University of West Bohemia in Pilsen
Department of Computer Science and Engineering
Univerzitni 8
30614 Pilsen
Czech Republic

Modely pro sledování spolehlivosti a životnosti komplexních řídicích systémů

Technical Report

Petr Dvořák, Marek Paška

Technical Report No. DCSE/TR-2007-17
December, 2007

Distribution: public

Technical Report No. DCSE/TR-2007-17
December 2007

Modely pro sledování spolehlivosti a životnosti komplexních řídicích systémů

Petr Dvořák, Marek Paška

Abstract

Tento report popisuje metodu, která slouží k řízení stárnutí a zastarávání dlouho žijících počítačových systémů (systémů kontroly a řízení, SKŘ). Tato metoda spočívá v konstrukci modelu sledovaného systému, tento model je založen na tzv. stromech poruch. Stromy poruch jsou pro potřeby metody rozšířeny tak, aby pracovaly s životnostmi komponent systému. Účelem modelu je zjistit, které části systému by měly být uvažovány pro modernizaci nebo nahrazení.

Copies of this report are available on
http://www.kiv.zcu.cz/publications/
or by surface mail on request sent to the following address:

University of West Bohemia in Pilsen
Department of Computer Science and Engineering
Univerzitni 8
30614 Pilsen
Czech Republic

Copyright ©2007 University of West Bohemia in Pilsen, Czech Republic

Obsah

1 Úvod **3**

2 Modely spolehlivosti **4**

2.1 Charakteristika popisovaných modelů 4

2.2 Spolehlivost komponent 4

2.3 Spolehlivostní parametry 5

2.3.1 Intenzita poruch 5

2.3.2 Pravděpodobnost poruchy 6

2.3.3 Pravděpodobnost bezporuchového provozu 6

2.4 Spolehlivost subsystémů 7

2.4.1 Stromy poruch 8

2.5 Shrnutí 10

3 Modely životnosti **11**

3.1 Vymezení pojmů 12

3.2 Životnost komponent 12

3.2.1 Používané veličiny 12

3.3 Životnost subsystémů 13

4 Model životnosti typu komponenty **15**

4.1 Životnost typu komponenty a čas záměny 15

4.2 Etapy života typu komponenty 16

4.2.1 Etapa I 16

4.2.2 Etapa II 16

4.2.3 Etapa III 17

4.2.4 Přehled mezních časů a etap života 17

4.3 Odhad životnosti typu komponenty 17

4.3.1 Riziko nedostupnosti náhrady 18

4.3.2 Potřebný počet náhradních komponent 19

4.3.3 Doba záměny 19

4.4 Výpočty v jednotlivých etapách 19
4.4.1 Etapa I 19
4.4.2 Etapa II 19
4.4.3 Etapa III 20

5 Závěr **20**

1 Úvod

Řada průmyslových systémů je navržena pro velmi dlouhý provoz. Například elektrárny obvykle pracují po desítky let. Tyto průmyslové systémy jsou velmi složité a jsou proto řízeny sofistikovanými systémy kontroly a řízení (SKŘ).

SKŘ jsou dnes založeny na počítačích. Toto digitální vybavení stárne rychleji než řízený průmyslový systém, protože elektronické technologie se prudce vyvíjejí [1].

Fyzické stárnutí digitálních komponent není hlavní problém, například mikroprocesory jsou schopné pracovat spolehlivě po mnoho let. Důležitější je morální stárnutí, tzn. *zastarávání*.

SKŘ je potřeba udržovat, aby dlouhodobě dostálo své funkci. Proces údržby obvykle vyžaduje podporu od původního výrobce, především dodávky náhradních dílů.

Elektronické technologie jsou zaměřeny na levné a masově produkované výrobky, jejichž životnost je velmi krátká (méně než dva až tři roky pro počítače a mobilní telefony). Tento extrémně krátký životní cyklus odráží rychlé změny v elektronických technologiích. Výrobci musí neustále obměňovat své výrobní linky, aby produkovaly nové a nové modely. Proto pro ně není udržitelné podporovat produkty příliš dlouhou dobu; po nějaké době už nejsou náhradní díly dostupné.

Ekonomické chování výrobců komponent je v rozporu s potřebami dlouho běžících systémů jakou jsou SKŘ. Proto musí být stárnutí a zastarávání SKŘ řízeno. Jedna z cest, jak se s tím vypořádat, je zavést řízení životního cyklu (Life Cycle Management, LCM) pro všechny podstatné části SKŘ. Cílem LCM je poskytnout podporu pro rozhodnutí, která část (komponenta, subsystém nebo celý systém) má být uvažována pro modernizaci nebo nahrazení, protože její provoz bude v blízké budoucnosti čelit problémům spojeným se stárnutím nebo zastaráváním.

Prvním krokem k zavedení LCM je získání (a následná údržba) dat o různých částech SKŘ, jejich stáří, provozních údajích a míry podpory od výrobce. Vytvoření takovéto databáze je zásadní, ale samo o sobě nedostatečné. Je potřeba vytvořit model sledovaného SKŘ, který podchycuje roli každé jednotlivé komponenty v systému. Pokud je tento model správně vytvořen, je možné sledovat možné následky selhání nějaké komponenty.

V tomto článku diskutujeme tzv. stromy poruch (s rozšířeními) jako jednu z vhodných metod pro vytvoření takového modelu.

2 Modely spolehlivosti

2.1 Charakteristika popisovaných modelů

Cílem této kapitoly je vytvořit a popsat modely vhodné pro vyhodnocení spolehlivosti komponent a subsystémů v komplexních řídicích systémech. Každý model potřebuje data. S čím větším množstvím dat pracuje, tím bývá mnohdy přesnější. Autoři si jsou vědomi, že sběr velkého množství spolehlivostních dat pro každou komponentu je obtížný úkol. Tato data nelze získat naráz, spíše půjde o jejich postupné doplňování a zpřesňování. V první fázi použití dále popisovaných modelů lze použít odhady hodnot spolehlivostních parametrů (zejména intenzit poruch) od výrobce komponenty.

Níže představovaný model je poměrně obecný a postačí k popisu spolehlivosti komponent i subsystému za doby jejich technického života. Aspekt morálního života (tzv. zastarávání – angl. obsolescence) tento model neobsahuje. Touto problematikou se zabývá upravený model pro životnost v následující kapitole.

Hlavním cílem dále popisovaného modelu je určit ze známých (zdrojových) spolehlivostních parametrů komponent SKŘ spolehlivost konkrétního subsystému či systému SKŘ. Jako zdrojové parametry slouží intenzity poruch instalovaných komponent SKŘ, hlavním určovaným spolehlivostním parametrem (výsledkem výpočtu) je pravděpodobnost poruchy příslušného subsystému či systému v nějakém zvoleném časovém intervalu, typicky v době mezi periodickými technologickými odstávkami zařízení.

2.2 Spolehlivost komponent

Spolehlivost komponenty je volně definovaná vlastnost (viz norma ČSN 01 0102 [3]), která udává, zda-li je komponenta schopna provozu, který je od ní očekáván, tj. jestli funguje správně v souladu se svou technickou specifikací.

Aby bylo možné vyhodnocovat spolehlivost subsystémů je nutné mít k dispozici spolehlivostní parametry jednotlivých komponent. Pokud tyto parametry výrobce neudává, je potřeba je stanovit nějakým expertním odhadem, popřípadě z provozních statistik poruch. Níže popsaný model znázorňuje též funkční vazby mezi komponentami z hlediska spolehlivosti a ukazuje, jak lze daných spolehlivostních charakteristik komponent využít pro výpočet stejných charakteristik jednotlivých subsystémů.

Ve vytvořeném modelu je pak možné najít komponenty, které nejvíce snižují spolehlivost subsystému (snižují ji pod určitou stanovenou mez).

2.3 Spolehlivostní parametry

Pro exaktní popis modelu je potřeba definovat některé používané veličiny, tzv. spolehlivostní parametry.

2.3.1 Intenzita poruch

Základním (resp. zdrojovým) spolehlivostním parametrem je *intenzita poruch* ($\lambda(t)$). Udává podmíněnou hustotu pravděpodobnosti vzniku poruchy v daném čase t. Podmíněnost znamená předpoklad, že do času t se uvažovaná komponenta (určitě) neporouchala. Časovým počátkem ($t = 0$) je okamžik uvedení komponenty do provozu. Pokud budeme u komponent předpokládat konstantní intenzitu poruch (tj. stejnou pravděpodobnost poruchy komponenty $\lambda.dt$ v každém krátkém časovém elementu dt v průběhu celé její doby života), jiné (zdrojové) parametry nejsou potřeba. V této kapitole budeme konstantní intenzitu poruch předpokládat, tj. uvažujeme $\lambda(\mathrm{t}) = \lambda$. U elektronických komponent bývá intenzita poruch po dobu projektované životnosti komponenty skutečně téměř konstantní, tudíž tento předpoklad nezanáší do modelu příliš velkou chybu. Mnohem větší chyba vzniká nepřesností při odhadování (konstantní) hodnoty této veličiny. Jednou z možností odhadu hodnoty intenzity poruch elektronické součástky (IC, deska s tištěným spojem osazená IC) je výpočet podle americké vojenské normy [2]. Zde popisovaný spolehlivostní model je ale navržen dostatečně obecně – tj. lze jej (po mírných úpravách některých vzorců) použít i pro komponenty s intenzitou poruch ovlivněnou fyzikální podstatou komponenty a způsobem její instalace.

Poznámka Pokud uvažujeme všechny instalované elektronické komponenty určitého typu, například desku sdílené paměti stavebnice Eagle - MSE-02, lze intenzitu poruch (za určitých okolností: zejména uvažujeme, že porouchaná komponenta je neprodleně vyměněna za náhradní) interpretovat jako střední frekvenci poruch komponenty příslušného typu. Pro odhad intenzity poruch z provozních dat pak stačí po určitou dobu T pro n instalovaných komponent sledovat celkový počet poruch k. Dále lze jednoduše určit střední dobu mezi poruchami pro jednu komponentu. Tato doba se označuje $MTBF$ – Mean Time Between Failures, v české literatuře pak jako T_s - střední doba bezporuchového provozu. Vztah pro určení $MTBF$ vypadá následovně:

$$MTBF = \frac{N \cdot n}{k}$$

Střední frekvence poruch je pak převrácená hodnota střední časové periody mezi poruchami, čili vztah pro odhad (konstantní hodnoty) intenzity poruch z provozních údajů je tento:

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

2.3.2 Pravděpodobnost poruchy

Pravděpodobnost poruchy ($Q(t)$) je funkce, která udává s jakou pravděpodobností bude v čase t komponenta porouchaná. Zadaný čas t je relativní k času uvedení komponenty do provozu ($t = 0$). Je to vždy funkce rostoucí, tj. během delší doby je vyšší pravděpodobnost vzniku poruchy.

Pravděpodobnost poruchy $Q(t)$ odpovídá distribuční funkci náhodného času poruchy, která je definována takto:

$$Q(t) = F(t) = \lim \int_0^t f(\tau) d\tau$$

kde $f(\tau)$ je hustota pravděpodobnosti náhodného času poruchy τ.

Průběh funkce lze rovněž odvodit ze známého průběhu intenzity poruch $\lambda(t)$. Pokud je intenzita poruch konstantní, tj. $\lambda(t) = \lambda$, získáme pravděpodobnost poruchy (tj. *pravděpodobnost, že se sledovaná komponenta porouchá od okamžiku uvedení do provozu $t = 0$ do obecné hodnoty t relativního času*) ve tvaru:

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

Pro další úvahy a vyhodnocování modelu budeme potřebovat právě pravděpodobnost poruchy.

2.3.3 Pravděpodobnost bezporuchového provozu

Pravděpodobnost bezporuchového provozu ($R(t)$) (z angl. reliability) je spolehlivostní parametr, který je nejblíže k obecnému pojmu *spolehlivost*. Je to *pravděpodobnost, že se sledovaná komponenta neporouchá od okamžiku uvedení do provozu $t = 0$ do obecné hodnoty t relativního času*, tj. je to doplňková hodnota (doplněk do 1) k pravděpodobnosti poruchy $Q(t)$:

$$R(t) = 1 - Q(t)$$

Poznámka Výše uvedené spolehlivostní parametry (charakteristiky) $Q(t)$ a $R(t)$ lze též vztáhnout ke konkrétnímu časovému intervalu, čímž odstraníme časovou závislost. Například lze jako $t = 0$ stanovit čas ukončení i-té odstávky. Při odstávce se důkladně testují komponenty, čili lze předpokládat, že jsou

plně funkční. Relativní čas do příští (i+1) odstávky je například $t = 1rok = 8760hodin$. Potom lze užívat symboly Q, R nikoliv jako časové funkce, ale jako hodnoty vztažené k době periody mezi odstávkami. Například $Q = 0,001$ pro určitou komponentu by znamenalo, že se tato komponenta mezi odstávkami porouchá s p-tí 0,001, tj. 1 promile.

2.4 Spolehlivost subsystémů

Pro vyhodnocení spolehlivosti vyšších celků – tj. subsystémů, systémů, atd. – potřebujeme znát spolehlivostní parametry komponent a zároveň funkční vazby mezi komponentami. Spolehlivostní vazby jsou v obecném případě jiné než vazby funkční (funkční vazba např. znamená, že vstupem nějaké komponenty je signál generovaný na výstupu jiné komponenty). Spolehlivostní vazby jsou dvou základních druhů označovaných jako paralelní a sériové spojení komponent.

Paralelně spojeny jsou (většinou stejné) komponenty, které jsou v systému nějak redundantní, tj. pro spolehlivý běh systému stačí jedna funkční komponenta a ty ostatní tvoří její zálohu, viz např. redundanci DHG ústředen nebo komunikačních sítí.

Naopak sériové spojení komponent značí nezastupitelnou úlohu takto spojených komponent. Většinou se jedná o různé komponenty (např. procesor a paměť). Sériové spojení znamená, že všechny takto spojené komponenty musí fungovat, aby fungovala celá skupina. Neboli porucha jediné z nich způsobí poruchu celé této skupiny.

Nebudeme zde z důvodu úspory místa uvádět příslušné matematické vztahy, lze je nalézt v literatuře, např. [6], [7]. Pro hrubou představu lze uvést, že pro sériové spojení se násobí dílčí hodnoty veličiny R na výslednou hodnotu celého spojení, pro paralelní spojení se naopak násobí hodnoty Q.

Sériové a paralelní spojení lze aplikovat nejen na jednotlivé komponenty, ale i na podobným spojením vzniklé skupiny komponent. Skupiny vyšší úrovně lze opět sériově a paralelně spojovat, až dospějeme ke skupině zahrnující všechny komponenty zkoumaného subsystému (resp. systému). Získáme tak hierarchický popis spolehlivostního chování komponent a jejich skupin prostřednictvím sério-paralelního spojení. Skupina komponent (dána nějakým druhem spolehlivostního spojení) ve vyšší úrovni v hierarchii hraje stejnou úlohu jako jednotlivá komponenta v nejnižší úrovni. Proto budeme dále takovéto skupiny komponent označovat pojmem složená komponenta.

2.4.1 Stromy poruch

Hierarchie spolehlivostních spojení komponent se často znázorňuje pomocí tzv. stromů poruch (angl. fault trees). Princip tohoto modelu je přímočarý a intuitivní. Jeho funkce je snadno pochopitelná pro techniky i manažery, o čemž svědčí i technická zpráva NUREG [4], popisující tuto modelovací techniku s doporučením jejího širšího použití v jaderné energetice. Přestože se jedná o jednoduchý model, je dostatečně obecný pro náš problém.

Cílem modelu stromů poruch je znázornit vazby mezi poruchami. V reálném systému může porucha nějaké konkrétní komponenty (základní porucha) způsobit selhání příslušného podsystému, a toto může následně způsobit selhání celého systému. Každá základní porucha tudíž může za určitých podmínek (daných vazbami mezi poruchami) způsobit selhání celého systému.

Standardní stromy poruch Standardní strom poruch je složen z uzlů, z nichž každý představuje nějakou konkrétní poruchu. Listy představují *základní poruchy*, tj. poruchy samotných (fyzických) komponent.

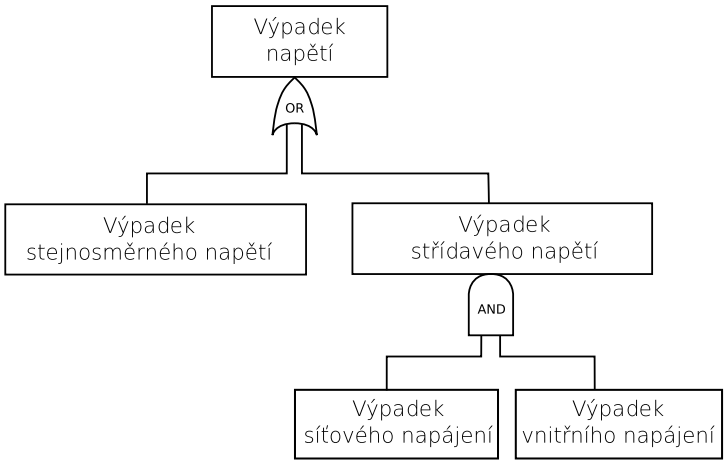
Nelistový uzel je každý uzel, který má přímou vazbu (tj. je čárou napojen) na nějaký uzel v nižší úrovni stromu. Nelistový uzel ve stromu poruch představuje tzv. *složenou poruchu*. Složená porucha může vzniknout jedině v případě, že vznikne porucha v nějakém připojeném uzlu v nižší úrovni stromu (tzv. *uzly potomci*). O tom, jestli složená porucha vznikne nebo ne, rozhoduje typ (viz níže) této poruchy na základě poruch uzlů potomků.

Kořen stromu je speciální případ složené poruchy. Představuje poruchu nejvyšší úrovně – tj. selhání (angl. failure) systému. Každá základní porucha se může rozšířit z listu až do kořenu, neboli každá *základní porucha* může způsobit selhání systému (je-li systém konstruován bez redundance).

Existují dva základní typy nelistových uzlů. Tyto typy je zvykem označovat prostřednictvím boolovských operátorů AND a OR.

AND uzel představuje paralelní spojení komponent, které jsou z hlediska zajištění funkce složené komponenty ekvivalentní (též je lze označit jakoredundantní). Pokud v tomto typu spojení jedna komponenta přejde do poruchového stavu, její funkce je stále poskytována jinou komponentou. Tudíž AND uzel se dostane do poruchového stavu, pouze pokud se v poruchovém stavu nalézají všechny s ním přímo spojené uzly v nižší úrovni stromu (potomci). OR uzel představuje sériové spojení komponent. V tomto typu spojení je funkce jednotlivých komponent nenahraditelná. Proto je OR uzel v poruchovém stavu, pokud je v poruchovém stavu jakýkoliv s ním přímo spojený uzel v nižší úrovni.

Obrázek 1 na zvoleném příkladu graficky přibližuje představu stromu poruch.



Obrázek 1: Příklad standardního (binárního) stromu poruch.

Na obrázku 1 je možné vidět, že porucha *Výpadek napětí* je způsobena poruchou *Výpadek síťového napájení* a poruchou *Výpadek vnitřního napájení* (paralelní spojení). Porucha *Výpadek napětí* je způsobena poruchou *Výpadek stejnosměrného napětí* nebo poruchou *Výpadek střídavého napětí* (sériové spojení).

Jak již bylo zmíněno výše, strom poruch má kořen představující selhání (sub)systému. Toto pojetí je možné snadno rozšířit. Je možné vytvořit několik různých stromů, které budou sdílet určité podmnožiny uzlů. Získáme tak víc kořenů, které představují různé možnosti selhání nebo jiné události.

Pravděpodobnostní rozšíření stromů poruch Model popsaný výše je v principu binární povahy – každý uzel buď je nebo není v porouchaném stavu. Lze snadno nahlédnout, která množina základních poruch může vést k celkovému selhání, ale není zřejmé jaké jsou pravděpodobnosti jednotlivých poruch.

S použitím pravděpodobnostních a spolehlivostních parametrů může být model rozšířen na spolehlivostní.

Pro operace skládání pravděpodobnostních parametrů komponent potřebujeme pracovat s pravděpodobností poruchy ($Q(t)$). Můžeme pak napsat příslušné formule pro skládání dílčích ukazatelů spolehlivostí do výsledné hodnoty:

sériové spojení (OR):

$$Q(t) = \prod_i Q_i(t)$$

paralelní spojení (AND):

$$Q(t) = 1 - \prod_i (1 - Q_i(t))$$

Tyto dvě formule umožňují rekurzivně (tj. v závislosti na struktuře stromu) spočítat pravděpodobnost celkového selhání subsystému nebo celého systému.

Model stromů poruch (v pravděpodobnostním rozšíření) dává komplexní pohled na hierarchii komponent v subsystémech. Umožňuje:

- určovat pravděpodobnosti poruchy jednotlivých komponent i subsystémů v daném čase;
- určit čas, kdy pravděpodobnost poruchy komponenty nebo subsystému překročí určitou zadanou mez;
- vytipovat komponentu, která nejvíce snižuje (ohrožuje) spolehlivost subsystému.

Model popisuje spolehlivostní chování jednotlivých komponent a zároveň i větších celků – subsystémů a systémů.

Poznámka Kromě uzlů AND a OR lze zavést ve stromech poruch i četné další operátory pro spolehlivostní konjunkci (poskládání vlivů poruch) prvků složené komponenty. Pro účely spolehlivostního modelování zejména přichází v úvahu operátor TMR (Triple Modular Redundancy) pro spolehlivostní konjunkci tří bezpečnostních okruhů. Příslušné vzorce zde z důvodu úspory místa neuvádíme, ale lze je v popisované metodice bez potíží využít, podobně jako i pro jiné způsoby spolehlivostního spojení komponent.

2.5 Shrnutí

Zde uvedeme stručné (manažersky orientované) shrnutí, jakým způsobem lze výše popisované spolehlivostní modely využít v rámci komplexních postupů LCM:

- Jednotlivé systémy SKŘ lze popsat stromem poruch, listy stromu odpovídají fyzickým komponentám systému (tj. elementární prvky modelu se rozlišují na úrovni tzv. výrobních čísel komponent SKŘ).
- Zdrojovým spolehlivostním parametrem je konstantní intenzita poruch λ, přiřazená ke každému typu komponenty (interpretace intenzity poruch viz výše, nejjednodušší interpretace je střední frekvence poruch). Způsob určení konstantní hodnoty intenzity poruch z provozního sledování poruch je uveden výše. Též je možné použít údaj výrobce, tento údaj je obvykle pesimističtější (tj. větší hodnota λ) než realita.

- Konstantní intenzita poruch je velmi dobrou aproximací intenzity poruch elektronických prvků v rozsahu doby jejich technické životnosti (min. 10 let u počítačových prvků se střední hustotou integrace součástek, u analogových prvků i delší doba). U jiných než elektronických typů prvků je náhrada intenzity poruch konstantou jen velmi přibližná, prezentovaný model má ale potenciál pro (postupné) doplnění sofistikovanějších odhadů intenzity poruch (tj. její okamžité hodnoty $\lambda(t)$ pro relativní čas t měřený od od okamžiku uvedení komponenty do provozu).

- Každému listu stromu poruch lze tedy přiřadit hodnotu intenzity poruch podle typu komponenty odpovídající listu stromu. Z této hodnoty je možné určit podle výše uvedených vzorců pravděpodobnost poruchy komponenty $Q(t)$ nebo doplňkovou pravděpodobnost bezporuchového provozu komponenty $R(t)$.

- Jako čas t v uvedených vztazích pro $Q(t)$ a $R(t)$ je nejvhodnější použít délku periody mezi pravidelnými technologickými odstávkami. Dále pak lze pracovat jen s hodnotami Q a R namísto s časovými funkcemi $Q(t)$ a $R(t)$. Tyto hodnoty lze - podobně jako zdrojový parametr λ – též přiřadit ke každému listu stromu poruch. Hodnota např. $Q = 0,001$ znamená, že se příslušná komponenta (= list stromu poruch) porouchá mezi odstávkami s p-tí 0,001.

- Podle výše uvedeného vztahu lze též určit tzv. *aposteriorní* pravděpodobnost poruchy komponenty (= listu stromu) $Q^*(t, t1)$, což je pravděpodobnost poruchy komponenty přepočítaná pro případ, že se komponenta od uvedení do provozu v čase $t = 0$ do obecného času t_1 (určitě) neporouchala. Čili s využitím tohoto vztahu lze odpovědět např. dotaz - s jakou pravděpodobností dojde k výrazným potížím v SKŘ až v posledním měsíci roční periody mezi odstávkami.

- Známe-li hodnoty λ (a odvozeně Q a R) pro každý list stromu poruch, lze relativně jednoduchým postupem (viz výše) přepočítat tyto hodnoty až na kořen stromu poruch, tj. lze určit hodnoty Q a R pro celý subsystém či systém SKŘ modelovaný stromem poruch, jinak řečeno: lze určit pravděpodobnost selhání příslušného systému či subsystému SKŘ v době mezi odstávkami.

3 Modely životnosti

Tato kapitola vychází z předchozí kapitoly o spolehlivosti a navazuje na výše představený model spolehlivosti.

3.1 Vymezení pojmů

Životnost je délka doby života komponenty (resp. subsystému). Každá komponenta má určitou dobu života danou opotřebováním – tzv. *technickou životnost*. V době charakterizované technickou životností je odhadnutelná intenzita poruch, je to buď konstanta (elektronické součástky a počítačové prvky z nich konstruované) nebo mírně narůstající funkce (např. mechanické součástky, vliv opotřebení). Po vyčerpání doby technické životnosti již nelze intenzitu poruch důvěryhodně odhadnout (prudce narůstá). Tedy i pravděpodobnost vzniku poruchy komponenty prudce narůstá. Tudíž odhady spolehlivosti komponent a systémů uváděné v předchozí kapitole mají smysl pouze v době vymezené jejich technickou životností.

Pro elektronické komponenty je technická životnost většinou velká. Celkovou životnost ale určuje (resp. ji snižuje) především *morální zastarávání* (angl. obsolescence) komponenty. Problém morálního zastarávání se v obecné rovině netýká konkrétní komponenty (lze ji vyměnit, pokud máme dostatek náhradních) ale *typu komponenty* (například zdroj 24V PSU).

Životnost typu komponenty se vyvíjí většinou v několika etapách. Nejdříve výrobce přestane komponentu vyrábět, ale stále poskytuje zákazníkům podporu (tj. opravy, případně je schopen sehnat kompatibilní náhradu komponenty). Po nějaké době pak dojde i k ukončení této podpory a náhradní díly jsou tudíž nedostupné. Je třeba včas naplánovat inovaci SKŘ tak, aby bylo možné nahradit konkrétní typ nepodporované komponenty jiným (novějším) typem. Následující podkapitoly pojednávají o životnosti konkrétních instancí komponent. Následující kapitola zavádí model pro popis životnosti typů komponent. Jedná se o dva rozdílné modely.

3.2 Životnost komponent

3.2.1 Používané veličiny

Projektovaná životnost Projektovaná životnost je odhadovaná časová hodnota délky života počítaná od jejího nasazení do provozu. Udává ji výrobce komponenty. Pokud tento údaj výrobce není schopen dodat, je potřeba projektovanou životnost stanovit expertním odhadem.

Zbytková životnost Zbytková životnost je proměnlivá veličina. Její hodnotu je potřeba stanovit k určitému časovému okamžiku (např. aktuální čas, čas plánované odstávky, ...). Zbytková životnost pak udává kolik času komponentě zbývá do konce života (stanoveného hodnotou projektované životnosti).

Projektovanou životnost bývá obtížné stanovit, proto bude dále používán spíše pojem *odhad očekávané životnosti*. Tento odhad definujeme jako náhodnou veličinu, kterou lze popsat pravděpodobnostním rozdělením, tj. hustotou pravděpodobnosti $f(t)$. Zjištění přesného tvaru pravděpodobnostního rozdělení je většinou obtížné, nicméně je možné jej aproximovat spojitým rovnoměrným rozdělením na intervalu $< t_{min}, t_{max} >$. Hodnoty t_{min} a t_{max} mohou být interpretovány jako minimální a maximální očekávaná životnost. Pro potřeby modelu je třeba tyto hodnoty získat z expertního odhadu (pesimistický a optimistický odhad, může to být i stejná hodnota). Hodnoty očekávaných životností je možné získat také od výrobce komponenty nebo výpočtem z teoretického modelu.

Poznámka: Hodnoty odhadů očekávané životnosti nejsou definitivní, ale je možné je různými metodami postupně zpřesňovat a postupně realizovat jejich implementaci v rámci uvažovaného SW systému pro podporu LCM. Například na základě provozních měření vhodně zvolených fyzikálních vlastností lze získat přesnější odhady očekávané životnosti komponenty. Výsledky získané z prezentovaného modelu životnosti jsou pak přesnější.

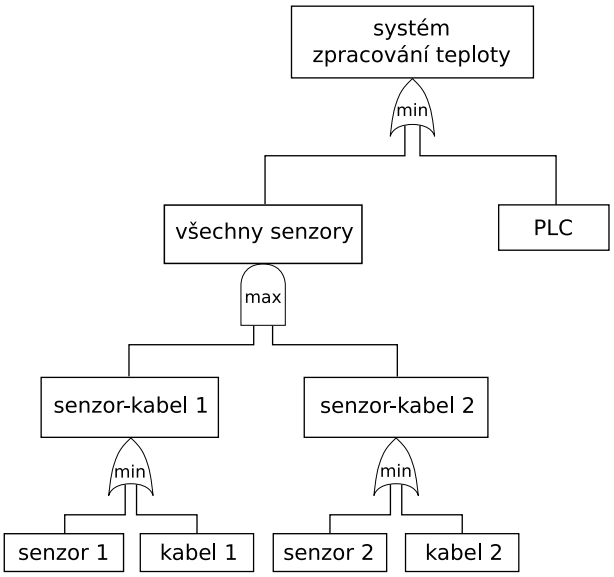
3.3 Životnost subsystémů

V předchozí kapitole byl představen model stromů poruch jako vhodný nástroj pro sledování spolehlivosti komponent a subsystémů. Vyhodnocování životností komponent a z nich složených subsystémů je jiná úloha, která ovšem pracuje nad stejnými komponentami. Vazby mezi komponentami jsou z hlediska spolehlivostního i životnostního rovněž stejné (obě hlediska sledují život komponenty). Proto je vhodné použít stejný model pro vyhodnocování spolehlivostí i životností.

Poznámka: Jedná se o model na úrovni instancí komponent (výrobních čísel), nikoliv na úrovni typu komponent.

Standardní metoda stromů poruch může být zobecněna tak, aby vyhovovala použití i k výpočtu životností složených komponent. Struktura stromu zůstane stejná, jen je třeba zavést několik sémantických změn. Nejdůležitější z nich je fakt, že uzly stromu nyní představují samotné komponenty, nikoli jejich poruchy. Porucha komponenty (resp. možnost poruchy) je jedna z jejích vlastností, proto zůstává struktura stromu stejná. Tato výrazná změna v pojetí stromu je důležitá, protože potřebujeme vytvořit obecnou strukturu, která bude umět pracovat s poruchami stejně jako s pravděpodobnostními parametry a hodnotami životností. Každé komponentě tedy můžeme kromě poruchového stavu přiřadit další vlastnosti (pravděpodobnosti poruchy, životnosti, aj.).

Pro účely vyhodnocení životnosti v LCM každý uzel obsahuje minimální a maximální životnost komponenty.



Obrázek 2: Příklad stromu poruch rozšířeného pro účely vyhodnocení životností v LCM.

Hodnoty minimální a maximální životnosti jsou relativní, takže v listových uzlech odpovídajících fyzickým komponentám (výrobním číslům) musíme uchovávat také absolutní čas uvedení komponenty do provozu (t_0). Tato hodnota musí být nastavena na aktuální čas pokaždé, když je komponenta vyměněna za novou. Zbytková životnost se proto určí takto:

$$t_{minzbytkovy} = t_0 + t_{min} - t_{now}$$

kde t_{now} je aktuální čas, tj. čas v němž (resp. pro nějž) model vyhodnocujeme.

Analogický vzorec lze napsat pro t_{max}.

Pro vyhodnocení stromu potřebujeme pozměnit význam nelistových uzlů, které reprezentují propojení v systému. Paralelní spojení (vyjádřené AND uzlem) má význam maxima z očekávané životností v uzlech potomcích. Sériové spojení (vyjádřené uzlem OR) má význam minima z očekávané životností v uzlech potomcích. Vyhodnocení probíhá odděleně pro hodnoty t_{min} a t_{max}, proto pro kořenový uzel dostaneme dvě konečné hodnoty t_{min} a t_{max}, které můžeme interpretovat jako pesimistický a optimistický odhad životnosti celého systému modelovaného příslušným stromem poruch.

Obrázek 2 ukazuje příklad rozšířeného stromu poruch. Strom je vytvořen nad dvěma teplotními čidly se dvěma kabely, která jsou obě připojena k PLC (Programmable Logic Controller). Tyto komponenty tvoří listy. Porucha *kabel*1 nebo *čidlo 1* způsobí poruchu *čidlo-kabel 1* (stejným způsobem pro *čidlo 2* a *kabel 2*).

Tato dvě čidla (s kabely) jsou ekvivalentní, redundantní. Tudíž až když nastanou obě poruchy *čidlo-kabel*, vznikne porucha *všechna čidla*. Obě čidla jsou připojena k jednomu PLC, tudíž porucha *všechna čidla* nebo porucha PLC způsobí selhání *zpracování teploty*.

Jako poruchy nebo selhání můžeme pro účely LCM považovat překročení životnosti komponenty. Pojmenujme životnosti následujících komponent *čidlo 1*, *kabel 1*, *čidlo 2*, *kabel 2* a PLC takto: t_{s1}, t_{c1}, t_{s2}, t_{c2} a t_p.

Potom můžeme vyjádřit životnost kořenu stromu (tj. celého systému) následovně:

$$t = \min(\max(\min(t_{s1}, t_{c1}), \min(t_{s2}, t_{c2})), t_p)$$

Uzly stromu mohou také uchovávat další informace o komponentách a vytvořená stromová datová struktura pak může být použita i pro jiné účely než výše zmiňované.

4 Model životnosti typu komponenty

Předchozí dvě kapitola se zabývala životností jednotlivých komponent a z nich složených subsystémů. Takovýto přístup, orientovaný na každou jednotlivou komponentu (výrobní číslo), může být složité implementovat a provozovat. Je totiž potřeba zjišťovat a průběžně aktualizovat data o každé komponentě.

Tato kapitola naopak popisuje životnostní model typu komponenty, kde všechny komponenty stejného typu jsou uvažovány jako jeden objekt – *typ komponenty*. Tj. např. všechna tlaková čidla stejného typu jsou pro účely modelu jedním typem komponenty. Dílčí rozdíly mezi jednotlivými kusy daného typu komponenty (místo použití, atd.) pro tento model nejsou důležité.

4.1 Životnost typu komponenty a čas záměny

Životnost typu komponenty lze definovat různě, nejužitečnější (pro navazující analýzy) se jeví zavést životnost typu komponenty jako *pravděpodobnost dostupnosti náhradního dílu k okamžité výměně, v případě, že se některá komponenta daného typu porouchala.*

Úlohou modelu životnosti typu komponenty je zejména sledování stavu dostupnosti náhradních dílů příslušného typu. V případě neomezené dostupnosti (aktivní produkt) lze model využít rovněž pro určení potřebného počtu náhradních dílů na skladě. Odvozenou složitější úlohou je určení vhodné doby, kdy je potřeba pro udržení dané spolehlivosti systému nebo subsystému SKŘ provést záměnu ohroženého typu komponenty za jiný (novější).

Poznámka: V této podkapitole bude pojem záměna označovat kompletní výměnu *typu komponenty* za jiný typ (nikoliv dílčí výměnu jedné porouchané komponenty).

4.2 Etapy života typu komponenty

V životě typu komponenty existují určité milníky, které výrazně mění životnostní parametry komponent příslušného typu. Vyčerpání (i odhadované) životnosti typu komponenty je výrazným podnětem pro plánování inovace SKŘ, zejména pokud se jedná o vyčerpání životnosti pro více typů komponent.

S ohledem na přijatelnou složitost a přehlednost výsledného modelu se jeví jako výhodnější (až téměř nezbytné) zkoumat životnost typu komponenty odděleně ve třech etapách.

Rozdělení života typu komponenty do (tří) etap v zásadě odpovídá stupňům rizika zastarání typu komponenty zavedeným v metodikách pro obsolescence management technologických procesů.

4.2.1 Etapa I

Etapa I začíná zahájením masové distribuce vyrobeného typu – značeno jako čas T_I. Etapa I končí v čase ukončení výroby typu komponenty – T_{II}. V této etapě je typ komponenty plně funkční, jeho životnost není ohrožena morálním zastaráváním (tj. nedostupností náhradní komponenty daného typu). Z tohoto důvodu v této etapě nemá smysl mluvit o záměně typu.

Pro komponenty kritické z hlediska dostupnosti (zejména PLC) je potřeba v této etapě udržovat na skladě dostatečné množství náhradních dílů, aby bylo splněno zvolené riziko nedostupnosti náhrady.

4.2.2 Etapa II

Etapa II začíná časem T_{II} (výrobce ukončil masovou výrobu daného typu komponenty) a končí časem $TIII$ (výrobce ukončil i podporu pro daný typ komponenty). V této etapě již není možné dokoupit nové náhradní díly. Výrobce nabízí jen možnost opravy stávajících porouchaných komponent. Pro každý typ komponenty je potřeba evidovat dobu opravy (T_{opr}) (čas, než se komponenta vrátí z opravy). Náhradních komponent je potřeba mít na začátku etapy na skladě dostatečné množství, aby nahradily porouchané komponenty po dobu jejich opravy.

Poznámka: Etapu II lze také popsal alternativním modelem, kdy během etapy

postupně narůstá riziko nedostupnosti náhradní komponenty. Model uvažuje předpoklad lineárního růstu intenzity nedostupnosti náhradní komponenty. V čase T_{II} je intenzita 0 a v čase T_{III} je riziko (pravděpodobnost) nedostupnosti náhrady rovno r_Z. Takovýto model pro vyhodnocování životnosti je poměrně složitý, proto nebyl použit.

4.2.3 Etapa III

Poslední etapa života komponenty běží od času T_{III}. V této etapě již nelze jednoduše zajistit náhradu porouchané komponenty. Je potřeba vystačit s množstvím náhradních dílů, které jsou k dispozici (např. na skladě) v čase T_{III}. V této etapě už pravděpodobnost dostupnosti náhradního dílu (zavedené výše jako číselná charakteristika životnosti typu komponenty) klesla pod stanovené riziko a s průběhem času dále klesá.

4.2.4 Přehled mezních časů a etap života

Mezní časy T_I – čas zahájení masové výroby daného typu komponenty T_{II} – čas ukončení masové výroby daného typu komponenty T_{III} – čas ukončení podpory (servisu) pro daný typ komponenty Hodnoty časů ukončení výroby a podpory nejsou většinou dopředu známé. V etapě II je třeba pro výpočty znát hodnotu T_{III}, kterou je nutné stanovit expertním odhadem (resp. měnit v rámci manažerských úvah kolem plánování potřebné inovace). Pro účely etapy III lze již tuto hodnotu považovat za známou, provede se tedy nahrazení odhadu z etapy II přesnější hodnotou.

Etapy života

1. Etapa I – interval $< T_I, T_{II} >$
2. Etapa II – interval $< T_{II}, T_{III} >$
3. Etapa III – interval $< T_{III}$, konec života>

4.3 Odhad životnosti typu komponenty

V etapě I a II života typu komponenty lze definovat pravděpodobnost dostupnosti náhradních komponent použitelných k okamžité výměně pro případ, že se některá komponenta daného typu porouchala, následujícím vzorcem:

$$P = \sum_{n=0}^{s} \frac{e^{-K\lambda T} \left(K\lambda T\right)^n}{n!}$$

Riziko nedostupnosti náhrady (vyčerpání skladu) v případě potřeby označíme r_Z. Toto riziko lze definovat jako doplněk pravděpodobnosti dostupnosti náhradního dílu do hodnoty 1.

$$r_Z = 1 - P$$

Význam použitého značení

n	sumační index
P	pravděpodobnost dostupnosti náhrady
s	počet náhradních dílů
K	počet komponent daného typu nasazených v systému
T	časová perioda pro vyhodnocování (liší se podle etapy života)
λ	počet poruch za jednotku času (lze určit jako $1/MTBF$, viz též kapitolu 2)
r_Z	pravděpodobnost, že při poruše komponenty nebude k dispozici náhradní kus pro výměnu

Proměnná T se určí podle etapy, v níž se s modelem pracuje. V etapě I se jedná o dobu potřebnou k opravě vadné komponenty a v etapě III se jedná o odhadovanou dobu od času T_{III} do doby záměny typu komponenty.

Pomocí výše uvedeného modelu je možné řešit následující tři úlohy:

- Stanovení rizika, že v dané době nebude pro výměnu k dispozici náhradní komponenta
- Určení počtu náhradních komponent
- Určení doby záměny

Následuje rozbor možných úloh, které lze řešit s využitím modelu popisovaného modelu životnosti typu komponenty.

4.3.1 Riziko nedostupnosti náhrady

Z daného počtu náhradních komponent s a zvolené periody T lze vypočítat riziko r_Z, že do doby záměny nevystačí zásoba náhradních komponent. Tato úloha je snadno vyčíslitelná přímým dosazením do vzorce v odstavci 4.3.

4.3.2 Potřebný počet náhradních komponent

Další aplikací modelu je úloha určení potřebného počtu náhradních komponent s takového, aby ze dobu T bylo riziko nedostupnosti náhrady maximálně r_Z.

Počet náhradních komponent s je potřeba určit iterativně. Dosazované hodnoty s a r_Z budou označeny s' a r'_Z, aby byly odlišeny od zadaných hodnot.

1. Do vzorce z odstavce 4.3 dosadíme $s' = 0$.
2. Spočteme příslušné riziko r'_Z.
3. Pokud je r'_Z větší než stanovené r_Z, zvýšíme s' o 1 a pokračujeme krokem 2.
4. Získané s' prohlásíme za s.

4.3.3 Doba záměny

Z daného počtu náhradních komponent a zvoleného rizika r_Z, že náhrada nebude k dispozici, lze z modelu vypočítat nejzazší dobu pro záměnu daného typu komponenty za nový typ T.

Tato úloha není jednoduše vyčíslitelná, ani spočitatelná jednoduchým iterativním postupem. Její řešení je ale možné pomocí numerických metod pro řešení rovnic. Alternativou k tomuto přesnému postupu je ruční dosazování časů záměny a sledování velikosti výsledného rizika. Postupným snižováním/zvyšováním doby záměny lze takto přibližně dospět k požadovanému riziku.

4.4 Výpočty v jednotlivých etapách

4.4.1 Etapa I

V etapě jedna je možné bez problémů dokupovat náhradní díly. Záměnu typu v této etapě proto neuvažujeme. Má smysl počítat úlohy Potřebný počet náhradních komponent a případně Riziko nedostupnosti náhrady. Jako periodu T pro vyhodnocování modelu zde volíme dobu opravy porouchané komponenty.

4.4.2 Etapa II

Etapa II se od Etapy II liší de facto jen tím, že nelze navyšovat skladové zásoby. Výrobce stále opravuje porouchané komponenty, proto periodu T volíme opět jako dobu opravy komponenty. Má smysl počítat úlohu *Riziko nedostupnosti náhrady* a *Doba záměny*.

4.4.3 Etapa III

V etapě III (tj. po čase T_{III}) je k dispozici definitivní počet s náhradních komponent. Tento počet v průběhu etapy klesá, proto s není konstanta. Při každém poklesu (tj. výměně komponenty) je potřeba přepočítat vzorce pracující s počtem náhradních dílů s. V této etapě je uvažována časová perioda T jako:

$$T = T_z - T_{III}$$

T_z označuje odhadovanou dobu záměny, nebo jinou dobu pro kterou model vyhodnocujeme (viz níže). V této etapě počítáme zejména úlohu *Doba záměny*. Případně pro stanovenou dobu záměny můžeme určovat *riziko nedostupnosti náhrady*.

5 Závěr

Tato práce prezentuje zveřejnitelné výsledky výzkumu prováděného jako součást zpracovávání studie pro zadavatele ČEZ, a.s.

V textu byly představeny modely pro vyhodnocování spolehlivosti a životnosti komponent, z nich složených subsystémů a dále typů komponent. Modely komponent a subsystémů vyžadují rozsáhlejší SW podporu. Analýza a návrh takového SW systému je provedena v neveřejných publikacích [8] a [9]. Na základě těchto modelů je možné sledovat zbytkovou životnost a spolehlivost instalovaných komponent a subsystémů v daném čase. Pokud některá z těchto veličin (např. v daném čase plánované odstávky) klesne pod zadanou mez, je třeba při odstávce vyměnit komponenty, které tento pokles významnou měrou způsobily.

Model typu komponent analyzuje životnost všech komponent daného typu jako celku. Příslušná podkapitola obsahuje vzorce a algoritmy vyhodnotitelné i bez podpory speciálního SW. Tyto jednodušší výpočty je možné realizovat pomocí tabulkového kalkulátoru (např. Microsoft Excel).

Reference

[1] „Management of life cycle and ageing at nuclear power plants: Improved I&C maintenance,“ TECDOC-1402, *International Atomic Energy Agency*, Vídeň, Rakousko, 2004

[2] „Military Handbook – Reliability prediction of electronic equipment,“ MIL-HDBK-217F, Department of Defense, USA 1991

[3] „Spolehlivost v technice,“ ČSN 01 0102, ČNI 1983

[4] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, „Fault Tree Handbook,“ NUREG-0492, *U.S. Nuclear Regulatory Commision (NRC)*, -, 1981

[5] J.-C. Geoffroy and G. Motet, „Design of Dependable Compiting Systems,“ *Kluwer Academic Publishers*, Dordrecht, The Netherlands, 1998

[6] R. Billinton and R. N. Allan, „Reliability Evaluation of Engineering Systems: Concepts and Techniques,“ *Plenum Press*, New York, USA, 1983

[7] D. P. Siewiorek and R. S. Swarz, „The Theory and Practice of Reliable System Design,“ *Digital Equipment Corporation*, Bedford, USA, 1982

[8] P. Dvořák, E. Janeček, M. Paška, S. Racek, „Studie současného stavu a trendů v systémech plánování inovace SKŘ na JE ČEZ a.s. se zvláštním zaměřením na ETE 1. etapa,“ *Západočeká univerzita*, Plzeň, 2006

[9] P. Dvořák, E. Janeček, M. Paška, S. Racek, „Studie současného stavu a trendů v systémech plánování inovace SKŘ na JE ČEZ a.s. se zvláštním zaměřením na ETE 2. etapa,“ *Západočeká univerzita*, Plzeň, 2007