ČESKÁ SPOLEČNOST PRO JAKOST
Novotného lávka 5, 116 68 Praha 1

MODELY PORUCH SE SPOLEČNOU PŘÍČINOU

Materiály z 26. setkání
odborné skupiny pro spolehlivost

Praha, únor 2006

OBSAH

Poruchy se společnou příčinou při vysokém stupni zálohování

Ing.Petr Babič, CSc.

Poruchy se společnou příčinou při vysokém stupni zálohování

Ing. Petr Babič

Setkání odborné skupiny pro spolehlivost
dne 27. 2. 2007
ČSVTS, Praha 1, Novotného lávka 5

CCF – Záběr, cíl a obsah příspěvku

- Záběr: Systémy související s bezpečností – je to obdoba záběru normy ČSN EN 61508 -1 (2002)
- Cíl: V oblasti metodiky odhadu podílů poruch se společnou příčinou (CCF) doplnit tuto normu o modelování poruch při vyšším stupni zálohování
- Témata:

1. Kdy komponentu (podsystém) zálohovat?
2. Jak účinné může v praxi být zálohování?
3. Zjevné a skryté příčiny společného selhání záloh
4. CCF jako souhrnný příspěvek reziduálních příčin
5. Degradace záloh prodělanými provozními šoky
6. Model BFR a metoda zobecněných beta faktorů

CCF – Kdy použít zálohování (1)

- **Kvalitativní bezpečnostní požadavky**

1. Odolnost vůči jednoduché poruše v systému (2*100%)
2. Odolnost vůči jednoduché poruše + možnost testovat části systému za provozu (3*100%)
3. Odolnost vůči nebezpečné poruše i vůči falešným povelům (majoritní zapojení 2 ze 3 podsystémů)

- **Kvantitativní bezpečnostní požadavky**

1. Požadovaná maximální hodnota pravděpodobnosti selhání funkce v náhodném okamžiku vyžádání
2. Požadovaná maximální hodnota pravděpodobnosti výskytu nebezpečné poruchy za hodinu (tzn. max. intenzita nebezpečných poruch)
3. Jiná kritéria – viz například úroveň integrity bezpečnosti (SIL) dle ČSN EN 61508-1

CCF – Kdy použít zálohování (2)

Příklad kvantitativních bezpečnostních požadavků
Úroveň integrity bezpečnosti (SIL) dle ČSN EN 61508-1 (zjednodušeno):

Režim:	s nízkým vyžádáním (méně než 1krát za rok)	s vysokým nebo nepřetržitým vyžádáním
	Pravděpodobnost poruchy při vyžádání	Intenzita nebezpečných poruch [1/hodina]
SIL 4	< 1E-5, 1E-4)	< 1E-9, 1E-8)
SIL 3	< 1E-4, 1E-3)	< 1E-8, 1E-7)
SIL 2	< 1E-3, 1E-2)	< 1E-7, 1E-6)
SIL 1	< 1E-2, 1E-1)	< 1E-6, 1E-5)

CCF – Kdy použít zálohování (3)

Vztah integrity bezpečnosti hardwaru, relativního podílu bezpečných poruch a odolnosti N proti vadám hardwaru (tj. N+1 vad může vést ke ztrátě funkce) (dle ČSN EN 61508-2, Tabulka 3) :

Poměr bezpečných poruch	odolnost proti vadám hardwaru (stupeň zálohování potřebný pro zvolenou hodnotu SIL, a to při ne zcela jasném poruchovém chování některé složky)		
	N=0	N=1	N=2
méně než 60%	nedovolena	SIL1	SIL2
< 60%, 90%)	SIL1	SIL2	SIL3
< 90%, 99%)	SIL2	SIL3	SIL4
více než 99%	SIL3	SIL4	SIL4

Účinnost zálohování - Přínos z přidání zálohy

1. Ideální případ – neexistence závislostí mezi poruchami v podsystémech - u záložních podsystémů je plně uplatněn princip nezávislosti a diverzity (různorodosti): jiný typ čidel, zpracování informací i akčních členů, jiné zdroje, jiná místnost apod.
2. Praktické příklady – existují shody v provedení podsystémů a vzájemné vazby (stejný výrobce, stejný materiál, stejná údržba, společně sdílené části, zdroje a služby, fyzické vazby, prostorová blízkost, týž způsob provozu, společná historie zátěží a šoků)

Orientační přínos pro pravděpodobnost/ intenzitu poruch celku :

- při zdvojení podsystému se ukazatel sníží cca o 1 řád (tj. klesne na desetinu hodnoty pro nezálohovaný systém)
- Přidání třetího podsystému tuto úroveň redukuje už jen na třetinu
- Čtvrtý podsystém výsledek sníží výsledek už jen na polovinu

CCF – Společné příčiny selhání podsystémů

Zjevné příčiny

- Selžou společně sdílené zdroje, komponenty, signály, povely, služby (chlazení)
- Potřeba a význam komponenty/systému závisí na stavu jiných komponent nebo systémů

Spolehlivostní analytik by tyto zjevné závislosti mezi zálohujícími se podsystémy měl zjistit a samostatně jmenovitě zahrnout do modelu selhání funkce systému

Skryté příčiny

- Skupina komponent obdobného typu, velikosti a funkce, od téhož výrobce, se stejným provozním stavem, s podobnou historií provozu, testovaná a udržovaná podle stejných postupů atd.
  = skupina podobných komponent náchylná ke vzniku CCF (tzv. CCF skupina)
- Do modelu se pro každou takovou skupinu kromě individuálních poruch zahrnou i příspěvky CCF, představující odhad souhrnného vlivu všech nejmenovaných příčin.

CCF – Model BFR se dvěma typy šoků

Intenzita CCF typu „porucha **k** komponent z **n**" se při užití metody Binomial Failure Rate (BFR) popisuje vztahem:

$$\beta(k,n) * \lambda = \begin{cases} \mu\, \rho^k (1-\rho)^{n-k} & \text{pro } k < n \\ \mu\, \rho^n + \omega & \text{pro } k = n \end{cases}$$

kde

λ = celková intenzita poruch komponenty (náhodné individuální poruchy i poruchy se společnou příčinou)

μ = četnost výskytu nevyřazujících šoků

ρ = pravděpodobnost vzniku poruchy komponenty při nevyřazujícím šoku

ω = četnost výskytu vyřazujících šoků (nastane-li tento šok, vyřadí všech n komponent z CCF skupiny)

CCF – Příklad hodnot zobecněných beta faktorů

Hodnoty β(k, n) pro následující parametry BFR modelu:
ρ = 0,333; μ = 0,405 * λ; ω = 0,005 * λ

k	n=2	3	4	5	6	7	8
2	0,05	0,03	0,02	0,01	0,009	0,006	0,004
3	-	0,02	0,01	0,007	0,004	0,005	0,002
4	-	-	0,01	0	0	0	0
5	-	-	-	0,007	0	0	0
6	-	-	-	-	0,006	0	0
7	-	-	-	-	-	0,005	0
8	-	-	-	-	-	-	0,005

Metodika analýzy poruch se společnou příčinou - přehled aktuálního stavu

RNDr. Jaroslav Holý, oddělení analýz spolehlivosti a rizik, ÚJV Řež a.s.

Úvod

Moderní vzorový postup analýzy násobných poruch se společnou příčinou byl vyvinut v oblasti vývoje a aplikací složitých pravděpodobnostních modelů analýz bezpečnosti, rizik a spolehlivosti jaderných elektráren. První pilíře postupu byly vytyčeny v americkém metodickém materiálu NUREG/CR-4780 [1] z roku 1988. Z něj vychází novější NUREG/CR-5801 [2] z roku 1993, který původní postup mírně modifikuje a snaží se být sofistikovanější a striktnější. V současné době je pak kvantitativní i kvalitativní analýza CCF většinou založena na základním materiálu NUREG/CR-5485 [3] z roku 1998, zohledňujícím řadu nových poznatků mechanismech vzniku násobných poruch a poskytujícím teoretický rámec pro kvantifikaci potenciálu pro jejich vznik. Přestože všechny uvedené zdroje metodologie vznikaly v souvislosti se zajišťováním postačující úrovně **bezpečnosti** průmyslových technologií jaderné energetiky, je jejich struktura, nástroje i závěry velmi široce a v řadě ohledů bez výjimky přenositelná i na spolehlivostní analýzy (využívající stejný fundamentální nástroj jako analýzy bezpečnosti - pravděpodobnostní míru) a na široké spektrum technologií spojených s původním subjektem analýz - systémy jaderných elektráren - jen velmi volnými vazbami.

Stručný přehled postupu analýzy CCF

V souladu s metodikou detailně rozebranou v [3] lze analýzu potenciálu pro vznik poruch se společnou příčinou a jeho integraci do spolehlivostního modelu technologického systému rozdělit do čtyř hlavních etap.

Etapa 1 – Sestavení logického modelu systému

Tato etapa není orientována ryze na poruchy se společnou příčinou, ale reprezentuje základní přípravné kroky pro vznik prostředí, v němž mohou být poruchy se společnou příčinou identifikovány, modelovány a dále analyzovány. Skládá se ze dvou hlavních kroků

Krok 1.1 - Seznámení se systémem

Důkladné seznámení se s modelovaným systémem je jádrem spolehlivostní analýzy systémů, ať již zahrnuje hodnocení potenciálu pro vznik CCF či nikoli. Selhání technologického systému nelze modelovat, dokud analytik neporozumí požadovaným funkcím systému, jeho komponentám a postupům pro provoz, testy a údržbu. Zvláštní pozornost v rámci kroku je věnována těm aspektům struktury, činnosti a nepohotovosti systému (z důvodu poruch, testů či oprav), jež by mohly ovlivnit provozuschopnost **více** (identických) komponent.

Krok 1.2 - Definování problému

V tomto kroku musejí být definovány hranice systému (například podle fyzických mezí nebo způsobu zajištění funkce systému), závislost provozuschopnosti systému na jiných systémech

(jeho podpůrné systémy), návaznosti na funkci ostatních systémů v daném technologickém uzlu a kritéria úspěšnosti fungování systému. Pro další využití při analýze CCF je třeba určit, které kořenové příčiny a prvky eventuálních závislostí mají být modelovány explicitně (příkladem příčin modelovaných explicitně jsou některé kategorie chyb obsluhy, jako chybná kalibrace nebo neodblokování zařízení a systémů po testu či opravě). Tím je vymezen rámec pro analýzu tzv. **residuálních CCF**, které jsou jako spektrum ostatních kořenových příčin podchyceny společně v CCF události, zastoupené speciálním objektem logiky spolehlivostního modelu. Analytik musí ve všech potřebných místech spolehlivostního modelu stanovit jednoznačný předěl mezi reziduálními CCF a mezi násobnými výpadky a jinými plošně se projevujícími události modelovanými explicitně, spolu s pojmenovanou konkrétní příčinou svého vzniku.

Při konstrukci spolehlivostních modelů systémů se zahrnutím CCF fenoménu jsou vyhledávány skupiny komponent, pro něž je třeba do vybraného logicko-pravděpodobnostního schématu přidat doplňující základní událost s významem "reziduální CCF". Při standardně prováděné analýze se pro výběr pozic spolehlivostního modelu, na něž jsou umisťovány CCF, aplikují následující principy, kdy komponenty v jednotlivých nadefinovaných skupinách musejí:

- být typově identické
- zabezpečovat shodný úkol
- náležet ke stejnému systému.

To znamená, že modelovaný vliv CCF s potenciálem působit na skupinu komponent provozovaných v rámci vymezeného technologického celku bývá omezen pouze na působení komponenty **stejného typu** uvnitř **jednoho systému** (a navíc ztrácející svou funkci stejným předdefinovaným způsobem - **ve stejném poruchovém módu**).

Etapa 2 - Třídění skupin komponent se společnou příčinou

Cílem etapy zaměřené na třídění je:

- zjistit, které skupiny komponent studovaných systémů mají být zahrnuty do analýzy reziduálních CCF anebo z ní naopak vyřazeny
- uspořádat skupiny zařazené do další analýzy podle jejich předpokládaného významu, aby čas a zdroje na analýzu CCF byly co nejlépe využity
- poskytnout technické argumenty jako pomoc pro analýzu dat v následné etapě
- poskytnout technické argumenty k formulaci alternativ obrany technologie proti CCF a podpořit tak doporučení zformulovaná v závěrečné etapě analýzy zaměřené na interpretaci výsledků.

Tyto cíle se realizují pomocí kvalitativního i kvantitativního kroku třídění. Přestože jsou oba kroky popisovány odděleně, v praxi se často provádějí souběžně, iterativním způsobem.

Krok 2.1 - Kvalitativní třídění

V tomto kroku se vyhledávají společné vlastnosti komponent a mechanismy vzniku poruchy, které by mohly vést k poruše od téže příčiny. Ke zjištění zřejmých známek závislosti mezi zálohujícími se komponentami slouží dosavadní zkušenosti i technická intuice. Zkušenosti a intuice se užívají rovněž při hodnocení obranných opatření, jež mají sloužit k vyloučení nebo

snížení potenciálu pro vznik určitých CCF jevů. Například analytik může předpokládat, že výskyt CCF u odlišných, navzájem nepodobných komponent je vzhledem k dosavadním zkušenostem nepravděpodobný. Z toho může vyjít úvodní výběr skupin komponent pro analýzu CCF.

Jako základ (nebo i další iterace) počátečního hledání projevů CCF potenciálu se provádí formální analýza kořenových příčin poruch zařízení. Efektivnost procesu analýzy se zvýší, pokud je analýza kořenových příčin prováděna až po kvantitativním třídění (viz krok 2.2). Analýza kořenových příčin poruch se zaměří především na tři obecné typy příčin:

- kořenové příčiny působící na podobná zařízení
- kořenové příčiny působící na zařízení ve stejném místě
- kořenové příčiny působící na zařízení, provozovaná podle týchž procedur.

Krok 2.2 - Kvantitativní třídění

V tomto kroku se přiřadí každé CCF události nějaká konzervativní hodnota pravděpodobnosti, vypočte se spolehlivostní charakteristika systému a určí se hlavní přispěvatele ke ztrátě jeho funkce. Následná úplná analýza CCF pak provede jen pro hlavní přispěvatele, jejichž výběr je v kroku 2.2 doložen aplikací metod analýzy citlivosti (*sensitivity analysis*) a analýzy důležitosti (*importance analysis*) na výsledky spolehlivostního zhodnocení modelu s konzervativními kvantitativními CCF vstupy.

Postup odhadu hodnot pravděpodobností výskytu CCF je tedy (nejméně) dvoukolový. Nejprve jsou základě získaných výchozích informací obecnějšího druhu utvořeny tzv. třídící hodnoty pravděpodobnosti výskytu pro všechny typy základních událostí s významem CCF. Třídící hodnotou číselného spolehlivostního parametru je takový odhad, jenž je dostatečně konzervativní a není pracný. Pokud se ani nadsazený konzervativní odhad po předběžné kvantifikaci celého modelu technologie nejeví jako numericky významný, není třeba tento odhad upřesňovat.

Pro ty základní události typu CCF, které splnily kritérium individuální důležitosti, tzn. události, pro něž předběžná kvantifikace modelu technologie ukázala, že míra jejich důležitosti je vyšší než zvolená mez, je nutné zredukovat konzervativizmus přibližného odhadu. U takto vybraných skupin komponent následuje další kolo přiřazování hodnot spolehlivostním parametrům, kdy se přikročí k provedení podrobných analýz, zaměřených na zlepšený, obvykle méně konzervativní, odhad pravděpodobnosti výskytu důležitých CCF.

Etapa 3 - Podrobné modelování poruch se společnou příčinou a analýza dat

Krok 3.1 - Definování základních událostí

Pro modelování CCF je výhodné zavést v metodě užité pro logicko-pravděpodobnostní reprezentaci chování systému (stromy poruch, bloková schémata) základní události typu CCF, tj. základní události představující vícenásobné poruchy u komponent, jež mají společnou kořenovou příčinu. Doprovodným efektem tohoto kroku může být předefinování základních událostí reprezentujících individuální poruchy komponent. V některých případech vede doplnění nových základních událostí CCF typu k další aktualizaci struktury logicko-pravděpodobnostního modelu.

Krok 3.2 - Volba pravděpodobnostního modelu pro CCF

Cílem tohoto kroku je sestavit modely, které poskytnou novým událostem z kroku 3.1 potřebnou strukturu pro kvantifikaci. Každé základní události (CCF nebo nezávislé) se přiřadí vhodný model pravděpodobnosti výskytu, založený například na konstantní intenzitě poruch anebo konstantní pravděpodobnosti poruchy při požadavku na činnost. Každý takový model má jeden či více číselných parametrů, odhadovaných na základě údajů z provozu analyzované technologie nebo určitých předpokladů. Tento krok je svázán s krokem 3.1, protože výběr číselného modelu má vliv na definice základních událostí a naopak.

Krok 3.3 - Klasifikace a třídění dat

Krok je zaměřen na posouzení a vyhodnocení zaznamenaných událostí z pohledu CCF objektů definovaných v modelu technologie v předchozích krocích. Zpracování informace o událostech vytváří vstupy pro odhady číselných parametrů CCF modelu. Nezbytné je odlišit závislé událost s příčinami závislosti modelovanými explicitně od událostí s příčinami zahrnutými mezi residuální CCF.

Dostupné zdroje dat typicky obsahují jednoduché i násobné poruchy. Vzhledem k tomu, že údaje o výskytech násobných poruch jsou u vyšetřované technologie obvykle chudé, je potřeba rozšířit hledání relevantních záznamů v provozní historii i na další exempláře stejné nebo obdobné technologie. Protože však tyto exempláře mohou být projektovány či provozovány odlišně, události zaznamenané na jedné realizaci technologie se nemusí uplatnit na jiné. Proto je prověření použitelnosti dat nezbytnou součástí každého dílčího kroku této fáze analýzy. Přezkoumání se soustředí na ty kořenové příčiny, vazební mechanismy a obranné strategie, jež se uplatňují u vyšetřované technologie. Vzhledem k tomu, že popisy poruch nejsou obvykle tak podrobné, jak by zpracovatel analýzy potřeboval, analýza událostí si vyžaduje velký díl úsudku a silně narůstá význam kvalitního zpracování dokumentace pro umožnění kontrolovatelnosti a opakovatelnosti analýzy.

Důležitým protipólem analýzy dostupných zdrojů dat je zjištění těch slabých míst vyšetřované technologie, jejichž příklady nejsou obsaženy v provozní zkušenosti. Pomoci často může obhlídka technologie a diskuse s provozním personálem o způsobu provozu a údržby systémů a o historii provozu. Lze tak získat důkladnou znalost případných unikátních slabin vyšetřované technologie v prevenci vzniku a účinku násobných poruch a zabránit podhodnocení četností výskytu CCF, ke kterému může dojít, pokud konkrétní studovaná technologie má nějakou unikátní slabinu, kterou nelze nalézt na jejích příbuzných exemplářích a tedy se s ní nesetkáme v databázi provozní informace. Příkladem by mohla být specifická konfigurace analyzovaného systému (převráceně namontované ventily vinou chybného dispozičního řešení), která učiní komponenty zranitelné některými příčinami poruch nebo která vytvoří vazbu mezi komponentami (nerovnoměrné průtočné množství u skupin čerpadel, zvýšená možnost ucpání průtočné trasy u skupiny armatur).

V případech, kdy u konkrétní technologie existuje zcela specifická slabina, jež není podchycena ve tříděných událostech, se zdá být logické, že skutečná četnost CCF by mohla být vyšší, než předpověď opírající se o utvořené statistiky. V literatuře lze nalézt podněty pro budoucí zlepšení metodiky analýzy CCF z těchto pohledů, ale prozatím není k dispozici nějaká praktická nebo všeobecně přijímaná metoda pro započtení specifických slabin. Jednou z možností je například

kombinovat poznatky o slabinách studované technologie, získané při obhlídce či jinými metodami, se statistikami, odvozenými z provozní zkušenosti pomocí analogie bayesovské aktualizace.

Krok 3.4 - Odhady hodnot parametrů

Cílem tohoto kroku je získat odhady hodnot číselných parametrů z modelů pravděpodobnosti výskytu CCF, a to na základě informací o použitelných jednoduchých i násobných poruchách z kroku 3.3. Existuje několik zdrojů nejistoty v interpretaci dat při hledání příčinných mechanismů vzniku poruch, při hodnocení možných důsledků pro modelovanou technologii a ve způsobu získávání údajů. Proto je při kvantifikaci žádoucí určovat nejen bodový odhad pravděpodobnosti vzniku poruchy daného druhu, ale i číselně ohodnotit nejistoty tohoto odhadu.

Etapa 4 - Interpretace výsledků

Krok 4.1 - Výpočty

Pravděpodobnosti výskytu CCF, získané v Etapě 3, se začlení do modelů nepohotovosti systémů a modelů četnosti výskytu poruchových sekvencí událostí a celý spolehlivostní model je následně kvantifikován.

Krok 4.2 - Analýza citlivosti a nejistot

Podrobný rozbor musí být proveden u těch skupin komponent, kde předběžná citlivostní analýza z úkolu ukázala velký vliv na celkové výsledky. Vzhledem k nejistotě ohledně výběru správného modelu CCF i odhadu odpovídajících parametrů je doporučeno zahrnout tyto nejistoty do odhadu celkových nejistot četnosti vzniku poruchového stavu. Další citlivostní analýza pak osvětlí vztah mezi předpoklady vztahujícími se k CCF, vstupními údaji a celkovými výsledky.

Krok 4.3 - Dokumentování analýz

Závěrečným krokem je zdokumentování analýz. Obzvlášť důležité je zřetelně specifikovat použité předpoklady a zjistit důsledky jejich použití.

Metody kvantifikace parametrů CCF modelů

Přestože je při obecném nedostatku potřebné provozní zkušenosti kvantifikace parametrů CCF modelů obtížným úkolem (anebo možná právě proto), existuje celá řada metod umožňujících transformovat provozní zkušenost a poznatky o designu studovaného systému a technologii na numerické hodnoty CCF parametrů. Jedná se například o tyto metody:

- metoda základních parametrů
- metoda alfa faktorů
- metoda beta faktoru
- metoda MGL (Multiple Greek Letters)
- metoda BFR (Binomial Failure Rate) se dvěma typy šoků.

Společným rysem všech metod je transformace informace o počtech událostí s různě vysokou ztrátou funkčnosti zálohujících se komponent do hodnot parametrů definujících potenciál pro

společný výpadek jakékoli vybrané konfigurace komponent z CCF skupiny. V následující části příspěvku bude podrobněji popsán proces kvantifikace parametrů využívající v praxi pravděpodobně nejčastěji aplikovanou metodu alfa faktorů.

Nejvyužívanější metoda kvantifikace pravděpodobností CCF- metoda alfa faktorů

Metoda alfa faktorů byla navržena jako parametrický model CCF, u něhož lze snadno získat odhad hodnoty parametrů z údajů o poruchách zkoumaného systému a zužitkovat přitom kvalitní odhad pravděpodobnosti náhodných individuálních poruch komponent z dané CCF skupiny.

Tento parametrický model používá celkem m+1 parametrů, kde m je počet komponent ve skupině podléhající násobným poruchám se společnou příčinou. Jedná se o celkovou četnost Q_t poruch komponenty a o soustavu m relativních podílů α_k na celkové četnosti, s nimiž se uplatňují poruchy násobnosti k, kde $1 \le k \le m$:

Q_t = celková četnost výskytu poruch u každé z komponent a to zahrnující jak nezávislé poruchy, tak i vícenásobné poruchy se společnou (residuální) příčinou

α_k (m) = (alfa faktor), relativní podíl četnosti výskytu poruch **právě k** komponent z celkového počtu m komponent ve skupině s výskyty CCF **na celkové četnosti** Q_t poruch komponenty

Z definice plyne následující normující vztah pro alfa faktory:

$$\alpha_1 (m) + \alpha_2 (m) + \ldots\ldots + \alpha_m (m) = 1.$$

Uváží-li se, že Q_i (m) je četnost výskytu některé základní události, představující současnou poruchu právě u i komponent z celkového počtu m komponent skupiny, a dále že celkový počet takových i-tic komponent ve skupině je dán příslušným kombinačním číslem, potom

$\binom{m}{i} Q_i(m)$ = sumární četnost výskytu všech událostí, představujících poruchu právě i komponent z m

$\sum_{i=1}^{m} \binom{m}{i} Q_i(m)$ = sumární četnost výskytu všech událostí, představujících poruchu aspoň jedné komponenty

Tedy pomocí základních parametrů Q_i (m) je možno definovat alfa faktory takto:

$$\alpha_k(m) = \frac{\binom{m}{k} Q_k(m)}{\sum_{i=1}^{m} \binom{m}{i} Q_i(m)} \qquad (1 \le k \le m)$$

Pro Q_t lze získat opačné vyjádření, tj. následující vztahy pro výpočet $Q_k(m)$, jsou-li známy hodnoty Q_t a α_k (m):

a) testy provozuschopnosti záložních zařízení rozprostřeny v čase

$$Q_k(m) = \frac{k}{\binom{m-1}{k-1}} \alpha_k(m) Q_t \qquad (1 \le k \le m))$$

b) testy provozuschopnosti prováděny najednou u celé skupiny

$$Q_k(m) = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k(m)}{\alpha_t} Q_t \qquad (1 \le k \le m)$$

kde

$$\alpha_t = \sum_{i=1}^{m} i * \alpha_i(m) = \alpha_1(m) + 2\alpha_2(m) + 3\alpha_3(m) + ... + m * \alpha_m(m) .$$

Maximálně věrohodný odhad pro α_k(m) je podle NUREG/CR-4780, vztah (C.58), dán vztahem

$$\alpha_k(m) = \frac{n_k}{\sum_{i=1}^{m} n_i} \qquad (1 \le k \le m)$$

kde n_k = počet zaznamenaných výskytů současných poruch u právě k komponent

Při detailnějším studiu vztahu pro odhad hodnot základních parametrů, je patrné, že ke stanovení hodnot alfa faktorů není nutno zjišťovat počty požadavků N_k na zapracování k-tic komponent. Tím je dána zásadní přednost tohoto modelu: namísto obtížně zjistitelných počtů požadavků (jež souvisejí s četností a strategiemi testů) se zjistí pouze počty poruch a z nich alfa faktory jako relativní podíly různých násobností poruch komponent CCF skupiny. Převod relativních hodnot na skutečné absolutní hodnoty spolehlivostních ukazatelů událostí se provede pomocí jakkoli získaného (separátní analýza, literatura) kvalitního odhadu Q_t. Pomocí známých hodnot alfa faktorů a Q_t se pak vypočtou hodnoty těch základních parametrů Q_k(m), které jsou zapotřebí pro kvantifikaci základních událostí modelujících různé příspěvky CCF ve stromech poruch systémů.

CCF a lidský faktor

Lidský faktor patří spolu s CCF mezi klíčové přispěvatele k pravděpodobnosti ztráty funkce technologie. Kromě separátního efektu tkví význam lidského faktoru i v jeho spojení s problematikou vzniku násobných poruch.

Při analýze spojení lidského faktoru a CCF je nutné rozlišit mezi dvěma typy závislostí projevujících se při obsluze technologie. První typ závislostí je dán faktem, že **jeden** konkrétní lidský zásah může, ať už při běžném provozu zařízení nebo při řešení abnormálního nebo mimořádného stavu, ovlivnit pohotovost více komponent. Podle rozsahu zařízení závislého na

daném lidském zásahu je odpovídající závislost zahrnuta na příslušné úrovni do logicko-pravděpodobnostního modelu technologie.

Jiným typem závislosti je závislost **mezi** lidskými zásahy. Úspěch nebo selhání jedné konkrétní akce obsluhy může ovlivnit pravděpodobnost úspěchu/selhání následující akce, a to dokonce ze dvou úhlů pohledu:

- úspěchem/neúspěchem akce vznikají objektivně lepší/horší podmínky pro úspěch nebo selhání akce následující (snižuje/zvyšuje se hladina stresu a dynamika vývoje situace, mění se vztah aktuální situace k scénářům řešeným při výcviku atd.)
- úspěch/neúspěch dané akce **sám o sobě vypovídá** o aktuálním stavu směny a její očekávané šanci na úspěch při akci další, bez ohledu na okolní podmínky (pokud směna nezvládne jednoduchou činnost, která by jí neměla činit problém, ukazuje to na aktuální přítomnost dosud neidentifikovaného závažného problému, který zpochybňuje její šance na úspěch i za příznivých okolních podmínek, a hrozí plošným postižením zařízení lidskou chybou).

Výsledky analýzy provozní historie různých typů technologie jednoznačně potvrzují velké ovlivnění potenciálu pro vznik poruchy se společnou příčinou dosaženou úrovní kvality a spolehlivosti práce obsluhy. Lze nalézt desítky zajímavých, velmi specifických případů, kdy selhání obsluhy vyvolalo násobnou poruchu více komponent. Navíc platí, že CCF události se zapojením lidského činitele (pracujícího obvykle s větším rozsahem technologie vcelku) mají v průměru výrazně větší negativní dopad než CCF poruchy zařízení z příčin ryze technologických, problematice lidského faktoru vzdálených.

Základní literatura k problematice CCF

[1] Mosleh A., Fleming K.N., Parry G.M., Paula H.M., Rasmuson D.M., Worledge D.H., „*Procedures for Treating Common Cause Failures in Safety and Reliability Studies*“, NUREG/CR-4780 (EPRI NP-5613), U.S. Nuclear Regulatory Commission, leden 1989

[2] Mosleh A., *Procedures for Analysis of Common Cause Failures in Probalistic Safety Analysis*, NUREG/CR-5801, duben 1993

[3] Marshall, F., M., Rasmuson, D.,M., Mosleh, A., *Guidelines on Modeling Common Cause Failures in Probalistic Risk Assessment*, NUREG/CR-5485, listopad 1998

Analýza potenciálu pro vznik poruch se společnou příčinou na základě dobře zmapované provozní zkušenosti

RNDr. Jaroslav Holý, oddělení analýz spolehlivosti a rizik, ÚJV Řež a.s.

Úvod

V roce 1998 byl publikován NUREG/CR-5497 "*Common Cause Failure Parameter Estimations*", obsahující velké množství informací o poruchách se společnou příčinou, ke kterým došlo při provozu tlakovodních a varných jaderných reaktorů v USA. Provozní informace je přímo v tomto materiálu transformována do hodnot parametrů umožňujících kvantifikovat základní prvky spolehlivostního modelu reprezentující poruchy se společnou příčinou. Tato práce je prvním zdrojem skutečně obsáhlých generických dat neopírajících se v rozhodující míře pouze o expertní odhad, ale odrážejících provozní zkušenost. Způsob zpracování dat a jeho výsledky lze hodnotit jako vhodný pro začlenění do spolehlivostních modelů průmyslových komponent, systémů a technologií v České republice.

Obecné rysy postupu pro odhad parametrů CCF modelů ze zaznamenaných událostí

Proces odhadu CCF parametrů z událostí zaznamenaných v databázích provozní historie technologie lze popsat následujícími kroky:

1. Předběžná klasifikace událostí z databáze provozní historie. Účelem tohoto kroku je nalézt ty události, jež mají vliv na vyšetřované typy komponent studované technologie a zhodnotit, zda představují jednoduché či násobné poruchy. Při analýze je třeba vyjít z explicitně definovaných hranic všech základních typů komponent ve spolehlivostní studii. Dále se v této etapě prací události přiřadí typ poruchy výběrem z předem definovaného souboru poruchových módů a klíčové ukazatele závažnosti poruchy.
2. Podrobná analýza každé události. V tomto kroku se události analyzují podrobněji. Cílem je maximálně průkazně identifikovat mechanismus, který řídil vznik poruchy. U degradací nebo u počínajícího ohrožení funkce komponenty se hodnotí jejich význam z hlediska kritéria úspěchu pro činnost komponenty užitého ve spolehlivostním modelu. Kromě toho se hledají jevy, jež těsně předcházely poruše, které mohou být indikátorem mechanismu jejího vzniku. Význam událostí se vyjádří pomocí tzv. vektoru následků.
3. Odvození statistik událostí z vektorů následků. Ze souboru vektorů následků se získají souhrnné počty událostí $N_{k,m}$, kdy je právě k komponent z CCF skupiny v poruše a m je stupeň zálohování, přitom $1 \leq k \leq m$.
4. Zjištění dalších slabých míst vyšetřované technologie. V této fázi často může pomoci obhlídka technologie doprovázená diskusí s provozním personálem o způsobu provozu a údržby systémů a o historii provozu. Lze tak získat dodatečné znalosti specifických slabin i silných míst v prevenci a řešení výskytu násobných poruch.
5. Odhad parametrů. Tento krok kombinuje informaci z předchozích dvou kroků. Kromě bodových odhadů se připravují i kvantitativní charakteristiky nejistoty.

Užití vektoru následků při hodnocení provozní zkušenosti zaměřeném na události CCF

Události typu CCF zahrnují jednak úplné, „katastrofické“ poruchy, jednak degradace nebo počínající ohrožení provozuschopnosti komponenty. Důležitou součástí analýzy je posouzení pohotovosti každé ze skupiny komponent, která byla subjektem CCF.

Výsledky podrobného posouzení události se formulují v podobě tzv. *vektoru následků*, kde je hlavní uchovávanou informací počet postižených komponent a v další fázi analýzy rovněž míra postižení každé komponenty. Vektor následků (*impact vektor*) pro CCF skupinu skládající se z m komponent má m+1 složek pokrývajících celý rozsah možných výsledků působení události z pohledu počtu postižených komponent:

$$I = \{I_0, I_1, \ldots\ldots\ldots\ldots, I_m\},$$

kdy jestliže v důsledku výskytu události selže k komponent, je k-tá složka vektoru rovna jedné a ostatní jsou nulové. Například vektor následků I = {0,0,1} reprezentuje systém dvou komponent (m=2), kde obě komponenty selhaly vinou společné příčiny (I_2=1).

Praktické zkušenosti s databázemi i individuálními hlášenkami ukazují, že ve velkém počtu případů nejsou popisy události jasné a není dostatečně přesně znám stav komponent v okamžiku vzniku události, aby bylo možno určit zcela přesně mechanismus poruchy. Proto si klasifikace události, včetně určení vektoru následků, může vynutit formulování několika hypotéz, z nichž každá představuje odlišný výklad události. V těchto případech je každé z hypotéz přiřazena pravděpodobnost W_1, vyjadřující míru důvěry analytika v jednotlivé hypotézy, tj. jejich relativní váhu. V takových případech, kdy nejistota ohledně počtu porušených komponent vede analytika k formulování více hypotéz a k přiřazení jejich pravděpodobností, není výsledkem analýzy už nula–jedničková podoba vektoru následků, ale varianta nazývaná *zprůměrovaný (vážený) vektor následků* (*average impact vector*), jehož k-tá složka I_k má tvar:

$$I = \sum_{i=1}^{N} W_i I_i$$

kde N je počet formulovaných hypotéz, W_i je pravděpodobnost či váha i-té hypotézy a I_i je její vektor následků. I-tá složka ve výsledném zprůměrovaném vektoru následků vlastně vyjadřuje pravděpodobnost, že zaznamenaná událost obsahuje násobnou poruchu právě i komponent.

Navržené pravděpodobnosti hypotéz odráží analytikův úsudek o původní příčině poruchy a způsobech vazby mezi komponentami. Proto jejich hodnoty lze v praxi odvodit pouze s výrazným zastoupením subjektivního úsudku. Je přitom možno navrhnout určitá obecná vodítka, která přiřazení váhy hypotéze usnadní. Jedním takovým vodítkem je, že číselné hodnoty parametrů CCF modelu nejsou příliš citlivé na malé změny v pravděpodobnostech vektoru následků. Jinými slovy, pokud je v databázi přítomna aspoň jedna nesporná CCF, potom rozdíl v hodnotě prvku vektoru následků např. mezi 0.7 a 0.75 není významný. Při vyjadřování svého

názoru na závažnost degradace nebo sílu vzájemné vazby se tak analytik nemusí koncentrovat na jemnosti.

Jestliže například není zcela jisté, zda daná událost znamenala výpadek dvou nebo tří komponent z CCF skupiny o třech komponentách, přičemž výpadek dvou komponent se jeví jako mnohem pravděpodobnější, je možné zformulovat dvě hypotézy:

H_1: vektor následků má tvar $I_1 = (0,0,1,0)$

H_2: vektor následků má tvar $I_2 = (0,0,0,1)$

a po přiřazení pravděpodobnosti 0.9 hypotéze H_1 a pravděpodobnosti 0.1 hypotéze H_2 vytvořit vážený vektor následků I nejlépe odrážející současný stav poznání provozní zkušenosti

$I = 0.9xI_1 + 0.1xI_2 = (0,0,0.9,0.1)$.

Postup lze zobecnit pro větší počet hypotéz a nenulovou pravděpodobnost většího počtu případů než dvou (znamenající ve svém důsledku nenulovou hodnotu více prvků vektoru následků, teoreticky i všech jeho prvků).

Uvedený postup vede k hodnotám prvků vektoru následků, jejichž součet je vždy roven jedné. Při zahrnutí možnosti hypotézy o **nezávislosti** jednotlivých segmentů události, projevujících se navenek jako CCF porucha, je součet prvků vektoru následků obecně větší než jedna. Jestliže například uvažujeme CCF skupinu o dvou komponentách A, B a pracujeme se dvěma primárními hypotézami

H_1: vektor následků má tvar $I_1 = (0,0,1)$ (společná porucha dvou komponent)

H_2: vektor následků má tvar $I_2 = (0,1,0)$ (nezávislé poruchy dvou komponent),

reprezentuje vektor následků druhé hypotézy vlastně dva vektory následků odpovídající hypotézám:

H_{2A}: nezávislá porucha komponenty A s vektorem následků $I_{2A} = (0,1,0)$

H_{2B}: nezávislá porucha komponenty B s vektorem následků $I_{2B} = (0,1,0)$.

Pokud například přiřadíme hypotéze o vzniku skutečné CCF váhu 0.6 a hypotéze o koincidenci nezávislých poruch váhu 0.4, je výsledný vektor následků roven

$I = 0.6xI_1 + 0.4xI_{2A} + 0.4xI_{2B} = (0,0.8,0.6)$.

Podobným způsobem lze zobecnit zformulování několika hypotéz a přiřazení odpovídajících vektorů následků se složkou nezávislé poruchy i pro větší CCF skupiny. Postup je zcela obecný a může být analytikem použit přímo, s výrazným zapojením expertního odhadu při tvorbě hypotéz a váhových koeficientů. Následující odstavce přinášejí některá vodítka pro tvorbu vektorů následků s váženými prvky, která se v praxi osvědčila. Nejčastější případy provozních událostí vyžadující vytvoření několika hypotéz lze rozdělit do tří kategorií:

- události s neúplným vyřazením komponent
- události vznikající na komponentách téže CCF skupiny nikoli současně, ale v relativně krátkém časovém odstupu

- události s násobným výpadkem, kde přítomnost mechanismu spojujícího výpadky do jedné události nelze prokázat s určitostí.

Události s různým stupněm vyřazení komponent CCF skupiny

V tomto případě musí analytik pro každou komponentu z CCF skupiny, která byla postižena CCF událostí, odhadnout míru ztráty její funkce (v podstatě to znamená odhadnout pravděpodobnost, že komponenta selže ve smyslu poruchového módu a mise definované ve spolehlivostním modelu). Pro kvantitativní ocenění míry degradace konkrétní komponenty p po CCF události lze využít následující přibližné schéma:

úplná ztráta funkce	p = 1
vysoce degradovaná funkce	p = 0.5
degradovaná funkce	p = 0.1
potenciální degradace, bez skutečného omezení činnosti komponenty -	p = 0.01
žádné ovlivnění CCF událostí	p = 0.

Výše uvedená stupnice představuje pouze orientační pomůcku pro konzervativní odhad analytika, přitom je vhodné si povšimnout, že stupnice není opticky lineárně symetrická - částečná degradace funkce má již přiřazen o řád nižší koeficient než úplná ztráta, tento fakt je nutné vzít v úvahu při expertním odhadu spojení míry poškození s budoucí funkcí komponenty v havarijním scénáři.

Po přiřazení úrovně degradace jednotlivým komponentám je možné určit prvky vektoru následků dané události F_i. K určení jsou využity výpočetně relativně jednoduché vztahy opírající se o zákony teorie pravděpodobnosti. Vztahy lze k určení prvků vektoru následků užít mechanicky, bez explicitní práce se statistickými hypotézami naznačené v předchozí kapitole. Například pro CCF skupinu se čtyřmi prvky má prvek vektoru následků F_2 při odhadnutých koeficientech míry degradace p_1, p_2, p_3, p_4 hodnotu

$$F_2 = p_1(1-p_2)(1-p_3)(1-p_4) + p_2(1-p_1)(1-p_3)(1-p_4) + p_3(1-p_2)(1-p_1)(1-p_4) + p_4(1-p_2)(1-p_1)(1-p_3)$$

Události s časovým posunem

Ke vzniku výpadku nebo degradace funkce komponent v CCF skupině může dojít nikoli současně, ale v jistém nepříliš velkém časovém odstupu. Klasický přístup k analýze událostí z provozní historie takové události původně považoval za projevy výskytu nezávislých poruch. Výskyt událostí, u kterých byl časový posun tak malý, že se nebylo možné vyhnout přinejmenším diskusi o jejich CCF charakteru, vedl k rozšíření původní definice CCF událostí o tento případ a vytvoření sady pravidel pro jednoduché kvantitativní postižení míry spojení individuálních událostí do rámce CCF události v závislosti na časovém odstupu a způsobu provozování komponenty. V praxi se totiž ukazuje, že stejný časový odstup událostí má pro rozdílné strategie údržby komponenty odlišnou vypovídací schopnost o možném propojení těchto událostí.

Pro transformování časového odstupu na hodnoty ukazatelů vektoru následků je zaveden *koeficient časového odstupu* q. Pravidla pro jeho určení rozlišují následující způsoby provozování a údržby komponenty:

A: **kontinuální provoz** komponenty po požadovanou dobu mise

B_{11}: požadavek k činnosti komponenty **na vyzvání** s předpokladem, že poruchový potenciál vzniká **v období vyčkávání** s latentním efektem, pro komponenty CCF skupiny (v jednotlivých větvích systému), které jsou **testovány společně** (*non-staggered testing strategy*)

B_{12}: jako B_{11}, ale jde o komponenty CCF skupiny, které jsou testovány v časovém posunu takovém, aby testy komponent celé dané CCF skupiny byly **pravidelně rozprostřeny v čase** (*staggered testing*)

B_2: požadavek k činnosti komponenty **na vyzvání**, ale poruchový potenciál vzniká **nárazem na odolnost komponenty** v okamžiku vyzvání k činnosti, způsob testování (ve smyslu rozlišení B_{11} a B_{12}) je irelevantní

a v souvislosti s těmito způsoby provozování pracují se specifickými časovými parametry a parametrem počtu vyzvání

T_m: doba požadované činnosti (mise) komponenty

T_I: doba mezi pravidelnými testy systému pro strategii *non-staggered testing* nebo pravidelnými testy jedné konkrétní větve systému pro strategii *staggered testing*

T_{IS}: doba mezi dvěma po sobě následujícími testy různých větví systému pro strategii *staggered testing*

r: počet vyzvání k činnosti mezi dvěma hodnocenými CCF událostmi

T: doba mezi vznikem hodnocených událostí na stejné CCF skupině.

Jako příklad lze uvést způsob provozování B_{12} (systém vyčkávajících, navzájem se zálohujících komponent, jejichž testy jsou pravidelně rozprostřeny v čase), kdy je pro dvě poruchové události s odstupem mezi vznikem splňujícím nerovnosti

$$T_{IS}/2 < T < T_{IS}$$

doporučená hodnota parametru q rovna **0.7**.

Události s nejistým CCF charakterem

Záznamy o události v databázi specifické informace z provozu elektrárny mohou být neúplné nebo nekvalitní a mohou vést k nejistotě o **samotné existenci společné příčiny** poruch. Tato nejistota je, na rozdíl od předchozích koeficientů odrážejících charakter události, vlastní neurčitostí analytického procesu (míry poznání a schopnosti analytika zpracovávajícího analýzu) a je tedy dalším příspěvkem ke znáhodnění analýzy, tvorbě hypotéz a přesnějšímu vystižení smyslu vektoru následků.

K matematickému popisu nejistoty ohledně společné příčiny se zavádí koeficient c "*míra opravdovosti sdílení společné příčiny*", který se přiřazuje na základě expertního zhodnocení vlastního zpracování dat o události s využitím následující orientační stupnice:

c=1 **velmi vysoká jistota** ohledně sdílení společné příčiny při poruchách

c=0.5 **vysoká jistota** ohledně sdílení společné příčiny při poruchách

c=0.1 **střední jistota** ohledně sdílení společné příčiny při poruchách

c=0.01 **relativně malá jistota** ohledně sdílení společné příčiny při poruchách

c=0 dané události vyhodnoceny jako **bez společné příčiny**.

Z bližšího zdůvodnění zavedení a využití parametru c vyplývá, že způsob ovlivnění vektoru následků tímto parametrem je obdobný jako u parametru q.

Obecný model a vektor následků pro událost se společnou příčinou

Událost provozní historie, která je podrobena analýze CCF, může vykazovat rysy neúplného poškození některých komponent, **současně** může být souborem dílčích událostí s časovým odstupem nevylučujícím působení společné příčiny a **navíc** může být její analýza zatížena inherentní nejistotou analytika ohledně samotné existence CCF příčiny. Odvození vektoru následků má zde několik fází spojených s postupným zahrnováním jednotlivých složek nejistoty. Ve finální části analýzy vektory následků odpovídající postupně hypotéze o CCF události a hypotézám o nezávislých poruchách k zúčastněných komponent nabývají tvar

$\mathbf{I_{CCF}} = [cqF_0, cqF_1,...,cqF_m]$

$\mathbf{I_1} = [(1-c](1-p_1), (1-cq)p_1,0,...,0)$ pro první komponentu, která je potenciálně subjektem násobné poruchy

.....

$\mathbf{I_k} = [(1-c](1-p_k), (1-cq)p_k,0,...,0)$ pro k-tou komponentu (poslední ve skupině m komponent), která je potenciálně subjektem násobné poruchy.

Výsledný vektor následků je získán jako součet vektorů následků I_{CCF} a I_j, j=1,...,k. Tento vektor následků reprezentuje nejuniverzálnější model zahrnutí události s nejistou společnou příčinou do statistiky tvořící podklad pro kvantifikaci CCF parametrů a tvoří přímý podklad pro výpočet parametrů CCF modelu.

Kvalitativní rozbor CCF

Součástí metodiky ocenění CCF potenciálu indikovaného provozní historií je i přiřazení některých kvalitativních atributů dané CCF události, charakterizujících především typ mechanismu, který zapříčinil opakování poruchy u další komponenty CCF skupiny. Následující tabulka je pomůckou pro toto přiřazení, které umožňuje detailněji proniknout do soustav možných příčin CCF a zavést pomocné statistiky, určené nikoli pro přímou kvantifikaci CCF parametrů spolehlivostní studie, ale i pro navržení opatření pro strategii předcházení CCF, která pak ve svém důsledku ovlivní charakter sběru další informace i jeho výsledky, které se již do spolehlivostní studie dané technologie přímočaře promítnou.

Tabulka: Soubor faktorů pro základní kvalitativní analýzu CCF událostí

Kategorie	Faktor
Technologický	Stejný vzhled (zaměnitelnost)
	Stejný design a konfigurace
	Stejné prvky
	Stejný výrobce
	Stejná konstrukce a instalace
Organizační	Stejná obsluha
	Stejné provozní postupy
	Stejné plány údržby
	Stejný personál údržby
	Stejné postupy pro údržbu
Environmentální	Určující (společné) rysy lokality umístění technologie
	Společné umístění komponent v rámci lokality (takové, že se neprojeví variabilní rysy konkrétních bodů v lokalitě technologie)
	Stejné rysy interního prostředí komponenty (přepravované médium, zdrojová a podpůrná média)

Souborné závěry a doporučení užití provozní informace v modelování a kvantifikaci potenciálu pro vznik poruchy se společnou příčinou

Závěry a doporučení vyplývající ze zkušeností s modelováním a kvantifikací CCF v praxi lze rozdělit na vybraná obecná doporučení a doporučení směrovaná na konkrétní aspekty využití provozní zkušenosti. Z obecných doporučení mají vazbu na práci s provozní zkušeností například tato:

- analýza CCF jako součást tvorby a aplikace spolehlivostního modelu technologie je vždy součástí širší úlohy „analýza závislých poruch“
- vždy je nutné v pracovním rámci konkrétní spolehlivostní studie znát předěl mezi příčinami závislých poruch modelovanými explicitně a příčinami ostatními, reprezentovanými souborně událostmi typu „reziduální CCF“
- při modelování CCF musí analytik bezpodmínečně vycházet ze znalosti zpracování **individuálních** poruch v daném spolehlivostním modelu, tj. ze znalostí hranic komponent, zavedených poruchových módů, kritérií úspěchu atd.

Jako konkrétní doporučení k práci s provozní zkušeností lze zformulovat například:

- CCF jsou vzácné události, proto ve většině případů nelze vycházet z údajů pouze pro vyšetřovanou technologii, specifická informace z provozu konkrétní studované technologie pro běžný objem provozní historie umožňuje pouze zpřesňovat odhady založené na generických datech
- v rámci analýzy se nehodnotí pouze případy násobných poruch, ale také individuální poruchy vyšetřované skupiny komponent, z obecného hlediska lze totiž na nezávislou poruchu jedné komponenty pohlížet jako na speciální případ poruchy CCF, kdy je poruchový potenciál u všech komponent CCF skupiny s výjimkou jediné komponenty tak malý, že je možné jej zanedbat
- podobně jako u běžné analýzy dat v rámci každého spolehlivostního modelu (analýzy nezávislých poruch) se nehodnotí pouze úplné (katastrofické/fatální) poruchy, ale analyzují se i případy degradace provozuschopnosti nebo i jen symptomy počínajícího ohrožení funkce komponenty
- u navzájem se zálohujících komponent podléhajících periodickým testům neznamená CCF nutně současně zjištěnou poruchu (porucha u další komponenty se může projevit až při příštím či ještě pozdějším testu)
- „společná příčina“ poruchy několika komponent často není jednoduchá událost, ale dlouhodobý proces spolupůsobení více příčin a negativních okolností
- informace o CCF poruchách bývají neúplné a výklad nejistý, proto se uplatňuje i subjektivní úsudek analytika – dokumentování všech dodatečných předpokladů a přijatých rozhodnutí by mělo být automatickou součástí výstupu analýzy
- u poznatků z událostí vzniklých na jiné technologii stejného nebo podobného druhu, jež lze zpracovávat statisticky obdobně jako vlastní provozní historii, je třeba hodnotit platnost původních závěrů i pro vlastní vyšetřovanou technologii (posoudit přenositelnost události)
- kromě analýzy datových záznamů z provozu je nutno pomocí obhlídky a jiných metod hledat případné specifické slabiny, které v zaznamenaných událostech nemusejí figurovat, protože se neprojevily díky omezenému objemu provozní historie.

Poruchy se společnou příčinou v civilním letectví

Ing. Jiří Sedlák, Oddělení analýz spolehlivosti a rizik, ÚJV Řež a.s.

Analýza společných příčin (CCA)

Ke splnění bezpečnostních požadavků kladených na každý letoun je třeba prošetřit možnou vzájemnou závislost mezi poruchami jednotlivých systémů a prokázat, že tam kde existuje, je pravděpodobnost výskytu závislých poruch se závažnými důsledky zanedbatelná. Analýza společných příčin hledá poruchové stavy nebo externí události, které mohou vést k důsledkům pro letoun klasifikovaným jako Catastrophic, Hazardeous a Major. Události se společnou příčinou s důsledkem Catastrophic musejí být apriori vyloučeny, potenciál pro vznik událostí s důsledkem Hazardeous nebo Major musí splňovat pravděpodobnostní kritéria. Bližší náhled na způsob klasifikace je v uveden v příloze.

Hodnocení poruch se společnou příčinou civilních leteckých prostředků se provádí společně s takzvaným „posouzením bezpečnosti a spolehlivosti systémů“ (System Safety Assessment - SSA). Tyto analýzy se v závislosti na třídě letounu a hodnocené funkci provádějí buď pouze kvalitativně, nebo kvalitativně i kvantitativně. V prezentaci bude uveden diagram s přehledem procesu hodnocení bezpečnosti z předpisu ARP 4761.

Názvosloví používané v letectví je poněkud jiné, než to které se používá při hodnocení spolehlivosti a poruch se společnou příčinou u „pozemních“ technologií (jaderně energetických zařízení). Provádí se analýza společných příčin (Common Cause Analyses – CCA), která sestává ze

- zonální analýzy (Zonal Safety Analysis - ZSA)
- analýzy mimořádných rizik (Particular Risk Analysis – PRA)
- analýzy společných způsobů *selhání* (Common Mode *failure* Analysis - CMA)

Zonální analýza (ZSA)

Cílem zonální analýzy je zmapovat rozmístění přístrojů a ostatní instalace v letounu a popsat možnosti jejich vzájemného negativního působení.

Smyslem analýzy je ujistit se, že instalace zařízení splňuje spolehlivostní požadavky ve smyslu:

- základního standardů projektu a palubní instalace
- vlivu poruchových stavů na letoun
- chyb údržby
- ověření, že projekt splňuje postulovanou vzájemnou nezávislost událostí ve stromech poruch (pokud se konstruují).

Provedení zonální analýzy je založeno na předběžném vytvoření schématu zón, subzón a subsubzón letounu. Poruchové stavy, které svým průběhem ovlivní další přístroje nebo instalaci v dané zóně můžeme rozdělit na stavy, které:

1. poškodí další zařízení hodnoceného systému,
2. poškodí zařízení jiného systému,
3. poruchy jiného systému, které poškodí zařízení hodnoceného systému.

Zonální analýza je v první řadě kvalitativní analýza zahrnující 3 hlavní úkoly:

1. Příprava předpisu pro projekt a instalaci
2. Prověření instalací v zónách (a subzónách)
3. Prověrka vzájemného působení systémů

Pro průkaz splnění požadavků je potřeba vytvořit seznam systémů a prvků v každé zóně letadla a jim odpovídající seznam poruchových módů. Tento seznam může být založen na provedené FME(C)A a na znalostech vnitřních rizik.

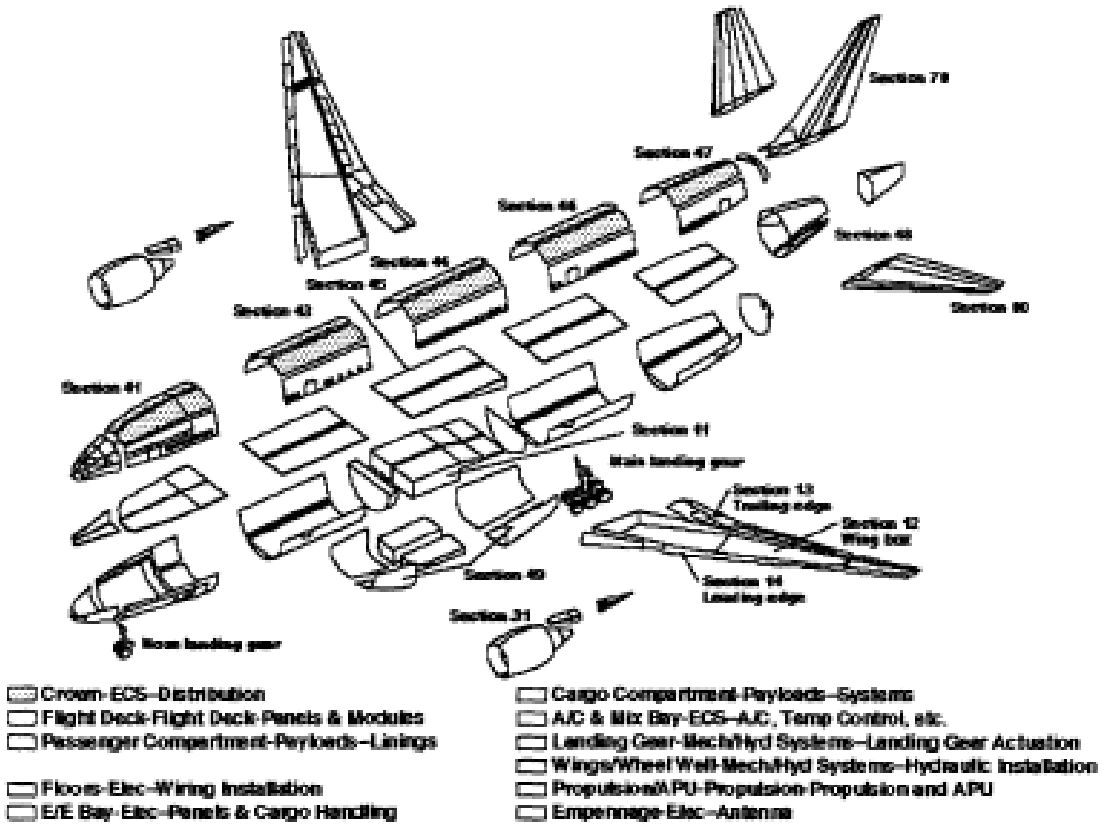

FIGURE I1 - Example of Aircraft Zones

Obrázek 1 Příklad rozdělení letounu na zóny

Analýza mimořádného rizika (PRA)

Mimořádné riziko je definováno jako události nebo vlivy, které jsou mimo hodnocený systém (resp. systémy) a jeho prvky, ale které mohou narušit požadavky na nezávislost poruch. Některá taková rizika musejí být analyzována z důvodů požadavků na letovou způsobilost, zatímco ostatní mohou vycházet ze známých ohrožení mimo systém nebo letoun. Typickými příklady rizik nebo objektů rizika reprezentujících jsou:

- požár
- vysoko-energetická zařízení (motor, nezávislý záložní zdroj - APU, ventilátory)
- tlakové nádoby
- rozvod tlakového vzduchu
- rozvod horkého vzduchu
- únik kapaliny (palivo, hydraulická kapalina, elektrolyt, voda)
- nepřízeň počasí (kroupy, led, sníh)
- srážka s ptákem
- prasknutí pneumatiky, uvolnění běhounu pneumatiky
- vystřelení součástky kola (ráfku)
- úder blesku
- vyzařované pole o vysoké intenzitě
- vyosená hřídel
- proražení přepážky.

Každé zjištěné riziko pro hodnocený projekt by mělo být detailně prozkoumáno z hlediska možnosti vyvolání souběžných nebo kaskádovitě se šířících nežádoucích událostí. Cílem je ověřit, že každý bezpečnostně významný vliv je buď projektem eliminován, nebo je vzniklé riziko přijatelné.

Analýza mimořádného rizika PRA je především kvalitativní nástroj a obsahuje následující kroky:

- detailní definice hodnoceného rizika
- určení modelu pro analýzu (např. model prasknutí pneumatiky)
- seznam požadavků předpisů
- zjištění dotčených zón nebo oblastí
- určení ohrožených systémů a prvků (viz ZSA)
- popis relevantních bezpečnostních opatření v projektu a v palubní instalaci

- určení následků rizika pro ohrožené prvky (viz též FMEA, SSA)
- určení následků rizika pro letoun v důsledku poruchových módů prvků nebo jejich kombinaci (viz SSA)
- zhodnocení přijatelnosti rizika
  - pro přijatelné riziko – zdokumentování průkazu a použití v SSA
  - pro nepřijatelné riziko – změna projektu

Analýza společných způsobů *selhání* (CMA)

Analýza společných způsobů selhání má zajistit, že žádná společná příčina ani kaskádovitě šířená porucha nemůže narušit v architektuře implementovaný bezpečnostní koncept. Rozbor společných způsobů poruch se zabývá závislými poruchami, které mohou ohrozit funkci částí systémů, které se navzájem ve větší či menší míře zálohují.

V podstatě má analýza společných způsobů – CMA za úkol prověřit, že jednotlivé události modelované ve stromech poruch (popřípadě v blokových nebo v Markovských diagramech) v logické vazbě „AND“ jsou navzájem nezávislé. Je tedy třeba analyzovat vliv projekčního provedení, výroby, chyb údržby a poruch prvků systému, které mohou narušit nezávislost těchto událostí. Také je nutné sledovat nezávislost funkcí a jejich monitorování.

Proces analýzy společných způsobů je založen na normě ARP 4761 a sestává z následujících kroků:

vytvoření soupisů (typy, zdroje a poruchy),

zjištění požadavků na analýzu společných způsobů poruchy

analýza projektu a kontrola plnění požadavků

dokumentace CMA procesu

Celý proces analýzy společných způsobů poruchy je orientován na prověření projektu a implementace s cílem nalézt prvky, které mohou oslabit redundanci nebo nezávislost funkcí. Tato analýza se provádí pomocí vyčerpávajícího soupisu (check-listu). Přitom je třeba každé porušení požadované redundance nebo nezávislosti buď vyloučit, nebo zdůvodnit jeho přijatelnost.

Zdrojem společných způsobů poruch mohou být obecně:

- materiálová vada
- výrobní vada
- chyba hardwaru
- chyba v softwaru
- špatná oprava
- mimořádné provozní namáhání

- špatná instalace
- špatné zadání projektu
- vliv prostředí (teplota, vibrace, vlhkost, prašnost apod.)
- kaskádovité poruchy
- společný vnější zdroj poruch.

Pro provedení analýzy společných způsobů poruch CMA je nezbytné se seznámit a pochopit způsob instalace a provozu hodnoceného systému, především s:

- architekturou projektu a způsobem zástavby
- charakteristikou zařízení a komponent
- údržbou a testováním
- předpisy pro posádku
- specifikacemi systémů, zařízení a softwaru.

Navíc musí být analytik seznámen s bezpečnostními opatřeními k eliminaci nebo snížení důsledků společných způsobů poruch, jako jsou

- diverzita, resp. redundance a bariéry
- testování a preventivní údržba
- řízení projektu a jeho kvality
- přehled instrukcí a specifikací
- výcvik obsluhy
- řízení jakosti.

Požadavky vzešlé ze stromů poruch (resp. blokových diagramů nebo Markovské analýzy)

Tyto požadavky mají původ v analýzách, které se provádějí na podporu rozboru funkčních rizik (Functional Hazard Analysis – FHA) nebo PSSA (Preliminary SSA).

Ke každému poruchovému stavu typu „Hazardous“ nebo „Catastrophic“ (FHA/PSSA) jsou zjišťovány kombinace s jinými poruchovými stavy reprezentované v širším modelu souvisejícími logickými operátory typu „AND“ a jsou určeny principy, na kterých je založen předpoklad nezávislosti poruch. Z této analýzy jsou stanoveny požadavky CMA.

Další požadavky CMA

Ne všechny požadavky lze odvodit z analýzy běžných logických schémat uplatňovaných při hodnocení spolehlivosti (stromů poruch, blokových diagramů nebo Markovských analýz) –

některé další mohou pocházet z předdefinovaných soupisů (checklistů) nebo výrobní a provozní zkušenosti. Tyto požadavky vycházejí z porovnání soupisů s projekčními postupy, detaily projektu, vybranými komponentami, způsobem výroby, zástavby a údržbářskými postupy. Každý zjištěný stav, který může přispívat k události se společným způsobem je převeden na požadavek CMA a zdokumentován. Příklady požadavků CMA, které nemusí být zjevné z logiky stromů poruch, jsou speciální poruchové módy komplexních komponent známé z generických seznamů, vlivy okolního prostředí, umístění komponent apod.

Řešení poruch se společnou příčinou

Pro každý z takto zjištěných požadavků CMA je třeba provést následující kroky:

- určit potenciál poruch se společnou příčinou pro každý zdroj
- analyzovat každý potenciál s cílem ověřit splnění kritérií nezávislosti
- v případě nesplnění kritérií iniciovat změnu projektu
- sledování nápravných opatření, ověření přijatelnosti výsledné změny projektu.

Závěr

Analýza poruch se společnou příčinou, resp. společných příčin, je v letectví prováděna poněkud jinak, než je zvykem v pravděpodobnostním hodnocení bezpečnosti jiných technologií. Důraz je kladen především na kvalitativní hodnocení a celý proces analýzy se tak podobá spíše preventivním úkonům a procesům realizovaným například v rámci předprovozní bezpečnostní zprávy jaderné elektrárny (PSAR). Kvantitativní hodnocení není explicitně vyžadováno, ale může být použito jako průkaz přijatelnosti vzniklého rizika.

Seznam použitých zkratek

CCA	analýza společných příčin (Common Cause Analyses)
CMA	analýza společných způsobů (Common Mode Analysis)
FHA	analýza funkčních rizik (Functional Hazards Analysis)
FMEA	analýza způsobů poruch a jejich důsledků (Failure Mode and Effects Analysis)
PFHA	předběžná FHA (preliminary FHA)
PRA	analýza mimořádných rizik (Particular Risk Analysis)
PSA	pravděpodobnostní hodnocení bezpečnosti (Probabilistic Safety Assessment)
PSAR	předprovozní bezpečnostní zpráva (Preliminary Safety Analysis Report)
PSSA	předběžná SSA (preliminary SSA)
SSA	posouzení bezpečnosti a spolehlivosti (System Safety Assessment)
ZSA	zonální analýza (Zonal Safety Analysis)

Seznam literatury

[1] ARP4761, Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE Aerospace Recommended Practice, 1996

[2] Certification and Specifications for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes (CS-23)

[3] ČSN IEC 1025/1990 : Analýza stromu poruchových stavů

[4] ČSN IEC 812/1992 : Metody analýzy spolehlivosti systému. Postup pro analýzu způsobů a důsledků poruch (FMEA)

[5] Equipment, Systems, and Installations in Part 23 Airplanes, Advisory Circular, Federal Aviation Administration (AC No: 23.1309-1C), Federal Aviation Administration, 1999

[6] Federal Aviation Regulations Part 23 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes (FAR Part 23)

[7] Holý, J., Sedlák, J., Analýzy spolehlivosti jako faktoru výrazně ovlivňujícího provozní technologičnost, ÚJV Řež, 2004

Příloha

Klasifikace závažnosti poruchových stavů letounu (výňatek z „Poradního oběžníku 23.1309-1C“ - Výstroj, soustavy a instalace v letounech podle předpisu Part 23)

***Poruchový stav*:** Stav, který má účinek buď na letoun nebo na osoby na palubě nebo na obojí, buď přímo nebo zprostředkovaně, který je způsoben nebo vznikne za přispění jedné nebo více poruch nebo chybami, s uvážením fáze letu a možných souvisících nepříznivých provozních podmínek a podmínek okolního prostředí nebo vnějších událostí. Provozní stavy lze klasifikovat podle jejich závažnosti následovně:

(1)*Bez účinku na bezpečnost*: Poruchové stavy, které by neměly mít žádný vliv na bezpečnost (tj. poruchové stavy, které by neměly ovlivnit provozní možnosti letounu nebo zvýšit pracovní zatížení posádky).

(2)*Nezávažné*: Poruchové stavy, které by neměly významně omezit bezpečnost letounu a ovlivnit činnosti posádky, které jsou zcela v rámci jejich možností. Nezávažné poruchové stavy mohou zahrnovat mírné omezení záloh bezpečnosti nebo funkčních možností, mírné zvýšení pracovního zatížení posádky (takové, jako jsou změny postupů letového plánu) nebo určité fyzické nepohodlí cestujících nebo posádky.

(3)*Závažné*: Poruchové stavy, které by mohly omezit možnosti letounu nebo schopnost posádky vyrovnat se s nepříznivými provozními podmínkami do té míry, že by mohlo dojít k významnému omezení záloh bezpečnosti nebo funkčních možností; významnému zvýšení pracovního zatížení posádky nebo k podmínkám snižujících účinnost posádky; nebo k nepohodlí letové posádky, fyzickému přetížení cestujících nebo kabinového personálu včetně možnosti jeho zranění.

(4)*Nebezpečné*: Poruchové stavy, které by mohly omezit možnosti letounu nebo schopnost posádky vyrovnat se s nepříznivými provozními podmínkami v rozsahu, který by mohl vést k:

(i) velkému omezení záloh bezpečnosti a funkční způsobilosti;

(ii) takovému fyzickému přetížení nebo většímu pracovnímu zatížení letové posádky, že se nelze spolehnout, že za takových podmínek provede příslušné úkony přesně nebo úplně; nebo

(iii) těžkému nebo smrtelnému zranění osoby jiné než letová posádka.

(5)*Katastrofální*: Poruchové stavy, u kterých se předpokládá, že budou mít za následek více případů usmrcení osob na palubě nebo invaliditu nebo těžké zranění letové posádky, obvykle spojené se ztrátou letounu. *Poznámky*: (1) Věta "předpokládá se, že budou mít za následek" neznamená, že je požadována 100 % jistota, že následek bude vždy katastrofální. Právě naopak, protože účinek dané poruchy by mohl být katastrofální za extrémních okolností, nepředpokládá se, že tyto poruchové stavy budou nutně katastrofální. (2) Termín "katastrofální" byl v dřívějších verzích předpisů a poradních materiálů definován jako poruchové stavy, které by mohly zabránit pokračování bezpečného letu a přistání.