ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Systémové řízení provozní bezpečnosti v leteckých údržbových organizacích

Systemic Safety Management of Aircraft Maintenance Organizations

Diplomová práce

Studijní program: Technika a technologie v dopravě a spojích

Studijní obor: Provoz a řízení letecké dopravy

Vedoucí práce: doc. Ing. Andrej Lališ, Ph.D.
Ing. Natalia Guskova

Bc. Zdeněk Žďánský

Praha 2023

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621.....Ústav letecké dopravy

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Zdeněk Žďánský

Studijní program (obor/specializace) studenta:

navazující magisterský – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Systémové řízení provozní bezpečnosti v leteckých údržbových organizacích**

Název tématu (anglicky): Systemic Safety Management of Aircraft Maintenance Organizations

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je stanovit postup a technické nástroje pro vývoj vybraných částí systému řízení provozní bezpečnosti (SMS) letecké údržbové organizace směrem k systémovému přístupu k bezpečnosti.
- Analyzujte systémový přístup k bezpečnosti a jeho současné metody.
- Analyzujte systém řízení provozní bezpečnosti (SMS) vybrané letecké údržbové organizace.
- Aplikujte systémový přístup k bezpečnosti na vybrané prvky SMS systému konkrétní letecké údržbové organizace.
- Stanovte postup a technické nástroje pro vývoj SMS dané konkrétní letecké údržbové organizace směrem k systémovému přístupu k bezpečnosti.
- Dosažené výsledky vyhodnoťte a porovnejte se současným stavem.

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury:
Hollnagel, Erik. Safety-I and Safety-II: The Past and Future of Safety Management. CRC Press, 2014.
ICAO, Doc. 9859: Safety Managment Manual, 4th Ed., Montréal, Quebec, 2018.
Leveson, Nancy. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.

Vedoucí diplomové práce: **doc. Ing. Andrej Lališ, Ph.D.**
Ing. Natalia Guskova

Datum zadání diplomové práce: **15. července 2022**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **15. května 2023**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

prof. Ing. Ondřej Přibyl, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Zdeněk Žďánský
jméno a podpis studenta

V Praze dne 15. července 2022

Abstrakt

Předkládaná diplomová práce se zabývá vývojem vybraných částí systému provozní bezpečnosti (SMS) vybrané údržbové organizace pomocí systémového přístupu. Na základě systémové analýzy současného stavu byla odhalena místa s potenciálem pro možný vývoj. Tato práce představuje využití procesu identifikace nebezpečí a hodnocení rizik a návrh registru nebezpečí, které jsou založeny na bezpečnostním modelu STAMP a analytické metodě STPA, v SMS vybrané údržbové organizace. Navržený registr nebezpečí obsahuje již 19 navržených systémových nebezpečí, která jsou výchozím bodem pro identifikaci dílčích nebezpečí. Diplomová práce obsahuje také návrh nové sady indikátorů bezpečnosti. Pro vytvoření indikátorů byla provedena analýza STPA vybrané údržbové organizace. Diplomová práce ukazuje, jakým způsobem lze využít systémový přístup k bezpečnosti pro analýzu současného stavu a vývoj SMS v konkrétní údržbové organizaci.

Klíčová slova: Údržba letadel, systém řízení provozní bezpečnosti, systémový přístup k bezpečnosti, System-Theoretic Accident Model and Process, System-Theoretic Process Analysis, registr nebezpečí, řízení rizik, indikátory bezpečnosti

Abstract

The presented thesis deals with the development of selected parts of the Safety Management System (SMS) of a chosen maintenance organization using a systemic approach. Based on the systemic analysis of the current state, areas with potential for possible development were identified. This thesis presents the utilization of the process of hazard identification and risk assessment, and the proposal of a hazard register based on the STAMP safety model and the analytical method of STPA, in the SMS of a selected maintenance organization. The proposed hazard register already contains 19 suggested systemic hazards, which serve as a starting point for identifying partial hazards. The thesis also includes a proposal for a new set of safety indicators. To create these indicators, an analysis of the STPA of the selected maintenance organization was conducted. The thesis demonstrates how a systemic safety approach can be used to analyse the current state and develop SMS in a specific maintenance organization.

Keywords: aircraft maintenance, Safety Management System, systemic approach to safety, System-Theoretic Accident Model and Process, System-Theoretic Process Analysis, hazard register, risk assessment, Safety Performance Indicators

Poděkování

Rád bych poděkoval doc. Ing. Andreji Lališovi, PhD. a Ing. Natalii Guskové za jejich spolupráci, podporu a odborné vedení při psaní této práce. Také bych rád tímto poděkoval Ing. Martinovi Orlitovi za poskytnuté postřehy z praxe. Závěrem bych chtěl poděkovat své rodině a přítelkyni za podporu a důvěru v moji osobu během studia a při psaní této diplomové práce.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Systémové řízení provozní bezpečnosti v leteckých údržbových organizacích vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 10. května 2023 .....

Podpis

Obsah

Seznam příloh

Seznam obrázků

Seznam tabulek

Seznam zkratek

Zkratka	Česky	Anglicky
AMO	Schválená údržbová organizace	Approved Maintenance Organization
AOC	Osvědčení letového provozovatele	Aircraft Operator Certificate
CAME	Výklad organizace zachování letové způsobilosti	Continuing Airworthiness Management Exposition
CAMO	Organizace zachování letové způsobilosti	Continuing Airworthiness Management Organisation
CAST	Analýza příčin založená na STAMP	Causal Analysis based on STAMP
CMES	Kombinované skóre efektivity zmírnění	Combined Mitigation Effectivness Score
ČR	Česká republika	Czech Republic
EASA	Agenturou Evropské unie pro bezpečnost v letectví	European Union Aviation Safety Agency
EU	Evropská unie	European union
FRAM	Metoda funkční rezonanční analýzy	Functional Resonance Analysis Method
ICAO	Mezinárodní organizace pro civilní letectví	International Civil Aviation Organization
MES	Skóre efektivity zmírnění	Mitigation Effectivness Score
MIT	Massachusettský technologický institut	Massachusetts Institute of Technology
MOE	Výklad organizace údržby	Maintenance Organisation Exposition
OPB	Oddělení provozní bezpečnosti	Safety Department
PMS	Závažnost před zmírněním	Pre-Mitigation Severity

PPMS	Potenciální závažnost po zmírnění	Post-Potential Mitigation Severity
RM	Odpovědný vedoucí	Responsible Manager
SARPs	Standardy a doporučené postupy	Standards and Recommended Practices
SDCPS	Systém sběru a zpracování bezpečnostních dat	Safety Data Collection and Processing Systems
SMM	Manuál řízení provozní bezpečnosti	Safety Management Manual
SMS	Systém řízení bezpečnosti	Safety Management System
SPIs	Indikátory bezpečnosti	Safety Performance Indicators
SRM	Řízení bezpečnostních rizik	Safety Risk Management
SSP	Státní program bezpečnosti	State Safety Programme
STAMP		System-Theoretic Accident Model and Process
STPA	Systémově-teoretická analýza procesů	System-Theoretic Process Analysis
UCA	Nebezpečná řídící akce	Unsafe Control Action
ÚCL	Úřad pro civilní letectví	Civil Aviation Authority
VPB	Vedoucí provozní bezpečnosti	Safety Manager

Úvod

Bezpečnostní inženýrství využívá modely, metody a postupy, které jsou založeny na myšlence lineární kauzality. Toto vnímání se však ukazuje být nedostatečné pro komplexní socio-technické systémy. Jedním z takových systémů je letecká údržba, která ve svém systému sdružuje člověka i velmi složité technologie. S rostoucí automatizací a s novými technologiemi je kladen stále větší důraz na jejich údržbu s cílem zajistit vysokou spolehlivost a bezpečnost těchto systémů.

K zajištění provozní bezpečnosti v údržbových organizacích slouží systém řízení provozní bezpečnosti (SMS). Ten je dle legislativních požadavků nově nutné zavádět ve schválených údržbových organizacích povinně. SMS se skládá z několika částí, které mají za cíl zajistit vysokou úroveň provozní bezpečnosti.

Cílem této práce je stanovit postup a technické nástroje vybraných částí systému řízení provozní bezpečnosti (SMS) letecké údržbové organizace směrem k systémovému přístupu. Systémový přístup zajistí hlubší poznání komplexních socio-technických systémů jakožto celku. Pomocí něj je možné pochopit souvislosti mezi jednotlivými komponenty systému, jak spolu vzájemně interagují a ovlivňují se. Před výběrem částí SMS, které budou dále vyvíjeny, je nutné nejdříve analyzovat samotný SMS. Ten je v práci analyzován jako celek. Na základě této analýzy jsou identifikována slabá místa, která jsou dále vyvíjena směrem k systémovému přístupu.

Pro analýzu současného systému údržbové organizace je zvolena proaktivní systémová metoda Systems-Theoretic Process Analysis (STPA), která je založená na modelu System-Theoretic Accident Model and Process (STAMP). Tato metoda ukazuje, jak systém údržbové organizace funguje jako celek. Výsledky analýzy jsou následně využity k vývoji vybraných částí SMS.

Navržené technické nástroje a postupy jsou první částí vývoje již zavedeného SMS v konkrétní údržbové organizaci směrem k systémovému přístupu k bezpečnosti. K návrhu postupů a technických nástrojů byly využívány systémové metody, které řeší problémy

současného přístupu k bezpečnosti, který je využíván bezpečnostním inženýrstvím. Lineární kauzalita neumožňuje zobrazení širšího kontextu bezpečnostních problémů komplexních systémů. Z toho důvodu je na tyto systémy nutné pohlížet systémově jako na celek. Vývoj SMS pomocí systémového přístupu může přinést přesnější data, jednodušší a účinnější systémy a v tomto důsledku také nižší náklady pro zajištění bezpečnosti.

1. Letecká bezpečnost

Letecká bezpečnost je odvětví, jehož cílem je zajištění bezpečného provedení veškerých procesů souvisejících s letem. Mezinárodní organizace pro civilní letectví (ICAO) definuje bezpečnost jako *„Stav, při kterém jsou rizika spojená s leteckými činnostmi souvisejícími s provozem letadel nebo jej přímo podporujícími snížena a řízena na přijatelné úrovni.“* [1].

Letecká bezpečnost se neorientuje pouze na samotné provedení letů, ale také na procesy, které letům předcházejí. Tyto procesy důležité pro zajištění bezpečnosti ve vzduchu se odehrávají na zemi před i po daném letu.

Letecká bezpečnost je dynamická a mění se v čase. Nová nebezpečí a rizika vyvstávají v letectví průběžně a je potřeba jejich možné dopady zmírňovat. Je proto nutné neustále rizika sledovat a udržovat na odpovídající a přiměřené úrovni, aby byla zajištěna vysoká bezpečnost letectví. Veškeré chápání a vnímání přijatelné bezpečnosti vždy závisí na lokálních a mezinárodních faktorech, kterými jsou zpravidla předpisy, normy a v neposlední řadě také kultura. [2]

V průběhu let se letecká bezpečnost, ale i bezpečnost obecně, vyvíjela. Tento vývoj lze popsat pomocí historických přístupů k bezpečnosti. V současné době ICAO uvádí 4 takové přístupy. Vývoj bezpečnosti a přístupů k bezpečnosti je zobrazen na Obrázku 1.

Technický přístup

Tento přístup je datován od počátku dvacátého století do konce 60. let. Zaměřoval se primárně na technické faktory a technická selhání. Technický přístup se věnoval především šetření a řešení technických faktorů vedoucích k nehodám a incidentům. Technologická vylepšení vedla k úbytku počtu nehod a bezpečnostní procesy nově zahrnovaly také sledování shody dodržování předpisů (compliance) a dohled nad bezpečností. [2]

Lidský činitel (Ergonomie)

Technologický přístup výrazně snížil počet leteckých nehod. Pro zajištění stále bezpečnějšího provozu se začalo přihlížet také na člověka a jeho souznění s jeho

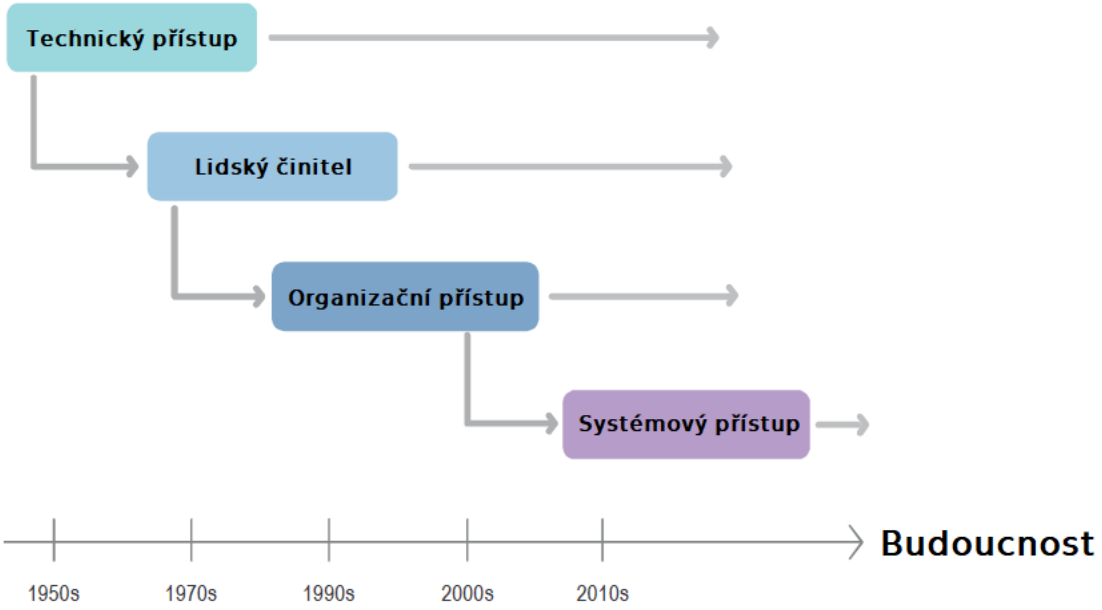
technickým okolím. I přes zvýšené snahy zmírňování rizik se lidský činitel stále častěji objevoval jako příčinný faktor leteckých nehod a incidentů. V období mezi 70. a 90. lety 20. století se k lidskému činiteli přistupovalo převážně individuálně a bez kontextu k organizační struktuře. [2]

Organizační přístup

Během 90. let 20. století se začal objevovat tzv. organizační přístup k bezpečnosti. Tento přístup upíral svůj pohled jak na technické faktory a ergonomii, tak i na organizační faktory, které přispívaly k nehodám. Začal být vnímán vliv organizační kultury, politik bezpečnosti a efektivity řízení rizik na leteckou bezpečnost. Využívány byly také reaktivní a některé proaktivní metody pro analýzu a sběr dat týkajících se bezpečnosti. [2]

Systémový přístup

ICAO považuje za systémový přístup (tzv. Total system approach) vyvinutý organizační přístup, který obsahuje předchozí přístupy na vyšší úrovni vyspělosti. Tento přístup zavádí systém řízení provozní bezpečnosti (SMS) a Státní program bezpečnosti (SSP). V tomto přístupu je snaha pohlížet na bezpečnost v kontextu celého systému letectví a vnímat tak napojení a spolupráce rozdílných organizací v leteckém průmyslu. [2]



Obrázek 1: Vývoj bezpečnosti (přeloženo a upraveno autorem z [2])

Regulace, normy, zákony a jiné standardy jsou nezbytným základem pro zajištění bezpečnosti v letectví. Avšak, i když mají tyto předpisy za cíl minimalizovat rizika a zajistit bezpečnost, bezpečnost v letectví není pouze o regulacích a standardech samotných. Tyto předpisy se spoléhají na předpoklad konstantní výkonnosti systému, ale v praxi se výkonnost může lišit kvůli mnoha faktorům, a je těžké ji přesně odhadnout. Rozdíl mezi teorií a praxí popisuje koncept odchylky praxe (practical drift), který označuje odchylku od teoretického návrhu systému k jeho skutečnému provozu. [2]

Bezpečnost je nedílnou součástí každé letecké společnosti a měla by patřit mezi hlavní priority. Primárním cílem každé letecké společnosti je ale především zajištění finančních příjmů a její další rozvoj. Zajištění bezpečnosti vyžaduje často nemalé finanční výdaje. Investovat však veškeré zisky do zajištění bezpečnosti by pro společnosti nebylo udržitelné. Z toho důvodu je nutné nalézt určitý balanc mezi investicemi do zajištění bezpečnosti a do dalšího rozvoje společnosti. Tento rozhodovací proces popisuje dilema řízení. [2]

1.1. Odchylka praxe (Practical drift)

Odchylka od praxe neboli practical drift je myšlenka, kterou popsal Scott A. Snook ve své knize Friendly fire: the accidental shootdown of U.S. Black Hawks over Northern Iraq. Tato myšlenka je uvedená také v ICAO Safety Management Manual (Doc 9859). [2]

Myšlenka popisuje, jak se výkonnost systému odchyluje od jeho původního návrhu. Postupy, úkoly, úlohy a vybavení jsou původně plánovány na teoretické prostředí pro ideální podmínky, kde téměř vše lze snadno predikovat a řídit. Návrh takového systému se zakládá na třech předpokladech [2]:

a) Technika a technologie potřebná k dosažení cílů je dostupná.

b) Personál je vyškolený, kompetentní a motivovaný ke správnému využití technologií.

c) Politika a procesy řídí systém a lidské chování.

Tyto předpoklady jsou platné do té doby, než je systém uveden do reálného provozu. Jakmile je systém uveden do reálného provozu, začnou se původní předpoklady stávat více a více neplatnými a v praxi se systém začne odchylovat od původního teoretického návrhu. Snook uvádí, že odchýlení od teoretického návrhu je nevyhnutelné pro kterýkoliv systém, bez ohledu na to, jak moc je původní návrh pečlivý a dobře myšlený. Příčin odchylky praxe může být mnoho a tyto příčiny se mohou vzájemně kombinovat. [2] [3] Například [2]:

a) Technika a technologie nefungují, jak bylo naplánováno

b) Některé postupy nemohou být provedeny podle plánu

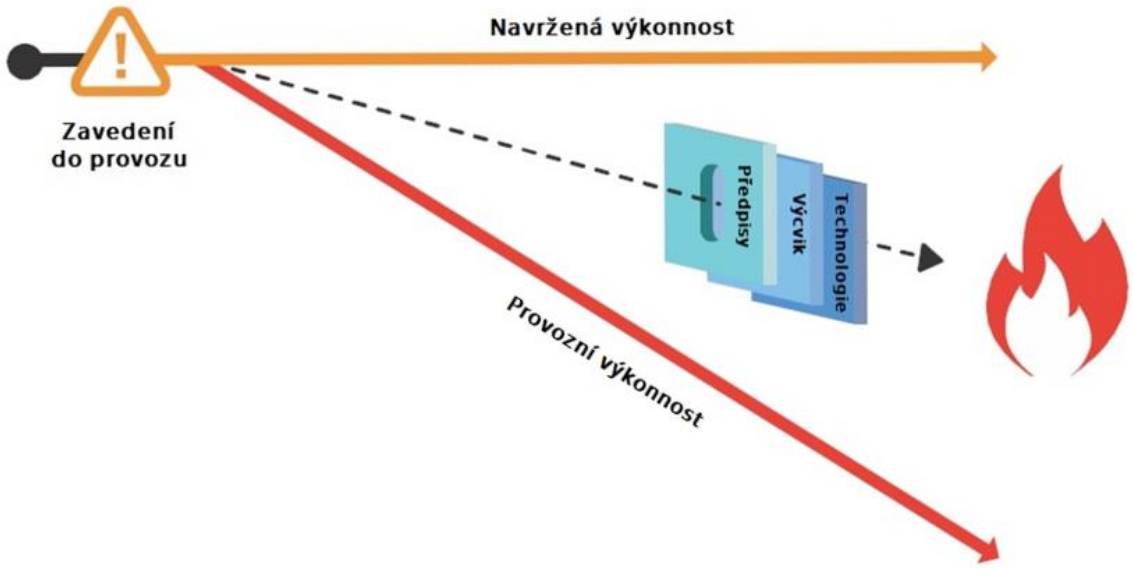
c) Nastávají změny systému

d) Systém interaguje s dalšími systémy

e) Kultura bezpečnosti

Odchylku praxe (Practical drift) graficky znázorňuje Obrázek 2. Oranžová šipka představuje směr, který je uveden v návrhu za předpokladu konstantní výkonnosti systému. Červená šipka představuje reálnou výkonnost, která se od tohoto směru odchyluje od okamžiku,

kdy dojde k zavedení do reálné praxe. Červený plamen představuje nehodu či incident, ke kterým dojde, pokud jim nezabrání navržené bezpečnostní bariéry – předpisy, výcvik, technologie.

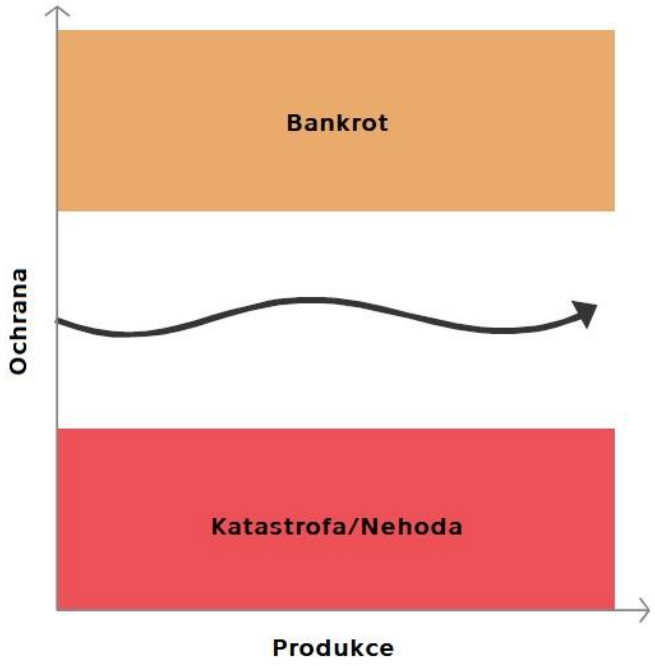


Obrázek 2: Odchylka praxe (Practical drift) (přeloženo a upraveno autorem z [2])

1.2. Dilema řízení

Dilema řízení (management dilemma) ukazuje, že je potřeba vyvažovat mezi ziskovostí a bezpečností, aby bylo možné zajistit jak rozvoj společnosti, tak její bezpečnost. [2]

Dilema řízení je rozhodovací proces především vedení společností. Letecké společnosti či organizace mají snahu zajistit bezpečnou službu. Do zajištění bezpečnosti musí společnosti investovat finanční prostředky. Na druhou stranu je cílem každé společnosti zvyšovat produkci a generovat zisk potřebný pro další chod a rozvoj společnosti či organizace. Do rozšíření produkce a rozvoje společnosti je nutné vynaložit nemalé zdroje. Mezi těmito dvěma druhy investic je nutné balancovat a zajistit rozumný poměr mezi nimi. Obrázek 3 ukazuje, že nejoptimálnější varianta je udržení se v tzv. bezpečném prostoru (safety space). Tento prostor je bezpečný jak pro ochranu/provozní bezpečnost (safety), tak i pro produkci. [2]



Obrázek 3: Koncept bezpečného prostoru (přeloženo a upraveno autorem z [2])

Pokud se společnost rozhodne investovat do prvku systému, který zvyšuje výkonnost v oblasti bezpečnosti, musí při tom zvážit dopad této změny na produktivitu společnosti. V případě, že by produktivita společnosti významně klesla v důsledku zavedení nového prvku systému, který zvyšuje výkonnost v oblasti bezpečnosti, dostane se společnost mimo bezpečný prostor (safety space) a přiblíží se bankrotu společnosti. [2]

Pokud by na druhou stranu společnost investovala do rozvoje produkce společnosti s cílem generovat větší zisk, může tím být snížena výkonnost v oblasti bezpečnosti a v tomto důsledku by mohlo dojít ke katastrofě. [2]

2. Řízení bezpečnosti

Řízení bezpečnosti je proces, který má za cíl proaktivně zmírňovat rizika před tím, než jejich důsledky zapříčiní nehodu či incident. Tohoto cíle je dosahováno na základě zavedení a udržování systému řízení provozní bezpečnosti (SMS) v jednotlivých organizacích a také pomocí Státního programu bezpečnosti (SSP). [2] [4]

2.1. Státní program bezpečnosti (SSP)

Státní program bezpečnosti (SSP), neboli State Safety Programme, je definovaný jako „integrovaný soubor pravidel a činností zaměřený na zvyšování bezpečnosti" [4]. SSP musí zavést a udržovat státem v rozsahu a příslušné náročnosti, která odpovídá potřebné úrovni civilního letectví daného státu. [4]

ICAO Annex 19 stanovuje 4 základní složky SSP [1]:

1) Politika a bezpečnostní cíle na úrovni státu
2) Řízení bezpečnostních rizik na úrovni státu
3) Zajištění bezpečnosti na úrovni státu
4) Prosazování bezpečnosti na úrovni státu

2.2. Safety Management System (SMS)

Safety Management System (SMS) se překládá jako systém řízení provozní bezpečnosti. ICAO definuje SMS jako *„Systematický přístup k řízení bezpečnosti včetně nezbytné organizační struktury, odpovědnosti, zodpovědností, zásad a postupů"* [2]. Cílem SMS je snaha proaktivně zmírňovat bezpečnostní rizika dříve, než vyústí v incident či nehodu. [2]

Základní požadavky na SMS stanovuje Annex 19 Chicagské úmluvy z roku 1944. V České republice (ČR) je pak tento Annex 19 implementován v rámci národní legislativy jako letecký předpis L19. Podrobný popis a návod na zavedení Safety Management System

do organizace či společnosti obsahuje dokument Doc 9859, Safety Management Manual (v současné době jeho nejaktuálnější verze ICAO SMM 4th edition). [1] [2] [4]

Safety Management System se skládá ze 4 základních komponentů, jak je definuje předpis L19 i Doc 9859. Tabulka 1 uvádí komponenty SMS včetně jejich podsložek (elementů). [2] [4]

Tabulka 1: Komponenty a elementy systému řízení provozní bezpečnosti [1] [4]

Komponent	Element
1. Politika a cíle bezpečnosti	1.1. Závazek vedení
	1.2. Odpovědnost a zodpovědnosti za bezpečnost
	1.3. Jmenování klíčového personálu
	1.4. Koordinace plánování mimořádných událostí
	1.5. SMS dokumentace
2. Řízení bezpečnostních rizik	2.1. Identifikace nebezpečí
	2.2. Hodnocení a zmírňování rizik
3. Zajištění bezpečnosti	3.1. Sledování a měření výkonnosti v oblasti bezpečnosti
	3.2. Řízení změn
	3.3. Průběžné zlepšování SMS
4. Prosazování bezpečnosti	4.1. Výcvik a vzdělávání
	4.2. Komunikace (sdílení) bezpečnosti

1. **Politika a cíle bezpečnosti**

Tento komponent SMS udává povinnost jasně specifikovat postoje společnosti či organizace vzhledem k bezpečnosti. Přijímá odpovědnost a poskytuje veřejný závazek k zajištění bezpečnosti ve všech jejích činnostech. [4]

2. **Řízení bezpečnostních rizik**

Je nezbytné pojmenovávat bezpečnostní rizika a identifikovat nebezpečí, která ohrožují či mohou ohrozit bezpečný provoz organizace či společnosti. Rizika je nutné pravidelně aktualizovat, analyzovat a ohodnocovat jejich závažnost. [4]

3. **Zajištění bezpečnosti**

Pro zajištění bezpečného provozu organizace či společnosti je nutné neustále a kontinuálně sledovat výkonnost v oblasti bezpečnosti. Je třeba si stanovit bezpečnostní cíle a ukazatele, které ověřují účinnost bezpečnostních postupů a procesů ve společnosti a ukazují současný stav a možný vývoj v oblasti bezpečnosti. Je také důležité uvědomovat si rizikovost zásadních změn, které mohou ovlivnit bezpečnost provozu. [4]

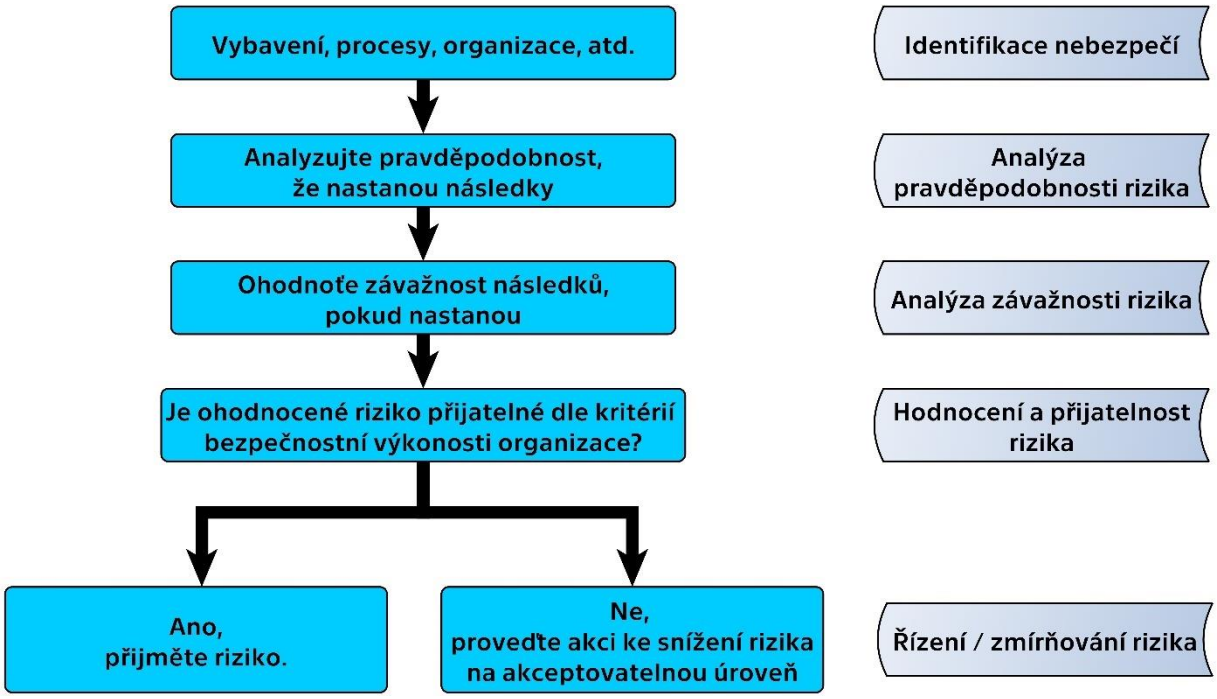
4. **Prosazování bezpečnosti**

Nastavení pozitivní kultury bezpečnosti je základním předpokladem pro zajištění bezpečnosti v organizaci či společnosti. Je nutné zajistit dostatečný výcvik a vzdělání personálu v oblasti bezpečnosti a nastavit systém pro sdílení informací, který distribuuje a vysvětluje veškeré postupy potřebné k zajištění bezpečnosti. [4]

2.3. Řízení bezpečnostních rizik

Řízení bezpečnostních rizik (SRM) je jedna z nejužitečnějších částí SMS pro řízení provozní bezpečnosti. Tento komponent SMS umožňuje identifikovat nebezpečí, která ohrožují bezpečnost celého systému. Dále je se při tomto procesu odhalí možná rizika (následky), ke kterým mohou daná nebezpečí vést. [2]

Detailní postup řízení rizik je vidět na Obrázku 4. Tento postup stanovuje ICAO v dokumentu Doc 9859.



Obrázek 4: Diagram identifikace nebezpečí a proces řízení rizik (přeloženo a upraveno autorem z [2])

Identifikace nebezpečí je první a důležitá část procesu řízení bezpečnostních rizik. Společnost či organizace by měla stanovit řádný postup pro identifikaci nebezpečí ve všech odvětvích jejích aktivit. Nebezpečí mohou být identifikována pouze uvnitř společnosti nebo také v rámci externích vstupů do procesů. Externími vstupy jsou myšleny externí organizace, které spolupracují s danou společností, ale nejsou její součástí. Jedná se například o organizace, které outsourcují část služeb nebo také úřady, které ovlivňují svou pravomocí procesy společnosti. Externím vstupem do procesů společnosti může být také požadavek klienta. Každé identifikované nebezpečí s sebou nese také možný následek. Následky, které dané nebezpečí může způsobit, mají rozdílné charaktery a rozdílné bezpečnostní dopady na systém. Je proto důležité dané následky (nebo také rizika) ohodnotit tak, aby bylo možné jasně stanovit priority v oblasti bezpečnosti. [2]

Druhý a třetí krok procesu řízení bezpečnostních rizik, jak je popisuje Doc 9859, obsahuje ohodnocení rizika dle pravděpodobnosti, že následek nastane, a dle závažnosti následku.

Dle ICAO alfanumerického systému ohodnocování rizik se pravděpodobnost rizika ohodnocuje v rozmezí hodnot 1-5, které ukazují, jak moc je pravděpodobné, že následek nastane. Tabulka 2 vysvětluje jednotlivé pravděpodobnosti a přikládá jim číselnou hodnotu. Obdobný postup je pak aplikován na ohodnocení závažnosti rizika v rozmezí hodnot A-E, což ukazuje Tabulka 3. [2]

Tabulka 2: Pravděpodobnost rizika (přeloženo a upraveno autorem z [2])

Pravděpodobnost	Význam	Hodnota
Časté	Pravděpodobně nastane mnohokrát (vyskytuje se pravidelně)	5
Občasné	Pravděpodobně občas nastane (vyskytuje se nepravidelně)	4
Vzdáleně pravděpodobné	Nepravděpodobné, že nastane, ale možné (vyskytuje se zřídka)	3
Nepravděpodobné	Velmi nepravděpodobné, že nastane (není známo, že by se vyskytovalo)	2
Extrémně nepravděpodobné	Téměř nepředstavitelné, že k této události dojde	1

Tabulka 3: Závažnost rizika (přeloženo a upraveno autorem z [2])

Závažnost	Význam	Hodnota
Katastrofické	• Letoun / vybavení zničeno • Několik úmrtí	A
Nebezpečné	• Vážná zranění • Významné poruchy vybavení	B
Vážné	• Vážný incident • Zranění osob	C
Méně vážné	• Nepříjemnost • Provozní omezení • Použití nouzových postupů • Malý incident	D
Zanedbatelné	• Malé dopady	E

Doc 9859 na základě hodnot pravděpodobnosti a závažnosti rizika představuje matici rizik, která přehledně zobrazuje hodnotu celkového rizika a umožňuje tak stanovení přijatelnosti rizik. Tuto matici rizik zobrazuje Tabulka 4.

Tabulka 4: Matice rizik (přeloženo a upraveno autorem z [2])

Bezpečnostní riziko	**Závažnost**				
Pravděpodobnost	Katastrofické A	Nebezpečné B	Vážné C	Méně vážné D	Zanedbatelné E
Časté 5	5A	5B	5C	5D	5E
Občasné 4	4A	4B	4C	4D	4E
Vzdáleně pravděpodobné 3	3A	3B	3C	3D	3E
Nepravděpodobné 2	2A	2B	2C	2D	2E
Extrémně nepravděpodobné 1	1A	1B	1C	1D	1E

Matice rizik je využívána k hodnocení a posouzení přijatelnosti rizika. Barvy rozdělují rizika do třech základních kategorií podle jejich přijatelnosti. Zeleně zabarvená rizika jsou obecně brána jako přijatelná. Oranžová barva značí rizika, která jsou považována jako tolerovatelná, ale mohou vyžadovat nastavení nápravných opatření. Červená barva pak zobrazuje rizika, která vyžadují okamžitou akci ke snížení hodnoty rizika. Taková rizika jsou považována jako nepřijatelná. [2]

Proces snižování hodnoty rizika se nazývá zmírňování rizik. Jde o proces, jehož cílem je řízení bezpečnostních rizik a snížení jejich hodnot na přijatelnou úroveň. Ke zmírnění rizika může dojít řízením a snížením závažnosti nebo pravděpodobnosti rizika. V praxi je častěji využíváno snížení pravděpodobnosti, protože je mnohem jednodušší než snižování závažnosti rizika. Doc 9859 uvádí tři kategorie strategií pro zmírňování bezpečnostních rizik. [2]

1. **Vyhnutí se riziku**: Zrušení aktivity nebo operace, když výhody riziko převyšuje výhody dané operace.
2. **Redukce (snížení) rizika**: Snížení frekvence provozu nebo aktivit nebo přijetí opatření ke snížení rozsahu závažnosti rizik.
3. **Segregace (oddělení) rizik**: Izolace účinků důsledku rizika nebo zavedení redundance na ochranu před těmito důsledky.

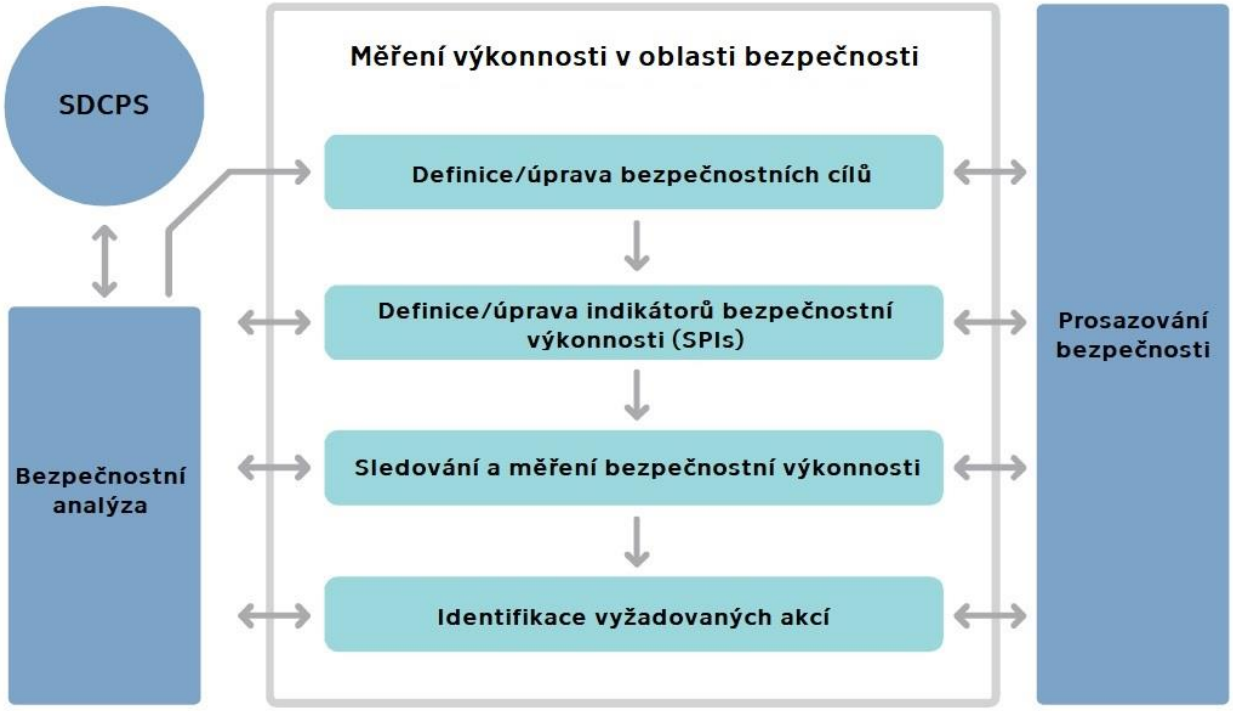
2.4. Indikátory bezpečnosti (SPIs)

Indikátory bezpečnosti (SPIs) jsou ukazatele, které organizaci ukazují, zda činnosti a procesy fungují efektivně pro dosažení bezpečnostních cílů. Pomocí indikátorů bezpečnosti se měří a sleduje výkonnost v oblasti bezpečnosti. ICAO Safety Management Manual (SMM) uvádí postup pro využití indikátorů bezpečnosti, jak je zobrazen na Obrázku 5. Zde je vidět také klíčová část procesu řízení výkonnosti v oblasti bezpečnosti, kterou je systém sběru a zpracování bezpečnostních dat (SDCPS). [2]

Indikátory bezpečnosti se dělí na dva typy – leading (proaktivní) a lagging (reaktivní). Rozdíl mezi nimi je především v tom, co ukazují. Leading indikátory jsou proaktivní a poukazují na budoucí změnu výkonnosti v oblasti bezpečnosti. Tyto indikátory je často velmi obtížné navrhnout, protože je málo způsobů, jak je měřit. Lagging indikátory jsou naopak reaktivní indikátory, které ukazují, jak se výkonnost v oblasti bezpečnosti změnila. Tyto indikátory jsou často snadno měřitelné, protože jsou založeny na již uplynulých událostech. [2]

Indikátory obecně by měly splňovat 4 základní předpoklady. Měly by být [2]:

a) související s bezpečnostním cílem, který chtějí uvést
b) vybrané nebo vyvinuté na základě dostupných údajů a spolehlivého měření
c) přiměřeně konkrétní a kvantifikovatelné
d) realistické s přihlédnutím k možnostem a omezením organizace



Obrázek 5: Měření výkonnosti v oblasti bezpečnosti [2]

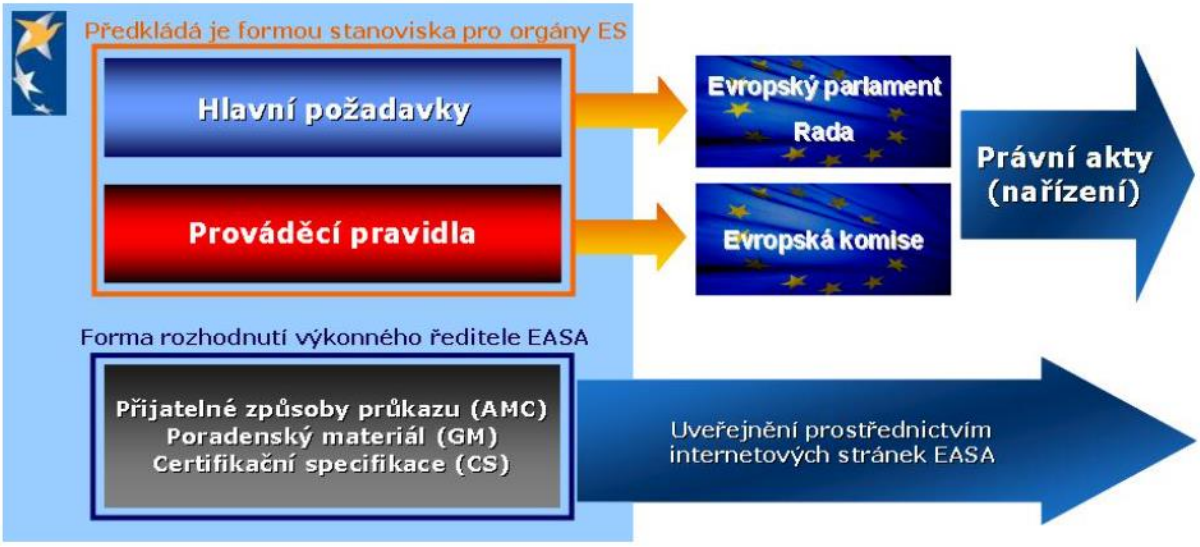
Pro využití indikátorů bezpečnosti k dosažení obecných bezpečnostních cílů organizace je nutné stanovit si také tzv. safety targets, což lze volně přeložit jako stanovené bezpečnostní cíle. Stanovené bezpečnostní cíle jsou hodnoty indikátorů bezpečnosti, které jsou pro organizaci přijatelné a kterých by indikátory bezpečnosti měly v nejlepším případě dosahovat. [2]

2.5. Legislativa

Bezpečnost letecké dopravy se v České republice řídí na základě několika legislativních dokumentů. Základním stavebním kamenem pro evropské a národní zákony členských států Mezinárodní organizací pro civilní letectví ICAO jsou dokumenty vydávané touto organizací, především pak Chicagská úmluva a její příslušné Annexy (Přílohy). Řízení provozní bezpečnosti letecké dopravy upravuje ICAO Annex 19. [5] [6]

ICAO Annex 19 je řazen do skupiny dokumentů pod zkratkou SARPs (Standards and Recommended Practices) – Standardy a doporučené postupy. Tyto dokumenty nejsou závazné zákony, nýbrž jsou základem pro tvorbu právně závazných dokumentů vydaných Evropskou unií (EU) a státními legislativními orgány. [6]

V Evropské unii je bezpečnost letecké dopravy řízena Agenturou Evropské unie pro bezpečnost v letectví (EASA). Tato agentura odpovídá za bezpečnost a ochranu životního prostředí v letecké dopravě. EASA sama o sobě nevydává závazné právní akty a není tak přímo regulačním úřadem pro státy Evropské unie. Evropská unie vydává závazné právní dokumenty prostřednictvím Evropského parlamentu, Rady EU a Evropské komise, jak je zobrazeno na Obrázku 6. EASA se nicméně významně podílí na tvorbě standardů a obsahu nařízení. [7] [8]



Obrázek 6: Proces vydávání právně závazných Nařízení pro členské státy EU [7]

V České republice (ČR) je letecké právo rovněž upravováno národními právními předpisy. Základním leteckým národním právním předpisem pro ČR je Zákon č. 49/1997 Sb., známý jako Zákon o civilním letectví. Tento zákon ustanovuje kromě jiného také vydání tzv. Leteckých předpisů řady L, které vydává Ministerstvo dopravy ČR. Návrhy znění

leteckých předpisů řady L pro Ministerstvo dopravy ČR připravuje Úřad pro civilní letectví (ÚCL) především na základě znění ICAO SARPs. [9] [10]

Znění národních leteckých předpisů se v některých ohledech může lišit oproti nařízením orgánů EU. Nařízení EU má však před národními předpisy aplikační přednost a jsou tedy Leteckým předpisům nadřazeny. [7]

3. Údržba letadel

Údržba letadel je v letectví nedílnou součástí procesů zachování letové způsobilosti. Procesy údržby jsou jasně nastavené technickou dokumentací, která je nezbytná pro zachování letové způsobilosti každého letadla. Tato kapitola pojednává především o údržbě a zachování letové způsobilosti složitých motorových letadel.

3.1. Organizace zachování letové způsobilosti (CAMO)

Technickou dokumentaci spravuje a udržuje příslušná Organizace pro zachování letové způsobilosti (CAMO). CAMO je v zemích Evropské unie schvalována příslušnými leteckými regulačními orgány. Organizace CAMO jsou schvalovány dle Part-CAMO Nařízení (EU) 1321/2014. Příloha CAMO tohoto nařízení udává požadavky kladené na organizace zachování letové způsobilosti. Organizace CAMO odpovídá za zajištění letové způsobilosti letadel po celou dobu své životnosti, a také za řízení programů údržby a kontrol letové způsobilosti, aby bylo zajištěno, že letadla jsou udržována při vysoké úrovni bezpečnosti a spolehlivosti. [11] [12]

Organizace CAMO je odpovědná za plánování a řízení údržby letadel, včetně dohledu nad činností údržby. Zajišťuje také, aby práce údržby byly prováděny kvalifikovaným personálem podle stanovených postupů. Organizace CAMO úzce spolupracuje s provozovateli letadel, organizacemi údržby a regulačními orgány, aby bylo zajištěno, že letadla jsou udržována a provozována bezpečně a efektivně. [11] [12]

Letečtí dopravci s osvědčením leteckého provozovatele (AOC) jsou povinni provozovat vlastní organizaci CAMO. Pro jiné typy provozu je možný outsourcing služeb CAMO. Každá CAMO organizace musí vydat a řídit vlastní Výklad organizace zachování letové způsobilosti (CAME), který obsahuje rozsah a omezení prací dané organizace. [11] [12]

3.2. Údržbová organizace (AMO)

Za fyzické provádění údržby letadel je odpovědná příslušná schválená údržbová organizace (AMO) s oprávněním podle Nařízení EK 1321/2014 – Part 145. Národní předpis, který v České republice upravuje pravidla letecké údržby a zachování letové způsobilosti jsou Letecký předpis L-6 a Letecký předpis L-8. Každá schválená údržbová organizace musí provádět údržbu dle schváleného programu údržby (AMP). Ten je definován pro transferová[1] letadla Nařízením Komise (EU) č. 1321/2014 (čl. M.A.302 nebo ML.A302) a pro annexová[2] letadla leteckými předpisy L-6 a L-8. [11]

Každá údržbová organizace musí zaměstnávat dostatečný počet kvalifikovaných techniků, kteří provádí údržbu letadel v souladu s příslušnými předpisy a standardy. Technici musí splňovat příslušné požadavky dle Part 66 Nařízení EK 1321/2014. [11]

Údržbová organizace musí mít k dispozici adekvátní vybavení a nářadí pro provádění údržby letadel. Organizace musí zavést také účinný systém řízení jakosti, který je schopen zajistit, že jsou veškeré úkony údržby prováděny v souladu s příslušnými předpisy a standardy. [11]

Důležitým aspektem údržby letadel je také dokumentace. Údržbová organizace musí udržovat přesnou a úplnou dokumentaci o všech prováděných úkonech údržby. Tato dokumentace musí být pravidelně revidována a uchovávána dle požadavků předpisu. [11] [12]

Vlastník letadla musí být schopen zajistit zachování letové způsobilosti daného letadla po celou dobu jeho životnosti. Dále je povinen zajistit potřebnou údržbu letadla prováděnou dle schváleného programu údržby. [11] [12]

[1] **Transferová letadla** = *„Letadla, jejichž typová osvědčení EASA vydala nebo uznala“* [15]

[2] **Annexová letadla** = *„Letadla, jejichž typová osvědčení **nebyla** převedena pod pravomoc EASA nebo letadla definovaná v Příloze (Annexu) I Nařízení Evropského parlamentu a Rady (EU) č. 2018/1139“* [15]

3.2.1. Rozdělení údržby podle rozsahu prací

Leteckou údržbu lze dělit několika způsoby. Základním rozdělením dle rozsahu prací se člení na dva, někdy tři druhy údržby [16]:

a) Traťová údržba – Line Maintenance (Lehká údržba)

b) Údržba na základně – Base Maintenance (Těžká údržba)

c) Dílenská údržba – Shop or Component Maintenance (Údržba komponentů)

Traťová údržba

Traťová údržba je taková údržba, která je provedena před letem s cílem zajistit provozuschopný stav letadla pro plánovaný let. Její provedení trvá v rozsahu jednoho až několika dní. Dle EASA Part 145, AMC 145.A.10 je traťová údržba taková, která zahrnuje následující úkony [12]:

- Řešení problémů (Trouble shooting)
- Odstranění závady
- Výměna součástí s použitím externího testovacího zařízení
- Údržba, která odhalí jasné nevyhovující stavy/nesrovnalosti/poruchy, ale nevyžaduje rozsáhlou hloubkovou kontrolu
- Opravy, úpravy a další úkony údržby, které nevyžadují rozsáhlou demontáž a lze je provést jednoduchými prostředky

Údržba na základně

Údržba na základně je nejrozsáhlejším druhem údržby, při kterém je provedena komplexní kontrola potřebných částí a systému letadla. Během údržby na základně je letadlo často rozebráno na jednotlivé díly. Provedení údržby na základně je časově náročný úkol, který trvá v rozmezí od několika dnů po několik měsíců podle rozsahu plánovaných prací. [16]

Dílenská údržba

Dílenská údržba je údržba, která neprobíhá přímo na letadle, ale probíhá v příslušné dílně. Komponenty, které jsou z letadla demontovány, jsou opravovány v příslušné dílně, která je pro daný typ opravy určena. Pokud má údržbová organizace dostupné dílny, je dílenská údržba zahrnuta v rámci údržby na základně. V opačném případě se pak demontované letadlové celky zasílají do opravy externě. [16]

Každá údržbová organizace schválená dle Part-145 Nařízení 1321/2014 by měla mít ve svém schváleném Výkladu organizace (MOE) definované rozsahy prací, které spadají pod traťovou údržbu a údržbu na základně. Obecnou hranici mezi lehkou a těžkou údržbou nelze přesně určit, proto je tato hranice určena dle MOE dané údržbové organizace. [12]

3.3. Legislativní požadavky na SMS v údržbových organizacích

Požadavek na zavedení systému řízení provozní bezpečnosti (SMS) uvádí ICAO Annex 19. Ten udává povinnost zavedení SMS pro letecké provozovatele komerční dopravy, schválené výcvikové organizace, projekční organizace, výrobní organizace, letiště a v neposlední řadě také pro schválené údržbové organizace. Tato povinnost ale není právně vymahatelná, protože ICAO Annexy obsahují pouze tzv. Standardy a doporučené postupy (SARPs). [1] [6]

Na základě ICAO Annex 19 vznikl v České republice národní předpis – Letecký předpis L-19. Tento předpis udává povinnost zavedení SMS stejným způsobem jako ICAO Annex 19 s tím rozdílem, že se již jedná o právně vymahatelný dokument. [1] [4] [6]

Schválené údržbové organizace (AMO) se řídí Nařízením (EU) 1321/2014. Požadavky na údržbové organizace, které musí být splněny pro vydání či zachování oprávnění k údržbě letadel a letadlových celků jsou uvedeny v Části 145 (Part-145) tohoto nařízení. Nařízení 1321/2014 ale neudává povinnost zavedení SMS v AMO. [11]

Evropská legislativa má před legislativou národní aplikační přednost. Z toho důvodu není pro schválené údržbové organizace zavedena dle Nařízení (EU) 1321/2014 povinnost SMS. [7]

3.3.1. Prováděcí nařízení Komise (EU) 2021/1963

Evropská Komise přijala v listopadu 2021 Prováděcí Nařízení Komise (EU) 2021/1963, které mění Nařízení (EU) 1321/2014 v souvislosti se systémy řízení provozní bezpečnosti v údržbových organizacích. [17]

Prováděcí Nařízení Komise (EU) 2021/1963 udává, kromě jiného, povinnost zavedení systému řízení pro údržbové organizace schválené podle Part 145. Zavádí také povinnost zřízení systému hlášení událostí. [17]

Prováděcí Nařízení Komise (EU) 2021/1963 přidává, kromě jiného, do Nařízení (EU) 1321/2014 článek 145.A.200. Ten udává, že údržbová organizace schválená podle Part-145 **musí** zavést systém řízení, který obsahuje identifikaci nebezpečí a hodnocení příslušných rizik včetně přijímání nápravných opatření pro zmírňování rizik a ověřování účinnosti těchto opatření. Na základě Prováděcího Nařízení 2021/1963 jsou tedy údržbové organizace povinny zavést komponenty, které odpovídají komponentům systému provozní bezpečnosti (SMS). To prakticky znamená povinnost implementace SMS do údržbových organizací schválených podle Part-145. [17]

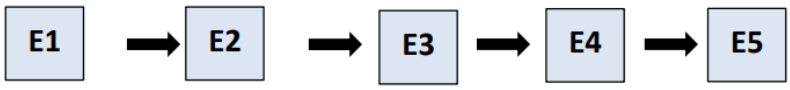
Organizace, které již oprávnění k údržbě letadel dle Part 145 získaly před 2. prosincem 2022 jsou povinné zavést požadavky tohoto prováděcího nařízení nejpozději do 2. prosince 2024. Pokud tak neučiní, bude jejich dosavadní oprávnění dočasně nebo trvale zrušeno. Údržbové organizace, které žádají získání oprávnění dle Part 145 po 2. prosinci 2022, musí již implementovat veškeré požadavky Prováděcího Nařízení Komise (EU) 2021/1963. V opačném případě jim nebude oprávnění vydané. [17]

4. Limitace současného stavu

Jak již bylo zmíněno, systém řízení provozní bezpečnosti (SMS) v údržbových organizacích je legislativně popsán v ICAO Annexu 19, Leteckém předpisu L-19, Nařízení (EU) 1321/2014 a nově také v Prováděcím nařízení Komise (EU) 2021/1963. Všechny tyto zmíněné dokumenty obsahují podmínky, které musí údržbová organizace splnit pro zavedení SMS. Žádný z nich však neudává praktický návod či podporu k tomu, jak takový SMS zavádět a následně udržovat.

V současnosti probíhá zavádění systémů řízení provozní bezpečnosti (SMS) schválených údržbových organizací (AMO). Organizace AMO, které jsou již držiteli oprávnění dle Part-145 musí zavést SMS do 2. prosince 2024. Jedním z hlavních poradních materiálů, které údržbové organizace mají pro zavedení SMS k dispozici, je Doc 9859, tzv. Safety Management Manual (SMM). V současné době je nejaktuálnější jeho čtvrté vydání. Tento dokument podrobně popisuje smysl SMS a udává praktické návody a doporučení, které mohou být využívány organizacemi pro zavedení a udržování SMS. [2]

SMM nabízí ukázku využití některých tradičních bezpečnostních metod a modelů jako jsou SHELL či Reasonův model. Tento pohled na bezpečnost je vesměs lineárního charakteru, jak zobrazuje Obrázek 7. To znamená, že vnímá vznik nehod jako lineární řetězec událostí, které následně vedou k nehodě. Tato lineární kauzalita však ne vždy správně popisuje reálný sousled událostí, protože se nezaměřuje na celý systém, ale pouze na jeho konkrétní části. [2] [18]

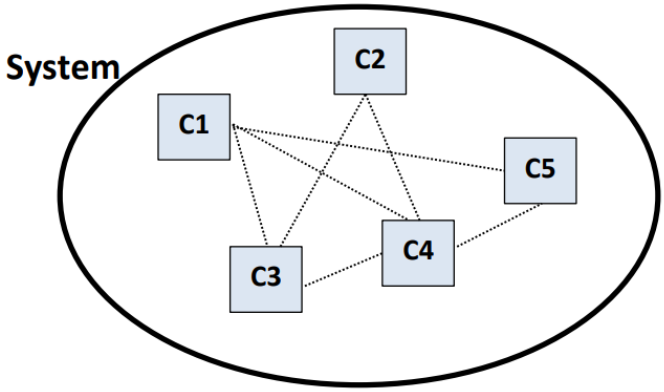


Obrázek 7: Řetězec událostí [19]

Údržbové organizace jsou komplexní socio-technické systémy. Tyto systémy jsou složeny z velkého množství komponent, které spolu navzájem interagují. Problémem lineární kauzality a celkově lineárního pohledu na bezpečnost v údržbových organizacích je, že tento přístup nedokáže dostatečně popsat veškeré interakce mezi komponenty

komplexních systémů. Komplexní systémy se neustále mění a jsou velmi dynamické. Lineární pohled na bezpečnost má své využití při zkoumání velmi omezené části těchto systémů. Pro popis komplexních socio-technických systémů, jakým je údržbová organizace, je lineární kauzalita nedostatečná a je třeba na ně pohlížet systémově.

Při pohledu na bezpečnost systémově lze vidět reálné fungování systému. Při využití systémového přístupu k bezpečnosti lze pochopit, proč dochází k nehodám, přestože části systému fungují tak jak byly navrženy. Nehody mohou vycházet z interakcí částí systému, což tradiční metody a modely, které popisuje například právě SMM, nedokážou zachytit. Komponenty komplexních systémů spolu interagují provázaně jak zobrazuje Obrázek 8. [19] [20]



Obrázek 8: Interakce komponentů systému [19]

Tato práce se zabývá postupy a technickými nástroji vybraných částí SMS konkrétní údržbové organizace. Výběr částí SMS a jejich současné limitace v konkrétní údržbové organizaci budou dále popsány.

4.1. Seznam dostupné literatury

Problematice systémového přístupu k bezpečnosti se věnuje publikace *Engineering a safer world: systems thinking applied to safety* od prof. Nancy G. Leveson. V této publikaci je vysvětlován rozdíl mezi standardním lineárním přístupem bezpečnostního inženýrství a systémovým přístupem k bezpečnosti na základě systémové teorie. [18]

Eurocontrol popisuje systémový přístup k bezpečnosti v publikaci *Systems Thinking for Safety: Ten Principles*, která přehledně popisuje jeho základní principy. Publikace vychází z výše zmiňované publikace od prof. Leveson a také z několika publikací prof. Hollnagela, který se zabývá systémovým přístupem k bezpečnosti. [20]

Profesor Erik Hollnagel vydal několik publikací s tématikou systémového přístupu k bezpečnosti. Za zmínku stojí publikace *Safety-I and Safety-II. The past and future of safety management,* kde zavádí tzv. Safety-II. Systémovou analýzu funkční rezonance (FRAM) založenou na Safety-II představuje prof. Hollnagel v publikaci *FRAM: Functional resonance analysis method*. [21] [23]

Na základě systémové teorie a systémového modelu STAMP popsaných v publikaci *Engineering a safer world*, je založena proaktivní analytická systémová metoda zvaná System-Theoretic Process Analysis (STPA). Ta je velmi podrobně popsána v publikaci *STPA Handbook* od prof Nancy G. Leveson a John. P. Thomas. [18] [19]

Součástí systému řízení provozní bezpečnosti (SMS) je analýza a řízení rizik. Publikace z amerického MIT s názvem *A System-Theoretic Approach to Risk Analysis* představuje analýzu rizik založenou na systémové metodě STPA. Autory práce jsou Dro J. Gregorian a Sam M. Yoo. Tato publikace přináší nové postupy pro hodnocení rizik založené na systémovém přístupu k bezpečnosti. [25]

5. Systém řízení provozní bezpečnosti konkrétní údržbové organizace

Tato práce si klade za cíl stanovit postup a technické nástroje pro vývoj vybraných částí systému řízení provozní bezpečnosti (SMS) letecké údržbové organizace směrem k systémovému přístupu k bezpečnosti.

Údržbové organizace obecně využívají pro řízení provozní bezpečnosti různé systémy, které jsou odlišné na základě velikosti organizace, rozsahu prací, struktury organizace a spousty dalších aspektů. Systémy řízení provozní bezpečnosti v údržbových organizacích by měly být vyvinuty pro potřeby dané konkrétní organizace. Proto se tato práce nevěnuje SMS v údržbových organizacích pouze v obecné rovině, ale zajímá se o konkrétní údržbovou organizaci schválenou dle Part-145 Nařízení (EU) 1321/2014 (dále jen „Údržbová organizace“).

Jako první krok je nutné analyzovat současný stav SMS v Údržbové organizaci a pochopit současný systém, který je v organizaci využíván.

5.1. Analýza současného stavu SMS Údržbové organizace

Aby bylo možné analyzovat SMS Údržbové organizace, je nutné pochopit jeho podstatu, procesy a systémy, které jsou v Údržbové organizaci využívány. V této části bylo zapotřebí absolvovat několik schůzek s vedením oddělení provozní bezpečnosti (OPB), které zde zavádí, řídí a spravuje SMS. Pro účely práce byl také umožněn náhled do interní dokumentace společnosti.

Údržbová organizace využívá již několik let zavedený systém řízení bezpečnosti. Tento systém je vytvořen a udržován OPB. Údržbová organizace je součástí společnosti, její pracovní aktivity se zaměřují na vícero oblastí letectví. Daná společnost je kromě schválené údržbové organizace (AMO) také organizace pro zachování letové způsobilosti (CAMO), letecký provozovatel a provozuje také handlingové služby. Současný SMS v této společnosti je vedený jako společný systém pro veškeré oblasti působnosti.

Důležitou součástí systému řízení v Údržbové organizaci a celkově v dané společnosti je interně navržený software, který umožňuje správu dat týkajících se bezpečnosti. Tento software je spravován jak OPB, tak i příslušnými vedoucími jednotlivých oddělení společnosti.

K analýze současného stavu bylo přistupováno systémově. Prvním krokem bylo samotné seznámení se současným stavem SMS. K tomu byla využita veškerá interní dokumentace Údržbové organizace. Dále proběhlo několik schůzek s vedoucím oddělení provozní bezpečnosti, který poskytl veškeré doplňující informace o systému celkově i o jeho jednotlivých částech. Pro analýzu současného stavu SMS bylo absolvováno také školení SMS obdobné tomu, kterého se účastní všichni zaměstnanci společnosti.

Aby došlo k hlubšímu poznání a chápání SMS, bylo nutné porozumět jeho podstatě nejen z pohledu vedení společnosti, ale také z pohledu samotných zaměstnanců Údržbové organizace. Na základě dotazů a osobní komunikace s vedoucím oddělení Údržby na základně a jeho personálem došlo k poznání praktického využití všech částí SMS. K další podrobné analýze procesů SMS pomohla účast na schůzce zástupců technického úseku a oddělení provozní bezpečnosti, která se týkala samotného procesu identifikace nebezpečí a hodnocení rizik. Díky tomu bylo možné tento proces vidět a analyzovat naživo.

Jedním z identifikovaných nedostatků současného SMS bylo jeho vnímání zaměstnanci organizace. I když jsou si zaměstnanci vědomi důležitosti zajištění bezpečnosti v letectví, mají pochybnosti o některých přínosech SMS. Jedním z často opakovaných důvodů byla složitost a časová náročnost procesů SMS, které vyžadují jejich účast. Zaměstnanci často nepovažovali SMS za něco, co by přinášelo společnosti hodnotu a mělo významný praktický dopad na bezpečnost.

Po analýze současného stavu SMS bylo zvoleno několik jeho částí, které v kontextu celého systému nebyly vyhodnoceny jako přínosné či účinné. Jejich přínos v rámci SMS se ukázal být malý ve srovnání s potenciálem využití v celé organizaci. Orientace v těchto částech z pohledu zaměstnanců se také ukázala jako snížená a zaměstnanci tyto části SMS a s nimi spojené postupy považovali za složité a časově náročné. Některé části pak také nenacházely

praktické využití vůbec nebo minimálně. Tyto části byly zavedeny do stávajícího SMS na základě legislativních požadavků a doporučení, ale jejich praktická využitelnost v systému byla nízká vzhledem k jejich současnému stavu. Registr nebezpečí byl jednou z takových částí. Všechny části SMS, které byly vybrány pro vývoj budou podrobněji rozebrány v kapitolách níže.

5.2. Řízení bezpečnostního rizika v Údržbové organizaci

Údržbová organizace využívá interní softwarový nástroj pro zpracování záznamů a hlášení. Tato databáze umožňuje vkládání, sběr a uchovávání dat. Tento nástroj také umožňuje vkládat identifikovaná nebezpečí, přiřazovat k nim rizika a ta následně ohodnocovat. Postup vkládání a správy dat do databáze popisuje diagram na Obrázku 9.

Šetření události, analýza kořenových příčin, identifikace nebezpečí a ohodnocování rizik má v Údržbové organizaci v kompetenci příslušný odpovědný manažer oddělení (Responsible Manager – RM), kterého k danému záznamu přiřadí manažer provozní bezpečnosti (VPB). VPB dohlíží na správnost šetření a poskytuje jednotlivým odpovědným manažerům (RM) odbornou pomoc.

5.2.1. Hlášení událostí (Reporting)

Správně fungující systém hlášení je klíčovým prvkem systému řízení provozní bezpečnosti (SMS). Systém hlášení umožňuje sběr důležitých dat o bezpečnosti letecké společnosti či organizace. Hlášení se obecně dělí na povinné a dobrovolné podle Nařízení Evropského parlamentu a Rady (EU) č. 376/2014. Toto nařízení udává povinnost zavádět systémy hlášení a udává také podmínky, které musí systémy splňovat. Každý z těchto typů hlášení přináší odlišné druhy dat. Povinné hlášení je dané legislativou a musí být provedeno v případě, že nastane incident nebo nehoda. Koncovým příjemcem povinného hlášení je příslušný úřad. Dobrovolné hlášení naopak upozorňuje na nesrovnalosti nebo nebezpečí, která ještě v incident nebo nehodu nevyústili. [2] [26]

Hlášení událostí probíhá v Údržbové organizaci několika možnými způsoby. Využívané systémy hlášení se dělí na interní a externí.

Údržbová organizace využívá systém interního hlášení pomocí předepsaného formuláře či pouze pomocí e-mailové zprávy. Hlášení v rámci interního systému hlášení je děleno na povinné a dobrovolné. Interní dobrovolné hlášení obsahuje:

- Otevřené hlášení – hlásící osoba je uvedena v reportu
- Tajné hlášení – hlásící osoba požádala o utajení identity
- Anonymní hlášení – hlásící osoba není známa

Druhým typem hlášení je hlášení pomocí externího systému. V rámci tohoto hlášení je report zaslán externím entitám jako jsou například úřady, jiný provozovatel, výrobce, aj.

5.2.2. Identifikace nebezpečí a ohodnocování rizik

Současný postup identifikace nebezpečí a ohodnocování rizik v Údržbové organizaci je rozdělen do třech základních kroků.

1. Identifikace nebezpečí

Prvním krokem je samotná identifikace nebezpečí. Jedná se o vnitřní proces odpovědného vedoucího, jehož výstupem je definice jednoho nebo více nebezpečí. Tato nebezpečí jsou definována na základě na základě sesbíraných informací během fáze šetření události, kterou odpovědný vedoucí prochází. Z těchto informací RM vyhodnotí a definuje nebezpečí, která považuje v daném případě za relevantní.

2. Stanovení důsledků

Ve druhém kroku stanovuje odpovědný vedoucí důsledky ke každému nebezpečí, které bylo identifikováno v prvním kroku. Těmito důsledky jsou události či ztráty, ke kterým dané nebezpečí může vést za určitých podmínek. Údržbová organizace zavádí ve svém interním softwaru kolonku s názvem „Risk (Consequence)“, do které se tyto důsledky vypisují. Označení „Risk“ neodkazuje na hodnotou rizika. Ta se uvádí v následujících sloupcích s označením „Assessment“, kam jsou zadávány hodnoty závažnosti a pravděpodobnosti.

3. Ohodnocování rizika

V tomto kroku odpovědný vedoucí ohodnocuje dané důsledky dvěma základními hodnotami – pravděpodobnosti a závažnosti. Údržbová organizace v tomto kroku využívá hodnot v rozmezí 1-5 pro pravděpodobnost i pro závažnost. Hodnocení rizika je v tomto případě založeno na tabulkách uvedených v Doc 9859 Safety Management Manual. Hodnota závažnosti je určována v závislosti na fyzických/hmotných ztrátách v kombinaci s finančním dopadem, který by dané riziko přineslo společnosti. Celková hodnota rizika je následně získaná součinem hodnot pravděpodobnosti a závažnosti.

Jakmile je proces identifikace nebezpečí a ohodnocování rizik dokončen, jsou stanovena nápravná opatření odpovědným vedoucím. Vedoucí provozní bezpečnosti (VPB) následně provede předběžnou kontrolu a revizi navržených nápravných opatření a celého záznamu. Následně stanoví datum kontroly účinnosti nápravných opatření. Po uzavření záznamu VPB jsou identifikovaná nebezpečí a rizika automaticky propsána do tabulky Registru nebezpečí.

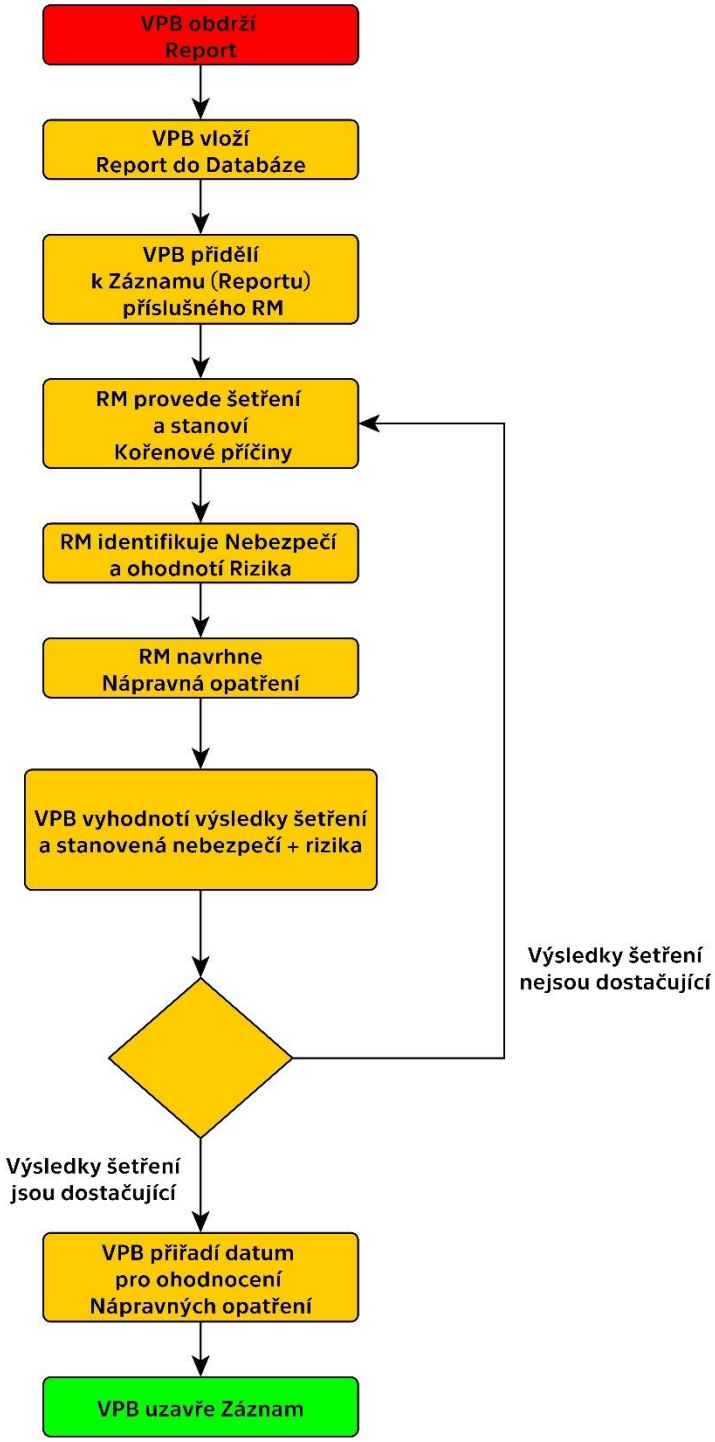
5.2.3. Registr nebezpečí

Registr nebezpečí je součástí nástrojů pro sledování a řízení rizik. Údržbová organizace využívá registr rizik ve formě excelové tabulky. Tato tabulka obsahuje seznam identifikovaných nebezpečí, jejich možné důsledky a číselnou hodnotu rizika rozdělenou na složky pravděpodobnosti a závažnosti. Současné rozdělení tabulky registru nebezpečí v Údržbové organizaci zobrazuje Tabulka 5.

Tabulka 5: Tabulka registru nebezpečí v Údržbové organizaci

ID	Nebezpečí	Riziko (Důsledek)	P 1	Z 1	Riziko 1	P 2	Z 2	Riziko 2
1	Nebezpečí 1	Důsledek 1	2	3	**6**	1	3	**3**
		Důsledek 2	5	4	**20**	2	2	**4**
	Nebezpečí 2	Důsledek 1	3	5	**15**	2	3	**6**
		Důsledek 2	5	1	**5**	2	1	**2**

Hodnota Riziko 1 ukazuje celkovou hodnotu rizika před zavedením nápravných opatření a Riziko 2 je hodnota rizika po zavedení nápravného opatření.



Obrázek 9: Postup vkládání dat do interního softwaru (Databáze) (Vedoucí provozní bezpečnosti (VPB), Responsible Manager (RM)) (vytvořeno autorem na základě procesů Údržbové organizace)

5.3. Zajištění bezpečného provozu

Zajištění bezpečného provozu je v Údržbové organizaci odpovědný manažer příslušného oddělení. Tento manažer zodpovídá jak za provoz oddělení, tak i za bezpečnost a řešení nehod a incidentů. Odpovědný manažer (RM) provádí šetření událostí i analýzu kořenových příčin. Identifikuje také nebezpečí a hodnotí rizika. V neposlední řadě pak RM navrhuje nápravná opatření ke zmírnění rizik. Tato opatření pak zavádí do praxe.

5.3.1. Indikátory bezpečnosti (SPIs)

Indikátory bezpečnosti slouží vedení společnosti ke sledování stavu bezpečnosti v organizaci a měly by být dále využívány pro rozhodování o dalším směřování v oblasti bezpečnosti.

V Údržbové organizaci probíhá identifikace, návrh a případná úprava SPIs v nepravidelných intervalech. Samotný proces návrhu SPIs probíhá převážně expertně. Identifikaci SPIs zajišťuje Rada bezpečnosti, která je složena z oddělení OPB a představitelů nejvyššího vedení společnosti. Tato rada pak v případě potřeby upravuje SPIs a navrhuje nové. Proces pro identifikaci SPIs není nijak stanoven ani zakotven v dokumentaci společnosti. Současné indikátory bezpečnosti jsou ve společnosti několik let nezměněné. Jejich aktualizace neprobíhá na pravidelné bázi.

Hodnoty nastavených indikátorů bezpečnosti se zaznamenávají do interní softwarové databáze. Odpovědnost za udržování záznamů má oddělení provozní bezpečnosti. Indikátory jsou zobrazovány pomocí grafů, které ukazují jejich postupný vývoj v čase. Grafické znázornění také umožňuje přehledně sledovat dosažení nastavených bezpečnostních cílů a výkonost v bezpečnosti.

5.4. Výběr částí SMS Údržbové organizace

Diskuse s oddělením provozní bezpečosti umožnila prvotně identifikovat části současného SMS v Údržbové organizaci, které mají potenciál pro další vývoj. Pro ověření nezaujatosti a hlubšího využití v praxi byla následně daná problematika konzultována s vedoucím

manažerem Údržbové organizace. Ten potvrdil potenciál a možný přínos, který by pro chod organizace a její SMS měl další vývoj jeho vybraných částí.

Na základě získaných podkladů, dokumentace a na základě analýzy současného SMS v Údržbové organizaci byly vybrány následující části SMS, jejichž další vývoj může být pro Údržbovou organizaci nejvíce přínosný. Tyto části byly doplněny do myšlenkové mapy, která je uvedena v Příloze 1. Zeleně označené buňky zde ukazují, které části byly vybrány pro vývoj v této práci. Jsou jimi:

- **Procesy hodnocení a řízení rizik**
- **Registr nebezpečí**
- **Indikátory bezpečnosti (SPIs)**

Tato práce se zabývá právě těmito částmi SMS, protože tyto části SMS byly identifikovány v rámci analýzy jakožto části, jejichž vývoj bude mít pro Údržbovou organizaci největší přínos. V návaznosti na tuto práci je dále možné rozvíjet další části SMS, které jsou uvedeny v Příloze 1.

5.5. Limitace současného stavu SMS v Údržbové organizaci

Analýza současného stavu SMS v Údržbové organizaci odhalila některá místa, jejichž další vývoj by přispěl k vylepšení současného systému. Současný SMS je pravidelně udržován, nicméně byl zaveden před více než 10 lety, kdy tehdejší poznání řízení letecké bezpečnosti bylo v raném stádiu. Během analýzy současného stavu SMS byly u vybraných částí zjištěny následující limitace.

5.5.1. Limitace současného stavu procesu hodnocení a řízení rizik v Údržbové organizaci

Současný proces hodnocení a řízení rizik v Údržbové organizaci byl popsán v kapitole Řízení bezpečnostního rizika v Údržbové organizaci. Proces hodnocení rizika odpovídá návrhu, který je uveden v ICAO Safety Management Manual.

Celkové riziko je počítáno na základě součinu hodnot pravděpodobnosti a závažnosti. Přijatelnost celkového rizika se pak určuje na základě ICAO matice rizik. V rámci analýzy SMS v Údržbové organizaci bylo identifikováno, že proces hodnocení rizik, a především přiřazení hodnot pravděpodobnosti, je obtížný pro odpovědné manažery, kteří hodnocení provádí. Hodnota pravděpodobnosti rizika by měla ukázat, jak moc je pravděpodobné, že při zachování stávajícího provozu dojde k nehodě či incidentu. Při hodnocení pravděpodobnosti mají manažeři k dispozici dostupnou tabulku (Tabulka 6), podle které se mohou orientovat při hodnocení.

Jak je vidět ve sloupci „Vysvětlení", pravděpodobnost je zde chápána retrospektivně. Odkaz na minulost navádí odpovědné manažery k tomu, aby hodnotu přiřadili na základě minulé zkušenosti. Hodnota pravděpodobnosti by však měla být spíše odhadem budoucí pravděpodobnosti [2], což splňuje pouze jeden (nejnižší) stupeň. Hodnoty spodního a horního limitu časového období také odkazuje na retrospektivní pohled.

Tabulka 6: Tabulka hodnocení pravděpodobnosti v Údržbové organizaci

Klasifikace		Spodní limit	Horní limit	Vysvětlení
5	Časté		1x za měsíc	• Nastane 1x za 100 letů • Nastává často v organizaci
4	Příležitostné	1x za měsíc	4x za měsíc	• Nastane 1x za 300 letů • Nastává občas v organizaci
3	Střední	4x za měsíc	1x za 2 měsíce	• Nastane 1x za 2 000 letů • Nastává zřídka v organizaci
2	Nepravděpodobné	1x za 2 měsíce	1x za 8 měsíců	• Nastane 1x za 10 000 letů • V historii nastalo v organizaci
1	Extrémně nepravděpodobné	1x za 8 měsíců		• Téměř nepředstavitelné, že by událost mohla nastat

Pro člověka, který určuje hodnotu pravděpodobnosti je velmi obtížné odhadnout tuto hodnotu. Hodnotitel může jen stěží předpovídat, jak často daná událost může nastat. Využívané materiály a data k odhadu pravděpodobnosti jsou pouze retrospektivní

s odkazem na události, které již nastaly. Jejich využití je omezené na detailně poznané události, které v organizaci nastávají s určitou pravidelností. Pro nehody a incidenty, které se v organizaci zatím nevyskytly či pouze zřídka, nemá hodnotitel data, která by mohl využít.

Součástí procesu řízení rizik je také identifikace nebezpečí. Ta je opět odpovědností příslušného manažera (RM) přiřazeného vedoucím provozní bezpečnosti (OPB). Pro záznam identifikovaných nebezpečí se využívá interní software společnosti. Nebezpečí se zaznamenávají do otevřeného pole, které není nijak omezené. V rámci každého záznamu jsou nebezpečí identifikována vždy nově od začátku a příslušný manažer tak nemá znalost, zda nebezpečí již nebylo v minulosti identifikováno a jaká rizika k němu byla přiřazena.

5.5.2. Limitace současného stavu registru nebezpečí v Údržbové organizaci

Registr nebezpečí je v Údržbové organizaci udržován ve formě excelové tabulky. Forma a rozdělení je zobrazena v Tabulce 5 v kapitole Registr nebezpečí.

Prvním problémem současného registru nebezpečí je jeho nepřehlednost a duplicita záznamů. Každý záznam řešený v interním softwaru, na který je kladen požadavek identifikace nebezpečí, má v registru nebezpečí vlastní pole/řádek. V současném registru nebezpečí je tedy možné zaznamenat stejné nebezpečí vícekrát. Duplicita záznamů vede k dlouhým seznamům nebezpečí, které se mohou, ale také nemusejí lišit v jejich významu.

Jelikož příslušný odpovědný vedoucí identifikuje nebezpečí vždy pro každý záznam nově do otevřeného pole, může být znění nebezpečí formulováno různými způsoby. Pro nebezpečí, která jsou stejného charakteru, je v takovém případě v registru několik formulací. Formulace nebezpečí odpovědného vedoucího se vztahuje ke konkrétnímu řešenému problému či události. Dané nebezpečí však může být relevantní pro celý systém, nikoliv jen pro jeho sledovanou část.

Výše zmíněné problémy vedou k nepřehlednosti registru, který v současném stavu obsahuje více než tisíc záznamů. Každý z nich obsahuje vždy minimálně jedno identifikované nebezpečí. Registr nebezpečí se udržuje napříč celou společností, která má velký rozsah působnosti. K různým událostem a záznamům může být přiřazen jiný

odpovědný vedoucí (RM), který následně identifikuje nebezpečí a důsledky a ohodnocuje rizika. Záznamy nejsou v registru nijak rozlišeny podle oddělení, kterých se týkají.

5.5.3. Limitace současného stavu indikátorů bezpečnosti

V současném stavu je v Údržbové organizaci zavedeno sledování pěti indikátorů bezpečnosti (SPIs). Indikátory jsou z většiny typu Lagging, tedy reaktivní.

Hlavní limitací současných SPIs je proces jejich návrhu. Indikátory jsou v Údržbové organizaci zaváděny expertně. To znamená, že pro jejich zavedení není využívána žádná metoda ani postup. Lze tedy jen těžko ověřit, zda indikátory sledují výkonnost v oblasti bezpečnosti celého systému nebo jen jeho části.

Proces zavádění a revize SPIs je založen primárně na zkušenostech z provozu, což do jisté míry odráží současné bezpečnostní problémy a potřeby organizace. Návrhy SPIs založené na jen minulé zkušenosti však nejsou zárukou toho, že pokrývají celý systém a odráží celkovou výkonnost v oblasti bezpečnosti. Při dosažení hodnot stanovených bezpečnostními cíli (safety targets) pak vzniká dojem, že výkonnost v oblasti bezpečnosti je na přijatelné úrovni, i když je sledována jen část systému.

Zavedení postupu pro návrh SPIs, které sledují celý systém přinese relevantní data o výkonnosti v oblasti bezpečnosti celého systému.

6. Systémový přístup k bezpečnosti

Vývoj letectví v posledních dekádách vede ke komplexnějším systémům a stále větší automatizaci. Zaměřit se separátně na jednotlivé složky těchto složitých a komplexních systémů není pro dnešní systémy dostatečné. Potřeba komplexnějšího pohledu na bezpečnost vyústila ve vývoj systémových modelů a metod. Tyto metody a modely pohlíží na systém jako celek, nikoliv jako na soubor prvků. [19] [21]

Za hlavní moderní směry, které jsou brány jako systémové, se považují Safety-II a Safety-III. Prvním, kdo touto formou označil systémový přístup byl prof. Erik Hollnagel. Ten ve své knize Safety-I and Safety-II: The Past and Future of Safety Management popisuje nedostatky stávajícího či minulého přístupu k bezpečnosti v moderní době. Tento bezpečnostní přístup označuje jako Safety-I. Jako Safety-II pak označil nový, systémový přístup k bezpečnosti, který nepohlíží na složky systému zvlášť, ale hledí na systém jako celek. V rámci Safety-II byla vyvinuta metoda funkční rezonanční analýzy (FRAM). [21]

Druhým systémovým směrem je tzv. Safety-III. Ten vychází ze systémové teorie. Tento systémový přístup popsala prof. Nancy G. Leveson ve své publikaci Engineering a Safer World. Na základě systémové teorie pak byl vyvinut bezpečnostní model Systems-Theoretic Accident Model and Processes (STAMP). Tento bezpečnostní model doplňuje lineární sekvenční model (Obrázek 6) o další prvky, a především vztahy mezi nimi. Zobrazuje tak systémy komplexně. Název Safety-III byl použit v publikaci Nancy G. Leveson, kde popisuje rozdíly mezi Safety-II a Safety-III. [19] [21] [22]

6.1. The Functional Resonance Analysis Method (FRAM)

FRAM (Functional Resonance Analysis Method) je analytická bezpečnostní metoda, která vychází z teorie Safety-II. FRAM je metoda využívající tzv. funkční rezonanci systému, což znamená kombinování (sčítání a odčítání) variabilit různých funkcí daného systému. Variabilita funkcí systému nebo systému je chápana jako rozdíl výkonnosti. Systémy jsou navrhovány na konstantní výkonnost. V praxi však tato výkonnost kolísá a není téměř nikdy konstantní. [23]

FRAM je založen na čtyřech základních principech [23]:

- Úspěchy a selhání jsou srovnatelné
- Výkonnost sociotechnických systémů je variabilní
- Princip emergence systému
- Princip rezonance

Princip emergence vysvětluje vlastnosti systému, který má daný systém pouze pokud obsahuje veškeré potřebné prvky. Jakmile je systém rozložen na jednotlivé části a ty jsou pak zkoumány parciálně, není možné vidět veškeré vlastnosti systému, které má jako celek.

Postup pro aplikování FRAM má základní 4 kroky.

1) Identifikace a popis funkcí systému

V tomto kroku jsou funkce vnímány jako aktivity, které jsou v systému vykonávány. Pro každou funkci existuje vstup (input), který tuto funkci spustí a dodá ji potřebné informace pro její výkon. Každá taková funkce pak funguje jako vstup pro další navazující funkci.

2) Identifikace variability výkonnosti

Jednotlivé funkce (aktivity) nemají pokaždé stejnou výkonnost. Ta se liší na základě vnějších či vnitřních vlivů a na ty také odlišně reaguje. Variabilita je v podstatě rozmanitost výkonnosti systému, která může být jak negativní, tak i pozitivní. Je nutné určit si hranice, kdy je variabilita stále v přijatelné normě, a kdy už je potřeba ji řešit. V analýze FRAM je měřena variabilita funkcí jako variabilita jejich výstupů (output).

3) Stanovení kombinací variabilit

Tento krok analýzy FRAM zhodnocuje variability funkcí a analyzuje, jakým způsobem se spolu jednotlivé variability kombinují a zda dochází k jejich žádoucím či nežádoucím rezonancím.

4) Návrh opatření proti nežádoucím rezonancím

Na funkce systému, jejichž výstupy vykazují vysokou variabilitu, je vhodné navrhnout opatření, která zabrání či sníží variabilitu funkce nebo zamezí nežádoucím rezonancím, tedy kombinacím s variabilitami dalších funkcí. [23] [24]

6.2. Systems-Theoretic Accident Model and Processes (STAMP)

STAMP (System-Theoretic Accident Model and Process) je bezpečnostní model založený na systémové teorii. Tento model vnímá problém s bezpečností jako problém s řízením. Pokud je v systému problém s bezpečností, jedná se podle STAMP o nedostatek v řízení procesů. STAMP vnímá systém jako soubor dynamických procesů mezi jednotlivými komponenty systému. Systém tedy není statický a jeho vlastnosti a on sám se v čase mění. [18]

Na modelu STAMP je založeno několik bezpečnostních metod, které jeho principy využívají. Nejužívanější jsou analytické metody STPA (System-Theoretic Process Analysis) a CAST (Causal Analysis based on System Theory). Metoda STPA se řadí mezi proaktivní analytické metody, což znamená, že zkoumá systém v jeho návrhu. Metoda CAST je pak analýzou retrospektivní a zkoumá tak konkrétní nehody a incidenty pomocí systémového přístupu. [18] [19]

Systémová teorie a STAMP jsou vyvinuté pro řešení komplexních socio-technických systémů. Tyto systémy jsou příliš komplexní pro zpracování kompletní analýzy a také příliš organizované pro využití statistiky. Typ těchto systémů je nazýván jako organizovaná komplexita. Pomocí STAMP jsou zobrazovány jako celek skládající se z několika dále dělitelných sub-částí, které spolu interagují. Systémová teorie předpokládá, že s některými součástmi systémů lze zacházet pouze pokud je znám celý systém jako celek. Systémová teorie se opírá o dvě párové myšlenky. [18]

Emergence a hierarchie

Komplexní systémy lze vyjádřit pomocí hierarchie úrovní systémů zobrazující různé úrovně organizace. Každá vyšší úroveň je vždy více komplexní než ta nižší. To znamená,

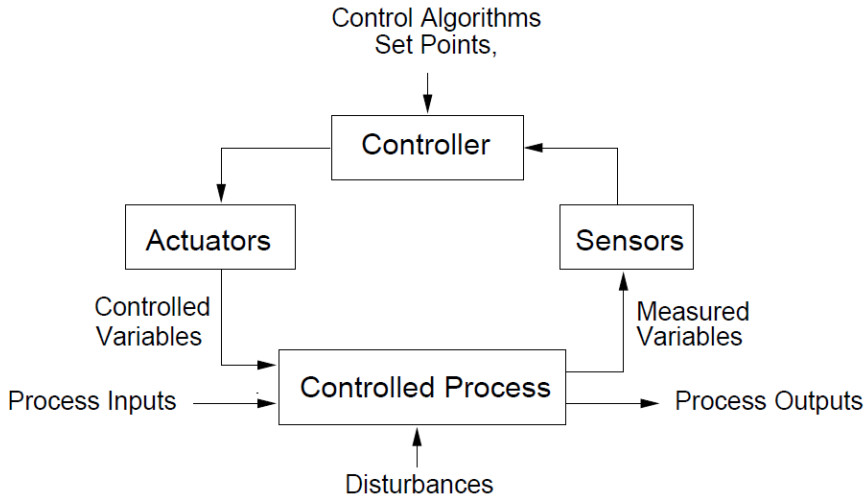
že na vyšších úrovních se setkáme s většími celky, které obsahují větší množství částí systému a také více procesů. Pro každou takovou úroveň jsou charakteristické emergentní vlastnosti. [18]

Princip emergence je zde chápán jako soubor vlastností, které vznikají a zanikají na různých úrovních systému. To znamená, že vlastnosti systému nejsou stejné ve všech úrovních systému. Na nižší úrovni systému, která je méně komplexní, má systém jiné vlastnosti, než když se budeme nacházet v hierarchicky vyšších úrovních. Tam je systém komplexnější a obsahuje mnohem větší množství procesů a částí systémů. [18]

Hierarchické zobrazení systémů pomáhá chápat strukturu systému a jeho jednotlivé úrovně. Hierarchická struktura zobrazuje nejen jednotlivé části systému v daných úrovních, ale také vztahy a interakce mezi nimi. [18]

Komunikace a řízení

Řízení v otevřených systémech je založeno na hierarchické struktuře organizace. Otevřeným systémem je systém, který interaguje s okolím a jehož prostředí je možné ovlivnit vnějším působením. Na základě hierarchie je v každém otevřeném systému tzv. řídící struktura, která popisuje, jak se různé úrovně systému ovlivňují a interagují spolu. Řízení musí být schopno zvládat nejistotu a změny, které se v systému mohou objevit. K tomu je důležité mít jasně definované procesy a postupy pro řízení rizik a zajištění dostatečné úrovně bezpečnosti systému. Komunikace je důležitá pro interakci mezi různými částmi a prvky systému, což je zobrazeno na Obrázku 10 v tzv. standardní řídící smyčce, která vyžaduje čtyři podmínky. [18]

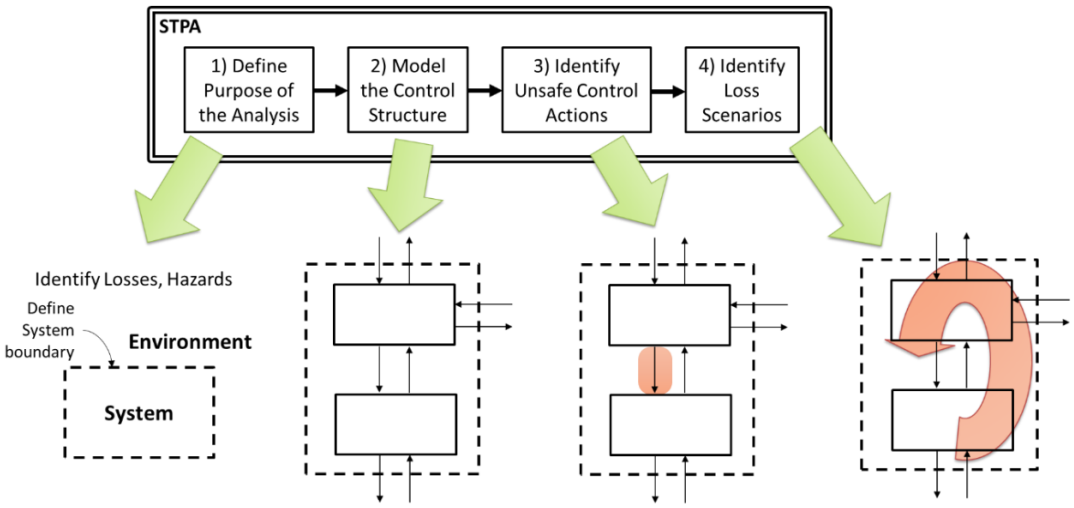


Obrázek 10: Standardní řídící smyčka [18]

- **Podmínka Cíle** – Řídící (Controller) musí mít definovaný cíl nebo více cílů
- **Podmínka Akce** – Řídící musí být schopný měnit stav systému. Toho dosahuje pomocí aktivních řídících prvků (Actuators).
- **Podmínka Modelu** – Řídící musí obsahovat model řízeného procesu. To znamená, že musí znát současný stav systému a také jakým způsobem je možné ovlivnit, aby bylo dosaženo požadované změny. Tento model je zakomponován v softwarové logice nebo v případě lidského řídícího se jedná o mentální model.
- **Princip Sledovatelnosti** – Řídící musí být schopen získat informace o stavu systému. Toho dosahuje také pomocí senzorů (Sensors). [18]

6.2.1. System-Theoretic Process Analysis (STPA)

System-Theoretic Process Analysis (STPA) je systémová analytická metoda, která je založena na bezpečnostním modelu STAMP. Jedná se o proaktivní systémovou analýzu. STPA je koncipována do čtyřech základních kroků, jak je ukázáno na Obrázku 11. [19]



Obrázek 11: Postup analýzy STPA [19]

1) **Definování účelu analýzy** – Prvním krokem STPA je určení účelu analýzy za pomocí definování ztrát, kterým se snaží systém vyvarovat, a identifikace systémových nebezpečí. Na základě identifikovaných systémových nebezpečí jsou pak určeny bezpečnostní omezení (safety constraints), jejichž formulace říká, co je nutné splnit, aby dané nebezpečí nezpůsobilo ztráty. Je také nutné stanovit si hranice systému, který bude analyzován.
2) **Modelování řídící struktury** – Druhý krok STPA zobrazuje řídící strukturu analyzovaného systému. Ta je důležitá pro zjištění hierarchie a interakcí mezi jednotlivými prvky systému. Interakce mezi prvky jsou trojího typu:
    - Řídící akce
    - Zpětná vazba
    - Koordinace – interakce mezi prvky na stejné hierarchické úrovni
3) **Identifikace nebezpečných řídících akcí (UCA)** – Třetím krokem STPA jsou identifikovány čtyři typy nebezpečných řídících akcí. Jsou to takové řídící akce, jejichž neposkytnutí, poskytnutí, poskytnutí brzy/pozdě a také jejich trvání krátce/dlouho vede za určitých okolností ke ztrátám.
4) **Určení ztrátových scénářů** – Posledním krokem STPA je určení ztrátových scénářů. Tyto scénáře vysvětlují, jakým způsobem může nebezpečná řídící akce způsobit ztrátu.

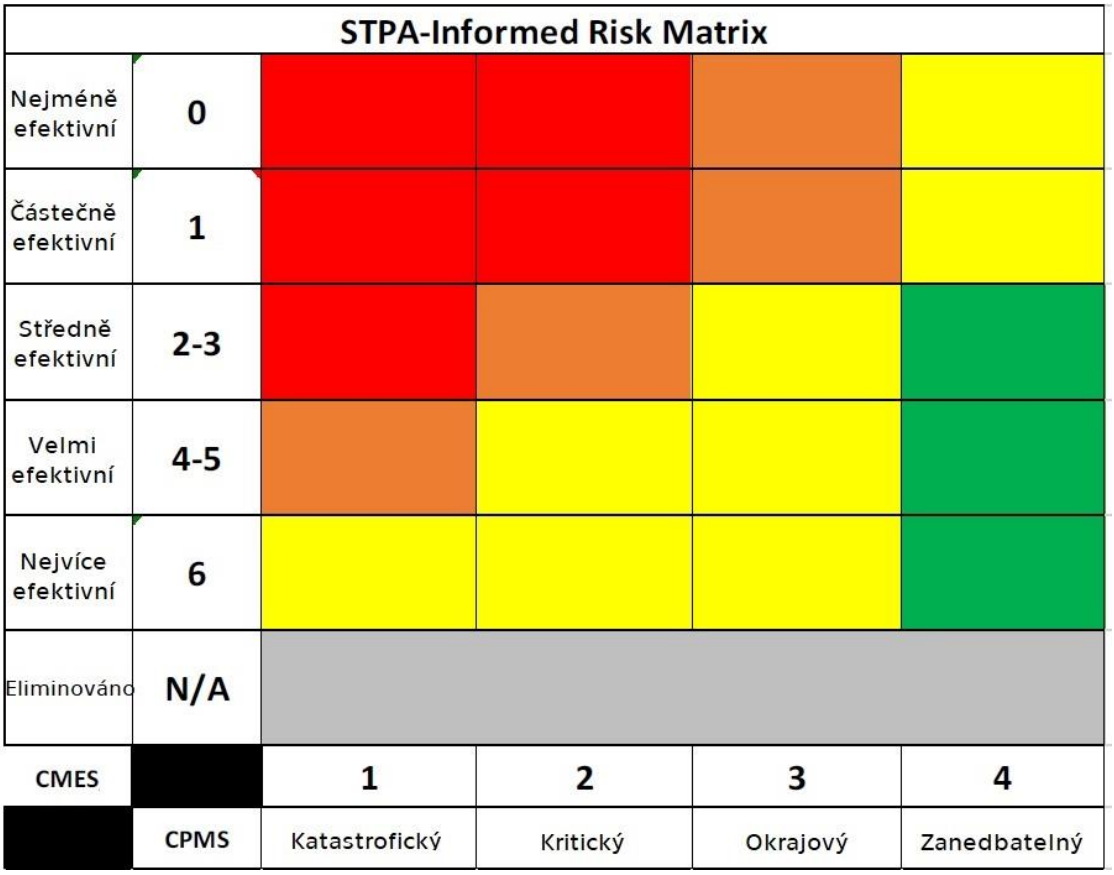
Tento krok se zaměřuje na širší souvislosti systému a interakce jeho prvků. Ke každé UCA může být definován jeden nebo více ztrátových scénářů. [19]

6.3. Analýza rizik pomocí STPA

Bezpečnostní inženýrství používá k ohodnocování rizika standardní matici rizik a postupy, které jsou uvedeny v ICAO Safety Management Manual. Systémový přístup vnímá standardní hodnocení rizik pomocí hodnot závažnosti a pravděpodobnosti jako nedostatečný pro komplexní systémy. Hodnocení závažnosti je relativně snadné určit na základě představy nejhoršího možného důsledku nebo dopadu. Pravděpodobnost je však u komplexních systémů téměř vždy neznámá a nerozpoznatelná. Pravděpodobnost lze zjistit pouze na základě historických dat. Problém nastává především u systémů, které historická data nemají, protože jsou nové nebo změněné. [18]

Problematiku standardního hodnocení rizika řeší systémový přístup pomocí nahrazení hodnoty pravděpodobnosti hodnotou efektivity zmírnění rizika. Tento postup představila dvojice Dro J. Gregorian a Sam M. Yoo na americké univerzitě MIT v publikaci „A System-Theoretic Approach to Risk Analysis“. [25] V této publikaci je představena nová matice rizik založená na analýze STPA (STPA-Informed Risk Matrix). Tato matice je zobrazena na Obrázku 12. STPA-Informed Risk Matrix (SRM) je vytvořena dle hodnot CMES (Combined Mitigation Effectiveness Score) a CPMS (Combined Post Mitigation Severity). [25]

Hodnota CMES (Celkové skóre účinnosti zmírnění rizik) nahrazuje v matici rizik subjektivní hodnocení pravděpodobnosti. Tato hodnota vyjadřuje kombinaci účinnosti jednotlivých nápravných opatření pro zmírnění rizik (MES). Hodnota CMES nezávisí na kvantitě nápravných opatření, ale hodnotí především jejich kvalitu a účinnost. V závislosti na účinnosti nápravných opatření jsou zavedeny tři typy zmírnění rizik – snížení rizika skrze návrh systému, detekce rizika s reakcí, výcvik a procesy. Tyto typy zmírnění včetně jejich numerických hodnot vysvětluje Tabulka 7. [25]



Obrázek 12: Matice rizik založená na STPA (SRM) [25]

Tabulka 7: Úroveň efektivity zmírnění rizik podle STPA-Informed Risk Matrix (přeloženo a upraveno autorem z [25])

Úroveň zmírnění	**Popis zmírnění**	**Hodnota efektivity zmírnění (MES)**
Eliminováno	Kauzální faktor může být eliminován skrze návrh systému nebo kombinací zmírnění. (Proaktivní)	ELIM.
Snížení skrze návrh	Výskyt kauzálního faktoru je možné redukovat nebo řídit skrze návrh systému. (Proaktivní)	3
Detekce rizika s reakcí	Kauzální faktor může být detekován a vyžaduje reakci pro jeho zmírnění. (Reaktivní)	2
Výcvik a procesy	Kauzální faktor může být zmírněn skrze doplňující výcvik a procesy. (Reaktivní)	1
Není	Neexistuje možnost zmírnění, nebo zmírnění není nikdy aplikováno.	0

Hodnota CPMS (Celková závažnost po zmírnění rizika) ukazuje, jaká je celková závažnost rizika po tom, co byla zavedena nápravná opatření pro zmírnění rizika. Tato hodnota kombinuje jednotlivé závažnosti, které jsou přiděleny po aplikování nápravných opatření. Je tedy určeno, jak každé nápravné opatření mění původní hodnotu závažnosti. Z těchto hodnot je pak vypočítána celková hodnota závažnosti po zmírnění rizika (CPMS), jak je ukázáno v Tabulce 8. Tabulka zobrazuje nejdříve původní hodnotu závažnosti před aplikováním nápravných opatření (PMS), následně jsou zde vidět hodnoty závažnosti po aplikaci jednotlivých nápravných opatření (PPMS) a z nich je pak nakonec vypočítána hodnota CPMS. [25]

Tabulka 8: Příklad tabulky hodnocení CPMS [25]

Risk ID	PMS	Mitigation ID	PPMS	CPMS
R1	1	RM01	4	**3**
		RM02	3	
		RM03	3	

Výpočet CPMS probíhá podle Rovnice 1, ke *N* je počet nápravných opatření.

$$CPMS = \frac{\sum_1^N PPMS}{N} \ (Zaokrouhli\ na\ nejnižší\ celé\ číslo) \tag{1}$$

Rovnice 1: Rovnice pro výpočet CPMS [25]

Tabulka 9 pak popisuje jednotlivé hodnoty závažnosti PMS, PPMS a CPMS. Ty jsou oproti standardní ICAO matici rizik pouze čtyři.

V publikaci „A System-Theoretic Approach to Risk Analysis" jsou představeny dva přístupy hodnocení rizik. Prvním je přístup založený na ztrátových scénářích podle STPA. Tento přístup je časově náročnější a vyžaduje důkladné provedení STPA. Jeho výhodou je však zachycení rizik, která by bez hloubkové systémové analýzy nebyla odhalena. Druhý přístup je založený na systémových nebezpečích. Tento přístup nevyžaduje učení všech možných scénářů a je tak časově méně náročný. Aby byla zajištěna dostatečná hloubka analýzy a nešlo k přílišnému zobecnění, využívá tento přístup identifikaci

sub-hazardů. Tyto sub-hazardy zpřesňují identifikovaná systémová nebezpečí a udávají větší míru detailu. Přístup založený na systémových nebezpečích je vhodný především pro rozsáhlejší systémy. [25]

Tabulka 9: Hodnocení PMS, PPMS a CPMS [25]

Popis	Označení Závažnosti	Možné důsledky nehod
Katastrofální	1	Může způsobit jedno nebo více z následujících: Smrt; trvalá totální invalidita; nevratný závažný dopad na životní prostředí; finanční ztráta nad 10 milionů USD včetně.
Kritická	2	Může způsobit jedno nebo více z následujících: Trvalá částečná invalidita; zranění nebo pracovní neschopnost, která může vést k hospitalizaci alespoň 3 pracovníků; vratný závažný dopad na životní prostředí; finanční ztráta nad 1milion USD, ale méně než 10 milionů USD.
Okrajová	3	Může způsobit jedno nebo více z následujících: zranění nebo pracovní neschopnost, která může vést ke ztrátě jednoho nebo více pracovních dnů; vratný středně závažný dopad na životní prostředí; finanční ztráta mezi 100 tisíci USD a 1 milionem USD.
Zanedbatelná	4	Může způsobit jedno nebo více z následujících: zranění nebo pracovní neschopnost, která vede ke ztrátě jednoho pracovního dne; minimální dopad na životní prostředí; finanční ztráta méně než 100 tisíc USD.

7. STPA analýza Údržbové organizace

Současný SMS Údržbové organizace byl navržen za pomoci standardního přístupu, který využívá bezpečnostní inženýrství. Metody a postupy, které jsou v současném SMS využívány nejsou založeny na systémovém přístupu. Aby bylo možné systémově vyvíjet části SMS, jehož současné limitace byly popsány výše, je třeba nejprve pochopit systém Údržbové organizace jako celek a takto ho také analyzovat. To umožní nalézt silné a slabé stránky systému.

Pro analýzu celého systému Údržbové organizace byla zvolena analýza STPA, která umožňuje systémový pohled na organizaci. Oproti analýze FRAM a Safety-II, které se orientují více na sociální složku systémů je STAMP a STPA více vhodná pro socio-technický systém, jakým je údržbová organizace. Z toho důvodu byla zvolena pro analýzu Údržbové organizace právě STPA.

7.1. Zvolení vhodné úrovně detailu

Dříve, než byla provedena samotná analýza, bylo nutné zvolit míru detailu, se kterým bude analýza prováděna. Jelikož je STPA tzv. Top-Down (tj. shora dolů), je možné začít s analýzou ve velmi obecné rovině. Takový přístup však nenabízí detailnější vhled do systému. Na druhou stranu je možné systém rozdělit na mnoho subsystémů, které samy o sobě také mohou být dále dělitelné. Zvolení příliš detailní a konkrétní úrovně by mohlo přinést nepřehledné výsledky. Kvantita dat by pak mohla být na škodu kvalitě a výstupy analýzy by nemusely být zcela jasné a přehledné.

Z těchto důvodů byla zvolena úroveň detailu, která odpovídá té ve Výkladu organizace (MOE). Následně pak byla daná úroveň dle potřeby mírně upravována.

7.2. Identifikace ztrát a nebezpečí

Prvním krokem STPA analýzy je definování ztrát a identifikace nebezpečí. Pro účely analýzy bylo definováno 5 základních ztrát, u kterých se předpokládá, že je jejich dosažení je pro Údržbovou organizaci velmi nežádoucí.

Definované ztráty:

L-1: Ztráta života nebo zranění

L-2: Finanční ztráta

L-3: Ztráta zákazníka

L-4: Ztráta reputace společnosti

L-5: Ztráta důvěry zaměstnanců

K definovaným ztrátám je následně nutné identifikovat systémová nebezpečí, která za určitých podmínek mohou tyto ztráty způsobit. Prvním identifikovaným systémovým nebezpečím je H-1.

H-1: Údržbová organizace vydá po provedení údržby osvědčení o uvolnění do provozu (CRS) bez provedení údržbových prací, jak bylo uvedeno v objednávce prací nebo ve smlouvě; mimo příslušné požadavky; a mimo schválené postupy údržbové organizace. (např. Údržbová organizace schválená podle Part-145 neprovedla objednanou údržbu v rámci schválených údajů o údržbě, údržba nebyla dokončena a dodána zákazníkovi, nebyly poskytnuty informace o odkládané údržbě zákazníkovi atd.)

Cílem bezpečnosti a systému řízení bezpečnosti je zabránit ztrátám. Ztráty mohou mít různý charakter a každá organizace je přizpůsobuje svému provozu a svým nastaveným prioritám. Údržbová organizace je právní subjekt, jehož jedním z hlavních cílů je generovat finanční zisk. Z toho důvodu se systém řízení Údržbové organizace snaží zabránit také finančním ztrátám. Na základě této skutečnosti bylo identifikováno druhé systémové nebezpečí (H-2), které za určitých podmínek vede ke ztrátě L-2.

H-2: Organizace neprovádí aktivity efektivně. (Např. Organizace neprovádí aktivity, které generují zisk, nebo provádí aktivity neefektivně tak, že mohou být méně nákladné nebo generovat větší zisk.)

Nebezpečí H-2 je při analýze uvedeno hlavně z toho důvodu, že Údržbová organizace uvažuje ve svém systému řízení jak bezpečnostní rizika, tak i finanční a provozní rizika,

která se nemusí týkat pouze provozní bezpečnosti, jak ji chápe ICAO. Jde převážně o rizika, která jsou nežádoucí z důvodu možného zastavení, zpomalení či zkomplikování běžného provozu a jejichž důsledkem by byla pouze finanční ztráta společnosti.

Ke každému identifikovanému nebezpečí se definují tzv. bezpečnostní omezení (SC), která vysvětlují, co je nutné splnit, aby dané nebezpečí nevedlo ke ztrátě. Níže uvedená bezpečnostní omezení jsou vždy přiřazena k výše zmíněným nebezpečím.

H-1: Údržbová organizace vydá po provedení údržby osvědčení o uvolnění do provozu (CRS) bez provedení údržbových prací, jak bylo uvedeno v objednávce prací nebo ve smlouvě; mimo příslušné požadavky; a mimo schválené postupy údržbové organizace. (např. Údržbová organizace schválená podle Part-145 neprovedla objednanou údržbu v rámci schválených údajů o údržbě, údržba nebyla dokončena a dodána zákazníkovi, nebyly poskytnuty informace o odkládané údržbě zákazníkovi atd.).

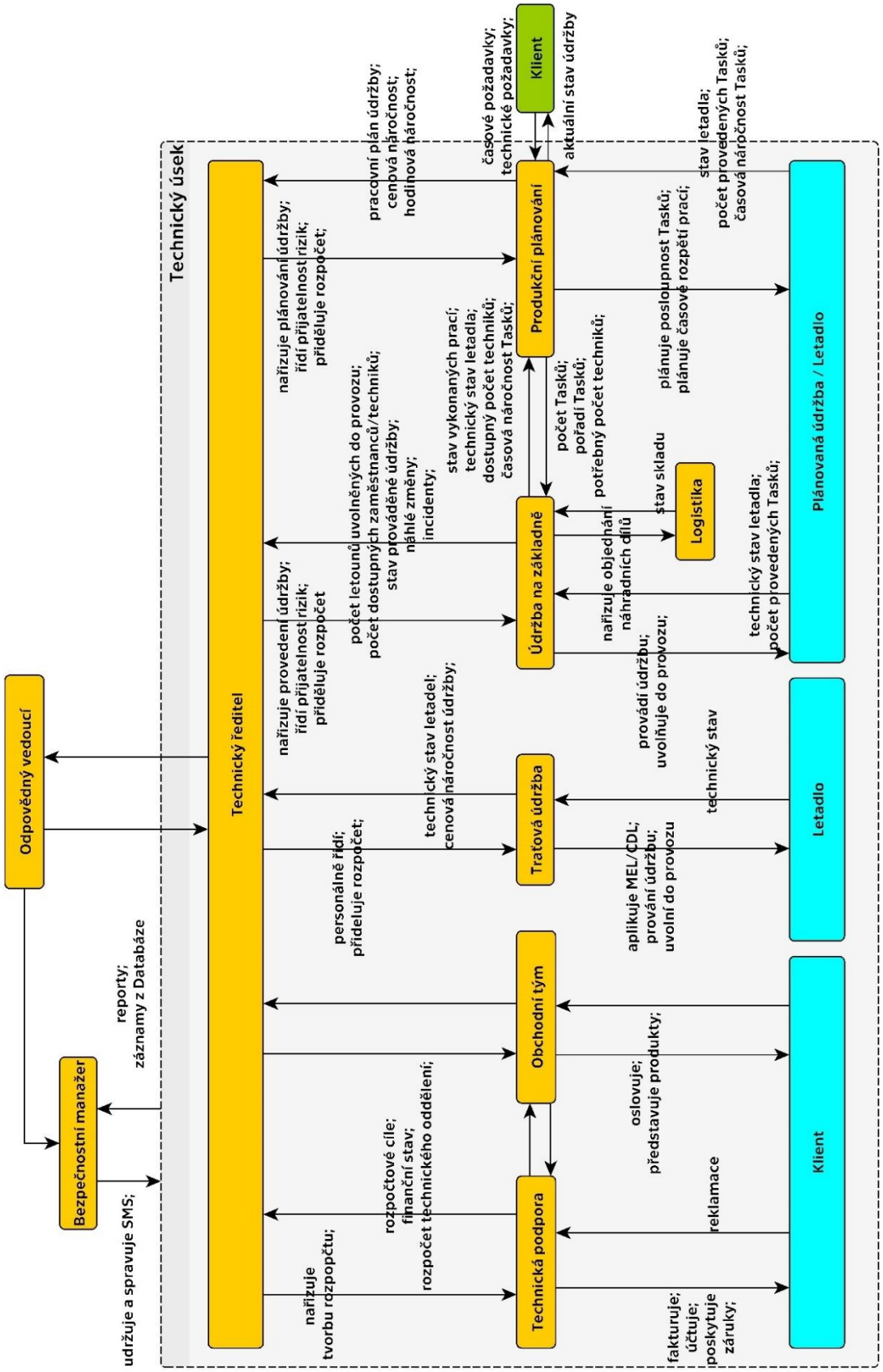
> SC: Údržbová organizace musí vydat CRS pouze pokud byly provedeny údržbové práce, jak jsou uvedeny v objednávce prací nebo ve smlouvě; podle příslušných požadavků; a dle schválených postupů organizace.

H-2: Organizace neprovádí aktivity efektivně. (Např. Organizace neprovádí aktivity, které generují zisk, nebo provádí aktivity neefektivně tak, že mohou být méně nákladné nebo generovat větší zisk.

> SC: Organizace musí provádět aktivity efektivně.

7.3. Model řídící struktury

Jako druhý krok analýzy byla vymodelována řídící struktura Údržbové organizace. Tento model zobrazuje Obrázek 13. Model řídící struktury obsahuje veškerá oddělení Údržbové organizace, která jsou potřebná pro její provoz. Detail modelu byl zvolen podle Výkladu organizace (MOE) Údržbové organizace.



Obrázek 13: Model řídící struktury Údržbové organizace

7.4. Nebezpečné řídící akce

V dalším kroku analýzy STPA bylo identifikováno 25 nebezpečných řídících akcí (UCA). Tyto UCA byly identifikovány na základě vytvořeného modelu řídící struktury. Řídící akce zobrazené v modelu řídící struktury šipkou směřující hierarchicky shora dolů mohou být při určitém stavu systému nebezpečné. UCA jsou obecně řazeny do 4 kategorií dle jejich typu. Kompletní seznam UCA je uveden v Příloze 2.

Nejčetnějším se ukázal být typ UCA, kdy správné poskytnutí řídící akce vede k nebezpečí. Taková řídící akce je provedena tak, jak byla navržena, avšak za určitých podmínek je její provedení nebezpečné. Příkladem tohoto typu nebezpečné řídící akce je UCA-7.

UCA-7: BM Team provede údržbu, když odborný personál nezná správné postupy.

Výše uvedená UCA-7 popisuje stav, kdy tým údržby na základně provede údržbu za stavu, kdy není dostatečně seznámen s postupy pro provádění daných úkonů. Původní účel provedení údržby měl za cíl zvýšit úroveň bezpečnosti a zajistit letovou způsobilost letadla. V případě, že personál, který údržbu provádí není dostatečně vyškolen, jedná se o nebezpečí, které za určitých podmínek může vést ke ztrátám.

7.5. Ztrátové scénáře

V posledním kroku analýzy STPA bylo určeno 38 možných ztrátových scénářů. Toto číslo není vysoké především proto, že míra detailu byla nastavena spíše v obecnější rovině. Kompletní seznam ztrátových scénářů je obsažen v Příloze 3. Jednou z nejčastějších příčin vzniku ztrátových scénářů se ukázalo být zpoždění údržby. To vede zaměstnance Údržbové organizace, především techniky, do časové tísně a stresu. Za takových podmínek pak dochází v současném nastavení systému k vynechání podstatných částí údržbového procesu a v důsledku toho dochází ke ztrátám.

Další z častých příčin vzniku ztrátových scénářů se ukázal být nedostatek techniků v důsledku nedostatečného plánování. Plánování může být v tomto případě nedostatečné

ze strany organizace. Plánování pak může být také značně ztíženo ze strany klienta, který mění požadavky na údržbu a komplikuje tak celý proces plánované údržby.

V neposlední řadě vyplynula z analýzy STPA jako příčina vzniku ztrátových scénářů nedostatečná technika, která může zpomalit údržbové procesy nebo ohrozit jejich provedení. Dále pak byl odhalen ztrátový scénář, který má vznik v nedostatečném financování Údržbové organizace a nízkém rozpočtu.

Vzhledem k tomu, že primárním cílem Údržbové organizace jakožto prosperující společnosti je generovat finanční zisk, je jednou ze ztrát také ztráta finanční. Pokud se oprostíme od ostatních ztrát (např. ztráta života nebo zranění), v jejichž důsledků může finanční ztráta vyplynout, je jedním ze ztrátových scénářů nedostatečná snaha získávat nové klienty a zakázky. Tento ztrátový scénář vede k zastavení či zpomalení provozu Údržbové organizace, což znemožní generovat finanční zisk potřebný pro další rozvoj společnosti.

8. Aplikace systémového přístupu k bezpečnosti na vybrané prvky SMS v konkrétní údržbové organizaci

Po analýze současného systému řízení provozní bezpečnosti (SMS) konkrétní údržbové organizace (dále jen „Údržbová organizace“) byly vybrány tři části tohoto SMS, jejichž další vývoj by měl pro Údržbovou organizaci největší přínos. Cílem této práce je navrhnout konkrétní nástroje a zlepšení současného SMS, které by zajistili jak vysokou úroveň bezpečnosti v Údržbové organizaci, tak i srozumitelné a praktické využití.

8.1. Identifikace nebezpečí a hodnocení rizik pomocí systémového přístupu

Současný proces identifikace nebezpečí a hodnocení rizik je založen na rozhodnutí odpovědných vedoucích (RM), kteří provádí bezpečnostní analýzu, identifikují nebezpečí a hodnotí rizika, jak bylo vysvětleno v kapitole 4 (Systém řízení provozní bezpečnosti konkrétní údržbové organizace). Údržbová organizace ukládá tyto úkony pro zajištění bezpečnosti do rukou odpovědných vedoucích (RM). Oddělení provozní bezpečnosti (OPB) udržuje v Údržbové organizaci SMS a na provedení potřebných úkonů dohlíží a v případě nutnosti je koriguje.

Pomocí systémového přístupu a dosud dostupných metod byl vytvořen návrh nového postupu při identifikaci nebezpečí a hodnocení rizik. Jak již bylo vysvětleno, jednou z limitací současného stavu procesu identifikace nebezpečí je málo specifikovaný postup. Odpovědný vedoucí má mnoho možností, jak nebezpečí definovat, což pak vede k různým definicím stejných nebezpečí, rozdílné míře detailu a ke spoustě dalších neshod v registru nebezpečí.

Návrh identifikace nebezpečí a hodnocení rizik pomocí systémového přístupu v Údržbové organizaci je zobrazen v Tabulce 10. Tato tabulka obsahuje veškeré navržené prvky procesu, které jsou využívány. Tabulka slouží jako součást registru nebezpečí pro zpřehlednění postupu a zvýraznění všech potřebných aspektů procesu, nicméně forma zaznamenávání

dat může být přizpůsobena potřebám Údržbové organizace a lze ji tak integrovat do interního softwaru.

Tabulka 10 představuje veškeré prvky nového návrhu procesu identifikace nebezpečí a hodnocení rizik v Údržbové organizaci. Tabulka vychází z přístupu založeném na nebezpečí, jak jej popisuje publikace „A System-Theoretic Approach to Risk Analysis". [25] Hodnoty rizik jsou v Tabulce 10 pouze orientační a jsou zobrazeny jako vzor hodnocení rizika. Konkrétní hodnoty přiřazuje Údržbová organizace s ohledem na bezpečnostní cíle a praktickou zkušenost.

Factor (UCA syntax)	Systémové nebezpečí		Sub-nebezpečí		PMS	RM ID	Nápravné opatření (RM)	MES	CMES	PPMS	CPMS	Riziko
Factor 1 (Fa-1): Technik neuklidil nářadí po údržbě v podvozkové šachtě.	H-15	H-15: Organizace neeviduje podrobnosti o údržbových pracích, které jsou prováděny v rozsahu jejího oprávnění.	H-15.1	Organizace neeviduje dostupné vybavení.	1	RM01	Zavedení databáze dostupného nářadí	3	ELIM.	3	2	ELIM.
						RM02	Zavedení kontroly databáze nářadí	3		3		
						RM03	Zavedení školení	1		2		
	H-17	H-17: Organizace nezavádí postupy, které by zajistily, že při údržbě budou brány v úvahu lidské faktory a doporučené postupy údržby.	H-17.1	Organizace nemá účinný systém dvojí kontroly údržby.	1	RM04	Zavedení double-check systému údržby	3	6	3	2	12
						RM05	Zavedení školení	1		2		
						RM06	Zavedení postupů kontroly po dokončení údržby	2		2		
			H-17.2	Organizace nezavádí postupy, které by zajistily, že po údržbě nezůstane uvnitř letadla žádný FOD.	1	RM07	Zavedení postupů kontroly po dokončení údržby	2	ELIM.	4	3	ELIM.
						RM08	Zavedení školení	1		3		
						RM09	Zavedení databáze dostupného nářadí	3		2		

Tabulka 10: Návrh tabulky identifikace nebezpečí a hodnocení rizik

Kauzální faktor (Factor)

Výchozím prvkem je kauzální faktor (Factor). Tento prvek využívá syntax nebezpečných řídících akcí (UCA), jak jsou popsány v STPA Handbook. [19] Tyto faktory jsou navrženy jako výstup analýzy a šetření událostí či hlášení, které jsou přijaty v rámci interního systému hlášení. Faktory zobrazují nejdetailnější pohled na konkrétní řešený problém či událost. V rámci jedné události či reportu může být identifikováno více faktorů, které vedou k systémovým nebezpečím či sub-nebezpečím.

Systémové nebezpečí

Provedená STPA analýza systému Údržbové organizace přinesla pouze dvě systémová nebezpečí. V navrženém procesu identifikace nebezpečí by využití pouze dvou systémových nebezpečí nebylo praktické. Proto je do nového návrhu procesu identifikace nebezpečí začleněno 19 předem nadefinovaných nebezpečí, která lze považovat za systémová, protože jsou relevantní pro celý systém Údržbové organizace. Tato systémová nebezpečí jsou rozdělena do 15 kategorií, podle základních požadavků, které musí každá údržbová organizace schválená podle Part-145 Nařízení (EU) 1321/2014 splňovat. Systémová nebezpečí byla navržena na základě platné legislativy a priorit Údržbové organizace. V Tabulce 11 je znázorněn příklad systémového nebezpečí s označením SysH-5, které je v novém návrhu začleněno.

Tabulka 11: Systémové nebezpečí SysH-5

Kategorie	ID Systémového nebezpečí	Systémové nebezpečí
Vybavení a nářadí	SysH-5	Organizace nepoužívá a nemá dostupné nezbytné vybavení a nářadí k provedení schváleného rozsahu práce.

Systémové nebezpečí SysH-5 popisuje stav, kdy organizace není dostatečně technicky vybavena pro vykonání údržby. Toto nebezpečí je platné pro celý systém Údržbové organizace. Platí proto pro každou část a každý prvek tohoto systému. Je však zřejmé, že toto nebezpečí je velmi obecné. Pro bližší identifikaci problému by se takové

nebezpečí dalo využít jen velmi obtížně. Z toho důvodu byla navržena tvorba tzv. sub-nebezpečí (sub-hazards), které dále rozvíjejí systémová nebezpečí a zobrazují větší detail.

Sub-nebezpečí

Sub-nebezpečí jsou podřazené systémovým nebezpečím. Jejich definice upřesňuje a konkretizuje systémové nebezpečí a přikládá mu vyšší míru detailu v kontextu s řešenou událostí. Sub-nebezpečí nejsou předdefinována předem a jejich tvorba či udržování záleží na aktuálních problémech a prioritách Údržbové organizace.

Nápravná opatření

Nápravná opatření (Recommended mitigation – RM) jsou doporučené akce pro zmírnění rizika. Tato opatření mění jak pravděpodobnost, že dojde ke ztrátě, tak i závažnost důsledků, pokud by nastaly. Nápravná opatření jsou tří typů:

- Změna systému skrze jeho návrh
- Detekce rizika s vyžadovanou reakcí
- Výcvik a procesy (postupy)

Typy nápravných opatření byly vysvětleny podrobněji v Tabulce 7. Každý typ nápravného opatření má dle svého zařazení přidělenou hodnotu MES (Mitigation Effectiveness Score) v rozmezí 1-3. V případě, že nápravné opatření neexistuje, je přiřazena hodnota 0.

Hodnocení rizika

Hodnocení rizika závisí na dvou základních hodnotách CMES (Combined Mitigation Effectiveness Score) a CPMS (Combined Post Mitigation Severity). CMES hodnotí celkovou účinnost všech nápravných opatření pro zmírnění rizika. Hodnoty CMES jsou popsány v Tabulce 7. CPMS pak hodnotí celkovou závažnost rizika po přijetí a aplikaci nápravných opatření. Hodnoty CPMS jsou odlišné od hodnot závažnosti (Severity), jak je uvádí ICAO Safety Management Manual. [2]

8.2. Registr nebezpečí

Návrh nového registru nebezpečí vychází z nově navrženého procesu identifikace nebezpečí a hodnocení rizik. Registr nebezpečí byl navržen ve dvou formách tabulek, které umožňují sledovat aktuální rizika v Údržbové organizaci.

První forma tabulky je reprezentována Tabulkou 10. Návrh této formy tabulky umožňuje Údržbové organizaci detailní pohled na jednotlivé kauzální faktory. Ke každému faktoru jsou přehledně zobrazena identifikovaná nebezpečí a jednotlivá hodnocení MES, PPMS. Dále je také možné přehledně porovnat, jak jednotlivá opatření přispěla ke snížení rizika.

Druhá forma tabulky registru nebezpečí slouží především pro obecný přehled nad stávajícími problémy, nebezpečími a riziky v organizaci. Obsah není tolik konkrétní a zaměřený na detail, avšak jeho využitelnost je vysoká především pro vyšší management, který sleduje stav bezpečnosti v celém systému Údržbové organizace. Tabulka 12 ukazuje příklad záznamu v registru nebezpečí. Je zde zobrazeno systémové nebezpečí včetně definovaných konkrétních sub-nebezpečí. Ke každému sub-nebezpečí je dále uveden seznam identifikovaných kauzálních faktorů, které souvisí s daným sub-nebezpečím. Jelikož pro více faktorů může být identifikováno stejné sub-nebezpečí, je v registru ke každému sub-nebezpečí přidělen jeden nebo více identifikovaných faktorů.

Stav, který je prezentován v Tabulce 12 ukazuje, že k Systémovému nebezpečí SysH-17 byla dosud identifikována 2 sub-nebezpečí. K SysH-15 je přiřazen zatím jedno sub-nebezpečí a SysH-16 zatím nemá identifikované žádné sub-nebezpečí. Takový stav registru je tedy teprve počáteční a bude dále rozvíjen na základě řešených událostí. Sub-nebezpečí uvedená v Tabulce 12 jsou pouze příklady možných navržených nebezpečí.

Tabulka 12: Návrh nového registru nebezpečí

Kategorie	ID SysH	Systémové nebezpečí	ID Sub-nebezpečí	Sub-nebezpečí	Faktor	Současné riziko
Uchování záznamů	**SysH-15**	**Organizace neeviduje podrobnosti o údržbových pracích, které jsou prováděny v rozsahu jejího oprávnění.**	H-15.1	Organizace neeviduje dostupné vybavení.	Fa-1	ELIM.
Hlášení událostí	**SysH-16**	**Organizace nezavádí a neudržuje systém hlášení událostí, včetně povinného a dobrovolného hlášení.**				
Procesy údržby	**SysH-17**	**Organizace nezavádí postupy, které by zajistily, že při údržbě budou brány v úvahu lidské faktory a doporučené postupy údržby.**	H-17.1	Organizace nemá účinný systém dvojí kontroly údržby.	Fa-1, Fa-2	12
			H-17.2	Organizace nezavádí postupy, které by zajistily, že po údržbě nezůstane uvnitř letadla žádný FOD.	Fa-1	ELIM.

8.3. Indikátory bezpečnosti

Hlavní motivací pro zavedení nové sady indikátorů bezpečnosti (SPIs) je systémové měření výkonnosti v oblasti bezpečnosti. Současné SPIs byly zavedeny expertně a bez předchozí analýzy systému. Nová sada SPIs je odvozena od výsledů analýzy STPA, která byla popsána v kapitole 7 (STPA Analýza Údržbové organizace). STPA analýza odhalila několik příčin možných ztrátových scénářů. Na základě nejčastějších příčin a faktorů byla vytvořena sada nových SPIs. Výsledná sada pěti SPIs je uvedena v Tabulce 13.

Tabulka 13: Návrh nové sady indikátorů bezpečnosti (SPIs)

	Název SPI	Měření	Vysvětlení	Poznámky
1	Zpoždění údržby-zanedbatelné	Počet zanedbatelně zpožděných zakázek údržby za časový interval (měsíc)	Zvýšený počet zanedbatelných zpoždění indikuje předpoklad nárůstu také vážných zpoždění.	Časový interval pro **"zanedbatelné zpoždění"** definuje společnost na základě zkušeností z praxe.
2	Zpoždění údržby-vážné	Počet vážných zpožděných zakázek údržby za časový interval (měsíc)	Vysoký počet vážných zpoždění indikuje možnost finančních ztrát, ztrát reputace společnosti či ztrátu klienta	Časový interval pro **"vážné zpoždění"** definuje společnost na základě zkušeností z praxe.
3	Přetížení/Nevyužití Techniků	Počet odpracovaných hodin technika na letadlech za určité časové období (měsíc).	Zvýšený počet odpracovaných hodin indikuje možné přetížení techniků. Nízký počet odpracovaných hodin indikuje nedostatečné využití techniků a možnou finanční ztrátu.	Interval optimálního využití Techniků definuje společnost na základě zkušeností z praxe
4	Technika a nářadí	Počet chybějícího nářadí. Měření při pravidelných kontrolách/po dokončení údržby.	Pravidelná kontrola nářadí používaného v údržbě. Měření počtu nedostupného či ztraceného nářadí.	
5	Technika a nářadí	Počet reportů, kterým je přiřazeno systémové nebezpečí SysH-5.	Zvýšený počet reportů, kterým je přiřazeno SysH-5 indikuje nedostatečnou vybavenost a dostupnost odpovídající techniky či nářadí.	SysH-5: Organizace nemá k dispozici a nepoužívá potřebné vybavení a nářadí k provádění schváleného rozsahu prací.

Prvním krokem pro vytvoření nové sady SPIs byla analýza systému Údržbové organizace pomocí STPA. Obecnější model řídící struktury umožnil přehlednější celkovou analýzu bez velkého počtu UCA a ztrátových scénářů.

Druhým krokem postupu pro návrh nových SPIs byla sumarizace výsledků do kategorií dle častých faktorů způsobujících ztrátové scénáře. Na základě těchto faktorů a příčin byly vytvořeny předběžné návrhy indikátorů.

Posledním krokem postupu bylo nutné navržené indikátory upravit tak, aby byly využitelné v praxi. Indikátory musely být v první řadě měřitelné a kvantifikovatelné. Dále byly upraveny tak, aby byly dostatečně konkrétní a jasně vysvětlené. V neposlední řadě pak muselo být ověřeno, zda má Údržbová organizace možnosti takové SPIs měřit vzhledem k dostupným systémům, struktuře a velikosti organizace.

9. Postup využití navržených technických nástrojů SMS

Navržené technické nástroje pro části SMS, jakými jsou nový **postup identifikace nebezpečí a hodnocení rizik**, nový **registr nebezpečí** a také nové **indikátory bezpečnosti (SPIs)**, jsou první částí vývoje současného systému řízení provozní bezpečnosti (SMS) v konkrétní údržbové organizaci schválené dle Part-145 Nařízení (EU) 1321/2014 (dále jen „Údržbová organizace"). Pro praktické využití těchto nástrojů SMS je potřebné vědět, jak tyto nástroje používat, aby fungovali dle jejich navrženého účelu.

9.1. Postup využití procesu identifikace nebezpečí a hodnocení rizik

Postup procesu identifikace nebezpečí se ve velké míře opírá o představenou Tabulku 9. Tato tabulka obsahuje potřebná data pro proces hodnocení rizik.

Hlášení a záznam

Prvním krokem celého procesu je obdržení hlášení v rámci interního systému hlášení. Toto hlášení obdrží oddělení provozní bezpečnosti (OPB) a na základě toho pak vytvoří záznam v interním softwaru. Poté přidělí vedoucí provozní bezpečnosti (VPB) příslušného vedoucího (RM), který tento záznam bude dále zpracovávat.

Šetření události

Jakmile je k danému záznamu (události/reportu) přiřazen příslušný vedoucí (RM), je provedeno šetření na základě doporučených postupů Údržbové organizace. Ta doporučuje využití několika základních analytických metod, jako je například metoda 5-Why. V současném stavu je výstupem tohoto šetření tzv. kořenová příčina, která nemá jasně definovanou syntax.

Proces šetření událostí není obsahem této práce. Tento proces je zde popisován, protože je nezbytným krokem pro zjištění kauzálních faktorů, které jsou vstupem do nově navrženého procesu identifikace nebezpečí a hodnocení rizik.

Jelikož systémový přístup k bezpečnosti neuvažuje pomocí lineárního řetězce událostí, je pravděpodobné, že výsledkem šetření bude více faktorů, které přispívají k řešené události. Navržený postup identifikace nebezpečí a hodnocení rizik tedy uvažuje jako výstup šetření jeden nebo více kauzálních faktorů, které přispívají ke vzniku incidentu nebo nehody. Syntax těchto faktorů je navržena dle syntaxe nebezpečných řídících akcí (UCA), jak je uvedena v STPA Handbook [19]. Tato syntax je popsána také níže.

<Zdroj (řídící)> <Typ> <Řídící akce> <Kontext>

Příklad (Fa-1): *Technik neuklidil nářadí po údržbě v podvozkové šachtě.*

Identifikace nebezpečí

Po určení kauzálních faktorů, které jsou výstupem šetření událostí, nastává proces identifikace nebezpečí. Nově navržený proces identifikace nebezpečí se skládá ze dvou základních kroků. Prvním krokem je výběr ze seznamu systémových nebezpečí, které byly navrženy na základě legislativních požadavků na údržbové organizace schválené dle Part-145 a dle priorit Údržbové organizace. Těchto systémových nebezpečí bylo navrženo celkem 19. Druhým krokem je identifikace tzv. sub-nebezpečí, která jsou konkrétněji definovaná vzhledem k řešené události či problému. Kompletní seznam systémových nebezpečí je uveden v Příloze 4 v rámci tabulky registru nebezpečí.

V prvním kroku vybere RM systémové nebezpečí ze seznamu a přiřadí toto nebezpečí ke kauzálnímu faktoru určenému během procesu šetření události. Ke každému kauzálnímu faktoru je možné přiřadit jedno nebo více systémových nebezpečí, jak také ukazuje Tabulka 9.

Po výběru systémových nebezpečí je nutné tato nebezpečí upřesnit, aby nedošlo ke ztrátě detailu a nebezpečí bylo spojeno s řešenou událostí nebo problémem. Tohoto upřesnění je dosaženo identifikací tzv. sub-nebezpečí. Příslušný vedoucí (RM) má při identifikaci sub-nebezpečí dvě možnosti. První možností je výběr z již identifikovaných sub-nebezpečí, která byla definována v minulosti. V případě, že takové nebezpečí ještě v Údržbové organizaci nebylo identifikováno, musí RM identifikovat nové sub-nebezpečí, které je vztaženo k řešené události.

Stanovení hodnoty PMS a určení nápravných opatření

Jakmile jsou identifikována veškerá sub-nebezpečí, je dalším krokem stanovení hodnoty závažnosti před zavedením nápravných opatření (PMS). Tato hodnota určuje nejhorší možný dopad, který by mělo nebezpečí, pokud by vedlo ke ztrátám. Hodnocení závažnosti probíhá podle Tabulky 9 v rozmezí hodnot 1-4.

Dalším krokem v procesu je návrh nápravných opatření pro zmírnění rizika. Typy těchto nápravných opatření jsou vysvětleny v Tabulce 7. Příslušný manažer navrhne k identifikovaným nebezpečím jedno nebo více nápravných opatření. Poté je nezbytné ohodnotit efektivitu navržených opatření, samostatně (MES) i společným působením (CMES). Aby bylo možné ohodnotit efektivitu je nutné každé navržené opatření zavést buď do reálné praxe nebo systém podrobit analýze, která již analyzuje systém po zavedení nápravných opatření.

Hodnocení efektivity jednotlivých nápravných opatření (MES) probíhá pomocí hodnot z Tabulky 7. Celková efektivita všech nápravných opatření (CMES) není vždy součtem všech hodnot MES. CMES závisí především na kvalitě navržených opatření. Například pokud hodnotící manažer určí, že navržená opatření jsou natolik efektivní, že riziko je eliminováno, je toto přiřazeno hodnotě CMES. Pokud jsou zavedené dvě opatření redukující riziko srze návrh, není hodnota CMES rovna 6, ale pouze 3. Pro dosažení hodnoty CMES rovné 6 je nutné zavést všechny tři typy nápravných opatření. Pokud příslušný hodnotící manažer následně určí, že i přes zavedení všech tří typů nápravných opatření není riziko eliminováno, přiřadí hodnotu CMES 6, jakožto součet hodnot MES.

Stanovení hodnot PPMS, CPMS a celkového rizika

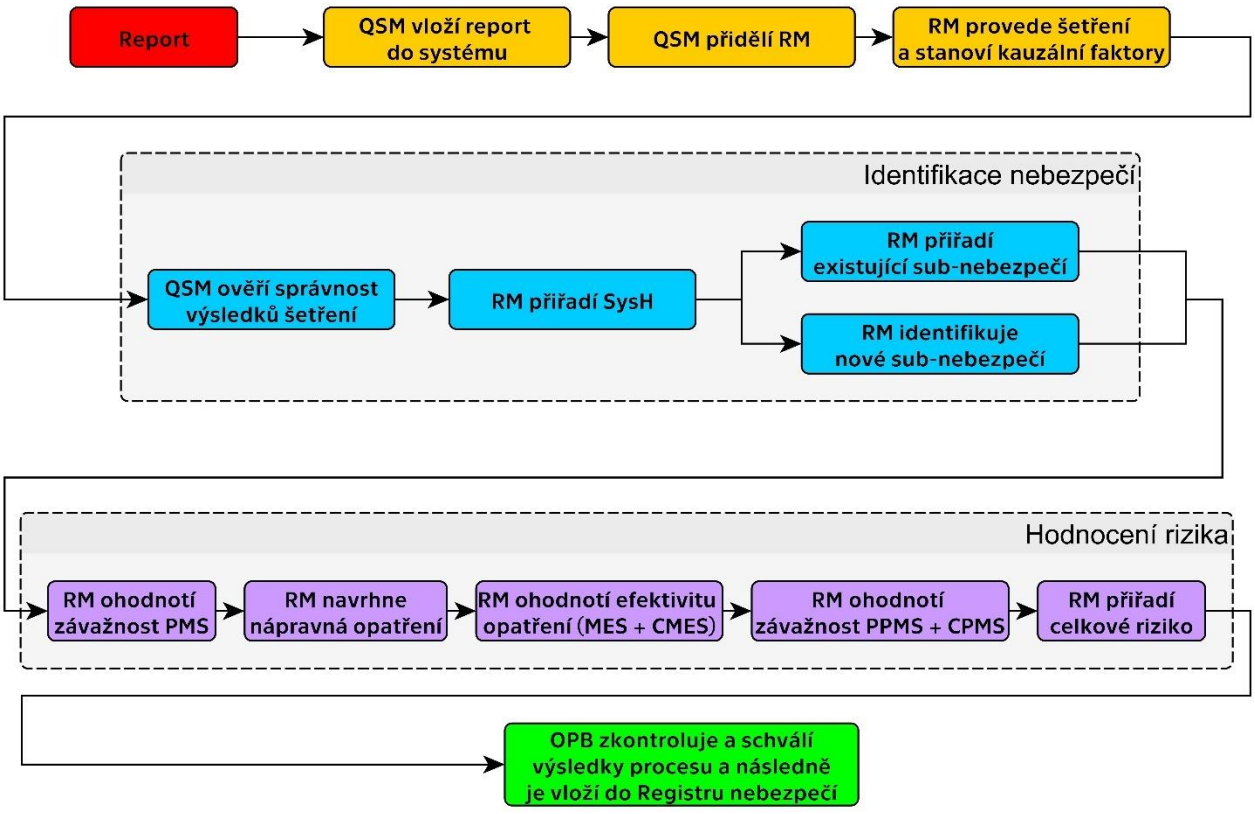
Po ohodnocení dílčí a celkové efektivity nápravných opatření je třeba znovu ohodnotit závažnost. Tentokrát je však tato hodnota uvažována po zavedení nápravných opatření pro zmírnění rizika. Hodnotící kritéria zůstávají stejná jako pro hodnocení PMS. Nejdříve dojde k ohodnocení závažnosti po zavedení jednotlivých nápravných opatření. To ukazuje, jak každé nápravné opatření jednotlivě ovlivňuje závažnost, jestli a jak moc ji snižuje. Tato hodnocení přestavují hodnoty závažnosti po zavedení nápravných opatření

pro zmírnění rizik (PPMS). Následně je určena celková závažnost po zavedení nápravných opatření pro zmírnění (CPMS) dle Vzorce 1.

Posledním krokem procesu hodnocení rizik je samotné určení celkového rizika. Hodnota celkového rizika je vypočtena součinem hodnot CMES a CPMS. To znamená, že celkové riziko je uvažováno po zavedení nápravných opatření. Celkové riziko je vyhodnoceno dle matice rizik STPA-Informed Risk Matrix, která je uvedená v Obrázku 12.

Jakmile RM ohodnotí identifikuje nebezpečí, navrhne nápravná opatření a ohodnotí rizika, je nutné nechat výsledky schválit oddělením provozní bezpečnosti (OPB). OPB zajistí a zkontroluje správnost provedení postupu. Tím je možné eliminovat například opakování stejných sub-nebezpečí v registru nebezpečí.

Kompletní postup identifikace nebezpečí a hodnocení rizik je graficky zobrazen na Obrázku 14.



Obrázek 14: Proces identifikace nebezpečí a hodnocení rizik

9.2. Postup využití registru nebezpečí

Nově navržený registr nebezpečí je složen ze dvou forem tabulek. První formu reprezentuje Tabulka 10. Tato tabulka obsahuje detailní data a přehled hodnocení rizik. Druhá a obecnější forma tabulky je zobrazena Tabulkou 12. Ta obsahuje kompletní seznam systémových nebezpečí a seznam dosud identifikovaných sub-nebezpečí. Ke každému sub-nebezpečí je doplněn seznam označení kauzálních faktorů, ke kterým bylo dané sub-nebezpečí přiřazeno během procesu identifikace nebezpečí.

Velmi důležitý je poslední sloupec této tabulky. V tomto sloupci je uvedeno současné riziko pro dané sub-nebezpečí. Jedná se o hodnotu rizika, která k tomuto sub-nebezpečí byla přiřazena jako poslední. Pokud je tedy pro určitý faktor identifikováno již existující sub-nebezpečí, je následně riziko nově ohodnoceno. V takovém případě pak musí být na základě tohoto hodnocení upravena i hodnota rizika v obecnější tabulce registru nebezpečí.

Registr nebezpečí by měl být udržován oddělením provozní bezpečnosti (OPB). Toto oddělení zajišťuje, že obě tabulky registru nebezpečí obsahují vždy aktuální data.

Registr nebezpečí je navržen jako nástroj pro sledování stavu bezpečnosti v Údržbové organizaci. Umožňuje přehledné zobrazení dosud identifikovaných nebezpečí včetně hodnocení rizik. V případě potřeby zjištění detailnějších informací je k managementu organizace k dispozici tabulka (Tabulka 10), která poskytuje kompletní záznam z procesu identifikace nebezpečí a hodnocení rizik.

Využití systémového přístupu a systémových nebezpečí dává managementu možnost užití nově navrženého registru nebezpečí napříč celou Údržbovou organizací. Systémová nebezpečí jsou platná napříč odděleními a celou organizací. Registr nebezpečí ve formě tabulky podle Přílohy 4 je přehledným nástrojem pro sledování a řízení rizik v celém systému Údržbové organizace.

Nově navržený registr nebezpečí napomáhá OPB a vedení Údržbové organizace k řízení rizik. Navržený registr umožňuje sledovat identifikovaná nebezpečí a rizika napříč celou Údržbovou organizací.

9.3. Postup využití indikátorů bezpečnosti

Nově navržená sada indikátorů bezpečnosti (SPIs) byla vytvořena na základě výsledků analýzy STPA Údržbové organizace. Model řídící struktury byl zobrazen na úrovni ekvivalentní zobrazení struktury Údržbové organizace tak, jak ji uvádí Výklad organizace údržby (MOE). Nová sada obsahuje 5 nově navržených SPIs (Tabulka 13).

Nová sada SPIs nemá dosud zavedené hodnoty, které jsou pro společnost přijatelné, a které ne. Prvním krokem, před samotným zavedením nových SPIs do SMS Údržbové organizace je určení stanovených bezpečnostních cílů (safety targets). Tyto cíle je nutné stanovit s ohledem na celkové bezpečnostní cíle celé společnosti. Na nich by se mělo shodnout především vedení Údržbové organizace a oddělení provozní bezpečnosti. Je také potřeba zohlednit praktickou zkušenost z provozu, která umožní korigovat stanovené bezpečnostní cíle tak, aby byly v praxi dosažitelné.

Měření nově navržených indikátorů bezpečnosti by mělo probíhat průběžně tak, jak jsou nastaveny jednotlivé intervaly. Oddělení provozní bezpečnosti zajistí, že požadované hodnoty SPIs budou pravidelně zaznamenávány v přehledné formě. Údržbová organizace již nyní využívá zobrazení SPIs pomocí grafů, které zobrazují průběh času na ose x a měřené hodnoty SPIs na ose y. Tato forma záznamu přehledně ukazuje minulý vývoj a měla by být využita i pro současné SPIs.

Pomocí navržených SPIs lze sledovat výkonnost v bezpečnosti systému Údržbové organizace tak, jak byl nastaven v době, kdy byl analyzován. Pokud dojde ke změně systému nebo jeho částí, je nutné SPIs aktualizovat. Změna systému by mohla vést k tomu, že aktuálně využívané SPIs nebudou již pro takový systém relevantní nebo nebudou odrážet stav výkonnosti v bezpečnosti celého systému.

Pro aktualizaci SPIs je nejprve nutné znovu analyzovat celý systém. K tomu by měla být využita systémová metoda, kterou je právě STPA. Na základě výsledků této analýzy by měla být provedena revize stávajících SPIs a zhodnocení, zda měří výkonnost v bezpečnosti celého systému. Pokud systém zůstává nezměněn a SPIs jsou navrženy tak, že měří celkovou výkonnost v bezpečnosti systému, není nutné je aktualizovat. Revize SPIs a analýza systému Údržbové organizace však zajistí kontrolu správné funkce SPIs, proto by měla být oddělením provozní bezpečnosti prováděna v pravidelných intervalech.

10. Diskuse

Předkládaná práce představuje postup a technické nástroje tří vybraných částí systému provozní bezpečnosti (SMS) konkrétní údržbové organizace schválené dle Part-145 Nařízení (EU) 1321/2014 pomocí systémového přístupu. Po analýze současného stavu SMS v Údržbové organizaci byly vybrány části SMS s největším potenciálem pro další vývoj. V rámci práce byl navržen nový postup identifikace nebezpečí a hodnocení rizik, nový registr nebezpečí a sada nových indikátorů bezpečnosti (SPIs).

Systém Údržbové organizace byl analyzován pomocí metody STPA. Analýza STPA Údržbové organizace byla provedena obecněji. Model řídící struktury byl zobrazen na podobné úrovni, jak je uvedený ve výkladu organizace (MOE) Údržbové organizace. Obecnější zobrazení organizace nachází výhodu v relativně nízkém počtu nebezpečných řídících akcí a ztrátových scénářů. Analýza tak neobsahuje příliš velké množství dat a je přehledná. Na druhou stranu je v takovém zobrazení ztracen detail, který lze vidět až rozčleněním některých sub-systémů na další dílčí prvky. Příkladem je například sub-systém údržby na základně, která je v STPA zobrazena jako „BM Team“ (tým těžké údržby). V takovém zobrazení není možné analyzovat jednotlivé procesy, které probíhají v rámci těžké údržby.

Navržený proces identifikace nebezpečí a hodnocení rizik je zcela odlišný od stávajícího procesu v Údržbové organizaci. Během dosavadní identifikace nebezpečí neměl hodnotící manažer (RM) k dispozici žádný dostupný seznam dosud identifikovaných nebezpečí. Nový návrh identifikace nebezpečí přináší 19 systémových nebezpečí vytvořených na základě legislativních požadavků na údržbové organizace. Detailnější sub-nebezpečí jsou udržována v registru, který má při identifikaci RM k dispozici. Možnost výběru již identifikovaných nebezpečí zabraňuje duplicitě nebezpečí v registru a také zjednodušuje hodnotícím manažerům (RM) celý proces.

Jako vstup do procesu identifikace nebezpečí byl navržen kauzální faktor. Ten by měl být na základě tohoto návrhu výstupem z procesu šetření události. Tato práce se procesem

šetření událostí nezabývá a tento proces je tedy předmětem pro další možný vývoj SMS v Údržbové organizaci.

V rámci hodnocení rizik bylo vynecháno hodnocení pravděpodobnosti. Tato proměnná byla nahrazena hodnocením efektivity nápravných opatření. Pravděpodobnost rizika je velmi náročné odhadnout. Hodnotící manažer se může opírat pouze o retrospektivní data, která však nemohou garantovat možný budoucí vývoj. Hodnocení efektivity nápravných opatření tak dává možnost zaměřit se na konkrétní návrh opatření a ohodnotit, jak toto opatření přispěje ke snížení rizika. Navržené stupnice hodnot závažnosti a efektivity nápravných opatření mohou být v budoucnu přizpůsobeny potřebám Údržbové organizace.

Současný návrh procesu identifikace nebezpečí a hodnocení rizik není přizpůsoben internímu softwaru Údržbové organizace, který je v současnosti využíván pro sběr a uchování dat. Pro plné začlenění nového návrhu do Údržbové organizace je třeba upravit stávající dedikovaný software a přeprogramovat jej, aby mohl být využit k nově navrženému řešení. To je také jedna z limitací tohoto návrhu.

Nový registr nebezpečí je navržen ve dvou formách tabulek. První forma je přehledným nástrojem pro sledování nebezpečí a rizik napříč celým systémem Údržbové organizace. Tato forma tabulky neobsahuje detailní informace o jednotlivých událostech, nicméně řeší jeden z problémů stávajícího registru nebezpečí, a to vysoký počet záznamů (řádků). Aby byl v rámci registru nebezpečí zachován detail, byla navržena druhá podrobnější tabulka, která obsahuje přehledně veškerá data z procesu identifikace nebezpečí a hodnocení rizik jednotlivých událostí.

Navržená sada indikátorů bezpečnosti (SPIs) vychází z výsledků analýzy STPA. SPIs umožňují vedení společnosti a OPB sledovat výkonnost v oblasti bezpečnosti. Nová sada SPIs má smysl především při sledování výkonnosti Údržbové organizace jako celku. Je tomu především proto, že model řídící struktury při STPA byl zobrazen s nižší mírou detailu na konkrétní procesy v rámci jednotlivých částí Údržbové organizace.

Nově nastavené indikátory bezpečnosti (SPIs) nejsou rozděleny dle jednotlivých sub-systémů organizace, kterými mohou být různá oddělení, dílny, týmy nebo jiné celky

organizace. Pro podrobnější sledování výkonnosti v oblasti bezpečnosti jednotlivých sub-systémů je potřeba analyzovat podrobněji konkrétní sub-systém a dle toho nastavit míru detailu zobrazení modelu řídící struktury během analýzy STPA.

Všech 5 nově navržených SPIs je typu lagging. To jsou takové indikátory, které nemá Údržbová organizace přímo pod kontrolou a vstupuje do nich složka, kterou organizace nedokáže ovlivnit. Navržená sada neobsahuje žádné indikátory typu leading především z důvodu jejich složité měřitelnosti. Dalším důvodem vynechání leading indikátorů je příliš obecná analýza celkového systému. Pro návrh leading indikátorů bezpečnosti je důležité znát podrobně veškeré procesy a technické vlastnosti systému. Provedení podrobné STPA analýzy, kde by model řídící struktury obsahoval jednotlivé elementární prvky sub-systémů, by mohlo ukázat mnohem podrobnější výstupy analýzy. Na základě těchto výstupů by pak mohla být určena řada leading indikátorů, za předpokladu, že budou měřitelné.

Předložené návrhy je možné aplikovat také na SMS Organizace zachování letové způsobilosti (CAMO), která se schválenými údržbovými organizacemi (AMO) úzce spolupracuje v rámci zachování letové způsobilosti. Navržené postupy a nástroje v této práci se však zaměřují výhradně na konkrétní AMO a neuvažují procesy CAMO organizací. V budoucím vývoji SMS by pak řada navržených nástrojů mohla být společná pro AMO i CAMO.

Navržené postupy a nástroje byly validovány diskusí s odborníkem z praxe. V rámci validace navrženého řešení bylo vzneseno několik dotazů a připomínek k navrženým řešením.

10.1. Validace

Předložené návrhy byly validovány manažerem oddělení Quality and Safety společnosti ABS Jets, která je také schválenou údržbovou organizací (AMO) dle Part-145 Nařízení (EU) 1321/2014. K předloženým návrhům bylo ze strany manažera vzneseno několik připomínek:

Výběr nebezpečí ze seznamu může v praxi vést ke snížení kvality identifikace nebezpečí ze strany příslušného hodnotícího vedoucího (RM). Mohlo by se stát, že RM bude pouze vybírat z již identifikovaných nebezpečí, aby si usnadnil práci.

Předdefinované systémové nebezpečí není jediným a konečným nebezpečím. Po přiřazení systémového nebezpečí je nutné stanovit sub-nebezpečí. Pokud již k danému systémovému nebezpečí byl identifikován větší počet sub-nebezpečí, mohlo by dojít ze strany RM k výběru bez předchozí úvahy. Tato situace má dvě řešení. První řešení je již obsaženo v samotném návrhu procesu. Jedná se o kontrolu a ověření správně identifikovaných nebezpečí. Toto ověření zajišťuje příslušné oddělení provozní bezpečnosti (OPB). Druhým řešením tohoto problému je přidání dalšího kroku před výběr systémového nebezpečí. V rámci tohoto kroku by RM prvotně navrhl konkrétní sub-nebezpečí bez znalosti a přístupu k seznamu již existujících sub-nebezpečí.

Jsou systémová nebezpečí tvořená podle Nařízení (EU) 1321/2014 kompletní?

Systémová nebezpečí byla navržena na základě požadavků na údržbové organizace obsažené v Nařízení (EU) 1321/2014. Navržená systémová nebezpečí jsou členěna do kategorií podle kapitol Part-145 tohoto nařízení. V případě, že by se časem ukázalo, že seznam nebezpečí není kompletní a je opomenuto některé systémové nebezpečí, je možné toto nebezpečí do seznamu kdykoliv doplnit. Pokud by také Údržbová organizace dospěla k závěru, že seznam obsahuje některé nebezpečí, které se jí netýká nebo je toto nebezpečí již obsaženo v jiném systémovém nebezpečí, může být ze seznamu odstraněno. Přidání ani odstranění systémových nebezpečí ze seznamu nenaruší funkci registru nebezpečí a ten může být dále využíván podle navržených postupů.

Zpoždění údržby měřené v indikátorech č.1 a č.2 by bylo možné měřit také vzhledem k jednotlivým úkolům údržby (Taskům). Aplikace, které využívají údržbové organizace umožňují měření délky trvání jednotlivých úkolů.

Měření zpoždění údržby vzhledem jednotlivým úkolům údržby by mohlo přinést průběžné informace o celkovém zpoždění údržby (projektu). Celkové zpoždění by tím mohla organizace ovlivnit již v zárodku. Takový indikátor by však vyžadoval velmi časté měření

a sledování, minimálně každý den. Velmi náročné by také bylo zajištění spolehlivosti záznamů v aplikaci. Pokud by došlo například k opomenutí některých časových záznamů (délky úkonu), informace o zpoždění by tak neodpovídala skutečnému zpoždění.

Přetížení nebo nevytížení techniků (viz. Indikátor č. 3) by bylo možné měřit pomocí efektivity techniků v závislosti na směnách. K tomu by bylo možné využít systémy, kam se technici přihlašují, a které počítají celkový čas strávený údržbou.

Takto navržený indikátor by zajistil mnohem přesnější údaje o přetížení či nevyužití techniků. Indikátor by dokázal měřit reálný čas strávený prací a nezapočítával by do celkového času přestávky. Problémem by opět mohlo být zajištění pravdivosti údajů uvedených v systému. Pokud by se pracovník zapomněl přihlásit nebo odhlásit ze systému, data v tomto systému by neodpovídala realitě.

Předložené návrhy úprav systému řízení provozní bezpečnosti konkrétní údržbové organizace byly shledány jako využitelné v praxi. To potvrzuje validační dokument obsažený v Příloze 5.

Závěr

Práce je zaměřena na vývoj vybraných částí systému řízení provozní bezpečnosti (SMS) vybrané schválené údržbové organizace. Aby bylo možné zvolit části SMS s největším potenciálem pro vývoj, bylo nutné analyzovat současný stav SMS vybrané údržbové organizace. Analýza současného stavu probíhala systémově. To znamená, že byl SMS analyzován jako celek. K analýze byly využity veškeré prostředky poskytnuté údržbovou organizací. Dostupným podkladem pro analýzu byla kompletní interní dokumentace společnosti. Dále byl SMS představen a vysvětlen vedoucím provozní bezpečnosti. V další fázi analýzy pak bylo analyzováno využití SMS v provozu údržbové organizace. Bylo umožněno účastnit se důležitých procesů, jako například procesu hodnocení a řízení rizik v návaznosti na konkrétní události. Dále bylo umožněno klást otázky na personál organizace a zjistit tak, jak je současný SMS ve společnosti vnímán a prakticky využíván.

Na základě systémové analýzy současného stavu SMS bylo identifikováno několik částí, jejichž vývoj by pro vybranou údržbovou organizaci mohl být přínosný. Tento předpoklad byl následně ověřen v údržbové organizaci. Pro vývoj řešený v rámci této práce byly vybrány tři části SMS, a to proces identifikace nebezpečí a hodnocení rizik, registr nebezpečí a indikátory bezpečnosti. Tyto tři části byly vybrány především vzhledem k jejich aktuálnímu stavu ve srovnání s ostatními identifikovanými částmi SMS. Dalším faktorem pro výběr právě těchto částí byla návaznost, se kterou mohou být tyto části vyvíjeny.

V rámci této práce byl navržen nový postup pro identifikaci nebezpečí a hodnocení rizik. Postup pro hodnocení využívá z velké části STPA-Informed Risk Matrix navrženou na americkém MIT. Tento postup nevyužívá těžce predikovatelnou pravděpodobnost rizika a nahrazuje jí hodnocením efektivity nápravných opatření. Pro proces identifikace nebezpečí bylo již předem navrženo 19 systémových nebezpečí, která jsou relevantní napříč celou údržbovou organizací. K těmto systémovým nebezpečím jsou dále během identifikace příslušným manažerem určena konkrétnější sub-nebezpečí, která přesněji popisují podstatu řešených událostí. Výhodou tohoto procesu je snadné třídění nebezpečí v rámci registru nebezpečí. Přiřazení systémových nebezpečí pak umožňuje sledovat stav

bezpečnosti napříč celou organizací a identifikovat, které problémy trápí organizaci obecně. Limitací nově navrženého řešení je současný proces šetření událostí, který není obsahem této práce a zůstává tak nezměněn. Jakožto zdroj primárních dat pro proces identifikace nebezpečí a hodnocení rizik je nutné postup šetření událostí upravit tak, aby jeho výsledky byly dále plně využitelné.

Navržený registr nebezpečí se skládá ze dvou forem tabulek. Každá z nich obsahuje informace v rozdílných detailech. Oproti stávajícímu registru nebezpečí ve vybrané údržbové organizaci je nově navržený registr přehledný a dává možnost vidět problémy napříč celým systémem organizace, nikoliv jen v souvislosti s částí systému.

Provedená analýza STPA odhalila časté faktory, které mohou vést k nebezpečím a následným ztrátám. Na jejich základě pak byla navržena nová sada pěti indikátorů bezpečnosti. Tyto indikátory jsou typu lagging. Hlavním nedostatkem se ukázal být příliš obecný model řídící struktury, který nezobrazuje detailní procesy uvnitř sub-systémů údržbové organizace. To znemožnilo navrhnout i některé leading indikátory, které vyžadují detailnější znalost systému.

Výsledky diplomové práce byly validovány v praxi a byla prokázána jejich využitelnost. Diskutované připomínky, které byly vzneseny během validace práce, byly přijaty a vysvětleny. Na výsledky této diplomové práce může být navázáno dalším vývojem systému provozní bezpečnosti.

Reference

[1] INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). Annex 19 – Safety Management. 2nd edition. Montreal, Quebec: International Civil Aviation Organization, 2016. ISBN 978-92-9249-965-5.

[2] ICAO, Doc 9859, Safety Management Manual (SMM) Fourth Edition. Montreal, 2018. [cit. 2023-04-10]. ISBN 978-92-9249-214-4.

[3] SCOTT A. SNOOK. Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq. In: *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq*. 2000. ISBN 9780691095189.

[4] MINISTERSTVO DOPRAVY ČR. Předpis L19. Řízení bezpečnosti. 2013 [online]. [cit. 2023-04-15]. Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm

[5] ŠIBLOVÁ, Kristýna. Právní aspekty letecké dopravy v EU [online]. Brno, 2014 [cit. 2023-04-16]. Dostupné z: https://is.muni.cz/th/y0yz9/. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Vladimír TÝČ.

[6] DIB, Chahinez. Publication spotlight: The ICAO Annexes to the Convention on International Civil Aviation. In: Unitingaviation.com [online]. 28.2.2022 [cit. 2023-04-16]. Dostupné z: https://unitingaviation.com/news/safety/publication-spotlight-the-icao-annexes-to-the-convention-on-international-civil-aviation/

[7] EASA [online]. Úřad pro civilní letectví [cit. 2023-04-16]. Dostupné z: https://www.caa.cz/dokumenty/easa/

[8] Agentura Evropské unie pro bezpečnost letectví (EASA) [online]. Evropská unie [cit. 2023-04-16]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/easa_cs

[9] Zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/1997-49/

[10] Letecké předpisy [online]. Úřad pro civilní letectví [cit. 2023-04-16]. Dostupné z: https://www.caa.cz/dokumenty/predpisy/letecke-predpisy/

[11] NAŘÍZENÍ KOMISE (EU) č. 1324/2014, o zachování letové způsobilosti letadel a leteckých výrobků, letadlových částí a zařízení a schvalování organizací a personálu zapojených do těchto úkolů [online]. [cit. 2023-04-20] Dostupné z: https://eurlex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R1321&from=en

[12] Easy Access Rules for Continuing Airworthiness (Regulation (EU) No 1321/2014) [online]. European Union Aviation Safety Agency (EASA) [cit. 2023-04-20]. Dostupné z: https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-continuing-airworthiness

[13] Programy údržby pro transferovaná letadla [online]. Úřad pro civilní letectví [cit. 2023-04-20]. Dostupné z: https://www.caa.cz/letadlova-technika/pokracujici-letova-zpusobilost/program-udrzby-pro-transferovana-letadla/

[14] Programy údržby pro annexová letadla [online]. Úřad pro civilní letectví [cit. 2023-04-20]. Dostupné z: https://www.caa.cz/letadlova-technika/pokracujici-letova-zpusobilost/program-udrzby-pro-annexova-letadla/

[15] Pokračující letová způsobilost [online]. Úřad pro civilní letectví [cit. 2023-04-20]. Dostupné z: https://www.caa.cz/letadlova-technika/pokracujici-letova-zpusobilost/

[16] Aircraft Maintenance. In: SKYbrary Aviation Safety [online]. [cit. 2023-04-20]. Dostupné z: https://skybrary.aero/articles/aircraft-maintenance

[17] PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2021/1963, kterým se mění nařízení (EU) č. 1321/2014, pokud jde o systémy řízení bezpečnosti v organizacích údržby, a opravuje uvedené nařízení [online]. [cit. 2023-04-26] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32021R1963

[18] LEVESON, Nancy G. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. [cit. 2023-04-28] ISBN 978-0-262-01662-9.

[19] LEVESON, Nancy G. and John P. THOMAS. STPA Handbook [online]. 2018. [cit. 2023-04-28] Dostupné z: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[20] Eurocontrol, Systems Thinking for Safety: Ten Principles [online]. 2014. [cit. 2023-04-28] Dostupné z: https://www.skybrary.aero/bookshelf/books/2882.pdf

[21] Hollnagel, Erik. Safety-I and Safety-II: The Past and Future of Safety Management. CRC Press, 2014. ISBN 9781472423054

[22] LEVESON, Nancy G. Safety III: A Systems Approach to Safety and Resilience [online]. 2020. [cit. 2023-05-03]. Dostupné z: http://sunnyday.mit.edu/safety-3.pdf

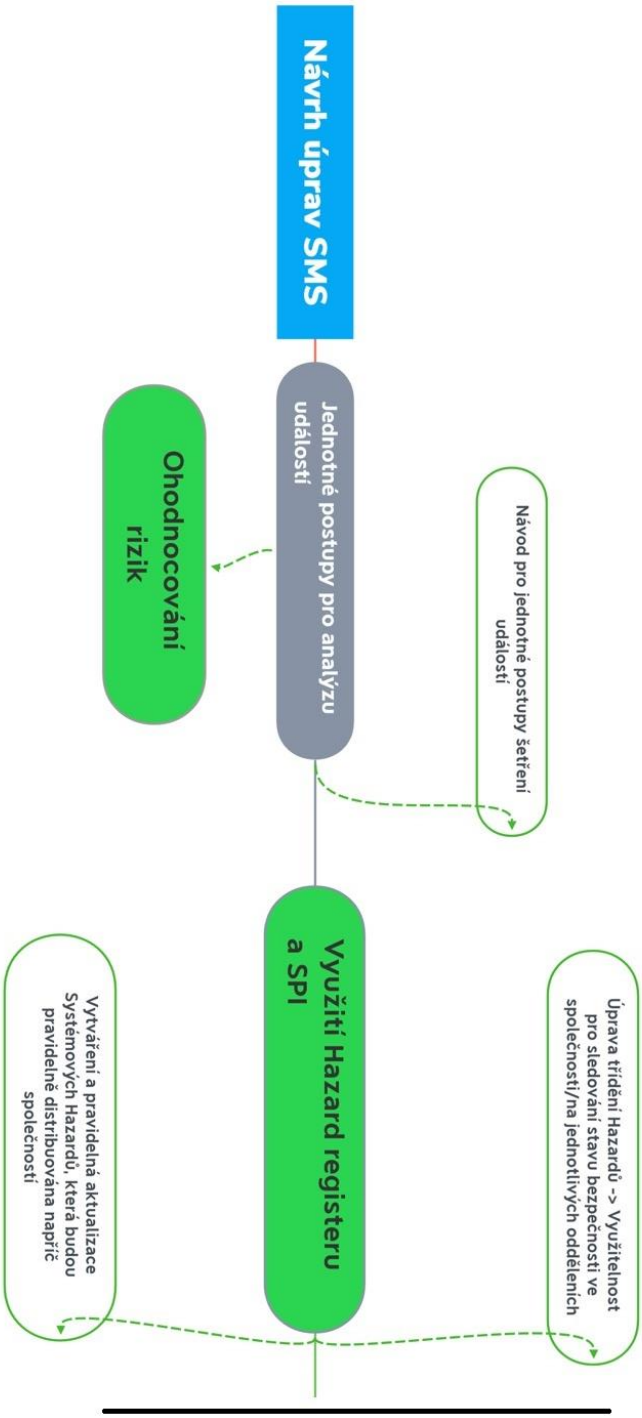
[23] Hollnagel, Erik. FRAM: the Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems, Taylor & Francis Group, 2012. ProQuest Ebook Central

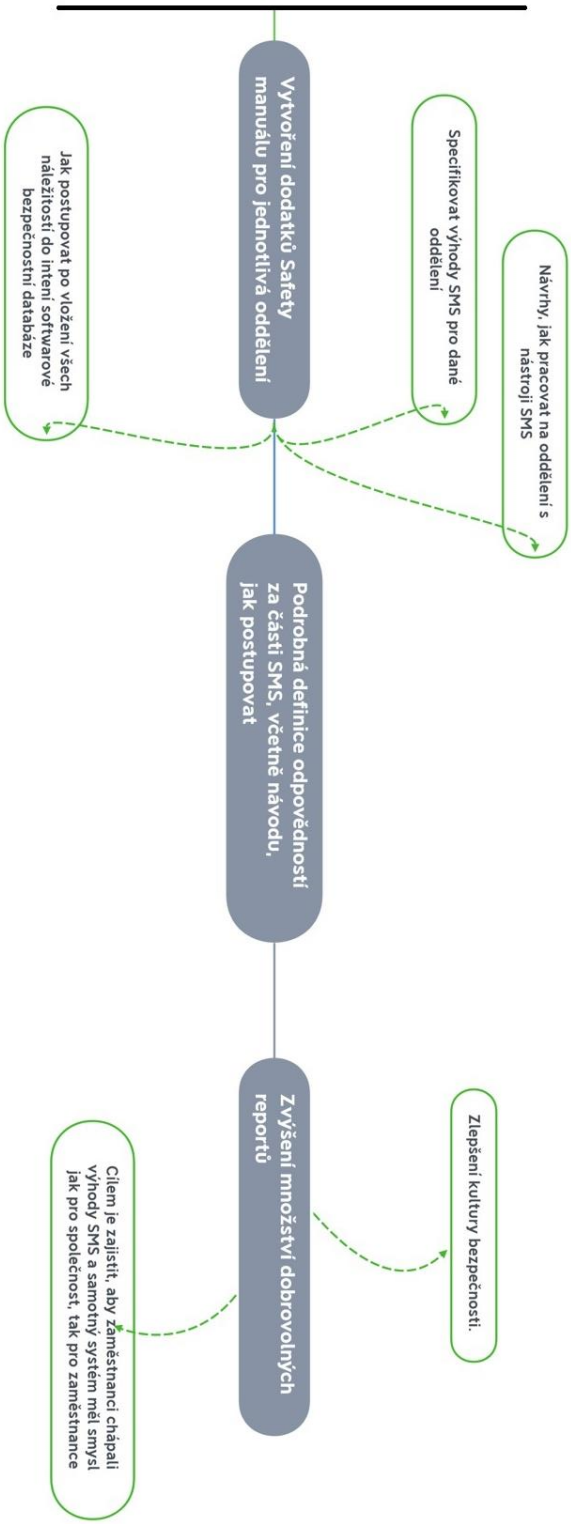
[24] HAVLÍČEK, Jakub. Hodnocení variability procesu bezpečnostní kontroly cestujících na letišti. Praha, 2020 [cit. 2023-05-03]. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/88214/F6-DP-2020-Havlicek-Jakub-DP_Havlicek.pdf?sequence=-1&isAllowed=y Diplomová práce. České vysoké učení technické v Praze. Fakulta dopravní. Vedoucí práce Andrej LALIŠ a Roman VOKÁČ.

[25] GREGORIAN, Dro J. and ŸOO, Sam M. A System-Theoretic Approach to Risk Analysis [online]. 2021 [cit. 2023-05-04]. Master's thesis. MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Vedoucí práce Joan Rubin. Dostupné z: https://dspace.mit.edu/bitstream/handle/1721.1/147729/yoo-samyoo-sm-sdm-2021-thesis.pdf?sequence=1&isAllowed=y

[26] NAŇÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 376/2014, o hlášení událostí v civilním letectví, analýze těchto hlášení a navazujících opatřeních [online]. [cit. 2023-05-09] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0376

Příloha 1: Mapa identifikovaných částí pro budoucí vývoj SMS Údržbové organizace




Vytvoření dodatků Safety manuálu pro jednotlivá oddělení
Specifikovat výhody SMS pro dané oddělení
Návrhy, jak pracovat na oddělení s nástroji SMS
Jak postupovat po vložení všech náležitostí do intení softwarové bezpečnostní databáze
Podrobná definice odpovědností za části SMS, včetně návodu, jak postupovat
Zvýšení množství dobrovolných reportů
Zlepšení kultury bezpečnosti.
Cílem je zajistit, aby zaměstnanci chápali výhody SMS a samotný systém měl smysl jak pro společnost, tak pro zaměstnance

Příloha 2: Nebezpečné řídící akce (UCA)

Řídící akce	Neposkytnutí řídící akce vede k nebezpečí			Poskytnutí řídící akce vede k nebezpečí			Řídící akce provedená brzy/pozdě vede k nebezpečí			Řídící akce trvá dlouho nebo krátce		
	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis
Technický ředitel (CTO) nařídí týmu Údržby na základně (BM Team) provedení údržby.				1	H-2	CTO nařídí BM Teamu provedení údržby, když není dostupný díl.						
Technický ředitel (CTO přidělí finanční zdroje týmu Údržby na základně (BM Team).	2	H-1, H-2	CTO nepřidělí dostatek finančních zdrojů BM Teamu.									
Tým Údržby na základně (BM Team) provede údržbu.	3	H-1	BM Team neprovede údržbu LC.	4	H-1, H-2	BM Team provede údržbu, když není dostatek odborného personálu (Techniků).				5	H-2	BM Team provádí údržbu déle, než byl plán práce.
				6	H-1, H-2	BM Team provede údržbu, když odborný personál nemá potřebné vybavení.						

Řídící akce	Neposkytnutí řídící akce vede k nebezpečí			Poskytnutí řídící akce vede k nebezpečí			Řídící akce provedená brzy/pozdě vede k nebezpečí			Řídící akce trvá dlouho nebo krátce		
	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis
Tým Údržby na základně (BM Team) provede údržbu.				7	H-1	BM Team provede údržbu, když odborný personál nezná správné postupy.						
Tým Údržby na základně (BM Team) uvolní do provozu letadlový celek (LC) nebo celé Letadlo.				8	H-1	BM Team uvolní do provozu LC nebo A/C, když LC nebo A/C je v neprovozus chopném stavu.	9	H-2	BM Team uvolní do provozu LC nebo A/C pozdě po plánovaném dokončení údržby.			
Tým Údržby na základně (BM Team) nařizuje objednání náhradních dílů.	10	H-2	BM Team nenařídí objednání náhradních dílů.	11	H-2	BM Team nařídí objednání náhradních dílů, když nejsou potřeba.	12	H-2	BM Team nařídí objednání náhradních dílů pozdě po zjištění, že je díl potřebný.			
Tým Produkčního plánování (PP Team) plánuje posloupnost prací a časové rozpětí prací.				13	H-1	PP Team plánuje posloupnost prací a časové rozpětí prací, když klient mění své požadavky.						

Řídící akce	Neposkytnutí řídící akce vede k nebezpečí			Poskytnutí řídící akce vede k nebezpečí			Řídící akce provedená brzy/pozdě vede k nebezpečí			Řídící akce trvá dlouho nebo krátce		
	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis
				14	H-2	PP Team plánuje údržbu, když není dostatek náhradních dílů.						
				15	H-1, H-2	PP Team plánuje posloupnost prací a časové rozpětí prací, když je nedostatek odborného personálu.						
Tým Traťové údržby (LM Team) provede údržbu.	16	H-1	LM Team neprovede údržbu.	17	H-1, H-2	LM Team provede údržbu, když odborný personál nemá dostatečné vybavení.						
				18	H-1, H-2	LM Team provede údržbu, když odborný personál nezná správné postupy.						

Řídící akce	Neposkytnutí řídící akce vede k nebezpečí			Poskytnutí řídící akce vede k nebezpečí			Řídící akce provedená brzy/pozdě vede k nebezpečí			Řídící akce trvá dlouho nebo krátce		
	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis	UCA	H*	Popis
Tým Traťové údržby (LM Team) aplikuje MEL/CDL.				19	H-1	LM Team aplikuje MEL/CDL, když ostatní části systému nejsou v provozusch opném stavu.						
				20	H-2	LM Team aplikuje MEL/CDL, když nezná letový plán.						
Tým Technické podpory fakturuje a účtuje provedení údržby klientovi.	21	H-2	Tým Technické podpory nefakturuje a neúčtuje provedení údržby klientovi.	22	H-2	Tým Technické podpory fakturuje a účtuje provedení údržby klientovi, když nezná cenu, za kterou byla údržba nabízena.						
Obchodní tým oslovuje klienty a prodává údržbu.	23	H-2	Obchodní tým neoslovuje klienty a neprodává údržbu.	24	H-1, H-2	Obchodní tým oslovuje klienty a prodává údržbu, když v údržbě nejsou volné kapacity.	25	H-1, H-2	Obchodní tým oslovuje klienty a prodá údržbu brzy před dokončením předchozí.			

Příloha 3: Ztrátové scénáře

UCA #	Popis UCA	Scénáře
1	CTO nařídí BM Teamu provedení údržby, když není dostupný díl.	Scénář 1 pro UCA 1: CTO nařídí provedení údržby, protože Logistický Team nezajistil dostupnost náhradního dílu. CTO o tomto stavu nebyl informován z důvodu nesprávné komunikace. V důsledku toho dojde ke zdržení či neschopnosti provedení údržby. (L-1, L-2, L-3, L-4)
2	CTO nepřidělí dostatek finančních zdrojů BM Teamu.	Scénář 1 pro UCA 2: CTO nepřidělí dostatek finančních zdrojů BM Teamu, protože je vedením společnosti nucen šetřit. BM Team nemá dostatek finančních zdrojů na nákup nářadí či technického vybavení, které je potřebné pro úkony údržby. (L-1, L-2, L-4, L-5) Scénář 2 pro UCA 2: CTO nepřidělí dostatek finančních zdrojů BM Teamu, protože je vedením společnosti nucen šetřit. BM Team nemá dostatek finančních zdrojů pro nábor zaměstnanců, což způsobí nízký stav pracovníků a práci pod tlakem. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5)
3	BM Team neprovede údržbu LC.	Scénář 1 pro UCA 3: BM Team neprovede údržbu a údržbový proces, protože tento proces chybí v seznamu úkolů od PP Teamu. To vede k uvolnění letadla do provozu v nezpůsobilém stavu a k následným ztrátám. (L-1, L-2, L-3, L-4)

UCA #	Popis UCA	Scénáře
4	BM Team provede údržbu, když není dostatek odborného personálu (Techniků).	Scénář 1 pro UCA 4: Organizace pracuje na více projektech, než zvládne personální kapacita, aby došlo ke zvýšení zisku organizace. Nedostatek odborného personálu (Techniků) způsobí časovou tíseň. Technici pracují pod tlakem, aby se zabránilo zpoždění údržby. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5) Scénář 2 pro UCA 4: Organizace pracuje na více projektech, než zvládne personální kapacita, aby došlo ke zvýšení zisku organizace. Nedostatek odborného personálu (Techniků) však způsobí zpoždění údržby. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. Samotný nedostatek odborného personálu způsobí ztrátu důvěry personálu v zaměstnavatele. (L-2, L-3, L-4, L-5)

UCA #	Popis UCA	Scénáře
5	BM Team provádí údržbu déle, než byl plán práce.	Scénář 1 pro UCA 5: BM Team provádí údržbu déle, než byl plán práce, protože nemá dostatek odborného personálu. Vznikne zpoždění údržby. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4) Scénář 2 pro UCA 5: BM Team provádí údržbu déle, než byl plán práce, protože nemá dostatek odborného personálu. V důsledku toho vznikne zpoždění údržby od počátku navazující údržby jiného letounu. To způsobí tlak na personál. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5)
6	BM Team provede údržbu, když odborný personál nemá potřebné vybavení.	Scénář 1 pro UCA 6: Potřebné vybavení není dostupné z důvodu nízkého finančního rozpočtu oddělení Údržby na základně. Provedení údržby bez potřebného vybavení (nářadí, technika) přiměje Techniky použít alternativní vybavení, které není určené k provedení daných úkonů. Použití nevyhovující techniky, která není určená k daným úkonům následně povede k nesprávnému provedení údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4, L-5)

UCA #	Popis UCA	Scénáře
7	BM Team provede údržbu, když odborný personál nezná správné postupy.	Scénář 1 pro UCA 7: Personál (Technici) je nedostatečně vyškolen pro daný úkon. Údržba daného letadlového celku je provedena v rozporu s manuálem či postupy údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4) Scénář 2 pro UCA 7: Personál (Technici), který je nedostatečně vyškolen pro daný úkon, pomáhá Technikům, který je dostatečně vyškolen pro daný úkon. V důsledku nedostatečné komunikace provede nedostatečně vyškolený personál údržbu daného letadlového celku v rozporu s manuálem či postupy údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4)
8	BM Team uvolní do provozu LC nebo A/C, když LC nebo A/C je v neprovozuschopném stavu.	Scénář 1 pro UCA 8: BM Team uvolní do provozu LC nebo A/C, když LC nebo A/C je v neprovozuschopném stavu, protože personál nemá dostatečné vybavení pro zjištění závady. To vede ke ztrátám. (L-1, L-2, L-3, L-4)

UCA #	Popis UCA	Scénáře
9	BM Team uvolní do provozu LC nebo A/C pozdě po plánovaném dokončení údržby.	Scénář 1 pro UCA 9: BM Team uvolní do provozu LC nebo A/C pozdě po plánovaném dokončení údržby, protože není dostatek odborného personálu. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4) Scénář 2 pro UCA 9: BM Team uvolní do provozu LC nebo A/C pozdě po plánovaném dokončení údržby, protože tým Logistiky neobjednal náhradní díl. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4)
10	BM Team nenařídí objednání náhradních dílů.	Scénář 1 pro UCA 10: BM Team nenařídí objednání náhradních dílů, protože v softwarovém systému údržby vidí jeho dostupnost na skladě. V reálu ale díl dostupný není. To vede ke zpoždění údržby. (L-2, L-3, L-4)
11	BM Team nařídí objednání náhradních dílů, když nejsou potřeba.	Scénář 1 pro UCA 11: BM Team nařídí objednání náhradních dílů, když nejsou potřeba, protože byla objednána údržba daného dílu a BM Team se bez kontroly předem domnívá, že díl bude nutné vyměnit. To může způsobit finanční ztrátu. (L-2)

UCA #	Popis UCA	Scénáře
12	BM Team nařídí objednání náhradních dílů pozdě po zjištění, že je díl potřebný.	Scénář 1 pro UCA 12: BM Team nařídí objednání dílu pozdě, protože nezná dostupnost dílu na trhu v důsledku nedostatečné komunikace s týmem Logistiky. BM Team předpokládá rychlé dodání, když to není možné. To způsobí zpoždění a možné finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4)

UCA #	Popis UCA	Scénáře
13	PP Team plánuje posloupnost prací a časové rozpětí prací, když klient mění své požadavky.	Scénář 1 pro UCA 13: Klient často mění své požadavky (technické a časové), protože smlouva o provedení údržby mu to umožňuje. V důsledku toho vzniká tlak na PP Team, který následně nehospodárně či v rozporu s legislativou a předpisy provede plánování údržby a správu dokumentace. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4) Scénář 2 pro UCA 13: Klient často mění své požadavky (technické a časové), protože smlouva o provedení údržby mu to umožňuje. Změny v plánování údržby vedou k nekontinuitní posloupnosti Tasků a procesů údržby, což má za následek zpoždění údržby. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4) Scénář 3 pro UCA 13: Klient často mění své požadavky (technické a časové), protože smlouva o provedení údržby mu to umožňuje. V důsledku toho vzniká tlak na BM Team. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5)
14	PP Team plánuje údržbu, když není dostatek náhradních dílů.	Scénář 1 pro UCA 14: Příčinou je neznalost stavu skladu PP Teamu v důsledku nedostatečné komunikace s týmem Logistiky. To může vést k finančním ztrátám a ztrátám reputace společnosti. (L-2, L-4)

UCA #	Popis UCA	Scénáře
15	PP Team plánuje posloupnost prací a časové rozpětí prací, když je nedostatek odborného personálu.	Scénář 1 pro UCA 15: PP Team plánuje posloupnost prací a časové rozpětí prací, když je nedostatek odborného personálu, protože Obchodní tým uzavřel více smluv o provedení údržby, než je organizace s ohledem na kapacitu personálu schopna pojmout. Příčinou toho je nedostatečná komunikace mezi Obchodním týmem a týmem Produkčního plánování. Nedostatek odborného personálu (Techniků) znemožní dodržet původně navržený plán práce a dodržet tak čas údržby, kterou si klient objednal. To způsobí finanční ztráty, ztrátu reputace společnosti a možnou ztrátu zákazníka. (L-2, L-3, L-4) Scénář 2 pro UCA 15: PP Team plánuje posloupnost prací a časové rozpětí prací, když je nedostatek odborného personálu, protože se předchozí údržbová zakázka zpozdila a není možné tak využít plnou kapacitu personálů na provedení nové zakázky. To způsobí finanční ztráty, ztrátu reputace společnosti a ztrátu zákazníka. (L-2, L-3, L-4)

UCA #	Popis UCA	Scénáře
16	LM Team neprovede údržbu.	Scénář 1 pro UCA 16: LM Team pošle letadlo do těžké údržby, když daný problém šlo vyřešit lehnou údržbou/opravou LC. Příčinou toho je velké množství letadel a časová tíseň. To způsobí zvýšené náklady a finanční ztrátu. (L-2) Scénář 2 pro UCA 16: LM Team neprovede údržbu, protože je na něj vyvíjen časový nátlak ze strany klienta. LM namísto údržby aplikuje MEL/CDL, což může vést k nehodě. (L-1, L-2, L-4) Scénář 3 pro UCA 16: LM Team neprovede údržbu, protože je na něj vyvíjen časový nátlak ze strany klienta. LM namísto údržby aplikuje MEL/CDL, což může zapříčinit, že letoun uvízne na cizím letišti, kde mu uplyne platnost MEL/CDL. To způsobí nespokojenost zákazníka a jeho možnou ztrátu a také finanční ztrátu. (L-2, L-3)
17	LM Team provede údržbu, když odborný personál nemá dostatečné vybavení.	Scénář 1 pro UCA 17: Potřebné vybavení není dostupné z důvodu nízkého finančního rozpočtu oddělení Traťové údržby. Provedení údržby bez potřebného vybavení (nářadí, technika) přiměje Techniky použít alternativní vybavení, které není určené k provedení daných úkonů. Použití nevyhovující techniky, která není určená k daným úkonům následně povede k nesprávnému provedení údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4, L-5)

UCA #	Popis UCA	Scénáře
18	LM Team provede údržbu, když odborný personál nezná správné postupy.	Scénář 1 pro UCA 18: Personál (Technici) je nedostatečně vyškolen pro daný úkon. Údržba daného letadlového celku je provedena v rozporu s manuálem či postupy údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4) Scénář 2 pro UCA 18: Personál (Technici), který je nedostatečně vyškolen pro daný úkon, pomáhá Technikům, který je dostatečně vyškolen pro daný úkon. V důsledku nedostatečné komunikace provede nedostatečně vyškolený personál údržbu daného letadlového celku v rozporu s manuálem či postupy údržby. To má za následek uvolnění letadla / letadlového celku v neprovozuschopném stavu. (L-1, L-2, L-3, L-4)

UCA #	Popis UCA	Scénáře
19	LM Team aplikuje MEL/CDL, když není ostatní části systému nejsou v provozuschopném stavu.	Scénář 1 pro UCA 19: LM Team aplikuje MEL/CDL na část systému, jejíž porucha byla odhalena. Tato porucha zakrývá komplexnější poruchu daného systému nebo poruchu jiného systému, na který nelze uplatnit MEL/CDL. Příčinou toho je nedostatečně zkušený a vyškolený personál. (L-1, L-2, L-3, L-4) Scénář 2 pro UCA 19: LM Team aplikuje MEL/CDL na část systému, jejíž porucha byla odhalena. Tato porucha zakrývá komplexnější poruchu daného systému nebo poruchu jiného systému, na který nelze uplatnit MEL/CDL. Příčinou toho je nedostatečné technické vybavení, které by umožnilo poruchu identifikovat. (L-1, L-2, L-3, L-4)
20	LM Team aplikuje MEL/CDL, když nezná letový plán.	Scénář 1 pro UCA 20: LM Team aplikuje MEL/CDL, což umožní přelet letounu do klientem zvolené destinace. Platnost MEL/CDL však skončí v dané destinaci, což má za následek nutnost objednání údržby od jiné MRO či vyslání techniků do dané destinace. Příčinou toho je nedostatečná komunikace mezi LM Teamem a provozním oddělením. (L-2)
21	Tým Technické podpory nefakturuje a neúčtuje provedení údržby klientovi.	Scénář 1 pro UCA 21: Tým Technické podpory nefakturuje a neúčtuje provedení údržby klientovi, protože neví, že daná údržba nebo úkony byly provedeny. Příčinou toho je nedostatečná komunikace s týmem Údržby na základně. Důsledkem je finanční ztráta. (L-2)

UCA #	Popis UCA	Scénáře
22	Tým Technické podpory fakturuje a účtuje provedení údržby klientovi, když nezná cenu, za kterou byla údržba nabízena.	Scénář 1 pro UCA 22: Tým Technické podpory nezná přesnou cenu, za kterou byla údržba nabízena, v důsledku nedostatečné komunikace s Obchodním oddělením. To vede k finanční ztrátě v případě, že je cena příliš nízká. V případě příliš vysoké ceny pak může být zákazník nespokojen. (L-2, L-3, L-4)
23	Obchodní tým neoslovuje klienty a neprodává údržbu.	Scénář 1 pro UCA 23: Obchodní tým neoslovuje zákazníky s nabídkou údržby, když kapacita údržbové organizace byla naplněna. Příčinou toho je nedostatečné plánování. To vede k prudkému úbytku zakázek údržby po dokončení dosud sjednaných údržeb. To zapříčiní finanční ztráty. (L-2)
24	Obchodní tým oslovuje klienty a prodává údržbu, když v údržbě nejsou volné kapacity.	Scénář 1 pro UCA 24: Obchodní tým prodává údržbu, když v údržbě nejsou volné kapacity. Příčinou toho je zpoždění předchozích zakázek a nedostatečná průběžná komunikace s týmem Údržby na základně nebo týmem Traťové údržby. Důsledkem je časový tlak na personál. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5)

UCA #	Popis UCA	Scénáře
25	Obchodní tým oslovuje klienty a prodá údržbu brzy před dokončením předchozí.	Scénář 1 pro UCA 25: Obchodní tým prodá údržbu nového letadla na termín, kdy ještě probíhá údržba na jiném letadle. Příčinou toho je zpoždění předchozích zakázek. To způsobí od počátku přijetí nového letadla do údržby zpoždění nových zakázek. To způsobí pak tlak na personál. Práce pod tlakem může zapříčinit opomenutí některých procesů či jejich nesprávné provedení. (L-1, L-2, L-4, L-5) Scénář 2 pro UCA 25: Obchodní tým prodá údržbu nového letadla na termín, kdy ještě probíhá údržba na jiném letadle. Příčinou je nedostatečná průběžná komunikace s týmem Údržby na základně nebo týmem Traťové údržby. To způsobí od počátku přijetí nového letadla do údržby zpoždění. V důsledku toho jsou v ohrožení finanční ztráty, ztráta reputace společnosti a možná ztráta zákazníka. (L-2, L-3, L-4)

Příloha 4: Tabulka registru nebezpečí

Category	System level Hazard ID	System level Hazard	Sub-Hazard ID	Sub-Hazard	Causal factor (Fa)	Current Risk
Terms of approval and scope of work	**H-1**	**The organisation does not comply with the terms of approval attached to the organisation certificate issued by the competent authority, and with the scope of work specified in the MOE.**				
Facilities	**H-2**	**The organisation does not ensure the working environment including aircraft hangars, component workshops and office accommodation is appropriate for the task carried out and in particular special requirements observed.**				
Personnel requirements	**H-3**	**The organisation does not define accountabilities and responsibilities of the employees. (e.g., The management structure of the organisation is not defined.)**				
Certifying staff and support staff	**H-4**	**The organisation does not ensure that certifying staff and support staff have an adequate understanding of the relevant aircraft or components, or both, to be maintained and of the associated organisation procedures.**				

Category	System level Hazard ID	System level Hazard	Sub-Hazard ID	Sub-Hazard	Causal factor (Fa)	Current Risk
Equipment and tools	**H-5**	**The organisation does not have available and use the necessary equipment and tools to perform the approved scope of work.**				
Components	**H-6**	**The organisation does not ensure that all components are classified into the categories according to Part M.**				
	H-7	**The organisation does not establish procedures for the acceptance of components, standard parts and materials for installation to ensure that components, standard parts and materials are in satisfactory condition.**				
Maintenance data	**H-8**	**The organisation does not hold and use applicable current maintenance data which is necessary in the performance of maintenance, including modifications and repairs.**				
	H-9	**The organisation does not ensure that all applicable maintenance data is readily available for use when required by maintenance personnel.**				
Production planning	**H-10**	**The organisation does not have a system appropriate to the amount and complexity of work to plan the availability of all necessary personnel, tools, equipment, material, maintenance data and**				

Category	System level Hazard ID	System level Hazard	Sub-Hazard ID	Sub-Hazard	Causal factor (Fa)	Current Risk
		facilities in order to ensure the safe completion of the maintenance work.				
	H-11	The organisation does not take into account human performance limitations, including the threat of fatigue for maintenance personnel, as part of the management system, the planning of maintenance tasks, and the organising of shifts.				
Performance of maintenance	H-12	The organisation carries out maintenance on an aircraft or component for which it is not approved.				
Certification of maintenance	H-13	A certificate of release to service is not issued before flight at the completion of maintenance.				
	H-14	A certificate of release to service is not issued by appropriately authorised certifying staff.				
Record-keeping	H-15	The organisation does not record the details of the maintenance work that is carried out within the scope of its approval.				
Occurrence reporting	H-16	The organisation does not establish and maintain an occurrence reporting system, including mandatory and voluntary reporting.				

Category	System level Hazard ID	System level Hazard	Sub-Hazard ID	Sub-Hazard	Causal factor (Fa)	Current Risk
Maintenance Procedures	**H-17**	**The organisation does not establish procedures which ensure that human factors and good maintenance practices are taken into account during maintenance.**				
Management System	**H-18**	**The organisation does not establish, implement, and maintain a management system.**				
Finance	**H-19**	**The organisation does not ensure income to provide maintenance activities.**				

Příloha 5: Potvrzení o validnosti diplomové práce

ABS JETS

Prohlášení o validnosti diplomové práce

Na základě prostudování diplomové práce týkající se návrhu na další vývoj Safety Management Systému (SMS) formou úpravy registru nebezpečí a rizik a návrhu indikátorů bezpečnosti vypracovaných Bc. Zdeňkem Žďánským, potvrzuji jejich využitelnost a potenciální přínos pro praxi.

Předložené návrhy jsou proveditelné v prostředí údržbové organizace a lze je reálně využít jako praktickou součást SMS.

Ing. Martin Orlita
Quality and Safety Manager
ABS Jets, a.s.