**ČESKÁ SPOLEČNOST PRO JAKOST**

**Novotného lávka 5, 116 68 Praha 1**

**35. SETKÁNÍ**
**ODBORNÉ SKUPINY PRO SPOLEHLIVOST**

pořádané výborem Odborné skupiny pro spolehlivost
k problematice

# Analýzy spolehlivosti a bezpečnosti v praxi

## (aneb jak přesvědčit zákazníka, že požadavky na spolehlivost a bezpečnost výrobku budou splněny)


**Materiály z 35. setkání**
**odborné skupiny pro spolehlivost**

Brno, červen 2009

# OBSAH:

# ZÁKLADNÍ FILOZOFIE PRŮKAZU SPOLEHLIVOSTI A BEZPEČNOSTI TECHNICKÉHO SYSTÉMU V POČÁTEČNÍCH ETAPÁCH ŽIVOTNÍHO CYKLU.

***prof. Ing. Zdeněk VINTR, CSc.***

*Univerzita obrany, Kounicova 65, 662 10 Brno, zdenek.vintr@unob.cz*

## 1. Úvod

Tento příspěvek je součástí širšího souboru příspěvků, které si kladou za cíl prezentovat možnosti využití prediktivních analýz spolehlivosti a bezpečnosti při hodnocení spolehlivosti a bezpečnosti technických systémů v předvýrobních etapách. Důraz je přitom položen na praktickou demonstraci využití prediktivních analýz, jako nástroje pro prokázání splnění požadavků na spolehlivost a bezpečnost systému. Konkrétní příklad aplikace prediktivních analýz k tomuto účelu je ukázán na příkladu brzdové soustavy dopravního letounu.

Požadavky na spolehlivost a bezpečnost se v současnosti stávají neoddělitelnou součástí technických požadavků kladených na moderní technické systémy a je jen obtížně představitelné, že by proces vývoje a návrhu nějakého moderního technického systému mohl být úspěšný bez toho, aby vycházel z jasně definovaných požadavků na spolehlivost a bezpečnost. Tyto požadavky obvykle formuluje budoucí uživatel systémů (v případě vývoje systému určeného konkrétnímu uživateli) nebo případně sám výrobce (u systémů určených pro hromadnou či sériovou výrobu, které nejsou vyvíjeny pro konkrétního uživatele). V případě systémů, jejichž poruchy mohou vést k ohrožení zdraví a životů lidí, velkým materiálním škodám či poškození životního prostředí, jsou často požadavky na spolehlivost a bezpečnost stanoveny závaznými předpisy (zákony, vyhlášky, směrnice, standardy …).

Běžnou praxí dnes je také požadavek na to, aby požadovaná úroveň spolehlivosti a bezpečnosti systému byla prokázána ještě předtím, než se přistoupí k vlastní výrobě systému, či jeho prototypu. Tento požadavek vyplývá ze zkušenosti, že každá vynucená změna v konstrukci systému se během předvýrobních etap realizuje podstatně jednodušeji a s výrazně menšími náklady než v etapách pozdějších. Velmi často se tak v praxi můžeme setkat s tím, že u systémů vyvíjených na zakázku, zákazník požaduje, aby mu již v počátečních etapách životního cyklu systému byl předložen důkaz o tom, že vyvíjený systém bude splňovat jeho požadavky na spolehlivost a bezpečnost. Běžně je přitom akceptováno, že jako tento důkaz jsou využity právě výsledky prediktivních analýz spolehlivosti a bezpečnosti.

## 2. Prediktivní analýzy spolehlivosti a bezpečnosti

Prediktivní analýzy spolehlivosti a bezpečnosti se používají k přezkoumání a předpovědi ukazatelů bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti systému. Analýzy spolehlivosti a bezpečnosti se provádí zejména v etapě volby koncepce a stanovení požadavků a v etapě návrhu a vývoje a to především pro posouzení zda byly splněny specifikované požadavky.

Analýza spolehlivosti a bezpečnosti systému je proces, jehož podstatou je získávání, zkoumání a uspořádání informací specifických a významných pro daný systém a potřebných pro rozhodování o něm a o stanovených cílech. Zkoumání probíhá obvykle na modelu systému. Konečným produktem tohoto procesu je soubor informací o vlastnostech modelu systému. V souladu s touto definicí je primárním cílem analýzy systému získávání informací o něm. Analýza musí být provedena podle jasně stanovených pravidel a postupů tak, aby proces analýzy byl opakovatelný a vždy vedl ke stejným výsledkům (dvě nezávisle provedené analýzy jednoho systémů nemůžou dospět ke vzájemně rozporným výsledkům).

Jestliže pak nastane okamžik, kdy je třeba na základě provedené analýzy učinit rozhodnutí, pak obvykle bez ohledu na rozsah prací, které byly vykonány, ještě nemusí být k dispozici všechny úplné a

vyčerpávající informace o úrovni spolehlivosti a bezpečnosti daného systému. V takovém případě výsledky analýzy i přijatá rozhodnutí nesou v sobě určitá rizika nejistoty. Tato rizika musí být pečlivě uvážena, musí být známá a odhadnutelná. Minimalizovat tato rizika znamená zaměřit se od samého začátku analýzy na hlavní charakteristiky systému, přičemž všechny významné charakteristiky musí být uváženy. Nejistoty ve výsledcích analýzy a přijatých rozhodnutích mohou vznikat v principu ze dvou důvodů:

- *z vnějších a vnitřních omezení* - tato omezení mají povahu fyzikální, geografickou, omezení funkcí systému, interference systému s jinými systémy (nižších nebo vyšších řádů), interference s lidským faktorem, s vnějším prostředím a pod.
- *z požadované hloubky analýzy* - je nezbytné hned na začátku specifikovat má-li být analýza provedena do hloubky subsystémů, hlavních agregátů nebo až do úrovně elementárních prvků, protože tyto požadavky limitují i případné nepřesnosti v řešení a závěrech analýzy.

Přirozeně že všechna tato omezení a nejistoty mohou být postupně během řešení redukována v důsledku nových nebo zpřesněných informací týkajících se použitých postupů, dílčích výsledků a cílů analýzy.

V první fázi je tedy výsledkem procesu analýzy *první model* systému. Dále se proces analýzy podle potřeby a požadavků několikrát opakuje a novými informacemi zpřesňuje. Po takových úpravách, studiích a revizích vzniká *finální model* systému.

Každý model systémů vytvořený pro potřeby analýzy spolehlivosti musí logicky popisovat funkčnost systému a elementy modelu musí představovat zcela konkrétní jevy, které v tomto případě mají zpravidla povahu náhodných jevů.

Model spolehlivosti by měl tedy postihnout podmínky pro požadovanou funkci, případně podmínky vzniku poruchy a to jak jeho jednotlivých prvků, tak v kombinaci poruch prvků selhání funkce celého systému. Model by také měl umožnit výpočet charakteristik spolehlivosti v podobě konkrétních ukazatelů.

Existují dva rozdílné metodologické postupy při provádění analýzy spolehlivosti a bezpečnosti systému: induktivní a deduktivní.

- *Induktivní postup:* je založen na provádění analýzy od specifických a elementárních problémů k obecnějším a globálnějším problémům. Od analýzy funkcí a poruch prvků (a jejich kombinací) na nejnižší úrovni členění systému se postupuje k analýze poruch a jejich důsledků na nadřazené systémy až k poruchám celého systému. Tento postup se uplatňuje například v metodě FMEA, kde se posuzují důsledky poruch prvků na funkci nadřazených systémů. Při zkoumání důsledků poruch se tedy uplatňuje induktivní postup.
- *Deduktivní postup:* je založen na provádění analýzy od globálních (obecných) problémů k problémům elementárním. Od analýzy poruch systému na nejvyšší úrovni členění se postupuje k analýze jejich příčin a podílu poruch elementárních prvků na těchto poruchách. Při zkoumání příčin vzniku poruch se tedy uplatňuje deduktivní postup. Tento postup se uplatňuje například v metodě stromu poruch.

Tak jak se vyvíjela spolehlivost jako vědní obor, rozvíjely se i metody analýzy spolehlivosti. Dnes jsou nejvýznamnější metody analýzy spolehlivosti již standardizovány a návody k jejich použití jsou k dispozici ve formě národních, mezinárodní či vojenských norem. V současné praxi se při provádění analýz spolehlivosti a bezpečnosti můžeme setkat zejména s následujícími metodami:

- Předběžná analýza nebezpečí (Preliminary Hazard Analysis – PHA) [4],
- Studie nebezpečí a provozuschopnosti (Hazard and Operability Studies – HAZOP Studies) [3],
- Operating and Support Hazard Analysis – O&SHA [4],
- Analýza způsobů a důsledků poruch (Falilure Mode and Effect Analysis – FMEA) [6],
- Analýza způsobů, důsledků a kritičnosti poruch (Failure Mode, Effect and Criticality Analysis - FMECA) [6],
- Analýza stromu poruchových stavů (Fault Tree Analysis – FTA) [7],

- Analýza stromu událostí (Event Tree Analysis – ETA),
- Analýza blokového diagramu bezporuchovosti (Reliability Block Diagram – RBD) [8],
- Markovovy metody [9],
- a další.

Charakteristiky základních metod analýzy spolehlivosti a možnosti jejich využití jsou uvedeny v normě ČSN IEC 60300-3-1 [5]. Nejužívanější z těchto metod jsou popsány a vysvětleny v následujících příspěvcích.

## 3. Hlavní kroky prediktivní analýzy

V principu existují čtyři hlavní kroky (etapy) při provádění prediktivní analýzy spolehlivosti a bezpečnosti to:

- Funkční a technická analýza.
- Kvalitativní analýza.
- Kvantitativní analýza.
- Syntéza výsledků analýzy.

Vzájemná návaznost těchto etap a přehled základních úkolů, které jsou v rámci každé etapy realizovány, je znázorněn na *Obr. 1*.

Funkční a technická analýza

V této etapě jsou shromažďována první data o systému a jeho účelu, cílových vlastnostech, funkčních a technických charakteristikách. Jde o data a informace nezbytné pro definování systému a jeho vlastností. Především je nutné shromáždit co nejpodrobnější informace o jeho prvcích, z nichž je systém vytvořen.

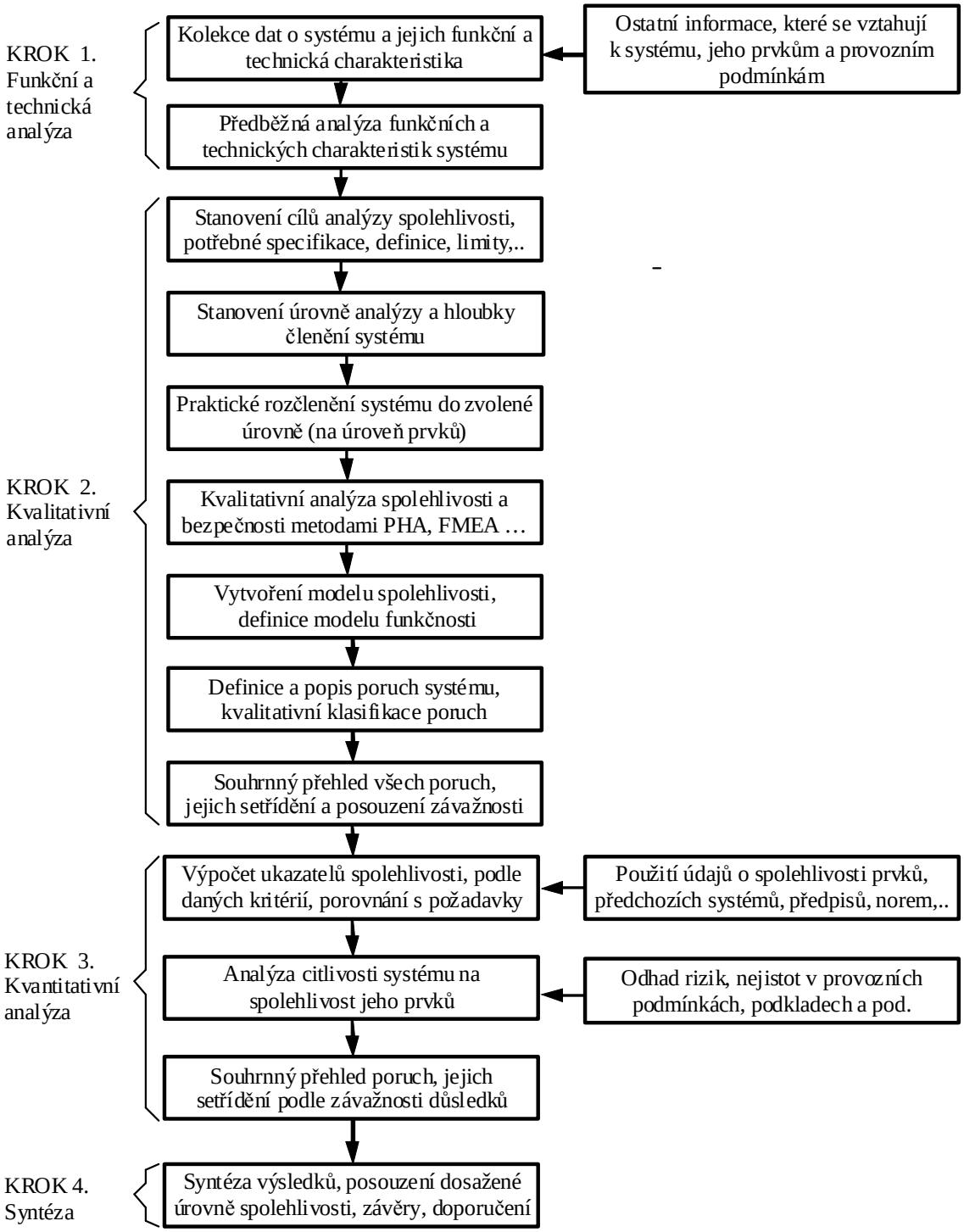
Je provedena první (předběžná) funkční analýza, která by měla vyústit v podrobnější identifikaci a definování hlavních funkcí systému. Je to významné i pro definování všech významných vnějších omezení funkčních vlastností a provozních podmínek. Je to předběžná (první) etapa kvalitativní analýzy, která pomáhá zkompletovat údaje, potřebné v dalších etapách analýzy, především pomůže identifikovat všechny funkce a jejich omezení.

Kvalitativní analýza

Konečným cílem kvalitativní analýzy je vyhledat všechny poruchy, jejich příčiny a popsat důsledky, které poruchy mohou mít a specifikovat jejich vliv na funkci systému. Existuje velký počet formálních postupů provedení analýzy a je na analytikovi aby k danému účelu zvolil nejlepší s ohledem na podklady, které má k dispozici a na cíle analýzy. Kvalitativní analýza poslouží především k vybudování odpovídajícího modelu spolehlivosti systému. Model musí vycházet ze strukturního členění systému a z řady předpokladů, přijatých pro řešení, např. k jaké konfiguraci systému nebo jeho provozní fázi se model vztahuje, které poruchy jsou *a priori* považovány za závažné, případně které faktory významně ovlivňují vznik těchto poruch.

Přirozeně že modelování spolehlivosti systému je těsně svázáno s modelováním fyzikálních jevů a procesů (degradačních procesů), které mohou vyústit v určité fázi provozu až do poruchového stavu.

Obecně řečeno, analytik je nucen postavit a analýzou ověřit řadu hypotéz a předpokladů o správné nebo poruchové funkci vztahujících se k analyzovanému systému. Jde o případy, kdy je např. analyzován vliv různých provozních podmínek, variant údržbových postupů, chování obsluhy v normálních nebo mezních situacích apod. na spolehlivou funkci systému nebo na podmínky vzniku předpokládané poruchy. Je potřeba zdůraznit, že kvalita provedené analýzy je přímo závislá na použitém modelu funkčnosti, který musí postihovat co nejpřesněji všechny významné poruchy a jejich vzájemné souvislosti.




**Obr. 1 Prediktivní analýza spolehlivosti a bezpečnosti systému**

Od samého začátku kvalitativní analýzy musí být jasně definovány její cíle**.** Je třeba zjistit, zda byla zpracována studie, obsahující koncepci spolehlivosti, stanovení požadavků na spolehlivost se zvláštním důrazem na požadavky bezporuchovosti, životnosti, udržovatelnosti, pohotovosti, bezpečnosti případně dalších ukazatelů.

Další důležitou součástí kvalitativní analýzy je stanovení rozsahu, zaměření a hloubky analýzy. Do jaké hloubky funkčního členění bude (nebo může být) analýza provedena. O tom rozhoduje obvykle hloubka a rozsah informací, které jsou o systému a jeho prvcích k dispozici a také úroveň rozpracovanosti systému. V souladu s požadavkem na hloubku analýzy musí být provedeno i

strukturní rozčlenění systému na prvky. I když hloubka členění je libovolná není účelné ji provést do větší hloubky, než do jaké jsou k dispozici konkrétní informace o spolehlivosti prvků systému, zejména o možných poruchách, jejich příčinách a důsledcích.

Označení *prvek sytému* je třeba chápat z praktického hlediska jako takovou část systému, pro kterou může být provedena analýza a pro kterou mohou být specifikovány projevy poruch, jejich příčiny, důsledky a pro kterou jsou k dispozici číselné údaje o poruchách. Ne vždy ovšem je nutné dělat analýzu spolehlivosti až do co nejnižší úrovně členění.

Kvantitativní analýza

V rámci kvantitativní analýzy se provádí výpočet (odhad) kvantitativní (číselné) hodnoty vhodně vybraných ukazatelů spolehlivosti v pojmech např.: *pravděpodobnosti vzniku poruchy***,** nebo *stupně závažnosti poruchy***,** nebo jiného ukazatele. Číselnou hodnotu pravděpodobnosti lze získat vhodnou a dovolenou manipulací s modelem a uvážením elementárních jevů, které model strukturovaně spojuje v analyzovaný (nežádoucí) poruchový stav systému.

Vzhledem k tomu, že samotný model a všechny jeho charakteristiky mají ze své podstaty stochastickou povahu, řídí se stochastickými zákony a jsou proto zatíženy určitou „nejistotou“ ve svých vlastnostech, bude i výsledek analýzy zatížen jistým rizikem nejistoty v závěrech a doporučeních. Míru tohoto rizika je možné snižovat, nelze ho však zcela odstranit. Nejistoty jsou např. spojeny s posouzením důsledků poruch prvků na závažnost poruchy systému, s odhadem pravděpodobností vzniku poruchy prvků, s posouzením vlivu změny provozních podmínek na vznik poruchy apod. Tyto nejistoty můžeme posoudit a do jisté míry zmenšit analýzou *citlivosti* systému na uvedené náhodné vlivy.

Kvantitativní analýzy je možné obecně provádět „ručně“ pokud jsou systémy jednoduché a ne příliš rozsáhlé, jinak se provádí pomocí výpočetní techniky a speciálních, k tomu účelu vypracovaných programů.

## 4. Hlavní charakteristiky prediktivní analýzy

Prediktivní analýza spolehlivosti a bezpečnosti se z obecného hlediska vyznačuje dvěma hlavními a významnými charakteristikami – interaktivností a iterativností.

Interaktivní povaha analýzy

Pro snadnější pochopení podstaty a cílů analýzy spolehlivosti byl postup jejího provádění rozdělen do čtyř samostatných a relativně nezávislých kroků. Ve skutečnosti ovšem toto dělení a nezávislost kroků nemá ostré hranice. Pro každý reálný systém, který má být definován, vyvinut a vyroben mají jednotlivé etapy, jimiž jeho vznik prochází v prováděných činnostech vzájemné průniky. Problém přibližují následující příklady:

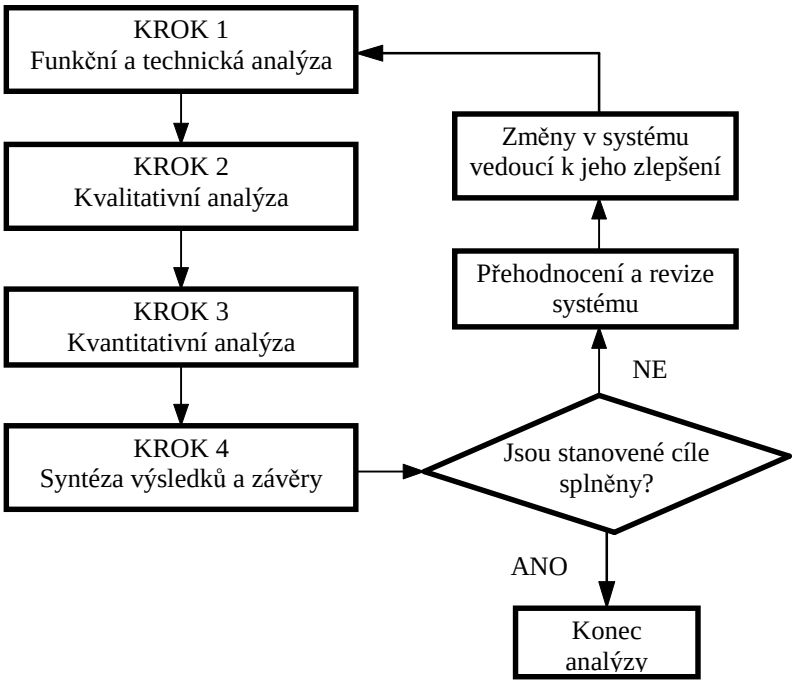
Výběr a definice prvků, provedený v průběhu počátečního dělení systému by měl vycházet ze skutečně existujících a dostupných informací o jejich spolehlivosti. Nebylo by rozumné ani užitečné provést nejdříve dělení systému na prvky bez znalosti těchto informací a dodatečně je zjišťovat. V takovém případě existuje riziko, že potřebné údaje nebudou pro všechny prvky k dispozici. Rozumnější je nejdříve se přesvědčit o dostupnosti údajů a tomu potom přizpůsobit hloubku a rozsah dělení systému.

Hloubka dělení systému, rozsah proveditelnosti analýzy, použité metody analýzy to vše závisí na prostředcích a informacích, které jsou pro analýzu k dispozici. Častěji je nutné počítat s tím, že budou použitelné jen omezené prostředky. Jestliže je dělení systému provedeno do příliš velké hloubky (příliš detailně) a zvolené metody analýzy složité a těžkopádné, analytik se může dostat do časové tísně z nadměrného rozsahu práce a může být ohrožen konečný termín ukončení analýzy.

Kvalitativní modelování, které je implicitní součástí analýzy má v sobě i kvantitativní aspekty. Identifikace a definice možných poruch, jejich projevů, důsledků a rizika jejich vzniku mají vždy stochastickou povahu a nesou v sobě i jistou chybu v odhadu. Proto vždy můžeme v analýze pouze předpokládat vznik poruch a jejich důsledků a to obvykle na základě zkušeností získaných empiricky z provozu stejných nebo příbuzných systémů. Tyto zkušenosti potom přenášíme do očekávaného

chování nového systému. Přitom je třeba uvážit i takové způsoby poruch případně též jejich kombinací, které jsou pouze předpověditelné, to jest i takových, které se dosud ještě nevyskytly a s nimiž nejsou žádné praktické zkušenosti. U nich potom nemáme k dispozici žádné ověřené kvantitativní informace o pravděpodobnosti jejich vzniku, musíme je odhadovat a tím do analýzy vnášíme další nejistoty stochastické povahy. Tyto nejistoty je možné případně korigovat teprve mnohem později až na základě skutečného provozu. Takže kvalitativní a kvantitativní aspekty analýzy jsou vzájemně úzce spojeny a podmíněny.

Závěry z kvalitativní a kvantitativní analýzy mohou objasnit řadu aspektů spojených se spolehlivostí systému a zpětně mohou korigovat i původní členění systému na prvky, jejich výběr, jejich spolehlivostní vlastnosti a ovlivnit i použitý model spolehlivosti systému.




**Obr. 2 Iterativní povaha analýzy spolehlivosti**

Iterativní povaha analýzy

Ze své povahy má analýza spolehlivosti iterativní charakter. Je integrální součástí všech vývojových prací na systému, přináší náměty a návrhy na změny systému, které jsou důsledkem odhalených nedostatků. První závěry z analýzy vedou ke změnám v systému a ke zvýšení jeho spolehlivosti. Vliv těchto změn a modifikací vyvolává potřebu opakování (aktualizaci) analýzy až do té doby, dokud nejsou splněny na začátku projekčních prací stanovené cíle. Iterativní aspekty, obsažené v analýze spolehlivosti ukazuje *Obr. 2.*

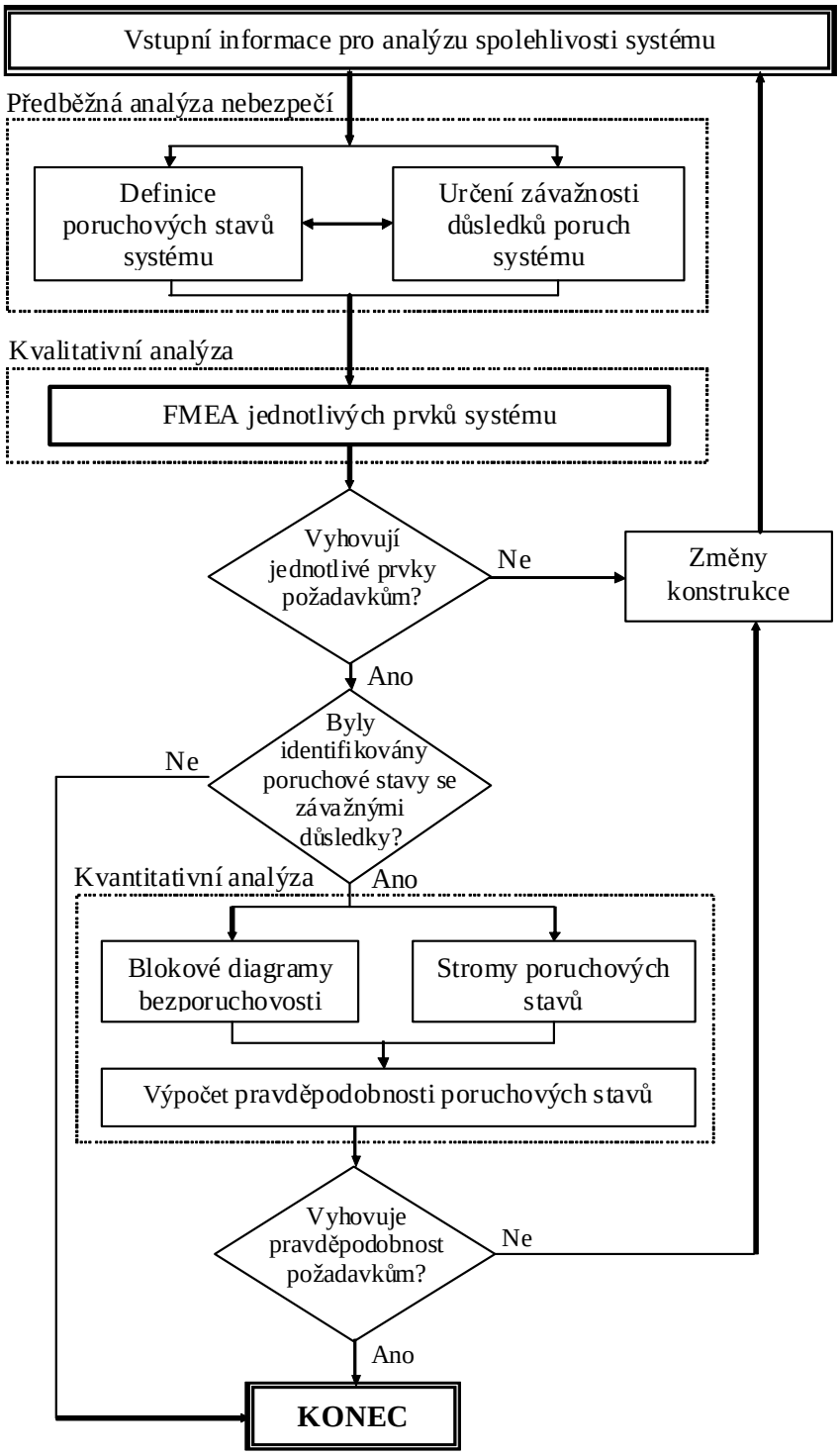
## 5. Průkaz spolehlivosti a bezpečnosti systémů

Jak již bylo uvedeno, prediktivní analýzy spolehlivosti a bezpečnosti mohou být využity pro celou řadu účelů. Dále bude podrobněji popsáno jejich využití, jako nástroje k průkazu splnění požadavků na spolehlivost a bezpečnost systému.

Celý postup analýzy je vhodné uspořádat do logicky navazujících kroků, které zajistí splnění požadovaných cílů analýzy. Platné normy pro spolehlivost nespecifikují jaké metody a postupy mají být při analýze použity a případ od případu se způsob provádění analýzy může lišit. Uvedený obecný postup je však široce aplikovatelný a běžně využívaný v celé řadě odvětví (letectví, železniční doprava, energetika …).

Prvním krokem postupu je provedení tzv. *hodnocení funkční nebezpečnosti* systému. Jedná se zpravidla o aplikaci předběžné analýzy nebezpečí (Preliminary Hazard Analysis), jejímž cílem je

určení a klasifikace nebezpečných poruchových stavů systému. V rámci této části analýzy by měly být identifikovány všechny poruchové stavy, které mohou vést k ohrožení zdraví a životů lidí, vzniku velkých materiálních škod nebo poškození životního prostředí, (poruchy se závažnými důsledky). Vychází se přitom z analýzy funkcí systému a posouzení důsledků selhání těchto funkcí. Výsledky této analýzy vždy mají předběžný charakter a je třeba je doplňovat a verifikovat na základě výsledků dalších kroků analýzy.




**Obr. 3 Průkaz spolehlivosti a bezpečnosti systému**

Na hodnocení funkční nebezpečnosti navazuje kvalitativní analýza spolehlivosti prvků soustavy, kde se posuzuje, zda jednotlivé prvky soustavy splňují příslušné požadavky. K realizaci tohoto kroku se obvykle využívá metoda *FMEA (FMECA)*. Ta umožňuje identifikaci všech způsobů poruch jednotlivých prvků a posouzení jejich důsledků na celý systém.

Dalším krokem postupu je potom kvantitativní analýza. Při ní se vychází z výsledků kvalitativní analýzy a s využitím takových metod, jako jsou *metoda analýzy stromu poruchových stavů* nebo *metoda blokového diagramu bezporuchovosti* se určí pravděpodobnosti všech poruchových stavů systému se závažnými důsledky a posoudí se zda tyto číselné hodnoty splňují příslušné požadavky.

Analýza každé systému může dospět k jednomu z následujících závěrů:

- systém splňuje všechny požadavky na spolehlivost a bezpečnost – potom se výsledky analýzy můžou předložit jako průkaz splnění příslušných požadavků;
- systém nesplňuje požadavky – potom se na základě výsledků analýzy navrhnou příslušné konstrukční úpravy k odstranění zjištěných nedostatků (po realizaci změn je třeba celý postup analýzy opakovat).

Logický postup analýzy a vzájemná návaznost jednotlivých kroků je zřejmá z vývojového diagramu na *Obr. 3.*

## 6. Závěr

Jednotlivé kroky průkazu spolehlivosti a bezpečnosti systému s využitím prediktivních analýz jsou podrobněji popsány v následujících příspěvcích a praktická aplikace jednotlivých metod je demonstrována na příkladu vybraného technického systému – brzdové soustavě dopravního letounu.

Prezentovaný postup průkazu byl autorským kolektivem opakovaně úspěšně použit u cele řady technických systémů např. u systémů letadlové techniky, kolejových vozidel, energetických zařízení a zbraňových systémů.

## Použitá literatura:


[1] MIL-STD-882D *Standard Practice for System Safety*. Washington D.C.: Department of Defence, 2000.

[2] ČSN IEC 300-3-9 *Management spolehlivosti. Část 3: Návod k použití. Oddíl 9: Analýza rizika technologických systémů*. Praha: Český normalizační institut, 1997.

[3] ČSN IEC 61882 *Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití.* Praha: Český normalizační institut, 2002.

[4] MIL-HDBK 764 *System Safety Engineering Design Guide for Army Material.* Washington : Department of Defence, 1990.

[5] ČSN IEC 60300-3-1 *Management spolehlivosti - Část 3-1: Pokyn k použití – Techniky analýzy spolehlivosti – Metodický pokyn.* Praha: Český normalizační institut, 2003.

[6] ČSN EN 60812 *Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA).* Praha: Český normalizační institut, 2007.

[7] ČSN EN 61025 *Analýza stromu poruchových stavů (FTA).* Praha: Český normalizační institut, 2007.

[8] ČSN EN 61078 *Techniky analýzy spolehlivosti – Blokový diagram bezporuchovosti a booleovské metody*. Praha: Český normalizační institut, 2007.

[9] ČSN EN 61165 *Použití Markovových technik*. Praha: Český normalizační institut, 2007.

# PŘEBĚŽNÁ ANALÝZA NEBEZPEČÍ (PHA) – ZÁKLAD RACIONÁLNÍHO NÁVRHU SYSTÉMU

***Ing. David VALIŠ, PhD.***

*Univerzita obrany, Kounicova 65, 662 10 Brno, david.valis@unob.cz*

## Úvod

Účelem této části je popsat základní principy a postupy při provádění předběžné analýzy nebezpečí (dále jen „PHA“ – z angličtiny: Preliminary Hazard Analysis). PHA je strukturovaná a systematická technika využívaná v rámci managementu spolehlivosti a bezpečnosti/rizika sestavená za účelem zkoumání stanoveného systému s následujícími cíly:

- rozpoznat potenciální nebezpečí v systému, přičemž dotyčná nebezpečí mohou zahrnovat jak nebezpečí, která se v zásadě vztahují pouze k bezprostřednímu okolí systému, tak nebezpečí s mnohem širší sférou vlivu, například některá nebezpečí pro životní prostředí,
- rozpoznat potenciální problémy s provozuschopností systému a zejména rozpoznat příčiny narušení provozu a výrobních odchylek, které pravděpodobně povedou k neshodným produktům.

Proces managementu spolehlivosti a bezpečnosti/rizika obsahuje mnoho různých prvků od počáteční identifikace zdrojů nebezpečí, specifikaci systému analýzy spolehlivosti, vlastní analýzy spolehlivosti a bezpečnosti/rizika až po vyhodnocení spolehlivosti a stanovení přijatelnosti rizika včetně identifikaci variant pro snížení potenciálního rizika pomocí volby, realizace a monitorování vhodných řídících opatření a opatření na snížení rizika.

Předběžná analýza nebezpečí, která je předmětem tohoto oddílu, je strukturovaný proces, který identifikuje jak pravděpodobnost, tak rozsah nepříznivých následků pocházejících z dané činnosti, zařízení nebo systému. V kontextu této části se nepříznivé následky týkají poškození zdraví lidí, majetku nebo životního prostředí.

Předběžná analýza nebezpečí (rizika) se stejně jako další metody pokouší při analýze systému/subsystému/soustavy odpovědět na několik základních otázek, mezi něž řadíme tyto následující základní:

| | |
|---|---|
| Co se může porouchat/pokazit? | (Pomocí identifikace nebezpečí); |
| S jakou pravděpodobností taková událost může stát? | (Pomocí analýzy četností); |
| Jaké budou následky takové události? | (Pomocí analýzy následků). |

Tato metoda odráží aktuální osvědčené praktické postupy volby a využití technik analýzy nebezpečí a rizika a neodkazuje se na nové nebo právě vyvíjené koncepce, u kterých nebylo dosaženo uspokojivé úrovně profesionální shody v názorech.

Prezentovaná metoda je ve své podstatě obecná - generická, takže může sloužit jako návod pro mnoho průmyslových aplikací a může být použita u různých typů systémů. V průmyslových odvětvích může totiž existovat mnoho specifických případů systémů, ve kterých se zavádějí některé přednostní metody a úrovně analýzy, které jsou specifické pro určité aplikace.

Metoda PHA pokrývá pouze určitou úzkou část širších činností při posuzování nebezpečí a rizika v rámci managementu spolehlivosti a bezpečnosti/rizika.

Důležitý přínos předběžné analýzy nebezpečí (PHA) spočívá v tom, že výsledné znalosti získané při strukturovaném a systematickém rozpoznávání potenciálních problémů týkajících se nebezpečí plynoucího z funkce systému velmi pomáhají při určování vhodných opatření k nápravě a jsou podkladem pro další navazující analýzy.

Charakteristickým rysem metody PHA je používání „pracovních formulářů“, pomocí kterých se výsledky analýzy zaznamenávají do přehledné formy. Tato technika pomáhá systematicky podněcovat představivost analytika, aby rozpoznal problémy týkající se potenciálního nebezpečí. Vhodnou formou

provedení celé analýzy je metoda tzv. „brain stormingu“ – pracovní/plodné/dynamické porady, kde je přítomen větší počet osob odborně zaangažovaných do analyzovaného projektu. Tímto způsobem je docílena větší provázanost výsledků analýzy s komplexním pojetím systému.

Na metodu PHA by se mělo pohlížet jako na iniciační metodu, která má za úkol zdokonalit (dobrý) projekt s použitím přístupů založených na zkušenostech, jako jsou praktické pokyny. Neměla by být v žádném případě vnímána jako náhrada nutných a potřebných přístupů. Jelikož je to metoda velmi důležitá, zaujímá významné místo mezi ostatními metodami užívanými v rámci procesů managementu spolehlivosti, bezpečnosti a rizika (např. RAMS).

Existuje mnoho různých nástrojů a technik, které jsou dostupné pro rozpoznávání potenciálních problémů týkajících se nebezpečí/rizika, např. od kontrolních seznamů, analýzy druhů poruchových stavů, jejich důsledků a kritičnosti (FMEA/FMECA), analýzy stromu poruchových stavů (FTA) až po OSHA nebo HAZOP. Některé techniky, jako jsou kontrolní seznamy a analýza typu „co se stane, když“, se mohou použít v počátečních etapách životního cyklu systému, kdy je k dispozici málo informací, nebo v pozdějších etapách, jestliže je zapotřebí méně podrobná analýza. Při analýze PHA se ale požaduje více podrobností o uvažovaném systému, ale získávají se při nich obsáhlejší informace o nebezpečích a chybách v projektu systému.

Zkratka PHA bývá často v obecném smyslu spojována s některými jinými technikami rozpoznávání nebezpečí (jako je např. HAZOP kontrolního seznamu, obecná HAZOP nebo HAZOP založený na znalostech, atd.). Použití tohoto termínu s takovými technikami se nepovažuje za příliš šťastné.

Metoda PHA by měla být jednou z počátečních analýz v rámci etapy návrhu a vývoje objektu. Jak již je zřejmé z názvu jedná se skutečně o jednu z prvních metod analýzy systému nebo konceptu systému. Metoda slouží především k identifikaci nebezpečí různých návrhových konceptů systému, jež jsou navrženy a posuzovány pro uspokojení požadovaných potřeb. Za využití nejkvalitnějších a nejdostupnějších informací o systému jsou posuzovány různé varianty konceptu systému, přičemž je hledána závažnost nebezpečí, pravděpodobnost nebezpečí a omezení funkce. Výsledky PHA jsou dále využity pro vyhodnocení různých konceptů a návrhů systému. PHA slouží dále ke stanovení a vymezení konceptu a rámce pro související analýzy nebezpečí a následující analýzy. Jelikož jsou informace z analýzy využity pro vylepšení posuzovaného systému, také analýza PHA musí být následně aktualizována.

Před zahájením předběžné analýzy PHA se má potvrdit, že to je pro daný úkol nejvhodnější technika (ať již se používá samostatně nebo v kombinaci s jinými technikami). Při tomto posuzování vhodnosti se má brát v úvahu účel analýzy, možná závažnost důsledků, vhodná úroveň podrobností a dostupnost příslušných dat a zdrojů.

Tato část byla vypracována jako návod pro širší spektrum průmyslových aplikací a systémů. V některých průmyslových odvětvích, zejména ve zpracovatelském průmyslu, v němž tato technika vznikla, existují specifičtěji zaměřené normy, metody a pokyny, v nichž jsou stanoveny preferované postupy použitelné pro tato průmyslová odvětví. Podrobnosti jsou uvedeny v bibliografii na konci tohoto textu.

## 1. Rámec metody

PHA je ve své podstatě induktivní metoda analýzy, jejímž cílem je vlastní identifikace nebezpečí, nebezpečných situací a událostí, které mohou způsobit při dané činnosti, u daného zařízení nebo u systému poškození nebo újmu. Nejčastěji se provádí v rané etapě vývoje projektu, kdy je k dispozici málo informací o podrobnostech návrhu nebo o provozních postupech, a může předcházet před dalšími studiemi. Je též užitečná při analyzování existujících systémů nebo při stanovení priorit nebezpečí tam, kde okolnosti brání použití pokročilejších metod.

Při PHA se zpracovává seznam nebezpečí a generických nebezpečných situací uvažováním charakteristik, jako jsou:

- používané nebo vytvářené materiály a jejich reaktivita,
- použitá zařízení,
- provozní prostředí,

- prostorové rozmístění,
- rozhraní mezi součástmi systému atd.

Metoda se dokončí identifikací možností, že k nehodě dojde, kvalitativním vyhodnocením rozsahu možných zranění nebo škod na zdraví, které mohou být důsledkem nehody, a identifikací možných opatření k nápravě. PHA se má aktualizovat v průběhu etap návrhu, konstrukce a zkoušení, aby se detekovala jakákoliv nová nebezpečí a aby se učinila opatření k nápravě, pokud to je nutné. Získané výsledky se mohou prezentovat různými způsoby, jako jsou tabulky a stromy.

Přestože hovoříme o analýze PHA, můžeme se v některých odvětvích setkat s jiným označením, které ale slouží k popisu principielně stejné metody [12]. Například v oblasti letectví a v leteckých předpisech je používanějším termínem FHA (Functional Hazard Assessment), který je pro oblast letectví formou metody zakotven například v dokumentech [13][14][15]. Začátek používání metody se datuje do počátku 60. let 20. století (viz [16] str. 101), kdy byla údajně poprvé použita ve Spojených státech amerických v rámci analýzy bezpečnosti raket na kapalná paliva. Později byla formálně formulována leteckým průmyslem (konkrétně firmou Boeing). Oblast letectví, ač pro mnohé poměrně vzdálená a specifická, zde uvádíme z důvodu záměru využít konkrétní aplikaci pro demonstraci popisované metody níže.

Kvalitně provedená metoda PHA může poskytnou následující informace:

1. Specifikace potenciálního nebezpečí v navrhovaném systému;
2. Pravděpodobná velikost a frekvence každého nepříjemného důsledku jevu na sledovaný systém jak „s“ tak „bez“ doporučených opatření pro snížení těchto důsledků. Tyto informace mohou být použity ve studiích hledajících kompromis a alternativní řešení;
3. Navrhovaná opatření pro eliminaci a řízení potenciálního ohrožení;
4. Kritické zařízení z hlediska bezpečnosti a rovněž identifikace kritických situací, na které se musí konstruktéři zaměřit v případě snah o eliminaci nebo snah o řízení nebezpečí;
5. Potenciální události (nehody) jež by měly být podrobeny detailní analýze pokud jsou k dispozici dodatečné informace. Tento bod je velmi důležitou a významnou složkou. Pokud jsou pomocí analýzy PHA identifikovány části systému nebo provozu, které mohou být nebezpečné, je nutné, aby následovaly hlubší a detailnější analýzy, které se uvedenými částmi budou zabývat. Navíc, pokud jsou rovněž identifikovány nebezpečné fáze provozu nebo části systému, ale ne pomocí analýzy PHA, je rovněž nutné se jimi detailně zabývat za využití jiných doplňkových analýz;
6. Identifikace možných chyb člověka, jež mohou vést k nehodám, a jež mohou být eliminovány schopnostmi konstruktérů (např. varování, procedurální instrukce, apod.);
7. Identifikace specifických bezpečnostně důležitých okolností, které splní požadavky standardů, specifikací nebo obdobných dokumentů;
8. Poznámky o nehodách, téměř úspěšných akcích, a jiných potenciálních bezpečnostních problémech, které nebyly odhaleny během zkušeností s předešlými systémy;
9. Potenciální nebezpečí jejichž řízení by mělo být verifikováno v následujících zkouškách specifického formátu.

Každé nebezpečí identifikované v PHA by mělo být dokumentováno ve zprávě o nebezpečí. Příklad takovéto zprávy je uveden například v [4].

Formát a technika, kterou analytik volí při provedení PHA bude více méně záviset na složitosti systému, osobních preferencích analytika, druhu informací, které mají být uvedeny a hloubce analýzy, která má být provedena. Nedílnou a neopomenutelnou skutečností je to, že snahou při provádění metody PHA musí být její integrace a kompatibilita s ostatními disciplínami a aktivitami, které jsou v rámci programu prováděny.

Cílem tohoto příspěvku je tedy prezentovat jednu konkrétní metodu analýzy spolehlivosti a bezpečnosti/rizika letecké techniky a vymezit místo, úlohu a zvláštnosti aplikace metody PHA při predikci spolehlivosti a bezpečnosti dopravního letounu a jeho soustav.

Jako příklad bude dále a poté v závěru prezentována konkrétní aplikace metody na leteckou techniku, při jejím zpracování se odkloníme od zavedených dokumentů, které o metodě PHA hovoří. Tradiční postupy budou uvedeny jako zavedená forma metody, kterou je možné za určitých okolností následovat.

## 2. Popis metody

Metoda PHA by měla být co nejvíce prakticky použitelná ve smyslu identifikace potenciálních ohrožení a indikace prostředků preventivních i nápravných opatření. Z tohoto důvodu musejí být všechny dříve posuzované objekty znova posouzeny (to znamená ty, které byly posuzované podle ještě dřívějších analýz a úvah např. dle postupů uvedených v [5]) tak, aby bylo zaručeno, že žádný nebyl vynechán.

Jelikož je analýza PHA prováděna v časných etapách životního cyklu systému, informace vstupující do analýzy mají převážně obecnou povahu a poskytují málo detailů. Nicméně, tyto předběžné informace mohou obsahovat dostatek indikátorů o potenciálním ohrožení a výsledných důsledcích pro to, aby uvědomily konstruktéry o nutnosti pro nápravnou změnu v návrhu.

Množství informací, které mohou být z analýzy PHA k dispozici závisí na mnoha okolnostech. Především na tom, zda posuzovaný systém jako celek je zcela nový v konceptu nebo zda lze získat data ze zkušenosti s provozem předešlého systému. V některých případech totiž systémy využívají subsystémy, komponenty nebo materiál z předešlých systémů nebo velmi podobný předešlým systémům než ty, které jsou právě analýze PHA podrobeny.

Zcela přesný obsah analýzy PHA není specifikovaný. Přehled zásadních a základních informací, které mají být v analýze uvedeny je uveden níže.

Princip této metody spočívá v systematickém hledání a odhalování událostí, které mají potenciál „být pro nás rizikové“. Riziko je obecně vnímáno jako takový výstup z jakékoliv události, který má negativní povahu. Všechny pozitivní výstupy z události (ač je podstupujeme s vědomím rizika) mají povahu zisku. Každý z nás ví, že je svým způsobem riskantní cestovat autem nebo letadlem. Většina z nás však takové riziko podstupuje, protože věří v zisk – dosažení cíle bez nehody (málo kdo je asi vyznavačem adrenalinu běžném životě). Pragmaticky a v ustáleném pojetí se riziko vnímá jako kombinace pravděpodobnosti nastoupení nežádoucí události, nežádoucích důsledků této události a rovněž někdy úrovní expozice a možnosti odhalení vzniku takové události. V určitých zdrojích se s tímto pojmem frekventovaně pracuje jako např. s *RPN* (*Risk Priority Number* viz např. [6]).

Při realizaci metody PHA se snažíme o zjišťování všech souvisejících okolností souvisejících s rizikem:

- od identifikace zdroje rizika a jeho popisu (*Činnost nebo objekt mající potenciál být pro nás nebezpečným. Neexistuje-li interakce mezi receptorem/příjemcem a zdrojem není možné hovořit o riziku ve vztahu k danému zdroji*),
- přes definice a specifikace fáze technického života kdy může k události dojít (provoz, údržba, modernizace, vypořádání, apod. Může být definována zcela konkrétně ale i obecně),
- přes specifikaci třídy možného důsledku a četnosti výskytu (danou pro určitou posuzovanou oblast, viz níže),
- až po doporučená opatření a výslednou míru ohrožení pro aplikaci doporučených opatření.

Aby mohla být analýza PHA správně provedena, musí být nejprve vyjednán a posouzen koncept/rámec vnímání událostí/poruch systému. Události/poruchy jsou obvykle výsledkem sekvence jevů, jež zahrnují velké množství vlivů. Z toho jednoznačně vyplývá, že nalezení jednotlivého nebezpečí je poměrně komplexní problém. Každá jednotlivá potenciální událost/porucha/nehoda u systému musí být tedy analyzována a posouzena s ohledem na sled jednotlivých jevů. Při správném provedení analýzy je v jejím úvodu nejprve třeba pečlivě analyzovat systém a stanovit hloubku provedení analýzy. Jedná se především o analýzu:

- konstrukčního provedení systému
    - využívá se výkresová dokumentace, apod.,
- jednotlivých funkcí systému

    - je specifikováno v technické zadávací dokumentaci a logicky se váže k jednotlivým prvků, systému,
- funkční provázanosti a souvislosti jednotlivých prvků
    - vyplývá z konstrukčního provedení a funkční struktury systému,
- hloubky provedení
    - obvykle je stanovena technickou specifikací a zadávací dokumentací,
- a stanovení škál a kritérií, podle kterých se události, jež mohou u systému vzniknout, budou posuzovat
    - jedná se o četnost/pravděpodobnost vzniku, závažnost důsledků, výsledná úroveň nebezpečí/rizika, apod.,
    - ke stanovení mezí/kritérií nebo škál slouží primárně zadávací dokumentace nebo sekundárně, není-li zadávací dokumentace k dispozici, legislativa),
- souladu systému se zadávací dokumentací
    - toto je provedeno posouzením vzhledu, konstrukce a především funkce systému za využití zadávací dokumentace. Již tímto krokem je možné předejít vzniku některých nebezpečných nežádoucích událostí u systému,
- formy záznamu analýzy
    - obvyklou formu analýzy tvoří tabulka, která může být dána zadavatelem analýzy, nebo může vyplývat z technické specifikace a zadávací dokumentace, nebo není stanovena (v takovém případě je možné využít standardní podobu, jeden z možných příkladů je uveden níže),
- ostatní.

Hlavním a primárním úkolem analýzy PHA je tedy posouzení nebezpečí, která mohou vyplývat z existence nebo provozu zařízení/systému.

V analýze je vhodné posuzovat rovněž nešťastné náhody/nehody než se soustředit pouze na pravděpodobnost a důsledky událostí vztažených k určitému jednotlivému nebezpečí. V rámci struktury a rámce systému je třeba posoudit velké množství vstupních faktorů, které je třeba posoudit, kombinovat a odvodit z nich možný negativní důsledek jako výstup z určité potenciálně možné události. K tomuto účelu slouží kritéria posouzení, která jsou uvedena níže. Scénář každého jednotlivého nebezpeční musí být jednoznačně popsán, zaznamenán a následně správně posouzen. Z tohoto důvodu se někdy při posouzení jednotlivých událostí dává přednost scénářům nebezpečí než jednotlivým ohrožením. Tím se zajistí lepší a komplexnější chápání možných nehod u systému.

Přestože se v rámci analýzy zabýváme složitými mechatronickými zařízeními, většina scénářů popisujících možná ohrožení a rizika jsou výsledkem vlivu elektrické energie nebo poškození mechanických částí. V analýze je důležité soustředit se na popis zařízení a jeho funkcí především v provozu. Jedině tam je totiž možné zaznamenat skutečné zapojení jednotlivých funkcí a důsledky jejich selhání. To znamená ve správných provozních podmínkách, po správně provedené instalaci, popřípadě v místech technické podpory kde je prováděna údržba systému. V rámci sestavování scénářů a provádění analýzy však můžeme rovněž posoudit i etapu instalace.

V principu provedené analýzy je nutné dále rozlišovat mezi dvěmi základními typy rizika/nebezpečí/ohrožení:

- primární – scénář popisuje možný primární přímý důsledek/zásah/dopad nebezpečí/ohrožení na obsluhu systému/zařízení nebo údržbový personál,
- sekundární – scénář popisuje možný sekundární důsledek/zásah/dopad nebezpečí/ohrožení na ostatní osoby v blízkosti, nebo na okolní zařízení, životní prostředí, apod.

## 3. Forma metody

Forma metody PHA může být dvojí. Buď se jedná o popisnou – stylizovanou formu (méně častá) nebo se jedná o tabulkovou formu (častější).

Tabulkový formát je nejčastěji používanou formou. Její splnění musí mít následující atributy zanesené v tabulce a to v určité posloupnosti.

1. Systém/subsystém/jednotka – tato informace popisuje příslušnou část systému, ke které je uvedený objekt vztažen. Každý záznam analýzy musí identifikovat tu část systému, která je posuzována, přičemž ale se její prezentace může lišit. Někteří analytici uvádějí popis systému v záhlaví přehledového listu a ve sloupcích uvádějí subsystémy, kterých se nebezpečí týká. Jiní analytici vypracovávají pro každý subsystém separátní list a uvádějí přehled subsystémů v záhlaví jednotlivých listů. Subsystémy nebo jednotky nižší úrovně systému musí mít všechny jednoznačnou identifikaci.
2. Fáze události/systému – v této položce/sloupci je identifikován stav systému. Příklady stavů systému jsou: provoz/plnění úkolu-mise/ údržba/ oprava/ přeprava/ skladování. Některé stavy mohou mít sub-stavy (například plnění úkolu-mission letounem může sestávat z pojíždění, vzletu, přistání, apod.)
3. Popis ohrožení – stručný popis ohrožení je uveden v této položce, přičemž má obsahovat různé způsoby a možnosti jak se může nebezpečí projevit. Rovněž tato položka má obsahovat informace o tom, zda je nebezpečí způsobeno normálními provozními podmínkami nebo poruchou nebo jinými abnormálními podmínkami.
4. Důsledek na systém – v této položce se uvádějí nežádoucí/nepříjemné důsledky, jež mohou vyplývat z nebezpečí. Informace může klidně zřetelně obsahovat možná zranění pro specifickou skupinu osob (např. personál údržby nebo kolem stojící) a/nebo pravděpodobné poškození na zařízení a majetku jež může vzniknout v případě, pokud nejsou zahrnuta a aplikována bezpečnostní opatření.
5. Posouzení rizika – kompletní posouzení rizika vyžaduje stanovení závažností důsledků nebezpečí a pravděpodobnosti toho, že se uvedené nebezpečí může stát. Pokud je metoda PHA provedena před tím, než je systém navržen, obvykle je jejím dostatečným výstupem závažnost důsledku události/jevu/poruchy. Neboť pokud vše jde tak, jak má, je nebezpečí eliminováno pečlivým návrhem. Pokud však návrhem nedojde k eliminaci nebezpečí, jsou informace o závažnosti nebezpečí a pravděpodobnosti vzniku nutné pro stanovení prioritních činností pro řízení nebezpečí nebo pro stanovení opatření na minimalizaci nebezpečí. Kategorie závažností důsledků byly stanoveny/vytvořeny nebo ujednány pro to, aby poskytly kvalitativní popis nejhorších možných neštěstí/nehod/událostí, jež mohou vyplývat z chyb člověka, podmínek provozního prostředí, nesouladů v návrhu, procedurálních nedostatků a/nebo poruch/selhání systému, subsystému nebo komponenty. Kategorie nebezpečí jsou uvedeny v tabulce níže, přičemž poskytují obecný návod pro širokou škálu programů. Nicméně pro specifický program může být nutné definovat neštěstí/nehody/poruchy detailněji. Jako příklad můžeme uvést nutnost minimálních požadavků pro definování toho, co všechno bude dotčeno poruchou systému – závažné poškození systému, nezávažné poškození systému, nemoc z povolání. Kvantitativní hodnota pravděpodobnosti nebezpečí nemůže být zjištěna dokud není systém vyroben a po určitou dobu používán. Kvantitativní pravděpodobnosti jsou důležité hodnoty pro další posuzování podobných systémů v budoucnu. Data slouží k expertním odhadům a/nebo posouzením/hodnocením založeným na historických datech o bezpečnosti systémů, podobných konstrukcí a návrhů. Z tohoto důvodu mohou být stanoveny hodnoty kvalitativních pravděpodobností. Z důvodu vysoké ovlivnitelnosti kvalitativních klasifikací individuální interpretací, je velmi důležité, aby byly všechny okolnosti posouzení kvalitativních hodnot pravděpodobnosti nebezpečí zaznamenány do zprávy.
6. Doporučená opatření – uvádějí se prostředky, které slouží k eliminaci nebezpečí nebo mohou posloužit k jeho řízení. Jelikož je metoda PHA prováděna ve raně počátečních etapách akvizičního procesu, je nutné uplatnit všechny možné prostředky pro redukci nebo eliminaci nebezpečí. Bezpečnostní opatření použité v předešlých systémech musejí být popsána a opatření doporučovaná/požadovaná zadávací dokumentací/legislativou musejí být beze zbytku uplatněna. Tam kde to je možné a účelné, je možné zmínit finanční dopad různých bezpečnostních opatření, která mají být aplikována.

7. Důsledek doporučeného patření – tato položka je výhradně využita pro dokumentování zlepšení (lze-li pozorovat) v oblasti posuzování rizika pokud je provedena akce, jež je doporučena v předešlém opatření (viz bod 6).
8. Poznámky – v této položce se uvede každá informace, o které se analytik domnívá, že má význam a není pokryta v jiném předchozím odstavci/sloupci. Informace v této rubrice může zahrnovat dokumenty, které lze využít, data/informace o předchozím výskytu událostí/poruch u podobných systémů a/nebo administrativní pokyny.
9. Status – v této položce se uvádí status/stav ohledně doporučených opatření ve smyslu řízení nebezpečí. Určité užitečné/doplňkové informace mohou být někdy uvedeny v dalších doplňkových sloupcích dle rozhodnutí analytika. Například
   a) Číselný indikátor – obvykle se jedná o první sloupec v doplňkových sloupích a uvádí číslo objektu. Obvykle je uvedena rovněž identifikace subsystému. Potom číslo objektu poskytuje efektivní referenční informaci o systému, která se dále zaznamenává do tabulky.
   b) Referenční materiál – tato položka může být doplněna proto, aby zmínila a uvedla výčet požadovaného vhodného materiálu, přičemž může obsahovat informace od jiného analytika, z jiných analýz, zkušebních záznamů, specifikací a kódových dokumentů.
   c) Ponaučení (Lessons learned) – informace vztažené k bezpečnosti a získané z předešlých systémů, jež mohou být spojeny s určitým specifickým nebezpečím v systému, který se právě analyzuje. Rovněž je zde možné uvést progres a rozvoj bezpečnostních opatření. To obsahuje informace o nehodách, téměř jistých úspěších, poruchách a vztažených zkušenostech.
   d) Další budoucí indikátory analytika – tato položka obvykle obsahuje doporučení pro budoucí analýzy specifických ohrožení. To znamená, pokud PHA odhalí zda komponenta resp. subsystém může způsobit nehodu, uvede se v tomto sloupci doporučení pro další analýzy např. FMEA/FMECA.
   e) Odpovědnost – tato položka může být použita pro nalezení a identifikování specifické osoby nebo organizace odpovědné za uskutečnění opatření pro eliminaci nebo redukci ohrožení/nebezpečí.

Stylizovaná forma metody PHA

V některých případech je tabulková forma metody nevhodná a/nebo neadekvátní pro druh materiálu nebo objektu, který má být analyzován. Tabulková forma může reprezentovat posuzované informace v ucelené podobě. Naproti tomu může být v některých případech vhodnější a efektivnější použít stylizovaný formát metody.

Stylizovaný formát je obvykle sestaveny tak, že každá část analýzy představuje hlavní předmět/objekt/systém posuzování bezpečnosti, přičemž odstavce a pododstavce popisují sub-kategorie hlavního objektu. Některé důvody pro volbu stylizovaného formátu jsou následující:

1. Zajistit to, aby všechny objekty, které jsou posuzovány, byly posouzeny na všechny možná nebezpečí a jsou kompletně probrány.
2. Musí být poskytnut dostatečný výklad pro uspokojení požadavky technické dokumentace a legislativy. Například může být vysvětlen důvod pro akceptování určité míry nebezpečí z důvodů charakteristických pro daný úkol nebo z důvodů vystavení jiného systému nebezpečí jinde. Uvedený text může rovněž vysvětlit jak navržený koncept může zajistit vyhnutí se problémům s bezpečností jež existují/existovaly u předchozích aplikací.
3. Rovněž je zde možné prezentovat data a fakta, pro něž není tabulkový formát výhodnou variantou. Je rovněž jasné, že tabulkový formát není schopen poskytnout dostatek prostoru pro informace, které se mohou objevit ve stylizované formě.
4. Rovněž je možné posuzovat a diskutovat vztaženou bezpečnost objektu/systému/subsystému nebo komponenty. Stylizovaný formát může být navíc vhodnější variantou než tabulková

forma pro vyjasnění a diskusi kompromisů mezi návrhem „s“ a „bez“ opatření pro snížení bezpečnosti – což může být vhodně zvoleno.

5. Tato forma může s úspěchem rovněž sloužit pro vhodnější popis systému, subsystému a komponenty jež je analyzována tak, že si čtenář učiní lepší představu o okolnostech a podmínkách, za kterých může nebezpečí existovat, o faktorech, které mohou nebezpečí způsobit a nepříjemných důsledcích, které mohou vyvstat.

Rovněž existuje kombinovaný formát analýzy PHA, který v sobě slučuje výhody a přednosti výše uvedených forem.

## 4. Typické podoby tabulkových forem metody a využívané škály pro posuzování

Výsledky analýzy jsou, jak bylo již zmíněno výše, obvykle prezentovány ve formě tabulky. Takto uspořádaní a přehledné výstupy slouží v počátečních stádiích návrhu k volbě vhodných soustav pro použití v systému (např. v letadle) a vytvoření seznamu prvků a soustav, u kterých je třeba důkladnější analýza. Níže jsou uvedeny známé a dalo by se říci, že klasické podoby tabulkových forem analýzy (viz tabulka Tab. 1 a Tab. 3). Dále je, z důvodu zaměření ilustračního příkladu níže, uveden oborově charakteristický příklad formátu FHA doporučený podle SAE ARP 4761 a používaný v oblasti letectví (je uvedený v tabulce Tab. 4 a Tab. 5).

Dále jsou uvedeny rovněž příklady a formy jednotlivých škál, které se v rámci provedené analýzy obvykle používají. Jejich přehled je uveden v tabulkách Tab. 6 a Tab. 11.

Tab. 1 Příklad tabulkové formy analýzy PHA

| Objekt č. | Subsystém nebo jednotka/ skupina | Fáze systému kdy může dojít k události | Popis nebezpečí | Důsledek na systém | Ponaučení | Posouzení rizika | Doporučené opatření | Důsledek provedeného doporučeného opatření | Zdrojový materiál | Poznámky | Záznamy analytika v budoucnu | Odpovědnost | Status provádění |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

Tab. 2 Příklad tabulkové formy analýzy PHA

| **Systém:**<br>**Subsystém:** | | *System* - **Preliminary Hazard Analysis** | | | | **List:**<br>**Revize:**<br>**Vypracoval:**<br>**Schválil:** | |
|---|---|---|---|---|---|---|---|
| **P.č.** | **Popis nebezpečí** | **Důsledek nebezpečí** | **Provozní fáze** | **Kategorie nebezpečí a pravděpodobnost** | **Doporučená opatření ke snížení nebezpečí** | **Výsledná úroveň nebezpečí po provedených opatřeních** | **Poznámky** |
| | | | | | | | |

Tab. 3 Příklad jednoduššího formátu tabulkové formy analýzy PHA

| PŘEDBĚŽNÁ ANALÝZA NEBEZPEČÍ<br>SYSTÉM: | | | | | | | |
|---|---|---|---|---|---|---|---|
| Objekt č. | Podmínky vzniku nebezpečí nebo události | Kategorie závažnosti nebezpečí | Příčina | Důsledek | Opatření | Pravděpodobnost výskytu po aplikaci opatření | Poznámky |
| | | | | | | | |

Tab. 4 Formulář FHA doporučený v SAE ARP 4761

| Funkce | Poruchový stav (popis rizik) | Fáze letu | Důsledek pro letadlo/posádku | Klasifikace | Odkaz na podpůrný materiál | Ověření |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

Tab. 5 Zjednodušený, nejčastěji používaný formulář FHA modifikovaný dle doporučení v SAE ARP 4761

| **FHA (Funkční analýza rizik)** |
|---|

| Letoun: | Datum: |
|---|---|
| Vypracoval: | Strana: |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Hodnocení důsledků pro letadlo/posádku | Poznámka |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

Pro obecně platné škály sloužící pro popis událostí/nehod/poruch uvádíme následující členění [5] nebo [8]. Pro klasifikaci závažností důsledků poruch je uvedena škála v tabulce Tab. 6.

Tab. 6 Klasifikace závažnosti důsledků událostí/poruch

| Úroveň závažnosti důsledku | | Důsledky na osoby a systém |
|---|---|---|
| I | Katastrofické | Vícenásobné úmrtí a/nebo mnohonásobná těžká zranění a/nebo závažné poškození životního prostředí a/nebo ztráty systému/zařízení. |
| II | Kritické | Jednotlivá úmrtí a/nebo několik vážných zranění a/nebo několik případů nemoci z povolání a/nebo vážné poškození životního prostředí a/nebo velké poškození systému. |
| III | Závažné | Lehká zranění a/nebo malý počet případů nemocí z povolání a/nebo závažné ohrožení pro životní prostředí a/nebo malé poškození systému. |
| IV | Nevýznamné | Možné lehké zranění a/nebo možnost nemoci z povolání a/nebo poškození systému. |

Frekvence výskytu jednotlivě zaznamenané události/nehody/poruchy je možné posuzovat s ohledem na všeobecně platná doporučení např. [5] nebo [8], škála je uvedena v tabulce Tab. 7.

Tab. 7 Klasifikace a frekvence událostí/poruch.

| Kategorie | | Popis |
|---|---|---|
| A | Časté | Existuje možnost častého výskytu. Nebezpečí působí trvale. |
| B | Pravděpodobné | Vyskytne se několikrát. Výskyt nebezpečí lze očekávat často. |
| C | Občasné | Je možné, že se vyskytne několikrát. Výskyt nebezpečí lze očekávat několikrát. |
| D | Ojedinělé | Je možné, že se vyskytne několikrát během životního cyklu objektu. Výskyt nebezpečí je možné očekávat přiměřeně často. |
| E | Nepravděpodobné | Nepříliš jisté že se vyskytne, ale možné. Můžeme předpokládat, že nebezpečí se může výjimečně vyskytnout. |
| F | Nemožné | Extrémně nemožné, že se vyskytne. Lze předpokládat, že nebezpečí se nevyskytne. |

Výsledná úroveň rizika/nebezpečí je získána vzájemným spojením získaných hodnot závažností důsledků události/poruchy a potenciálu četnosti výskytu. Obvyklá škála klasifikace rizika/nebezpečí je uvedena v tabulce Tab. 8, přičemž rozlišujeme riziko přijatelné a nepřijatelné.

- Nepřijatelné riziko: musí být eliminováno
- Přijatelné riziko: může být přijato bez jakýchkoliv opatření

Tab. 8 Klasifikace rizika.

| | | **Závažnost důsledku události/poruchy** | | | |
|---|---|---|---|---|---|
| **Četnost výskytu události/poruchy** | | **I** | **II** | **III** | **IV** |
| Častá (probability > $10^{-3}$/h) | **A** | | | | |
| Pravděpodobná ($10^{-4}$/h < probability ≤ $10^{-3}$/h) | **B** | | | | |
| Občasná ($10^{-5}$/h < probability ≤ $10^{-4}$/h) | **C** | | | | |
| Ojedinělá ($10^{-7}$/h < probability ≤ $10^{-5}$/h) | **D** | | | | |
| Nepravděpodobná ($10^{-9}$/h < probability ≤ $10^{-7}$/h) | **E** | | | | |
| Nemožná (probability ≤ $10^{-9}$/h) | **F** | | | | |

Zóna nepřijatelného rizika.

Zóna přijatelného rizika.

V odborné literatuře a ve specifických technických odvětvích (jako je například letectví) se můžeme setkat s mírně modifikovanými a specifickými příklady hodnotících škál. Jejich příklady převzaté z dokumentů a oběžníků [3], [12] a [14] jsou uvedeny níže v tabulkách Tab. 9, Tab. 10 a Tab. 11.

Tab. 9 Příklad klasifikace závažností důsledků událostí/poruch používaný v letectví ve vztahu k dokumentu [3].

| Klasifikace poruchových stavů | Nezávažné (Minor) | Závažné (Major) | Katastrofické (Catastrophic) |
|---|---|---|---|
| Důsledek pro letadlo | Mírné snížení funkčních schopností nebo rezerv bezpečnosti | Významné snížení funkčních schopností nebo rezerv bezpečnosti | Poruchové stavy vylučující pokračování v letu a přistání |
| Důsledek pro cestující | Mírné fyzické potíže pro cestující | Fyzické strádání u cestujících | |
| Důsledek pro osádku | Mírný nárůst pracovního zatížení osádky nebo použití nouzových postupů | Fyzické potíže nebo značný nárůst pracovní zátěže | |
| | Přípustné pravděpodobnostní nastoupení poruchy za 1 letovou hodinu, založené na průměrné době trvání letu daného typu letounu. (U funkcí, které jsou používány pouze pro určitou část letu, např. vzlet, přistání, apod., by přípustná pravděpodobnost měla být založená na době trvání této operace) | | |
| | > $10^{-5}$ | $10^{-5}$ – $10^{-9}$ | < $10^{-9}$ |

Tab. 10 Příklad klasifikace závažností důsledků událostí/poruch používaný v letectví (pro typ letounu do max. 19 sedadel + piloti a nejvyšší maximální vzletová hmotnost 19 000lb) ve vztahu k dokumentu [13].

| Klasifikace poruchových stavů | Bez vlivu na bezpečnost | Nezávažné (Minor)[1] | Závažné (Major)[1] | Nebezpečné (Hazardous)[3] | Katastrofické (Catastrophic)[2] |
|---|---|---|---|---|---|
| Důsledek pro letadlo | Žádný důsledek pro provozní schopnosti a bezpečnost | Mírné snížení funkčních schopností nebo rezerv bezpečnosti | Významné snížení funkčních schopností nebo rezerv bezpečnosti | Velké snížení funkčních schopností nebo rezerv bezpečnosti | Běžně zahrnuje zkázu trupu |
| Důsledek pro cestující | Nepohodlí pro cestující | Fyzické potíže pro cestující | Fyzické strádání u cestujících včetně možných zranění | Vážné nebo smrtelné zranění jednoho cestujícího | Několikanásobné smrtelné zranění cestujících |
| Důsledek pro osádku | Bez důsledku na letovou posádku | Mírný nárůst pracovního zatížení osádky nebo použití nouzových postupů | Fyzické potíže nebo značný nárůst pracovní zátěže | Fyzické strádání nebo nadměrné pracovní zatížení osádky narušuje schopnost plnit úkoly | Smrtelné zranění nebo zbavení způsobilosti |
| Rozdělení typů letadel: | Přípustné pravděpodobnosti (za 1 letovou hodinu) | | | | |
| Třída 1 – SRE (pod 6 000 lb.) | Žádná požadovaná pravděpodobnost | $< 10^{-3}$ | $< 10^{-4}$ | $< 10^{-5}$ | $< 10^{-6}$ |
| Třída 2 – MRE nebo STE (pod 6000 lb.) | Žádná požadovaná pravděpodobnost | $< 10^{-3}$ | $< 10^{-5}$ | $< 10^{-6}$ | $< 10^{-7}$ |
| Třída 3 – SRE, STE, MRE, MTE (rovno nebo větší než 6 000 lb.) | Žádná požadovaná pravděpodobnost | $< 10^{-3}$ | $< 10^{-5}$ | $< 10^{-7}$ | $< 10^{-8}$ |
| Třída 4 – pro sběrnou dopravu | Žádná požadovaná pravděpodobnost | $< 10^{-3}$ | $< 10^{-5}$ | $< 10^{-7}$ | $< 10^{-9}$ |

SRE – Single Reciprocating Engine – jednomotorový letoun s pístovým motorem
MRE – Multiple Reciprocating Engine – vícemotorový letoun s pístovými motory
STE – Single Turbine Engine – jednomotorový letoun s turbínovým motorem
MTE – Multiple Turbine Engine – vícemotorový letoun s turbínovými motory
Pozn.
1 – obvykle není požadována kvalitativní analýza pro *nezávažné* a *závažné* poruchové stavy,
2 – na úrovni funkce celého letounu nebude mít samostatná porucha za následek vznik situace s katastrofickými následky,
3 – na úrovni funkce celého letounu nebude mít samostatná porucha za následek vznik *nebezpečné* situace.
V tabulce jsou oproti znění předpisu vynechány pasáže, které se dotýkají hodnocení úrovně bezpečnosti software.

Tab. 11 Klasifikace závažnosti důsledků událostí/poruch a jejich výskytů ve vztahu k dokumentům [3] a [13]

| Důsledek | Pravděpodobnost nastoupení jevu | Poznámka |
|---|---|---|
| Nezávažný (MINOR) | Může být pravděpodobné (probable) | Očekává se, že k nastoupení tohoto jevu může dojít jednou nebo vícekrát během technického života letounu. |
| Závažný (MAJOR) | Musí být s řídkým výskytem (remote) nebo nepravděpodobné (improbable) | Požaduje se, aby bylo nepravděpodobné nastoupení tohoto jevu během celého technického života letounu. Porucha se však může několikrát objevit, pokud zahrneme všechny vyrobené a provozované letouny daného typu. |
| Nebezpečný (HAZARDOUS) | Musí být nepravděpodobné (improbable) nebo s velmi řídkým výskytem (extremely remote) | Požaduje se, aby bylo nepravděpodobné nastoupení tohoto jevu během celého technického života letounu. Porucha se však může několikrát objevit, pokud zahrneme všechny vyrobené a provozované letouny daného typu. |
| Katastrofický (CATASTROPHIC) | Musí být vysoce nepravděpodobné (extremely improbable) | Požaduje se, aby bylo nepravděpodobné nastoupení tohoto jevu během celého technického života všech vyrobené a provozovaných letounů daného typu. |
| Samozřejmě je třeba v této souvislosti upozornit na rozdílnosti výše uvedeného českého překladu předpisů. Angličtina je bohatší jazyk a čeština bohužel nemá pro všechna vyjádření svůj ekvivalent, proto je nutné dbát ostražitosti při rozdílech mezi slovy např. „improbable“ a „remote“ a jejich českých překladů. Z tohoto důvodu, aby nedošlo ke špatnému výkladu požadavků, je někdy vhodnější pracovat s originálními termíny a jejich výkladem (to samozřejmě za předpokladu, že je analytik dostatečně jazykově zdatný a vnímá rozdílnosti v těchto skutečnostech). | | |

Co se využití hodnotících škál týče, jedná se o velmi slabé místo analýzy a to z důvodů eventualit verifikace a validace provedeného postupu. Každý analytik má svůj specifický přístup k provedení analýzy a z tohoto důvodu je potřebné k provedení analýzy přistupovat. Již samotná škála tento potenciál otvírá, protože je obvykle (i v příkladech výše) definovaná vágně. Ideálním stavem tak, jak bylo uvedeno výše, se jeví sestavení analytického týmu. Pokud to není možné musí analytik svá rozhodnutí ve znění analýzy zdůvodnit.

Dále bude uveden postup, dle kterého by měla být samotná analýza provedena. Pokud bychom se přidrželi požadavků na počáteční vstupní požadavky pro uskutečnění analýzy uvedené v části 2, strana 5, jsou záležitosti konstrukce, funkce, provázanosti a hloubky provedení analýzy uvedeny v referenčním dokumentu [17].

## 5. Příklad aplikace metody PHA v praxi

Při zpracování příkladu z praxe se odkazujeme na referenční dokument [17], kde jsou uvedeny základní požadavky na letoun, resp. jeho soustavu, která bude dílem posouzena analýzou PHA.

Podle leteckých předpisů [3], [13], [14] nebo [15] musí být prvky a letadlové systémy z nich vytvořené uvažovány jednotlivě, ve vzájemném spojení i ve spojení s ostatními systémy letounu navrženy a zhotoveny tak, aby za všech předvídatelných podmínek provozu:

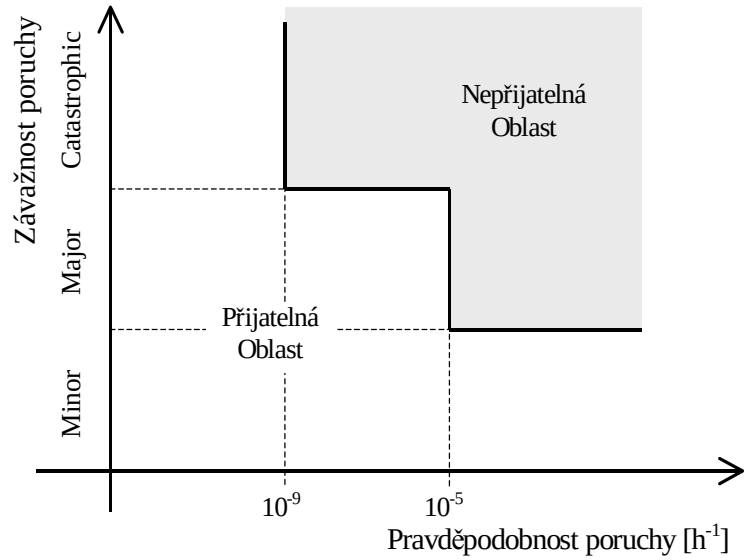
- výskyt jakéhokoliv poruchového stavu, který by mohl znemožnit pokračování bezpečného letu a přistání letounu byl extrémně nepravděpodobný (poruchové stavy tohoto typu jsou označovány jako katastrofické poruchové stavy - Catastrophic);
- výskyt jakéhokoliv poruchového stavu, který by mohl omezit (snížit, redukovat) schopnost letounu nebo posádky letounu zvládnout nepříznivé provozní podmínky byl nepravděpodobný (poruchové stavy tohoto typu jsou označovány jako závažné poruchové stavy - Major).

Poruchové stavy, které významně nesnižují bezpečnost letounu mohou být pravděpodobné (tyto poruchové stavy jsou označovány jako nezávažné – Minor). Jednotlivé poruchové stavy jsou podle předpisů [5] považovány za:

- pravděpodobné jestliže pravděpodobnost jejich výskytu je větší než $1{,}0 \cdot 10^{-5}$ za hodinu letu.
- nepravděpodobné jestliže pravděpodobnost jejich výskytu je menší než $1{,}0 \cdot 10^{-5}$ za hodinu letu ale větší než $1{,}0 \cdot 10^{-9}$;
- extrémně nepravděpodobné pokud pro pravděpodobnost jejich výskytu během jedné hodiny letu platí, že je menší než $1{,}0 \cdot 10^{-9}$.

V leteckých předpisech se tedy požaduje, aby každý poruchový stav měl pravděpodobnost nepřímo úměrnou jeho závažnosti. Grafické vyjádření tohoto požadavku – viz obr. 1.

Dále předpisy nepřipouští, aby poruchový stav, který je důsledkem pouze jediného druhu poruchy byl považován za extrémně nepravděpodobný. Jinak řečeno – je nepřijatelné, aby jednotlivá porucha některého z prvku letadlových systémů vedla ke katastrofickým důsledkům.




**Obr. 1 Vztah mezi závažností poruchových stavů a jejich přípustnou pravděpodobností**

Prvním krokem postupu je provedení tzv. *hodnocení funkční nebezpečnosti* každé soustavy letounu. Jedná se v podstatě o modifikovanou *předběžnou analýzu rizik* (Preliminary Hazard Analysis), jejímž cílem je určení a klasifikace nebezpečných poruchových stavů letadlových soustav. V rámci této části analýzy by měly být identifikovány všechny závažné a katastrofické poruchové stavy každé soustavy. Vychází se přitom z analýzy funkcí jednotlivých předpokládaných prvků soustavy a posouzení důsledků selhání těchto funkcí. Výsledky této analýzy vždy mají předběžný charakter a je třeba je doplňovat a verifikovat na základě výsledků dalších kroků analýzy. Výstupy analýzy po posouzení základních požadavků na systém jsou vstupem pro konstrukční a návrhové zpracování soustavy brzd letounu. Její navržená konstrukční podoba je uvedena v dokumentu [19].

V rámci provedení předběžné analýzy nebezpečí byly u této části soustavy identifikovány, mimo jiné, dva následující poruchové stavy [1]:

- přistání letounu se zabrzděnými koly;
- selhání brzdové soustavy při pohybu letounu po zemi.

Další poruchové stavy, které byly u soustavy identifikovány zde nejsou uváděny, protože jejich znalost není pro uváděný příklad podstatná.

Vlastní provedení analýzy je zaznamenáno do tabulek (viz vzor tabulky uvedený výše - Tab. 5 a Tab. 2), přičemž jednotlivé rubriky jsou vyplněny za využití tabulek Tab. 9, Tab. 10 nebo Tab. 11.

1) Provedení analýzy

**FHA (Funkční analýza rizik)**

| | |
|---|---|
| Letoun: L 610 | Datum: 29.04.2009 |
| Vypracoval: Vališ | Strana: 1 |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Důsledek poruchového stavu na letadlo/osádku | Hodnocení důsledků pro letadlo/cestující/posádku | Poznámka |
|---|---|---|---|---|---|---|
| BP | Brzdění pojezdových kol podvozku letadla | Pojezd | Selhání částečné nebo úplné brzdové soustavy při pojezdu letounu po zemi. | Posádka letadla není s to zastavit letoun během pojezdu nebo při příjezdu k bráně, který vede ke kontaktu s terminálem, vozidlem nebo jiným letadlem v malé rychlosti. | Závažný/ Závažný / Závažný | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. |
| BP | Brzdění pojezdových kol podvozku letadla | Pojezd | Selhání (částečné nebo úplné) brzdové soustavy při pojezdu letounu po zemi. | Posádka řídí letadlo bezpečně a je schopna se vyhýbat překážkám, přičemž volá pro mobilní schody nebo pro vodící vozidlo. | Nezávažný/ Nezávažný / Nezávažný event. Bez důsledku na bezpečnost | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. |
| BP | Brzdění pojezdových kol podvozku letadla | Pojezd | Selhání (částečné nebo úplné) brzdové soustavy při pojezdu letounu po zemi. | Posádka není s to bezpečně/adekvátně zastavit letoun před překážkou což vede ke kontaktu s ní v nízké rychlosti. | Nezávažný/ Nezávažný / Nezávažný | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. |
| BP | Brzdění pojezdových kol | Pojezd | Selhání (částečné nebo úplné) brzdové soustavy | Osádka není s to bezpečně/adekvátně | Nezávažný/ Nezávažný / Nezávažný | Letadlo lze přibrzďovat nebo úplně zastavit |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Důsledek poruchového stavu na letadlo/osádku | Hodnocení důsledků pro letadlo/cestující/posádku | Poznámka |
|---|---|---|---|---|---|---|
| | podvozku letadla | | při pojezdu letounu po zemi. | zastavit letoun před překážkou což vede ke kontaktu s ní v nízké rychlosti. | | pomocí reversace tahu motorů. |
| BP | Brzdění pojezdových kol podvozku letadla | Pojezd | Selhání (částečné nebo úplné) brzdové soustavy/nesymetrie v brzdovém účinku na brzděných kolech při pojezdu letounu po zemi. | Letadlo se mírně odchyluje od požadovaného směru. | Nezávažný/ Nezávažný / Nezávažný – event. Bez důsledku na bezpečnost | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání | Přistání letounu se zabrzděnými koly | Při dosednutí dojde ke smyku pneumatik, jejich přehřátí a mechanickému přetížení a pravděpodobně k destrukci, která může vést až ke katastrofě. | Závažný/ Závažný / Nebezpečné | Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání/odvolaný vzlet-start | Přistání, resp. odvolaný start letounu a nemožnost zabrzdění provozními brzdami. | Posádka není s to zpomalit letoun, což může vést k překročení maximální pojezdové rychlosti. | Katastrofický/ Katastrofický / Katastrofický | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání | Detekce ztráty možnosti zpomalit letoun provozními brzdami při přistání. | Posádka není s to zpomalit letoun při přistání, přičemž vybírá náhradní vhodnější | Nebezpečný/ Nebezpečný / Nebezpečný | |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Důsledek poruchového stavu na letadlo/osádku | Hodnocení důsledků pro letadlo/cestující/posádku | Poznámka |
|---|---|---|---|---|---|---|
| | | | | letiště, uvědomí pozemní záchranný sbor a připraví pasažéry na přistání zvýšenou rychlostí. | | |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání | Ztráta možnosti zpomalit letoun provozními brzdami při přistání před koncem přistávací dráhy. | Posádka není s to zpomalit letoun při přistání před koncem přistávací dráhy, což může vést k překročení rychlosti při přistání a sjetí z dráhy. | Nebezpečný/ Nebezpečný / Nebezpečný | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol podvozku letadla | Vzlet | Ztráta možnosti rozjet letoun při vzletu-startu. | Posádka není s to vzlétnout s letadlem, protože ve stejném momentě kdy je požadován tah, je zaveden brzdový účinek na kolech. To může vést ke sjetí z dráhy. | Nebezpečný/ Nebezpečný / Nebezpečný | |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání/odvolaný start | Ztráta automatické možnosti zpomalit/zastavit letoun provozními brzdami. | Posádka aktivuje automatický režim pro zastavení/zpomalení při přistání, resp. odvolaném startu. Poté je ale zjištěno, že systém nefunguje. Osádka situaci registruje a aktivuje manuální režim pro zpomalení-zastavení. | Nebezpečný/ Nebezpečný / Nebezpečný | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Důsledek poruchového stavu na letadlo/osádku | Hodnocení důsledků pro letadlo/cestující/posádku | Poznámka |
|---|---|---|---|---|---|---|
| | | | | Reakční čas posádky může vést ke sjetí z dráhy. | | |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání/odvolaný start | Ztráta automatické možnosti zpomalit/zastavit letoun provozními brzdami. | Posádka okamžitě aktivuje manuální režim pro zpomalení-zastavení. | Bez důsledků na bezpečnost | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání/odvolaný start | Ztráta možnosti zpomalit letoun při přistání – nesymetrie v brzdění a zpomalení provozními brzdami. | Posádka není připravena na nesymetrii v brzdění-zpomalení, přičemž reaguje příliš pozdě na to, aby udržela požadovaný směr. To může vést ke sjetí z dráhy. | Nebezpečný/ Nebezpečný / Nebezpečný | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol podvozku letadla | Přistání/odvolaný start | Ztráta možnosti zpomalit letoun při přistání – nesymetrie v brzdění a zpomalení provozními brzdami. | Posádka je připravena na nesymetrii v brzdění-zpomalení, přičemž reaguje vhodnými zásahy a technikou řízení směrovek a předního kola letadla. | Nezávažný/ Nezávažný / Nezávažný – event. Bez důsledku na bezpečnost | Letadlo lze přibrzďovat nebo úplně zastavit pomocí reversace tahu motorů. Tento druh poruchového stavu subsystému může vést ke katastrofickým důsledkům. |
| BP | Brzdění pojezdových kol | Přistání/odvolaný start | Ztráta možnosti zpomalit letoun při přistání – | Letoun se mírně odchyluje od | Nezávažný/ Nezávažný / Nezávažný – event. Bez | Letadlo lze přibrzďovat nebo úplně zastavit |

| Označení funkce | Funkce | Fáze letu | Poruchový stav | Důsledek poruchového stavu na letadlo/osádku | Hodnocení důsledků pro letadlo/cestující/posádku | Poznámka |
|---|---|---|---|---|---|---|
| | podvozku letadla | | nesymetrie v brzdění a zpomalení provozními brzdami. | požadovaného směru. | důsledku na bezpečnost | pomocí reversace tahu motorů. |
| | | | | | | |
| Poznámky:<br>BP – brzdění podvozkem | | | | | | |

Výtah výše uvedených rubrik do jiné tabulkové podoby. Jedná se o redukovaný vzor.

| **Systém: Letadlo L 610**<br>**Subsystém: Brzdová soustava** | **Aircraft Brake System - Preliminary Hazard Analysis** | | | | | **List: 1**<br>**Revize:**<br>**Vypracoval: Vališ**<br>**Schválil: Vintr** | |
|---|---|---|---|---|---|---|---|
| **P.č.** | **Popis nebezpečí** | **Důsledek nebezpečí** | **Provozní fáze** | **Kategorie nebezpečí a pravděpodobnost** | **Doporučená opatření ke snížení nebezpečí** | **Výsledná úroveň nebezpečí po provedených opatřeních** | **Poznámky** |
| 1. | Selhání brzdové soustavy při pojezdu letounu po zemi. | 1. Pro letadlo: Závažný<br>2. Pro cestující: Závažný<br>3. Pro osádku: Závažný | Pojezd | Závažné/ nepravděpodobné | 1. Brzdová soustava musí být navržena a všechny její části vyrobeny v souladu technickou specifikační a zadávací dokumentací YY.<br>2. Vložení signalizačního | Nezávažná/ Velmi řídká | Při návrhu, vývoji, výrobě, montáži a provozu je nutné dbát ustanovení technické specifikační a zadávací dokumentace YY |

| Systém: Letadlo L 610<br>Subsystém: Brzdová soustava | **Aircraft Brake System - Preliminary Hazard Analysis** | | | | | List: 1<br>Revize:<br>Vypracoval: Vališ<br>Schválil: Vintr | |
|---|---|---|---|---|---|---|---|
| **P.č.** | **Popis nebezpečí** | **Důsledek nebezpečí** | **Provozní fáze** | **Kategorie nebezpečí a pravděpodobnost** | **Doporučená opatření ke snížení nebezpečí** | **Výsledná úroveň nebezpečí po provedených opatřeních** | **Poznámky** |
| | | | | | diagnostického prvku, který uvědomí obsluhu o tom, že v soustavě není dostatečný provozní tlak potřebný pro funkci brzd.<br>3. Montáž musí být provedena dle stanovených postupů (utahovací momenty, montážní prvky, pomůcky, nářadí, provozní náplně, proškolený a zkušený personál, apod.).<br>4. Údržba soustavy musí být prováděna dle stanovených intervalů, ve stanoveném rozsahu a s využitím | | |

| Systém: Letadlo L 610<br>Subsystém: Brzdová soustava | **Aircraft Brake System - Preliminary Hazard Analysis** | | | | | List: 1<br>Revize:<br>Vypracoval: Vališ<br>Schválil: Vintr | |
|---|---|---|---|---|---|---|---|
| **P.č.** | **Popis nebezpečí** | **Důsledek nebezpečí** | **Provozní fáze** | **Kategorie nebezpečí a pravděpodobnost** | **Doporučená opatření ke snížení nebezpečí** | **Výsledná úroveň nebezpečí po provedených opatřeních** | **Poznámky** |
| | | | | | stanovených diagnostických přístrojů (vše je uvedeno v dokumentu YY.<br>5. | | |
| 2. | Přistání letounu se zabrzděnými koly | 1. Pro letadlo: Závažný<br>2. Pro cestující: Závažný<br>3. Pro osádku: Nebezpečný | Přistání | Závažné/ nepravděpodobné | 1. Brzdová soustava musí být navržena a všechny její části vyrobeny v souladu technickou specifikační a zadávací dokumentací YY.<br>2. Vložení signalizačního diagnostického prvku, který uvědomí obsluhu o tom, že v soustavě je v době nezatíženého podvozku provozní tlak, který může způsobit zablokování kol | Nezávažná/ Velmi řídká | Při návrhu, vývoji, výrobě, montáži a provozu je nutné dbát ustanovení technické specifikační a zadávací dokumentace YY |

| Systém: Letadlo L 610<br>Subsystém: Brzdová soustava | **Aircraft Brake System - Preliminary Hazard Analysis** | | | | | List: 1<br>Revize:<br>Vypracoval: Vališ<br>Schválil: Vintr | |
|---|---|---|---|---|---|---|---|
| **P.č.** | **Popis nebezpečí** | **Důsledek nebezpečí** | **Provozní fáze** | **Kategorie nebezpečí a pravděpodobnost** | **Doporučená opatření ke snížení nebezpečí** | **Výsledná úroveň nebezpečí po provedených opatřeních** | **Poznámky** |
| | | | | | před dosednutím letadla při přistání.<br>3. Montáž musí být provedena dle stanovených postupů (utahovací momenty, montážní prvky, pomůcky, nářadí, provozní náplně, proškolený a zkušený personál, apod.).<br>4. Údržba soustavy musí být prováděna dle stanovených intervalů, ve stanoveném rozsahu a s využitím stanovených diagnostických přístrojů (vše je uvedeno v dokumentu YY. | | |

2) Závěr – vyhodnocení analýzy

Z výše uvedených výsledků analýzy brzdové soustavy letadla je patrné, že počáteční analýza provedená na letadle je především iniciačním vstupem pro práci konstruktérů a rovněž další následující kvalitativní i kvantitativní analýzy. Problematické chování soustavy v jednotlivých charakterizovaných nepřijatelných poruchových stavech lze vyřešit konstrukčními zásahy. Konstruktér může například navrhnout vložení výstražné signalizace do soustavy tak, aby piloty informovala o existenci příslušného poruchového stavu, tedy o tom, že v době kdy nejsou podvozkové nohy zatíženy (za letu) je brzdový systém pod tlakem nebo naopak o tom, že v soustavě není požadovaný provozní tlak potřebný k vyvolání dostatečného provozního brzdného účinku. Realizací těchto opatření zkoumaný poruchový stav ztratí v prvém případě skrytý charakter a ve druhém případě usnadní identifikaci místa poruchy a je možno je dále považovat za *nezávažné*. Po této úpravě již soustava bude splňovat požadavky leteckých předpisů.

Zde je třeba podotknout, že poruchové stavy se stejnými důsledky (tlak v brzdové soustavě za letu nebo naopak nedostatečný tlak v soustavě při pojezdu letadla) mohou být způsobeny také poruchami řady dalších prvků, které se podílí na podpoře funkce brzdové soustavy (generují a přenáší signál o zatížení podvozků, generují tlak brzdícího média, slouží ke snímání diagnostických a ovládacích veličin, apod.). Zavedením výstražné signalizace se tak sníží závažnost i všech těchto dalších poruchových stavů.

## 5. Závěr

Metoda PHA je v současnosti v oblasti bezpečnosti letecké dopravy spolu s ostatními metodami považována za jednu z nejdůležitějších metod analýzy bezpečnosti a bezporuchovosti leteckých konstrukcí. Nicméně na závěr je třeba zdůraznit některé závažné aspekty související s její aplikací, které jsou ale platné pro všechny následující a navazující techniky a analýzy:

- Analytik, resp. tým analytiků, kteří metodu aplikují musí dokonale znát jak použití vlastní metody, tak i soustavu kterou analyzují, proto musí při vlastní analýze úzce spolupracovat s celou řadou dalších odborníků – konstruktérů, pilotů, provozních techniků, atd. Jedině tak lze zajistit, aby nic závažného při vlastní analýze nebylo opomenuto.
- Metoda sama o sobě není všemohoucí, vyčerpávající a bezvadná, proto musí být vždy při analýzách bezpečnosti a bezporuchovosti letounu používána v kombinaci s jinými standardními a doporučenými analytickými technikami a postupy, se kterými se vzájemně doplňuje.

## Použitá literatura:


[1] HOLUB, R. a VINTR, Z.: *Analýza spolehlivosti a bezpečnosti systému ovládání brzd s protiblokovacím zařízením letounu L-610 G*. [Výzkumná zpráva]. Brno: Vojenská akademie 1995.

[2] HOLUB, R. and VINTR, Z.: Integrated Safety Program of L-610G Transport Aeroplane Development. In: *PSAM 5 - Probabilistic Safety Assessment and Management – Proceedings of 5th International Conference on Probabilistic Safety Assessment and Management*. Tokyo: Universal Academy Press 2000.

[3] HOLUB, R. and VINTR, Z.: The Reliability/Safety Analyses of Transport Aeroplane Systems in Process of their Certification. In: *Safety and Reliability in Transport - Proceeding of the 16th ESReDA Semminar*. Luxembourk: European Communities 2000.

[4] Federal Aviation Regulations – FAR Part 25. Washington: Federal Aviation Administration 1988.

[5] IEC 61882 Hazard and operability studies (HAZOP studies) – Application guide

[6] ČSN IEC 60 812:2006 – Metody analýzy spolehlivosti systémů. Postup analýzy způsobů a důsledků poruch (FMEA). Praha: ČSNI 1992.

[7] MIL-HDBF-882C/882D System safety programme requirements

[8] MIL-HDBK 764 *System Safety Engineering Design Guide for Army Material.* Washington : Department of Defence, 1990.

[9] EN 50126:1999 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[10] *A Guide to Hazard and Operability Studies.* Chemical Industries Association, London, UK, (1977).

[11] *Guidelines for Hazard Evaluation Procedures.* Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA, 1999, ISBN 0-8169-0491-X.

[12] HLINKA, J. Posuzování bezpečnosti a spolehlivosti letadlové techniky v průběhu návrhu a certifikace, Brno: VUT 2007, habilitační práce.

[13] Advisory Circular AC 23.1309-1C: Equipment, Systems, and Installations in Part 23 Airplanes. Federal Aviation Administration, Washington D.C., www.faa.gov, 3/1999, 30 str.

[14] Advisory Circular AC 25.1309-1A: System Design and Analysis. Federal Aviation Administration, Washington D.C., www.faa.gov, 6/1988, 19 p.

[15] ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE Warrendale USA, 12/1996, 331 p.

[16] VILLEMEUR, A. Reliability, Availability, Maintainability and Safety Assessment, Vol.1, New York: John Wiley & Sons 1992. p. 748.

[17] VINTR, Z.: *Základní filozofie průkazu spolehlivosti a bezpečnosti technického systému v počátečních etapách životního cyklu*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

[18] HLINKA, J.: *Modelování spolehlivosti a bezpečnosti systému jako celku*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

[19] VINTR, M.: *Metoda FMECA jako nástroj analýzy bezpečnosti a spolehlivosti komponent systému*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

# METODA FMECA JAKO NÁSTROJ ANALÝZY BEZPEČNOSTI A SPOLEHLIVOSTI KOMPONENT SYSTÉMU

***Ing. Michal VINTR***

*Vysoké učení technické v Brně, Fakulta strojního inženýrství*
*Technická 2896/2, 616 69 Brno, Email: vintr@fme.vutbr.cz.*

## 1 Úvod

Cílem tohoto příspěvku je popsat a prakticky aplikovat metodu, která umožňuje posoudit splnění požadavků zákazníka v oblasti bezpečnosti a spolehlivosti, které jsou kladeny na jednotlivé komponenty systému. K tomu je v příspěvku použita metoda analýzy způsobů, důsledků a kritičnosti poruch (FMECA). V první části příspěvku je popsána metoda FMECA a její použití, v druhé části je provedena praktická aplikace metody na příkladu brzdového systému dopravního letounu.

## 2 Metoda FMECA

### 2.1 Podstata a rozdělení metody

V literatuře a praxi se můžeme setkat používáním zkratek FMEA (*Failure Modes and Effects Analysis*) a FMECA (*Failure Modes, Effects and Criticality Analysis*), vycházejících z anglických názvů. Dle platných norem ČSN [1] jsou tyto názvy překládány jako Analýza způsobů a důsledků poruch, resp. Analýza způsobů, důsledků a kritičnosti poruch. Je však možno se setkat i s jinými pojmenováními (podrobněji viz [1]).

Metoda FMEA je strukturovaná, kvalitativní analýza sloužící k identifikaci způsobů poruch systémů, jejich příčin a důsledků. Metoda FMECA je logickým rozšířením metody FMEA spočívajícím v tom, že jsou do ní zahrnuty prostředky pro klasifikaci závažnosti způsobů poruch.

Metoda FMEA/FMECA (dále jen FMECA) je dle způsobu použití nejčastěji rozdělována na:

- konstrukční FMECA (Design FMECA), někdy také nazývána FMECA návrhu, která se používá pro potřeby analýzy produktu, respektive technického návrhu produktu.
- procesní FMECA (*Process FMECA*), která se používá pro potřeby analýzy procesu.

Tento příspěvek je primárně zaměřen na FMECA konstrukční.

### 2.2 Historie a standardizace metody

Metoda FMECA byla vytvořena v 50. letech 20. století Armádou Spojených Států Amerických. Ta v roce 1949 vydala první armádní proceduru pro použití metody FMECA – *MIL-P-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. Metoda byla v počátcích používána zejména v oblasti letectví a ozbrojených sil jako nástroj umožňující určovat důsledky poruch systémů a jejich komponent.

K výraznému rozšíření metody FMECA došlo v 60. letech minulého století v souvislosti s potřebou zabezpečovat spolehlivost nových technických systémů, které se vyznačovaly značnou složitostí a jejichž selhání mohlo vést ke katastrofickým důsledkům značného rozsahu. Jednou z prvních známých aplikací metody FMECA bylo její použití v agentuře NASA při realizaci projektu APOLLO. Metoda se osvědčila a její použití se rychle rozšířilo do celé řady dalších oborů lidské činnosti. Jako výsledek vývoje byl Armádou USA v roce 1974 poprvé vydán vojenský standard *MIL-STD-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, který zobecnil získané zkušenosti a zformuloval základní zásady pro provádění a použití metody. Poslední verze normy pochází z roku 1980 [2].

Metoda nezůstala stranou zájmu mezinárodních standardizačních organizací. V roce 1985 Mezinárodní elektrotechnická komise IEC vydala normu *IEC 812 Procedure for Failure Mode and Effects Analysis*, která byla v roce 1992 zavedena také v ČR jako ČSN IEC 812. V současné době je platná aktualizovaná verze normy *ČSN EN 60812 Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)* vydaná v roce 2007 [1].

Metoda se také rozšířila v oblasti automobilového průmyslu. V roce 1994 byla v USA Společností automobilových inženýrů SAE poprvé vydána norma *SAE J1739 Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery (Machinery FMEA).* V současné době je platná revize z roku 2002 [4]. Norma je určena pro použití zejména v automobilovém průmyslu. SAE také vydala v roce 2001 normu *SAE ARP5580 Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications* [3], která je určena pro použití mimo oblast automobilového průmyslu.

Metoda nezůstala stranou pozornosti ani Sdružení automobilového průmyslu VDA, které v roce 2007 vydalo aktualizovanou normu VDA 4 Zajišťování kvality před sériovou výrobou, kapitola: FMEA produktu a procesu. Norma vyšla v roce 2008 také v českém jazyce.

### 2.3 Charakteristika metody

FMECA je metodou induktivní, která umožňuje provádět kvalitativní a kvantitativní analýzu bezpečnosti a spolehlivosti systému od nižší k vyšší úrovni členění systému a zkoumá, jakým způsobem mohou objekty na nižší úrovni selhat a jaký důsledek mohou mít tato selhání pro vyšší úrovně systému. Nejvýznamnější využití metoda nachází především v etapě návrhu a vývoje, kde slouží jako součást přezkoumání návrhu a sehrává zde roli tzv. metody předběžného varování, která má zabránit pozdějším problémům vyplývajícím z nespolehlivosti systému. Svoje uplatnění však nachází i v etapě tvorby koncepce a specifikace požadavků, jako nástroj předběžné analýzy rizik, a při modifikacích a modernizacích systému nebo při změnách provozních podmínek jako prostředek identifikace a posouzení důsledků konstrukčních změn a provozních podmínek na spolehlivost a bezpečnost systému. Často bývá metoda používána při prokazování, že navrhovaný systém splňuje v oblasti spolehlivosti a bezpečnosti požadavky norem, předpisů nebo uživatele.

Mezi hlavní důvody provádění FMECA je možné zahrnout následující:

- zjištění poruch, které mají nežádoucí důsledky pro provoz systému, např. znemožňují nebo významně zhoršují provoz nebo ovlivňují bezpečnost;
- splnění požadavků smlouvy se zákazníkem, pokud jsou v ní uvedeny;
- možnosti zlepšení bezporuchovosti nebo bezpečnosti systému (např. modifikacemi návrhu nebo opatřeními k zajištění kvality);
- možnosti zlepšení udržovatelnosti systému.

Mezi hlavní cíle provádění FMECA lze zahrnout následující body:

- zevrubná identifikace a vyhodnocení všech nežádoucích důsledků a posloupností událostí, které způsobil zjištěný způsob poruchy systému z jakýchkoliv příčin na rozličných stupních funkční hierarchie systému;
- stanovení kritičnosti nebo významnosti každého způsobu poruchy s ohledem na správnou funkci či technické parametry systému;
- klasifikace zjištěných způsobů poruch podle příslušných charakteristik včetně snadnosti jejich detekce, podle způsobilosti být diagnostikován, podle testovatelnosti, kompenzace poruch a provozních opatření;
- zjištění funkčních poruch systému a odhad míry závažnosti a pravděpodobnosti poruchy;
- tvorba plánu na zlepšení návrhu, aby se zmírnily způsoby poruch;
- podpora tvorby plánu údržby, aby se zmírnily následky nebo aby se snížila pravděpodobnost vzniku poruchy.

Možnosti využití metody FMECA jsou patrné z následujícího přehledu nejvýznamnějších aplikací a přínosů metody:

- poskytnout systematický, přesný a jednotný postup pro pochopení funkcí systému a jeho částí;
- identifikovat všechny potenciálně možné poruchy a určit takové, které, i když se vyskytnou, mají diferencované důsledky (od přijatelných až po nepřijatelné). Dále určit ty způsoby poruch, které mohou významně ovlivnit očekávaný nebo požadovaný provoz;
- stanovit požadavky na zvýšení spolehlivosti a bezpečnosti kritických komponent, zálohování, zjednodušení návrhu, snížení hladin namáhání apod.;
- stanovit požadavky na alternativní řešení, výběr komponent, materiálů, technologií apod.;
- identifikovat poruchy se závažnými až katastrofickými důsledky a vyvolat tím potřebu přezkoumání, případně revize návrhu;
- poskytnout logický model a podklady pro odhady pravděpodobnosti vzniku poruchových provozních stavů nebo nežádoucích provozních podmínek;
- odhalit kritická místa v návrhu a kritické komponenty, u nichž by mohly vzniknout problémy s bezpečností nebo s právní odpovědností za produkt nebo odhalit nesoulad s požadavky předpisů nebo zákazníka;
- poskytnout věcné podklady k tomu, aby zkušebním programem bylo možno odhalit potenciální způsoby poruch;
- odhalit provozní cykly (podmínky, situace), při kterých by mohlo dojít k nežádoucím způsobům poruch, nežádoucí degradaci funkcí a tím umožnit jejich prevenci;
- zaměřit pozornost na klíčové oblasti a prvky řízení kvality, kontrolu výrobního procesu, prvků logistické podpory apod.;
- vyvarovat se pozdějších nákladných modifikací včasnou identifikací nedostatků návrhu;
- stanovit požadavky na sběr údajů pro vývojové, výrobní a provozní zkoušky;
- poskytnout informace pro výběr míst pro preventivní údržbu, pro vypracování typických technologií oprav, pro výběr testovaných míst a vestavěných i externích testovacích zařízení;
- usnadnit nebo zdůvodnit stanovení zkušebních podmínek, programů zkoušek, diagnostických postupů apod.;
- poskytnout věcně zdůvodněné podklady pro opatření v provozu, vedoucí k eliminaci důsledků poruch, pro návrh alternativních způsobů provozu, změn konfigurace provozu apod.;
- usnadnit způsoby řešení problémů mezi všemi partnery a účastníky kontraktu.

Jako snad každá metoda, má i FMECA jisté nedostatky a omezení. Použití metody FMECA může být složité, pracné a časově náročné zejména v případě komplexních systémů, které mají mnoho funkcí a sestávají z mnoha komponentů nebo je-li metoda aplikována na složitý systém poprvé. Jiným omezením je skutečnost, že FMECA a priori nezahrnuje důsledky chyb lidského faktoru. Další omezení se objeví v případě, když se významně projevují vlivy provozních podmínek a prostředí. Uvážení těchto vlivů vyžaduje dokonalou znalost charakteristik, práce a reakce různých komponentů systému na tyto vlivy.

## 3 Postup provádění FMECA

Postup provádění analýzy FMECA lze rozdělit do tří základních částí:

- přípravná část;
- vlastní FMECA jednotlivých komponent systému;
- vyhodnocení analýzy.

### 3.1 Přípravná část

Obsahem této části je shromáždění informací a podkladů potřebných pro provedení vlastní analýzy. K základním informacím, které jsou k provedení analýzy nezbytné, patří zejména:

a) Účel a cíle analýzy.

b) Termíny provedení analýzy.

c) Požadovaná hloubka analýzy.

d) Požadavky na spolehlivost a bezpečnost systému (technické a legislativní požadavky).
e) Informace o struktuře a funkcích systému.
f) Informace o provozních podmínkách (specifikace podmínek provozu, dob a fází provozu).
g) Informace o systému údržby (systém preventivní a nápravné údržby).
h) Informace o podmínkách prostředí.
i) Požadavky na využití softwarové podpory.

***Ad a) Účel a cíle analýzy***

Musí být přesně vymezeno, k jakému účelu je analýza prováděna. Například se analýza provádí proto, aby:

- Bylo možné prokázat, že systém splňuje požadavky na spolehlivost a bezpečnost.
- Byly vyspecifikovány kritické komponenty systému z hlediska nepříznivých důsledků jejich poruchy pro plnění základních funkcí systému.
- Poskytla vstupní informace pro návrh optimálního systému technické údržby a diagnostiky systému.

***Ad c) Požadovaná hloubka analýzy***

Je nezbytné stanovení nejnižší úrovně, která je předmětem analýzy. Všechny komponenty na této úrovni jsou potom pro potřeby analýzy považovány za dále nedělitelné prvky, které plní jasně definované funkce a mají jednoznačně vymezené způsoby poruch. Při volbě nejnižší úrovně analýzy je třeba brát v úvahu zejména:

- stanovený účel a cíle analýzy;
- složitost analyzovaného systému;
- úroveň znalostí o funkcích a způsobech poruch (případně intenzitách poruch) systému na jednotlivých úrovních struktury systému;
- specifikovanou nebo zamýšlenou úroveň nápravné a preventivní údržby;
- možnosti symbolického znázornění (modelování) funkcí systému na jednotlivých úrovních jeho struktury;
- možnosti software použitého pro analýzu.

Obecně lze říci, že nejnižší úroveň analýzy musí být zvolena tak, aby na ní bylo možno věrohodně identifikovat funkce jednotlivých prvků, způsoby jejich selhání a v případě kvantitativního hodnocení i stanovit hodnoty intenzity poruch těchto prvků. Z tohoto pohledu může v rámci jednoho analyzovaného systému prvek představovat jak jednotlivou součást, tak i složitý subsystém. Při analýze je potom každý prvek na zvolené úrovni analýzy považován za tzv. „černou skříňku“, jejíž vnitřní struktura a funkce již nejsou předmětem analýzy.

***Ad e) Informace o struktuře a funkcích systému***

Musí být k dispozici slovní popisy konstrukčního uspořádání a použitého technologického řešení systému, doplněné o podrobnou výkresovou dokumentaci, schémata, grafy apod.

K dispozici musí být také podrobný výčet všech důležitých funkcí systému a komponent, které musí plnit a které musí být podrobeny analýze. Funkce musí být definovány tak, aby bylo možné studovat (modelovat) jejich vzájemné souvislosti, podmíněnost, posloupnost, vazby na provozní podmínky systému. Z definice musí být možné odvodit závažnost důsledků jejich neplnění, možnosti vzájemné oddělitelnosti jednotlivých funkcí apod.

V návaznosti na funkce systému musí být definováno funkční členění systému, které specifikuje, do jakých funkčních subsystémů se systém člení a to až do požadované hloubky analýzy. Funkční členění může být shodné nebo podobné konstrukčnímu členění, ale není to pravidlem. Funkční a konstrukční členění systému je nutné odlišovat, protože produkt jednoho konstrukčního typu může plnit celou řadu odlišných funkcí a tomu musí být přizpůsobeno i odpovídající funkční členění.

Musí být přesně definováno rozhraní systému, které vymezuje hraniční body a komponenty, kde dochází ke vzájemné interakci s okolními systémy nebo s vnějším okolím systému. V nich potom musí být vymezeny okrajové podmínky pro analýzu systému. Definice rozhraní má za cíl vyloučit průniky více systémů tak, aby se stejné analyzované funkce, poruchy apod. neopakovaly vícekrát v různých systémech.

O všech komponentech systému, až do zvolené úrovně, která je určena požadovanou hloubkou analýzy, musí být k dispozici alespoň následující informace:

- jednoznačná identifikace komponent – mohou to být například čísla výkresů, katalogová čísla, čísla prvků na schématech a výkresech apod.;
- popis funkcí komponent;
- popis možných způsobů poruch komponent;
- popis důsledků poruch komponent;
- intenzity (pravděpodobnosti) jednotlivých způsobů poruch komponent (pokud je požadováno provedení kvantitativní analýzy);
- zdroj informací o intenzitách poruch (vyžaduje obvykle zákazník).

### 3.2 Vlastní FMECA jednotlivých komponent systému

Při vlastní analýze se u každého komponentu (prvku) systému (na zvolené nejnižší úrovni) realizují zejména tyto základní kroky:

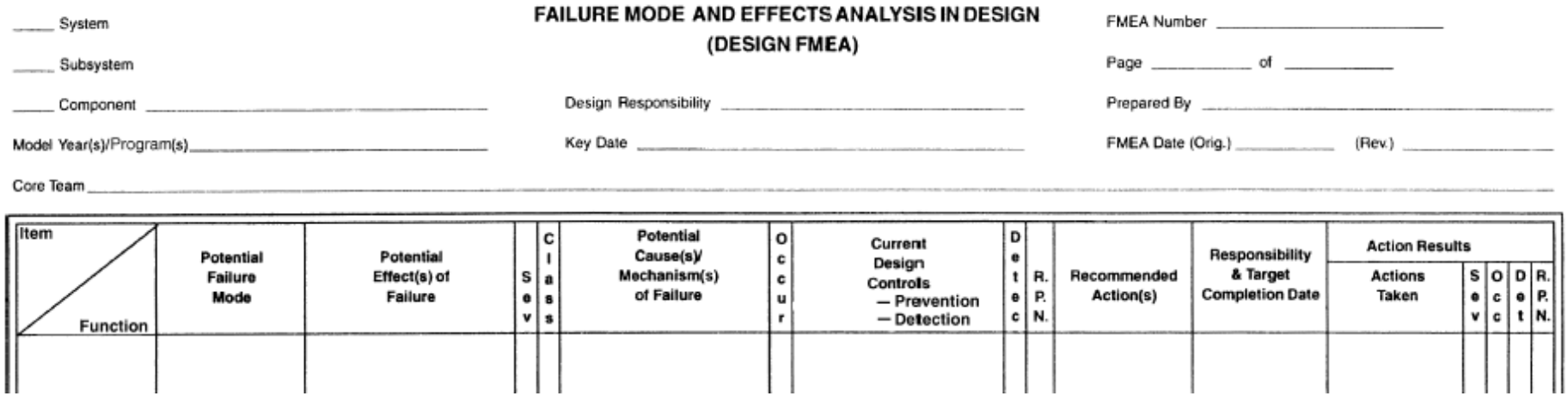
- identifikace způsobů poruch prvku, jejich důsledků a pravděpodobných příčin;
- identifikace metod a opatření k detekci a izolaci poruch;
- kvalitativní posouzení významnosti poruch a alternativní opatření;
- vyhodnocení pravděpodobnosti poruch (v případě kvantitativního hodnocení);
- určení kritičnosti poruch (v případě kvantitativního hodnocení).

Tento základní rozsah analýzy může být podle potřeby rozšířen o další kroky, v rámci kterých se budou účelově zjišťovat (analyzovat) další informace, potřebné pro posouzení spolehlivosti či bezpečnosti systému.

Jednotlivé kroky vlastní analýzy je vhodné zaznamenávat do uspořádaných pracovních formulářů. Použití formulářů, mimo jiné, vytváří předpoklady proto, že analýza bude provedena systematicky, tj. nic nebude opomenuto (každá položka formuláře musí být vyplněna). V současnosti neexistuje žádný závazný předpis, upravující obsah a uspořádání pracovního formuláře pro realizaci FMECA. Uspořádání formuláře může být proto velice různorodé. Některá doporučení a návrhy jsou součástí norem [1], [2], [4]. Vždy by však obsah a uspořádání mělo odpovídat specifickým cílům analýzy a charakteru analyzovaného systémů. Příklady formulářů jsou uvedeny na Obrázku 1 (z ČSN EN 60812 [1]) a Obrázku 2 (z SAE J1739 [4]).

| Koncový objekt:<br>Období provozu: | | | Objekt:<br>Revize: | | | | | Vypracoval:<br>Datum: | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Odkaz na objekt** | **Popis a funkce objektu** | **Způsob poruchy** | **Kód způsobu poruchy** | **Možné příčiny poruchy** | **Místní důsledek** | **Konečný důsledek** | **Metoda detekce** | **Opatření na kompenzaci poruchy** | **Třída závažnosti** | **Četnost nebo pravděpodobnost výskytu** | **Poznámky** |
| | | | | | | | | | | | |

**Obrázek 1 – Příklad formuláře FMECA**



FAILURE MODE AND EFFECTS ANALYSIS IN DESIGN
(DESIGN FMEA)

_____ System
_____ Subsystem
_____ Component _____
Model Year(s)/Program(s) _____
Core Team _____

Design Responsibility _____
Key Date _____

FMEA Number _____
Page _____ of _____
Prepared By _____
FMEA Date (Orig.) _____ (Rev.) _____

| Item / Function | Potential Failure Mode | Potential Effect(s) of Failure | Sev | Class | Potential Cause(s)/ Mechanism(s) of Failure | Occur | Current Design Controls — Prevention — Detection | Detec | R.P.N. | Recommended Action(s) | Responsibility & Target Completion Date | Action Results: Actions Taken | Sev | Occ | Det | R.P.N. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |

**Obrázek 2 – Příklad formuláře FMECA**

Na základní úrovni by měl pracovní formulář umožňovat zaznamenání následujících informací.

***Identifikační číslo prvku***

Musí zajistit jednoznačnou identifikaci prvků v systému a zajistit sjednocení údajů v dokumentaci analýzy s výrobní dokumentací. Vhodné je využít systém identifikace prvků použitý při návrhu systému (např. pozice prvků na výkresu sestavy). Identifikační číslo by mělo umožnit bezpečné rozlišení konstrukčně různých prvků se stejným názvem a identifikaci konstrukčně shodných prvků použitých v různých částech systému. Vedle identifikačního čísla je možno použít další upřesňující údaje, např. čísla výrobních výkresů, sériová čísla, výrobní čísla, označení prvků podle katalogu náhradních dílů, označení prvků v blokových diagramech.

***Název prvku***

Měl by korespondovat s názvem použitým ve výrobní dokumentaci tak, aby se předešlo možným nedorozuměním. Spolu s identifikačním číslem musí zajistit naprosto jednoznačnou identifikaci každého prvku. Pokud je používán pro konstrukčně rozdílné prvky stejný název, musí být název vždy používán s dalšími doplňujícími údaji, které ho jednoznačně identifikují a odlišují od ostatních prvků.

***Funkce prvku***

Funkci prvku je třeba chápat jako činnost, prostřednictvím které plní svůj účel. Je to důvod, pro který existuje. Proto je definice a popis funkcí klíčovou částí analýzy a je nutné definicím funkcí věnovat velkou pozornost. Je nutné definovat jak očekávané a přijatelné způsoby činnosti systému jako celku a základních prvků, z nichž se skládá, tak i charakteristiky činností, které jsou považovány za nepřijatelné a jsou poruchou, chybovou funkcí nebo mezním stavem. Popis funkcí by měl zahrnovat definici přijatelné činnosti pro všechny požadované nebo stanovené charakteristiky při všech provozních i mimo provozních stavech, pro všechna uvažovaná časová období a pro všechny podmínky prostředí. Funkce prvků musí být definovány jak ve vztahu k nadřazenému systému tak i k celému systému.

Součástí definice funkcí je i definování podmínek prostředí a požadavků předpisů. Prostředí (teplota, vlhkost, vibrace, atd.), v němž se předpokládá, že bude systém pracovat, by mělo být jasně definováno i s jeho vlivem na funkce systému a prvků. U systémů řízených a obsluhovaných člověkem by se měly uvážit i vlivy, spojené s lidským faktorem. Do pracovních formulářů se funkce zapisují výstižným a co nejjednodušším způsobem (obvykle jednoslovným, nebo holou větou). Správná formulace funkcí prvku usnadňuje stanovení možných způsobů selhání prvku.

***Způsob poruchy***

Způsob poruchy je definován jako jev, prostřednictvím něhož je porucha na prvku pozorována. Vhodným způsobem se tedy zaznamenávají všechny způsoby, kterými se selhání prvků projeví. Pro každý prvek může být definováno více než jen jeden způsob poruchy, pokud je to žádoucí. Pro zjednodušení celé analýzy a zvýšení srozumitelnosti výsledků analýzy je vhodné provést klasifikaci způsobů poruch, která definuje použitelné způsoby popisu selhání prvků. Příklad klasifikace způsobů poruch je uveden na Obrázku 3 [1]. Další příklady lze nalézt v normách (např. [4]).

| OZN. | ZPŮSOB PORUCHY |
|---|---|
| **1** | **PORUCHA BĚHEM PROVOZU** |
| **2** | **PORUCHA ZAHÁJENÍ PROVOZU V PŘEDEPSANÉM ČASE** |
| **3** | **PORUCHA UKONČENÍ PROVOZU V PŘEDEPSANÉM ČASE** |
| **4** | **PŘEDČASNÝ PROVOZ** |

**Obrázek 3 – Příklad klasifikace způsobů poruch**

Důležité je, aby při analýze byly do úvahy vzaty všechny možné způsoby poruch prvku a žádný nebyl dopředu z analýzy vylučován jen proto, že je krajně nepravděpodobný. Otázka pravděpodobnosti nastoupení jednotlivých způsobů poruch v této části analýzy není podstatná, jediným rozhodujícím kritériem pro zařazení každého způsobu poruchy do analýzy je zde předpoklad možnosti a předpověditelnosti takového způsobu poruchy (bez ohledu na praktickou pravděpodobnost poruchy). To, že do analýzy jsou zahrnuty všechny předpověditelné a reálně možné způsoby poruchy každého prvku je podstatným základem analýzy.

Při definování způsobů poruch je možné využít databázi *FMD-97 – Failure Mode/Mechanism Distributions* [6] (Rozložení způsobů poruch), která obsahuje údaje o pravděpodobnosti výskytu jednotlivých způsobů poruch u konkrétních elektronických, elektrických, elektromechanických a mechanických prvků. Nebo je možno použít novější verzi uvedené databáze, a to databázi *SPIDR™ – System and Part Integrated Data Resource* (Integrovaný zdroj dat o systémech a prvcích).

***Příčina poruchy***

Stanovení příčiny poruchy není původním, ani prioritním cílem analýzy a někdy bývá z analýzy zcela vypuštěno. Je nezbytné stanovit všechny pravděpodobné (možné) příčiny spojené s každým daným způsobem poruch. Identifikace potenciálních příčin každého způsobu poruch se provádí především proto, aby bylo možné odhadnout zdroj jejich výskytu, aby se odhalily sekundární důsledky a aby bylo možné doporučit soubor nápravných opatření. Jelikož způsob poruchy může mít více než jednu příčinu, musí být stanoveny a popsány všechny možné nezávislé příčiny pro každý způsob poruchy.

***Důsledky poruchy***

Analýza důsledků poruch je prioritním cílem analýzy. Zjistí se, vyhodnotí a zaznamenají důsledky všech předpokládaných způsobů poruch jak na činnost, funkci a stav vlastního prvku systému, tak i na všechny vyšší úrovně systému až po úroveň systému jako celku. Podle zvolených kritérií se potom každému důsledku přiřadí stupeň závažnosti. Obvykle se rozlišují důsledky místní (na úrovní prvků) a konečné (na úrovni systému).

V rámci lokálního důsledku se analyzují důsledky poruchy na vlastní prvek. Vyhodnocení těchto důsledků poskytuje výchozí informace pro vyhodnocení alternativních opatření nebo pro doporučení nápravných opatření. V některých případech neexistuje jiný lokální důsledek než sám způsob poruchy.

Pro posouzení konečného důsledku poruchy, tedy důsledku poruchy prvku na činnost, funkci a stav celého systému je nutné vyhodnotit důsledky každé poruchy na všech nižších úrovních. Přitom je nutné brát v úvahu všechny možné kombinace s dalšími poruchami systému, protože porucha jednoho prvku, která sama o sobě může mít nezávažné důsledky, může v kombinaci s jinou poruchou vést ke katastrofickým důsledkům. Proto v pracovních formulářích musí být tyto důsledky vyplývající z násobných poruch také uvedeny.

***Metody detekce poruch***

Je třeba popsat možné způsoby detekce poruch a prostředky, jejichž pomocí je uživatel nebo údržbář informován o poruše. Informace z této části analýzy jsou důležité pro návrh případných preventivních opatření, jakými mohou být například návrhy na vybavení systému přístroji palubní diagnostiky, nebo návrhy do oblasti údržby systému. Zvláštní pozornost je třeba věnovat tak zvaným „skrytým poruchám“ o kterých obsluha není včas informována zabudovaným systémem signalizace a varování a které by mohly svojí existencí způsobit selhání systému až v okamžiku, kdy se od něj očekává plnění jeho funkce.

***Klasifikace závažnosti poruchy***

Klasifikace závažnosti poruchy je posouzení významnosti důsledku způsobu poruchy pro provoz objektu. K tomu je vhodné vytvořit systém kategorizace důsledků poruch, který by pokrýval všechny předpověditelné důsledky jednotlivých poruch systému a umožňoval jednoznačné zařazení

každé poruchy do některé z navržených kategorií. Systém kategorizace důsledků poruch, je vždy třeba přizpůsobit konkrétnímu systému a podmínkám jeho použití.

Příklady klasifikace závažnosti důsledků poruch jsou uvedeny v příspěvku pojednávajícím o předběžné analýze nebezpečí (PHA) [9].

***Pravděpodobnost výskytu poruchy***

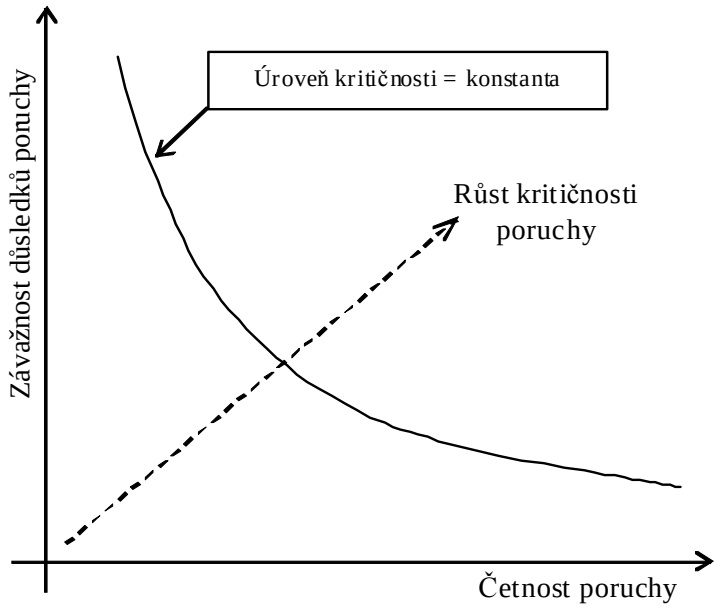
Pro každý způsob poruchy se uvede pravděpodobnost jejího výskytu. Odhad této pravděpodobnosti může být proveden řadou způsobů, například s využitím:

- dat od dodavatelů;
- zkoušek bezporuchovosti;
- dat z provozu (stejných nebo obdobných prvků);
- databází bezporuchovosti (např. NPRD-95, EPRD-97, SPIDR);
- metodik predikce bezporuchovosti (např. MIL-HDBK-217F, FIDES, 217Plus, PRISM);
- expertních odhadů.

Údaje uvedené v této části slouží jako vstupní údaje pro hodnocení kritičnosti poruch a pro případný výpočet pravděpodobností jednotlivých způsobů poruch celého systému, nebo jeho částí. Pokud má analýza ověřit, jestli systém vyhovuje kvantitativním požadavkům na spolehlivost a bezpečnost je znalost pravděpodobnosti jednotlivých způsobů poruch všech prvků systému nezbytná.

***Kritičnost poruchy (riziko)***

Hodnocením kritičnosti poruchy prvku se rozumí „ohodnocení“ závažnosti důsledků daného způsobu poruchy při uvažování jeho četnosti (pravděpodobnosti vzniku). Filozofie hodnocení kritičnosti poruchy je naznačena na Obrázku 4. Konkrétní příklady hodnocení jsou analogické s hodnocením rizika, které je nastíněno v příspěvku pojednávajícím o předběžné analýze nebezpečí (PHA) [9].




**Obrázek 4 – Filosofie hodnocení kritičnosti poruch**

### 3.3 Vyhodnocení analýzy

Vyhodnocení analýzy musí směřovat k přijetí souboru účinných nápravných opatření, zaměřených na odstranění příčin nejzávažnějších typů poruch nebo na snížení stupně jejich závažnosti. Výsledky analýzy se vždy porovnávají s požadavky stanovenými v normách a předpisech (pokud existují) nebo s požadavky, které byly stanoveny pro daný produkt (např. zákazníkem).

Na základě výsledků tohoto porovnání a dalších poznatků získaných při realizaci analýzy se navrhnou konkrétní nápravná opatření. Ke každé poruše a jejím příčinám, pokud to je třeba, se navrhnou taková opatření, která povedou:

- k úplnému odstranění příčin poruchy;
- ke snížení pravděpodobnosti vzniku poruchy;
- ke snížení stupně kritičnosti důsledků poruchy.

Mimo to je možné na základě výstupů z analýzy, pokud je to požadováno, navrhnout:

- zdůvodněný program potřebných zkoušek spolehlivosti kritických prvků;
- účelný systém údržby, zaměřený na předcházení vzniku závažných poruch;
- účelný systém technické diagnostiky, zaměřený na včasné odhalení příčin vzniku poruch.

Mimo tyto základní výstupy lze nalézt celou řadu dalších aplikací, které nebudou, vzhledem omezenému prostoru, dále rozváděny.

## 4 Příklad praktické aplikace metody

V této kapitole je popsána praktická aplikace metody FMECA na příkladu hydraulického ovládání brzd dopravního letounu. Při zpracování příkladu se odkazuji na první příspěvek sborníku [8], ve kterém jsou definovány požadavky na analyzovaný systém a jeho komponenty.

Předpokládá se, že do okamžiku zahájení analýzy metodou FMECA proběhl návrh systému, jenž je podrobně popsán dále, a že při návrhu byly zohledněny výsledky analýzy PHA. Metoda FMECA je aplikována především za účelem posouzení, zda jednotlivé komponenty navrženého systému splňují požadavky na ně kladené.

Při praktické aplikaci metody bude dodržen postup provádění FMECA popsaný v kapitole 0. V rámci omezeného prostoru bude provedena analýza dvou vhodně zvolených komponent systému.

### 4.1 Přípravná část

Obsahem této části je shromáždění informací a podkladů potřebných pro provedení vlastní analýzy. Dále jsou uváděny jen vybrané informace s ohledem k faktu, že se jedná o ukázkový příklad.

***Účel a cíle analýzy***

Prvním cílem analýzy je prokázání splnění požadavků zákazníka v oblasti bezpečnosti a spolehlivosti, které jsou kladeny na jednotlivé komponenty systému (brzdové soustavy dopravního letounu). Druhým cílem je vyspecifikování kritických komponent systému z hlediska nepříznivých důsledků v oblasti bezpečnosti.

***Požadovaná hloubka analýzy***

Hloubka analýzy je jednoznačně dána schématem uvedeným na Obrázku 5, které charakterizuje nejnižší úroveň rozčlenění systému.

***Požadavky na spolehlivost a bezpečnost systému***

Jsou definovány v prvním příspěvku sborníku [8].

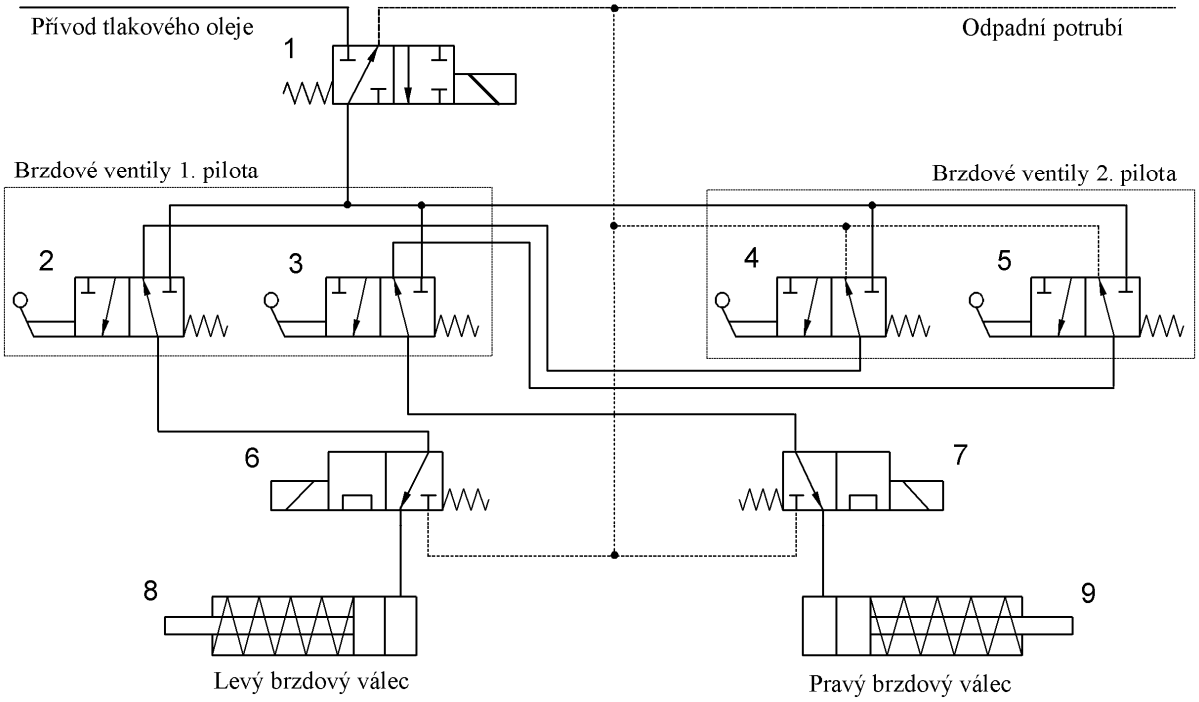
***Informace o struktuře a funkcích systému***

Jedná se o brzdovou soustavu dopravního letounu, jejíž schéma je uvedeno na Obrázku 5.

Hydraulická kapalina je do systému přiváděna přes elektromagnetický rozvaděč 1, který je otevřen, pokud je podvozek letounu zatížen (letoun se pohybuje po zemi). Vlastní brzdění je řízeno buď prvním pilotem brzdovými ventily 2 a 3, nebo druhým pilotem brzdovými ventily 4 a 5. Při ovládání brzdových ventilů má prioritu první pilot. Z brzdových ventilů kapalina proudí do brzdových válců 8 a 9, které přímo ovládají kotoučové brzdy hlavního podvozku letounu. Mezi brzdové ventily a brzdové válce jsou vloženy elektromagnetické ventily 6 a 7, které plní funkci akčních členů systému ABS a které zajišťují krátkodobé přerušování brzdění v případě zablokování a prokluzu kol.

Rozhraními systému jsou: napojení přívodu tlakového oleje; napojení odpadního potrubí; pedály jednotlivých brzdových ventilů; konce brzdových válců.

Veškeré údaje o vhodně zvolených komponentech jsou zaznamenány ve formuláři FMECA (viz. Obrázek 6).




**Obrázek 5 – Zjednodušené schéma hydraulického ovládání brzd letounu**

***Informace o provozních podmínkách***

Systém bude analyzován ve fázi *přistání*, protože jeho funkce je požadována jen při přistání. V jiných fázích provozu se případná porucha systému neprojeví, neboť jeho funkce není vyžadována.

### 4.2 Vlastní FMECA

Výsledky vlastní analýzy dvou vybraných komponent (Elektromagnetický rozvaděč 1, Brzdový ventil 2) jsou zaznamenány ve formuláři uvedeném na Obrázku 6. Pro záznam údajů byl zvolen formulář doporučovaný normou ČSN [1], který byl modifikován s ohledem k potřebám řešeného problému.

Pravděpodobnosti výskytu jednotlivých způsobů poruch byly pro potřeby článku stanoveny způsobem uvedeným v poznámce. Při hodnocení závažnosti konečných důsledků poruch (na úrovni letounu, cestujících a osádky) byla použita kategorizace uvedená na Obrázku 7. Při vyhodnocení kritičnosti poruch byla využita matice kritičnosti uvedená na Obrázku 8. Podrobnosti o možných způsobech kategorizace důsledků poruch a pravděpodobností jejich vzniku lze nalézt v příspěvku pojednávajícím o předběžné analýze nebezpečí (PHA) [9].

| Letoun:<br>Systém: Brzdová soustava | **FMECA**<br>**Analýza způsobů, důsledků a kritičnosti poruch** | List: 1/2<br>Vypracoval: M. Vintr<br>Datum: 20.5.2009<br>Revize: A1 |
|---|---|---|

| Řádek | Prvek | Popis funkce | Způsob poruchy | Důsledek pro systém | Důsledek konečný | Způsob detekce | Intenzita poruch [$h^{-1}$] | Závažnost důsledků | Kritičnost poruchy | Poznámky |
|---|---|---|---|---|---|---|---|---|---|---|
| 1-01 | Elektromag. rozvaděč (1) | Po přivedení napětí na svorky, propouští tlakovou kapalinu do brzdového systému (otevřeno). Po odpojení napětí, uzavírá přívod tlakové kapaliny do brzdového systému (uzavřeno). | Po přivedení napětí se neotevře nebo se samovolně uzavře. (50,0%) | V brzdovém systému není tlak v době, kdy je to požadováno (když je podvozek zatížen). | Letoun nelze brzdit provozními brzdami. (Lze brzdit jinými způsoby). | Skrytá porucha. | $5{,}5 \cdot 10^{-8}$ | Nezávažné | Přijatelná | Zdroj intenzity: MIL-217, EPRD97 |
| 1-02 | Elektromag. rozvaděč (1) | Dtto. | Po odpojení napětí se neuzavře nebo se samovolně otevře. (50,0%) | V brzdovém systému je tlak v době, kdy je to nežádoucí (když není podvozek zatížen). | Možnost dosednutí letounu se zabrzděnými koly (pokud je některý brzdový ventil otevřen před úplným dosednutím letounu). | Skrytá porucha. | $5{,}5 \cdot 10^{-8}$ | Katastrofické | Nepřijatelná | Zdroj intenzity: MIL-217, EPRD97 |
| 2-01 | Brzdový ventil (2) | Po sešlápnutí pedálu brzdového ventilu propouští tlakovou kapalinu k levému brzdovému válci (otevřeno). Po uvolnění pedálu, uzavírá přívod tlakové kapaliny k levému brzdovému válci (uzavřeno). | Nelze přestavit polohu z uzavřeno do otevřeno. (49,3%) | Brzdovým ventilem nelze ovládat brzdění (nelze brzdit) levého brzdového válce. | Možnost nesymetrického brzdění letounu (pokud bude brzdění ovládat 1. pilot). | Skrytá porucha. | $1{,}0 \cdot 10^{-5}$ | Nezávažné | Přijatelná | Zdroj intenzity: Provozní data |

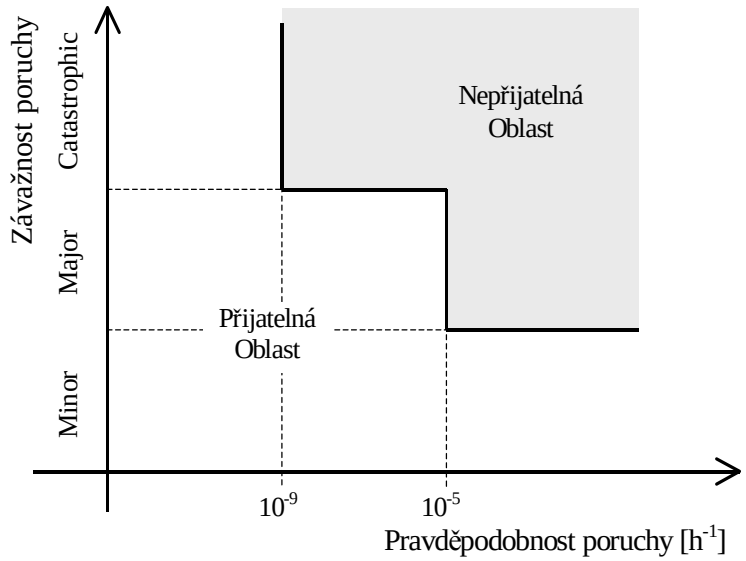
| Letoun: | **FMECA** | List: 2/2 |
|---|---|---|
| Systém: Brzdová soustava | **Analýza způsobů, důsledků a kritičnosti poruch** | Vypracoval: M. Vintr<br>Datum: 20.5.2009<br>Revize: A1 |

| Řádek | Prvek | Popis funkce | Způsob poruchy | Důsledek pro systém | Důsledek konečný | Způsob detekce | Intenzita poruch [$h^{-1}$] | Závažnost důsledků | Kritičnost poruchy | Poznámky |
|---|---|---|---|---|---|---|---|---|---|---|
| 2-02 | Brzdový ventil (2) | Dtto. | Nelze přestavit polohu z otevřeno do uzavřeno. (49,3%) | Brzdovým ventilem nelze přerušit nebo ukončit brzdění levého brzdového válce. | Možnost náhlého nesymetrického brzdění letounu ihned po úplném dosednutí letounu. | Skrytá porucha. | $1,0 \cdot 10^{-5}$ | Závažné | Přijatelná | Zdroj intenzity: Provozní data |
| 2-03 | Brzdový ventil (2) | Dtto. | Samovolné přestavení polohy z uzavřeno do otevřeno. (0,7%) | Nežádoucí (samovolné) brzdění levého brzdového válce. | Možnost náhlého nesymetrického brzdění letounu ihned po úplném dosednutí letounu. | Skrytá porucha. | $1,5 \cdot 10^{-7}$ | Závažné | Přijatelná | Zdroj intenzity: Provozní data |
| 2-04 | Brzdový ventil (2) | Dtto. | Samovolné přestavení polohy z otevřeno do uzavřeno. (0,7%) | Nežádoucí (samovolné) přerušení nebo ukončení brzdění levého brzdového válce. | Nesymetrické brzdění letounu. | Skrytá porucha. | $1,5 \cdot 10^{-7}$ | Nezávažné | Přijatelná | Zdroj intenzity: Provozní data |

**Obrázek 6 – FMECA vybraných komponent**

| Úroveň závažnosti | | Nezávažné (Minor) | Závažné (Major) | Katastrofické (Catastrophic) |
|---|---|---|---|---|
| Popis důsledků | Pro letoun | Mírné snížení funkčních schopností nebo rezerv bezpečnosti | Významné snížení funkčních schopností nebo rezerv bezpečnosti | Poruchové stavy vylučující pokračování v letu a přistání |
| | Pro cestující | Mírné fyzické potíže pro cestující | Fyzické strádání u cestujících | |
| | Pro osádku | Mírný nárůst pracovního zatížení osádky nebo použití nouzových postupů | Fyzické potíže nebo značný nárůst pracovní zátěže | |

**Obrázek 7 – Kategorizace důsledků poruch**




**Obrázek 8 – Matice kritičnosti poruch**

### 4.3 Vyhodnocení analýzy

Z výše uvedené analýzy dvou vybraných komponent (Elektromagnetický rozvaděč 1, Brzdový ventil 2) je patrné, že analyzovaný systém (brzdová soustava letounu) a některé jeho komponenty nesplňují požadavky na ně kladené. Konkrétně byla kritičnost způsobu poruchy elektromagnetického rozvaděče uvedeného na řádku 1-02 klasifikována jako nepřijatelná.

Na základě výsledků analýzy je nezbytné provést změny v návrhu systému (např. zabudování výstražné signalizace) a předepsat adekvátní údržbu kritických komponent, aby došlo ke splnění stanovených požadavků.

## 5 Závěr

V příspěvku je představena a popsána jedna z nejpoužívanějších metod v oblasti hodnocení spolehlivosti a bezpečnosti – FMECA. V závěrečné části příspěvku je na příkladu brzdového systému dopravního letounu předvedena praktická aplikace metody.

Je nezbytné podotknout, že pro komplexní zhodnocení spolehlivosti a bezpečnosti jakéhokoliv systému musí být metoda FMECA použita ve vhodné kombinaci s dalšími metodami, z nichž nejpoužívanější jsou představeny v tomto sborníku.

## Použité zdroje


[1] ČSN EN 60812 (01 0675). *Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA).* Praha: Český normalizační institut, 2007.

[2] MIL-STD-1629A. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis.* Washington: Department of Defense, 1984.

[3] SAE ARP5580. *Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications.* Warrendale: Society of Automotive Engineers, 2001.

[4] SAE J1739. *Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery (Machinery FMEA).* Warrendale: Society of Automotive Engineers, 2002.

[5] HOLUB, R. – VINTR, Z. *Základy spolehlivosti.* 1. vyd. Brno: Vojenská akademie v Brně, 2002.

[6] *Failure Mode/Mechanism Distributions (FMD-97).* Rome: Reliability Analysis Center (RAC), 1998.

[7] http://elsmar.com/

[8] VINTR, Z. *Základní filozofie průkazu spolehlivosti a bezpečnosti technického systému v počátečních etapách životního cyklu.* 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009.

[9] VALIŠ, D. *Předběžná analýza nebezpečí – základ racionálního návrhu systému.* 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009.

[10] HLINKA, J. *Modelování spolehlivosti a bezpečnosti systému jako celku.* 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009.

# Modelování spolehlivosti a bezpečnosti systému jako celku

***Doc. Ing. Jiří HLINKA, Ph.D.***
*Vysoké učení technické v Brně, Fakulta strojního inženýrství*
*Technická 2896/2, 616 69 Brno, Email: hlinka@fme.vutbr.cz.*

**Použité značení:**

$\lambda$ – *intenzita poruch (failure rate)*

$\mu$– *intenzita opravy (repair rate)*

A($\infty$) – *součinitel asymptotické pohotovosti (asymptotic availability)*

R – *pravděpodobnost bezporuchového provozu (reliability)*

n – *počet prvků v systému*

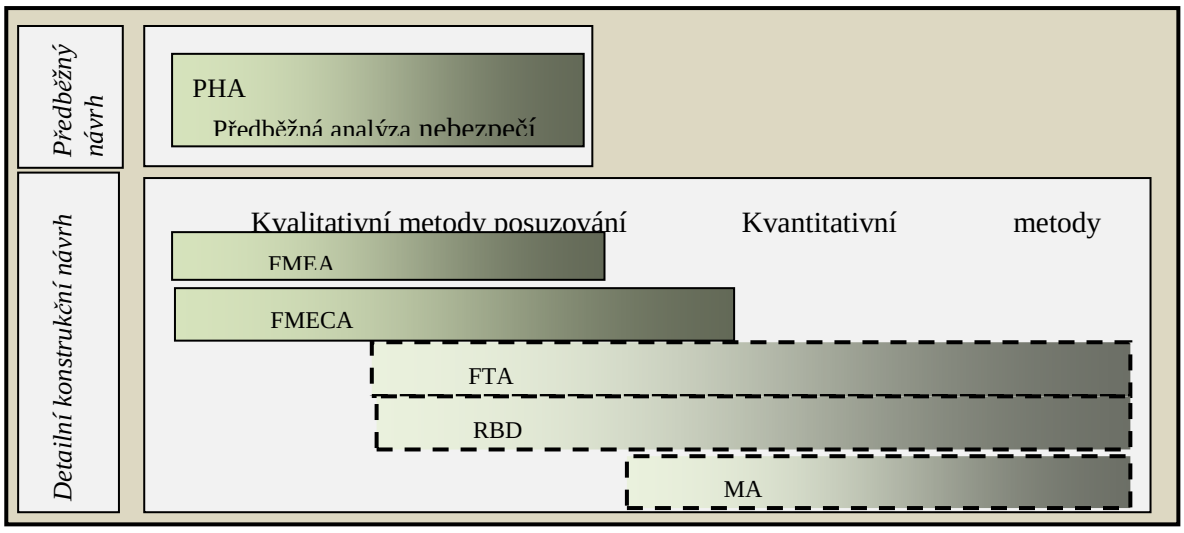
| | | | |
|---|---|---|---|
| PHA | *Předběžná analýza nebezpečí* | RBD | *Blokové diagramy bezporuchovosti* |
| FMEA | *Analýza druhů poruch. stavů a jejich důsledků* | SSM | *Analýza prostorů a stavů* |
| FMECA | *Analýza druhů, důsl. a kritičnosti poruch. stavů* | ETA | *Analýza pomocí stromů událostí* |
| FTA | *Analýza pomocí stromu poruchových stavů* | FHA | *Rozbor funkčních rizik* |

## 1 Úvod

Příspěvek je součástí rozsáhlejšího souboru příspěvků popisujících metody prediktivních analýz pro zajištění spolehlivosti a bezpečnosti technických systémů. Předcházející příspěvky se zabývaly různými postupy zajišťujícími požadovanou úroveň spolehlivosti v průběhu předběžného návrhu a detailního návrhu moderních technických systémů. Oblast předběžného návrhu pokrývaly zejména metody předběžných analýz nebezpečí (PHA). Z oblasti detailního návrhu pak byla prezentována zejména metoda FMEA, popř. FMECA, sledující posuzování důsledků jednotlivých poruch prvků.

Předchozí témata budou doplněna o souhrn metod posuzování bezpečnosti a spolehlivosti systému jako celku. Bude se zaměřovat zejména na analýzy neopravovaných systémů (plnících kritické funkce). Praktická realizace bude demonstrována na příkladu brzdové soustavy dopravního letadla.

Vymezení oblasti zájmu příspěvku je patrné ze zjednodušeného grafického znázornění vybraných metod analýz spolehlivosti a bezpečnosti, viz. obr. 1.




**Obr. 1 Výběr metod, které jsou předmětem zájmu příspěvku (ohraničeny čárkovaně) a jejich vymezení vůči ostatním metodám, kterým je věnován soubor příspěvků**

**Cílem příspěvku není poskytnutí vyčerpávající informace o metodách a postupech jejich řešení. Příspěvek je spíše věnován možnostem využití různých metod v různých obdobích návrhu nového produktu.** Dalším cílem pak je seznámení čtenářů s praktickým využíváním metod v různých průmyslových oborech.

Samostatnou kapitolou je aplikace vybraných metod na příkladu brzdové soustavy dopravního letounu.

## 2 Metody modelování složitých poruchových stavů systémů

Historicky bylo vytvořeno velké množství různých metod, které si kladly za cíl modelovat parametry spolehlivosti a provést kvalitativní nebo kvantitativní hodnocení úrovně spolehlivosti systému jako celku.

Metody analýz lze v zásadě rozdělit do dvou skupin: Na analýzy opravovaných systémů a na analýzy neopravovaných systémů. Velmi často se v průmyslu používají **analýzy neopravovaných systémů**. Jejich použití není pouze u výrobků, které se po poruše neopravují, ale obecně ve všech kritických aplikacích z hlediska bezpečnosti. Např. u kritických systémů letadel není možné po poruše kritického systému provádět opravy za letu. V průběhu návrhu se tedy k takovému kritickému systému přistupuje jako k neopravovanému, u kterého je nutné zajistit bezpečnou funkci po dobu letu.

Poté, co je zajištěna akceptovatelná úroveň spolehlivosti kritických funkcí, se zájem obvykle obrací k optimalizaci provozních a ekonomických parametrů (se zahrnutím vlivů údržby). V této fázi jsou důležité **analýzy opravovaných systémů**.

**V příspěvku bude důraz kladen zejména na metody analýz neopravovaných systémů**.

Nejrozšířenějšími metodami modelování chování systémů se v průběhu času staly následující metody:

- **Reliability Block Diagrams (RBD)** – *Blokové diagramy bezporuchovosti* – metoda kvalitativní a kvantitativní analýzy široce používaná v průmyslu (obvykle pro analýzy neopravovaných systémů). Bližší informace o metodě jsou uvedeny v kapitole 3.
- **Fault Tree Analysis (FTA)** – *Analýza pomocí stromu poruchových stavů* – obdobně jako RBD jde o metodu kvalitativní a kvantitativní analýzy široce používanou v průmyslu (obvykle pro analýzy neopravovaných systémů). Bližší informace o metodě jsou uvedeny v kapitole 4. Často se také aplikuje provázání metody s Markovovými technikami do tzv. dynamických stromů.
- **Truth Table Method** – *Pravdivostní tabulka* – používá se často ve spolupráci s blokovými diagramy. Někdy je také uváděna jako jedna z metod řešení RBD. Častěji je ovšem v literatuře uváděna samostatně. Princip spočívá v sestavení a řešení všech kombinací stavů prvků systému.
- **State Space Methods (SSM)** – *Analýza prostorů a stavů* – metoda používaná obvykle k analýzám opravovaných systémů nebo tam, kde není možné použít RBD či FTA. Řešení lze provádět za pomoci Markovových technik, ale existují i ne-Markovovské (non-Markovian) techniky. Pro získání bližších informací o použití Markovových technik je možné využít například normu ČSN EN 61165 [3]. Tato norma je použitelná ve všech průmyslových odvětvích, ve kterých je nutné analyzovat systémy, které vykazují chování závislé na stavu. Rozsáhlý materiál o řešení metodou SSM je uveden rovněž v lit. [4].
- **Event Tree Analysis (ETA)** – *Analýza pomocí stromů událostí* – metoda kvalitativní a kvantitativní analýzy. Poprvé byla aplikována mezi lety 1972 a 1975 v jaderném průmyslu. V tomto průmyslovém odvětví je také nejrozšířenější.

Souhrn nejčastěji uváděných výhod a nevýhod metod je uveden v tab. 1. Vzhledem k obrovské šíři nástrojů řešení různých metod, nemusí vyjmenovaná základní omezení mít vždy absolutní platnost. Výhody a nevýhody jsou sestaveny tak, jak jsou při běžném průmyslovém využití nejčastěji vnímány (a popsány v literatuře).

***Tab. 1** Přehled hlavních výhod a nevýhod vybraných metod analýz (popis vychází z [5] s modifikacemi)*

| **Blokové diagramy bezporuchovosti (RBD)** | **Stromy poruchových stavů (FTA)** |
|---|---|
| Výhody:<br>- Často umožňuje téměř přímou konstrukci blokového diagramu z funkčního diagramu<br>- Umožňuje snadnou identifikaci kombinací poruch vedoucích k selháním systému<br>- Umožňuje snadný odhad bezporuchovosti u neopravovaných systémů.<br>- Částečně umožňuje řešení vybraných opravovaných systémů. | Výhody:<br>- Identifikuje všechny příčiny poruch vedoucí k nežádoucím vrcholovým událostem (významně pomáhá analytikovi sestavit všechny kombinace jevů vedoucí ke sledované vrcholové události)<br>- Identifikuje některé závislosti mezi poruchami<br>- Poskytuje seznam minimálních kritických řezů<br>- Umožňuje odhad pravděpodobnosti nastoupení nežádoucí události<br>- Je možné jej aplikovat na širokou škálu různých systémů<br>- Částečně umožňuje řešení vybraných opravovaných systémů. |
| Nevýhody:<br>- Není přizpůsobeno pro řešení složitých opravovaných systémů s komplikovanými strategiemi údržby<br>- Problematické řešení úloh s nutností zahrnutí časové posloupnosti událostí<br>- Neumožňuje analýzu vztahů mezi příčinami a důsledky poruch | Nevýhody:<br>- Může vést k velmi velkým stromům, nezvladatelným i při použití specializovaného softwaru.<br>- Není přizpůsobeno pro řešení složitých opravovaných systémů s komplikovanými strategiemi údržby |
| **Stromy událostí (ETA)** | **Analýza prostorů a stavů (SSM)** |
| Výhody:<br>- Identifikuje všechny možné důsledky počáteční události<br>- Poskytuje pravděpodobnosti nastání nechtěných sekvencí událostí<br>- Ukazuje interakce mezi elementárními systémy | Výhody:<br>-Identifikuje všechny funkční i poruchové stavy opravovaných systémů včetně přechodů mezi nimi<br>-Poskytuje informace o bezporuchovosti, pohotovosti a udržovatelnosti opravovaného systému<br>-Bere v úvahu složité strategie údržby. |
| Nevýhody:<br>- Neumožňuje prokázat, že byly zahrnuty všechny iniciující události<br>- Metoda by měla být použita dohromady s jinými metodami pro analýzy generických událostí<br>- Neumožňuje řešení velmi složitých strategií údržby | Nevýhody:<br>- Kvantitativní analýza se může rychle stát velmi komplikovanou pro systémy s velkým počtem stavů (již systémy s omezeným počtem prvků mohou mít velký počet různých stavů; podstatné omezení přehlednosti modelu a jeho práce s ním) |

Příklad využití různých metod ve specifickém odvětví – letectví – je uveden v tab. 2. Z tabulky je možné vyčíst použití metod u různých výrobců letadel s důrazem na domácí průmysl. Blíže budou rozebrány zejména dvě nejpoužívanější metody analýzy, RBD a FTA. Jejich bližší popis je předmětem kapitol 3 a 4.

Z hlediska průmyslové aplikace je velmi důležitá také možnost **kvalitativního a kvantitativního vyhodnocení** metod.

### 2.1 Kvalitativní vyhodnocení

Oproti čistě kvalitativním metodám typu PHA, FMEA je při modelování bezpečnosti a spolehlivosti systému jako celku metodami FTA, RBD, apod. obvykle spíše důležité vyhodnocení kombinací poruchových stavů prvků vedoucí ke sledované události.

Nejčastěji jde o vyhodnocení tzv. **„kritických řezů“** nebo **„minimálních kritických řezů“**. Kritickými řezy rozumíme kombinace selhání prvků, které vedou na sledovaný poruchový stav. Minimálními kritickými řezy potom kombinace selhání nejmenšího počtu prvků, které vede na sledovaný poruchový stav. **Pro průkaz bezpečnosti a spolehlivosti analyzovaného systému je potom obvykle podstatné jaké kombinace poruch vedou ke vzniku poruchového stavu.**

*Například v letectví je požadováno, aby selhání systému vedoucí ke katastrofickým poruchovým stavům nemohlo vzniknout v důsledku selhání samostatného prvku.* Poruchové stavy s katastrofickými důsledky jsou obvykle identifikovány pomocí metod PHA (FHA) nebo FMEA. Analýza kombinací selhání prvků, které na tyto poruchové stavy vedou se však již obvykle provádí za pomoci kvalitativního vyhodnocení RBD (blokových diagramů bezporuchovosti) či FTA (stromů poruchových stavů).

***Tab. 2** Příklad využití běžných metod analýz spolehlivosti v oblasti leteckého průmyslu*

| Metoda | Použití |
|---|---|
| **RBD** *(Blokové diagramy bezporuchovosti)* | Používají se velmi často k modelování a analýzám složitých poruchových stavů, kdy dojde k současnému selhání několika prvků. Blokové diagramy využíval v minulosti LET Kunovice, v současnosti metodu v České republice využívá zejména společnost EVEKTOR (zaměřená na vývoj a výrobu malých sportovních a malých dopravních letadel). |
| **FTA** *(Analýza pomocí stromů poruchových stavů)* | Princip základního použití metody je v podstatě stejný jako u blokových diagramů bezporuchovosti. Z domácích výrobců metodu v minulosti využilo například Aero Vodochody, ve světě je to zejména společnost Boeing, ale také další výrobci. |
| **MA** *(Markovovy techniky)* | Používají se k analýzám velmi složitých poruchových stavů, obvykle tam, kde není možné použít metody FTA nebo RBD. Často jsou také kombinovány s FTA (dynamické FTA). Metoda je předmětem výzkumu např. v NASA, ale i u nás (VZLÚ Praha) a byla omezeně využita také v Aero Vodochody. |

### 2.2 Kvantitativní vyhodnocení

V rámci kvantitativní analýzy se provádí výpočet (odhad) kvantitativních (číselných) hodnot vybraných parametrů spolehlivosti, např. pravděpodobnosti nastoupení poruchového stavu, intenzity poruch, apod. [6]. Vzhledem k tomu, že samotný model a všechny předchozí veličiny mají ze své podstaty stochastickou povahu, řídí se stochastickými zákony a jsou proto zatíženy určitou „nejistotou“ ve svých vlastnostech, bude i výsledek analýzy zatížen jistým rizikem nejistoty v závěrech a doporučeních.

Kvantitativní analýzy je možné obecně provádět „ručně“ pokud jsou systémy jednoduché a ne příliš rozsáhlé, jinak se provádí pomocí výpočetní techniky a speciálních, k tomu účelu vypracovaných programů [6].

## 3 Blokové diagramy bezporuchovosti (RBD)

Blokové diagramy bezporuchovosti byly historicky první metodou pro analýzy spolehlivosti a bezpečnosti systému jako celku. Kořeny této metody pravděpodobně sahají zpět do doby, kdy se začínala formovat teorie spolehlivosti a související matematické nástroje [4]. V 60-tých letech se ukázalo, že samotné blokové diagramy nejsou dostatečným nástrojem pro řešení problémů spolehlivosti a došlo k rozvoji dalších metod, např. FTA a FMEA. Použití blokových diagramů bezporuchovosti je však stále rozsáhlé a tato metoda patří k základním metodám řešení neopravovaných systémů. V některých případech je využitelná i pro analýzy opravovaných systémů. **Lze ji použít jak pro kvalitativní vyhodnocení, tak pro kvantitativní vyhodnocení**.

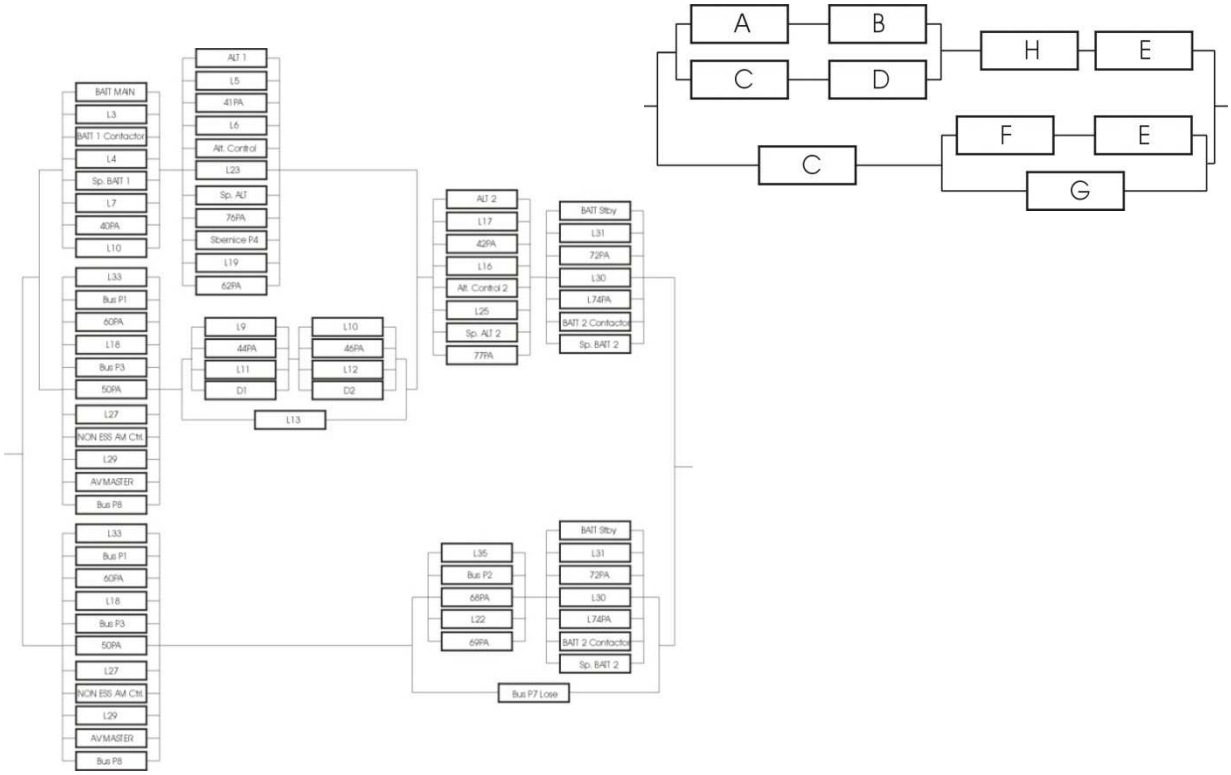
**Parts Count Method:**

Speciálním případem je metoda nazývaná nejčastěji **„Parts Count Method“**, která je rovněž hojně využívaná. Metoda předpokládá, že systém funguje, pouze pokud fungují všechny jeho komponenty (sériové uspořádání prvků v systému). Intenzitu poruch systému pak tvoří suma intenzit poruch komponentů: $\lambda_S = \sum_{i=1}^{n} \lambda_i$ (2.1) [14]. Používá se často tam, kde je k dispozici informace o počtu a typu prvků v systému, ovšem vytvoření blokového

**Blokové diagramy bezporuchovosti jsou často s výhodou používány pro modelování vybraných funkcí elektrických obvodů a logických obvodů**, kde lze vycházet i z konstrukčních schémat těchto obvodů.

**Blokový diagram bezporuchovosti (RBD) je podle definice ČSN EN 61078 [1] obrazová reprezentace bezporuchovosti systému. Znázorňuje logické spojení (fungujících) součástí potřebných pro úspěšný provoz systému (který se dále označuje jako „úspěch systému“).** Technika modelování RBD se má používat především u systémů bez opravy a v případech, kdy nezáleží na pořadí vzniku poruch. U systémů, v nichž je nutné brát v úvahu pořadí vzniku poruch, nebo když se u nich mají provádět opravy, je vhodnější použít jiné techniky modelování, jako je Markovova analýza.

V některých oborech je mnohem používanější modelování poruch (místo bezporuchovosti). Například v letectví jsou analyzovány vybrané poruchové stavy a **blokové diagramy poruch** představují efektivnější nástroj analýzy než klasické RBD. Samotné grafické vyjádření blokového diagramu se v tomto případě neliší, liší se pouze význam bloků. V blokových diagramech poruch jednotlivé bloky reprezentují „prvky, které musí selhat pro nastoupení sledovaného poruchového stavu“. Ukázka blokového diagramu poruch je na obrázku 2.




**Obr. 2 Úplný blokový diagram poruchového stavu (výpadek kritických letových ukazatelů u malého sportovního a turistického letounu s katastrofickými důsledky) – vlevo dole; a jeho zjednodušená podoba pro kvantitativní vyhodnocení – vpravo nahoře**

V nejjednodušší formě se např. výpočet bezporuchovosti z blokových diagramů provádí s využitím základních vztahů pro sériové (2.2) a paralelní systémy (2.3).

$$R_S = \prod_{i=1}^{i=N} R_i \tag{2.2}$$

$$R_S = 1 - \prod_{i=1}^{i=N} (1 - R_i) \tag{2.3}$$

Moderní matematické nástroje potom nabízejí širokou škálu metod řešení blokových diagramů tam, kde není možné aplikovat tyto jednoduché metody. Například za předpokladu, že všechny poruchové stavy v blokovém diagramu jsou nezávislé, lze blokový diagram z obr. 2 popsat pomocí následujícího jevového zápisu:

$$S = H \cap E \cap (A \cap B \cup C \cap D) \cup C \cap (G \cup E \cap F) \tag{2.4}$$

Řešení je potom možné s využitím pravděpodobnostního počtu a Booleovy algebry.

Rozsáhlejší a detailnější rozbor metod řešení blokových diagramů je mimo rozsah příspěvku. S využitím moderních softwarových prostředků je ovšem možné řešit prakticky libovolný blokový diagram (ať už bezporuchovosti nebo poruchy). Bližší informace o metodách řešení blokových diagramů je mimo výše zmiňované normy možné najít např. v [4], [6], [14].

Blokové diagramy bezporuchovosti mohou být za určitých omezených podmínek použity i pro **řešení opravovaných systémů** [4]. Lze tak provádět odhad bezporuchovosti, pohotovosti nebo parametrů údržby. Základními omezeními, pro řešení opravovaných systémů pomocí blokových diagramů bezporuchovosti jsou:

- *Žádný prvek (blok) se nesmí v blokovém diagramu vyskytovat více než jednou*
- *Je uvažováno, že je k dispozici tolik pracovníků údržby, kolik je prvků komponent; strategie údržby musí být vzájemně nezávislé*
- *V systému je obsažena pouze „aktivní záloha“*

Nejjednodušším postupem řešení je potom aplikace zjednodušeného vztahu (2.5) pro odhad asymptotické pohotovosti A(∞) sériového systému a (2.6) pro odhad asymptotické pohotovosti paralelního systému [4].

$$A(\infty) \cong 1 - \sum_{i=1}^{n} \frac{\lambda_i}{\mu_i} \tag{2.5}*$$

$$A(\infty) \cong 1 - \prod_{i=1}^{n} \frac{\lambda_i}{\mu_i} \tag{2.6}*$$

* Vztah platí za předpokladu platnosti zjednodušení: $\lambda_i / \mu_i \ll 1$; dále za předpokladu, že $\lambda$ a $\mu$ jsou v čase konstantní

## 4 Stromy poruchových stavů (FTA)

**Historie metody:**

Analýza pomocí metody stromů poruchových stavů byla vyvinuta panem H.A. Watsonem z Bell Telephone Laboratories. Poprvé ji použil v roce 1961-62 při analýze bezporuchovosti startovacího systému rakety Minuteman [4]. Tato aplikace byla považována za úspěšnou a využití FTA bylo panem D. Haaslem (ze společnosti Boeing) rozšířeno na celou raketu Minuteman. Poté ji převzaly další divize Boeingu a aplikovaly při návrhu civilních dopravních letadel [8]. V roce 1965 byla metoda široce publikována díky konferenci, kterou pořádala Washingtonská univerzita (a sponzorovala firma Boeing).

Další významná průmyslová oblast, která začala používat metodu FTA po leteckém průmyslu byla jaderná energetika. Poté se metoda rozšířila i do chemického průmyslu, automobilního a železničního průmyslu a dalších odvětví.


V roce 1967, po katastrofickém požáru kosmické lodi Apollo 1 najala NASA společnost Boeing

**Analýza stromu poruchových stavů (FTA - Fault tree analysis) se podle definice v ČSN EN 61025 [2] zabývá identifikací a analýzou podmínek a faktorů, které způsobují nebo mohou potenciálně způsobit výskyt nebo přispívat k výskytu specifikované vrcholové události.** Při analýze FTA je touto událostí obvykle „zadření“ nebo zhoršené fungování systému, snížení bezpečnosti nebo zhoršení jiných důležitých provozních atributů, zatímco při analýze STA (Success Tree Analysis - analýze stromu úspěchů) je touto událostí atribut popisující úspěch (bezporuchový stav).

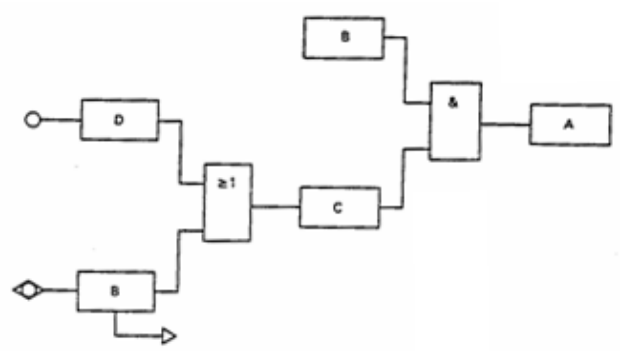
FTA se často uplatňuje při analýze bezpečnosti systémů (jako jsou dopravní systémy, elektrárny nebo jakékoliv jiné systémy, u kterých se vyžaduje vyhodnocení bezpečnosti jejich provozu). Analýzu stromu poruchových stavů lze též použít pro analýzu pohotovosti a udržovatelnosti.

Mimo citované normy mají některá průmyslová odvětví vlastní specifické dokumenty, které definují a popisují metodu (včetně postupů analýz). Například v letectví je takovým dokumentem SAE ARP 4761 [7], který kromě základní definice objasňuje i doporučený způsob použití. V tomto případě jde zejména o „identifikaci samostatných poruch a kombinací poruch, které mohou nastat“ a dále pak o „kvantifikaci pravděpodobnosti nastoupení vrcholové události“, „průkaz plnění kvalitativních a kvantitativních požadavků“, atd.

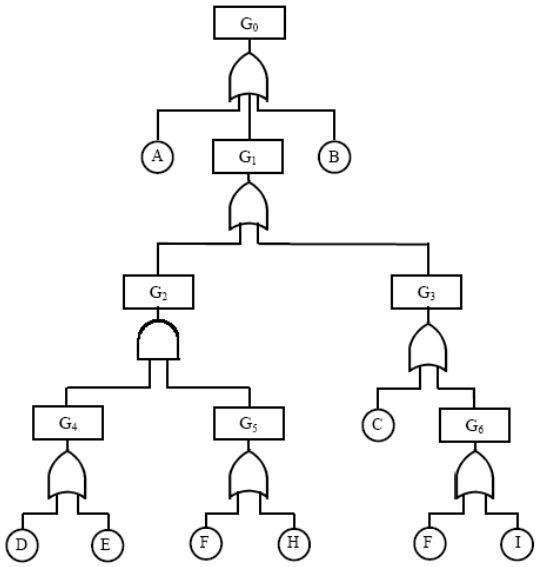
Při aplikaci metody stromu poruchových stavů jsou k dispozici dva základní způsoby vyhodnocení, ***kvalitativní*** a ***kvantitativní***.

Kvalitativní přístup, při kterém se pravděpodobnost události a faktorů, které k ní přispívají (vstupních událostí), nebo jejich četnost výskytu nesleduje je také znám jako tradiční FTA. Široce se používá v aplikacích v jaderném průmyslu a v mnoha jiných případech, kdy se hledají potenciální příčiny poruchových stavů [2].

Druhý přístup, který se přejímá v mnoha průmyslových odvětvích, je převážně kvantitativní přístup, při kterém se pomocí podrobné analýzy FTA modeluje celý produkt, proces nebo systém, a velká většina základních událostí, ať již poruchových stavů, nebo událostí, má v modelu nějakou pravděpodobnost výskytu stanovenou pomocí analýzy nebo zkoušky. V tomto případě je konečným výsledkem pravděpodobnost výskytu vrcholové události reprezentující pravděpodobnost bezporuchového provozu nebo pravděpodobnost poruchového stavu či poruchy [2].



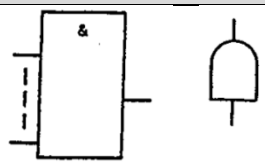
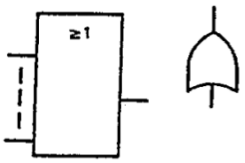
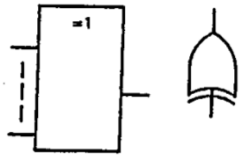
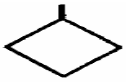
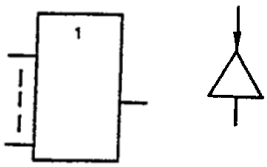
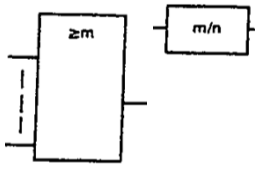
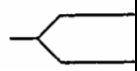
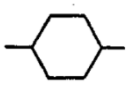
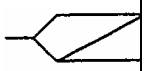
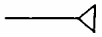

**Obr. 3 Ukázka jedné z možných variant grafického zpracování stromu poruchových stavů – starší norma ČSN IEC 1025 (vlevo)**




**Obr. 4 Jiná (obvyklejší) varianta grafického zpracování stromu poruchových stavů - [6]**

Pro praktickou tvorbu stromu poruchových stavů byla vytvořena celá řada grafických „symbolů“ (zobrazení hradel), které umožňují postihnout širokou paletu kombinací základních událostí. Jejich stručný výčet je v tab. 3, ze které je také možné udělat si představu o možnostech řešení a využitím stromů poruchových stavů. Praktická tvorba stromu poruchových stavů bude patrná z kapitoly 5 (aplikace na brzdové soustavě dopravního letounu).

***Tab. 3** Hradla používaná v konstrukci stromů poruchových stavů*

<table>
<tr><td colspan="2">A (AND)</td><td colspan="2">Blok pro popis události (Event description block)</td></tr>
<tr><td> 
</td><td>Událost nastane pouze tehdy, když nastanou všechny dostupné události.</td><td>  </td><td>Název nebo popis událostí; kód událostí a pravděpodobnost výskytu (pokud se požaduje) se má uvést mezi značkami.</td></tr>
<tr><td colspan="2">Nebo (OR)</td><td colspan="2">Základní událost (Basic event)</td></tr>
<tr><td> 
</td><td>Událost nastane pouze tehdy, když nastane libovolná vstupní událost, a to sama nebo libovolná kombinace událostí.</td><td>  </td><td>Událost, která se dále nedělí.</td></tr>
<tr><td colspan="2">Nonekvivalence (Exclusive-OR)</td><td colspan="2">Nerozvíjená událost (Undeveloped event)</td></tr>
<tr><td> 
</td><td>Událost nastane pouze tehdy, když jedna vstupní událost nastane sama.</td><td>  </td><td>Událost, která nebyla dále dělena (obyčejně proto, že se to nepovažovalo za nutné)</td></tr>
<tr><td colspan="2">Ne (NOT)</td><td colspan="2">Událost analyzovaná jinde (Analyzed elsewhere)</td></tr>
<tr><td> 
</td><td>Událost reprezentuje podmínku, která je inverzní k podmínce definované jako vstupní událost.</td><td>  </td><td>Událost, která je dále rozvíjena v jiném stromu poruchových stavů.</td></tr>
<tr><td colspan="2">m/n (Redundant structure)</td><td colspan="2">Dům (House)</td></tr>
<tr><td> 
</td><td>Událost nastane tehdy, pokud nastane minimálně m z n vstupních událostí.</td><td>  </td><td>Událost, která určitě nastala nebo určitě nastane.</td></tr>
<tr><td colspan="2">Zdržení (INHIBIT)</td><td colspan="2">Nulová událost (Zero Event)</td></tr>
<tr><td rowspan="5">  </td><td rowspan="5">Událost nastane pouze tehdy, když společně působí vstupní událost a událost spojená s platností podmínky uvnitř hradla.<br>Pokud je událost spojená s jinou podmínkou, hradlo INHIBIT zavede časování událostí.</td><td>  </td><td>Událost, která určitě nastala nebo nastane.</td></tr>
<tr><td colspan="2">Přenos do (Transfer-in)</td></tr>
<tr><td>  </td><td>Událost definovaná kdekoliv ve stromě poruch.</td></tr>
<tr><td colspan="2">Přenos ven (Transfer-out)</td></tr>
<tr><td>  </td><td>Událost definovaná kdekoliv ve stromě poruch.</td></tr>
</table>

## 5 Poruchové stavy brzdové soustavy dopravního letounu (praktický příklad)

Pro demonstraci praktické aplikace stromu poruchových stavů bude použit stejný příklad jako v souvisejících příspěvcích [15],[16] a [17]. Jde o brzdovou soustavu dopravního letounu, viz. obr. 5. K přiblížení vlastního řešení je nezbytné alespoň základní objasnění funkce systému:

*Hydraulická kapalina je do systému přiváděna přes elektromagnetický rozvaděč 1, který je otevřen pokud je podvozek letounu zatížen (letoun se pohybuje po zemi). Vlastní brzdění je řízeno buď prvním pilotem brzdovými ventily 2 a 3, nebo druhým pilotem brzdovými ventily 4 a 5. Při ovládání brzdových ventilů má prioritu první pilot. Z brzdových ventilů kapalina proudí do brzdových válců 8 a 9, které přímo ovládají kotoučové brzdy hlavního podvozku letounu. Mezi brzdové ventily a brzdové válce jsou vloženy elektromagnetické ventily 6 a 7, které plní funkci akčních členů systému ABS a které zajišťují krátkodobé přerušování brzdění v případě zablokování a prokluzu kol.*

**Při předběžné analýze rizik byl identifikován zejména následující poruchový stav:**

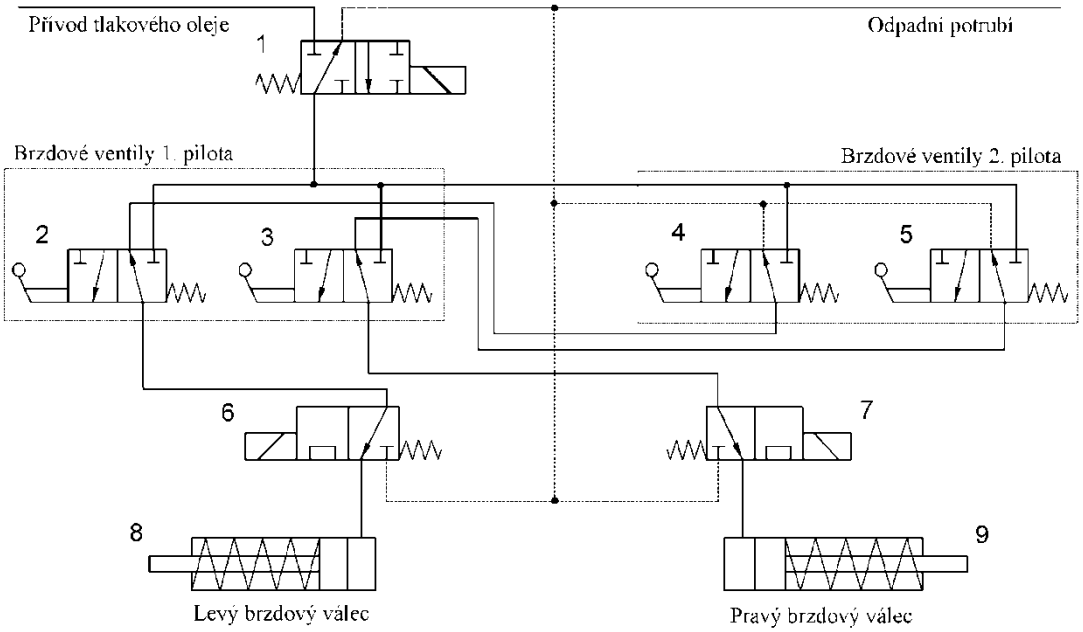
- Přistání letounu se zablokovanými koly ***(CATASTROPHIC** – katastrofické důsledky)*

Další poruchové stavy, které byly u soustavy identifikovány zde nejsou uváděny, protože jejich znalost není pro uváděný příklad podstatná.

Letecké předpisy CS-25 [9], popř. FAR-25 [10] a související dokumenty [11] definují celou řadu požadavků na soustavy letadel. Nejdůležitějšími z nich jsou:

- **Selhání samostatného prvku nesmí způsobit katastrofickou událost***
- Pravděpodobnost nastoupení událostí s katastrofickými důsledky by neměla u dopravních letadel být vyšší než $1 \cdot 10^{-9}$ vztaženo 1 hodinu letu.

* - jako katastrofické jsou posuzovány poruchové stavy, které vylučují bezpečné pokračování v letu a přistání – včetně smrtelných zranění cestujících a posádky.



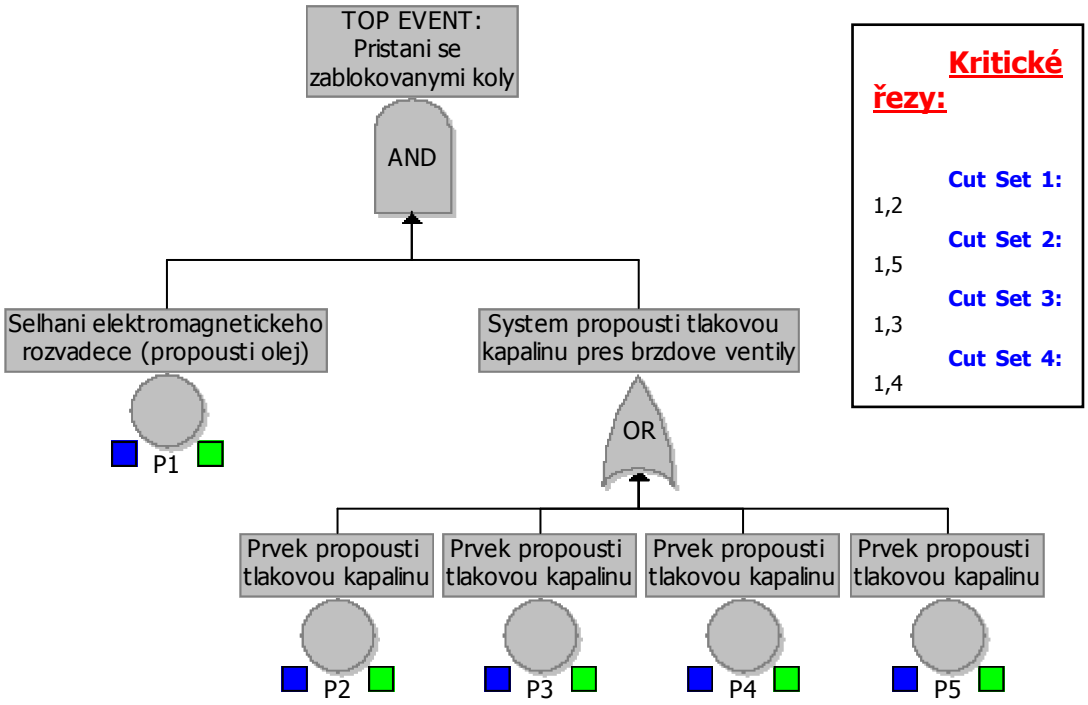

**Obr. 5 Zjednodušené schéma hydraulické soustavy ovládání brzd dopravního letounu**

Aby bylo možné mimo kvalitativního vyhodnocení i vyhodnocení kvantitativní, budou pro řešení zvoleny hodnoty intenzit poruch vybraných poruchových stavů uvedené v tab. 4.

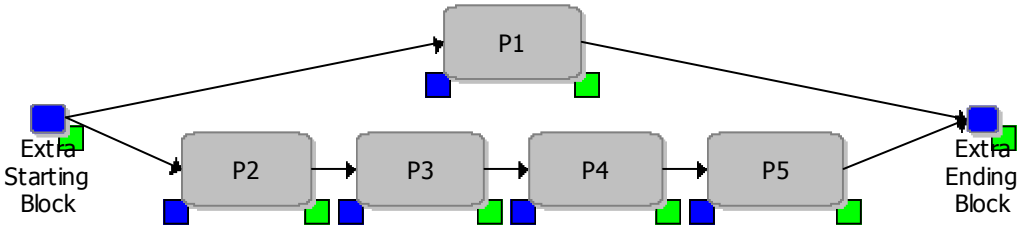
***Tab. 4** Intenzity poruch vybraných prvků zvolené pro potřeby praktického příkladu*

| Prvek | Intenzita poruch [$h^{-1}$] | Zdroj dat |
|---|---|---|
| **Elektromagnetický ventil** (1) | | MIL-HDBK-217F, EPRD97 |
| **samovolné otevření/uzavření** | **$1 \cdot 10^{-7}$** | |
| ventil nelze otevřít/uzavřít | $1 \cdot 10^{-8}$ | |
| **Brzdový ventil** (2), (3), (4), (5) | | Provozní data (předchozí typ) |
| nelze přestavit polohu | $2 \cdot 10^{-5}$ | |
| **samovolné přestavení polohy** | **$3 \cdot 10^{-7}$** | |

Pozn.: V letectví jsou tam, kde nejsou k dispozici provozní data jako doporučené zdroje dat pro odhady intenzit poruch lit. [7] uváděny MIL-HDBK-217 [12] a NPRD [13].




**Obr. 6 Strom poruchových stavů pro vrcholovou událost „přistání se zablokovanými koly“ (vytvořený v softwaru Reliasoft BlockSim 6.2 FTI)**




**Obr. 7 Blokový diagram bezporuchovosti vytvořený pro stav modelovaný v předchozím stromu poruchových stavů - viz. obr. 6 (RBD byl vytvořen přímo ze stromu poruchových stavů v softwaru BlockSim 6.2 FTI „jedním kliknutím myši“)**

Strom poruchových stavů pro sledovanou vrcholovou událost „přistání se zablokovanými koly“ je na obrázku 6. Aby bylo demonstrováno řešení s využitím moderních softwarových prostředků, byl výstup vytvořen s využitím softwaru Reliasoft BlockSim 6.2 FTI. Obdobně blokový diagram vztahující se ke stejnému modelovanému stavu je uveden na obrázku 7. V tomto případě je nutné poznamenat, že z hlediska analýzy by bylo vhodnější místo blokového diagramu bezporuchovosti modelovat blokový diagram poruchy. Tento blokový diagram by bylo rovněž možné lépe analyzovat kvalitativně (s jasně patrnými kombinacemi prvků, jejichž selhání vede na sledovaný poruchový stav). Takový způsob modelování je i běžný pro oblast letectví. Bohužel, komerční software často není uzpůsobený k modelování blokových diagramů poruch.

Součástí obr. 6 je i seznam kritických řezů – rovněž nabídnutý jako výstup ze softwaru Reliasoft BlockSim 6.2 FTI. Tímto **kvalitativním vyhodnocením** je proveden **průkaz požadavku, že selhání jednoho prvku nesmí způsobit katastrofickou událost**. V tomto případě by patrně byl do postupů v Letové příručce daného typu letounu zahrnut požadavek, aby piloti začali používat brzdy na pedálech až po dosednutí letounu (aby byly splněny všechny předpoklady analýzy).

Pro **kvantitativní vyhodnocení** (*odhad pravděpodobnosti nastoupení zvoleného poruchového stavu za jednu hodinu letu*) bylo potřeba definovat několik zjednodušení, která umožňují udržet praktické výpočty na úrovni dostatečně jednoduché pro každodenní průmyslové využití. Zvolená zjednodušení opět vycházejí z doporučení SAE ARP4761 [7] praktikovaných v leteckém průmyslu:

- *Použití exponenciálního rozdělení pro popis poruchových stavů. (Problematický, nicméně např. v letectví běžně používaný předpoklad.)*
- *Při výpočtech lze použít zjednodušující vztah pro výpočet hodnoty distribuční funkce F(t) (resp. pravděpodobnosti poruchy Q):*

$$F(t_1) = 1 - \exp(-\lambda t_2)$$
$$Q = F(t_2) - F(t_1) \doteq \lambda \Delta t$$

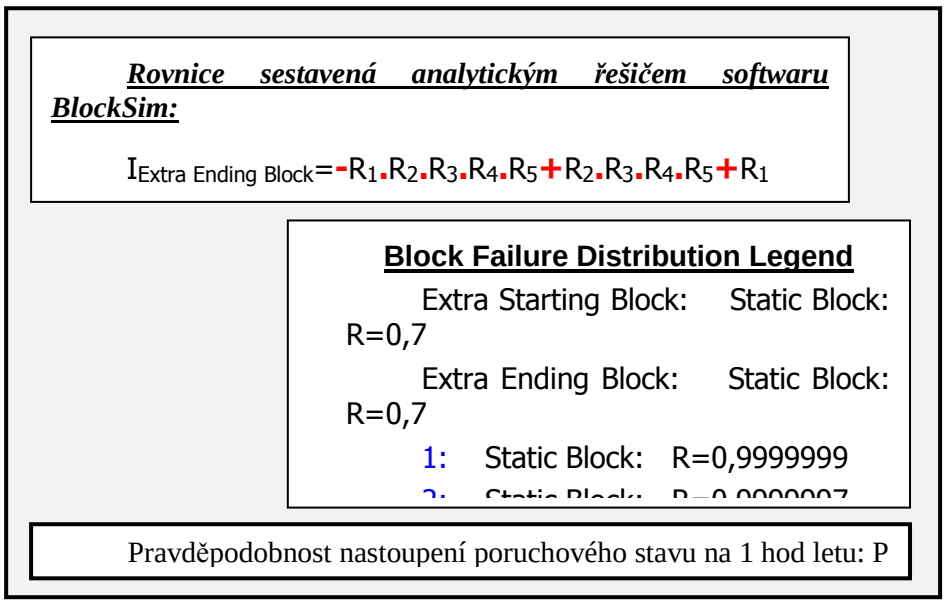
*Uvedené zjednodušení platí za předpokladu, že* $\lambda t << 1$.

*SAE ARP 4761 ([7], str. 84) připouští použití zjednodušení všude tam, kde* $\lambda t < 0{,}1$.

- *Nalezené minimální kritické řezy vyššího řádu (selhání většího počtu prvků současně) budou ve srovnání s kritickými řezy nižších řádů výrazně méně pravděpodobné a je možné je vyloučit (vhodnost aplikace tohoto zjednodušení musí být posuzována v každém jednotlivém případě zvlášť). SAE ARP 4761 [7] udává, že kritické řezy s 5 nebo více základními událostmi mají obvykle velmi malý dopad na pravděpodobnost nastoupení sledovaného jevu (poruchového stavu).*

Ve většině případů není v běžné průmyslové praxi možné aplikovat metody jako FTA či RBD v plné šíři bez zjednodušujících předpokladů. V různých průmyslových oblastech jsou proto využívány různé postupy pro zjednodušení analýz komplexních technických systémů. Jako příklad lze uvést zjednodušení aplikovaná při vývoji nadzvukového dopravního letounu Concorde. Pro účely analýz systémů a instalací tohoto letounu nebyly uvažovány minimální kritické řezy s vyšším řádem než 4 (současné selhání více než 4 prvků nebylo pro svoji extrémně malou pravděpodobnost nastoupení vůbec uvažováno). Obdobně nebyly v rámci analýz

Také kvantitativní vyhodnocení stromu poruchových stavů bylo provedeno s využitím výše jmenovaného softwaru. Shrnutí výstupů je uvedeno v obr. 8.




**Obr. 8 Výstupy řešení ze softwaru Reliasoft BlockSim 6.2 FTI**

## 6 Závěr

V současné době existuje široká škála metod, které umožňují modelování a kvalitativní i kvantitativní vyhodnocení úrovně spolehlivosti systémů. Každá průmyslová oblast má vlastní specifika pro jejich použití, nicméně je možné najít přístupy aplikovatelné všeobecně. Příspěvek shrnuje informace o nejpoužívanějších metodách, postupech a zjednodušeních, které je možné použít pro praktické průmyslové aplikace.

V příspěvku je rovněž obsažena řada dalších informací související s historií nepoužívanějších metod a jejich aplikací v různých průmyslových oborech (nejčastěji v letectví). Závěr příspěvku je věnován praktické ukázce využití stromů poruchových stavů pro analýzu poruchového stavu brzdové soustavy dopravního letounu.

## Použitá literatura:


[20] ČSN EN 61078 *Techniky analýzy spolehlivosti – Blokový diagram bezporuchovosti a booleovské metody*. Praha: ČSNI 2007.

[21] ČSN EN 61025 *Analýza stromu poruchových stavů (FTA)*. Praha: ČSNI 2007.

[22] ČSN EN 61165 *Použití Markovových technik. Praha*: ČSNI 2007

[4] VILLEMEUR, A. *Reliability, Availability, Maintainability and Safety Assessment, Vol.1*, John Willey & Sons, ISBN 0 417 93048 2, 1992, 363 str.

[5] VILLEMEUR, A. *Reliability, Availability, Maintainability and Safety Assessment, Vol.2*, John Willey & Sons, ISBN 0 417 93049 0, 1992, 377 str.

[6] HOLUB, R. a VINTR, Z.: *Spolehlivost letadlové techniky (elektronická učebnice)*, VUT-FSI, Brno, 2001, 233 str.

[7] ARP 4761 *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, SAE Warrendale USA, 12/1996, 331 str.

[8] Ericson, C. A.: *Fault Tree Analysis – A History*, Proceedings of The 17th International System Safety Conference, Orlando (USA), 1999

[9] CS-25 *Certification Specifications for Large Aeroplanes*, European Aviation Safety Agency (EASA), www.easa.eu.int, 2003

[10] FAR Part 25 Airworthiness standards: *Transport category airplanes*. Federal Aviation Administration, Washington D.C., www.faa.gov, 7/2002

[11] Advisory Circular AC 25.1309-1A: *System Design and Analysis*. Federal Aviation Administration, Washington D.C., www.faa.gov, 6/1988, 19 p.

[12] MIL-HDBK-217F *Reliability Prediction of Electronic Equipment*, US Department of Defense, Washington DC 20301, 2/1991, 205 str.

[13] NPRD-95C *Non-Electronic Parts Reliability Data*, Reliability Analysis Center, US Department of Defense, Rome, New York 13440, 1995

[14] RAUSAND, M.; HOYLAND, A. *System Reliability Theory – Models, Statistical Methods, and Applications*, 2nd Edition, John Willey & Sons, ISBN 0-471-47133-X, 2004, 636 str.

[15] VINTR, Z.: *Základní filozofie průkazu spolehlivosti a bezpečnosti technického systému v počátečních etapách životního cyklu*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

[16] VALIŠ, D.: *Předběžná analýza nebezpečí – základ racionálního návrhu systému*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

[17] VINTR, M.: *Metoda FMECA jako nástroj analýzy bezpečnosti a spolehlivosti komponent systému*, 35. Setkání odborné skupiny pro spolehlivost (ČSJ), Brno, 2009

Název: Analýzy spolehlivosti a bezpečnosti v praxi (aneb jak přesvědčit zákazníka, že požadavky na spolehlivost a bezpečnost výrobku budou splněny)

Kolektiv autorů

Počet stran: 66

Tisk: 1. vydání 2009, Brožovaná vazba

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

**ISBN 978-80-02-02156-8**