D.
Technická univerzita v Liberci, Studentská 2, Liberec 461 17
jaroslav.zajicek@tul.cz

1 Úvod

Splnění vysokých nároků na pohotovost a bezpečnost poskytované funkce ovlivňuje jak samotná inherentní poruchovost, tak i způsob provozování a údržby jednotlivých zařízení. Kritická místa systému lze efektivně zodolnit standardním zálohováním nebo použitím tzv. výběrového systému.

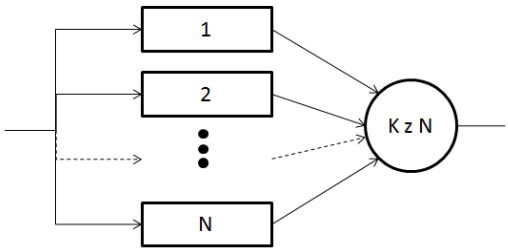
Výběrové systémy jsou systémy, u kterých je pro splnění funkce postačující, aby byl z celkového počtu komponent provozuschopný alespoň nějaký, předem definovaný, počet těchto komponent. Takový typ zálohování je využitelný pro statická (např. chladiče), rotační (např. čerpadla) i elektrická/elektronická (např. měření teploty) zařízení.

Zmíněné standardní zálohování pomocí paralelního uspořádání vzhledem k poskytované funkci je v podstatě tou nejjednodušší variantou výběrového systému, kdy pro splnění funkce celého systému je dostačující provozuschopnost jedné z komponent. Fyzické uspořádání komponent v takovém systému často též odpovídá paralelnímu uspořádání, ale není to podmínkou, a je zcela zásadní nezaměňovat fyzické a funkční zapojení komponent v systému.

2 Výběrový systém

V odborné literatuře se výběrové systémy nejčastěji označují dvěma způsoby, a to K-out-of-N nebo M-good-of-N. Systém M-good-of-N je provozuschopný, pokud alespoň M komponent z celkového počtu N je provozuschopných. Označení K-out-of-N ovšem není jednoznačně používáno a v literatuře je definováno buď stejně jako systém M-good-of-N nebo naopak takovým způsobem, že systém se stává neprovozuschopným, pokud je v neprovozuschopném stavu alespoň K komponent z celkového počtu N. V tomto článku budeme systém označovat jako K z N a definován bude první variantou.

Schematicky se výběrový systém znázorňuje dle Obr. 1.



Obr. 1 Schéma výběrového systému K z N

Existují realizace, kdy je hodnota N pevně dána a hodnota K se mění na základě dalších podmínek. Typickým příkladem je například systém chladičů, u kterého pro dostatečné chlazení média potřebujeme jiný počet funkčních chladičů v letním a v zimním období.

3 Provozní podmínky výběrového systému

Tentýž výběrový systém, sestávající se z fyzicky i funkčně stejných komponent, může vykazovat různé spolehlivostní parametry při odlišné vrcholové funkci systému a při odlišném způsobu péče o zařízení. Např. „záložní“ komponenty, které se za předpokladu provozuschopnosti všech dílčích částí systému vyskytují v počtu N-K, mohou být provozovány formou horké či studené zálohy.

3.1 Horká a studená záloha

Horká záloha je forma zálohování, kdy všechny komponenty systému vykonávají paralelně funkci, zatímco u studené zálohy vykonává funkci pouze K komponent a při poruše některé z nich je následně nahrazena provozuschopnou komponentou v záloze.
Toto rozlišení je důležité pro systémy složené z komponent s neexponenciálním pravděpodobnostním rozdělením poruch, kdy se navíc zjednodušeně předpokládá, že komponenta stárne pouze při vykonávání své funkce. V případě exponenciálního rozdělení pravděpodobnosti poruchy (konstantní intenzita poruch) by se mohlo zdát, že není nutné typ zálohy rozlišovat, pokud předpokládáme, že komponenta ve studené záloze dokáže funkci nahradit neprodleně po náhodné poruše a nehrozí tedy krátkodobá ztráta funkce a s ní například spojené výrobní ztráty či ohrožení bezpečnosti. I v tomto případě může být volba horké/studené zálohy důležitá, a to z důvodu ovlivnění doby latence u skrytých poruch. Především u zařízení, u kterých může nastat porucha i v offline režimu (a výše zmíněným předpokladem exponenciálního rozdělení) je vhodnější je provozovat ve stavu horké zálohy.

3.2 Zjevnost poruch

Jak již bylo nastíněno v předchozím odstavci, dalším členění, které je nezbytné (nejen u výběrových systémů) zohlednit, je způsob identifikace poruch, respektive poruchových stavů. Poruchy dělíme na poruchy zjevné a skryté. Porucha je zjevná, pokud je ihned identifikována, a to například pomocí ztráty funkce, autodiagnostiky, řídicího a informačního systému apod. Naopak porucha skrytá je odhalena až při požadavku na vykonání funkce nebo pomocí pravidelných inspekčních kontrol stavu komponenty, které se vykonávají právě z důvodu zjištění latence poruch. Skrytost poruch se týká především systémů s nízkým vyžádáním funkce, mezi které patří například bezpečnostní systémy. Uvědoměním si zjevnosti poruch lze u obnovovaných/opravovaných systémů řídit hodnotu pohotovosti, a to právě pomocí doby do obnovy, která je často z dominantní části tvořena právě dobou latence.

3.3 Způsob údržby

K výběrovému systému lze přistupovat z pohledu údržby dvěma hlavními způsoby. Prvním způsobem je provádění preventivních zásahů na systému. Preventivním zásahem na systému pak rozumíme nejen preventivní údržbové úkony na jednotlivých komponentách, ale i výměnu/opravu komponent v poruchovém stavu, které dosud nezpůsobily poruchu funkce celého systému. Preventivní údržba výběrového systémů dává na výběr velký počet možností a není zpravidla snadné určit, která z variant je optimální. Podrobněji se preventivní údržbě budeme věnovat v kapitole 5 a v případové studii (kapitola 6).
Druhou alternativou je tzv. „běh do poruchy“ (z anglického „Run to Failure“ - značí se RTF), kdy na systému není vykonávána žádná preventivní údržba a zásah do komponent/systému následuje až po ztrátě funkce systému. Na systému může být realizováno sledování stavu pro případ latence poruchy funkce, toto však nepovažujeme za preventivní zásah do zařízení, který ovlivní poruchovost.

3.4 Požadavek na bezporuchovost / pohotovost

Základní dva spolehlivostní ukazatele, které se pro ohodnocení v oblasti spolehlivosti pro technická zařízení používají, jsou bezporuchovost a pohotovost.
Zatímco bezporuchovost vyjadřuje pravděpodobnost, že systém vydrží bez poruchy alespoň po dobu T, pohotovost je vyjádřením pravděpodobnosti, že se systém nachází v provozuschopném stavu. Bezporuchovost lze stanovit u obnovovaných i neobnovovaných systému, zatímco pohotovost se určuje pouze u obnovovaných systémů, protože do výpočtu navíc vstupuje i doba obnovy funkce.
V případech, kdy jsou hodnoty těchto ukazatelů velmi blízké hodnotě 1 (resp. 100 %), používá se vyjádření pomocí doplňkových ukazatelů.
Bezporuchovost je důležitým ukazatelem zejména u systémů s nákladnou obnovou, stanovení pohotovosti se pak často realizuje v případech, kdy náklady, případně riziko u bezpečnostních systémů, poruchy jsou úměrné (zpravidla se nejedná o přímou úměrnost) době obnovy.

4 Výpočet ukazatelů spolehlivosti

4.1 Základní výpočet bezporuchovosti a pohotovosti

Nejprve budeme uvažovat výběrový systém K z N složený z identických komponent dle schématu na obr. 1. Celkovou bezporuchovost systému označíme R_S a bezporuchovost jednotlivých komponent R_x. Bezporuchovost systému odpovídá následujícímu vztahu (1).

$$R_S = \sum_{i=K}^{N} \binom{N}{i} \cdot R_x{}^{i} \cdot (1 - R_x)^{N-i} \qquad (1)$$

Na základě tohoto vztahu jsou v tab. 1 přiřazeny možné typy výběrových systémů (v tabulce je označení jako K/N) pro různé hodnoty bezporuchovosti komponenty a požadovanou bezporuchovost systému.

Tab. 1 Příklady výběrových systému, které při hodnotách bezporuchovosti komponenty splňují požadovanou bezporuchovost systému

Bezporuchovost systému R_S	Bezporuchovost komponenty R_x					
	0,5	0,6	0,7	0,8	0,9	0,95
$x \in (0; 0{,}5 >$	2/3 3/4 3/5 4/5	3/4 4/5				
$x \in (0{,}5; 0{,}7 >$	2/4	2/3 3/5	3/4 4/5			
$x \in (0{,}7; 0{,}9 >$	2/5	2/4	2/3 3/5	2/3 3/4 4/5		
$x \in (0{,}9; 0{,}95 >$		2/5	2/4	3/5	3/4 4/5	
$x \in (0{,}95; 0{,}99 >$			2/5	2/4	2/3	3/4 4/5
$x \in (0{,}99; 0{,}999 >$				2/5	2/4 3/5	2/3 3/5
$x \in (0{,}999; 1)$					2/5	2/4 2/5

Při odlišných hodnotách bezporuchovosti jednotlivých komponent nelze použít zjednodušení pomocí sumy a kombinačního čísla, ale bylo by nutné sečíst všechny pravděpodobnosti vyhovujících disjunktních stavů systému. Princip výpočtu zůstává samozřejmě totožný.
Vzhledem k tomu, že bezporuchovost i pohotovost jsou pravděpodobnosti, je vztah (1) použitelný i pro výpočet pohotovosti systému (značíme A_S), pouze bezporuchovost komponent R_x nahradíme pohotovostí komponent A_x.

Při exponenciálním rozdělení pravděpodobnosti poruchy komponent se hodnota bezporuchovosti R_x vypočte dle vztahu (2), hodnota pohotovosti A_x pak dle vztahu (3),

$$R_x = e^{-\lambda \cdot t} \quad (2)$$

$$A_x = \frac{\mu}{\lambda+\mu} = \frac{\frac{1}{MTTR}}{\frac{1}{MTBF}+\frac{1}{MTTR}} = \frac{MTBF}{MTBF+MTBF} \quad (3)$$

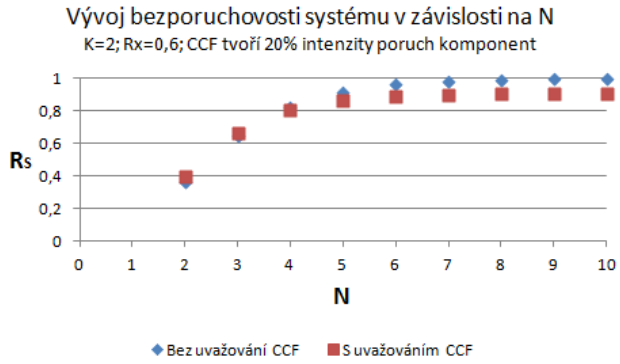
kde:

- t je čas [h],
- λ je intenzita poruch [h^{-1}],
- μ je intenzita obnovy [h^{-1}],
- $MTBF$ je střední doba mezi poruchami [h],
- $MTTR$ je střední doba do obnovy [h].

V případě bezporuchovosti se hodnota mění v závislosti na čase t, pohotovost je zde chápána jako ustálená hodnota pohotovosti v čase $t \rightarrow \infty$.

4.2 Poruchy se společnou příčinou

Pro větší přiblížení výpočtového modelu skutečnosti je v některých případech nutné zohlednit i tzv. poruchy se společnou příčinou (značí se CCF), které mají tu vlastnost, že z jisté příčiny nastane ztráta funkce na více (v nejhorším případě všech) komponentách systému souběžně a celý systém přestane plnit požadovanou funkci.
Může se jednat například o ztrátu napájení, poruchu vyhodnocovacího členu, klimatický jev, mechanické poškození apod.
Uvažovat poruchy se společnou příčinou je důležité především pro výběrové systémy s vysokou hodnotou N, přičemž za vysokou hodnotu lze považovat již hodnotu 5 nebo 6 (závisí na poměrovém zastoupení poruch se společnou příčinou). Zvyšování hodnoty N výběrového systému tak nevede ke zvyšování bezporuchovosti limitně k hodnotě 1, ale k hodnotě bezporuchovosti spočtené z intenzity poruch ze společných příčin. Neuvážené navyšování hodnoty N pak může být nejen plýtváním finančními prostředky, ale i vytvořením složitého systému s obtížnou obsluhou a údržbou.
Příklad závislosti bezporuchovosti systému bez / s uvažováním poruch se společnou příčinou na hodnotě N je znázorněn na obr. 2.

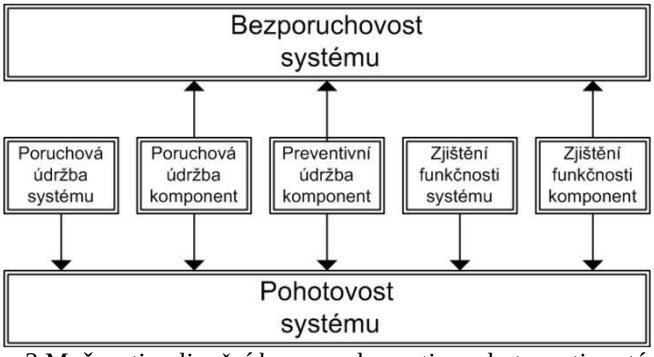


Obr. 2 Vliv CCF na bezporuchovost výběrového systému

V tomto případě se předpokládalo, že porucha se společnou příčinou se projeví na všech komponentách výběrového systému. Pokud by ovlivňovala jenom některé, muselo by se k výpočtu přistoupit tak, že komponenty jsou odlišné, případně je rozdělit po skupinách a výpočet provést pomocí výčtu všech disjunktních možností, tak jako již bylo výše popsáno u základního výpočtu bezporuchovosti v kap. 4.1.

4.3 Zařazení údržby do výpočtu spolehlivostních ukazatelů

Pomocí jistých úkonů lze v některých případech zásadním způsobem ovlivnit spolehlivostní ukazatele výběrových systému. Mezi tyto úkony patří především úkony preventivní a poruchové údržby, přičemž do preventivní údržby se zahrnují i úkony prediktivní. V případě latentnosti poruch je pak žádoucí aplikovat i úkony sledování stavu, a to na úrovni komponent výběrového systému i na úrovni systému jako celku. Ovlivnění bezporuchovosti a pohotovosti systému uvedenými úkony znázorňuje obr. 3.



Obr. 3 Možnosti ovlivnění bezporuchovosti a pohotovosti systému

K těmto úkonům se stanovují spolehlivostní a ekonomické ukazatele.

U poruchové a preventivní údržby je to především:

- typ úkonu,
- interval provádění,
- ND skladem Ano/Ne,
- doba trvání úkonu (včetně zahrnutí případné doby dodání ND a všech přípravných prací),
- ztráta funkce během doby údržby Ano/Ne,
- náklady úkonu údržby (mzdové, materiálové, ztráty z nevýroby).

U zjištění funkčnosti je pak důležitý interval provádění a náklady za provedení úkonu.

Před přiřazením úkonu do programu údržby je nutné zjistit, případně odhadnout, podle jakého rozdělení pravděpodobnosti se daný způsob poruchy chová. Například způsob poruchy s exponenciálním rozdělením, tj. rozdělením, kdy je intenzita poruchy v čase konstantní, nebo s jiným rozdělením, kde intenzita poruch s časem dokonce klesá, není vhodný pro jakoukoliv časovou preventivní údržbu.

Pozn.: Časová údržba se provádí v pravidelných intervalech, přičemž řídícím parametrem mohou být kromě času (provozního nebo kalendářního) například najeté kilometry, počet vyrobených kusů apod.

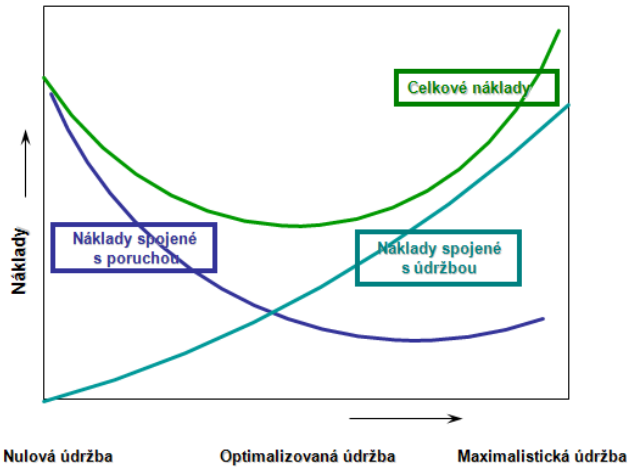
U takových zařízení se pak lze rozhodnout pro údržbu prediktivní nebo vědomé provozování zařízení do poruchy.

Souběžně s plánováním programu údržby je nutné stanovit, jakým způsobem se údržba projeví na samotném rozdělení pravděpodobnosti poruchy. V praxi není standardně možné takovou závislost získat matematicky pro nedostatek generických dat, proto se většinou přistupuje k expertním odhadům základních ukazatelů spolehlivosti, například střední doby mezi poruchami MTBF s tím, že u časového průběhu intenzity poruchy se omezíme na znalost toho, zda je v čase konstantní, klesající nebo rostoucí.

5 Řízení rizika výběrových systémů

Cílem aplikace výběrových systémů není dosažení co nejvyšší hodnoty bezporuchovost nebo pohotovosti, ale dosažení ekonomického nákladového minima při zohlednění výrobních a bezpečnostních rizik, případně dosažení co nejvyššího poměru mezi snížením rizika plynoucího z poruchy a mezi náklady investovanými na snížení tohoto rizika. V prvním případě hovoříme o

absolutní hodnotě úspor, standardně vztažených na období 1 rok, a v druhém případě o indexu efektivnosti, který se například v metodice RCM (Reliability Centered Maintenance) označuje jako MEI (Maintenance Effectivity Index).
Speciálním případem jsou bezpečnostní systémy a systémy podléhající určitým legislativním nařízením, kde je prvořadé dosažení hraniční hodnoty udávaného spolehlivostního ukazatele a teprve následně je možné zohledňovat ekonomické minimum.
Obecná ekonomická optimalizace systému pomocí údržby je zobrazena na následujícím obr. 4. Náklady jsou sumou nákladů materiálových, mzdových, plynoucích z neprodukce, bezpečnostních (v oblasti zdravotní i životního prostředí).



Obr. 4 Optimalizace údržby systému

U výběrových systémů je situace poněkud složitější, především pokud takový systém chceme teprve navrhnout na základě požadovaných parametrů.
Nejprve uvažujme výběrový systém, který je již definován (používán) a pro dosažení ekonomického minima při zajištění požadovaných spolehlivostních ukazatelů lze variovat pouze s programem údržby. Údržba výběrového systému může být dle následujících modelů:

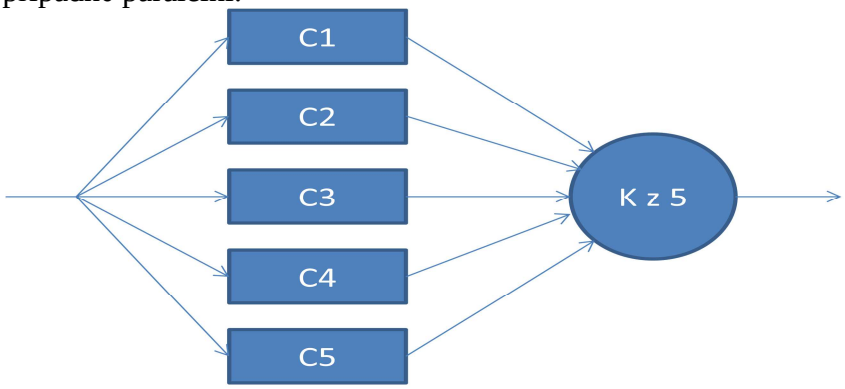
- provoz celého systému do poruchy,
- časová údržba/oprava/výměna všech komponent systému,
- časová oprava/výměna komponent v poruchovém stavu,
- sledování stavu komponent + údržba/oprava/výměna konkrétní komponenty na základě zjištěného stavu,
- sledování stavu komponent + hromadná údržba/oprava/výměna všech komponent na základě zjištěného stavu,
- oprava/výměna komponent v poruchovém stavu po poruše X-té komponenty,
- oprava/výměna všech komponent po poruše X-té komponenty,
- kombinace výše uvedené časové údržby a údržby po poruše s preferencí „co nastane dříve“.

Bez znalosti informací o konkrétním systému nelze rozhodnout a vhodnosti jednotlivých variant, tento výčet má sloužit především k uvědomění si všech možností při plánování údržby výběrového systému.
Pokud je součástí úlohy i samotný návrh výběrového systému, je úkolem řízení rizika, tedy jeho ekonomické optimalizace, zvolit i typ komponent a hodnoty K a N výběrového systému, přičemž pro odhad hodnoty bezporuchovosti výsledného systému lze použít tabulku 1. Důležité je již v tuto chvíli zohledňovat možné varianty programu údržby, které budou ovlivňovat hodnotu bezporuchovosti komponent R_x v tabulce, respektive ve vztahu (1).

Z výše uvedeného textu je patrné, že hodnocených variant může být značné množství a je tedy nezbytné na základě zkušeností vybrat do porovnání pouze ty varianty, které jsou realizovatelné a potenciálně vhodné.

6 Příklad - systém chladičů

V této kapitole si představíme konkrétní systém, na kterém budou následně simulovány různé přístupy v plánu preventivní údržby. Jedná se o chladicí systém, sestávající z pěti stejných chladičů, jejichž fyzické uspořádání je paralelní.
Spolehlivostní uspořádání může vypadat různým způsobem. Pokud budeme zkoumat například netěsnosti na přírubách či samotných chladičích, bude spolehlivostní uspořádání sériové. V případě zkoumání požadované úrovně chlazení bude uspořádání vypadat jako výběrové, případně paralelní.



Obr. 5 Funkční zapojení systému

V rámci tohoto příspěvku bude zkoumána pouze možnost vnitřního zanášení. Vzhledem k tomu, že k zanášení nedochází skokově a chladič se tedy nechová dvoustavově, bude hodnota K ze schématu chápána jako součet účinků přes všechny chladiče.
Provozní a spolehlivostní parametry pro každý z chladičů jsou:

- kromě pravidelné každoroční odstávky celého provozu fungují v režimu 24/7,
- pouze během této odstávky je možné chladič vyčistit bez čerpání výrobních ztrát,
- poruchovost odpovídá normálnímu rozdělení s parametry střední hodnoty = 60 měsíců a směrodatnou odchylkou = 10 měsíců,
- na začátku simulace jsou chladiče ve 100% stavu, stejně jako po každém čištění.

Pro začátek předpokládejme, že systém je funkční, pokud je chladicí účinek alespoň ve výši chladicího účinku 3 zcela čistých chladičů (K=3). Pro tento předpoklad budeme simulovat následující varianty:

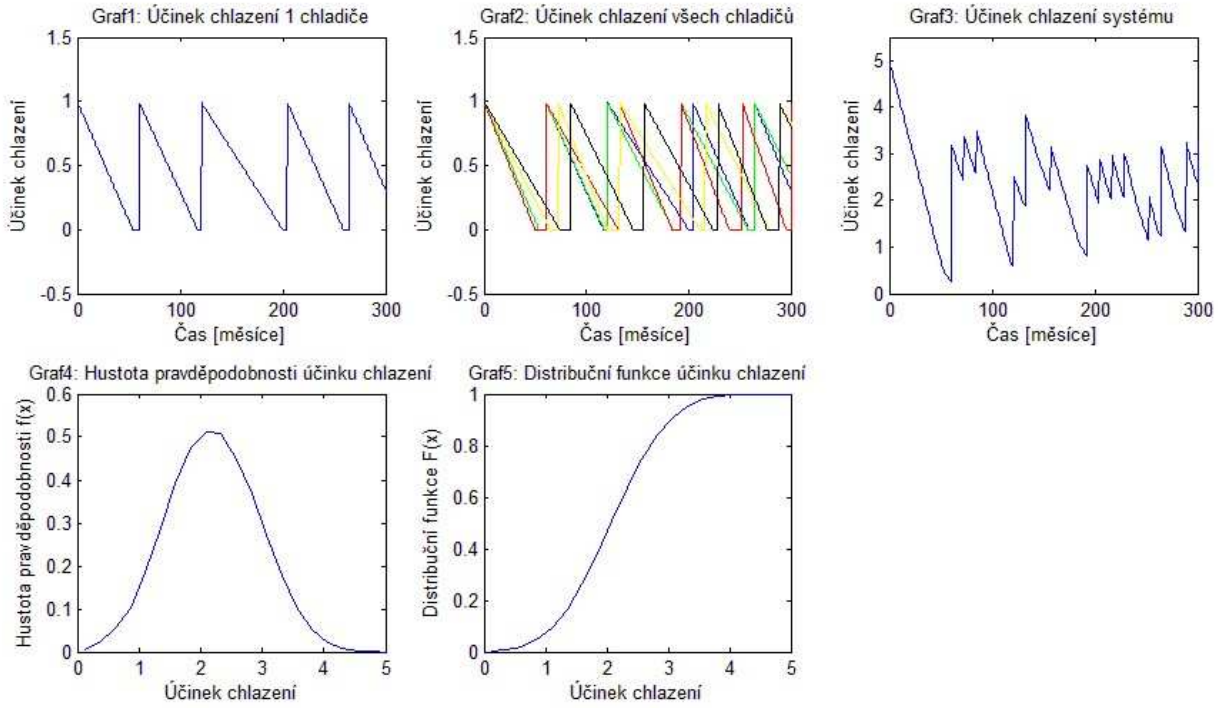
- chladiče se zanášejí postupně; pokud je chladič zcela zanesen, čištění se provede následující odstávku,
- stejně jako varianta 1 + všechny chladiče se budou čistit vždy po 60 (48, 36, 24 nebo 12) měsících.

6.1 Varianta 1: čištění zcela zanesených chladičů

Simulace byly realizovány v prostředí Matlab, z něhož jsou i všechny grafické výstupy.
Tato i všechny další simulované varianty budou obsahovat 5 grafů, které ve směru zleva doprava po řádcích znázorňují chování jedné komponenty, všech komponent a následně celého systému jako celku.

- Graf 1: Znázorňuje chování jednoho kusu chladiče. Ten je po celkovém zanesení vyčištěn v následující pravidelné odstávce.

- Graf2: Stejně jako Graf1, pouze jsou vykresleny stavy pro všech 5 chladičů.
- Graf3: Jedná se o součtovou funkci stavů jednotlivých chladičů. Na základě tohoto grafu je zřejmé, že výše uvedený požadavek na funkci (K=3) není ve většině případů splněn.
- Graf4: Jedná se o hustotu pravděpodobnosti účinku chlazení celého systému.
- Graf5: Je znázorněna distribuční funkce účinku chlazení celého systému. Z toho grafu lze odečíst, že u této varianty není ve více než 80 % případů splněn požadavek na funkci chlazení.

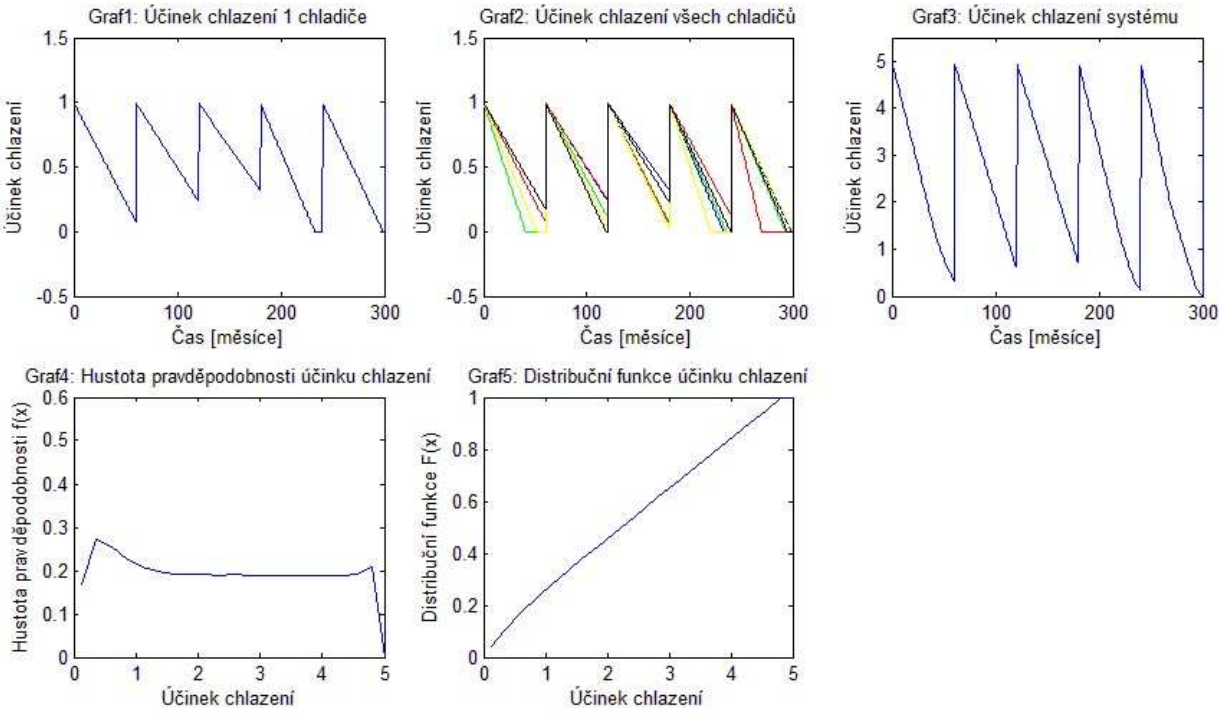


Obr. 6 Chování systému při čištění chladičů po jejich zanesení

Uvedené grafy budeme dále srovnávat se simulacemi v následující kapitole, která řeší preventivní údržbu chladičů v předem stanoveném intervalu.

6.2 Varianta 2a: čištění zcela zanesených chladičů + pravidelné čištění po 60 měsících

Zlepšení situace, simulované v předchozí variantě, je možné dosáhnout pomocí vložení pravidelného čištění. V této variantě bude simulován interval 60 měsíců, který bude v dalších variantách postupně krácen.

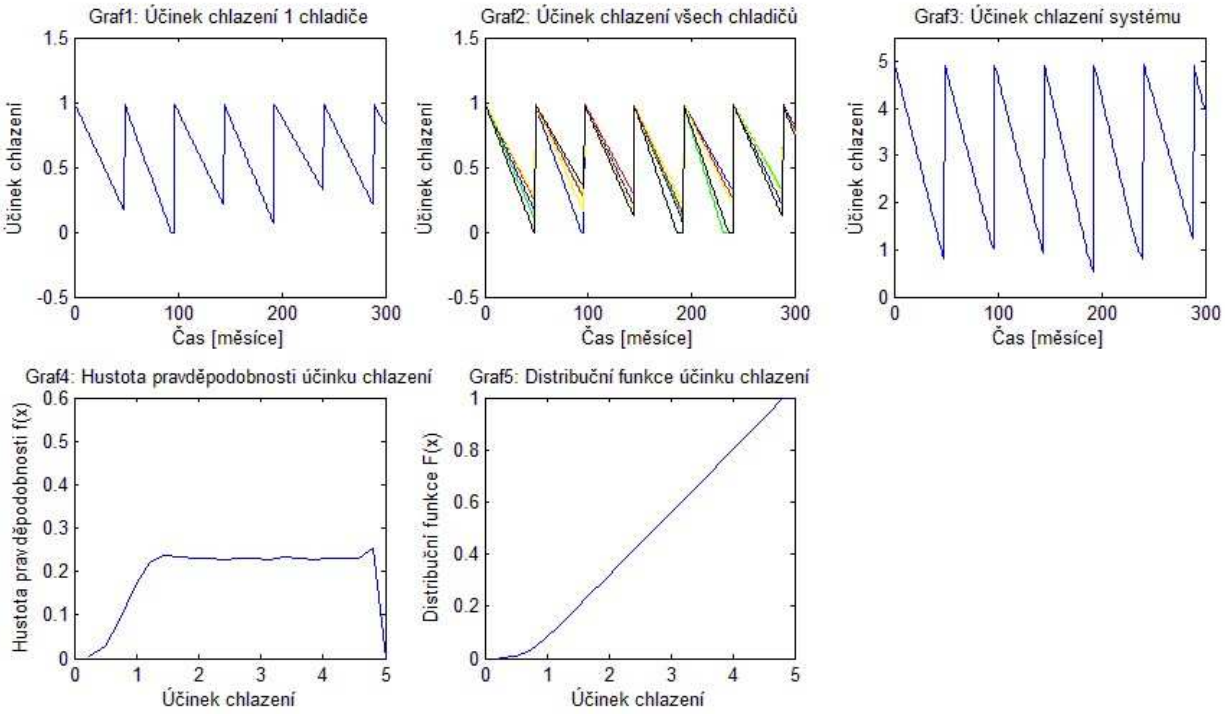


Obr. 7 Chování systému při čištění chladičů po jejich zanesení +pravidelné čištění po 60 měsících

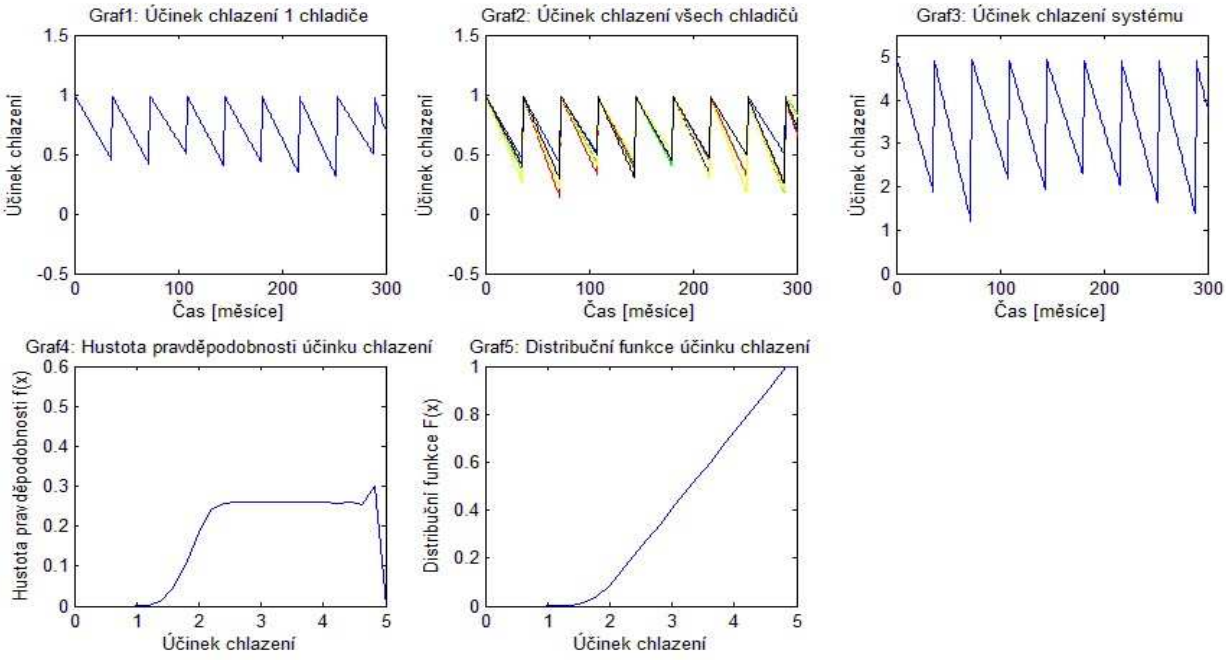
Výsledek této varianty je zcela jistě lepší oproti té předchozí, ale je stále nedostačující. Požadované funkce systém nedosahuje ve více než 60 % případů. Interval 60 měsíců byl zvolen spíše tréninkově, protože 60 měsíců je zároveň střední doba, za kterou se chladič zcela zanese, a nedá se předpokládat, že by výrazně zlepšil stav celého systému.

6.3 Varianta 2b až 2e: čištění zcela zanesených chladičů + pravidelné čištění po 48, 36, 24, 12 měsících

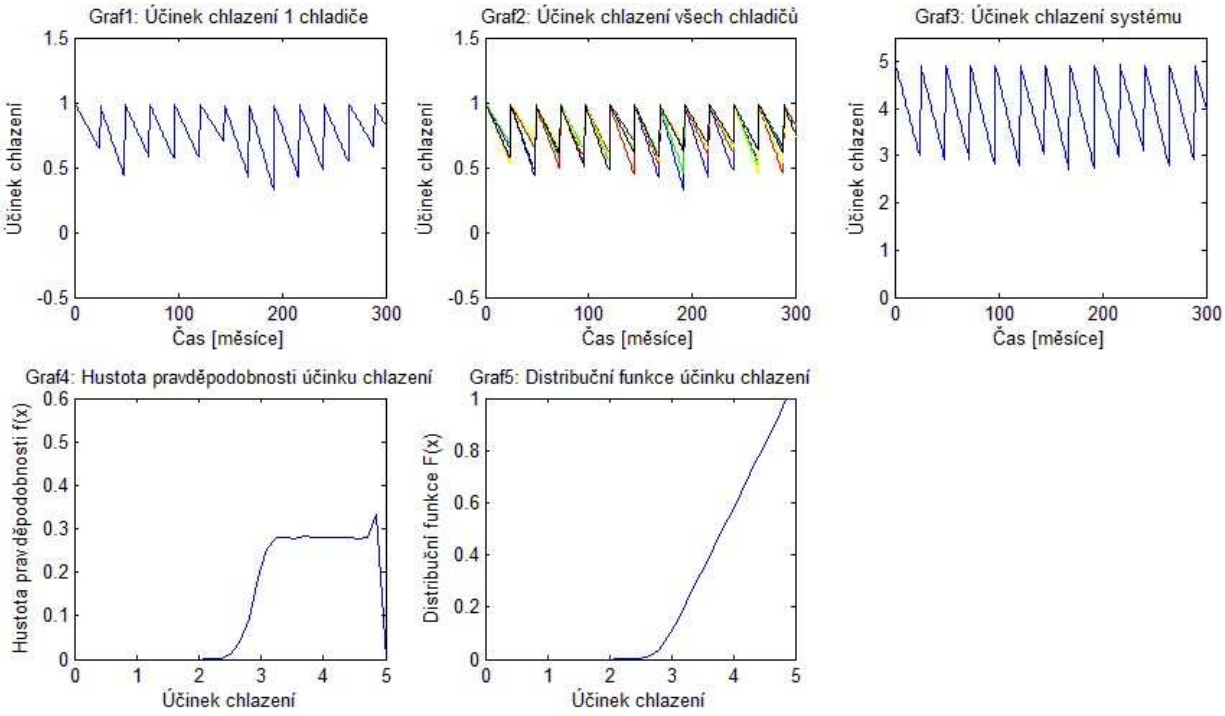
Interval 60 měsíců byl postupně zkracován, a to vždy přesně o rok (interval pravidelných odstávek). Níže jsou vloženy grafy postupně pro všechny simulované intervaly, tedy pro 48, 36, 24 a 12 měsíců.



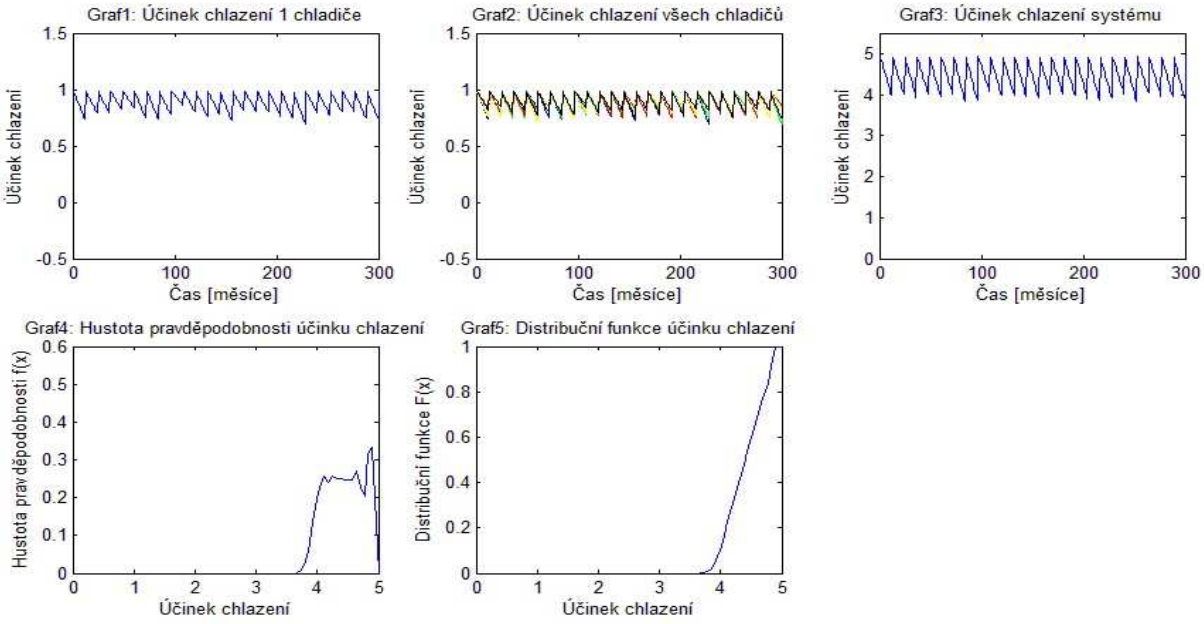
Obr. 8 Chování systému při čištění chladičů po jejich zanesení +pravidelné čištění po 48 měsících



Obr. 9 Chování systému při čištění chladičů po jejich zanesení +pravidelné čištění po 36 měsících



Obr. 10 Chování systému při čištění chladičů po jejich zanesení +pravidelné čištění po 24 měsících



Obr. 11 Chování systému při čištění chladičů po jejich zanesení +pravidelné čištění po 12 měsících

Z uvedených grafů vyplývá, že vhodnými variantami k dalšímu posouzení by byly poslední dvě možnosti - pravidelné čištění po 24 nebo 12 měsících. Při pravidelném čištění po 24 měsících je požadavek splněn z cca 85 % provozního času, při pravidelném čištění po 12 měsících je splněn téměř ze 100 %. Do rozhodování o vhodné variantě by následně musely vstoupit ekonomické parametry, jako například cena čištění, cena snížení produkce atd. Toto ovšem již nebylo předmětem zkoumání.

6.4 Další možné varianty

V příspěvku bylo simulováno pouze několik možných variant přístupu k programu údržby, které byly mezi sebou porovnány. Mezi další možnosti patří například tyto varianty:

- každý rok bude vyčištěn chladič, který je nejvíce zanesený (lze predikovat například z tlakové diference),
- v odstávce budou vyčištěny všechny chladiče, jejichž chladicí výkon je nižší než X %,
- mimo odstávku budou vyčištěny všechny chladiče, pokud chladicí výkon klesne pod požadované parametry (vhodné při nízkých ztrátách na produkci),
- chladiče používat ve formě studené zálohy; při nedostatečném chladicím výkonu teprve zprůchodnit záložní chladič, který se nemohl do této doby zanést,
- atd.

Dalším provozním aspektem, který komplikuje úlohu, jsou proměnlivé požadavky na chladicí výkon v průběhu roku. Největší výkon bude potřebný v letním období. Pokud je možné pravidelnou odstávku naplánovat do libovolného ročního období, z pohledu systému chlazení je vhodné ji směrovat před letní období. Po odstávce a pravidelné údržbě má chladicí systém nejlepší parametry a jejich následné zhoršení do zimního období nemusí být pro provoz zásadní.

7 Závěr

Výběrových systémů je využíváno v situacích, kdy je nutné zajistit vysokou míru bezporuchovosti či pohotovosti, nebo v případech, ve kterých je nutné zajistit důvěryhodnost předávaných dat výběrem nebo výpočtem (např. modus) z více vstupů. V druhém jmenovaném případě je pak součástí i vyhodnocovací jednotka, kterou je též nutné zohlednit do výpočtu, buď jako spolehlivostně sériovou komponentu, nebo formou poruch se společnou příčinou.
Cílem článku bylo vytvořit základní přehled v oblasti způsobu návrhu, provozu a údržby výběrových systému při respektování inherentních vlastností komponent, respektive parametrů jejich způsobů poruch, a zamezit tak intuitivnímu přístupu. Aby bylo zřejmé, kolik variant je nutné zohlednit při výběru způsobu provozování a údržby výběrového systému, byl zařazen příklad týkající se systému chlazení. I takto jednoduchý systém vygeneroval velké množství variant, které nebylo možné v rámci matematických schopností autora řešit deterministicky, a proto byl zvolen simulační přístup.

LITERATURA

[1] Barlow, R.E., Proschan, F. - Statistical theory of reliability and life testing: probability models. 1975. New York: Holt, Rinehart and Winston.
[2] Valis, D., Koucky, M., Vintr, Z. - Maintenance optimization of k-out-of-n systems based on costs. 2010. Proceedings of the European Safety and Reliability Conference, p. 1288-1294. ISBN 978-0-415-60427-7.
[3] Moubray, J. M. - Reliability-centred Maintenance. Second edition. Butterworth-Heineman, Oxford, 1997
[4] IEC 60300-3-11: Dependability management - Part 3-11: Application guide - Reliability centred maintenance

Poděkování:
Tato práce vznikla za podpory Technologické Agentury České republiky, projekt TA01030833 - Integrovaný informační systém pro silniční přepravu nebezpečných chemických látek

Zálohování technických systémů

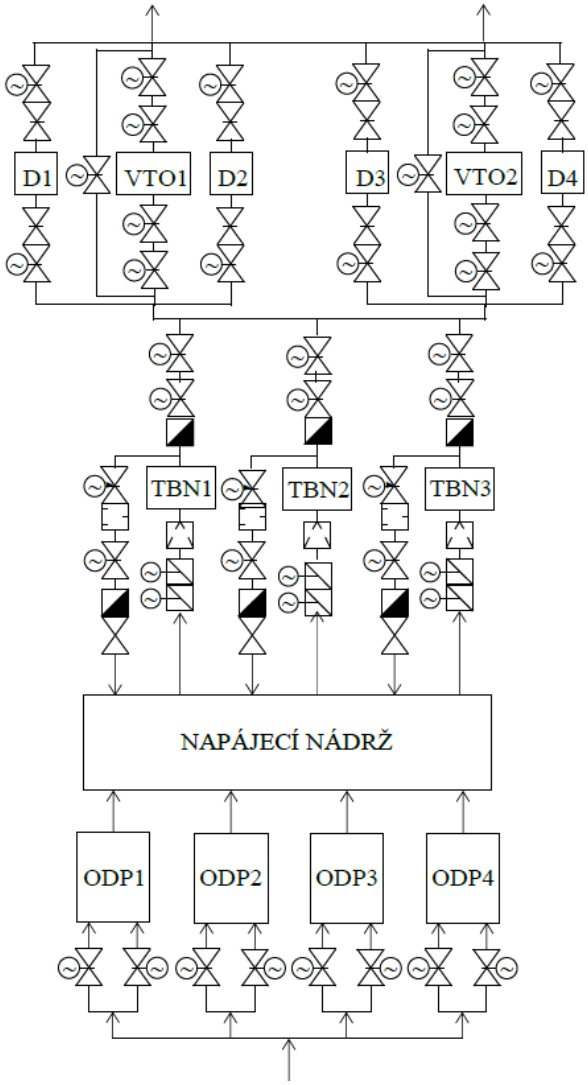
doc. Ing. Pavel Fuchs, CSc.
Technická univerzita v Liberci, Studentská 2, Liberec 461 17
pavel.fuchs@tul.cz

1 Úvod

Zálohování technických systémů představuje velmi rozmanitou množinu řešení. Již samotný pojem zálohování v sobě obsahuje očekávání, že mám k dispozici něco navíc, co nám umožní překonat kritickou situaci. Při zálohování se setkáváme s pojmem redundance (nadbytečnost) a diverzita (rozmanitost). Každé zálohování vždy představuje redundantnost, ale ne vždy diverzitu, pokud se jedná o použité prostředky zálohování.
Při návrhu redundantních systémů je třeba mít na zřeteli celou řadu aspektů. V tomto příspěvku není možné byť jen letmo věnovat pozornost těm fundamentálním. Rovněž není cílem tohoto příspěvku prezentovat základní struktury zálohovaných systémů a základní matematické vztahy pro výpočty spolehlivosti jednotlivých způsobů zálohování. Ty lze nalézt v základních učebnicích spolehlivosti. Příspěvek se soustřeďuje na 2 aspekty, se kterými je možné se v technické praxi setkat při zálohování systémů. Prvním aspektem je výkonová závislost bezporuchovosti a pohotovosti systému, druhým aspektem je problematika poruch se společnou příčinou v zálohovaných systémech. S ohledem na rozsah příspěvku není ani v jednom případě účelem popis přesného řešení a matematických postupů. Podstatou příspěvku je upozornění na nejčastější úskalí, se kterými se návrháři a analytici zálohovaných systémů mohou potkat.

2 Bezporuchovost a pohotovost systému jako funkční závislost

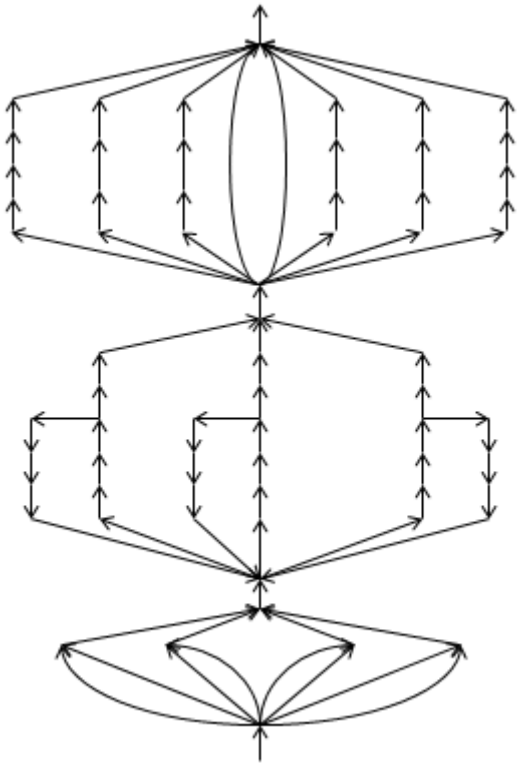
S vyjádřením bezporuchovosti a pohotovosti jako funkce, se v technické praxi lze setkat často. Zpravidla jako s vyjádřením této funkce v závislosti na čase, kilometrickém proběhu, počtu sepnutí apod. Druhou a v praxi mnohdy podceňovanou funkční závislostí je závislost spolehlivosti na hodnotě požadované funkční výkonnosti. Zpravidla se při zálohování velkých technologických celků setkáváme s případy, že zálohujeme na různých úrovních požadovaného výkonu, např. 1 x 100 %, 2 x 50 % apod. Automaticky se předpokládá, že při výpadku provozovaného zařízení naběhne horká či studená záloha s určitou pravděpodobností.
Jako příklad zálohovaného technického systému může posloužit napájecí systém. Je to poměrně složité a strukturálně komplikované zařízení, viz obr. 1. Jeho funkce spočívá v napájení sekundární strany parogenerátorů odplyněným kondenzátem. Kondenzát je nejprve odplyněn v odplyňovačích (ODP1 – ODP4) a shromažďován v napájecí nádrži.
Následně je čerpán dvěma pracovními turbonapáječkami (TBN1, TBN2) přes systém vysokotlaké regenerace (VTO1, VTO2) s dochlazovači (D1 – D4) do napájecího kolektoru parogenerátoru. Třetí turbonapáječka (TBN3) slouží jako studená záloha a uplatňuje se pouze v případě poruchy některé pracovní turbonapáječky. Každá turbonapáječka je schopna samostatně dodávat takové množství napájecí vody, které postačuje k provozu bloku na 60 % jeho nominálního výkonu (1000 MW).



Obr. 1: Technologické schéma napájecího systému

Z uvedeného příkladu vyplývá, že se jedná o úlohu, která není jednoduše řešitelná pomocí běžných metod jako je metoda stromu poruchových stavů FTA, metoda blokových diagramů bezporuchovosti RBD či metodou Markovské analýzy. Je to způsobeno tím, že pro různé konfigurace uspořádání systému v závislosti na možných poruchách dostáváme různé výkonové úrovně a k tomu by u těchto metod bylo zapotřebí sestavení příslušného počtu spolehlivostních modelů. Mnohem efektivnější je pro řešení této úlohy použít metodu orientovaných ohodnocených grafů [1].

Pro potřeby výpočtu byl analyzovaný systém převeden do podoby stochastické sítě, viz obr. 2. Hrany sítě jednoznačně korespondují s prvky systému z obr. 1 a jsou ohodnoceny doplňkem (do 100 %) snížení výkonu, který způsobí porucha daného prvku. Například hrany odpovídající každé turbonapáječce jsou v provozuschopném stavu ohodnoceny 60 (každá turbonapáječka je schopna samostatně dodávat takové množství kondenzátu, které postačuje k provozu bloku na 60 % jeho nominálního výkonu). Analogicky jsou ohodnoceny ostatní hrany. Kromě kapacit jsou každé hraně přiřazeny pravděpodobnostní parametry charakterizující rozdělení doby přechodu mezi jednotlivými stavy (např. doby do poruchy, doby obnovy apod.).



Obr. 2: Síť reprezentující napájecí systém

Takový způsob analýzy zálohovaného systému pak umožňuje modelování spolehlivosti v celém rozsahu jeho požadované funkční výkonnosti. V uvedeném případě pak vedl k těmto závěrům:

- nízký podíl řídicího systému na poruchovosti a nepohotovosti systému napájení parogenerátorů jako celku,
- nadbytečnost třetí napáječky,
- dostatečná bezporuchovost a pohotovost napájení v celém požadovaném rozsahu výkonu napájecího systému.

Podobným příkladem funkční závislosti může být brzdový systém kolejového vozidla, kdy na použití druhu brzdy, počtu brzděných podvozků a velikosti brzdných sil závisí brzdná dráha vozidla. Vždy však závisí na návrhu brzdového systému a schopnosti analytika vybrat vhodný model spolehlivosti k popisu systému.

Ale zcela rozhodující je vyčíslování bezporuchovosti a pohotovosti jako funkční závislosti u systémů síťového charakteru. Jedná se tedy o závislost spolehlivosti na přenosové kapacitě či propustnosti např. v systému rozvodu elektrické energie, v komunikačních systémech, dopravních systémech apod. V těchto případech pro korektní analýzy spolehlivosti se nelze obejít bez speciálních metod spolehlivosti k posouzení bezporuchovosti a pohotovosti v příslušném rozsahu funkční výkonnosti.

3 Poruchy se společnou příčinou

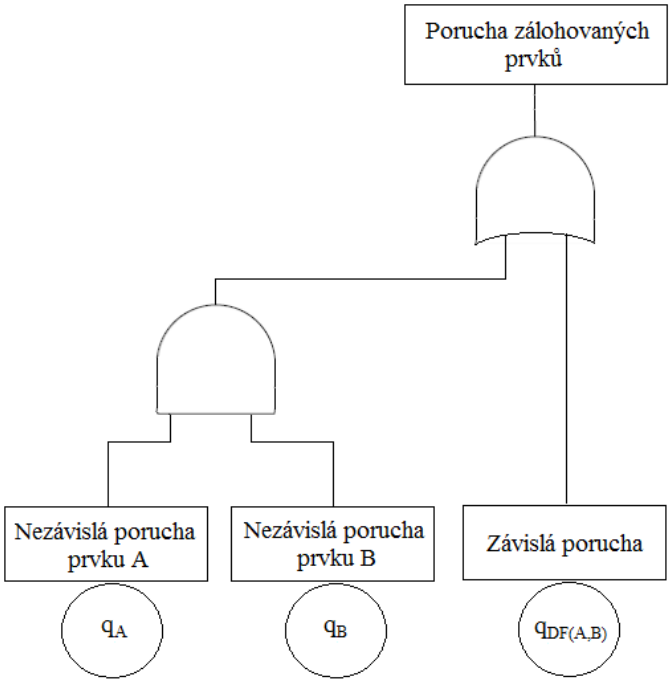
Pravděpodobnost náhodného současného výskytu poruchy na důsledně nezávislých částech redundovaného (zálohovaného) systému je dána součinem pravděpodobností výskytů poruch na částech (tzv. single failures). U vysoce spolehlivých částí se s takovým přístupem dochází k nevěrohodně vysoké spolehlivosti systému. V případech, kdy funkci systému zajišťuje více zálohujících se částí (prvků) s vysokou spolehlivostí, současná teorie modelování proto opouští předpoklad úplné nezávislosti částí a zavádí pro ně poruchu vyvolanou společnou příčinou CCF (Common Cause Failure). Podle ČSN IEC 60050-191, odstavec 191-04-23, jsou poruchy se

společnou příčinou definovány jako poruchy různých objektů způsobené jednou událostí, přičemž tyto poruchy nejsou následky jedna druhé.

Analýzou závislých poruch se rozumí analýza a modelování možností poruch se společnou příčinou, které mohou zmařit zálohování. Z hlediska způsobu podchycení v modelu lze rozlišit dva typy závislostí v systému – explicitní a implicitní.

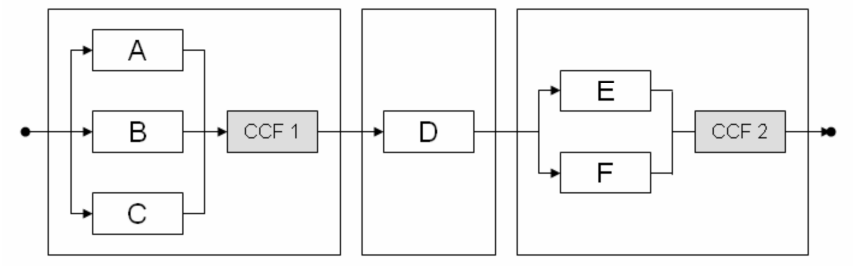
Při prvním způsobu jde o explicitní podchycení všech zjevných závislostí vyplývajících jednak z vnitřní struktury systému, jednak ze sdílených vnějších vlivů, tj. ze sdílených služeb (např. napájení elektro, chlazení), vnějších signálů, zásahů obsluhy nebo z výskytu iniciačních události či jiných vnějších podmínek.

Pokud by bylo možné takové příčiny jednoznačně identifikovat, bylo by možné je do výpočtu přímo zahrnout prostřednictvím explicitně vyčíslené pravděpodobnosti závislé poruchy DF (Dependent Failure). Tento explicitní přístup je uveden na obr. 3.



Obr. 3: Přímé zahrnutí závislých poruch do modelu a výpočtu

Při druhém způsobu jde o souhrnné podchycení tzv. reziduálních poruch se společnou příčinou, tj. shrnutí všech ostatních myslitelných příčin (chyby vývoje, materiálu, výroby, montáže, nedostatečná údržba, provozní šoky) násobného selhání prvků do jedné či několika reprezentativních událostí. Obvykle se CCF uvažuje jen u skupiny stejných (podobných) prvků, se stejným způsobem provozu, stejnou funkcí a stejným místem v systému (prvky realizují záložní zajištění téže funkce). Reprezentativní událost typu CCF se do modelu přidává v logickém součtu s náhodnými individuálními poruchami komponent, viz obr. 4 [3].



Obr. 4: Zahrnutí závislých poruch do modelu a výpočtu jako CCF prvek [3]

Událost typu násobná porucha se společnou příčinou z reziduálních příčin může mít podobu CCF všech prvků ve skupině identických prvků nebo CCF určité dvojice prvků, CCF určité trojice prvků apod.

Zdroj příčiny závislé poruchy není zpravidla identifikován (jinak by příčina byla explicitně zahrnuta v modelu), nýbrž se postuluje jako hypotetická příčina. Proto bývá tento přístup označován jako implicitní. Zahrnuje příčiny, které leží jak v okolí prvků systému, tak uvnitř nich, jako společné vlastnosti zálohujících se prvků. Takový přístup se ukázal jako opodstatněný i v praxi a standardy pro posuzování bezpečnostních systémů jej předpokládají a vyžadují.
Implicitní přístup může úplně pokrýt závislé poruchy, ale vznikají př tom velké nejistoty z důvodu nedostatku dat týkajících se poruchových mechanismů prvků, kdy je obtížné odlišit oddělit způsob a příčinu poruchy. Důsledná aplikace implicitního přístupu přináší nebezpečí nedostatečné analýzy systému (například stromem poruchových stavů) projevující se např. opominutím strukturálních/ funkčních závislostí.
Pro zahrnutí poruch se společnou příčinou CCF do výpočtu spolehlivostních parametrů redundovaných technických systémů existuje několik výpočetních modelů. Jsou založeny právě na implicitním přístupu k určování pravděpodobnosti závislých poruch (poruch se společnou příčinou). Základním je Marshall – Olkin model, široce se využívá model β – faktoru a MGL (Multiple Greek Letter) model. V následujícím textu budou prezentovány první dva modely

3.1 Marshall – Olkin model

Marshall – Olkin model [2] reprezentuje základní model pro výpočet pravděpodobnosti poruch systémů, jejichž prvky nejsou nezávislé.

<u>1. Model výpočtu bez závislých poruch</u>

Příklad: Systém tvořený 3 identickými prvky A, B, C tvoří systém se zálohováním *2* ze *3*

Systém je v poruše, kdy selžou dva prvky:

AB, AC, BC

Pravděpodobnost poruchy (resp. nepohotovost) systému:

$$Q_S = q_A \cdot q_B + q_A \cdot q_C + q_B \cdot q_C - 2q_A \cdot q_B \cdot q_C$$

Vztahy lze zjednodušit a zapsat následující formou:

Zjednodušení: $Pr(A \cup B) \approx Pr(A) + Pr(B)$

Pravděpodobnost poruchy je u všech prvků stejná: $q_A = q_B = q_C = Q_{k=1}$,

kde k (k = 1, 2, ..., n) znamená počet prvků postižených poruchou

Pravděpodobnost poruchy systému v konfiguraci 2 ze 3 bez uvažování závislých poruch (poruch se společnou příčinou) je daná výrazem:

$$Q_s = q_A \cdot q_B + q_A \cdot q_C + q_B \cdot q_C = 3 \cdot Q_1^2$$

<u>2. Model výpočtu se závislými poruchami</u>

Pravděpodobnosti kombinací poruch prvků

q_{AB}, q_{BC}, q_{AC}

q_{ABC}

Budeme-li předpokládat, že se jedná o identické prvky, můžeme použít zápis pravděpodobnosti poruchy se společnou příčinou (závislá porucha)

$q_{AB} = q_{BC} = q_{AC} = \ldots = Q_{k=2}$

$q_{ABC} = Q_{k=3}$

Příklad výpočtu pro systém v konfiguraci 2 ze 3

pravděpodobnost poruchy se společnou příčinou postihující 2 prvky:

$$q_{AB} + q_{BC} + q_{AC} = 3 \cdot Q_2$$

pravděpodobnost poruchy se společnou příčinou postihující 3 prvky:

$$q_{ABC} = Q_3$$

<u>3. Výpočet pravděpodobnosti systému se závislými poruchami</u>

$$Qs = \Sigma Pr \text{ (nezávislých poruch)} + \Sigma Pr \text{ (závislých poruch)}$$

Pro systém v konfiguraci 2 ze 3 pak platí vztah pro výpočet pravděpodobnosti poruchy (resp. nepohotovosti)

$$Qs = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$$

4. Pravděpodobnost poruchy prvku ve skupině redundantních prvků

Označíme Q_t jako celkovou pravděpodobnost poruchy prvku ve skupině redundantních prvků se zahrnutím všech vzájemných závislostí. Vztah mezi Q_t a Q_k je popsán následující rovnicí

$$Q_t = \sum_{k=1}^{n} \binom{n-1}{k-1} . Q_k$$

kde binomický člen lze vyjádřit vztahem

$$\binom{n-1}{k-1} = \frac{(n-1)!}{(n-k)! \, . \, (k-1)!}$$

Tento vztah určuje počet kombinací poruch prvku s (k-1) různými prvky ve skupině tvořené (n-1) identickými prvky.

Pro systém tvořený skupinou 3 redundantních prvků lze pak stanovit celkovou pravděpodobnost selhání prvku ve skupině (systému) výrazem

$$Q_t = \binom{3-1}{1-1} . Q_1 + \binom{3-1}{2-1} . Q_2 + \binom{3-1}{2-1} . Q_3 = Q_1 + 2 . Q_2 + Q_3$$

Tento zápis znamená, že celková pravděpodobnost poruchy prvku ve skupině 3 redundantních prvků je dána součtem jeho vlastní (nezávislé) pravděpodobnosti poruchy a pravděpodobnosti vzájemně závislé poruchy s jedním či druhým prvkem ve skupině a pravděpodobnosti vzájemně závislé poruchy všech 3 prvků ve skupině.

5. Výpočet pravděpodobnosti poruchy se společnou příčinou

Výpočet vychází ze znalosti výskytu počtu poruch a stanoví se podle rovnice

$$Q_k = \frac{n_k}{\binom{n}{k}}$$

kde n_k je počet poruch ve skupině k prvků u systému k z n prvků.

3.2 Model β – faktoru

Model β – faktoru předpokládá současnou poruchu všech prvků dané zálohující se skupiny a používá jednoduchý parametr, který přidává do celkové pravděpodobnosti poruchy zálohujících se částí příspěvek úměrný hodnotě β z pravděpodobnosti poruchy komponenty v zálohující se skupině. Jedná se tedy model, který zavádí pro závislé poruchy tyto zjednodušující předpoklady:

- Poruchy ve skupině redundantních prvků jsou buď nezávislé, nebo všechny z n prvků selhávají.
- Při $k = 1$, $Q_k = 1$ je pravděpodobnost poruchy od nezávislých poruch.
- Při $k = n$, $Q_k = n$ je pravděpodobnost poruchy od (zcela) závislých poruch.
- Všechny ostatní kombinace poruch jsou vyloučeny z definice, takže $Q_k = 0$ pro $n > k > 1$ (pro ostatní kombinace poruch).

Obecně pro systém m z n platí

$$Q_t = Q_1 + Q_n$$

a β – faktor je definován vztahem

$$\beta = \frac{počet\ závislých\ poruch}{počet\ všech\ poruch}$$

$$\beta = \frac{Q_n}{Q_1 + Q_n} = \frac{Q_n}{Q_t}$$

Z uvedeného vyplývá, že

$$\beta \, . \, Q_t = Q_{k=n}$$

$$\beta \, . \, (Q_1 + Q_n) = Q_{k=n}$$

což spolu se vztahem

$$Q_n = Q_t - Q_1$$

dává

$$Q_{k-1} = Q_t . (1 - \beta)$$

Výsledný vztah při aplikaci β – faktoru je následující

$Q_k = (1 - \beta) . Q_t$ pro $k = 1$

$Q_k = 0$ pro $m > k > 1$

$Q_k = \beta . Q_t$ pro $k = n$

Budeme-li uvedený model β – faktoru aplikovat na zálohovaný systém *2* z *3*, získáme pravděpodobnost poruchy systému ze vztahu

$$Q_s = 3 . (1 - \beta)^2 . Q_t^2 + \beta . Q_t$$

4 Závěr

Nebylo možné s ohledem na omezený rozsah příspěvku vyčerpat všechny zajímavé skutečnosti, které se vyskytují v zálohovaných systémech a které musí analytik brát na vědomí. Dalším takovým zajímavým případem je vliv diagnostikovatelnosti na bezporuchovost a pohotovost zálohovaných systémů. Otázka detekovatelnosti poruch při diagnostice, vliv diagnostikovatelnosti na dobu latence nebezpečných poruch v zálohovaných systémech a jiné zajímavé případy snad přijde na řadu v některém budoucím semináři OSS.

Literatura

[1] KOUCKÝ, M.: RelNet - softwarový nástroj pro analýzu performability sítí. In *Sborník z 11. semináře Odborné skupiny pro spolehlivost České společnosti pro jakost „Softwarová podpora v oblasti spolehlivosti“*. Česká společnost pro jakost, Praha, 2003. Dostupné na WWW: http://www.csq.cz/uskutecnene-seminare/

[2] VESELY, W.E. Estimating common cause failure probabilities in reliability and risk analyses: Marshal-Olkim specializations. pp. 314 – 341. Nuclear Systems Reliability Engineering and Risk Assessment: Papers. SIAM, Philadelphia, 1977, ISBN 0898710413.Dostupné na WWW: http://www.google.cz/books?hl=cs&lr=&id=vLgW3iiJ_JMC&oi=fnd&pg=PA314&dq=Marshall-Olkin+Model&ots=ia2dZVA0JN&sig=weV1vI1yL4ujDAOTn94Wcy4GnGI&redir_esc=y#v=onepage&q=Marshall-Olkin%20Model&f=false

[3] IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Česká společnost pro jakost

ISBN 978-80-02-02586-3

Bezporuchovost a pohotovost

Sborník přednášek
kolektiv autorů
1. vydání
rok vydání 2015
vazba brožovaná, počet stran 29