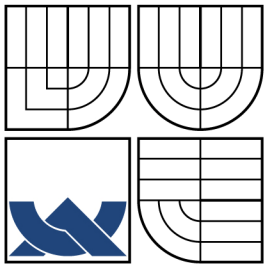

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
LETECKÝ ÚSTAV

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF AEROSPACE ENGINEERING

PŘECHOD OD PROGRMU PREVENCE NEHOD A BEZPEČNOSTI LETŮ K SYSTÉMU ŘÍZENÍ BEZPEČNOSTI U MALÉHO LETECKÉHO DOPRAVCE

TRANSITION FROM ACCIDENT PREVENTION AND FLIGHT SAFETY PROGRAMME TO SAFETY MANAGEMENT SYSTEM IN A SMALL AIR OPERATOR

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. ALEŠ HLOUCAL
AUTHOR

VEDOUCÍ PRÁCE — Ing. ONDŘEJ SCHAUMANN, Ph.D.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Letecký ústav
Akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Aleš Hloucal

který/která studuje v **magisterském navazujícím studijním programu**

obor: **Letecký provoz (3708T011)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Přechod od Programu prevence nehod a bezpečnosti letu k Systému řízení bezpečnosti u malého leteckého dopravce

v anglickém jazyce:

Transition from Accident Prevention and Flight Safety Programme to Safety Management System in a small air operator

Stručná charakteristika problematiky úkolu:
V souladu s obvyklými trendy v civilním letectví vnikl v posledních letech požadavek na další navyšování úrovně bezpečnosti formou řízení možných rizik komplexním systémem integrovaným do všech součástí letecké společnosti, tj. do oblastí letového provozu, pozemního provozu, výcviku veškerého personálu i zachování letové způsobilosti včetně údržby letadel. Tento tzv. systém řízení bezpečnosti (Safety Management System) významně rozvíjí stávající požadavky EU-OPS na tzv. Program prevence nehod a bezpečnosti letu, který byl omezeně zaměřen především na letový provoz.
Tento požadavek odráží nejen navrhované změny ICAO Annex 6/I, ale i další připravované legislativy EU (Part OPS,…). Pro letecké společnosti, které dosud nezavedly SMS v navrhované podobě na dobrovolné bázi, tak vzniká potřeba budoucího přechodu od již zavedených minim na novou úroveň s mnoha dopady na celou organizaci.
Úkolem diplomanta bude popsat výchozí stav, prostudovat požadavky a doporučení ICAO Doc.9859 a navrhnout postup přechodu na plně integrovaný systém řízení bezpečnosti, s přihlédnutím k řade specifik malého provozovatele letecké dopravy. Práce bude obsahovat též popis "cílového stavu"", všech vstupu, výstupu a hlavních funkcí, začlenění do systému jakosti a do organizace společnosti jako celku.

Cíle diplomové práce:
Návrh postupu přechodu na plně integrovaný systém řízení bezpečnosti, s přihlédnutím ke specifikum malého leteckého provozovatele

Seznam odborné literatury:

ICAO Doc.9859 AN/460
Nařízení komise (ES) č.859/2008, vč. přílohy III (EU-OPS)
Předpis L6 – Provoz letadel, případně zdrojový Annex 6/I (ICAO)
Další doporučení a stanoviska ÚCL a Ministerstva dopravy ČR vztahující se k dané problematice

Vedoucí diplomové práce: Ing. Ondřej Schaumann, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2009/2010.

V Brně, dne 20.11.2009

L.S.

_____	_____
prof. Ing. Antonín Píštěk, CSc.	prof. RNDr. Miroslav Doupovec, CSc.
Ředitel ústavu	Děkan fakulty

Anotace

Cílem této diplomové práce je návrh postupu přechodu na plně integrovaný systém řízení bezpečnosti, s přihlédnutím ke specifikům malého leteckého provozovatele. To znamená popsání výchozího stavu, prostudování požadavků a doporučení ICAO Doc.9859 a návrh postupu přechodu na plně integrovaný systém řízení bezpečnosti, s přihlédnutím k řadě specifik malého provozovatele letecké dopravy. Práce rovněž obsahuje popis "cílového stavu", všech vstupů, výstupů a hlavních funkcí, začlenění do systému jakosti a do organizace společnosti jako celku.

Annotation

The aim of the Master´s thesis is the design process of transition to a fully integrated safety management system, taking into consideration the unique characteristics of small air operators. It means describing the initial situation, studying the requirements and recommendations of ICAO Doc.9859 a proposal for the transition to fully integrated security management system, taking into account the specifics of a small air operators. Work also includes a description of the "target state", all inputs, outputs and main functions, integration into the quality system and the organization of society as a whole.

Klíčová slova

Systém řízení bezpečnosti, politika bezpečnosti, řízení bezpečnostního rizika, GAP analýza, vedoucí bezpečnosti

Key words

Safety management system, safety policy, safety risk management, GAP analysis, safety manager

Bibliografická citace

HLOUCAL, A. Přechod od Programu prevence nehod a bezpečnosti letů k Systému řízení bezpečnosti u malého leteckého dopravce. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2010. 40s. Vedoucí diplomové práce Ing. Ondřej Schaumann, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem byl seznámen s předpisy pro vypracování diplomové práce, a že jsem celou diplomovou práci vypracoval samostatně, pod odborným vedením vedoucího diplomové práce s použitím uvedené literatury.

V Brně 29.4. 2010 .....

Bc. Aleš Hloucal

Poděkování

Děkuji svému vedoucímu diplomové práce panu Ing. Ondřeji Schaumannovi, Ph.D. za jeho ochotu a cenné rady a připomínky. Dále bych pak chtěl poděkovat panu Ing. Františku Vlčkovi z ÚCL a panu Aleši Kvíčalovi, vedoucímu jakosti společnosti CCA, za jejich užitečné informace.

Obsah

1. Úvod

Bezpečnost je jedním ze základních požadavků pro všechny druhy dopravy. Bohužel neexistuje nic takového, jako absolutní bezpečnost. V letectví, ani jinde, není možné úplně odstranit všechna bezpečnostní rizika. Můžeme však jejich výskyt snížit na přijatelné minimum. Nástroj, který by toto měl zajistit se nazývá Systém řízení bezpečnosti (Safety Management System – SMS). Tento nový systém má nahradit Program prevence nehod a bezpečnosti letů, který byl omezeně zaměřen především na letový provoz. Hlavním důvodem pro zavedení Systému řízení bezpečnosti je zvýšení současné úrovně bezpečnosti v letectví pomocí systematického procesu identifikace, vyhodnocování a zmirňování nebezpečí. Výhodou tohoto systému je, že pokrývá všechny provozní části společnosti (letový provoz, pozemní provoz i systém zachování letové způsobilosti) a vnáší tak potřebné bezpečnostní principy do všech důležitých provozních úseků. Tím omezuje výskyt případné nehody a snižuje tak možnost vzniku negativního obrazu letecké společnosti v očích veřejnosti.

2. Problematika řízení bezpečnosti

Vzhledem k povaze letectví není v lidských silách eliminovat všechny nehody a vážné incidenty. Žádné lidské snažení a úsilí, nebo lidmi vytvořený systém, nemohou být zcela osvobozeny od možného výskytu chyb. Vždy existuje určitá míra rizika. Stále se musí očekávat, že může dojít k nějakému selhání, a to i přes co nejvyšší vynaložené preventivní úsilí. Proto je zde snaha o co největší snížení výskytu možných chyb a tím zmenšení rizika.

2.1 Vývoj řízení bezpečnosti

V počátcích rozvoje letecké dopravy se přístupy k prevenci nehod zaměřovaly zejména na zajištění technické bezpečnosti. To se týkalo hlavně konstrukcí a výroby letadel. Později se začaly zaměřovat i na nebezpečné a nezodpovědné chování provozního personálu. Zavedená opatření pro zvýšení bezpečnosti se týkala pouze zjištěných skutečností. To znamená, že se problémy začaly řešit až poté, co došlo k nějaké nehodě. Často bylo pouze zjištěno „co“, „kdo“, „kdy“ a „jak“, ale již ne „proč“. Organizační souvislosti a souvislosti s lidským činitelem a prostředím, které byly nejednou hlavní příčinou chyb, byly často opomíjeny a přijatá opatření byla zaměřena pouze na dané zjištěné příznaky.

V padesátých letech minulého století se prevence nehod zaměřovala téměř výhradně na technické příčiny nehod. V sedmdesátých letech se došlo vývojem k poznání, že lidský faktor hraje stále důležitější roli ohledně bezpečnosti. A to zejména proto, že letadla byla už dostatečně technicky vyspělá, že k nehodám z technických příčin docházelo spíše ojediněle. Proto dochází k zavádění prvních bezpečnostních programů a postupů, jejichž cílem je prevence nehod a incidentů.

Dochází k vyšetřování a analyzování příčin drobných incidentů a selhání jak techniky, tak lidského činitele. Je čím dál více jasné, že výskyt mnoha malých selhání, která samy o sobě nemají prakticky žádný dopad na bezpečnost, může vést k celému řetězci událostí, který ve svém důsledku může způsobit leteckou katastrofu. Se zavedením velkokapacitních letadel jako je Boeing 747, McDonell Douglas DC-10 nebo Airbus A300 měl výskyt takové letecké katastrofy velký dopad na širokou veřejnost, zejména pak díky publicitě v médiích po celém světě.

Zatímco v dnešní době dochází ke katastrofám pouze zřídka, menší incidenty jsou celkem běžnou součástí leteckého provozu. Nemůžeme je však úplně ignorovat, protože by mohly být signálem blížící se katastrofy. Proto je dnes základem každého bezpečnostního systému práce s provozními daty jejich sbírání, porovnávání, vyhodnocování a následná nápravná opatření.

V devadesátých letech se dospělo k závěru, že lidskou činnost významně ovlivňují také organizační faktory. Jedná se o veškeré procesy, které v organizační struktuře leteckého provozovatele probíhají, zejména z hlediska kvality rozhodovacího procesu vrcholového vedení organizace. V současné době se zkoumání příčin nehod zaměřuje i na procesy v organizaci, skryté předpoklady, pracovní podmínky, lidský faktor, dostatečnost ochranných nástrojů a také na aktivní selhání.

Důležitou roli hrají také peníze. Je nutné uvědomit si, co všechno může letecká katastrofa pro leteckou společnost znamenat. Kromě ztráty letadla bude muset odškodnit pozůstalé po obětech a také přijde o svoji pověst a zákazníky. Pro malou leteckou společnost to znamená prakticky likvidaci. Proto je lepší investovat peníze do prevence nehod a sytému

bezpečnosti. Ovšem vyvstává otázka: Kolik investovat? Na tuto otázku neexistuje jednoduchá odpověď.

Pakliže letecká společnost investuje příliš mnoho peněz do zajištění bezpečnosti, může tím ve svém důsledku ohrozit vlastní provoz a existenci. Přesunutí velké části finančních zdrojů do systému bezpečnosti sice zvýší bezpečnost, ale zároveň způsobí, že finance budou scházet jinde. Naopak nedostatečná investice do systému bezpečnosti může mít za následek katastrofickou událost. Proto by mělo vedení letecké společnosti volit střední cestu mezi těmito dvěma možnostmi, viz. kapitola 7.4.3 Přidělování finančních prostředků.

3. Základní pojmy a definice

Důležité pojmy k pochopení Systému řízení bezpečnosti definované podle ICAO Doc. 9859 Safety Management Manual.

Systém řízení bezpečnosti (Safety Management System - SMS)

je to organizovaný přístup k řízení bezpečnosti, včetně nutné organizační struktury, odpovědností a přístupu k bezpečnosti. Systém řízení bezpečnosti je zaměřen na pro-aktivní přístup k zjišťování nebezpečí a řízení bezpečnostního rizika.

Zjišťování nebezpečí (Hazard Identification)

je aktivní proces sběru, analýzy a zdokumentování nebezpečí formou bezpečnostních údajů. Zabývá se vytvářením zpětné vazby o nebezpečí a s ním spojenými bezpečnostními riziky, která ovlivňují bezpečnost všech provozních činností organizace. Zjišťování nebezpečí ve vyspělém SMS je nikdy nekončícím a stále pokračujícím procesem.

Řízení bezpečnostního rizika (Safety Risk Management)

je proces od identifikace a analýzy nebezpečí k vyhodnocení a zmírnění bezpečnostních rizik následků nebezpečí na úroveň tak nízkou, jak je přiměřeně možné (As Low As Reasonably Practicable – ALARP).

Bezpečnost (Safety)

je to stav, ve kterém je riziko újmy osob nebo poškození majetku omezeno na přijatelnou úroveň a udržováno na přijatelné úrovni nebo pod ní, a to pomocí průběžného a neustálého procesu zjišťování nebezpečí a řízení bezpečnostního rizika. Jinými slovy, bezpečnost je stav, ve kterém riziko újmy nebo poškození je omezeno na přijatelnou úroveň.

4. Systém řízení bezpečnosti

Systém řízení bezpečnosti (Safety Management System – SMS) je organizovaný přístup k řízení bezpečnosti, včetně nutné organizační struktury, odpovědností a přístupu k bezpečnosti. Systém řízení bezpečnosti je zaměřen na systémový pro-aktivní přístup k zjišťování nebezpečí a řízení bezpečnostních rizik. Zahrnuje provozní i technické části organizace. To znamená, že je zaměřen jak na letový provoz, tak i na pozemní provoz, údržbu letadel, na výcvik personálu a další. Systém řízení bezpečnosti usiluje o zvýšení a zlepšení organizačního přístupu k řízení bezpečného a efektivního leteckého provozu. Hlavním důvodem pro zavedení SMS je zvýšení současné úrovně bezpečnosti v letectví pomocí systematického procesu zjišťování nebezpečí a vyhodnocování a zmirňování rizik.

Důležité je uvědomit si, že SMS je systém „od shora dolů“, což znamená, že odpovědný vedoucí je odpovědný za zavedení a průběžné vyhovění SMS. Bez naprosté a bezvýhradné podpory odpovědného vedoucího nebude SMS účinný. Není možné sestavit model, který by byl jako jediný vhodný pro všechny organizace. Složitý model SMS je nevhodný pro malé organizace. Proto by malé organizace měly přizpůsobit svůj SMS k rozsahu, povaze a složitosti svého provozu a činností. To znamená podle toho přidělovat své zdroje.

Bezpečnost nemůže být zajištěna pouhým zavedením předpisů, pravidel a směrnic, které se týkají postupů a které musí být dodržovány provozními zaměstnanci. Na zachování úrovně bezpečnosti má největší vliv většina činností v organizaci. Proto musí řízení bezpečnosti začít u vrcholového vedení organizace a účinky na bezpečnost musí být přezkoumávány na všech úrovních této organizace. SMS je tedy systematický, organizovaný a pro-aktivní přístup k řízení bezpečnosti, včetně organizační struktury, odpovědností, politiky a postupů. Sjednocuje provozní a technický systém s řízením finančních a lidských zdrojů za účelem zajištění bezpečného provozu s tak nízkým rizikem, jak je přiměřeně možné (As Low As Reasonably Practicable – ALARP).

Pro-aktivním přístup k řízení bezpečnosti je metoda aktivního přístupu k řízení bezpečnosti. Tato metoda se zaměřuje na prevenci pomocí procesu neustálé, průběžné a aktivní identifikace nebezpečí a procesu řízení bezpečnostních rizik. Řízení bezpečnostních rizik znamená vyhodnocení a zmírnění bezpečnostních rizik následků nebezpečí dříve, než by mohlo dojít k událostem ovlivňujících bezpečnost. Pro-aktivní přístup k řízení bezpečnosti je tedy založen na podstatě, že selhání systému může být minimalizováno identifikací bezpečnostních rizik následků nebezpečí a provedením nutné činnosti pro jejich zmírnění v daném systému dříve, než tento daný systém selže.

Všechny tyto nutné činnosti spojené s řízením bezpečnosti by měly být pečlivě zdokumentovány a být hlavní součástí všech řídících činností organizace. SMS je organizovaný a systematicky řízený tehdy, pokud jsou tyto činnosti prováděny v souladu s předem stanoveným plánem a aplikovány důsledně napříč celou organizací.

4.1 Dokumenty zabývající se SMS

Systémem řízení bezpečnosti se zabývá především ICAO Safety Management Manual (Doc.9859) – Second Edition. Dokument slouží jako průvodce touto problematikou a je určen nejen pro letecké provozovatele, ale také pro provozovatele letišť, poskytovatele servisních

služeb a řízení letového provozu. Dále se v podstatě SMS věnuje i část Annexu 6/I (ICAO) a Nařízení komise (ES) č.859/2008, vč. přílohy III (EU-OPS), která se v části 1.037 zabývá Programem prevence nehod a bezpečnosti letů.

Mezinárodní organizace pro civilní letectví ICAO požaduje zavedení řízení bezpečnosti, které se skládá ze státního programu bezpečnosti (State Safety Programme - SSP) a ze systému řízení bezpečnosti (Safety Management System - SMS). Za zavedení a udržování SSP je odpovědný příslušný členský stát ICAO. V České Republice se o tyto náležitosti stará Ministerstvo dopravy. SMS by měl vycházet ze státního programu bezpečnosti a za jeho zavedení a udržování je odpovědná každá příslušná organizace v letectví (provozovatelé obchodní letecké dopravy, provozovatelé letišť, poskytovatelé služeb řízení letového provozu a údržbové organizace). Zavedení a udržování SMS by mělo být průběžně dozorováno příslušným Leteckým úřadem. V České Republice je to Úřad pro civilní letectví.

4.2 Strategie SMS

Existují tři druhy přístupu k řízení bezpečnosti:

Re-aktivní strategie

Tato strategie reaguje na události, které se již staly. Jejím cílem je dosáhnout takových opatření, aby se daná událost v budoucnosti nemohla opakovat.

Pro-aktivní strategie

Cílem tohoto aktivního přístupu je identifikovat bezpečnostní problémy dříve, než vyvolají nežádoucí událost.

Prediktivní strategie

Tato strategie se zabývá identifikací možného bezpečnostního problému v reálném čase při normálním běžném provozu organizace.

Systém řízení bezpečnosti pro svoje správné a efektivní fungování vyžaduje kombinaci těchto tří strategií.

4.3 Vstupy a výstupy SMS

4.3.1 Vstupy SMS:

- **Zpráva o kvalitě z letu (Quality report)**
  Formulář zprávy o kvalitě obsahuje hlášení o různých nedostatcích jako je například nevyhovující ubytování pro posádku, nedostatečná úroveň přípravy kabiny a podobně. Je určena zejména pro systém kvality a je primárně zaměřena na jakost celého procesu dopravy z pohledu klienta - cestujícího. Tento formulář vyplňuje posádka (kapitán letadla).

- **Systém kvality, nálezy auditů**
  Obsahuje bezpečnostní checklisty a výsledky auditů zajišťovaných systémem jakosti.

- **Hlášení z letů**
  Toto hlášení podává posádka letadla a týká se technických selhání, srážky s ptáky (birdstrike), zásahů bleskem a podobně.

- **Hlášení o překročení doby ve službě**
  Pakliže posádka letounu překročí maximální povolenou dobu ve službě nebo zkrátí minimální předepsaný odpočinek o méně než jednu hodinu, musí vyplnit interní hlášení o překročení doby ve službě. Při překročení doby ve službě nebo zkrácení základního odpočinku o více než jednu hodinu se musí podat hlášení i na ÚCL.

- **Systém prevence nehod a bezpečnosti letů**
  Je založen na analýze zpráv z anonymního hlášení událostí a z ústního hlášení událostí vedoucímu bezpečnosti, vedoucímu letového provozu nebo odpovědnému vedoucímu.

- **Technický deník, kniha letů**
  Obsahují závady na letadle, zjištěné za letu.

- **Osobní zjištění vedoucího bezpečnosti**
  Bezpečnostní informace získané osobním rozhovorem se zaměstnanci organizace.

- **Ostatní**
  Ostatní možné způsoby získání bezpečnostních informací.

4.2.2 Výstupy SMS:

- Úpravy provozních příruček a postupů v organizaci
- Informační bulletiny
- Prezentace stavu bezpečnosti v rámci výcviku
- Komunikace otázek bezpečnosti mezi provozními úseky
- Specializovaný bezpečnostní výcvik a vzdělávání
- a další

viz. kapitola 9. Podpora bezpečnosti

4.4 Bezpečnostní kultura organizace

Jedním z nejdůležitějších atributů pro účinné fungování SMS je úroveň bezpečnostní kultury organizace. Pozitivní bezpečnostní kultura tak jako celý systém řízení bezpečnosti musí být vytvářena „od shora dolů“. Úroveň bezpečnostní kultury organizace je založena na vysokém stupni důvěry mezi zaměstnanci a vrcholovým vedením. Zaměstnanci musí věřit a mít jistotu, že budou mít podporu pro rozhodnutí, které udělají v zájmu bezpečnosti. Musí ale rovněž pochopit, že nedbalost, nebo úmyslné porušení bezpečnosti, které ohrožuje provoz, nebude tolerováno.

Bezpečnostní kultura organizace je soubor trvalých hodnot a postojů, vztahujících se k problematice bezpečnosti, sdílených všemi příslušníky na každé úrovni organizace. Úroveň bezpečnostní kultury organizace závisí:

- Na úrovni a hloubce uvědomování si rizika a neznámých nebezpečí každým jednotlivcem nebo skupinou v dané organizaci.
- Na chování, které udržuje a zvyšuje bezpečnost.
- Na vůli postavit se čelem k bezpečnostním problémům.
- Na vůli sdílet a šířit informace o bezpečnostních problémech.
- Na důsledném vyhodnocování reakcí, týkajících se problémů bezpečnosti.

Základem pro účinný systém řízení bezpečnosti je účinný systém bezpečnostních hlášení. Kromě povinného hlášení nehod a incidentů by měl být zaveden především dobrovolný systém hlášení bez jakýchkoli postihů pro ohlašovatele, nebo důvěrný systém hlášení nebezpečí událostí, nedostatků, chyb a pochybností týkajících se bezpečnosti. Jinými slovy: Má-li někdo z provozního personálu pochybnosti o bezpečnosti, měl by to ohlásit aniž by se musel bát případného postihu. Účinný systém bezpečnostních hlášení je tedy základem pro získání bezpečnostních údajů. Jakmile jsou bezpečnostní údaje získány, musí být následně analyzovány a řízeny.

Účinný systém bezpečnostních hlášení musí být postaven na těchto základech:

- Vrcholové vedení klade velký důraz na identifikaci nebezpečí a uvědomuje si důležitost šíření a předávání bezpečnostních informací na všech úrovních organizace.
- Vrcholové vedení i provozní personál mají reálný pohled na nebezpečí, kterým čelí organizace při svých činnostech.
- Vrcholové vedení definuje požadavky pro podporu aktivního hlášení nebezpečí. Zajišťuje, že klíčové bezpečnostní údaje jsou řádně zaznamenávány a zavádí opatření na základě rozboru následků.
- Vrcholové vedení zajišťuje, že klíčové bezpečnostní údaje jsou řádně chráněny. Podporuje systém kontrol tak, že hlášení nebezpečí nebude použito jinak, než pro co bylo zavedeno.
- Personál je školen tak, aby rozpoznal a nahlásil nebezpečí a také rozuměl jeho následkům v činnostech, které zajišťuje jeho organizace.

Charakteristika organizace z hlediska její bezpečnostní kultury závisí na tom, jak reaguje na informace o nebezpečí a na řízení bezpečnostních informací:

Charakteristiky	**Bezpečnostní kultura**		
	Špatná	**Byrokratická**	**Pozitivní**
Oznámení nebezpečí je:	Potlačeno	Ignorováno	**Aktivně vyhledáváno**
Zaměstnanci, kteří nebezpečí oznámí jsou:	Odrazováni, nebo jinak negativně postiženi - označováni jako „potížisté“	Trpěni	**Cvičeni, povzbuzováni, odměňováni**
Odpovědnost za bezpečnost je:	Vyhýbavá	Roztříštěna	**Sdílena**
Šíření bezpečnostních informací je:	Odrazováno	Dovoleno, ale odrazováno	**Systémově zajištěno, odměňováno**
Selhání vede k:	Přikrytí, „zametení pod koberec“	Lokálnímu zafixování	**Šetření a systémové nápravě**
Nové nápady jsou:	potlačovány	považovány za nový problém, nikoli za příležitost	**Vítány a podporovány**

Tabulka 4.1 Druhy bezpečnostních kultur organizace (přepracováno podle [6])

Bez ohledu na velikost organizace a jejího provozu, úspěšné fungování SMS závisí na míře, s jakou vrcholové vedení věnuje čas a úsilí bezpečnosti jako stěžejní záležitosti celkového řízení organizace.

Vrcholové vedení v čele s odpovědným vedoucím má konečnou odpovědnost za celkový přístup organizace k otázce bezpečnosti. Pozitivní bezpečnostní kultura organizace bude záviset na přístupu vrcholového vedení k zajištění bezpečného provozu.

Nesprávný přístup vrcholového vedení k bezpečnosti může mít i fatální následky. Zde je příklad nesprávného přístupu, který vedl k selhání lidského faktoru, když posádka letounu musela jednat pod tlakem vedení společnosti na úkor bezpečnosti. Tento případ se stal 20. prosince 2001.

Cessna Citation HB-VLV přiletěla po charterovém letu z East Midlands do Zürichu ve 20:31. Letadlo mělo naplánován přelet do Bernu na tentýž večer. Odlet však musel byl odložen kvůli zhoršujícímu se počasí. To znamenalo zvýšení tlaku na posádku, protože letadlo muselo přistát v Bernu do 22:30. Pro tento přílet dostal generální ředitel společnosti zvláštní povolení. Ve 21:43 posádka obdržela povolení pro spouštění motorů. Posádka pojížděla na dráhu 34 a poté, co obdržela povolení ke vzletu ve 22:05:54, zahájila vzlet. V této době byla meteorologická dohlednost pouhých 100 m. Po dosažení výšky 500 až 600 ft nad úrovní terénu letadlo začalo ztrácet výšku. Posádka zahájila nápravný manévr i když nebyla schopna zabránit nárazu letadla do země. Letadlo dopadlo na zmrzlou zem 400 m jihovýchodně od konce RWY 34. Oba piloti při nárazu zahynuli.

K nehodě došlo tím, že posádka HB-VLV nepokračovala ve stoupání po vzletu, v důsledku čehož letadlo přešlo do klesání a narazilo do terénu. Šetření stanovilo následující příčinu nehody: S vysokou mírou pravděpodobnosti posádka po vzletu ztratila prostorovou orientaci, což vedlo k neúmyslné ztrátě výšky.

K nehodě přispěly tyto faktory:

- Základního výcvik druhého pilota v létání podle přístrojů neobsahoval noční vzlety podle přístrojů.
- **Způsob práce posádky byl nepříznivě ovlivněn velkým časovým tlakem**.
- Vzlet nebyl přizpůsoben převládajícím meteorologickým podmínkám.
- V letadle nebyl žádný systém, který by spustil poplach v případě ztráty výšky po vzletu (GPWS).
- Přístrojové vybavení na palubní desce u druhého pilota nebylo optimální.

K této tragické nehodě by vůbec nedošlo, kdyby posádka letounu dokázala odolat tlaku vedení společnosti a přelet letounu do Bernu odložila do doby, než se zlepší meteorologické podmínky.

4.5 Plán pro zavedení systému řízení bezpečnosti

Prvním krokem pro zavedení Systému řízení bezpečnosti je zpracování plánu pro jeho zavedení. Plán představuje reálnou strategii zavedení SMS, která splňuje všechny potřeby organizace a stanovuje přístup k řízení bezpečnosti. Tento plán by měl být podepsán všemi členy vrcholového vedení a schválen odpovědným vedoucím organizace.

Obsah plánu by měl zahrnovat:

1) Politiku bezpečnosti (přístup k bezpečnosti)
2) Plánované záměry ve vztahu k bezpečnosti a cíle bezpečnosti
3) Popis systému
4) Diferenční analýzu (GAP analýzu), to znamená určit, které SMS komponenty a prvky má již organizace zavedeny a které chybějící komponenty a prvky musí být zavedeny nebo změněny, aby byly splněny požadavky na plné zavedení SMS.
5) Komponenty a prvky SMS
6) Funkce a odpovědnosti vzhledem k bezpečnosti

7) Přístup k podávání bezpečnostních hlášení, tedy politika hlášení událostí a nedostatků ve vztahu k bezpečnosti
8) Prostředky pro zapojení zaměstnanců
9) Bezpečnostní komunikaci (předávání a šíření bezpečnostních informací)
10) Vyhodnocování kvalitativní úrovně bezpečnosti
11) Přezkoumávání kvalitativní úrovně bezpečnosti vedením
12) Výcvik v oblasti bezpečnosti

Výše zmíněné požadavky jsou určené spíše pro velké letecké provozovatele. Jak již bylo zmíněno, složitý model SMS není vhodný pro malé organizace. Proto by malé organizace měly zpracovat zjednodušený plán zavedení SMS, který obsahuje:

1) Přístup provozovatele k řízení bezpečnosti tak, aby splňoval jeho potřeby z hlediska bezpečnosti
2) Součinnost se systémem řízení bezpečnosti jiných organizací, se kterými vzájemně spolupracují při poskytování služeb (organizace, které poskytují danému provozovateli služby na základě smlouvy)
3) Odsouhlasení vrcholovým vedením a způsob zajištění předávání informací napříč celou organizací

5. Komponenty a prvky systému řízení bezpečnosti

SMS by měl obsahovat následující čtyři komponenty, obsahující dvanáct prvků:

a) Politika bezpečnosti a záměry ve vztahu k bezpečnosti

1) Závazek a odpovědnost vedení
2) Odpovědnost vedoucích pracovníků za bezpečnost
3) Jmenování klíčového personálu ve vztahu k bezpečnosti
4) Plán pro nouzové situace
5) Dokumentace a záznamy

b) Řízení bezpečnostního rizika

1) Proces identifikace nebezpečí
2) Proces vyhodnocení a zmírnění rizika

c) Zajištění bezpečnosti

1) Sledování kvalitativní úrovně bezpečnosti, vyhodnocování a přezkum
2) Řízení změn
3) Průběžné zdokonalování systému bezpečnosti

d) Podpora bezpečnosti

1) Výcvik a vzdělávání
2) Bezpečnostní komunikace (předávání, šíření a sdílení bezpečnostních informací)

Výše uvedenými body se budu podrobněji zabývat v následujících kapitolách.

6. Politika bezpečnosti

Politika bezpečnosti je přístup organizace k bezpečnosti. Zabývá se popisem metod a procesů, které chce organizace použít k dosažení požadované úrovně bezpečnosti. Vytvoření pozitivní bezpečnostní kultury se odvíjí od profesionálního vedení v čele s odpovědným vedoucím. Programové prohlášení k bezpečnosti vyjadřuje závazek celé organizace k bezpečnosti a mělo by být podepsáno odpovědným vedoucím.

Příprava politiky bezpečnosti by měla být prováděna ve spolupráci vrcholového vedení s pracovníky, kteří mají na starost kritické oblasti z hlediska bezpečnosti (zejména odpovědný vedoucí, vedoucí bezpečnosti, vedoucí letového provozu, vedoucí systému údržby, případně další). To přispěje ke zvýšení odpovědnosti všech zaměstnanců. Měla by být prokazatelně sdělována a přenášena napříč celou organizací, to znamená, že s politikou bezpečnosti musí být seznámeni všichni zaměstnanci. K prokazatelnému sdělování informací, týkajících se bezpečnosti, může sloužit například informační oběžník. Přečtení a proškolení potvrdí zaměstnanci svým podpisem.

Organizace musí jmenovat odpovědného vedoucího, který má i celkovou odpovědnost za zavedení a udržování systému řízení bezpečnosti. Odpovědným vedoucím může být ředitel, generální ředitel, výkonný ředitel, prezident a podobně. Tento vedoucí má plnou odpovědnost za finanční, lidské a materiální zdroje. Také má přímou odpovědnost za všechny činnosti a záležitosti týkajících se bezpečnosti. U malých organizací je běžné, že jeden člověk zastává více funkcí zároveň, proto může jedna osoba vykonávat současně funkci jak odpovědného vedoucího, tak některé další funkce, příslušející osobám vrcholového vedení. Rovněž musí být stanovena odpovědnost za bezpečnost všech řídících pracovníků a ostatního personálu. U malých provozovatelů by se měly stanovit především odpovědnosti za zjišťování nebezpečí a řízení bezpečnostního rizika. To vše musí být řádně zdokumentováno a uloženo, aby bylo v případě mimořádné události jasné, kdo za co zodpovídá.

Dokumentace SMS by měla být úměrná velikosti a složitosti organizace. Jiný způsob dokumentace bude u velkého leteckého dopravce s desítkami letadel a rozsáhlou sítí linek než u malého charterového nebo business dopravce. Obecně platí, že dokumentace musí obsahovat:

- Použitelné předpisy
- SMS záznamy
- Řízení záznamů
- Příručky řízení bezpečnosti

Je nutné, aby organizace ukládala záznamy o všech opatřeních, která byla přijata v rámci systému řízení bezpečnosti. Tyto záznamy slouží jako důkaz o probíhajících procesech v rámci SMS a také pro sledování úrovně bezpečnosti.

Malé organizace musí vytvořit a udržovat dokumentaci SMS, která by především charakterizovala jejich bezpečnostní politiku, postupy a hlavní výstupy z SMS. Součástí dokumentace musí být také Příručka řízení bezpečnosti (SMM – Safety Management manual).

Pro správný chod SMS je stěžejní jmenování vedoucího bezpečnosti (SM - Safety Manager). Zřizování bezpečnostních výborů není u malých společností nezbytně nutné. Vedoucí bezpečnosti bude odpovědný za rozvoj a udržování účinného SMS. Měl by být zároveň členem vrcholového vedení nejen z důvodu potřebné autority a pravomocí, ale také proto, aby byla zajištěna přímá komunikace s ostatními členy vrcholového vedení v záležitostech týkajících se bezpečnosti. Podřízen by měl být přímo odpovědnému vedoucímu.

Vedoucí bezpečnosti je koordinátor s odpovědností za rozvoj a udržování správného chodu SMS. Není však odpovědný za kvalitativní úroveň bezpečnosti. Odpovědnost za účinný systém řízení bezpečnosti leží na **odpovědném vedoucím,** nikoli na vedoucím bezpečnosti.

6.1 Vedoucí bezpečnosti

Vedoucí bezpečnosti by měl mít řídící zkušenosti z provozu s dostatečnou odbornou způsobilostí. Kromě toho by měl mít zkušenosti a dovednosti pro práci s lidmi, analytické dovednosti a schopnosti pro řešení problémů, dovednosti pro zpracování, řízení a předkládání návrhů a také ústní a písemné komunikační dovednosti a schopnosti. To vše je třeba, aby mohl zajišťovat následující činnosti:

- Řídit plán zavádění SMS v organizaci jménem odpovědného vedoucího.
- Usnadňovat proces řízení rizika, který by měl zahrnovat zjišťování nebezpečí, vyhodnocení rizika a zmírnění rizika.
- Sledovat jakákoli nápravná opatření pro zmírnění rizika
- Zajišťovat pravidelná hlášení o kvalitativní úrovni bezpečnosti v organizaci
- Udržovat dokumentaci týkající se bezpečnosti
- Plánovat a organizovat bezpečnostní výcvik personálu
- Poskytovat nezávislá doporučení a rady v záležitostech bezpečnosti
- Poskytovat vrcholovému vedení nezávislá doporučení v záležitostech bezpečnosti
- Být nápomocen nižším složkám vedení ve věcech bezpečnosti
- Dohlížet na systém pro zjišťování a analýzu nebezpečí
- Být zapojen do vyšetřování událostí/nehod
- Sledovat vyhovění všem normám

Malým leteckým společnostem v České Republice bylo úřadem pro civilní letectví doporučeno, aby funkci vedoucího bezpečnosti vykonával pilot. Tento pilot však musí být vyškolen v oblasti řízení bezpečnosti. To v praxi znamená, že musí absolvovat úplný výcvikový kurz SMS, který je organizovaný a zajišťovaný některou z oprávněných organizací (ICAO, EASA, JAA Training apod.). Toto řešení je zavedeno například u DSA, ABS Jets, Travel Service nebo Silesia Air.

Obecně existují dva způsoby začlenění vedoucího bezpečnosti do organizační struktury leteckého provozovatele.

1. způsob:

Tento způsob organizačního uspořádání řeší bezpečnost letového úseku a úseku údržby odděleně. Vedoucí bezpečnosti zastává funkci koordinátora mezi oběma úseky. Toto řešení není příliš vhodné a v praxi se téměř nepoužívá.

2. způsob:

U této varianty organizačního uspořádání je vedoucí bezpečnosti na stejné úrovni s vedoucím jakosti. To znamená, že spolu spolupracují a vedoucí bezpečnosti je řídícím článkem v otázkách bezpečnosti. Tento způsob je proto vhodnější – viz schéma na další straně.

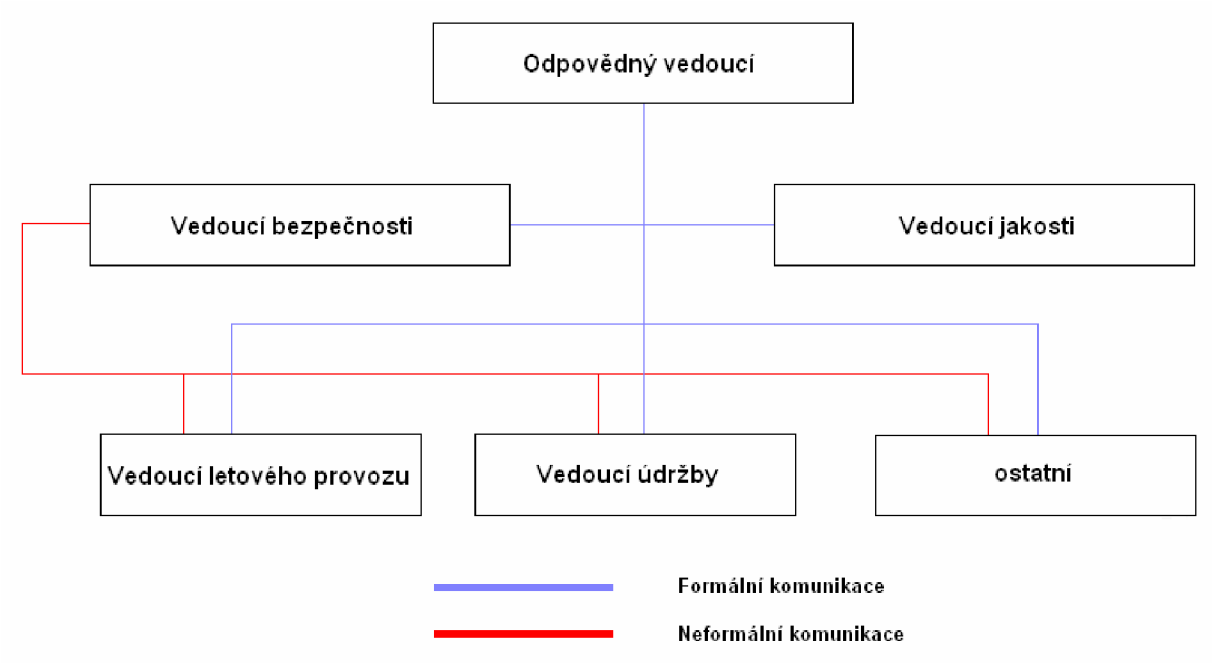

Schéma 6.1 Organizační struktura organizace (přepracováno podle [1])

7. Řízení bezpečnostního rizika

7.1 Základní pojmy k řízení bezpečnostního rizika

Nebezpečí
je jakýkoli stav nebo událost, která může způsobit nežádoucí následky (rizika).

Následek nebezpečí
je definován jako možný výsledek nebo dopad zjištěného nebezpečí. Nebezpečí může zapříčinit jeden nebo více následků. Rovněž se používá i termín **riziko**.

Bezpečnostní riziko
je předpověď pravděpodobnosti a vážnosti následků nebezpečí s odkazem na nejhorší předvídatelnou situaci. Jedná se tedy o bezpečnostní riziko následků nebezpečí.

Příklad pro lepší přehled a orientaci v procesu řízení bezpečnostního rizika:

- Vítr o síle 15 kts, který fouká pod úhlem 90-ti stupňů na přistávací a vzletovou dráhu, je **nebezpečí**.
- Možnost vyjetí z dráhy, protože pilot nemusí být schopen ovládnout letadlo během startu a přistání, je jeden z **následků nebezpečí** (riziko).
- Vyhodnocení případného vyjetí z dráhy jako následku nebezpečí, vyjádřeného z hlediska pravděpodobnosti a závažnosti alfanumerickým kódem, je **bezpečnostní riziko**.

Typický proces řízení bezpečnostního rizika:

Zjistit nebezpečí vzhledem k zařízení, majetku, personálu nebo organizaci.	**ZJIŠŤOVÁNÍ NEBEZPEČÍ (HAZARD IDENTIFICATION)**
Vyhodnotit možnou pravděpodobnost následků nebezpečí.	**ZHODNOCENÍ / ANALÝZA RIZIKA (RISK ASSESSMENT / ANALYSIS) Pravděpodobnost**
Vyhodnotit závažnost následků nebezpečí.	**ZHODNOCENÍ / ANALÝZA RIZIKA/ (RISK ASSESSMENT / ANALYSIS) Vážnost**
Je následné riziko přijatelné v rámci kvalitativních bezpečnostních kritérií organizace ?	**ZHODNOCENÍ RIZIKA (RISK ASSESSMENT) Přijatelnost**

ANO **Riziko je přijatelné**	**NE** **Provést činnost pro snížení rizika na přijatelnou úroveň**	**ZMÍRNĚNÍ RIZIKA (RISK MITIGATION)**

Tabulka 7.1 Proces řízení bezpečnostního rizika (přepracováno podle [1])

7.2 Identifikace nebezpečí

Identifikace nebezpečí je proces, při kterém dochází k rozpoznání nebezpečných stavů nebo podmínek, které představují ohrožení pro leteckého provozovatele. Možnost výskytu nebezpečí je široká a může se objevit na všech úrovních organizace.

7.2.1 Druhy nebezpečí

Obecně lze nebezpečí rozdělit podle vlivů do následujících tří skupin:

Nebezpečí z přírodních vlivů

To může být způsobeno povětrnostními nebo klimatickými událostmi jako jsou hurikány, sněhové bouře, období sucha, tornáda, bouřky, blesky nebo střih větru. Nepříznivými povětrnostními podmínkami jako námraza, mrznoucí srážky, silný déšť, sníh, boční vítr a omezená viditelnost. Dále se mohou vyskytnout geofyzikální procesy jako zemětřesení, vulkány, tsunami, záplavy nebo sesuvy půdy. Značný vliv na bezpečnost mají také geografické podmínky, jako například terénní překážky.

Nebezpečí z technických vlivů

Představuje ztráta některého zdroje energie jako například ztráta elektrické energie, nedostatek paliva, nízký hydraulický nebo pneumatický tlak, atd. Nebezpečí může být způsobeno selháním nějaké kriticky důležité funkce, např. selhání hardwaru, nebo výskytem závady na softwaru apod. Možná nebezpečí z technických vlivů se týkají:

- Letadel a letadlových komponentů, systémů, podsystémů a příslušného vybavení
- Zařízení organizace, nástrojů a příslušného vybavení
- Zařízení, systémů a podsystémů a příslušného vybavení, které využívá organizace z vnějších zdrojů

Nebezpečí z ekonomických vlivů

jsou následkem socio-politického prostředí, ve kterém se provoz ve vztahu poskytování služeb provádí. Příklady nebezpečí mohou být:

- Hospodářský růst organizace a s tím spojený nábor nových, nezkušených pracovníků
- Hospodářský pokles a s tím spojené propouštění zaměstnanců
- Finanční náklady na výcvik, přeškolování a rozvoj zaměstnanců
- Finanční náklady na materiál, zařízení a vybavení, apod.

7.2.2 Vyhledávání nebezpečí

Pro identifikaci nebezpečí se používají interní nebo externí zdroje informací. Interní zdroje tvoří dobrovolný systém hlášení událostí, průzkumy nebo audity odhalující případné nedostatky v zajištění bezpečnosti. Externí zdroje tvoří závěrečné zprávy z vyšetřování nehod. K identifikaci nebezpečí se používají stejné strategie jako při řízení bezpečnosti.

Re-aktivní metoda

je metoda okamžité reakce zjišťování nebezpečí. Reaguje na události, které se již staly. Zabývá se příčinami nehod a vážných incidentů, to znamená, že reaguje na aktuální i předešlé bezpečnostní události.

Pro-aktivní metoda

je aktivní přístup ke zjišťování nebezpečí. Tato metoda je založena na tom, že selhání systému může být omezeno na minimum identifikací bezpečnostních rizik a přijetím opatření

pro jejich zmírnění dříve, než systém zcela selže. Jinými slovy: Cílem aktivního přístupu ke zjišťování nebezpečí je identifikovat nebezpečí dříve, než vyvolá nežádoucí událost.

Praktickými příklady pro-aktivní metody zjišťování nebezpečí jsou například systém povinného hlášení událostí, systém dobrovolného a důvěrného hlášení událostí, bezpečnostní audity, bezpečnostní průzkumy apod. Tato metoda zahrnuje také identifikaci nebezpečí, která mohou vzniknout v souvislosti se zaváděním nových systémů a vybavení, nových provozních postupů, nebo jejich změn. Především změny dlouhodobě zažitých postupů mohou vyvolat nebezpečí vzniklá chybou lidského činitele, který nemá dostatečně osvojené nové postupy a jedná podvědomě (podle starých postupů). Také odhaluje nebezpečí vzniklá důsledkem změn v organizaci, jako jsou například změny v organizační struktuře. To se týká zejména rozšiřování provozu a s tím spojený nábor nových pracovníků, nebo redukce provozu a s tím spojené propouštění pracovníků, možná privatizace organizace atd.

Prediktivní metoda

je v podstatě statistickým systémem sběru bezpečnostních údajů. Jedná se o metodu identifikace potencionálního problému selhání v reálném čase při normálním běžném provozu. Zahrnuje např. program vyhodnocování letových údajů a sledování běžného a každodenního provozu.

Vyhledávání nebezpečí musí být neustálé a efektivní a musí se o něj snažit každý zaměstnanec společnosti. Obzvláště se mu musí věnovat pozornost v případě, že dochází k nárůstu počtu nebezpečných událostí, nebo když v organizaci dochází k velkým, nebo provozním změnám. Proto musí být v organizaci vytvořen úsek vedoucího bezpečnosti, který se bude specializovat na vyhledávání nebezpečí a bude spolupracovat s řízením jakosti. Postup vyhledávání nebezpečí je zhruba následující:

1) Stanovení oblasti ve, které se může vyskytovat případné nebezpečí - např. část letiště v rekonstrukci.
2) Další upřesnění oblasti - uzavřené pojezdové dráhy a překážky v rekonstruované části letiště.
3) Různé oblasti případného nebezpečí vedou ke specifickým rizikům – letedlo omylem vjede do uzavřené části letiště a narazí křídlem do překážky

Důležitým prvkem při identifikaci nebezpečí je dokumentace. Veškeré informace týkající se bezpečnosti by měly být uloženy, nelépe na jednom místě, aby bylo možné v případě potřeby snadno dohledat potřebné informace. Jako například oblasti, kde došlo v minulosti k problémům, jak se dané problémy řešily, co bylo výsledkem řešení, kdo byl za problém odpovědný, kdo vedl vyšetřování a podobně. Tyto informace slouží k vypracování různých bezpečnostních studií, analýz, ale i jako podklady pro bezpečnostní školení.

7.2.3 Bezpečnostní systémy hlášení událostí

Systém povinného hlášení událostí

Je systém hlášení, který se týká hlášení určitých předepsaných typů událostí, jako jsou nehody a incidenty.

Systém dobrovolného hlášení událostí

Kterýkoli zaměstnanec organizace je vedením vyzýván a podporován k tomu, aby podával **dobrovolně** informace o událostech a nebezpečích. Takto získané informace nesmí být použity proti zaměstnanci, který je nahlásil. Jinými slovy: Ohlašovatel nesmí být trestán ani jinak postihován. Navíc musí být zajištěna ochrana zdroje těchto informací, aby zaměstnanci nebyli odrazováni od dobrovolného hlášení. Neměl by vzniknout ani nejmenší náznak jakýchkoli postihů, pokud se jedná o hlášení událostí zapříčiněných neúmyslným porušením, neúmyslnými chybami, pochybnostmi, závadami, zkušeností a podobně.

Systém anonymního hlášení událostí

Systém důvěrného hlášení v rámci dobrovolného hlášení událostí umožní zajistit mnohem větší rozsah získaných bezpečnostních informací. Cílem systému hlášení událostí je identifikovat nežádoucí tendence, nebo odhalit nedostatky uvnitř organizace. Toho je dosaženo pomocí stanoveného systému hlášení, který pomůže zlepšit úroveň bezpečnosti a rovněž zajistí nepostižitelnost autora, který hlášení podal. Proto je možné hlášení podat i anonymně.

V souvislosti s touto prací jsem oslovil některé menší letecké společnosti. Dotazoval jsem se na jejich SMS a především na systém anonymního hlášení událostí. Z leteckých společností v České Republice jsem oslovil ABS Jets, Central Connect Airlines, Silesia Air, Travel Servis, Grossmann Jet Service a ČSA pro porovnání s větší společností. Ze zahraničních společností jsem oslovil Triple Alpha, Solid Air, DC Aviation, Global Jet Concept, Next Jet, Mena Aerospace a Prestige Jet. Z oslovených českých společností reagovaly pouze Silesia Air a Central Connect Airlines (CCA), ze zahraničních společností mi neodpověděla bohužel žádná. Proto zde mohu uvést příklady z praktického fungování systému anonymního hlášení událostí bohužel pouze u těchto dvou společností.

7.2.4.1 Systém anonymního hlášení událostí u společnosti CCA:

U společnosti Central Connect Airlines používají pro anonymní hlášení událostí speciální formulář. Po vyplnění hlášení se formulář vloží do speciální schránky označené štítkem „Safety Reports“. Tato schránka je umístěna v místnosti pro posádku a přístup do ní má pouze vedoucí bezpečnosti. Vedoucí bezpečnosti použije nashromážděné informace k tomu, aby o nich informoval ostatní zaměstnance/členy posádky, nebo je využije za účelem rozboru trendů a systémových nedostatků systému hlášení. Systém také využívá vyhodnocování zapisovače letových údajů (AFDRS) k odhalení chybných, nebo nepříznivých tendencí a chyb v letové technice pilota.

Takovéto informace jsou velmi užitečné při navrhování preventivních opatření. Systém hlášení událostí je součástí celkového monitorovacího systému a podporuje postupy již zavedené v praxi. Nicméně, tento systém může být využit také k identifikaci případů, kdy rutinní postupy selhaly a tím tedy přispívá ke zlepšení např. výcvikových postupů, posloupnosti a efektivitě organizačních procedur. Důležitost hlášení se nemusí projevit ihned, ale až při pozdější příležitosti, protože jedna událost může být považována za izolovaný incident, ale dvě podobné události mohou znamenat začátek nežádoucí tendence. Z tohoto důvodu je nutné hlášení shromaždovat a uschovávat.

7.2.4.2 Organizace Systému bezpečnostních hlášení událostí u společnosti CCA:

- Piloti mohou vhodit hlášení do speciální uzamčené schránky, která je označena štítkem Safety Reports. Tato schránka by se měla nacházet v blízkosti místnosti pro piloty.
- Je-li to možné, hlášení by se měla vyplňovat na předepsaný formulář, dostupný přímo v letadle a v elektronické podobě na počítači v místnosti pilotů. Hlášení v jakékoli jiné podobě jsou také vítána. Přístup do schránky má pouze vedoucí bezpečnosti.
- Vedoucí bezpečnosti sesbírá a roztřídí hlášení a užitečné informace rozešle prostřednictvím Programu bezpečnosti letu. Informace, které svědčí o systémových nedostatcích, budou předány bez uvedení čísla letu vedoucímu jakosti k dalšímu zpracování.
- Vedoucí bezpečnosti a vedoucí jakosti archivují důležité informace na bezpečném místě po dobu 5 let.

Pravidla, kterými se musí řídit všichni účastníci:

- Nashromážděné informace jsou důvěrné. Při jejich rozesílání musí být vyloučena možnost identifikace zaměstnance/člena posádky nebo letu.
- Zaměstnanec/člen posádky může, i když není povinen, uvést své jméno nebo číslo letu.
- V případě, že jméno nebo let uvede, tyto informace mohou být použity pouze za účelem získání konkrétních poznatků o případu.
- Informace poskytnuté zaměstnanci/členy posádek v systému hlášení událostí nesmí být v žádném případě použity proti nim.
- Informace jsou dále zpracovávány a předávány anonymně, ledaže by zaměstnanec/člen posádky dal řádný souhlas ke zveřejnění své totožnosti ve zprávě.

7.2.4.3 Uspořádání zprávy Systému bezpečnostních hlášení událostí u společnosti CCA

Vzájemné poznatky mohou být užitečné pouze za předpokladu, že je poskytnuto určité minimum informací, které umožní specifikovat okolnosti incidentu a sled událostí. Proto se doporučuje vyplňovat hlášení v předepsaném formátu. Jestliže zpráva obsahuje jméno zaměstnance/člena posádky a číslo letu, je možné po něm požadovat doplňující informace, nebo vyhodnotit data z letového zapisovače. Záleží jedině na zaměstnanci/posádce, zda poskytne informace o sobě nebo o letu. Jestliže chce pilot zveřejnit svoje jméno, musí s tím souhlasit kolegové z posádky. I v případě, že pilot chce zůstat v anonymitě, měla by se posádka podělit o své poznatky, jelikož tyto informace jsou velice citlivého charakteru.

Doporučení týkající se hlášení:

- Totožnost (dobrovolné) – jméno pilota, zaměstnance/člena posádky, číslo letu, typ letounu, datum a čas incidentu
- Případně: Letové podmínky – počasí (Meteo-podmínky pro přístrojové lety, Meteo-podmínky pro let za vidu, turbulence, námraza, bouřka atd.), nadmořská výška, rychlost, fáze letu (vzlet, stoupání, let v hladině, klesání, přiblížení, přistání), konfigurace letounu, výkon motoru, provozní program autopilota
- Popis incidentu

- Zhodnocení incidentu
- Získané poznatky (pozitivní/negativní)
- Datum a podpis (pouze v pokud souhlasí se zveřejněním totožnosti)

7.2.4.4 Způsoby podání anonymního hlášení

Způsobů podání anonymního hlášení existuje více než jen výše popsaný způsob hlášení pomocí speciálního formuláře, který používá Central Connect Airlines. Další možností podání hlášení je pomocí faxu. Mezi nejrozšířenější způsoby však patří podání hlášení prostřednictvím emailu. V takovém případě má letecká společnost pro tato hlášení zřízenu zvláštní emailovou adresu. Tento způsob hlášení využívá například společnost Sielsia Air. Zaměstnanci této společnosti mohou podávat svá anonymní hlášení z libovolného počítače připojeného k internetu, který je k dispozici i v kancelářích společnosti, pomocí přístupu na webovém rozhraní k účtu pošty stiznost@silesiaair.cz , s jim známým heslem, uvedeným ve vnitřně přístupné firemní dokumentaci a zasláním podmětu na známé adresy členů vedení společnosti.

Pro co nejvyšší efektivitu by systém hlášení měl obecně splňovat následující podmínky:

- Systém podávání zpráv by měl být jednoduchý a účinný
- Hlášení musí být důvěrná
- Žádná disciplinární opatření
- Rychlá zpětná vazba, která je všem přístupná a je plně informativní. To je důležité pro celkovou úroveň bezpečnostní kultury organizace

7.2.4.5 Problém anonymity hlášení

U velmi malých společností do 20 zaměstnanců je anonymní systém hlášení problematický. Představme si hypotetickou situaci:

Na jednom typu letadla létá pouze jedna posádka. Pomocí anonymního systému hlášení přijde zpráva, že velitel letadla ne zcela precizně dodržuje některý z předepsaných postupů. Už v okamžiku, kdy takové hlášení přijde, přestává být anonymní. Z důvodu, že hlášení je považováno za důvěrné, vedoucí bezpečnosti nemůže dotyčného "chybujícího" oslovit s žádostí o nápravu, protože by tím odhalil zdroj svých informací. Může ale například doporučit přeškolení, které může zajistit nápravu, a nebo také nemusí. Pak se ovšem nachází ve výchozím bodě. Organizace zaplatila za školení a nyní stojí před dilematem, zda přijít o pilota, nebo v rozporu se zavedeným "anonymním" systémem sáhnout k disciplinárnímu opatření. Žádná z možností tedy není úplně ideální a osvědčuje se zde spíše přímé a otevřené jednání vedoucího bezpečnosti. Toto je důvod, proč v malých společnostech anonymní systémy prakticky nepřinášejí žádné výsledky a skoro se nevyužívají. U společnosti CCA je tento systém využit maximálně 2x do roka, u společností Silesia Air, DSA nebo ABS Jets se tento systém v praxi nevyužívá vůbec.

7.2.5 Analýza nebezpečí

Pro identifikaci nebezpečí je důležité, aby bezpečnostní informace byly ze získaných bezpečnostních údajů důkladně vytaženy. Tyto důležité informace získáme pomocí analýzy nebezpečí, která se skládá ze tří kroků.

Praktický příklad analýzy nebezpečí:

1) Identifikace obecného nebezpečí
   - Stavební práce na letišti
   - Vítr o síle 15 kts
2) Identifikace specifických nebezpečí nebo komponentů obecného nebezpečí
   - Stavební stroje a vybavení, uzavřené pojezdové dráhy, nejasná letištní značení, atd.
   - Boční vítr 15 kts ze směru 90 na RWY, atd.
3) Propojení specifických nebezpečí s potenciálními následky nebezpečí
   - Kolize letadla se stavebními stroji (komponent: stavební stroje), použití špatné pojezdové dráhy (komponent: zavřená pojezdová dráha), atd.
   - Ztráta kontroly pilota nad letadlem při vzletu nebo přistání, vyjetí letadla z RWY, poškození podvozku letadla, atd.

Následky nebezpečí musí být popisovány z provozního hlediska. Mnoho nebezpečí má potenciál nejhoršího možného následku, to je ztráty lidských životů. Většina nebezpečí má potenciál ztráty majetku, ekologické škody a podobně. Popis následků nebezpečí z takového extrémního hlediska způsobí komplikace pro stanovení strategie pro zmírnění bezpečnostního rizika. Proto musí být následky nebezpečí popisovány především z provozních než z extrémních hledisek. Silný boční vítr představuje nebezpečí, jehož následkem z provozního hlediska je vyjetí letadla z dráhy, nikoli následek z extrémního hlediska, kterým je ztráta lidských životů.

7.3 Proces vyhodnocení a zmírnění rizika

Bezpečnostní riziko následků nebezpečí je vyjádřené jako předpověď pravděpodobnosti a vážnosti následků nebezpečí. Často bývá vyjádřeno alfanumerickým kódem, který nám umožňuje jeho měření a porovnávání.

7.3.1 Pravděpodobnost bezpečnostního rizika

Pravděpodobnost bezpečnostního rizika následků nebezpečí je definována jako pravděpodobnost, že by mohlo dojít k nebezpečné události, nebo by se mohl vyskytnout nebezpečný stav. Jinými slovy, pravděpodobnost bezpečnostního rizika následků nebezpečí je možná pravděpodobnost výskytu nebezpečné situace.

Vyhodnocení bezpečnostního rizika z hlediska pravděpodobnosti je možné pomocí následujících otázek:

- Jedná se o ojedinělou událost, nebo byla v minulosti již taková událost řešena?

- Mohou mít podobné závady i jiná zařízení nebo používané vybavení?
- Jak velký počet personálu se řídí postupy, o nichž jsou pochybnosti?
- A další podobné otázky

Pro takovéto vyhodnocování možné pravděpodobnosti výskytu nebezpečné události je důležitý přístup k starším bezpečnostním údajům. Tyto údaje by měly být zdokumentované a uschované v registru bezpečnostních záznamů tak zvané „Safety library“. K lepšímu vyhodnocení pravděpodobnosti by měly být využity kromě interních informací i externí zdroje bezpečnostních informací.

	Význam	Hodnota
Častý	Pravděpodobně se může stát velmi často (stalo se často)	**5**
Občasný	Pravděpodobně se může někdy stát (stalo se nepříliš často)	**4**
Vzdálený	Nepravděpodobně, ale s možností, že se může stát (stalo se zřídka)	**3**
Nepravděpodobný	Velmi nepravděpodobné, že by se mohla stát (není známo, že by se stala)	**2**
Extrémně nepravděpodobný	Téměř nemyslitelné, že událost by se mohla stát	**1**

Tabulka 7.2 Pravděpodobnost bezpečnostního rizika (přepracováno podle [1])

7.3.2 Vážnost bezpečnostního rizika

Po vyhodnocení bezpečnostního rizika nebezpečné události z hlediska možné pravděpodobnosti je nutné provést také vyhodnocení jeho vážnosti následků nebezpečí.

Vážnost bezpečnostního rizika následků nebezpečí je definována jako vážnost možných následků nebezpečné události nebo stavu s odhledem na nejhorší předvídatelnou situaci, která by mohla nastat.

Vyhodnocení bezpečnostního rizika z hlediska vážnosti je možné pomocí následujících otázek:

- Kolik životů je v ohrožení? (např. zaměstnanců, cestujících, přihlížejících a veřejnosti všeobecně)
- Jaký je pravděpodobný rozsah poškození majetku nebo finanční újmy? (např. přímá ztráta majetku provozovatele, poškození letecké infrastruktury)
- Jaká je pravděpodobnost nežádoucích vlivů na životní prostředí? (např. únik paliva nebo jiných nebezpečných látek, narušení nebo zničení přirozeného životního prostředí)
- Jaký je rozsah poškození dobrého jména letecké společnosti, mediální ohlas?
- A další podobné otázky

Vymezení	Význam	Hodnota
Katastrofický	• Celková destrukce zařízení/vybavení • Hromadné úmrtí	**A**
Nebezpečný	• Rozsáhlé snížení míry bezpečnosti, takové fyzické a reálné ohrožení nebo pracovní zatížení, že provozovatelé se nemohou spolehnout, že budou schopni plnit své úkoly přesně nebo beze zbytku • Vážné zranění nebo usmrcení určitého počtu osob • Závažné poškození vybavení	**B**
Závažný	• Podstatné snížení míry bezpečnosti, omezení schopnosti provozovatelů vyrovnat se s nepříznivými provozními podmínkami zapříčiněnými zvýšeným pracovním zatížením nebo podmínkami, oslabujícími jejich výkonnost • Vážný incident • Zranění osob	**C**
Méně závažný	• Svízel, mrzutost • Provozní omezení • Použití náhradních postupů • Méně závažné incidenty	**D**
Zanedbatelný	• Malé následky	**E**

Tabulka 7.3 Vážnost bezpečnostního rizika (přepracováno podle [1])

7.3.3 Snesitelnost bezpečnostního rizika

Vyhodnocení snesitelnosti bezpečnostního rizika se provádí sloučením hodnot z tabulek pravděpodobnosti a vážnosti následků nebezpečí. Tímto sloučením dostaneme matici pro zhodnocení bezpečnostního rizika.

Pravděpodobnost bezpečnostního rizika	**Vážnost bezpečnostního rizika**				
	Katastrofický A	**Nebezpečný B**	**Závažný C**	**Méně závažný D**	**Zanedbatelný E**
Častý 5	**5A**	**5B**	**5C**	**5D**	**5E**
Občasný 4	**4A**	**4B**	**4C**	**4D**	**4E**
Vzdálený 3	**3A**	**3B**	**3C**	**3D**	**3E**
Nepravděpodobný 2	**2A**	**2B**	**2C**	**2D**	**2E**
Extrémně nepravděpodobný 1	**1A**	**1B**	**1C**	**1D**	**1E**

Tabulka 7.4 Snesitelnost bezpečnostního rizika (přepracováno podle [1])

Výsledná alfanumerická hodnota se nazývá index bezpečnostního rizika.Tento index se následně převede do matice snesitelnosti bezpečnostního rizika, která nám udává kritéria snesitelnosti bezpečnostního rizika.

Matice snesitelnosti:

Řízení bezpečnostního rizika	Index bezpečnostního rizika	Doporučená kritéria
Nepřijatelná oblast	5A, 5B, 5C, 4A, 4B, 3A	Bezpečnostní riziko je nepřijatelné za daných okolností
A L A R P Snesitelná oblast	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Přijatelné na základě zmírnění bezpečnostního rizika. Manažerské rozhodnutí by mohlo být požadováno. Je požadována analýza nákladů a výnosů
Přijatelná oblast	3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E	Přijatelné

Tabulka 7.5 Matice snesitelnosti (přepracováno podle [1])

Příklad: Pravděpodobnost bezpečnostního rizika byla vyhodnocena jako „občasný (4)“ a vážnost bezpečnostního rizika jako „nebezpečný (B)“. Složenina pravděpodobnosti a vážnosti (4B) je index bezpečnostního rizika, který nám udává bezpečnostní riziko následků daného nebezpečí. Zhodnocené bezpečnostní riziko jako 4B je podle matice snesitelnosti bezpečnostního rizika „nepřijatelné za daných okolností“. To znamená, že bezpečnostní riziko následků nebezpečí je nepřijatelné.

7.4 Zmírnění bezpečnostního rizika

Dalším důležitým krokem v procesu vyhodnocení a zmírnění bezpečnostního rizika následků nebezpečí je stanovení strategie pro zmírnění bezpečnostního rizika. To znamená stanovit opatření pro zmírnění bezpečnostního rizika a dostat pod kontrolu organizace pravděpodobnost a vážnost bezpečnostního rizika následků nebezpečí.

Podle předchozího příkladu bylo bezpečnostní riziko následků nebezpečí vyhodnoceno jako „nepřijatelné za daných okolností“. Proto musí být stanovena taková opatření aby se bezpečnostní riziko dostalo do snesitelné oblasti. To znamená do takové oblasti, kde bezpečnostní riziko je na úrovni tak nízké, jak je přiměřeně možné (As Low As Reasonably

Practicable – ALARP). Jestliže není možné dosáhnout snesitelné oblasti, potom by měly být provoz nebo daná nebezpečná činnost zastaveny.

7.4.1 Obecné strategie pro zmírnění bezpečnostního rizika

Zrušení

Provoz nebo činnost je zrušena. Pakliže by se provoz nebo činnost uskutečnily, bezpečnostní rizika by převyšovala jejich prospěch. Například uskutečnění letu na letiště se složitou geografickou polohou v horách bez potřebných prostředků, nebo provoz v RVSM prostoru s letadlem, které nemá pro tento provoz požadované vybavení.

Omezení

Provoz je omezen, nebo se provede opatření pro snížení míry následků přijatelných rizik. Například uskutečnění letu na letiště se složitou geografickou polohou v horách bez potřebných prostředků bude omezen pouze na denní dobu za vizuálních podmínek, nebo uskutečnění letu letadlem, které nemá pro provoz RVSM požadované vybavení, bude provedeno nad nebo pod RVSM prostorem.

Vyloučení vystavení se vlivu ohrožení

Znamená udělat opatření za účelem izolace účinků následků nebezpečí, nebo začlenit zálohu pro ochranu před nimi. Jinými slovy snížit vážnost bezpečnostního rizika následků nebezpečí. Například strategie založená na vyloučení vystavení se vlivu ohrožení zahrnuje : Provedení letu na letiště se složitou geografickou polohou v horách bez nezbytných prostředků je omezeno na letadlo s přesně stanovenou navigační výkonností. Letadlu, které nemá pro provoz RVSM požadované vybavení, nebude povolen RVSM provoz v prostoru RVSM.

Strategie pro zmírnění bezpečnostního rizika následků nebezpečí jsou založeny především na posílení již existujících obranných nástrojů, nebo zavedení nových nebo dodatečných obranných nástrojů. Často se využívá strategie založená na kombinaci obojího.

Obranné nástroje můžeme rozdělit do následujících kategorií:

- **Technika** - nové nebo modernizované zařízení a vybavení atd.
- **Výcvik** - nové nebo zdokonalené postupy pro výcvik veškerého provozního personálu. Především pak pro výcvik klíčového personálu, jakým jsou letové posádky, personál údržby, atd.
- **Postupy a předpisy** - zavedení dodatečných nebo změněných postupů nebo předpisových požadavků. Nové, doplněné, nebo změněné postupy pro dozor nad činnostmi organizace, atd.
- Jakékoli další možnosti pro zmírnění bezpečnostního rizika nebo jejich vzájemná kombinace

Pro zmírnění bezpečnostního rizika je důležité určit, proč je použití nových nebo dodatečných obranných nástrojů nutné, nebo proč musí být již existující obranné nástroje posíleny. K tomuto účelu můžeme použít následující otázky:

- Existují obranné nástroje k ochraně před bezpečnostními riziky následků nebezpečí ?
- Fungují obranné nástroje tak, jak bylo zamýšleno?
- Jsou obranné nástroje prakticky využitelné s přihlédnutím k aktuálním provozním podmínkám?
- Je si personál vědom rizik a do provozu zavedených obranných nástrojů?
- Jsou skutečně nezbytná dodatečná opatření pro zmírnění bezpečnostního rizika?
- A další podobné otázky

7.4.2 Celkový proces zmírnění bezpečnostního rizika

1) Je zjištěno možné bezpečnostní riziko. Následky tohoto rizika jsou analyzovány a bezpečnostní riziko je vyhodnoceno, poté následuje:

2) Vyhodnocení účinnosti a efektivity již existujících obranných nástrojů, vztahujících se k daným následkům nebezpečí. Výsledkem tohoto zhodnocení je posílení existujících, nebo zavedení nových obranných nástrojů. Případně kombinace obojího.

3) Na základě posílení již existujících obranných nástrojů nebo zavedení nových obranných nástrojů je počáteční bezpečnostní riziko znovu přehodnoceno. Tímto přehodnocením se stanoví, jestli je nyní bezpečnostní riziko tak nízké, jak je přiměřeně možné (ALARP). Tedy třetím krokem v rámci procesu zmírnění bezpečnostního rizika je opatření pro zmírnění bezpečnostního rizika.

4) Po přehodnocení bezpečnostního rizika by měla být potvrzena účinnost a efektivita strategie pro zmírnění bezpečnostního rizika. Proto čtvrtým krokem v rámci provedeného zmírnění bezpečnostního rizika na přijatelnou úroveň je potvrzení zmírnění bezpečnostního rizika. Tohoto potvrzení se docílí pomocí následujících otázek:

    - Je zmírnění bezpečnostního rizika skutečně účinné?
    - Je provedené zmírnění bezpečnostního rizika přiměřené a vhodné ?
    - Nevytváří zvolená strategie zmírnění další dodatečná rizika?

Jestliže je provedené zmírnění bezpečnostního rizika přijatelné, zavedená výsledná strategie by měla být zpětnou vazbou k obranným prostředkům, na jejichž základě je strategie zmírnění bezpečnostního rizika založena. Tím bude zabezpečena integrita a dostatečná účinnost obranných prostředků v nových provozních podmínkách.

Schéma procesu zmírnění bezpečnostního rizika:

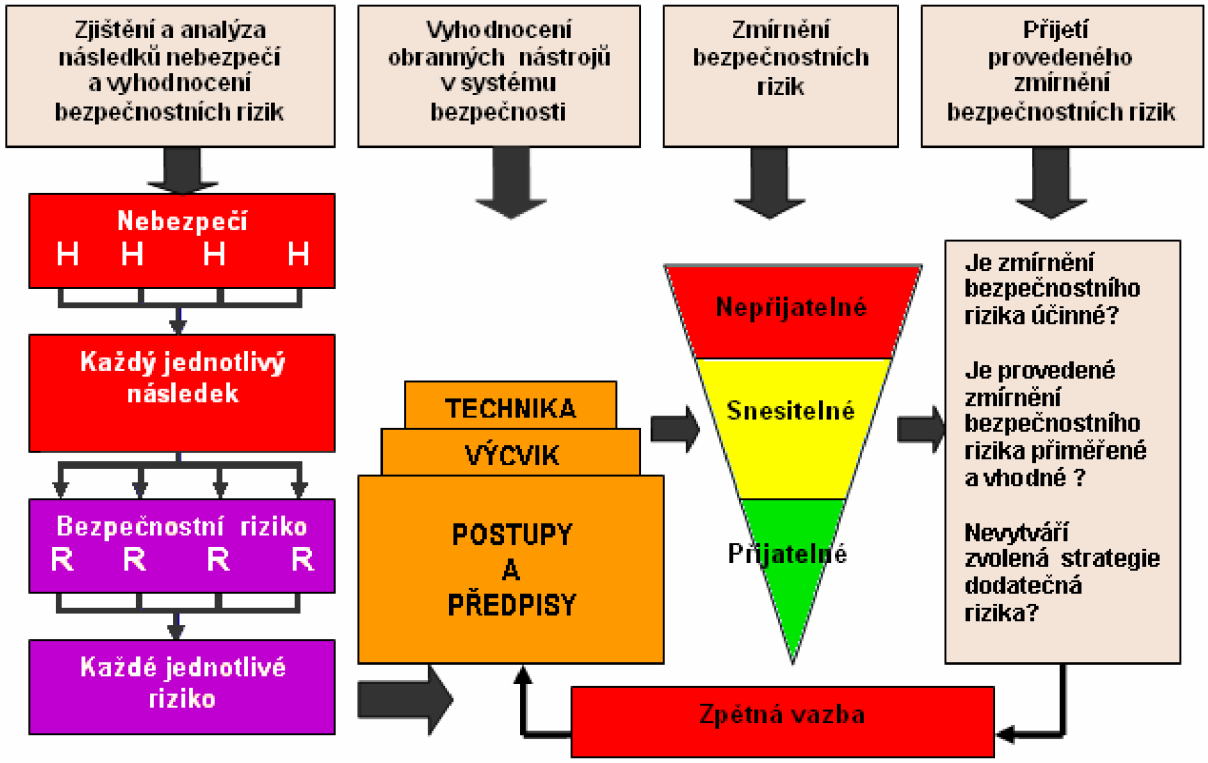

Schéma 7.6 Proces zmírnění bezpečnostního rizika (přepracováno podle [1])

7.4.3 Přidělování finančních prostředků

Řízení bezpečnostního rizika je klíčovým komponentem celého systému řízení bezpečnosti, a proto hraje zásadní roli při rozhodování, které musí vrcholové vedení organizace provádět z hlediska přidělování finančních prostředků. Efektivní a zároveň bezpečný provoz vyžaduje rovnovážný stav mezi cílem co nejvíce vyprodukovat, to znamená poskytnout co nejvíce služeb za účelem zisku a cílem co nejvyšší bezpečnosti.

Letový provoz s sebou přináší jisté bezpečnostní riziko. Úplné odstranění tohoto rizika nemůže být efektivní z hlediska vynaložených finančních nákladů. Proto je nutné, aby bezpečnostní riziko spojené se zjištěným nebezpečím bylo zmírněno na úroveň tak nízkou, jak je přiměřeně možné (ALARP).

Pro stanovení co je „přiměřeně možné“ je nutné vzít v úvahu jak technickou proveditelnost dalšího snižování bezpečnostního rizika, tak vynaložené finanční náklady. Z toho vyplývá, že musí být provedena analýza nákladů a výnosů. Prokázání, že bezpečnostní riziko je ALARP, znamená, že jakékoli další snižování bezpečnostního rizika je buď nerealizovatelné, nebo výrazně převáženo finančními náklady. I když organizace přijme bezpečnostní riziko, neznamená to, že je tím veškeré bezpečnostní riziko odstraněno. Vždy zůstane nějaké zbytkové bezpečnostní riziko. Organizace však akceptovala, že toto zbytkové bezpečnostní riziko je pro ni přijatelné a je tak nízké, že může být převáženo finančním prospěchem.

Musí být také pečlivě zváženy finanční prostředky vynaložené na zmírnění bezpečnostních rizik vůči nežádoucím následkům, pokud by zmírnění bezpečnostních rizik nebylo dostatečné. Výše těchto finančních nákladů v případě nehody nebo vážného incidentu představuje přímé finanční náklady, které mohou být sníženy pojištěním. Ovšem daleko vyšší mohou být ve svém důsledku nepřímé finanční náklady, které nejsou pokryty pojištěním. Mohou to být například omezení, nebo úplná ztráta obchodní činnosti, poškození dobrého jména společnosti a s tím spojené snížení zisku, případné soudní žaloby, pokuty a podobně.

7.5 Celkový proces řízení bezpečnostního rizika

Jestliže je bezpečnosti věnována patřičná pozornost, odhalí se tak nebezpečí a analyzují se následky nebezpečí. Rovněž se vyhodnotí bezpečnostní rizika následků nebezpečí z hlediska pravděpodobnosti a vážnosti pro stanovení míry bezpečnostního rizika. Tato bezpečnostní rizika mohou být následně vyhodnocena jako přijatelná nebo nepřijatelná.

Pokud je bezpečnostní riziko vyhodnoceno jako přijatelné, přijme se příslušné opatření a provoz nebo činnost organizace pokračuje. Pro účely zpětné vazby pomocí registru bezpečnostních údajů je vše řádně zdokumentováno.

Je-li ovšem bezpečnostní riziko vyhodnoceno jako nepřijatelné, potom je nutné použít následující otázky:

1) Může být bezpečnostní riziko odstraněno? Pokud odpověď zní „ANO“, přijmou se příslušná opatření a zajistí se zpětná vazba pomocí registru bezpečnostních záznamů. Pokud odpověď zní „NE“, je nutné si položit další otázku.

2) Může být bezpečnostní riziko zmírněno? Jestliže odpověď zní „NE“, provoz nebo činnost musí být zastaveny. Je-li odpověď „ANO“, přijmou se příslušná opatření pro zmírnění bezpečnostních rizik a musíme si položit následující otázku.

3) Je zbytkové bezpečnostní riziko přijatelné? Pokud „ANO“, provedou se případná opatření a zajistí se zpětná vazba pomocí registru bezpečnostních záznamů. Pokud je odpověď „NE“, provoz nebo daná činnost musí být zastaveny.

Je tedy zřejmé, že ani ta nejlepší strategie pro zmírnění bezpečnostního rizika nikdy nemůže zcela odstranit bezpečnostní rizika, protože vždy tu bude určité zbytkové bezpečnostní riziko. Bezpečnostní rizika musí být řízena tak, aby byla na úrovni tak nízké, jak je přiměřeně možné (ALARP). Toho se dá dosáhnout pomocí zmírnění vážnosti možných následků, zmírnění pravděpodobnosti nastání události, nebo zmírněním vystavení se bezpečnostnímu riziku. Nápravná opatření musí brát v úvahu již existující obranné prostředky a jejich neschopnost dosáhnout přijatelnou míru bezpečnostního rizika. Výsledek těchto nápravných opatření by měl být dále vyhodnocen, aby se vyloučilo, že nebylo do provozní činnosti zaneseno případné další bezpečnostní riziko.

Schéma procesu řízení bezpečnostního rizika:

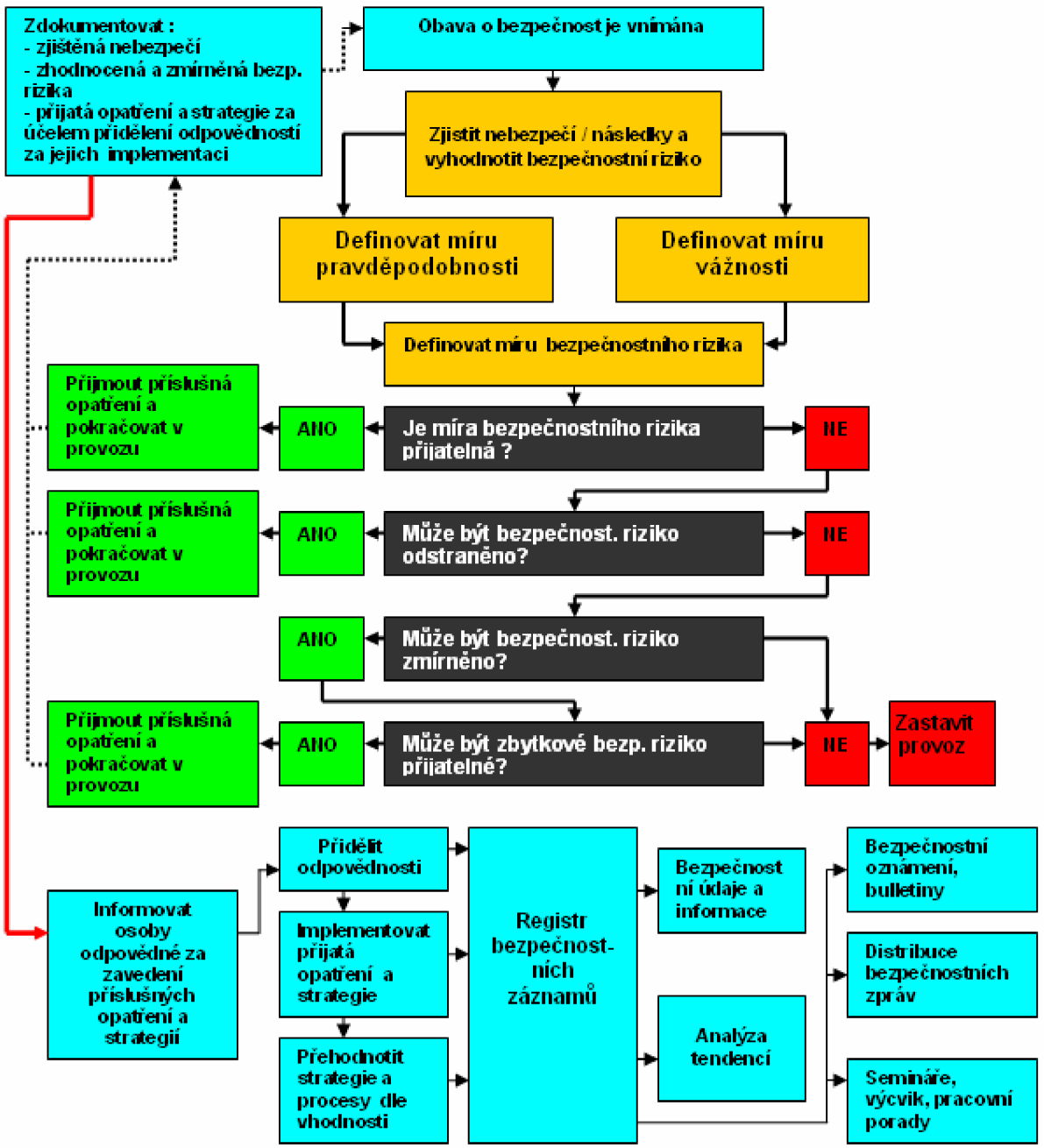

Schéma 7.7 Proces řízení bezpečnostního rizika (přepracováno podle [1])

8. Zajištění bezpečnosti

Pomocí procesu řízení bezpečnostního rizika se provede identifikace nebezpečí a vyhodnocení bezpečnostního rizika následků nebezpečí. Následný proces zmírnění bezpečnostního rizika následků nebezpečí zajistí, že bezpečnostní riziko bude na úrovni tak nízké, jak je přiměřeně možné (ALARP). Následně je nutné ověřit si a zkontrolovat, že výsledky zmírnění bezpečnostního rizika byly uvedeny do provozu tak jak bylo zamýšleno. K tomu slouží proces zajištění bezpečnosti.

Proces zajištění bezpečnosti slouží kromě kontroly výsledků zmírnění bezpečnostního rizika také ke zjišťování nových nebezpečí, která vyžadují nová vyhodnocení a následná zmírnění nových bezpečnostních rizik následků nebezpečí, ke kterým došlo kvůli změnám v provozní činnosti organizace.

Proces zajištění bezpečnosti používá metody a prostředky, kterými neustále a průběžně kontroluje a ověřuje, že provoz a činnosti organizace splňují požadavky na úroveň kvality bezpečnosti. Jinými slovy: Proces zajištění bezpečnosti se zabývá neustálým ověřováním správné funkce systému řízení bezpečnosti.

8.1 Sledování kvalitativní úrovně bezpečnosti, vyhodnocování a přezkum

Sledování kvalitativní úrovně bezpečnosti je důležité pro ověření efektivity řízení bezpečnostních rizik následků nebezpečí. Kvalitativní úroveň bezpečnosti by měla být ověřována vůči stanoveným ukazatelům kvalitativní úrovně bezpečnosti a vůči cílům kvalitativní úrovně bezpečnosti. Tyto ukazatele bývají zaváděny pomocí bezpečnostních požadavků.

Ukazatelé kvalitativní úrovně bezpečnosti

Jsou obecná vyjádření na základě údajů o četnosti výskytu incidentů a ostatních událostí, vztahujících se k bezpečnosti. Příklady ukazatelů kvalitativní úrovně bezpečnosti:

- Počet incidentů na 1000 letových hodin nebo cyklů
- Počet nálezů při provozních auditech
- Počet podaných bezpečnostních hlášení
- Míra výskytu odchylek a překročení v rámci analýzy letových údajů (FDM). Tento ukazatel se týká leteckých společností provozujících letadla s MTOW nad 27000kg.
- A další

Cíle kvalitativní úrovně bezpečnosti

Požadované cíle kvalitativní úrovně bezpečnosti jsou časově měřitelné a musí být reálné a dosažitelné. Tyto cíle by měly být takové, aby bylo možné je posoudit a monitorovat s použitím ukazatelů kvalitativní úrovně bezpečnosti. Příklady cílů kvalitativní úrovně bezpečnosti:

- Snížit počet incidentů na 1000 letových hodin o X% během příštích Y let
- Zvýšit počet bezpečnostních hlášení o X% během příštích Y let
- Snížit přímé i nepřímé finanční náklady zaviněné incidenty nebo nehodami o X% během příštích Y let
- Snížit počet provozně technických incidentů o X% během příštích Y let
- Snížit počet nálezů u externích auditů o X% během příštích Y let
- A další.

Bezpečnostní požadavky

Jsou prostředky pro dosažení ukazatelů kvalitativní úrovně bezpečnosti a cílů kvalitativní úrovně bezpečnosti. Obsahují provozní postupy, vybavení, systémy a programy, u kterých musí být definována míra spolehlivosti, výkonnosti, kvalitativní úrovně nebo přesnosti.

8.1.1 Zdroje informací pro ověřování a kontrolu

Zdroji informací pro průběžné ověřování kvalitativní úrovně bezpečnosti a pro kontrolu efektivity řízení bezpečnostních rizik by měly být:

1) Systémy bezpečnostních hlášení

- Systém povinného hlášení událostí
- Systém dobrovolného hlášení událostí
- Systém anonymního hlášení událostí

viz. kapitola: 7.2.3 Bezpečnostní systémy hlášení událostí

2) Bezpečnostní dotazování a průzkum

Bezpečnostní dotazování a průzkum slouží především k vytvoření zpětné vazby od personálu, hlavně pak od letových posádek a techniků údržby letadel. Zjišťuje bezpečnostní informace z problémových oblastí každodenního provozu pomocí názorů provozního personálu.

Bezpečnostní dotazování může být iniciováno buď zpětnou vazbou nebo dobrovolným hlášením za účelem identifikace problémů, které by mohly přispět ke vzniku nebezpečí. Jsou to například:

- Problémové oblasti nebo překážky v denním provozu
- Nahlížení na způsobilost personálu s možnými bezpečnostními následky
- Slabá týmová práce a spolupráce mezi skupinami zaměstnanců a jednotlivými organizačními celky
- Nesouhlas s rozhodovacím procesem vedoucích organizace nebo zmatky a případná nedorozumění
- Nebezpečné pracovní postupy nebo podmínky
- Prodlužování pracovní doby, nebo dlouhodobý výpadek z pracovního rytmu

K bezpečnostnímu dotazování a průzkumu mohou být použity kontrolních seznamy, dotazníky nebo informativní důvěrné rozhovory se zaměstnanci.

3) Bezpečnostní audity

Cílem bezpečnostních auditů je průběžné ověřování, že systém řízení bezpečnosti je schopný zaručit odpovídající úroveň personálu, plnění schválených postupů, předpisů a nařízení.

4) Bezpečnostní posuzování

Bezpečnostní posuzování je základním komponentem řízení změn. Provádí se při zavádění nového vybavení, nebo při změnách stávajících nebo zavádění nových postupů.

5) Bezpečnostní studie

Bezpečnostní studie je analýza zahrnující rozsáhlé obavy o bezpečnost. Zabývá se přezkoumáváním bezpečnostních záležitostí v širších souvislostech v globálním rámci. Pro lepší pochopení zde uvedu příklad.

U leteckého provozovatele se objevila zvýšená tendence nestabilizovaných přiblížení. Množství nehod při přiblížení na přistání vyvolalo znepokojení i na globální úrovni. Proto byly provedeny studie, jejichž výsledkem je několik bezpečnostních doporučení. Letecký

provozovatel může tato globální doporučení a studie použít pro svoji vlastní bezpečnostní analýzu.

6) Interní bezpečnostní vyšetřování

Týká se událostí, u kterých není vyžadováno, aby byly hlášeny Ústavu pro odborné zjišťování příčin leteckých nehod a ÚCL, nebo jimi šetřeny.

Rozsah interního bezpečnostního vyšetřování by měl být takový, aby odhalil hlavní příčinu události a všechna skrytá nebezpečí. Výsledky vyšetřování i s přijatými opatřeními by měly být šířeny organizací.

8.2 Řízení změn

Změny probíhající v každé organizaci představují dodatečná bezpečnostní rizika, která mohou mít vliv na procesy pro zmírnění bezpečnostních rizik. Proto je nutné tyto změny řídit. Hlavním zdrojem informací pro řízení změn je bezpečnostní posuzování. Změny můžeme rozdělit na interní nebo externí. Interní změny mohou být změny v řízení organizace, nové postupy nebo nové vybavení. Externí změny se týkají předpisů a požadavků.

8.3 Průběžné zdokonalování systému bezpečnosti

Účelem průběžného zdokonalování je zvýšení pod-standardní úrovně bezpečnosti organizace pomocí činností uvedených v rámci Zajištění bezpečnosti. Prováděné změny by měly být účinné a efektní. Zajištění bezpečnosti je založeno na principu cyklu průběžného zdokonalování a zajišťuje kontrolu kvalitativní úrovně bezpečnosti pomocí neustálého ověřování a zdokonalování provozního systému.

Průběžné zdokonalování může být provedeno pomocí vyhodnocení dokumentace a postupů organizace prostřednictvím auditů nebo bezpečnostního dotazování a průzkumu, prováděných systémem jakosti, nebo ověření, jak zaměstnanci plní svoje povinnosti ve vztahu k bezpečnosti.

Systém jakosti organizace by měl rovněž provádět re-aktivní vyhodnocování účinnosti systému řízení bezpečnosti. Především by pak měl ověřovat účinnost a efektivitu systému pro zmírnění bezpečnostních rizik následků nebezpečí.

9. Podpora bezpečnosti

Podpora bezpečnosti tvoří výstup ze systému řízení bezpečnosti a můžeme ji rozdělit na dvě části:

- Výcvik a vzdělávání
- Bezpečnostní komunikaci

9.1 Výcvik a vzdělávání

Veškerý personál organizace by měl absolvovat bezpečnostní výcvik, který přísluší k jejich odpovědnosti za bezpečnost. Především pak všichni vedoucí pracovníci a provozní personál by měli být řádně vycvičeni k vykonávání jejich povinností v rámci systému řízení bezpečnosti. Program bezpečnostního výcviku malých organizací může zahrnovat „e-learning“ nebo podobný výcvik, který je zajišťován oprávněným poskytovatelem výcviku.

9.2 Bezpečnostní komunikace

Bezpečnostní komunikace představuje systém předávání, šíření a celkového sdílení bezpečnostních informací napříč celou organizací. Rovněž tvoří základ pro rozvoj a udržování vhodné bezpečnostní kultury organizace. Způsoby bezpečnostní komunikace jsou například:

- Informační bulletiny
- Prezentace stavu bezpečnosti
- Bezpečnostní oznámení
- Informační schůzky, konané za účasti provozního personálu a odpovědného vedoucího nebo případně vrcholového vedení

Organizace by měla zavést komunikaci v záležitostech bezpečnosti, která má:

- Zajistit, že veškerý personál si je plně vědom důležitosti SMS a bezpečnostní kultury organizace
- Sdělovat kritické bezpečnostní informace, zejména které se vztahují k vyhodnoceným bezpečnostním rizikům a zanalyzovaným nebezpečím
- Vysvětlovat, proč jsou přijímána určitá opatření
- Vysvětlovat, proč jsou postupy týkající se bezpečnosti zaváděny nebo měněny

Malé organizace by navíc měly pořádat pravidelná shromáždění s personálem, na kterých budou podávány informace, diskutována opatření nebo postupy v záležitostech bezpečnosti.

10. Spolupráce SMS se systémem jakosti

Systém řízení organizace by měl v ideálním případě zahrnovat dva odlišné, ale navzájem se doplňující systémy. Systém jakosti (Quality Systém - QS) a systém řízení bezpečnosti (SMS). Systém jakosti a systém řízení bezpečnosti by měly být srovnatelné svým rozsahem a složitostí vzhledem k velikosti a složitosti organizace.

Zavedení systému jakosti umožňuje organizaci kontrolu dodržování předpisů, postupů a standardů stanovených organizací pro zajištění bezpečného provozu organizace. K tomu slouží audity, dotazování a průzkumy. Tyto bezpečnostní audity společně s bezpečnostním dotazováním a průzkumem jsou nedílnou součástí zajištění bezpečnosti organizace. Systém jakosti tak nezávisle sleduje a kontroluje správnou funkci systému řízení bezpečnosti.

Rozdíl mezi systémem řízení bezpečnosti (SMS) a systémem jakosti (QMS):

- SMS se zaměřuje na bezpečnostní aspekty organizace.
- QMS se zaměřuje na služby a produkty organizace.
- Zatímco QMS je zaměřen na shodu, SMS se zaměřuje na rizika. Neshody i nebezpečí mohou mít dopad bezpečnost.

Oba systémy zvyšují bezpečnost a jsou nezbytnými nástroji pro správu organizace. SMS nemůže být účinný bez použití zásad řízení kvality.

V organizační struktuře organizace by měli být vedoucí bezpečnosti i vedoucí jakosti na stejné úrovni, viz obrázek 2. způsob v kapitole 6.1 Vedoucí bezpečnosti. To znamená, že by měli spolupracovat. Vedoucí bezpečnosti je řídícím článkem v otázkách bezpečnosti.

11. GAP Analýza

GAP analýza neboli diferenční analýza má za úkol určit, které komponenty a prvky systému řízení bezpečnosti má organizace již zavedeny a které chybějící komponenty a prvky musí být zavedeny nebo změněny, aby byly splněny požadavky na plné zavedení SMS. Pro provedení této analýzy ICAO vydalo formulář, který se skládá z následujících čtyř částí:

- Bezpečnostní politika a cíle
- Řízení bezpečnostního rizika
- Zajištění bezpečnosti
- Podpora bezpečnosti

Každá z těchto čtyř částí obsahuje jednoduché otázky, na které lze odpovědět buď „Ano“ nebo „Ne“. Pakliže je odpověď kladná, znamená to, že daný komponent nebo prvek byl již organizací zaveden a do druhé kolonky se uvede, kde v dokumentaci organizace je daný prvek nebo komponent popsán. Jestliže je odpověď záporná, znamená to, že daný komponent nebo prvek nebyl dosud zaveden, nebo je v rozporu s požadavky. V tomto případě se do druhé kolonky uvede, jak bude daný komponent nebo prvek zaveden, případně jak bude docíleno jeho nápravy.

11.1 Problémové oblasti

Zavádění systému řízení bezpečnosti je déletrvající a složitý proces, který může organizaci působit jisté problémy. Každá organizace je jiná, má jiný výchozí stav pro zavedení SMS a jinak se dokáže vypořádat s případnými komplikacemi.

U malých leteckých dopravců bude zřejmě jednou z nejproblematičtějších oblastí řízení bezpečnostního rizika, konkrétně pak systém anonymního hlášení událostí, u kterého nelze zajistit plnou anonymitu, jak již bylo zmíněno v kapitole 7.2.4.5 „Problém anonymity hlášení“. Toto relativně obtížné získávání vstupních dat může způsobit, že celý zavedený systém bude mít tendenci pracovat „naprázdno“ a pouze formálně. Malá společnost znamená také malé počty výskytu všech potenciálně nepříznivých událostí a tedy statisticky obtížně zpracovatelné podklady.

K jistým problémům pak může docházet v oblasti podpory bezpečnosti. Tyto problémy může představovat nedostatečná formální komunikace uvnitř organizace. To zanamená, že zaměstnanci organizace si mezi sebou sdělí potřebné bezpečnostní informace, ale již nedochází k vedení příslušných záznamů o této komunikaci dostupných pro pozdější vyhodnocovaní účinností sytému. V případě, kdy dojde k nějaké mimořádné události způsobené například nesparávným postupem některého ze zaměstnanců organizace, se pak velmi těžko dokazuje, že byl dotyčný zaměstanaec seznámen s daným postupem, nebo riziky s ním spojenými. Tímto se také zmenšuje možnost odhalení a nápravy případných chybných postupů, dříve než způsobí mimořádnou událost.

Další problémy může způsobit samotný Safety Management Manual tím, že pro některé organizace může být až příliš obecný, nebo některými organizacemi toto může být naopak vnímáno jako jistá výhoda. Ve finále by pak mohlo dojít k tomu, že organizace bude mít sice formálně zavedený a popsaný SMS podle požadavků příslušného leteckého úřadu, ale tento systém nemusí v praxi zcela správně fungovat a přinášet tak pro organizaci předpokládáný přínos.

Velmi důležité pro správné fungování celého systému řízení bezpečnosti je včasné a správné odhalení a vyhodnocení bezpečnostního rizika – tedy zavedení všech procesů zaměřených tímto směrem. Tento postup je velmi komplexní a v řadě případů ho není možné úspěšně zavádět po částech, protože tyto samostatné subprocesy nemusí samy o sobě plnit požadovanou funkci bez napojení na ucelený SMS. Tato vlastnost vede opět k dilematu managementu, tedy k otázce přijatelné výše nákladů a dostupnosti zdrojů, jak ekonomických, tak personálních.

Jak již zde bylo zmíněno, každá organizace se potýká s jinými problémy a proto nelze jednoznačně určit všechny problémové oblasti v obecné rovině. Z provedené GAP analýzy však musí jasně vyplynout, co je pro kterou společnost problémem, jak formálně, tak reálně a naopak, které postupy jsou již nyní nastaveny na systémově přijatelné úrovni.

12. Zavádění SMS

Zavedení celého systému řízení bezpečnosti není možné provést najednou. Je nutné přihlédnout k daným možnostem organizace. Přesný postup zavádění SMS není pevně určený, ale jeho zavádění by mělo být systematické a probíhat v jednotlivých návazných krocích. Ovšem ne vždy je nutné všechny části SMS nově zavádět. U některých organizací tyto požadované části SMS již existují, nebo je stačí pouze poupravit do požadované podoby.

Podle doporučení ICAO by měl být SMS zaveden v těchto čtyřech fázích:

1) Plánování zavedení SMS

Cílem první části je navrhnout plán pro zvedení a začlenění SMS do organizace, dále pak stanovení odpovědností a provedení GAP analýzy. Z výsledků GAP analýzy může organizace určit aktuální stav řízení bezpečnosti a může tak začít podrobné plánování rozvoje řízení bezpečnosti.

2) Re-aktivní proces řízení bezpečnosti

Cílem druhé fáze je zavést základní procesy řízení bezpečnosti a odstranit nedostatky stávajících postupů řízení bezpečnosti.

3) Pro-aktivní a prediktivní proces řízení bezpečnosti

Úkolem této fáze je zavést pro-aktivní procesy řízení bezpečnosti tak, aby bylo možné provádět bezpečnostní analýzy založené na informacích, získaných prostřednictvím re-aktivní, pro-aktivní a prediktivní metody sběru bezpečnostních dat.

4) Provozní zajištění bezpečnosti

Čtvrtá fáze je závěrečnou fází zavádění SMS. Provozní zajištění bezpečnosti je posuzováno pomocí pravidelného sledování, zpětné vazby a průběžných nápravných opatření, tak aby bylo zajištěno účinné řízení bezpečnostního rizika v rámci měnících se provozních podmínek.

12.1 Cílový stav SMS

Provozovatelé obchodní letecké dopravy, provozovatelé letišť, poskytovatelé služeb řízení letového provozu a údržbové organizace mají povinnost provést nezbytné kroky k zajištění řádného zavedení požadavku Annexu 6 ICAO. Postupné zavádění SMS musí být u všech provozovatelů dokončeno do 1. ledna 2012. ICAO Safety Management Manual (Doc.9859) stanovuje obecný návod, podle kterého by se měl SMS ve finální fázi skládat ze čtyř komponentů obsahujících dvanáct prvků, tak jak bylo uvedeno v kapitole 5. Komponenty a prvky systému řízení bezpečnosti.

V dokumentu NPA 2008-22c EASA zapracovala standard ICAO, týkající se SMS do PART-OR (Organization Requirements) jako požadavek OR.GEN.200 na systém řízení (Management System), který se skládá z SMS a systému sledování pro vyhovění (Compliance Monitoring System), což je prakticky současný systém jakosti (Quality System).

Návrh požadavku ustanovení OR.OPS.100.GEN uvedeného v dokumentu NPA 2009-02c se týká odpovědností provozovatelů obchodní letecké dopravy. Účelem GM k OR.OPS.100 GEN je poskytnutí rady provozovatelům pro tvorbu standardních provozních postupů (Standard Operational Procedures).

Podle vyjádření Ing. Vlčka z ÚCL ČR se jedná pouze o návrhy, které vydala EASA formou NPA (Notice of Proposed Amendments). V současné době již skončilo připomínkové řízení a nyní je nutné počkat, až toto nařízení bude vydáno jako právně závazné. Prováděcí nařízení EU by mělo vstoupit v platnost nejpozději k 08.04. 2012.

NPA 2008-22c uvádí v odstavci OR.GEN.200 "Management System":

Stávající návrhy/tendence:

a) Organizace musí vytvořit a udržovat systém řízení, který zahrnuje:
1) Bezpečnostní politiku
2) Proces identifikace nebezpečí a proces vyhodnocování a řízení rizik s tím spojených
3) Jasně definovanou linii odpovědností za bezpečnost v celé organizaci, včetně přímé odpovědnosti za bezpečnost ze strany vrcholového vedení
4) Personál vyškolený k plnění svých úkolů
5) Proces hlášení a analýzy nebezpečí a proces pro provádění nápravných činností pro předcházení jejich opakování
6) Příručku organizace obsahující všechny procesy systému řízení, včetně procesu, kterým se zabezpečí, aby si personál uvědomoval svoje povinnosti
7) Funkci sledování, aby systém řízení vyhověl příslušným požadavkům a postupům. Sledování pro vyhovění musí zahrnovat zpětnou vazbu k odpovědnému vedoucímu pro zajištění nápravných opatření ke zjištěným nedostatkům dle potřeby.
8) Jakékoli dodatečné požadavky předepsané částí-OR

b) Systém řízení musí odpovídat velikosti, povaze a složitosti činností a nebezpečí a souvisejících rizik spojených s těmito činnostmi.

Konečný výsledek - vize do budoucnosti:

V budoucnosti by mělo dojít ke kombinaci systému jakosti, systému řízení bezpečnosti a „celkového“ systému řízení. Touto kombinací vznikne SQMS (Safety and Quality Management System).

Následující tři skutečnosti postihují integrovaný přístup, jak vytvořit a udržovat spojení bezpečnosti a systému řízení jakosti:

- Dříve - bez uvážení požadavků na SMS. Provozovatelé se zabývali různými požadavky. Bylo snazší jim vyhovět, pokud existoval jeden jediný systém jakosti, který sledoval dodržování těchto norem a požadavků.

- Skutečnost, že dnešní požadavky na systém jakosti jsou součástí požadavků na SMS, vede k dalšímu rozvoji stávajících systémů jakosti podle nových požadavků (účelem systému jakosti je zajistit bezpečný provoz a letuschopnost letadel)

- EASA se snaží izolovat organizační témata, včetně řízení rizik a zajištění bezpečnosti v systému řízení. V důsledku toho pojem „systém jakosti“ pravděpodobně zanikne, protože nový přístup povede k systému řízení (Management System), obsahujícímu systém sledování pro vyhovění (Compliance Monitoring System), což je prakticky současný systém jakosti (Quality System), který pojme i příručku pro řízení bezpečnosti (Safety Management Manual), která bude pokrývat oblast řízení bezpečnosti.

Tento závěr je potvrzen prohlášením v NPA 2008-22a:

Koncept systému jakosti, jak je znám v rámci systému JAA a ve stávajících EASA Parts, je začleněn jako systém sledování pro vyhovění (Compliance Monitoring System) a stává se prvkem systému řízení organizace. Řízení tohoto systému sledování pro vyhovění (Compliance Monitoring System) včetně jeho programu je částečně také v odpovědnosti vedoucího bezpečnosti.

Jinými slovy: Vedoucí systému sledování pro vyhovění (Compliance Monitoring System) přesune část povinností spojených s bezpečností na vedoucího bezpečnosti.

13. Závěr

Zavedení systému řízení bezpečnosti zvyšuje současnou úroveň bezpečnosti v civilní letecké dopravě pomocí systematického procesu identifikace, vyhodnocování a zmírňování nebezpečí. Tento systém pokrývá všechny provozní části společnosti a vnáší tak potřebné bezpečnostní principy do všech důležitých provozních úseků. Ne vždy je nutné všechny části SMS nově zavádět. U některých organizací určité požadované části SMS již existují, nebo je stačí pouze poupravit do požadované podoby. Přechod na plně integrovaný SMS není možné provést najednou, je nutné přihlédnout k daným ekonomickým a personálním možnostem organizace. Zejména pak právě u malých leteckých dopravců, u kterých je na jednu stranu dostačující zavedení některých částí SMS pouze ve zjednodušené podobě, ovšem na druhou stranu tito dopravci nemívají k dispozici tolik potřebných zdrojů jako velké letecké společnosti. Postupný přechod na úplný systém řízení bezpečnosti však musí být u všech provozovatelů dokončen nejpozději do 1. ledna 2012. Jaký ale bude skutečný přínos SMS ? Odpověď na tuto otázku není jednoduchá.

Oslovil jsem několik menších leteckých společností v České republice i ve světě s otázkou, zda má zavedení SMS pro jejich provoz nějaký přínos. Bohužel jsem se dočkal pouze dvou odpovědí, a to od letecké společnosti Silesia Air a CCA. U letecké společnosti CCA mají naplánováno plné zavedení systému řízení bezpečnosti na polovinu roku 2010, a proto zatím na tuto otázku nedokáží odpovědět. Přesto vedoucí jakosti osobně žádný větší přínos tohoto systému nevidí, protože 92% SMS již pokrývají systémem jakosti.

Situace u společnosti Silesia Air je v mnohém podobná. Zavedení systému řízení bezpečnosti bude na základě požadavků ÚCL provedeno v zatím neupřesněném termínu. Podle vyjádření vedoucího jakosti hlavní přínosy tohoto systému nejsou zatím zcela zřejmé – stojí na očekáváních v teoretické rovině. Také zde platí, že hlavní parametry jsou už nyní pokryty systémem jakosti, a kdyby nebyli nuceni k zavedení SMS „zvnějšku“, v dohledné době a popisované podobě by k němu pravděpodobně nedošlo.

Je-li ovšem již většina komponentů SMS v organizaci zavedena, pak přínosem přechodu na plně integrovaný SMS bude dokonalá součinnost těchto komponentů. Systém řízení bezpečnosti zavádí i některé nové prvky do celého systému bezpečnosti organizace, jako je například funkce vedoucího bezpečnosti.

Myslím si, že SMS jako takový je a bude zcela jistě přínosný, hlavně pak pro ty organizace, které v současné době nepokrývají tak velkou část řízení bezpečnosti systémem jakosti jako již zmíněné společnosti Silesia Air a CCA. Jaký však bude skutečný přínos SMS, ukáže až budoucnost.

14. Seznam použitých zdrojů

Literatura:

[1] ICAO Doc.9859, Safety Management Manual (SMM) Second Edition, Montreal 2009, ISBN 978-92-9231-295-4

[2] Nařízení komise (ES) č.859/2008, příloha III (EU-OPS), Brusel 2008

[3] Směrnice OLP Provoz obchodní letecké dopravy (letouny), CAA-OLP-01-1/08, ÚCL ČR, Praha 2008

[4] Předpis L6 Provoz letadel, část 1, ÚCL ČR, Praha 2009

[5] Diplomová práce: Bc. Michal Šalanda, Zavedení systému řízení bezpečnosti u malého leteckého dopravce, VUT v Brně, Brno 2008

[6] IEM k ACJ OPS 1.037

[7] NPA 2009-02c, EASA 2009

[8] NPA 2008-22c, EASA 2008

[9] AIC C 10/2010, Praha 2010

Počítačové prezentace:

[1] ICAO Safety Management Systems (SMS) Course, Module No: 1 – 10, ICAO 2008

[2] Vince Galotti, Harmonization of Safety Management Systems (SMS), ICAO 2006

Internetové stránky:

[1] www.ukfsc.co.uk

[2] www.bazl.admin.ch

[3] www.aviation-safety.net