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

ZAJIŠŤOVÁNÍ BEZPEČNOSTI TECHNICKÝCH OBJEKTŮ

**MATERIÁLY ZE 16. SETKÁNÍ
ODBORNÉ SKUPINY PRO SPOLEHLIVOST**

Praha, září 2004

Obsah

ZAJIŠŤOVÁNÍ BEZPEČNOSTI UPLATNĚNÍM MANAGEMENTU RIZIK

Doc. Ing. Antonín Mykiska, CSc.
Fakulta strojní ČVUT v Praze

1. Východiska a souvislosti řešení problematiky bezpečnosti

Nejvýznamnější skupinou inherentních znaků jakosti jsou funkční vlastnosti (funkčnost, výkonnost atd.) a s nimi bezprostředně svázaná **bezpečnost** a **spolehlivost.** Zajištění stanovené nebo očekávané bezpečnosti je požadováno zákazníky, společností a dalšími zainteresovanými stranami a týká se produktů (výrobků), procesů, projektů, systémů, organizací atd. Požadavky na bezpečnost jsou pak obsahem celé řady právních předpisů, technických norem a normativních dokumentů, zahrnující i stanovení postupů posuzování a prokazování shody s těmito požadavky.

BEZPEČNOST (SAFETY) = VLASTNOST, VYJADŘUJÍCÍ SCHOPNOST OBJEKTU (PRODUKTU/VÝROBKU, PROCESU, SYSTÉMU, ORGANIZACE ATD.) BÝT VE STAVU, KDY **RIZIKO** OHROŽENÍ ŽIVOTA A ZDRAVÍ LIDÍ, ŽIVOTNÍHO PROSTŘEDÍ A POŠKOZENÍ MAJETKU JE OMEZENO NA PŘIJATELNOU ÚROVEŇ.

Intuitivní chápání termínu riziko je v očekávání něčeho nepříznivého, přičemž zahrnuje dva aspekty:
- očekávání výskytu nepříznivé (nebezpečné) události,
- výši poškození (újmy) spojené s nepříznivou událostí, pokud skutečně nastane.

Přitom nepříznivá událost může vzniknout náhodně v čase a prostoru, výše poškození (újmy) může být známa předem (tj. je determinována) nebo je rovněž náhodného charakteru.

Řešení je obecně založeno na **zjištění a zkoumání rizik** nastání všech možných **nebezpečí** jako zdroje potenciálního poškození (újmy) nebo situací s potenciální možností poškození (újmy), přičemž **poškozením** se obecně rozumí tělesné zranění nebo škoda na zdraví, majetku nebo životním prostředí.

Výchozím krokem je proto systematická **identifikace** jakýchkoliv možných **nebezpečí**, definování jejich charakteristik a možností způsobit poškození. Z hlediska povahy **vyvolaných následků nebezpečných událostí** se např. podle IEC 300-3-9 rozlišují čtyři základní kategorie rizik:
- individuální následky (s dopadem na jednotlivce),
- následky z povolání (s dopadem na pracovníky),
- společenské následky (s celkovým dopadem na veřejnost),
- škody na majetku a ekonomické ztráty (včetně přerušení podnikání, pokut apod.).

Obě složky definující riziko, tj. výskyt nežádoucí události a její následky, je možné kvantifikovat. Ve vztahu k nebezpečným událostem nebo jevům se **riziko** kvantitativně vyjadřuje kombinací jejich pravděpodobnosti (nebo četnosti) výskytu a kvantifikovaných následků:

RIZIKO = {PRAVDĚPODOBNOST (NEBO ČETNOST) VÝSKYTU **x** KVANTIFIKOVANÉ NÁSLEDKY }NEBEZBEČNÉ UDÁLOSTI

Pravděpodobnost nastání nebezpečné události je sice bezrozměrná veličina, v praxi bývá často vztažena k nějakému parametru (rok, km, počet cyklů apod.), rovněž následky mohou být kvantifikovány různě (hmotná škoda, počet úmrtí atd.).

Jak již bylo uvedeno, požadavky na bezpečnost k ochraně obyvatelstva před riziky ohrožení života a zdraví lidí, životního prostředí a poškození majetku – tj. před **riziky ohrožení oprávněných (veřejných) zájmů –** jsou **obsahem** řady **právních předpisů.** Proto nezbytnou součástí řešení problematiky bezpečnosti je dále:
- vymezení a akceptování požadavků, které se z obecných právních předpisů vztahují na daný konkrétní případ,
- volba a uplatnění vhodných nástrojů zajišťování bezpečnosti včetně prevence s vymezením odpovědností a přidělením zdrojů, **jako složek managementu rizik**.

2. Právní odpovědnost za bezpečnost

Právní odpovědnost za bezpečnost v podmínkách ČR (v souladu s právem ES) **je** řešena **v oblasti**
- **výrobků (produktů)**,
- **organizací (zejména průmyslových podniků)**,

a to v obou případech v oblasti:
a) soukromoprávní ochrany,
b) veřejnoprávní ochrany.

Ad a) Struktura právních předpisů **odpovědnosti za výrobek** a jeho bezpečnost **v oblasti soukromoprávní ochrany**:
⇒ **Občanský zákoník** – zákon 40/1964 Sb. ve znění všech pozdějších dalších úprav,
⇒ zákon 634/1992 Sb. **o ochraně spotřebitele** ve znění pozdějších právních úprav,
⇒ zákon 59/1998 Sb. **o odpovědnosti za škodu způsobenou vadou výroku** ve znění zákona 209/2000 Sb. (z hlediska přiměřené úrovně bezporuchovosti a bezpečnosti pro mimosmluvní vztahy odpovídá výrobce nebo distributor za škodu způsobenou vadou výrobku, prokáže-li poškozený vadu výrobku, vzniklou škodu - tj. škodu na zdraví nebo následnou škodu na jiné věci než je vadný výrobek - a příčinnou souvislost mezi vadou výrobku a vzniklou škodou).

Ad b) Vymezení **právní odpovědnosti v oblasti veřejnoprávní ochrany** má složitější strukturu. Základním právním předpisem je **zákon** 102/2001 Sb**. o obecné bezpečnosti výrobků**, na který navazuje vymezení právní odpovědnosti:
A) pro **výrobky s užitím ve specifikovaných oblastech**, např.:
- ⇒ zákon č. 111/1994 Sb. **o silniční dopravě** ve znění pozdějších předpisů,
- ⇒ zákon č. 266/1994 Sb. **o drahách** ve znění pozdějších předpisů,
- ⇒ zákon č. 266/1995 Sb. **o vnitrostátní plavbě** ve znění zákona č. 358/1999 Sb. a dalších předpisů,
- ⇒ zákon č. 38/1995 Sb. **o technických podmínkách provozu silničních vozidel na pozemních komunikacích** ve znění pozdějších předpisů,
- ⇒ zákon 114/1995 Sb. **o vnitrostátní přepravě** ve znění pozdějších předpisů,
- ⇒ zákon 18/1997 Sb. **o mírovém využití jaderné energie a ionizujícího záření** (atomový zákon) ve znění zákona č. 83/1998 Sb.,
- ⇒ zákon 258/2001 Sb. **o ochraně veřejného zdraví;**

B) pro **skupiny výrobků vymezených speciálním zákonem**, např.:
- ⇒ zákon č. 79/1997 Sb. **o léčivech,**
- ⇒ zákon č. 110/1997 Sb. **o potravinách a tabákových výrobcích** atd.;

C) **pro výrobky stanovené zákonem** č. 22/1997 Sb. **o technických požadavcích na výrobky** ve znění zákona č. 71/20000 Sb., kde konkrétní skupiny stanovených výrobků, technické požadavky na ně a postupy posuzování shody s těmito požadavky jsou upravovány jednotlivými Nařízeními vlády.

Největším rizikem ohrožení oprávněných veřejných zájmů jsou průmyslové provozy. Pro tuto oblast ohrožení oprávněných veřejných zájmů průmyslovými provozy vymezují povinnosti a právní odpovědnost např. tyto další právní předpisy:
⇒ zákon č. 244/1992 Sb. **o posuzování vlivu na životní prostředí** ve znění dalších právních úprav,
⇒ zákon č. 125/1997 Sb. **o odpadech** ve znění zákona č. 167/1998 Sb. a dalších právních úprav,
⇒ zákon č. 222/194 Sb. **o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o Státní energetické inspekci** ve znění zákona č. 83/1998 Sb.,
⇒ zákon č. 138/1973 Sb. **o vodách** (vodní zákon) ve znění pozdějších předpisů,
⇒ zákon 353/1999 Sb.**o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami a chemickými přípravky** a navazující vyhlášky č. 6, 7, 8 z roku 2000.

V oblasti bezpečnosti a ochrany zdraví při práci je pak základní právní normou **zákoník práce** - zákon 155/2000 Sb. v platném znění.

Na uvedené základní právní předpisy **navazuje řada mezinárodních norem ISO, IEC, EN** (přejatých do soustavy českých norem jako ČSN ISO, ČSN EN ISO, ‚CSN ISO/IEC, ČSN IEC, ČSN EN atd.), na něž se právní předpisy odkazují a které se pak v těchto případech stávají právně závazné.

3. Zajištění bezpečnosti a management rizika

Zajištění bezpečnosti v organizacích se obecně týká
I. **výrobků**, které organizace vytváří a dodává na trh,
II. **zařízení, procesů a činností** pomocí nichž organizace svou produkci uskutečňuje.

Zajištění bezpečnosti u objektů typu technických zařízení a systémů (jak výrobků typu technických objektů různé složitosti, tak technických zařízení v rámci výrobních procesů apod.) úzce souvisí s řešením obecné problematiky **spolehlivosti** a je nedílnou součástí obecné péče o jakost, s níž má společnou **stránku**:

- **manažerskou** - tj. stanovení cílů a následné stanovení odpovědností a pravomocí, procesů, postupů, zdrojů atd. pro jejich realizaci v podmínkách organizace,
- **ekonomickou** - tj. analýzu a řízení nákladů s cílem dosahovat optimální nebo alespoň ekonomicky efektivní řešení,
- **technickou** - tj. stanovení konkrétních používaných technik a metod.

Zajištění a realizace manažerské stránky je obecně označováno jako **management rizik**:

> **MANAGEMENT RIZIK** = SYSTEMATICKÉ UPLATŇOVÁNÍ POLITIK, POSTUPŮ A PRAKTIK MANAGEMENTU ORGANIZACE PŘI ŘEŠENÍ ÚKOLŮ IDENTIFIKOVÁNÍ, ANALYZOVÁNÍ, HODNOCENÍ, POSOUZENÍ A REGULOVÁNÍ (OŠETŘOVÁNÍ) RIZIK.

Management rizik, jehož základní strukturu a obsah zachycuje obr. 1, je v současnosti nezbytná součást managementu organizace. Bývá mnohdy dále rozčleněn:

- ve vztahu k riziku ohrožení životního prostředí jako součást **environmentálního managementu** (EM), neboli management zaměřený na ochranu životního prostředí,
- ve vztahu k identifikaci, analýzám, posuzování (ohodnocování) a omezování rizik při práci jako **management bezpečnosti a ochrany zdraví** (BOZP),
- ve vztahu k výrobně technologickým systémům jako **management rizik technologických systémů**,
- ve vztahu k projektům jako **managament rizika projektu** apod.

*Poněkud odlišnou svým obsahem je problematika **bezpečnosti informačních technologií a informačních systémů** (IT/IS). Navíc se doporučuje namísto termín bezpečnost (safety) používat český termín **zabezpečení** jako překlad anglického termínu security.*

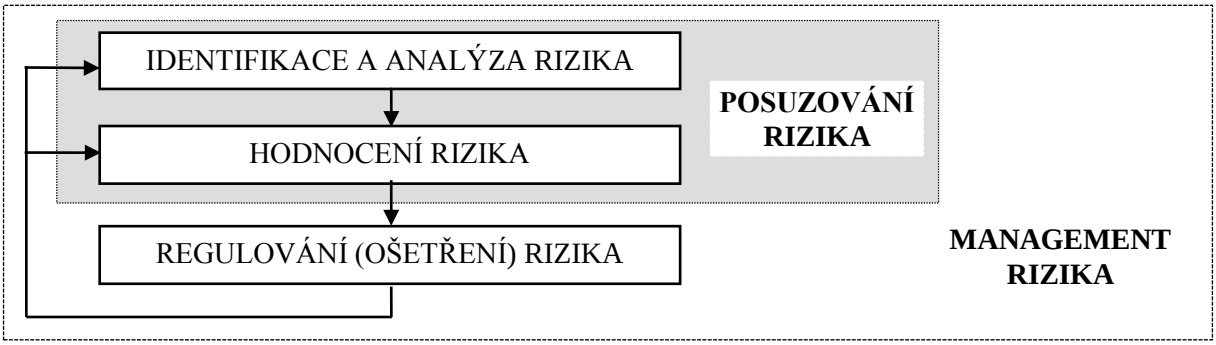
Před prováděním úkolů a činností managementu rizik je obecně vždy nezbytné:

- přesně vymezit jeho předmět, tj. na co nebo na jakou oblast bude uplatňován,
- stanovit cíle, organizační a strategická omezení (právní, smluvní, technická, finanční a tržní hlediska),
- stanovit **kritéria přijatelnosti a únosnosti rizik** ve vazbě na právní a normativní požadavky, uplatnit smluvní a samozřejmě i ekonomická (finanční) hlediska.

Obecný postup řešení problematiky bezpečnosti, tj. zajištění specifikované přijatelné úrovně bezpečnosti, zahrnuje v každém konkrétní případě tyto základní kroky (obr. 1):

- **identifikace** všech potenciálně možných **nebezpečných událostí**,
- **jejich analýza** a **ohodnocení mírou rizika** (jako kombinace pravděpodobnosti výskytu a kvantifikace následků),
- **posuzování** jejich **přijatelnosti** a následná **regulace** (řízení, ošetření) **nepřijatelných rizik** vhodnými opatřeními,

a to jako obsah a součást managementu rizika.



Obr. 1 - Struktura posuzování rizika a managementu rizika

3.1 Identifikace, analýza a hodnocení rizik

Obsahem **identifikace** je zjišťování a zkoumání všech potenciálně možných rizik daného objektu (výrobku, činnosti, procesu, systému, projektu atd.), přičemž se vychází ze systematického zkoumání a hledání odpovědí na otázky:

"CO SE MŮŽE STÁT?", "JAK SE TO MŮŽE STÁT?"

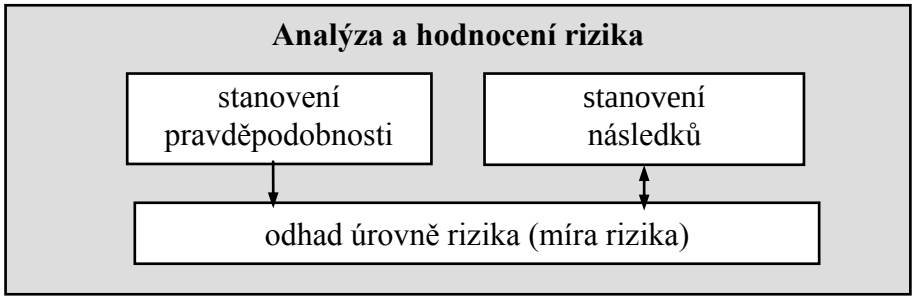
Účelem je nalézt, zaznamenat a charakterizovat všechna rizika vzniku nebezpečných událostí, která mohou ovlivnit bezpečnost, zejména které se vztahují k požadavkům zákonů a nařízení na bezpečnost (safety), zabezpečení (security), spolehlivost, zdraví a životní prostředí atd., a mající vztah k dalším odsouhlaseným cílům managementu, zahrnující např. závaznost, náklady, čas a jakost. Proces identifikace bývá mnohdy nutné během analýzy opakovat.

Analýzy jednotlivých identifikovaných rizik zahrnují:

- zjištění mezí a efektivních hranic rizika a jakékoliv jejich závislosti,
- odhad pravděpodobnosti výskytu a s ním spojeného dopadu (následku) na odsouhlasené cíle.

Hodnocení identifikovaných rizik v rámci analýzy bývá založeno na **volbě míry rizika** pro odhad úrovně rizika, tj. v kvantitativním vyjádření:

- pravděpodobnosti (četnosti) vzniku nebezpečných událostí a
- následků nebezpečných událostí.



Obr. 2 - Analýza identifikovaných rizik

Analýza a hodnocení rizik se provádí kvalitativně a/nebo kvantitativně s využíváním různých technik a postupů**.** Základní nezbytné aktivity pak jsou plánování, provádění a dokumentování, dále specifikování požadavků na jakost pro analýzu rizika a nakonec vyhodnocení, dokumentace a prezentace výsledků.

Termín **analýza rizik** se v praxi často používá souhrnně pro **identifikaci**, vlastní **analýzu** a kvantitativní **hodnocení**. Mnohdy se pod tento termín zahrnuje i **posuzování rizik.**

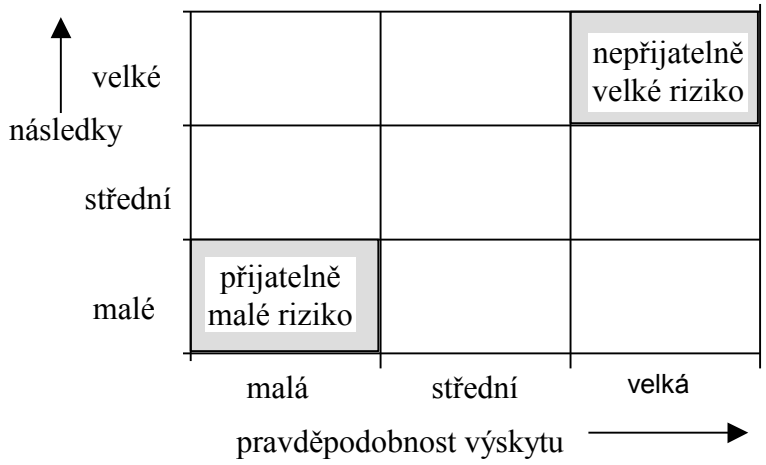
Identifikace, analýza a hodnocení rizik poskytuje vstupní údaje pro posuzování rizik a následné činnosti managementu rizika, tj. o rozhodování o přijatelnosti identifikovaných rizik, zhodnocení volitelných možností jejich snižování a o "manažersky" zajištěných rozhodnutích o opatřeních k jejich snižování.

Volba možných prostředků regulace (ošetření rizik) je zásadně ovlivňována etapou životního cyklu, v nichž se nápravná opatření ke snižování rizikovosti provádějí a využívají. Předběžnou kvalitativní analýzu se doporučuje provádět v časných etapách životního cyklu výrobku nebo fázi přípravy projektu. V dalších

etapách se doporučuje provádět kvantitativní analýzy, pokud jsou k dispozici potřebná data.

3.2 Posuzování rizika

Posuzování rizika spočívá ve **srovnání** analýzou **stanoveného odhadu** úrovně identifikovaného rizika (míry rizika) **s kritérii přijatelnosti** a stanovení priorit pro regulaci (ošetření) nepřijatelných rizik. Pro znázornění specifikovaných přípustných a nepřípustných oblastí rizik se používají různé jednoduché grafické prostředky, např. diagramy rizika, matice rizika (obr. 3) apod.



Obr. 3 – Matice rizik

Filozofie posouzení přijatelnosti a nepřijatelnosti rizika vychází z reality, že úplné vyloučení všech rizik je prakticky nemožné, určitá míra rizika se považuje za přijatelnou vzhledem k současnému stavu vědeckých, technických a dalších poznatků a s nimi souvisejících možností. Tato "malá" **zbytková rizika** mohou být přijata bez ošetření. Je však nutné je uvádět v seznamu všech identifikovaných rizik, aby mohlo být prováděno jejich monitorování. Rizika, která nebyla přijata, musí být ošetřena, tj. musí být navržena a provedena nápravná opatření k jejich snížení nebo odstranění.

3.3 Regulace (ošetření) rizika

Účelem **regulace** (ošetření, řízení) **rizika** je zjistit a **uplatnit** ekonomicky efektivní **opatření, která učiní rizika přijatelnými,** zahrnující:

- zjištění a vyhodnocení volitelných možností,
- výběr z volitelných možností,
- vypracování strategie ošetření,
- uplatnění zvoleného ošetření.

Obecně jde o **rozhodovací proces s** volitelnými **možnostmi**:

- úplné zabránění rizika odstraněním příčin vzniku nebezpečné události, je-li to "technicky" možné a ekonomicky únosné,
- snížení pravděpodobnosti výskytu rizika na přijatelnou hodnotu,
- snížení nepříznivých následků rizika pro případ, že by nebezpečná událost nastala, např. vypracování plánů na zotavení z jeho následků, návrhem a realizováním obnovy.

Opatření ke snižování rizikovosti objektů typu technických zařízení a systémů se provádí v různých etapách jejich životního cyklu. **Nejefektivnější** jsou **opatření** uplatněná **v etapách návrhu a vývoje**, např. v podobě úprav návrhu (konstrukce nebo projektu), návrhu výrobních a dalších procesů (včetně využívání různé formy, stupně a rozsahu nadbytečnosti s efektem odstranění nebo snížení příčin rizikovosti), podmínek užívání (namáhání, zatížení, koncepce údržby, obsluhy, podmínek prostředí) apod.

Pokud se provádí analýza v pozdějším stádiu života objektu, např. **v období uvádění do provozu nebo vlastního provozu**, stává se, že z ekonomických, konstrukčních, provozních či jiných důvodů se dostaneme za hranici označovanou jako zbytková rizikovost, aniž by se jí podařilo snížit na požadovanou úroveň. Protože pak přetrvávají zbytková rizika, která nelze akceptovat, musí být přijata příslušná **bezpečnostní opatření**, která se poté musí **uplatňovat při provozu**. Jde o opatření, která vedou zpravidla k "pasivnímu"

potlačení rizikovosti upravením podmínek užívání, zejména návodů k obsluze, dovybavením varovnými, výstražnými a dalšími upozorněními (např. použitím příslušných bezpečnostních značek).

3.4 Prokazování, přezkoumání a monitorování rizika

Prokazování, že byla v podmínkách organizace navržena a provedena všechna potřebná opatření ke snížení všech potenciálních rizik na přijatelnou úroveň je obsahem **bezpečnostních auditů.** Bezpečnostní audit je systematické a nezávislé posouzení (prověření) celkové bezpečnosti s cílem ověřit, jak je vyhověno platným předpisům a normám a může být v organizaci zaměřen na jeho management a organizační strukturu, jednotlivá pracoviště, provozy, procesy, pracovní postupy atd.

Přezkoumání a monitorování rizika má za úkol zjistit jakákoliv nově vzniklá rizika a zajistit, že ošetření rizika zůstane efektivní, což má být vždy přezkoumáváno. Přezkoumávání rizika během životního cyklu také zajišťuje, že všechny příslušné dokumenty, normy, postupy a seznamy jsou průběžně aktualizovány a udržovány. **Monitorování rizika** má být nepřetržité po celou dobu života a zahrnuje i vyšetřování nákladů. Hlavní činnosti monitorování se provádí v klíčových milnících vývoje, výroby a instalace a vždy, kdy se významně změní okolní podmínky.

4. Techniky analýz a hodnocení rizik

Techniky, tj. metody a postupy používané k analýzám a hodnocení rizika lze dělit do tří kategorií podle stupně podrobnosti analýzy rizika a schopnosti kvantifikace míry rizika.

KATEGORIE 1: SROVNÁVACÍ POSTUPY A METODY

Metody a postupy zaměřené zejména na identifikaci zdrojů rizik. Pracují většinou na základě porovnávání a aplikování provozních zkušeností získaných z provozu nebezpečných zařízení, doplněné prohlídkou zařízení. Jejich cílem je odhalení slabin nebezpečného zařízení a seřazení systémů, skupin, uzlů podle subjektivního posouzení jejich potenciálně možného podílu na příčinách a průběhu nebezpečné události. Jsou schopny upozornit na potenciálně nebezpečné části hodnoceného zařízení, neumožňují však ani kvantifikovat pravděpodobnost selhání jednotlivých systémů, ani nedefinují podíl jednotlivých komponent nebezpečného zařízení na pravděpodobnosti vzniku nebezpečné události. Nelze pomocí nich vyčíslit míru rizika. Představitely této kategorie jsou např.:

- **Bezpečnostní audit** (**SA**/SR - Safety Audit/Review),
- **Analýza** (procesu/systému) **kontrolním seznamem** (**CA** – (Process/Systém) Checklist Analysis),
- **Relativní klasifikace** (**RR** - Relative Ranking) - Dow and Mond Hazard Indices.

KATEGORIE 2: ANALYTICKÉ POSTUPY A METODY ZALOŽENÉ NA DETERMINISTICKÉM PŘÍSTUPU.

Metody a postupy zaměřené na identifikaci zdrojů rizik. Analyzují příčiny nastání nebezpečných událostí a scénáře jejich rozvoje, jsou schopny upozornit na potenciálně nebezpečné části hodnoceného zařízení. Neumožňují však ani kvantifikovat pravděpodobnost selhání jednotlivých systémů, ani nedefinují podíl jednotlivých komponent nebezpečného zařízení na pravděpodobnosti vzniku nebezpečné události. Neumožňují stanovit pravděpodobnost výskytu nebezpečných jevů, pravděpodobnosti selhání pro bezpečnost důležitých komponent, systémů a zásahů obsluhy. Nelze pomocí nich vyčíslit míru rizika. Představiteli této kategorie jsou např.:

- **Předběžná analýza nebezpečí** (**PHA** - Preliminary Hazard Analysis),
- **Studie provozuschopnosti** (**HAZOP** - Hazard Operability Studies),
- **Analýza** "**Co se stane, když** …" (**W-I A** – "What if" Analysis),
- **Analýza druhů a důsledků poruch** (**FMEA** - Failure Mode and Effect Analysis)
- **Analýza stromu poruch** (**FTA** – Failure Tree Analysis) - kvalitativní,
- **Analýza stromu událostí** (**ETA** – Event Tree Analysis) - kvalitativní,
- **Analýza příčin a následků** (**CCA** – Cause-Consequence Analysis) – kombinace FTA a ETA,
- **Analýza bezporuchové činnosti** (spolehlivosti) **člověka** (**HRA** – Human Realiability Analysis).

KATEGORIE 3: ANALYTICKÉ METODY A POSTUPY ZALOŽENÉ NA PRAVDĚPODOBNOSTNÍM PŘÍSTUPU.

Skupina metod a postupů, které jsou jediné schopny hodnotit rizika kvantitativně (číselně). Obdobně jako u metod 2. kategorie se na základě provedených analýz vzniku a rozvoje nebezpečné události sestavuje

seznam všech primárních jevů (poruch komponent, systémů, chyb obsluhy, nepříznivých externích vlivů atd.), které samostatně nebo v kombinacích vedou ke vzniku nebezpečné události. K primárním jevům jsou přiřazeny pravděpodobnosti jejich výskytu a vypočítává se pravděpodobnost vzniku nebezpečné události. K nejznámějším a nejpoužívanějším analytickým metodám a postupům, které pracují s pravděpodobnostním hodnocením, náleží:

- **Analýza stromu poruch/událostí – kvantitativní** (Fault/Event Tree Analysis),
- a metody a postupy, založené na využití aparátu (teorie) **blokových diagramů** (RBD), **orientovaných grafů** a **Markovských procesů** (MA).

Mezi nejpoužívanější metody této skupiny náleží zejména kvantitativní metoda FTA, často v kombinaci s metodou ETA. Pro počítačovou podporu jejich aplikace je vyvinuta a nabízena řada SW produktů od profesionálních softwarových firem včetně databází hodnot ukazatelů pravděpodobnosti poruch nejtypičtějších a nejobvyklejších komponent technologických, řídicích a elektrických systémů.

Analytické metody a postupy založené na pravděpodobnostním přístupu začaly být systematičtěji využívány nejdřív v jaderné energetice a to pod souhrnným označením **pravděpodobnostní hodnocení bezpečnosti/rizika** (PSA/PRA - Probability Safety/Risk Assessment), resp. PSA/PRA studie, zejména pro stanovení pravděpodobnosti úniku radioaktivních látek a jeho následků (PSA studie 1. - 3. stupně).

V jaderné energetice začaly být tyto postupy využívány cca od poloviny 70. let 20. století, kdy na základě systematického sledování poruchovosti systémů, komponent a chyb/omylů/selhání lidské obsluhy se postupně získávaly dostatečně obsáhlé databáze věrohodných dat, které umožnily pravděpodobnosti příčin nebezpečných událostí pomocí matematicko statistických kvantifikovat.

.V dalších nebezpečných průmyslových oborech se pro využívání těchto metod a postupů častěji používá označení **kvantifikované hodnocení rizika** (QRA - Qauntified Risk Assessment), v chemickém průmyslu je aplikace těchto metod a postupů označována jako **kvantifikovaná analýza rizik chemických procesů** (CPQRA - Chemical Process Quantitative Risk Analysis).

Volba technik analýz a hodnocení rizika je obecně dána složitostí řešeného problému, úrovní podrobnosti analýzy, dostupností SW produktů pro jejich podporu a dostupností údajů.

Literatura:

[1] BABINEC, F.: *Bezpečnostní inženýrství*. Učební text. VUT v Brně, Brno 2000 (73 s.)

[2] MYKISKA, A.: *Identifikace, analýza a ošetření rizik v reprodukčním procesu*. In. Sborník semináře Soudobé trendy v řízení jakosti - X. VŠB Ostrava – ČVUT v Praze - ZČU Plzeň – ČSJ - ISQ PRAHA, Zlenice, listopad 2003 (21 str.)

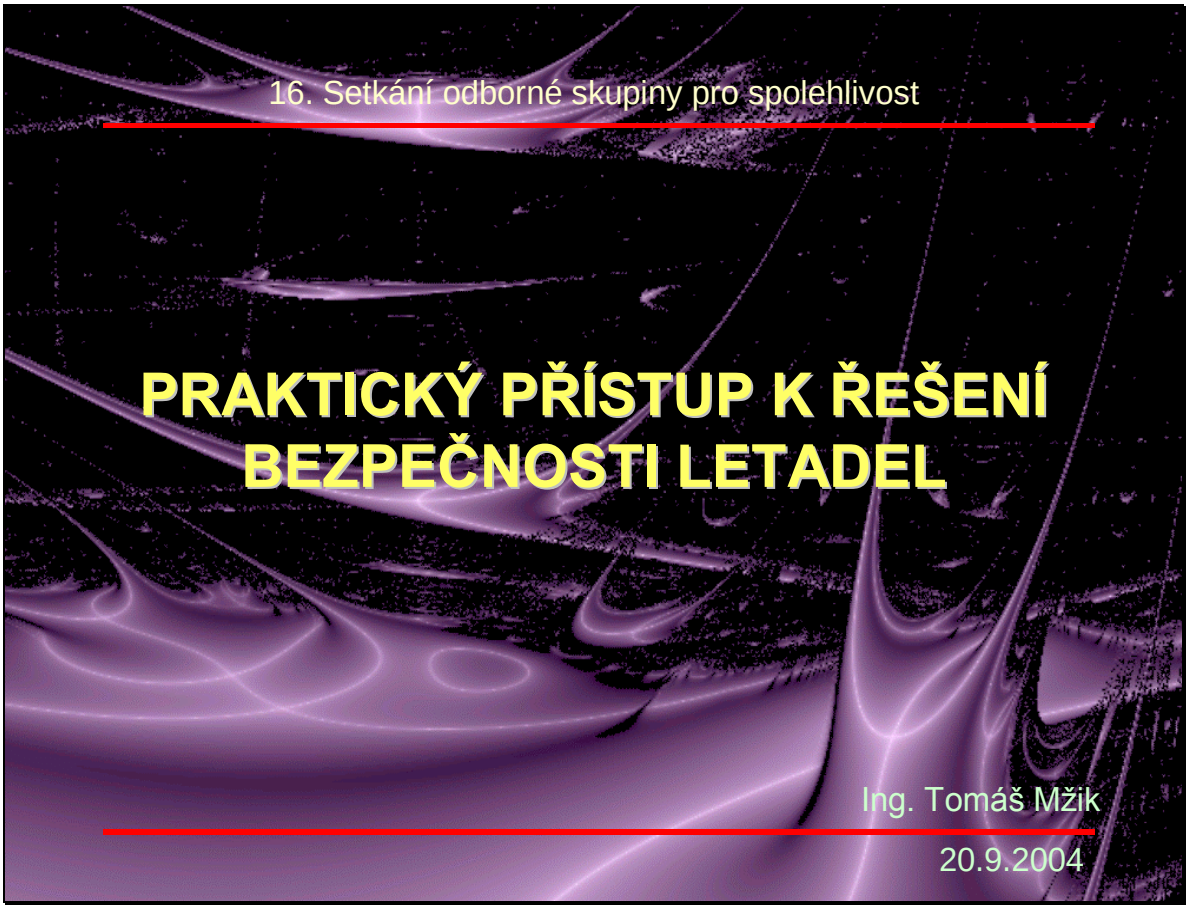
[3] MYKISKA, A.: *Bezpečnost a spolehlivost technických systémů*. Skripta. Vydavatelství ČVUT, Praha 2004 (206 str.)

[4] FUCHS, P.: *Pravděpodobnostní hodnocení rizika*. In: Sb. semináře "Spolehlivost a analýza rizik" odborné skupiny pro spolehlivost při ČSJ. Česká společnost pro jakost (ČSJ), Praha 2003

[5] *Přehled metodik pro analýzu rizik*. Ministerstvo vnitra - Generální ředitelství HZS ČR, č.j.: PO-58-7/PLA-2004

Praktický přístup k řešení bezpečnosti letadel

Ing. Tomáš Mžik (Aero Vodochody)



Obsah prezentace

- Otázka bezpečnosti v letectví
- Předpisy a směrnice
- SAP
- FHA
- PSSA/SSA
- FTA
- FMEA/FMECA
- Matice hodnocení rizik
- Závěr

Otázka bezpečnosti v letectví

V leteckém průmyslu jsou na bezpečnost kladeny vysoké nároky. Cílem výrobců je zajistit bezpečnost letounu, ještě před tím, než je letoun postaven. Z tohoto důvodu vznikají předběžné studie a analýzy, které slouží k odhalení a eliminování možných poruch s katastrofickým důsledkem.

Oblast bezpečnosti je prioritní částí spolehlivosti. Často však platí, že zvyšováním počtu záloh (bezpečnost) se snižuje spolehlivost celku, v letectví se tím nepřímo zvyšuje hmotnost letounu a rostou další náklady na výrobu. Kolik a jak mají vypadat systémy a jejich zálohy určují předpisy podle kterých je letoun stavěn.

Problematikou bezpečnosti se v AV zabývá oddělení spolehlivosti. V této době probíhá certifikace civilního letounu Ae270 u Úřadu civilního letectví ČR. Oddělení zajišťuje analýzy spolehlivosti a bezpečnosti, které budou popsány dále.

Otázka bezpečnosti v letectví

Praktické řešení analýz bezpečnosti spočívá na úzké spolupráci analytika s konstruktéry a se zkušebními piloty. Na základě možných poruch, které byly zjištěny analýzou, může dojít ke změnám v pilotní příručce nebo případně konstrukce letounu. Tyto zásahy následně pomáhají zvyšovat bezpečnost letounu.

Předpisy a směrnice

Aby mohl být letoun používán pro komerční účely, musí mu být vydáno „Osvědčení o letové způsobilosti“. Toto osvědčení se vydává až po ukončení procesu certifikace a po získání „Typového osvědčení“ (certifikátu), které vystavuje příslušný národní úřad pro letectví (ÚCL). Typové osvědčení je doklad o tom, že letoun splňuje všechny požadavky stavebního předpisu pro danou kategorii letounu.

Ve stavebním předpisu jsou uvedeny požadavky na bezpečnost a které je nutné dodržet.

U letounu Ae270 probíhá certifikace podle předpisu FAR 23.1309. Oblast bezpečnosti obsahují odstavce a) a b).

Návod jak provádět analýzy a jak je hodnotit je rozepsán v poradním oběžníku AC 23.1309-1C, který slouží pouze jako doporučení k předpisu FAR 23.1309.

Předpisy a směrnice

V Evropě se řídí certifikace dle úřadu EASA předpisu CS – 23 (dříve organizace JAA a předpis JAR 23.1309).

Dalším velmi významným zdrojem informací pro provádění analýz je dokument SAE ARP4761. Tento dokument je rovněž považován jako doporučení k předpisu FAR 23.1309.

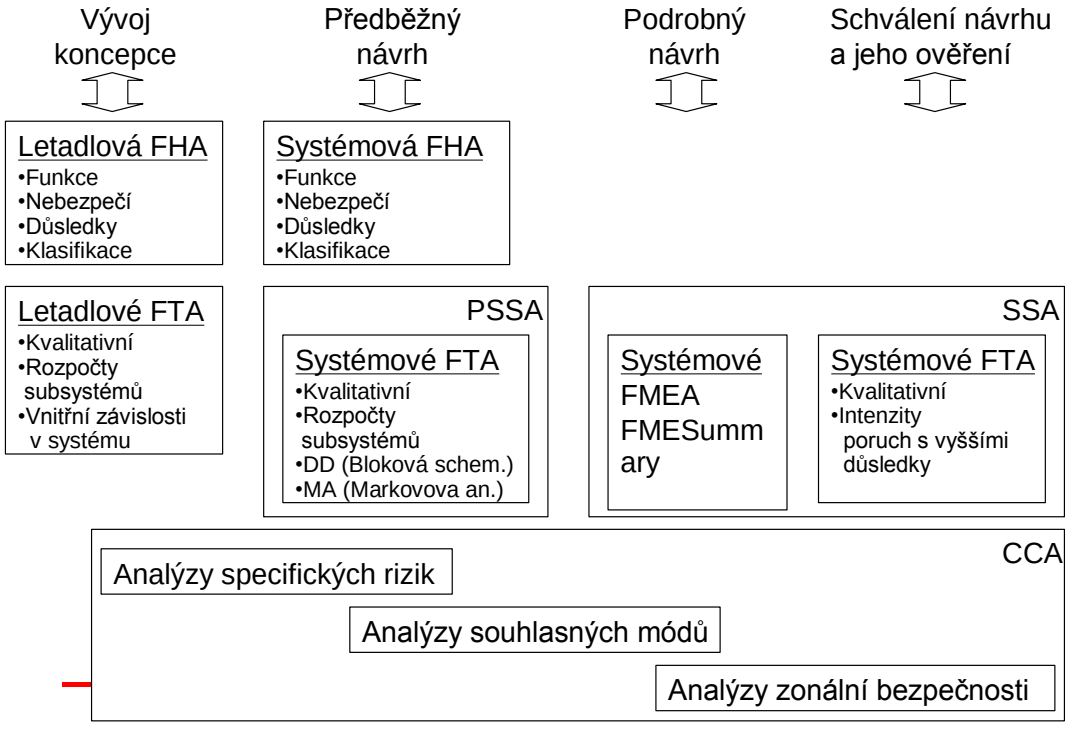
SAP - Procesy posuzování bezpečnosti (ARP 4761)

Proces posuzování bezpečnosti zahrnuje vytváření a zhodnocení požadavků, které podporují vývojové činnosti. Proces dále poskytuje metodologii pro řešení letadlových funkcí a návrhů systémů tak, aby rizika spojená s těmito funkcemi a systémy byla správně popsána.

Pro systémy má SAP význam v podobě stanovení bezpečnostních cílů a zároveň určuje , že realizování těchto cílů bude dosaženo.

SAP začíná spolu s vývojem koncepce letounu při kterém se určují bezpečnostní požadavky a končí ověřením toho, že návrh splňuje stanovené bezpečnostní požadavky. Během tohoto procesu se spolu s návrhem zpřesňují i požadavky na bezpečnost.

SAP - Procesy posuzování bezpečnosti (ARP 4761)



FHA – Posouzení nebezpečí z funkčního hlediska

FHA je definován jako systematický, úplný rozbor funkcí pro rozpoznání a klasifikování poruchových stavů těchto funkcí podle stupně jejich závažnosti. FHA by měla určit poruchové stavy pro každou fázi letu.

FHA se obvykle dělí na dvě části a to:

- Letadlovou
- Systémovou

Letadlová FHA

Kvalitativně posuzuje základní funkce letounu, které byly definovány na počátku vývoje. Měla by určit a klasifikovat poruchové stavy spojené s funkcemi na úrovni letounu. Klasifikace poruchových stavů stanovuje bezpečnostní požadavky, které musí letoun splňovat.

FHA – Posouzení nebezpečí z funkčního hlediska

Systémová FHA

Rovněž kvalitativní posouzení, které je mnohem více svázáno se systémovým řešením. Zahrnuje poruchy nebo kombinace poruch systémů, které mají vliv na funkce letounu.

Výsledky ze systémové FHA slouží jako podklad pro PSSA/SSA.

Poruchové stavy klasifikované jako Catastrophic a Hazardous se musí rozpracovat pomocí analýzy FTA nebo FMECA. Poruchový stav Major se řeší po dohodě s příslušným úřadem. Stavy klasifikované v FHA jako Minor a No safety effect se dále neřeší.

FHA – Posouzení nebezpečí z funkčního hlediska

Příklad systémové FHA

ATA	Funkce	Č. f. por	Poruchový stav	Fáze	Vliv poruchového stavu na letoun nebo posádku	Klasifi-kace	Odkaz na podpůrný materiál
A2900/-01	Zdroje tlaku hydraulické kapaliny.	01	Současná ztráta tlaku hlavního i nouzového zdroje.	Přistání	Ztráta všech silových funkcí hydraulického systému. - Přistání na břicho.	Hazardous	BR12291CZ_S
A2910/-01	Hlavní zdroj hydraulického tlaku .	01	Ztráta tlaku v hlavním okruhu.	Přistání	Ztráta diferencovaného brzdění, ztráta ovládání vztlakových klapek. - Vysunout podvozek a brzdit nouzově.	Major	BR12291CZ_S
A2910/-01	Hlavní zdroj hydraulického tlaku	02	Výstřik hydraulické kapaliny na horkou část motoru	Let	Možnost vzniku požáru motoru.	Hazardous	BR12291CZ_S

PSSA/SSA – Předběžné posouzení bezpečnosti systému

PSSA je systematický rozbor navrhované systémové struktury, který určuje jak mohou poruchy způsobit nebezpečí z funkčního hlediska stanovené v FHA.

Výstupem s PSSA je kvalitativní zhodnocení provedené pomocí FTA. Tato analýza nebyla v AV prováděna.

SSA je systematický rozbor systému, jeho architektury a instalace jehož výsledkem je prokázání shody s bezpečnostními požadavky. Tento rozbor zahrnuje jak kvalitativní tak kvantitativní zhodnocení prováděné pomocí FTA nebo FMEA/FMECA.

FTA – Analýza stromu poruchových stavů

FTA je deduktivní metodou při které se sleduje jedna konkrétní nechtěná událost a zjišťují se příčiny vzniku této události. FTA analýza je založena na principu postupu od vrcholového jevů směrem dolů.

Při provádění FTA je velice důležité dbát na dodržení postupu seshora dolů („top-down“). U jednoduchých stromů se tato vlastnost neprojeví natolik jako u složitých. Pokud se postup obrátí a analýza je prováděna zespodu směrem k postupnému určení vrcholového jevu může dojít k složitě definovaným událostem, které budou navíc různě podmíněny.

Pro kvantitativní vyjádření se používá operací Booleovy algebry. Jednotlivá hradla reprezentují logické součty (OR) nebo součiny (AND).

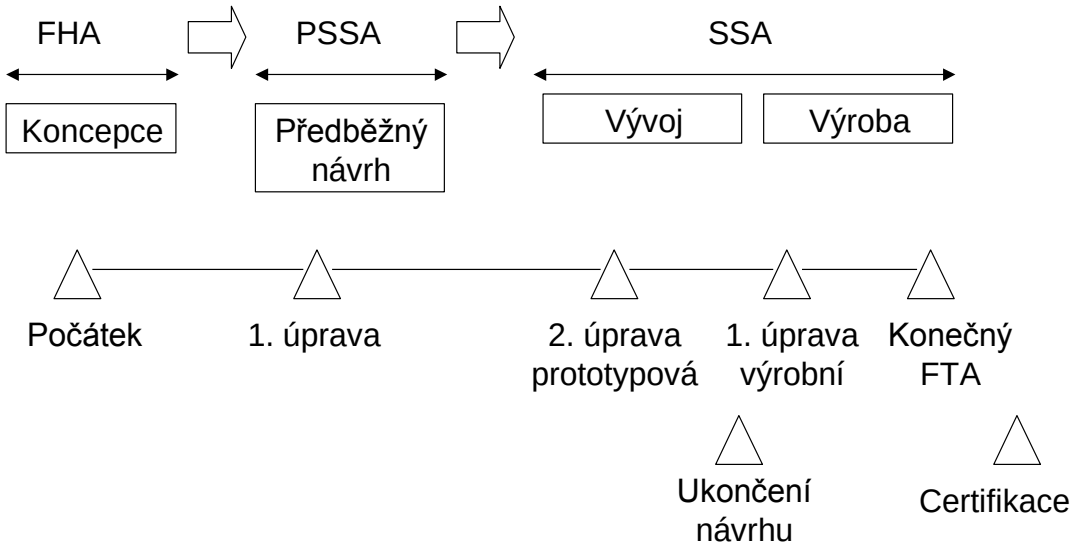
FTA – Analýza stromu poruchových stavů

FTA řeší i jevy, které jsou časově závislé. Jedná se např. o zálohy. Tento problém se řeší pomocí hradla PAND (Priority AND gate). Pro kvantitativní vyjádření se zde používá Markovových řetězců.

Výhodou analýzy je možnost kombinací více poruch v systému.

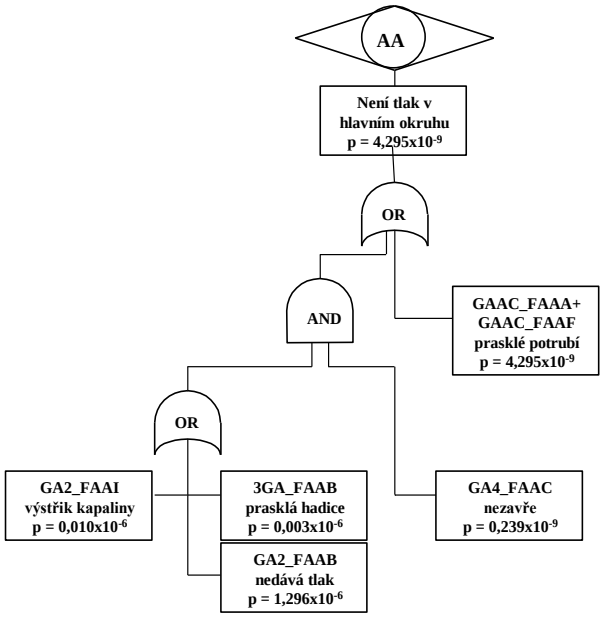
FTA – Analýza stromu poruchových stavů

Příklad FTA v průběhu vývoje letounu



FTA – Analýza stromu poruchových stavů

Příklad FTA



FMEA/FMECA

FMEA (Analýza způsobů a důsledků poruch) je systematická metoda spočívající v identifikování způsobů poruch systémů, prvků, funkcí a určující důsledky na vyšší stupeň projektu.FMEA začíná na nejnižším stupni a postupuje směrem k vyššímu.

Výhodou analýzy je to, že počítá pouze s jedinou poruchou v systému a sleduje její důsledky.

Existují dva základní typy analýz FMEA:

- Funkční
- Fyzická

Funkční FMEA sleduje funkční poruchu v systému. Je výhodná pro složitější systémy. U poruchy není potřeba do detailu rozvádět všechny poruchové stavy prvku.

FMEA/FMECA

Naproti tomu FMEA s fyzickým rozpadem sleduje všechny poruchové stavy prvku s jejich vlivem na vyšší úroveň. Tato metoda je vhodná pro jednodušší systémy.

FMECA je rozšířenou analýzou FMEA o kvantitativní ohodnocení. Provádí se při poruše prvku s vyššími následky, které jsou ohodnoceny dle matice rizik.

Určování intenzit poruch se v AV provádí podle těchto podkladů:

- Statistické sledování a vyhodnocování poruch na letounech L29 – L159.
- Elektronické části se řeší podle MIL-HDBK-217F
- Neelektronické části se řeší podle NPRD 95

FMEA/FMECA

Příklad výstupu z FMECA – funkční rozpad

SYSTÉM: Hlavní okruh

==========

PRVEK: Hydraulická nádrž
FIN: GA1
ATA: A2916GA01
VÝZNAMNÁ FUNKCE: AA # Zásobník hydraulické kapaliny.
FUNKČNÍ PORUCHA: 01 # Změna tvaru nádrže.
KOMPENZAČNÍ OPATŘENÍ: Žádné.
Intenzita funkční poruchy×1000000: 2.985900

==========

***** Možné druhy poruch (FM) způsobující uvedenou funkční poruchu *****

==========

FAAA: Koroze. Deformace. Přefouknutí.
<> Porucha nemá vliv na bezpečnost
<> Porucha je posádce letounu po startu motoru až po vypnutí motoru skrytá
<> DETEKCE: Vizuálně.
<> KOMPENZAČNÍ AKCE: Žádná.
<> DŮSLEDEK: Žádný.
<> Intenzita druhu poruchy ×1000000: 2.985900 se závažností 1, tj. No Safety Effect, ve fázi *, tj. Všechny fáze

---

MATICE HODNOCENÍ RIZIK

ZÁVAŽNOST:
1 NO SAFETY EFFECT
2 MINOR
3 MAJOR
4 HAZARDOUS
5 CATASTROPHIC

PRAVDĚPODOBNOST:
A PRAVDĚPODOBNÉ (>= 10^{-5})
B MÁLO PRAVDĚPODOBNÉ (< 10^{-5})
C VELICE MÁLO PRAVDĚPODOBNÉ (<10^{-7})
D NEPRAVDĚPODOBNÉ (< 10^{-8})

H – HIGH RISK – NEPŘIJATELNÉ
M – MEDIUM RISK – PŘIJATELNÉ S VÝHRADAMI
L – LOW RISK – PŘIJATELNÉ BEZ VÝHRAD

ZÁVAŽNOST	PRAVDĚPODOBNOST			
	A	**B**	**C**	**D**
5	**H**	**H**	**H**	**M**
4	**H**	**H**	**M**	**L**
3	**M**	**M**	**L**	**L**
2	**L**	**L**	**L**	**L**
1	**L**	**L**	**L**	**L**

Závěr

Problém bezpečnosti je v leteckém průmyslu velmi významný a na jeho řešení se vynakládají nemalé prostředky.

Pokusil jsem se zde nastínit etapy vývoje letounu z hlediska bezpečnosti a spolehlivosti od počátečního návrhu po certifikační zkoušky.

I přesto jaký důraz se klade na letovou bezpečnost stále dochází k leteckým neštěstím. Ať již předpisy řeší jakékoliv situace ve snaze předejít těmto neštěstím, nemohou jim zabránit, protože řeší technickou stránku věci. Bezpečnost tedy bývá dostatečně zajištěna po technické stránce, ale velkým hráčem na poli bezpečnosti zůstává lidský faktor, který ve většině případů bývá příčinnou leteckých nehod (pozn. L39 – 77%, u dopravních letounů až 90%).

Děkuji za pozornost.

ANALÝZA RIZIK V OPTIMALIZACI A ÚDRŽBY

Ing. Pavel Fuchs, CSc.
Technická univerzita v Liberci

1 ÚVOD

Téma volně navazuje na přednášku „Pravděpodobnostní hodnocení rizika“, která byla prezentována 4. 3. 2003 na 10. setkání Odborné skupiny pro spolehlivost [1]. Proto již nejsou opakovány základní termíny a definice z oblasti hodnocení rizik. Pozornost je věnována problematice využití analýzy rizik při optimalizace údržby. Z tohoto pohledu je třeba připomenout, že riziko je spojeno s realizací nežádoucí události bez ohledu na to, zda následky nežádoucí události hodnotíme po stránce bezpečnosti, ekologických škod či finančních ztrát. Riziko je tedy univerzální a jen podle třídění následků nežádoucích událostí lze třídit riziko (ekonomické, zdravotní a bezpečnostní, ekologické apod.). Proto při optimalizaci údržby jde vždy o to, aby prostředky vynakládané na údržbu byly úměrné riziku spojenému s poruchami technických objektů. Vnější vlivy (ať již přírodního charakteru, lidského zásahu formou extrémistického činu, či jiného charakteru) nejsou uvažovány.

2 BEZPEČNOST TECHNICKÝCH OBJEKTŮ

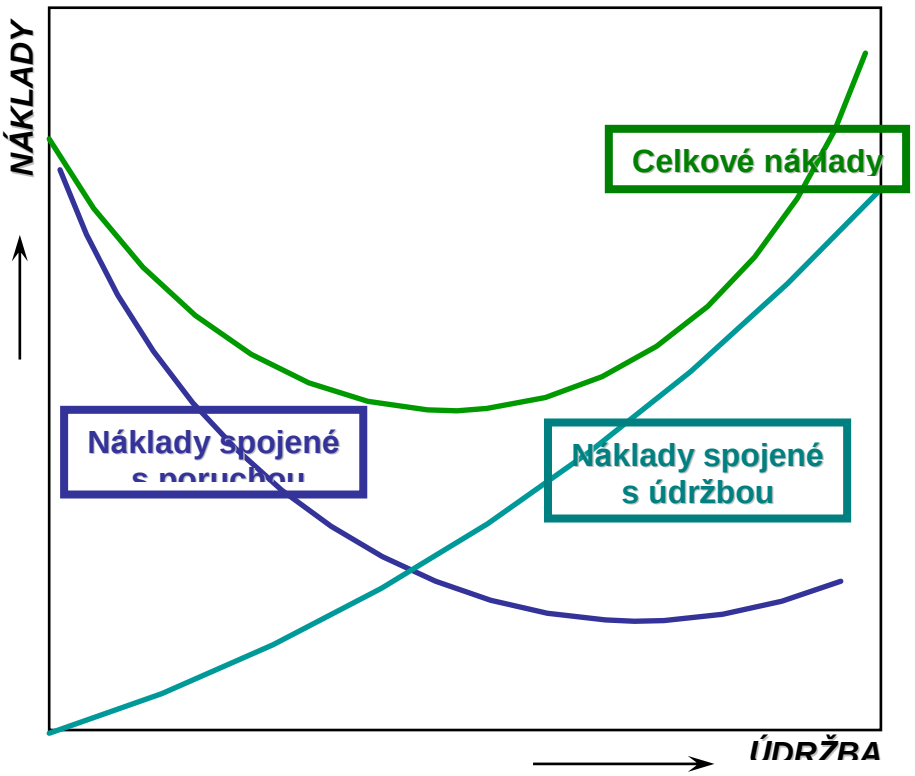
V souladu s klasifikací nežádoucích událostí [1] lze o bezpečnosti technických objektů hovořit pouze v případě ohrožení zdraví a života člověka. Typickým představitelem jsou například technické objekty jaderné i klasické energetiky, plynárenství, petrochemie apod. Existuje řada technických objektů, jejichž provoz a poruchy nemají tak zřejmý vliv na zdraví a životy obyvatelstva jako v předchozím případě. Zdálo by se, že zde nelze hovořit o problematice bezpečnosti a riziko vyplývá např. jen z výrobních či jiných ztrát způsobených jejich poruchou. V mnoha případech je tento pohled zužující, protože i běžné technické objekty charakteru strojního, přístrojového či jiného vybavení skrývají v sobě potenciál možného zranění či usmrcení obsluhujícího personálu (zachycení rotující částí, úraz elektrickým proudem, popálením apod.). Proto se hodnotí i faktor bezpečnosti těchto objektů prostřednictvím analýzy rizik jejich provozu a údržby. Tento fakt je názorně dokumentován i v připravované revizi standardu ISO 14121 [1].

Uvedené skutečnosti jsou důvodem k tomu, aby při optimalizaci údržby se vždy zvažovaly všechny 3 kategorie následků spojených s provozem a poruchami technických objektů (ekonomické, zdravotní a bezpečnostní, ekologické). Tyto kategorie následků jsou pak převáděny do finančního ocenění pro účely porovnání s náklady na údržbu a pro možnost jejich optimalizace.

3 OPTIMALIZACE ÚDRŽBY A ANALÝZA RIZIK

Základním principem optimalizace údržby je, aby prostředky vynakládané na údržbu byly v souladu s přínosy, které tato údržba přináší. Zjednodušeně lze říci, že údržba se může pohybovat mezi dvěma krajními polohami:
nulová údržba - zařízení je provozováno až do poruchy (havárie),
maximalistická preventivní údržba - zařízení je provozováno (teoreticky) bez poruchy.

V prvním případě jsou náklady na údržbu nulové a ztráty plynou jen z následků poruch, včetně ztrát z disponibility zařízení vlivem poruchy. Ve druhém případě jsou ztráty z následků poruch nulové, ale je třeba vynakládat značné prostředky na monitorování stavu zařízení, preventivní údržbu a uvažovat ztráty z disponibility zařízení vlivem údržby. Reálně se údržba pohybuje mezi těmito polohami jak dokumentuje obr. 1.



Obr.1: Náklady a údržba

Vzhledem k tomu, že riziko je zjednodušeně řečeno kombinace pravděpodobnosti výskytu poruchy a důsledků poruchy, jsou analýzy rizika základním nástrojem optimalizace údržby. Při této optimalizaci jde v podstatě o jednoduché ekonomické hodnocení, zda roční náklady na preventivní údržbu zařízení jsou v rozumném poměru k riziku, kterému údržba zabránila. Jinými slovy řečeno, náklady na údržbu nikdy nesmí být vyšší než ztráty plynoucí z rizika, které údržba odstranila.

Tuto skutečnost lze vyjádřit jednoduchým vztahem indexu efektivnosti údržby (1).

$$I\,[1] = \frac{R_{NO}[Kč/rok] - R_{UO}[Kč/rok]}{N_{PU}\,[Kč/rok]} \qquad (1)$$

I ... index efektivnosti údržby
R_{NO} ... riziko neudržovaného objektu (bez preventivní údržby)
R_{UO} ... riziko udržovaného objektu (s preventivní údržbou)
N_{PU} ... náklady na preventivní údržbu

S ohledem na definici rizika je zřejmé, že riziko objektu bez preventivní údržby je dáno velikostí následků poruchy a pravděpodobností vzniku poruchy neudržovaného objektu podle vztahu (2) a pro riziko preventivně udržovaného objektu pak obdobně podle vztahu (3).

$$R_{NO}\,[Kč/rok] = \frac{N_F\,[Kč]}{MTBF_{NO}[rok]} \qquad (2)$$

$$R_{UO}\,[Kč/rok] = \frac{N_F\,[Kč]}{MTBF_{UO}[rok]} \qquad (3)$$

N_F ... následky poruchy ve finančním ocenění
$MTBF_{NO}$ ... střední doba mezi poruchami neudržovaného objektu
$MTBF_{UO}$ ... střední doba mezi poruchami udržovaného objektu

Obecně platí, že $MTBF_{NO}$ (vycházející z nulové údržby) je odhadovaný dolní limit MTBF, zatímco $MTBF_{UO}$ (kdy se předpokládá optimální preventivní údržba), je odhadovaný horní limit MTBF. Pro vztah těchto parametrů platí rovnice (4).

$$MTBF_{NO} \langle\ MTBF \langle\ MTBF_{UO} \qquad (4)$$

Aby preventivní údržba měla ekonomické opodstatnění, je zřejmé, že index efektivnosti údržby musí být větší než 1, viz (5).

$$I = \frac{R_{NO} - R_{UO}}{N_{PU}} = \frac{\frac{N_F}{MTBF_{NO}} - \frac{N_F}{MTBF_{UO}}}{N_{PU}} \rangle 1 \qquad (5)$$

Ze vztahu (5) je vyplývá, že pro optimalizaci údržby tak, aby byla nákladově efektivní, je třeba znát pouze 4 parametry. Problém zpravidla spočívá v tom, jak získat jejich hodnoty.

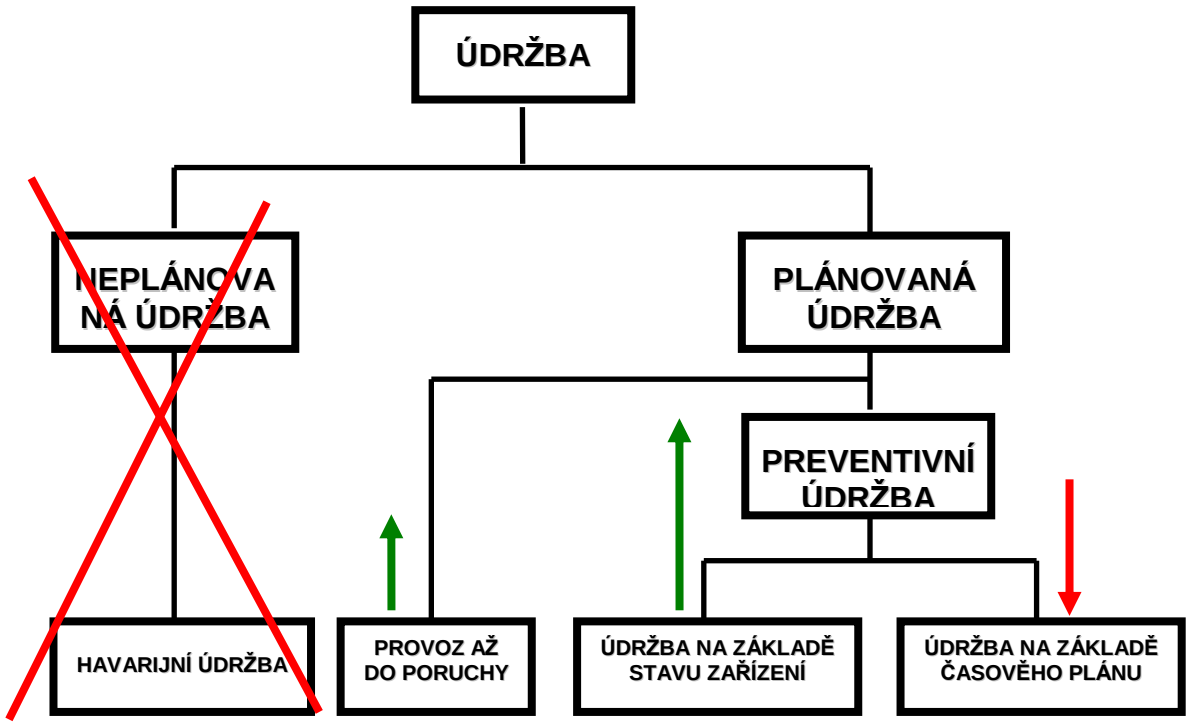
Uvedené skutečnosti byly založeny na předpokladu, že zařízení se porouchává pouze jedním způsobem (módem). Ve skutečnosti se zařízení může porouchat různým způsobem a pak vztahy (1) až (5) je třeba aplikovat ke každému módu poruchy.

4 OPTIMALIZACE ÚDRŽBY V PODMÍNKÁCH PROVOZU

Zpravidla nejméně problematické je v provozu získání hodnoty N_{PU}, protože náklady na údržbu jsou evidovány a sledovány ekonomickými systémy podniku. Ne vždy je však možné provést jejich alokaci na konkrétní zařízení, protože bývají sledovány zpravidla podle vnitropodnikové struktury.

Hodnoty $MTBF_{NO}$, $MTBF_{UO}$ a N_E jsou získávány v rámci analýzy rizik. $MTBF_{NO}$ a $MTBF_{UO}$ zpravidla formou odhadů založených na zkušenostech s provozem zařízení v reálných provozních podmínkách. Hodnoty N_E se získávají formou odhadů či výpočtů ztrát.

Optimalizace údržby potom probíhá volbou vhodných úkolů preventivní údržby, kterými je u jednotlivých módů poruch dosaženo prodloužení MTBF či snížení nákladů na údržbu tak, aby byla efektivní. Při optimalizaci údržby je snaha maximálně eliminovat neplánovanou (havarijní) údržbu a omezit plánovanou údržbu prováděnou na základě časového plánu. Preferovanými typy údržby, viz obr. 2, je údržba prováděná na základě skutečného stavu zařízení a u zálohovaného zařízení je často výhodným běh až do poruchy (run to failure).



Obr.2: Preferované postupy údržby

Protože praktické zkušenosti s optimalizací údržby na základě hodnocení přínosů a nákladů (CBA - Cost Benefit Analysis) prokázaly velkou efektivitu využití postupů analýzy rizika při stanovení programu preventivní údržby, byly tyto postupy standardizovány a zařazeny do norem managementu spolehlivosti [3] jako údržba zaměřená na bezporuchovost (RCM - Reliability Centred Maintenance).

Tyto postupy jsou zpravidla v jednotlivých odvětvích přizpůsobeny specifickým podmínkám a využívají i softwarovou podporu k provádění analýz. Příkladem může být např. společnost Shell, která pro optimalizaci údržby v petrochemickém průmyslu vyvinula systém pro řízení rizika a bezporuchovosti (RMM - Risk&Reliability Management). Systém RRM zahrnuje následující, sice vzájemně propojené, ale v zásadě samostatné, metodiky:

- S-RCM (Shell Reliability Centred Maintenance - Údržba zaměřená na spolehlivost - dle metodiky Shell) představuje metodologii pro optimalizaci údržbových prací. Jedná se o usměrněnou a více ekonomicky orientovanou verzi tradičního/klasického procesu RCM.

- S-RBI (Shell Risk Based Inspection - Inspekce na základě rizika - dle metodiky Shell) je metodologie pro optimalizaci inspekčních a monitorovacích prací. Používá se k řízení integrity tlakových zařízení.

- SIFpro je klasifikační a implementační metodologie ochranných funkcí bezpečnostních systémů. Jejím účelem je poskytnout uživatelům návod pro bezpečný, nákladově efektivní a konzistentní design a údržbovou strategii pro ochranné funkce bezpečnostních systémů.

5 ZÁVĚR

Úspěšná implementace analýzy rizik pro optimalizaci údržby formou RCM vyžaduje dobré pochopení funkce zařízení spolu s pochopením možných poruch a důsledků těchto poruch pro zařízení a jeho okolí. Aplikace metody RCM vyžaduje podrobnou analýzu zařízení a jeho funkcí, což klade značné nároky na kapacity pracovníků a tudíž je relativně nákladné. Z tohoto důvodu je RCM využívána pouze tam, kde je údržba kritická z hlediska bezpečnosti a efektivnosti provozu zařízení a kde by poruchy mohly mít vážné následky pro bezpečnost, životní prostředí nebo provoz. Je zřejmé, že optimalizace údržby prováděná na základě analýzy rizika představuje značný ekonomický potenciál, který může být rozhodující pro výkonnost a tedy i konkurenceschopnost výrobních subjektů. A to zejména u subjektů s vysokou investiční náročností, nepřetržitým provozem a s možností značných následků v případě jejich havárie (energetika, petrochemie, plynárenství apod.).

LITERATURA

[1] FUCHS, P.: Pravděpodobnostní hodnocení rizika. In: 10. seminář Odborné skupiny pro spolehlivost České společnosti pro jakost - Spolehlivost a analýza rizik. Praha, 2003.

[2] ISO 14121: 1999 Safety of machinery - Principles of risk assessment.

[3] ČSN IEC 60300-3-11: 1999 Management spolehlivosti. Část 3-11: Návod k použití - Údržba zaměřená na bezporuchovost.