ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Vývoj systému řízení provozní bezpečnosti Letiště Pardubice

Diplomová práce

Studijní program: Technika a technologie v dopravě a spojích
Studijní obor: Provoz a řízení letecké dopravy

Vedoucí práce: Ing. Slobodan Stojić, Ph.D.
doc. Ing. Andrej Lališ, Ph.D.

Bc. Ondřej Vašata

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. Ondřej Vašata

Studijní program (obor/specializace) studenta:

navazující magisterský – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Vývoj systému řízení provozní bezpečnosti Letiště Pardubice**

Název tématu (anglicky): Development of Pardubice Airport Safety Management System

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je stanovit postup a technické nástroje pro další vývoj vybraných částí systému řízení provozní bezpečnosti (SMS) Letiště Pardubice.
- Analyzujte dostupné metody bezpečnostního inženýrství.
- Analyzujte standardy pro řízení bezpečnosti v letecké dopravě.
- Analyzujte systém řízení provozní bezpečnosti (SMS) Letiště Pardubice.
- Stanovte postup a technické nástroje pro další vývoj SMS Letiště Pardubice jakožto celku.
- 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:
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.
Stolzer, A., Goglia, J. Safety Management Systems in Aviation. 2. Edition, Routledge, 2016.

Vedoucí diplomové práce: **Ing. Slobodan Stojić, Ph.D.**
doc. Ing. Andrej Lališ, Ph.D.

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. Ondřej Vašata
jméno a podpis studenta

V Praze dne 15. července 2022

Abstrakt

Diplomová práce se zabývá návrhem vývoje systému řízení provozní bezpečnosti Letiště Pardubice. Pomocí systémového modelu STAMP a jeho metodiky STPA se provede analýza systému symbolizujícího činnosti prováděné provozovatelem civilní části letiště, aby bylo možné hlouběji porozumět složkám systému, jeho interakcím a potenciálním nebezpečím. Na základě zjištění a získaných výstupů z analýzy STPA jsou vyvinuty nové bezpečnostní nástroje, které mají řešit zjištěná omezení a zvýšit bezpečnostní výkonnost systému ve vybraných oblastech SMS letiště Pardubice, který v současné době prochází přeměnou. Práce se rovněž zabývá strategiemi implementace, výzvami a očekávanými přínosy spojenými s přijetím těchto nových bezpečnostních nástrojů.

Klíčová slova: provozní bezpečnost, systém pro řízení provozní bezpečnosti, systémový přístup, System-Theoretic Process Analysis

Abstract

The diploma thesis deals with the design of the development of the Safety Management System at Pardubice Airport. Using the STAMP system model and its STPA methodology, an analysis of the system symbolizing the activities carried out by the civil part of the airport operator will be carried out in order to gain a deeper understanding of the system components, its interactions and potential hazards. Based on the findings and the sampled safety data from the STPA analysis, new safety tools are developed to address the identified limitations and improve the safety performance of the system in selected areas of the SMS of Pardubice Airport, which is currently undergoing a transformation. The thesis also discusses the implementation strategies, challenges and expected benefits associated with the adoption of these new security tools.

Keywords: safety, safety management system, System-Theoretic Process Analysis, system theory

Poděkování

Tímto bych rád poděkoval doc. Ing. Andreji Lališovi, Ph.D. a Ing. Slobodanovi Stojićovi, Ph.D.za jejich trpělivost, ochotu, konzultace, a rady, které mi při vytváření mé diplomové práce poskytli. Rád bych také poděkoval své rodině a blízkým za nesmírnou podporu při celém studiu a zástupcům Letiště Pardubice, kteří mi předali cenné rady a informace pro tvorbu práce.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Vývoj systému řízení provozní bezpečnosti Letiště Pardubice 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).

Praze dne 15. května 2023 .....

Bc. Ondřej Vašata

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AMC	Acceptable Means of Compliance	Přijatelné způsoby zajištění shody
CAST	Causal Analysis based on System Theory	
CLV		Centrum leteckého výcviku
EASA	European Union Aviation Safety Agency	Agentura Evropské unie pro bezpečnost letectví
EBA	East Bohemian Airport	
ECCAIRS	European Co-ordination centre for Accident and Incident Reporting Systems	
EK	European Commission	Evropská komise
EU	European Union	Evropská unie
GM	Guidance Material	Poradenský materiál
GOM	Ground Operations Manual	Příručka pro pozemní operace
H	Hazard	Nebezpečí
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
PDCA	Plan-Do-Check-Act	
QMS	Quality Management System	Systém řízení kvality
SA	Safety Assurance	Zajištění bezpečnosti
SC	Safety Constrain	Bezpečnostní omezení
SMM	Safety Management Manual	Příručka řízení provozní bezpečnosti
SMS	Safety Management System	Systém pro řízení provozní bezpečnosti
SPI	Safety Performance Indicator	Indikátor bezpečnosti
SRM	Safety Risk Management	Řízení bezpečnostních rizik
STAMP	System-Theoretic Accident Model and Process	

STPA	System-Theoretic Process Analysis	
UCA	Unsafe Control Action	Nebezpečné řízení
UML	Unified Modeling Language	

Úvod

Letecká doprava je nejrychleji se rozvíjející druh hromadné přepravy lidí a nákladu. Nárůst objemu leteckého provozu s sebou přináší rychlý rozvoj technologií a systémů souvisejících s tímto odvětvím. Stále se zvyšující poptávka po létání ovšem znamená, že se kladou větší nároky na zajištění kontinuity provozu, dostatečné infrastruktury, ale i na bezpečnost, která představuje nejdůležitější aspekt leteckého provozu. Bezpečnost je dnes brána jako naprostý standard, který je při cestování letadlem automaticky očekáván. Jde popsat jako přijatelný stav, kterého chceme v našem systému pomocí různých podpůrných prostředků dosáhnout. Zpočátku se bezpečnost řešila hlavně v oblasti technických problémů fyzických komponent systému, později se přidal vliv lidského činitele, a nyní se bezpečnost řeší pohledem na celkové fungování systému jako celku. Tyto socio-technické systémy jsou robustnější a stále složitější na pochopení, jelikož v sobě zahrnují kromě technologií a lidského faktoru například vlivy okolního prostředí. S novými systémy se zákonitě objevují nové druhy nebezpečí a rizik, která je třeba včas identifikovat a stanovit taková opatření, aby bylo vzniku těmto nebezpečím zabráněno. Pro zajištění bezpečnosti se v letectví používá, pro tento účel vytvořený, systém pro řízení provozní bezpečnosti (SMS).

Systém řízení provozní bezpečnosti (SMS) je systematický přístup, který organizace používají k identifikaci, hodnocení a zmírňování rizik s cílem zajistit bezpečnost provozu a personálu. Zahrnuje stanovení bezpečnostních politik a cílů, provádění hodnocení rizik, zavádění kontrolních opatření a podporu kultury bezpečnosti. Cílem systému SMS je proaktivní řízení bezpečnosti prostřednictvím neustálého sledování a zlepšování výkonnosti v oblasti bezpečnosti, dodržování předpisů a podpory zapojení zaměstnanců. Začleněním bezpečnostních postupů do všech aspektů organizace pomáhá systém SMS předcházet mimořádným událostem, zlepšuje rozhodování a podporuje proaktivní přístup k řízení bezpečnosti. SMS se běžně uplatňuje ve vysoce rizikových odvětvích, jako je právě letectví nebo námořní doprava a zdravotnictví, ale lze jej přizpůsobit různým odvětvím a zlepšit tak postupy řízení bezpečnosti.

Cílem této diplomové práce je navrhnout nové technologické nástroje a postupy pro systém řízení provozní bezpečnosti, který je implementován konkrétně na letišti v Pardubicích. Výběr tohoto letiště vychází z působení autora práce v organizaci provozující civilní část letiště. Návrh architektury samotných nástrojů i jejich vzájemného propojení je založen na výstupech z bezpečnostní metody STPA, která využívá systémový přístup dle modelu STAMP, který představuje rámec používaný k analýze složitých systémů a k pochopení příčin nehod nebo incidentů. Přesahuje rámec tradičních lineárních modelů příčina-následek tím, že zohledňuje interakce a vzájemné závislosti mezi různými prvky systému. Zaměřuje na řídicí strukturu systému, včetně jeho prvků a jejich interakcí, které ovlivňují chování systému. Zkoumáním těchto faktorů se STAMP snaží identifikovat potenciální zranitelnosti a nebezpečí, která mohou vést k nehodám.

Pomocí této detailní analýzy, která je aplikována na systém provozovatele civilní části letiště se získá širší přehled o množství bezpečnostních hrozeb, které by šetřením již vzniklých událostí nebyly odhaleny. Jelikož se metoda STPA řadí mezi proaktivní, je možně s pomocí této metody odhalit nebezpečí, která se zatím v systému nevyskytla. Společně s výstupy z bezpečnostní analýzy STPA bude při tvorbě nástrojů brán zřetel i na aktuálně probíhající přeměnu SMS na pardubickém letišti, kdy je cílem této přeměny nastavení SMS pouze na činnosti, které provozovatel civilní části vykonává a může je ovlivňovat. V poslední kapitole jsou jednotlivé návrhy nástrojů představeny včetně jejich možné implementace, přičemž je navrženo i jejich vzájemné propojení a využití v rámci celého SMS. Ověření celého návrhu proběhlo jednak použitím bezpečnostních dat získané analýzou STPA, ale i pomocí zpětné vazby od pracovníků letiště.

1. Provozní bezpečnost

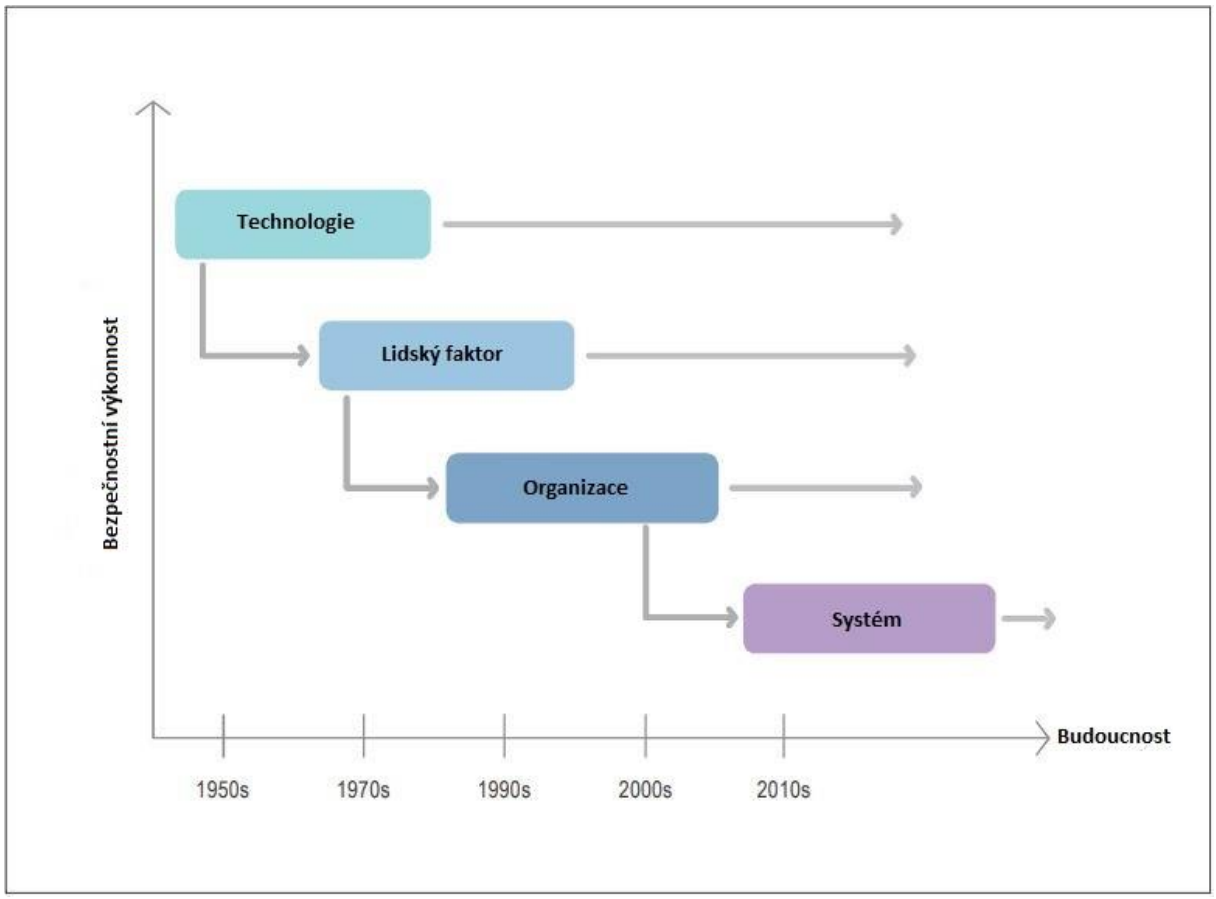
Provozní bezpečnost („Safety") definuje Mezinárodní organizace pro civilní letectví známá pod zkratkou ICAO jako *stav, ve kterém jsou rizika spojená s činnostmi letectví související s provozem letadel nebo s přímou podporou provozu letadel snížena a řízena na přijatelné úrovni.* [1]. Znamená to tedy, že pro dosažení takového stavu, kdy lze provozování činností spojených s letectvím považovat za bezpečné, je nutné neustále identifikovat a vyhodnocovat všechna možná rizika spojena s těmito činnostmi a dle stanovených postupů a bezpečnostních opatření tyto rizika snižovat a následně je udržovat na takové úrovni, kterou lze označit dle definic ICAO za přijatelnou. [1]

Samotný vývoj v bezpečnosti lze zjednodušeně rozdělit do čtyř časových období podle toho, jak se k řešení otázek v oblasti bezpečnosti přistupovalo od dob rozmachu civilního letectví ve 20. století až po současnost. Níže jsou jednotlivá období popsána a graficky znázorněna na Obrázku 1. [2]

- **Technická éra** – Od počátku 20. století téměř až do konce 60. let 20. století se letectví proměnilo ve formu hromadné dopravy, v níž zjištěné bezpečnostní nedostatky zpočátku souvisely převážně s technickými faktory a technologickými poruchami a nedokonalostmi. Veškerá pozornost byla převážně soustředěna na zkoumání a zlepšování technických faktorů (například konstrukce letadla). Ke konci padesátých let 20. století vedla technologická zlepšení k postupnému snižování četnosti leteckých nehod a bezpečnostní procesy už zahrnovaly i dodržování a dohled nad stanovenými předpisy.
- **Éra lidského faktoru** – Počátkem 70. let 20. století se četnost leteckých nehod opět výrazně snížila díky významnému technologickému pokroku a zlepšení bezpečnostních předpisů. Letectví se stalo bezpečnějším druhem dopravy a do popředí zájmu bezpečnostních analytiků se dostal lidský faktor, včetně takových věcí, jako je například spolupráce člověka se stroji. Navzdory investicím prostředků do zmírňování chyb je lidský faktor i v současnosti stále uváděn jako opakující se hlavní příčina leteckých nehod. Prvotní přístupy k lidskému faktoru měly zpočátku tendenci zaměřovat se pouze na jednotlivce, aniž by plně zohledňovaly provozní a organizační kontext systému, ve kterém se daní

jednotlivci nacházeli. Teprve na počátku 90. let 20. století se začalo počítat s faktem, že jednotlivci pracují ve složitém prostředí, které zahrnuje mnoho faktorů, jež mohou v konečném důsledku ovlivnit jejich chování v systému.

- **Organizační éra** – V polovině 90. let se na bezpečnost začalo nahlížet ze systémového hlediska a bezpečnostní procesy začaly zahrnovat jak technické, tak i lidské a organizační faktory. Tento pohled zohledňoval vliv organizační kultury a politiky společností na účinnost bezpečnostních analýz možných rizik. Kromě toho rutinní sběr a analýza bezpečnostních údajů pomocí reaktivních metodik umožnily organizacím sledovat známá bezpečnostní rizika a s přispěním proaktivních metod odhalovat vznikající bezpečnostní trendy. Tato vylepšení poskytla poznatky a základy, které vedly k současnému přístupu k řízení bezpečnosti.
- **Systémová éra** – Od počátku 21. století mnoho států a poskytovatelů služeb k již zavedeným bezpečnostním přístupům vyvinulo zcela nové systémy, které jim umožnily přechod na vyšší úroveň bezpečnostní vyspělosti. Začaly se zavádět státní bezpečnostní programy nebo systémy určené k řízení provozní bezpečnosti. Zaměření se převážně na individuální bezpečnostní výkonnost a místní kontrolu s minimálním ohledem na širší kontext celého leteckého průmyslu se tedy postupně rozšířilo a začalo zohledňovat složitosti leteckého systému a různých organizací jako celku, který se na bezpečnosti letectví podílí. Existuje mnoho příkladů z historie letecké dopravy, které ukazují, že vzájemné interakce jednotlivých organizací přispěly k negativním důsledkům, které vedly k leteckým nehodám a incidentům. [2]



Obrázek 1: Vývoj přístupu k bezpečnosti (upraveno z [2])

1.1 Reaktivní a proaktivní přístup k bezpečnosti

Reaktivní přístup k bezpečnosti znamená, že opatření jsou přijímána až po vzniku nehody nebo incidentu. Jinými slovy, zaměřuje se na reakci na již vzniklou událost a zmírnění jejích následků. Reaktivní opatření zahrnují například provádění šetření, zjišťování příčin incidentu a zavádění změn, které mají zabránit jeho opakování v budoucnu. Nedostatkem reaktivního přístupu je fakt, že úroveň bezpečnosti je založena na hlášených bezpečnostních událostech, které mají svá omezení, mezi která patří zkoumání pouze skutečných poruch, nedostatečné údaje pro určení bezpečnostních trendů, nedostatečný vhled do řetězce příčinných a přispívajících událostí a v neposlední řadě například existence a úloha skrytých nebezpečných podmínek. [2][3]

Naopak proaktivní přístup k bezpečnosti znamená, že se přijímají taková opatření, která zabrání vzniku odchylek ve fungování systému. Důraz je kladen na identifikaci

potenciálních nebezpečí a rizik před tím, než se stanou bezpečnostním problémem, a na následné zavedení takových opatření, která povedou ke zmírnění nebo odstranění těchto identifikovaných rizik. Proaktivní opatření zahrnují například kontinuální provádění hodnocení rizik, zavádění bezpečnostních postupů a zásad, poskytování školení a vzdělávání svým zaměstnancům a pravidelnou revizi a aktualizaci bezpečnostních protokolů. [2][3]

Reaktivní i proaktivní přístup k bezpečnosti má své klady i zápory. Reaktivní opatření jsou důležitá pro poučení se z minulých chyb a zlepšení bezpečnostních postupů, zatímco proaktivní přístup pracuje se systémem a zkoumá odchylky od jeho reálného stavu od toho, jak by podle návrhu měl fungovat. V ideálním případě by měl komplexní bezpečnostní program zahrnovat prvky obou přístupů, aby byly zajištěny co nejlepší výsledky. [2]

2. Řízení provozní bezpečnosti

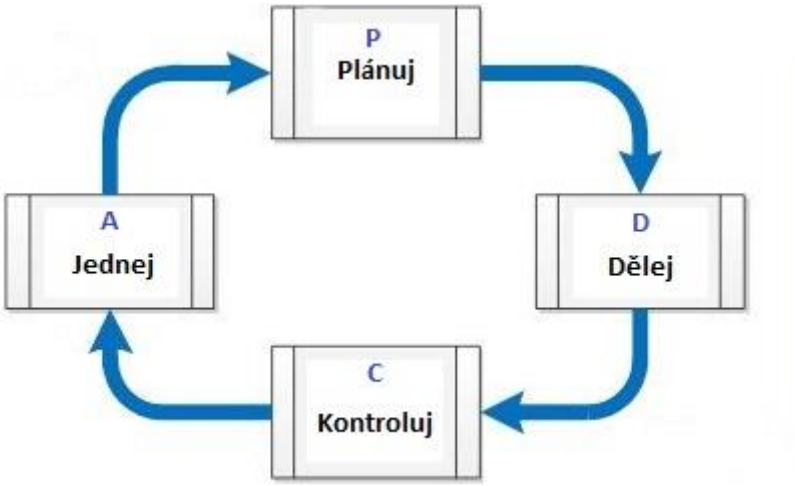
Řízení bezpečnosti v letectví je stále probíhající proces identifikace nebezpečí, hodnocení a zmírňování rizik s cílem udržet bezpečné a zdravé pracovní prostředí organizace pro zaměstnance, zákazníky a veřejnost. Řízení bezpečnosti mimo jiné zahrnuje vypracování a zavedení bezpečnostních zásad, postupů a praktických poznatků pro prevenci vzniku událostí, mezi něž patří incidenty, nehody, úrazy apod., jakož i reakci na incidenty a mimořádné události, pokud k nim dojde. [2][4]

Efektivní řízení bezpečnosti se netýká pouze letecké dopravy, potažmo hromadné dopravy obecně. Je rovněž nezbytné pro podniky a organizace v různých odvětvích, včetně výroby, stavebnictví, zdravotnictví a dalších. [5]

V rámci řízení bezpečnosti se taktéž využívá tzv. Demingův model, který je známý i pod anglickou zkratkou PDCA. Tento model obsahuje čtyři fáze: [6]

1) Plan (Plánuj)
2) Do (Dělej)
3) Check (Kontroluj)
4) Act (Jednej)

V první fázi probíhá analýza současné situace, shromažďování relevantních údajů a hledání způsobů, jak připravit zlepšení systému. Ve fázi *Dělej* jsou jednotlivé plány realizovány v souladu s definovanými metodami z první etapy. Třetí fáze (*Kontroluj*) vyžaduje určení, zda všechny procesy a navrhnutá zlepšení fungují tak, jak bylo plánováno, nebo zda je zapotřebí opětovná revize. V poslední etapě *Jednej* jsou navrhována opatření proti stávajícím odchylkám mezi plány a skutečnými výsledky a veškerá zlepšení a změny jsou implementovány do praxe. Tento cyklus se poté neustále opakuje (viz. Obrázek 2), protože jak už je zmíněno výše, řízení bezpečnosti je kontinuální proces. [6]



Obrázek 2: Model PDCA [vlastní tvorba]

Aby bylo řízení bezpečnosti efektivní a mělo jasně definovanou strukturu, by navrženy nástroje, které tomu napomáhají a které jsou popsány v následujících podkapitolách:

2.1 Systém řízení kvality (QMS)

Systém řízení kvality byl představen v šedesátých letech. Je zastoupen v mnoha odvětvích letecké dopravy v podobě systémů kontroly kvality (QC) a zajištění kvality (QA). Nesouvisí primárně tedy přímo s bezpečností, ale některé jeho prvky jsou převzaty v současných systémech určených pro řízení bezpečnosti. Jeho primární funkce spočívá v definování politiky jakosti a cílů. V případě, že je systém správně implementován, zajišťuje, že jsou postupy organizace prováděny důsledně v souladu s platnými požadavky, problémy identifikovány a vyřešeny, a že organizace neustále zlepšuje své postupy, produkty a služby. Systém tedy zajišťuje přítomnost nezbytných prvků ke zvýšení efektivity a snížení rizik spojených primárně se službami. Uplatňování principů QA v řízení bezpečnostních procesů pomáhá zajistit, že potřebná systémová bezpečnostní opatření byla přijata s cílem podpořit organizaci při dosahování daných bezpečnostních cílů. [7]

Systém řízení kvality v sobě mimo jiné zahrnuje následující prvky: [7]

- Návrh a dokumentace postupů
- Monitorování provozu
- Kontroly a zkušební metody

- Použití statistických analýz
- Interní a externí audity
- Sledování přijatých opatření

2.2 Systém řízení provozní bezpečnosti (SMS)

Tento systém se začal vyvíjet později a dá se považovat za nástupce výše zmíněného systému řízení kvality. Jedná se už o systém zaměřený pouze na řízení provozní bezpečnosti, přičemž je definován jako *systematický přístup k řízení provozní bezpečnosti, včetně nezbytných organizačních struktur, odpovědností, zásad a postupů*. [2]

Systém řízení bezpečnosti se, na rozdíl od QMS, zaměřuje více na lidskou výkonnost, lidské a organizační faktory a vhodně je integruje s technickými aspekty a procesy managementu kvality s cílem přispět k dosažení vysoké úrovně bezpečnosti. Hlavní cíl SMS je obdobný jako obecné cíle zajištění bezpečnosti – identifikace bezpečnostních rizik, kterým musí organizace čelit a zajistit, aby byla tato rizika pod stálou kontrolou. Před zavedením SMS je nezbytné si definovat stěžejní body na základě kterých bude systém následně postaven a cíle, které by měly být jeho zavedením a provozováním splněny. Provozovatel nebo uživatel letiště, který tento systém zavádí, nebo v budoucnu plánuje zavést, by měl mít představu, jakým způsobem bude systém zaveden, což je pro efektivní výsledek jeden z nejdůležitějších faktorů. Důležité je také zmínit, že je zákonem daná povinnost mít zaveden systém řízení provozní bezpečnosti. [1][7]

Pro zavedení Safety Management Systému se na počátku zvolí strategie, která je nejvhodnější k potřebám a cílům daného provozovatele, potažmo uživatele letiště a která by měla obsahovat tyto body: [7]

- Popis sytému společně s výčtem jednotlivých komponentů a prvků (ať již zavedených nebo těch, které se budou zavádět)
- Definice politiky bezpečnosti a plánovaných cílů bezpečnosti
- Schéma funkcí, odpovědností a prostředků pro zapojení pracovníků a k tomu náležící dokumentace
- Definice systému hlášení, interní komunikace a veškerého přenosu informací

- Stanovení postupů kontroly a vyhodnocování úrovně bezpečnosti
- Způsob školení zaměstnanců

2.2.1 Složky SMS

Zavedený systém řízení provozní bezpečnosti se následně dělí do čtyř komponentů, kde každý komponent obsahuje prvky, které popisují konkrétní funkce, činnosti a procesy pro úspěšné zavedení a udržování systému řízení provozní bezpečnosti. Níže jsou jednotlivé komponenty popsány a pro přehlednost ilustrovány na Obrázku 3. [5][8]

Systém řízení provozní bezpečnosti (SMS)	
Komponenty	**Prvky**
1 Bezpečnostní politika a cíle	1.1) Závazek vedení společnosti 1.2) Odpovědnost za bezpečnost 1.3) Jmenování bezpečnostního personálu 1.4) Koordinace plánování reakce na mimořádné události 1.5) Dokumentace systému řízení bezpečnosti
2 Řízení bezpečnostních rizik	2.1) Identifikace nebezpečí 2.2) Hodnocení a zmírňování bezpečnostních rizik
3 Zajištění bezpečnosti	3.1) Sledování a měření výkonu v oblasti bezpečnosti 3.2) Řízení změn 3.3) Neustálé zlepšování SMS
4 Podpora bezpečnosti	4.1) Vzdělávání a výcvik 4.2) Komunikace bezpečnosti

Obrázek 3: Struktura SMS (upraveno z [8])

Bezpečnostní politika a cíle

Vedení společnosti by mělo učinit bezpečnost nedílnou součástí firemních hodnot a denně dávat najevo svůj závazek. Nejvyšší vedení musí zejména stanovit bezpečnostní cíle, definovat bezpečnostní politiku a zároveň se viditelně a osobně podílet na jejich plnění. Měla by být jasně definována odpovědnost a povinnosti zaměstnanců a společnosti v oblasti bezpečnosti, například úloha vedoucího týmu řídit bezpečnost stejným způsobem, jakým dohlíží na ostatní oblasti podnikání, a povinnost bezpečnostních manažerů zajistit účinnost kontroly bezpečnostních rizik. [2] [5]

Po určení pracovníků, v jejichž kompetenci je zajištění bezpečnosti, by měly být stanoveny také procesy dokumentace, protože systém řízení bezpečnosti bude pravidelně přezkoumáván, aby se zajistilo, že zůstane relevantní a vhodný pro organizaci. Dokumentace systému řízení bezpečnosti může mít podobu samostatné příručky (SMM – Safety Management Manual) nebo může být začleněna do stávajících postupů vedení záznamů. [2] [5]

Řízení bezpečnostních rizik

Tato složka SMS představuje jednu z nejdůležitějších součástí řízení bezpečnosti. Řízení rizik („Safety Risk Management" – SRM) v sobě zahrnuje následující procesy: [2]

- Identifikace nebezpečí[1]
- Hodnocení rizik[2]
- Zmírňování rizik

Prvotní činnost v rámci SRM je proces zvaný **Identifikace nebezpečí**. Nebezpečí existují na všech úrovních organizace a lze je zjistit z mnoha zdrojů včetně systémů určených pro hlášení událostí, interních inspekcí, auditů, odborného posouzení apod. Cílem je proaktivně identifikovat nebezpečí dříve, než povedou k nehodám, incidentům nebo jiným událostem souvisejících s bezpečností systému. Důležitým mechanismem pro proaktivní identifikace nebezpečí je dobrovolný systém hlášení událostí, pochybení zaměstnanců atd. Informace shromážděné prostřednictvím těchto systémů hlášení mohou být doplněny pozorováním nebo zjištěním zaznamenaným během běžných inspekcí na pracovišti nebo organizačních auditů. Nebezpečí lze také identifikovat při přezkoumání nebo studiu bezpečnostních doporučení. Zohlednění nebezpečí při přezkoumávání zpráv o vyšetřování nehod nebo incidentů je dobrým způsobem, jak zlepšit způsob identifikace nebezpečí v organizaci. To je zvláště důležité v případech, kdy kultura bezpečnosti organizace ještě není na takové úrovni, aby podporovala účinné dobrovolné podávání zpráv o bezpečnosti, nebo v malých organizacích s omezeným počtem událostí nebo zpráv. Důležitým zdrojem specifických nebezpečí spojených

[1] Nebezpečí = Stav nebo objekt, který může způsobit zranění personálu, poškození zařízení nebo konstrukcí, ztrátu materiálu nebo snížení schopnosti plnit předepsanou funkci. [2]
[2] Riziko = pravděpodobnost a závažnost následku nebezpečí [2]

s provozem a činnostmi jsou externí zdroje, jako je ICAO, obchodní sdružení nebo jiné mezinárodní orgány. [2][9]

Po identifikaci nebezpečí následuje **hodnocení rizik**. Riziko se ohodnocuje jednak z pohledu jeho závažnosti a jednak dle pravděpodobnosti jeho výskytu. Závažnost rizika je definována *jako očekávaný rozsah poškození, který nastane jako následek identifikovaného nebezpečí.* [1] Pro klasifikaci závažnosti se musí zvážit všechny možné následky, tedy od poškození letadla či letištní infrastruktury až po lidská zranění či dokonce úmrtí. Škála závažnosti je vymezena od A do E, kde: [2]

- A = katastrofální (např. zničení letadla)
- B = hazardní (vážné zranění personálu)
- C = významné (vážný incident)
- D = méně významné (použití nouzových postupů)
- E = zanedbatelné (absence nebo minimální počet následků)

Pravděpodobnost rizika je míra očekávání toho, že dojde k nějakému následku. Škála pravděpodobnosti je od 1 do 5, kde: [2]

- 1 = extrémně nepravděpodobné
- 2 = nepravděpodobné
- 3 = vzdáleně pravděpodobné
- 4 = občasné
- 5 = časté

ICAO zavedlo univerzální alfanumerickou matici rizik (Tabulka 1), která se využívá právě při hodnocení rizik identifikovaných nebezpečí. Přiřazením závažnosti a pravděpodobnosti riziku dojde k jeho zařazení do jedné z tří kategorií – zelené, oranžové a červené. Zelená kategorie symbolizuje tzv. akceptovatelnou oblast, ve které se nacházejí pouze přijatelná rizika. Rizika, která se nacházejí v oranžově podbarvené oblasti, se také dají označit za rizika přijatelná, musí se však podrobit analýze a na základě výsledků určit další postup řízení těchto rizik. Červená barva znázorňuje kategorii nepřijatelných rizik. Do této kategorie spadají rizika, která jsou za daných okolností naprosto netolerovatelná a musí být vyřešena (= zmírněna či eliminována) co nejdříve. [2]

Tabulka 1: Matice rizik (upraveno z [2])

Bezpečnostní riziko		*Závažnost*				
Pravděpodobnost		*Katastrofální A*	*Hazardní B*	*Významná C*	*Méně významná D*	*Zanedbatelná E*
Častá	5	5A	5B	5C	5D	5E
Občasná	4	4A	4B	4C	4D	4E
Vzdáleně pravděpodobná	3	3A	3B	3C	3D	3E
Nepravděpodobná	2	2A	2B	2C	2D	2E
Extrémně nepravděpodobná	1	1A	1B	1C	1D	1E

Poté následuje proces **zmírňování rizik**. Jedná se o proces navrhování nápravných opatření nebo preventivních kontrol, které vedou ke snížení závažnosti a/nebo pravděpodobnosti rizika. Obecně platí, že je snadnější snížit pravděpodobnost než se pokoušet snížit závažnost. Zmírňování rizik často vyžaduje změny definovaných procesů a postupů. Dělí se do tří kategorií: [2]

- **Vyhýbání se riziku** („avoidance“) - Operace či činnost je zrušena nebo je jí zabráněno, protože bezpečnostní riziko výrazně převyšuje přínosy pokračování v této činnosti. Tímto krokem je bezpečnostní riziko zcela eliminováno.
- **Snížení rizika** („reduction“) - Sníží se četnost operací, potažmo činností (tímto se sníží pravděpodobnost) nebo se přijmou opatření ke snížení rozsahu následků bezpečnostního rizika (snížení závažnosti).
- **Oddělení rizika** („segregation“) - Přijímají se opatření k izolaci důsledků bezpečnostního rizika nebo se zavádí redundance na ochranu před nimi.

Pro nalezení optimálního řešení je důležité zvážit celou škálu možných kontrolních opatření. Každá navrhovaná alternativa zmírnění bezpečnostních rizik by měla být prozkoumána i z hledisek efektivity, časové náročnosti, nákladů a podobně. [2]

Zajištění bezpečnosti

Zajištění bezpečnosti („Safety Assurance“ – SA) je složkou systému řízení bezpečnosti, která se zabývá sledováním zajištění bezpečnosti během provozu. Po strategickém zavedení kontrolních opatření by měla být vyhodnocena i jejich výkonnost a účinnost.

Zajišťování bezpečnosti se skládá z procesů a činností prováděných za účelem zjištění, zda systém řízení bezpečnosti funguje v souladu s očekáváními a požadavky. To zahrnuje průběžné sledování jeho procesů i provozního prostředí s cílem odhalit změny nebo odchylky, které mohou přinést nová bezpečnostní rizika nebo zhoršit ta stávající. Takové změny nebo odchylky pak mohou být řešeny prostřednictvím procesu SRM. Mezi běžné funkce SA patří inspekce, interní audity, vyšetřování, monitoring pomocí indikátorů bezpečnosti a systémy dobrovolného i povinného hlášení zaměstnanců. [2] [9]

Interní audity se provádějí za účelem posouzení účinnosti systému řízení bezpečnosti a identifikace oblastí, které je možné zlepšit. V případě zjištění neshod a dalších problémů by měly být tyto nedostatky vyšetřeny a analyzovány příčiny a faktory přispívající k těmto nedostatkům. Interní audit se zaměřuje především na zásady, procesy a postupy, které zajišťují řízení bezpečnostních rizik. Interní audity jsou nejúčinnější, pokud je provádějí osoby nebo oddělení nezávislá na auditovaných oblastech. Při plánování interních auditů je třeba zohlednit kritičnost procesů z hlediska bezpečnosti a výsledky předchozích auditů. Interní audity by měly identifikovat nesoulad s předpisy a zásadami, procesy a nastavenými postupy. Měly by také identifikovat systémové nedostatky, nedostatečnou účinnost kontrol bezpečnostních rizik a identifikovat nové příležitosti ke zlepšení auditovaného systému. [2]

Posuzování výkonnosti v oblasti provozní bezpečnosti se provádí prostřednictvím shromažďování bezpečnostních údajů a informací o provozní bezpečnosti z různých zdrojů, které má organizace obvykle k dispozici. Dostupnost údajů je jedním z nejdůležitějších aspektů systému řízení bezpečnosti. Využívání těchto údajů pro sledování a měření výkonnosti v oblasti bezpečnosti jsou zásadní činnosti, které vytvářejí informace nezbytné pro rozhodování o bezpečnostních rizicích. Dosažená výkonnost v oblasti provozní bezpečnosti je ukazatelem chování organizace a také měřítkem účinnosti SRM. Pro sledování výkonnosti bezpečnosti daného systému se stanovují následující nástroje: [1][2]

- **Bezpečnostní cíle** – měly by být stanoveny jako první, aby odrážely strategické úspěchy nebo požadované výsledky související s bezpečnostními nedostatky.
- **Indikátory bezpečnosti** (jsou popsány níže)

Indikátory bezpečnosti („Safety Performance Indicators“ – SPI) se používají k měření provozní bezpečnosti poskytovatele služeb a výkonnosti jeho SMS. SPI se opírají o sledování údajů a informací z různých zdrojů včetně systému hlášení o bezpečnosti. Měly by být specifické pro konkrétní systém a měly by být propojeny s již stanovenými bezpečnostními cíli. Při stanovování SPI by měly být zohledněny následující aspekty: [2]

- Měření správných parametrů
- Dostupnost měřených dat
- Spolehlivost naměřených dat

V rámci SMS se nejčastěji používají dva druhy indikátorů bezpečnosti – reaktivní a proaktivní. [2]

Reaktivní indikátory měří události, které již nastaly. Označují se také jako "SPI založené na výsledcích" a obvykle (ale ne vždy) se jedná o negativní výsledky, kterým se organizace snaží vyhnout. Pomáhají organizaci pochopit, co se stalo v minulosti, a jsou užitečné pro dlouhodobé trendy. Reaktivní indikátory mohou taktéž měřit účinnost přijatých bezpečnostních opatření. Jsou účinné při ověřování celkové bezpečnostní výkonnosti systému. Například sledování "vývoj počtu kolizí na odbavovací ploše na počet pohybů vozidel po změně značení na stojánce" poskytuje měřítko účinnosti nového značení. [2]

Proaktivní indikátory bezpečnosti měří procesy a vstupy, které jsou zaváděny za účelem zlepšení nebo udržení bezpečnosti. Jsou také známé jako "indikátory aktivity nebo procesu", protože monitorují a měří podmínky, které mají potenciál vést k určitému výsledku nebo k němu přispět. Příklady proaktivních SPI zahrnují například "procento zaměstnanců, kteří úspěšně a včas dokončili školení o bezpečnosti" nebo "četnost činností plašení ptáků v letištním perimetru". [2]

Při nastavování indikátorů bezpečnosti by vždy mělo být definováno: [2]

- Popis toho, co indikátor zaznamenává
- Účel indikátoru (co sleduje a koho informuje)
- Měrné jednotky a popis jejich výpočtu
- Zodpovědnost za shromažďování, ověřování, monitorování, podávání zpráv a jednání na základě záznamů SPI

- Kde a jak jsou data zaznamenávána
- Četnost vykazování, shromažďování, monitorování a analýzy naměřených dat

Dalšími zdroji pro sledování a měření výkonnosti v oblasti bezpečnosti mohou být následující činnosti: [2]

- Bezpečnostní studie
- Analýzy bezpečnostních údajů
- Bezpečnostní průzkumy/dotazníky
- Systémy sběru provozních dat

Podpora bezpečnosti

Bezpečnost organizace nemůže být postavena pouze na striktních předpisech, nebo mechanickém provádění postupů. Důležitá je i podpora bezpečnosti pro vytvoření takového prostředí, které přispěje k souhře stanovených postupů, procesů a využití technických prostředků s lidským činitelem. Aby bylo dosaženo takového prostředí, je nezbytné, aby byli zaměstnanci seznámeni s celým systémem, jeho funkcemi a ideálně se všemi jeho aspekty, principy a částmi. Podpora bezpečnosti podporuje pozitivní kulturu bezpečnosti a pomáhá dosahovat bezpečnostních cílů poskytovatele služeb kombinací technické způsobilosti, která je neustále zvyšována prostřednictvím školení a vzdělávání, účinné komunikace a sdílení informací. Vrcholové vedení zajišťuje propagaci kultury bezpečnosti v celé organizaci. Vedení společnosti by mělo zavést a uplatňovat procesy a postupy, které usnadňují účinnou obousměrnou komunikaci na všech úrovních organizace. To by mělo umožňovat komunikaci "zdola nahoru", která podporuje otevřenou a konstruktivní zpětnou vazbu od všech pracovníků. [2][7]

Zásadními prvky podpory bezpečnosti tedy jsou: [2]

- Výcvik a vzdělávání
- Komunikace

Annex 19 požaduje, aby *poskytovatel služeb vypracoval a udržoval program bezpečnostního školení, který zajistí, že pracovníci jsou vyškoleni a způsobilí k výkonu svých povinností v rámci systému SMS*. [1] Dále stanovuje, aby *rozsah programu bezpečnostního školení odpovídal zapojení každého jednotlivce do systému řízení*

bezpečnosti. [1] Za zajištění existence vhodného programu bezpečnostního školení odpovídá vedoucí bezpečnosti. Program školení zahrnuje poskytování vhodných bezpečnostních informací relevantních pro konkrétní bezpečnostní problémy, s nimiž se organizace a její zaměstnanci setkávají. Program školení by také měl zahrnovat požadavky na počáteční a opakované školení k udržení kompetencí. [1] [2]

Organizace by měla určit, kdo by měl být proškolen a do jaké míry, což bude záviset na jeho zapojení do systému SMS. Většina lidí pracujících v organizaci má nějaký přímý nebo nepřímý vztah k bezpečnosti letectví, a díky tomu mají i povinnosti v oblasti SMS. To se týká všech pracovníků přímo zapojených do činností organizace a pracovníků zapojených do výborů organizace pro bezpečnost. [2]

Neméně důležitá je komunikace bezpečnosti. Měla by probíhat na všech úrovních organizace, ať už mezi bezpečnostním manažerem a vedením organizace, tak i s provozními pracovníky, a to skrze organizaci i přímo. Komunikace by měla mít za cíl uvědomění všech pracovníků o zásadách a principech SMS, vysvětlovat bezpečnostní procedury, informovat o přijímání daných opatření a poskytovat relevantní užitečné informace týkající se bezpečnosti. Pro účelnou komunikaci by měly být využívány všechny dostupné zdroje, kterými daná organizace disponuje. Komunikace může probíhat napřímo mezi zaměstnanci a vedením, nebo s využitím různých nástrojů (dotazníky, emailová korespondence, interní komunikační technologie apod.). [2][7]

Tyto aspekty by měly výrazně přispívat ke tvorbě kultury bezpečnosti v organizaci. Kultura bezpečnosti označuje sdílené hodnoty, postoje, přesvědčení a postupy, které utvářejí přístup jednotlivců a skupin k bezpečnosti v organizaci. Je výsledkem individuálních a skupinových hodnot, postojů, vnímání a kompetencí, které určují závazek organizace k řízení bezpečnosti. Zdůrazňuje význam prosazování bezpečnosti jako základní hodnoty, stanovení jasných bezpečnostních zásad a postupů, podpory otevřené komunikace a spolupráce, poskytování průběžného školení a rozvoje a podpory neustálého zlepšování řízení provozní bezpečnosti. Zahrnuje také identifikaci potenciálních nebezpečí a rizik, posouzení jejich pravděpodobnosti a dopadu a přijetí proaktivních kroků k jejich zmírnění. [10]

Pozitivní kultura bezpečnosti podněcuje zaměstnance, aby hlásili incidenty, skoronehody[3], vlastní pochybení a nebezpečí a aby převzali odpovědnost za svou bezpečnost a bezpečnost ostatních. Kultura bezpečnosti je v konečném důsledku zásadní pro dosažení vysoké úrovně bezpečnosti a snížení rizika nehod a mimořádných událostí. [10]

2.2.2 Výhody funkčního SMS

Zavedení funkčního systému řízení bezpečnosti přináší kromě řízení provozní bezpečnosti i řadu dalších výhod: [2]

- **Posílení kultury bezpečnosti** – kulturu bezpečnosti organizace lze posílit zviditelněním závazku vedení a aktivním zapojením zaměstnanců do řízení bezpečnostních rizik. Pokud vedení aktivně podporuje bezpečnost jako prioritu, je to obvykle dobře přijímáno personálem a se stává součástí běžného provozu.
- **Dokumentace postupů** – jasný a dokumentovaný přístup k dosažení bezpečného provozu, který je srozumitelný pro zaměstnance a lze jej použít jako podklad v případě externích auditů.
- **Lepší včasné odhalování nebezpečí** – zlepšuje schopnost organizace odhalovat vznikající bezpečnostní problémy, což může zabránit nehodám a incidentům díky proaktivní identifikaci nebezpečí a řízení bezpečnostních rizik.
- **Rozhodování založené na bezpečnostních datech** – zlepšuje schopnost organizace určit prioritní oblasti zájmu na základě shromážděných dat.
- **Porozumění bezpečnostním cílům organizace a jejím ukazatelům výkonnosti v oblasti bezpečnosti (SPI), které udávají směr a motivují k bezpečnosti.** Zaměstnanci si budou lépe uvědomovat výkonnost organizace a pokrok, kterého bylo dosaženo při plnění stanovených bezpečnostních cílů, a také to, jak přispívají k úspěchu organizace.
- **Možné finanční úspory** – efektivní řízení provozní bezpečnosti díky zavedenému SMS dokáže organizaci přinést i finanční úspory díky včasné identifikaci bezpečnostních problémů. SMS taktéž umožňuje snížení nákladů na provoz díky odhalení neefektivity stávajících procesů a systémů.

[3] Skoronehoda = Událost, jiná než nehoda, spojená s provozem letadla, která ovlivňuje nebo by mohla ovlivnit bezpečnost provozu. [11]

3. Bezpečnostní hlášení

Systémy pro hlášení nebezpečí jsou nezbytnými prvky v procesu identifikace možných bezpečnostních rizik. Systémy hlášení by měly být co nejjednodušší pro přístup, vytváření a podávání bezpečnostních hlášení. Hlášení nehod a incidentů se týká všech zúčastněných stran v letectví. Provozní personál je povinen hlásit nehody a určité typy incidentů co nejdříve a nejrychlejšími dostupnými prostředky státnímu úřadu pro civilní letectví. [2]

Systémy **povinného hlášení** o bezpečnosti by měly usilovat o zachycení všech cenných informací o události, včetně informací typu: co se stalo, kde se to stalo, kdy se událost stala a komu je hlášení adresováno. Kromě toho by systémy povinného bezpečnostního hlášení měly umožnit zachycení některých specifických nebezpečí, o nichž je známo, že přispívají k nehodám, a jejichž včasná identifikace a sdělení jsou považovány za cenné (např. běžné meteorologické podmínky, sopečná činnost atd.). [2]

Dalším ze způsobů, jak identifikovat nebezpečí, je **dobrovolné hlášení**. Měly by být zřízeny dobrovolné systémy hlášení o bezpečnosti, které by shromažďovaly údaje o bezpečnosti a bezpečnostní informace, které nebudou zachyceny v povinném systému hlášení o bezpečnosti. Tato hlášení jdou nad rámec typického hlášení incidentů. Dobrovolná hlášení obvykle odkrývají skryté podmínky, jako jsou nevhodné bezpečnostní postupy nebo předpisy, lidská pochybení atd. V systémech dobrovolného hlášení neexistují žádné donucovací prostředky, ohlášené informace by neměly být použity proti pracovníkům, kteří událost či informaci ohlásili. Je zde poskytnuta ochrana zdroje pro zpětnou podporu tohoto typu bezpečnostního hlášení. [2] [7]

V souvislosti se systémy bezpečnostního hlášení se často naráží na neochotu personálu organizace, zejména pokud se jedná o hlášení vlastních pochybení. Důvody mohou být například strach z potrestání, z přiznání vlastní chyby apod. V tomto ohledu může mít poměrně velký přínos školení a dobrá komunikace o principech a přínosech systémů hlášení. [7]

4. Standardy pro řízení bezpečnosti v letecké dopravě

Tato kapitola shrnuje národní a mezinárodní normy a předpisy, které se týkají řízení provozní bezpečnosti v letectví. Mezi tyto normy a předpisy patří například Mezinárodní normy pro bezpečnost letectví (ICAO), předpisy Evropské unie o bezpečnosti letectví, nebo předpisy vydané Ministerstvem dopravy ČR.

4.1 ICAO Annex 19 (předpis L19)

Annex 19 byl poprvé vydán 25. listopadu 2013, platný pro všechny členské státy ICAO se stal 14. listopadu 2019. Jedná se o komplexní mezinárodní normu vypracovanou Mezinárodní organizací pro civilní letectví (ICAO), která poskytuje rámec pro zavádění systémů řízení bezpečnosti (SMS) v letectví, jehož konečným cílem je snížit riziko nehod a incidentů v letecké dopravě. Účelem Annexu 19 je stanovit nezbytné požadavky a postupy k zajištění proaktivního přístupu k řízení bezpečnostních rizik v leteckém provozu. [4]

Nastiňuje základní zásady SMS a poskytuje návod, jak zavést SMS v leteckém provozu, včetně identifikace bezpečnostních rizik, hodnocení rizik a vypracování účinných strategií pro jejich zmírnění. Zabývá se také klíčovými prvky SMS, jako jsou bezpečnostní politika a cíle, řízení bezpečnostních rizik, zajištění bezpečnosti a podpora bezpečnosti. Annex 19 navíc zdůrazňuje význam silné kultury bezpečnosti a zapojení všech zúčastněných stran do udržování bezpečného leteckého systému. Vyžaduje, aby letecké organizace zavedly systém řízení bezpečnosti odpovídající jejich velikosti a složitosti a aby pravidelně hodnotily a monitorovaly účinnost svého systému řízení bezpečnosti. [4]

V České republice jsou uveřejňovány Ministerstvem dopravy ČR letecké předpisy řady L, které obsahově vychází z mezinárodních norem (Annexů) vypracovaných Mezinárodní organizací pro civilní letectví. V tomto případě je tedy národní norma předpis L19 vycházející z Annexu 19. [1]

4.2 Nařízení EK č. 139/2014

Nařízení EK č. 139/2014, známé také jako nařízení EU o letištích, je právním předpisem Evropské unie, který upravuje proces získávání a udržování licencí k provozování letišť v Evropské unii. Nařízení se vztahuje na všechna letiště s komerčním leteckým provozem, včetně civilních i vojenských letišť. [12]

Hlavním cílem nařízení je zajistit vysokou úroveň bezpečnosti a kvality provozu letišť a sjednotit pravidla a postupy pro certifikaci letišť napříč členskými státy EU. Nařízení stanovuje požadavky a postupy pro získání a udržení provozní licence letiště, včetně povinností provozovatelů letišť, kritérií pro vydávání a odnímání licencí a mechanismů dohledu a prosazování, které zajišťují dodržování nařízení. Nařízení rovněž obsahuje ustanovení o řízení bezpečnostních rizik při provozu letišť, včetně vypracování systémů řízení bezpečnosti (SMS) a provádění programů dohledu nad bezpečností ze strany vnitrostátních leteckých úřadů. Kromě toho stanoví požadavky na výcvik a kvalifikaci letištního personálu, včetně řídících letového provozu, bezpečnostního personálu a dalšího personálu zapojeného do provozu letiště. [12]

Celkově hraje Nařízení EK č. 139/2014 zásadní roli při zajišťování bezpečnosti a kvality provozu letišť v Evropské unii a pomáhá prosazovat harmonizovaný a konzistentní přístup k certifikaci letišť a dohledu nad nimi ve všech členských státech. [12]

4.3 Nařízení EK č. 376/2014

Nařízení EK č. 376/2014 je právní předpis Evropské unie, který stanoví rámec pro shromažďování, analýzu a sdílení bezpečnostních informací v civilním letectví. Cílem nařízení je zlepšit bezpečnost letectví tím, že se zajistí, aby se bezpečnostní informace shromažďovaly a analyzovaly standardizovaným způsobem ve všech členských státech EU a aby se tyto informace účinně sdílely mezi příslušnými organizacemi. [13]

Nařízení vyžaduje, aby byl v každém členském státě zřízen vnitrostátní systém hlášení o bezpečnosti letectví, který umožní zúčastněným stranám v letectví hlásit bezpečnostní události, nebezpečí a rizika. Shromážděné údaje o bezpečnosti jsou následně analyzovány s cílem určit bezpečnostní trendy a vypracovat strategie pro zmírnění rizik. Nařízení rovněž zřizuje Evropské koordinační centrum pro hlášení leteckých incidentů

(ECCAIRS), které má podporovat sběr, správu a analýzu bezpečnostních údajů na evropské úrovni. Kromě toho nařízení stanoví požadavky na ochranu bezpečnostních informací, včetně důvěrnosti informací a ochrany osob, které hlásí bezpečnostní události. Vyžaduje rovněž, aby letecké organizace, včetně leteckých společností, letišť a poskytovatelů letových provozních služeb, zavedly systémy řízení bezpečnosti (SMS), které zajistí, aby byla bezpečnostní rizika identifikována a proaktivně řízena. [13]

4.4 Prováděcí Nařízení EK č. 2015/1018

Toto nařízení stanoví seznam klasifikovaných událostí v civilním letectví, které podléhají povinnému hlášení podle Nařízení č. 376/2014. [14]

Rozdělení událostí, které mají být hlášeny podle Nařízení č. 376/2014, do kategorií bylo vytvořeno s cílem umožnit osobám určeným tímto nařízením identifikaci událostí, které jimi mají být hlášeny. Události spadajících do systému povinného hlášení jsou zařazen do následujících příloh: [14]

1. Události související s provozem letadla
2. Události související s technickými podmínkami, údržbou a opravou letadla
3. Události týkající se letových navigačních služeb a zařízení
4. Události související s letišti a pozemními službami
5. Události týkající se letadel jiných než složitých motorových letadel, včetně kluzáků a vzdušných dopravních prostředků lehčích než vzduch

4.5 EASA Easy Access Rules for aerodromes

Účelem EASA Easy Access Rules je zajistit vysokou úroveň bezpečnosti provozu letišť v Evropské unii. Easy Access Rules představují konsolidovanou verzi regulačního rámce pro letiště, která zahrnuje prováděcí pravidla a certifikační specifikace přijaté Agenturou Evropské unie pro bezpečnost letectví (EASA). Pravidla zahrnují širokou škálu témat, včetně projektování, výstavby, údržby, provozu a plánování reakce na mimořádné události na letištích. Tím, že poskytují jednotný zdroj informací, usnadňují provozovatelům letišť, vnitrostátním orgánům a dalším zúčastněným stranám pochopení a dodržování požadavků regulačního rámce. To podporuje harmonizaci v celé EU a zajišťuje jednotný přístup k bezpečnosti letišť. [15]

4.6 EASA AMC & GM

EASA AMC je zkratka pro přijatelné prostředky shody („Acceptable Means of Compliance“) Evropské agentury pro bezpečnost letectví (EASA). [16]

Přijatelné prostředky shody jsou souborem poradenských materiálů vypracovaných agenturou EASA, které mají pomoci zajistit dodržování platných předpisů v evropském leteckém průmyslu. AMC poskytuje podrobnější vysvětlení, jak dodržovat regulační požadavky stanovené v evropských předpisech o bezpečnosti letectví. Dále poskytuje praktické pokyny a příklady, které pomáhají organizacím při prokazování souladu s předpisy. Lze jej použít jako referenční příručku pro projektování, konstrukci, provoz, údržbu a certifikaci letadel a souvisejících výrobků, letadlových částí a zařízení, jakož i pro dohled nad těmito činnostmi ze strany příslušných orgánů. [16]

AMC nejsou povinné, ale zúčastněné strany v odvětví jej mohou využít k vypracování vlastních postupů a procesů, pokud jsou v souladu s předpisy. AMC jsou pravidelně revidovány a aktualizovány, aby se zajistilo, že zůstanou aktuální a bude odpovídat potřebám letecké dopravy. [16]

EASA GM je zkratka pro poradenský materiál („Guidance Material“) Evropské agentury pro bezpečnost letectví (EASA). GM poskytují další informace a vysvětlení regulačních požadavků a osvědčených postupů týkajících se bezpečnosti letectví a doplňují tak výše zmíněné AMC. Agentura EASA vypracovává tyto materiály s cílem pomoci organizacím při prokazování souladu s platnými předpisy a podpořit bezpečnost v evropském leteckém průmyslu. GM pokrývá širokou škálu témat souvisejících s leteckou bezpečností, včetně projektování, výroby, údržby a provozu letadel, jakož i uspořádání letového provozu, letišť a požadavků na výcvik leteckého personálu. [16]

4.7 ICAO doc. 9859

ICAO Doc 9859 je příručka s názvem "Safety Management Manual (SMM)", která poskytuje pokyny pro zavádění systémů řízení bezpečnosti (SMS) leteckými organizacemi. Příručku vydává Mezinárodní organizace pro civilní letectví (ICAO), která stanovuje normy a předpisy pro mezinárodní civilní letectví. [2]

Příručka řízení bezpečnosti (SMM) poskytuje strukturovaný a systematický přístup k řízení bezpečnosti s cílem zlepšit výkonnost v oblasti bezpečnosti v celé letecké dopravě. Příručka poskytuje pokyny ke čtyřem složkám systému řízení bezpečnosti: bezpečnostní politika a cíle, řízení bezpečnostních rizik, zajištění bezpečnosti a podpora bezpečnosti. ICAO do. 9859 rovněž popisuje začlenění SMS do celkového systému řízení letecké organizace, včetně vývoje ukazatelů výkonnosti v oblasti bezpečnosti, podávání zpráv o bezpečnosti a kultury bezpečnosti. [2]

5. Systémový přístup k provozní bezpečnosti v letectví

Jak už bylo zmíněno v první kapitole, postupem času se přístup k bezpečnosti měnil z plně technologického zaměření na aktuální přístup zabývající se kompletním systémem, jeho strukturou a fungováním. Problematice systémového přístupu k bezpečnosti se věnuje profesorka Nancy Leveson z americké univerzity MIT, která na toto téma vydala množství knih a publikací, včetně knihy s názvem Engineering a Safer World: Systems Thinking Applied to Safety. [2][17]

Kniha představuje systémově-teoretický přístup k bezpečnostnímu inženýrství, který vnímá bezpečnost jako vlastnost systému, nikoli jako charakteristiku jeho jednotlivých součástí. Systémová teorie nastíněná v knize zdůrazňuje důležitost pochopení interakcí a vzájemných závislostí mezi různými složkami systému a roli, kterou tyto interakce hrají při určování bezpečnosti systému. Podle prof. Levesenové a její systémové teorie se systémy skládají ze složek, které na sebe vzájemně působí, aby dosáhly souboru cílů. Takovými interakcemi mohou být interakce lidské, sociální, technické, informační, politické, ekonomické, organizační a další. Tyto vzájemné interakce mohou vést k emergentním vlastnostem, které nejsou původně přítomny v jednotlivých složkách, včetně bezpečnostních vlastností. Bezpečnost systému je tedy podle této teorie funkcí interakcí a vzájemných závislostí mezi jednotlivými složkami systému. Dřívější průmyslové bezpečnostní modely se spíše zaměřují na nebezpečné úkony a podmínky, systémové modely se zaměřují na to, co se pokazilo celkově v organizaci systému. [17]

Systémová teorie také zdůrazňuje význam zpětnovazebních smyček v bezpečnosti systému. Zpětnovazební smyčky mohou zesilovat nebo tlumit účinky poruch na systém a mohou pomoci udržet nebo obnovit stabilitu systému. Pochopení a řízení zpětnovazebních smyček je proto pro dosažení a udržení bezpečnosti systému zásadní. [17]

5.1 Model STAMP

Model STAMP (System-Theoretic Accident Model and Processes) je model používaný v bezpečnostním inženýrství k analýze nehod a incidentů ve složitých systémech. Model STAMP, jehož autorkou je rovněž Nancy Levesonová, využívá výše zmíněný systémový přístup, který zohledňuje interakce a závislosti mezi složkami systému a také prostředí, v němž systém funguje. Jedná se o prediktivní model bezpečnosti, který vysvětluje bezpečnost jako problém řízení v rámci organizace. Model pracuje se základním předpokladem, že bezpečnostní problém (nehoda, incident) se projevuje jako důsledek selhání nastavené řídicí struktury, ve které jsou lidé organizováni do provozních a manažerských pozic v interakci s technologickými zařízeními. STAMP považuje za klíčovou distribuci informací napříč celým systém, zejména klade důraz na zpětnou vazbu z řízených procesů do řídících prvků. Výhodou analýz dle modelu STAMP je využití systémového pohledu pro popis bezpečnostních událostí, na rozdíl od tradičního popisu událostí pomocí lineárního modelování kauzálních řetězců, bariér nebo s využitím statistiky pro identifikaci základních trendů ve sledovaných typech událostí (indikátorech bezpečnosti). [17][18]

Model STAMP využívá tři základní koncepty z teorie systémů: emergence a hierarchie, komunikace a řízení, a procesní modely. [19]

Emergence a hierarchie

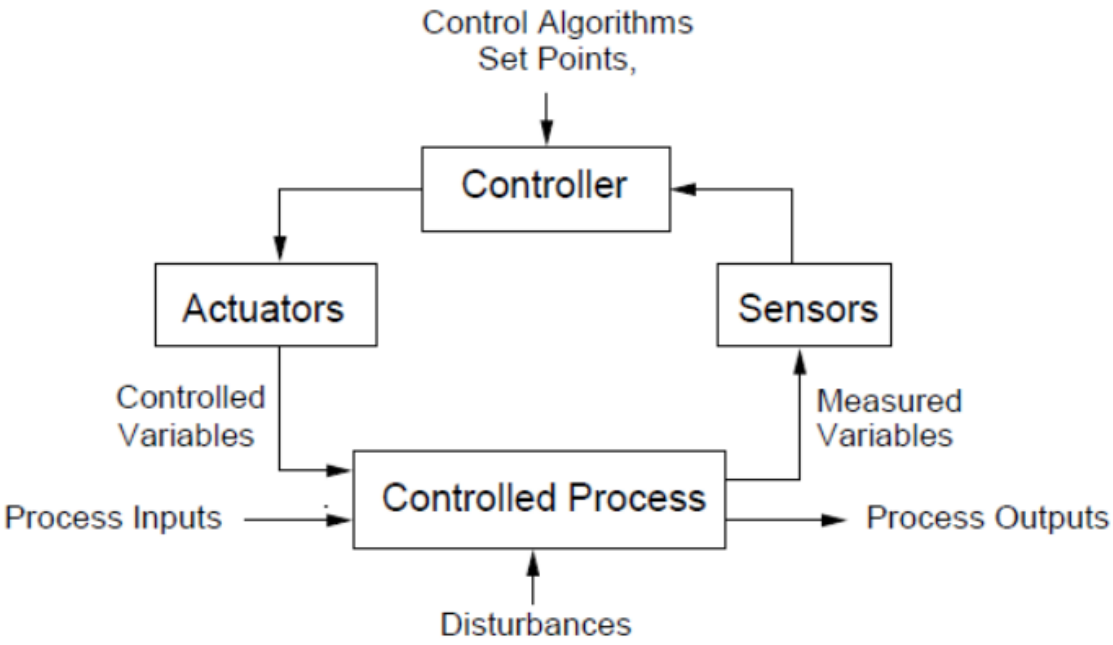
Bezpečnost je emergentní vlastností systémů, protože bezpečnost lze určit pouze v kontextu celku. Hierarchie popisuje vztahy mezi jednotlivými úrovněmi, včetně toho, co úrovně vytváří, co je odděluje a co je spojuje. Komplexní systémy lze vyjádřit pomocí hierarchie, ve které jsou uspořádány jednotlivé úrovně organizace, z nichž každá nadřazená úroveň systému je složitější než úroveň jí podřazená. Na vrcholu hierarchie je tedy nejkomplexnější část celého systému. [17][19]

Komunikace a řízení

Řídicí procesy většinou probíhají na rozhraních mezi dvěma úrovněmi hierarchie a vždy jsou doprovázeny definováním bezpečnostních omezení. STAMP používá koncept definování omezení v rámci chování systému, aby se spíše zabránilo nebezpečným

událostem nebo stavům, než aby se zaměřoval na zamezení selhání jednotlivých komponent. [17]

Mezi hierarchickými úrovněmi jednotlivých bezpečnostních řídicích struktur jsou během řídicích procesů zapotřebí účinné komunikační kanály. Komunikace směrem na nižší úroveň poskytuje informace potřebné k prosazení bezpečnostních omezení na nižší úrovni. Komunikace mířící z nižší na vyšší úroveň poskytuje zpětnou vazbu o tom, jak efektivně jsou omezení plněna. Komunikace také určuje, zda bylo možné zavést řídicí procesy nebo dosáhnout očekávaných cílů. [17][19]



Obrázek 4: Standardní řídicí smyčka [17]

Obrázek 4 znázorňuje koncept nazývající se „standardní řídicí smyčka“, který se dá aplikovat na všech úrovních hierarchie organizace. Základním předpokladem je, že řídicí prvek („Controller“) má již předem definované meze či nastavené hodnoty („Control Algorithms Set Points“), ve kterých proces bude řídit. K zajišťování funkčního procesu se využívají aktivní řídicí prvky („Actuators“), které mají za úkol řídit proměnné hodnoty („Controlled Variables“) tak, aby řídicí prvek byl schopen ovlivnit probíhající proces („Controlled Process“). Samotný proces obsahuje jak vstupy („Process Inputs“), tak výstupy („Process Outputs“). Proces může být ovlivňován rušivými elementy – šumem

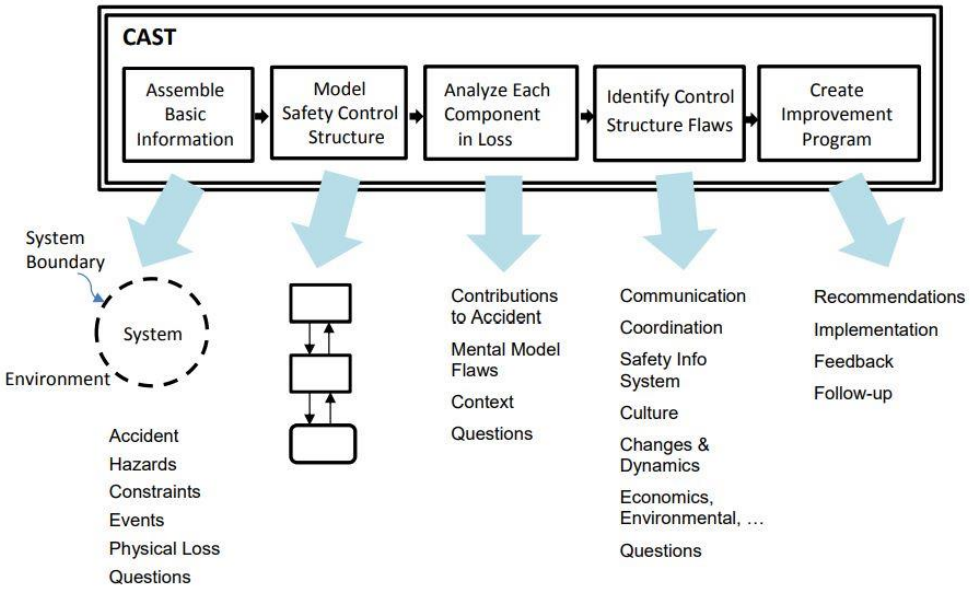
(„Disturbances“). Řídící prvek dále dostává informace o aktuálním stavu procesu ze senzorů („Sensors“), které je mohou získávat v určitých intervalech. Tyto informace se získávají z naměřených dat („Measured Variables“). [17]

Procesní model

Každý řídicí prvek, ať už lidský nebo automatizovaný, potřebuje model řízeného procesu, aby mohl již konkrétní proces účinně řídit. Účelem použití modelu procesu je určit, jaké řídicí akce jsou potřebné na základě znalosti aktuálního stavu řízeného procesu, a odhadnout vliv různých řídicích akcí na tento stav. [17][19]

5.2 Metoda CAST

Metodika CAST (Causal Analysis based on System Theory) je používaná pro vyšetřování nehod a incidentů a je založená na principech systémové teorie. Přístup CAST předpokládá, že nehody jsou způsobeny systémovými selháními a že je nelze vysvětlit zaměřením pouze na jednotlivé nebo izolované faktory. Metoda proto zahrnuje identifikaci systémových faktorů, které přispěly k nehodě, dále analyzuje organizaci, její procesy a interakce mezi nimi. CAST zahrnuje několik kroků (Obrázek 5), včetně definování systému, identifikace událostí a faktorů, které vedly k nehodě a identifikace řídicí struktury společně s analýzou řídicí struktury a jejích slabých míst. [10]



Obrázek 5: Kroky CAST metody [10]

5.3 Metoda STPA

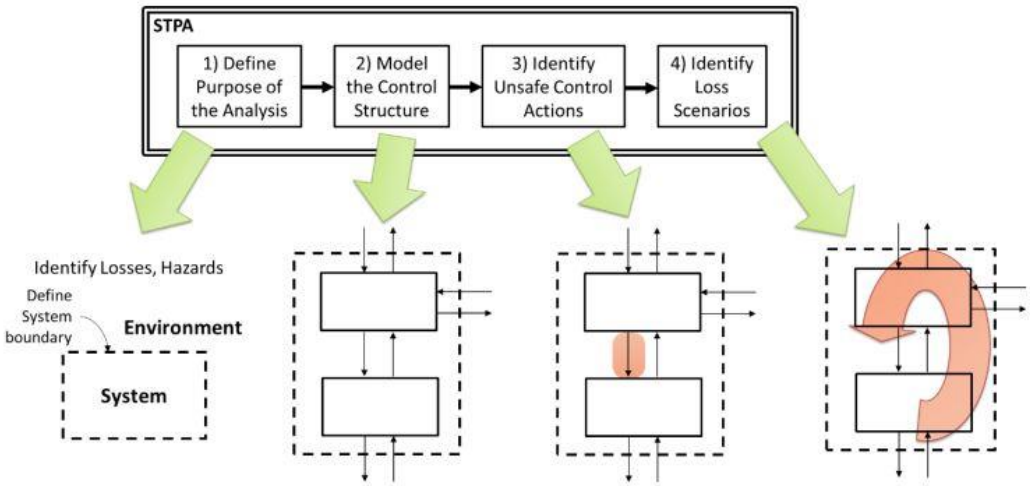
STPA, což je zkratka pro System-Theoretic Process Analysis, je metoda analýzy systémových nebezpečí[4]. [20] Jelikož je metodika STPA taktéž založena na modelu STAMP, využívá systémový přístup k analýze, která se zaměřuje na proaktivní identifikaci potenciálních systémových nebezpečí a navrhování kontrolních mechanismů ke zmírnění těchto nebezpečí ve složitých systémech. Ačkoliv se stále jedná o relativně novou bezpečnostní metodu, byla už použita v celé řadě průmyslových odvětví, včetně letectví, zdravotnictví, automobilového průmyslu a dalších, a je všeobecně uznávána jako účinný přístup k analýze bezpečnosti. [20]

Metoda STPA je jedinečná v tom, že bere v úvahu systém jako celek, nikoliv pouze jednotlivé komponenty, a bere v úvahu také interakci systému s jeho okolím. Tento holistický přístup k analýze nebezpečí umožňuje identifikovat potenciální nebezpečí, která nemusí být při izolovaném pohledu na jednotlivé komponenty zřejmá. Kromě toho STPA podporuje používání řídicích strategií, které jsou spíše proaktivní a preventivní než

[4] Systémové nebezpečí = nebezpečí, které vyplývá ze vzájemného působení a chování součástí systému jako celku, nikoli z jednotlivých součástí samotných [17]

reaktivní, což pomáhá snižovat pravděpodobnost selhání systému a výskytu nehod a incidentů. [20]

Metodu STPA použít v kterékoli fázi systému, od fáze před samotným návrhem až po konečnou fázi – implementaci systému. Jednotlivé kroky metody (Obrázek 6) jsou představeny níže: [20]



Obrázek 6: Kroky STPA [20]

Definování účelu analýzy

První krok analýzy spočívá v samotné definici jejího účelu. Vytyčují se hranice systému a definuje se, jak systém vypadá a do jaké hloubky se systém bude zkoumat. Definuje se, zda systém má i nějaké podsystémy a popisuje se i prostředí celého systému a jak toto prostředí na systém působí. V rámci tohoto kroku se identifikují systémové ztráty a systémová nebezpečí. Poté, co jsou definována nebezpečí, je třeba specifikovat související bezpečnostní omezení převedením těchto identifikovaných nebezpečí na nápravná opatření. [20]

Ztráta zahrnuje něco, co má pro zúčastněné strany hodnotu. Ztráty mohou zahrnovat ztrátu lidského života nebo zranění lidí, škody na majetku, znečištění životního prostředí, ztrátu poslání, ztrátu pověsti, ztrátu nebo únik citlivých informací nebo jakoukoli jinou ztrátu, která je pro zainteresované strany nepřijatelná. [20]

Aby mohla být identifikována nebezpečí na úrovni systému, je nutné nejprve určit systém, který má být analyzován, a hranice tohoto systému. Je třeba rozhodnout, co je do systému zahrnuto a na co už nebude brán v rámci analýzy zřetel. S ohledem na bezpečnostní inženýrství je nejužitečnějším způsobem, jak definovat hranici systému pro účely analýzy, zahrnout ty části systému, nad nimiž mají konstruktéři systému určitou kontrolu. Po určení systému a hranice systému je dalším krokem definování nebezpečí na úrovni systému určením stavů nebo podmínek systému, které povedou ke ztrátě v nejhorších podmínkách systémového prostředí. Identifikovaná nebezpečí mohou vést k jedné nebo více ztrátám a každé nebezpečí by mělo být v rámci analýzy propojeno k výsledné ztrátě. Tato zpětná sledovatelnost se obvykle dokumentuje v závorkách za popisem nebezpečí. [20]

Pro popis systémových nebezpečí by se vždy měla používat stanovená taxonomie: [20]

<Specifikace nebezpečí> = <Systém> <Nebezpečný stav> <Odkaz na ztráty>

Jakmile jsou identifikována nebezpečí na úrovni systému, je snadné identifikovat omezení na úrovni systému, která musí být prosazena: stačí obrátit jejich podmínku. [20]

Příklad pro ilustraci:

Ztráta: L1 = Ztráty na životech nebo zranění osob

Nebezpečí: H1 = Letadla porušují normy pro minimální rozestupy [L1]

Omezení nebezpečí: SC1 = Letadla **musí** splňovat minimální normy pro rozestupy od ostatních letadel a objektů. [H1]

Modelování řídicí struktury systému

Druhým krokem analýzy STPA je vytvoření hierarchické struktury řízení systému a modelování vzájemných vazeb systému pomocí sady zpětnovazebních řídicích smyček. Každý proces je řízen prostřednictvím určitých "řídicích akcí", jako je nakládka zavazadel, přistavení cisterny apod. STPA analyzuje takové přímé řídicí akce, aby dokázala identifikovat scénáře, ve kterých se určitá akce nebo její neuskutečnění může stát nebezpečnou. Taková analýza se provádí pomocí řídicích struktur. Každý řídicí prvek systému se skládá z modelu procesu a řídicího algoritmu. Model procesu využívá

zpětnou vazbu poskytovanou procesem k určení "přesvědčení" řídicích prvků o stavu systému. [20]

Algoritmus řízení určuje reakci řídicího prvku na jeho "přesvědčení". Například pro lidského řídicího pracovníka může být být řídicím algoritmem jeho prosté chápání procesu. U automatizovaného řídicího prvku se obvykle jedná o počítačový algoritmus. Chyby mohou pocházet z chybné zpětné vazby, chybného modelu procesu, chybného algoritmu řídicího prvku atd. Struktura řízení je kombinací všech řídicích smyček (Obrázek 4), které v systému existují, uspořádaných hierarchicky. Struktura řízení objasňuje hierarchii řízení (kdo je komu nadřazený) a také jasně definuje vlivy, které na sebe jednotlivé komponenty mají. STPA používá takové řídicí struktury ke studiu procesů. To umožňuje identifikovat nebezpečné interakce systému a odvodit případné chybějící požadavky na řídicí prvky. [20]

Identifikace nebezpečného řízení

Po definování struktury řízení systému je dalším krokem určení, jak se řízený systém může dostat do nebezpečného stavu. Nebezpečný stav je stav, který porušuje bezpečnostní omezení definovaná pro systém. STPA považuje nebezpečné stavy za důsledek neúčinného řízení. Posuzování proto pokračuje identifikací potenciálně nevhodných řídicích činností. Nebezpečné řídicí činnosti spadají do následujících čtyř obecných kategorií: [20]

1. Požadovaná řídicí akce není provedena.

2. Je provedena nesprávná nebo nebezpečná řídicí akce, která způsobuje systémové nebezpečí.

3. Potenciálně správná nebo přiměřená řídicí akce je poskytnuta příliš brzy, příliš pozdě nebo mimo pořadí.

4. Správná řídicí akce je zastavena příliš brzy.

Řídicí akce mohou být nutné k řešení poruch komponent, poruch prostředí nebo nefunkčních interakcí mezi komponentami. Nesprávné nebo nebezpečné řídicí akce mohou také způsobit nefunkční chování nebo interakce mezi součástmi. Nevhodné řídicí akce mohou, ale nemusí být přítomny ve skutečném systému. Jedná se o hypotézy, které

je třeba potvrdit nebo zamítnout na základě zkoumání chování systému, jak byl navržen a postaven. Aby bylo zajištěno úplné posouzení, musí být postupně prozkoumána každá řídicí činnost. [20]

Identifikace scénářů ztrát

Jakmile jsou rozpoznány všechny způsoby, kterými se řídicí akce stávají nebezpečnými, jsou identifikovány scénáře, které by mohly vést k takovým nebezpečným řídicím akcím. Tyto scénáře se identifikují pro každou nebezpečnou řídicí akci postupně tak, že se analyzuje celá příslušná řídicí smyčka a hledají se způsoby, jak mohou být různé části smyčky zodpovědné za nebezpečnou řídicí akci. V potaz se berou jakékoliv nesprávné zpětné vazby, neadekvátní požadavky, selhání jednotlivých komponentů systému, chyby v návrhu či další faktory negativně ovlivňující systém. Jakmile jsou identifikovány příčinné scénáře, je možné vypracovat doporučení, jak jim předcházet, a tím zabránit všem výsledným nebezpečným řídicím akcím. [20]

6. Přehled odborné publikace

Stěžejní zdroj pro tuto práci je *ICAO doc. 9859*. Jedná se o klíčový dokument pro systémy řízení provozní bezpečnosti v letectví a mnoho leteckých organizací po celém světě přijalo jeho zásady a postupy. Dokument popisuje zásady a postupy řízení bezpečnosti a poskytuje návod, jak zavést a udržovat systém řízení bezpečnosti. Je pravidelně aktualizován, aby odrážel nejnovější vývoj v oblasti řízení bezpečnosti a zajistil, že zůstane relevantní a účinný pro pracovníky v oblasti řízení bezpečnosti v letectví.

Problematice systémů řízení provozní bezpečnosti a jeho zavádění se taktéž věnuje publikace s názvem *Implementing safety management systems in aviation.* [5] Poskytuje ucelený přehled o systémech řízení provozní bezpečnosti (SMS) v letectví a praktického průvodce zaváděním SMS v leteckých organizacích. Kniha se zabývá různými aspekty SMS, včetně politiky a cílů bezpečnosti, řízení bezpečnostních rizik, zajištění bezpečnosti, podpory bezpečnosti a sledování a měření výkonnosti v oblasti bezpečnosti. Pojednává také o regulačních požadavcích a pokynech pro zavádění SMS a o organizačních a kulturních faktorech, které mohou ovlivnit úspěšnost zavádění SMS. Autoři uvádějí četné případové studie a příklady zavádění SMS v různých typech leteckých organizací, včetně leteckých společností, letišť, poskytovatelů letových provozních služeb a výrobců letadel. Kniha rovněž obsahuje praktické nástroje a šablony pro zavádění SMS, jako jsou šablony bezpečnostní politiky, kontrolní seznamy pro řízení bezpečnostních rizik a nástroje pro sledování výkonnosti v oblasti bezpečnosti.

Metoda STPA je populární a široce používaný přístup k analýze bezpečnosti a existuje mnoho publikací a studií, které tuto metodu používají k analýze systémů kritických z hlediska bezpečnosti. Pro tuto práci jsou tyto publikace přínosné zejména díky podrobným návodům a praktickým provedením analýzy v konkrétních situacích. Zde je několik příkladů:

Studie s názvem *Comparison of the FMEA and STPA safety analysis methods* [21] představuje srovnání dvou metod – FMEA a STPA, s využitím metodiky případové studie. Obě metody byly aplikovány na stejný systém pro předcházení čelním kolizím, aby bylo možné porovnat účinnost metod a zjistit, jaké jsou mezi nimi hlavní rozdíly. Výsledky analýzy FMEA byly porovnány s výsledky analýzy STPA, které byly prezentovány

v předchozí studii. Srovnání ukázalo, že analýzy FMEA a STPA poskytují podobné výsledky. Metodu porovnávání dvou a více bezpečnostních analýz využila i studie s názvem *Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems* [22], která zkoumá a porovnává výsledky rovnou čtyř bezpečnostních metod aplikovaných na systém nouzového brždění.

Publikace *Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model* [23] naopak popisuje případ využití pouze STPA analýzy, konkrétně v rámci bezpečnostní studie zabývající se technologiemi využívaných v autonomních automobilech. Z oblasti letectví lze pak uvést například studii nazvanou *Using STPA in the Evaluation of Fighter Pilots Training Programs* [24], která se věnuje problematice výcviku armádních pilotů letadel F-16 a ve které byla aplikována metoda STPA na konkrétní cvičný let těchto letounů.

7. Limitace současného stavu

Přestože se systém SMS široce rozšířil a prokázal svou účinnost, v současné době existují některá omezení, která mohou v konečném důsledku zpochybnit účinnost nastaveného systému pro řízení provozní bezpečnosti. Jedním z klíčových problémů je nedůsledné nebo neúplné zavádění SMS v organizacích. Některé společnosti nemusí plně integrovat systém SMS do svého provozu nebo nevyčlení dostatečné zdroje na jeho zavedení, což vede k nedostatkům v řízení provozní bezpečnosti. Toto může být příklad menších organizací, které často čelí při zavádění systému SMS jedinečným výzvám kvůli omezeným zdrojům, nedostatku odborných znalostí a konkurenčním prioritám. Tato omezení mohou bránit jejich schopnosti zavést spolehlivý systém řízení bezpečnosti, což je činí zranitelnějšími vůči bezpečnostním rizikům. Další důležitou věcí ohledně fungování SMS je přístup k bezpečnosti, který je v rámci tohoto systému aplikován. Mnoho implementací systému SMS má tendenci být reaktivních a zaměřují se na analýzu minulých událostí a údajů s cílem předcházet podobným událostem. Tento přístup nemusí účinně řešit vznikající rizika nebo předvídat budoucí bezpečnostní problémy.

V některých organizacích se uplatňuje kultura zaměřená výhradně na dodržování předpisů, kdy je systém SMS vnímán spíše jako soubor regulačních požadavků, které je třeba splnit než jako proaktivní nástroj pro zlepšování bezpečnosti. Tento způsob myšlení může omezit účinnost SMS při identifikaci a zmírňování potenciálních rizik. Úspěšný systém SMS závisí na aktivním zapojení a angažovanosti zaměstnanců na všech úrovních. [2]

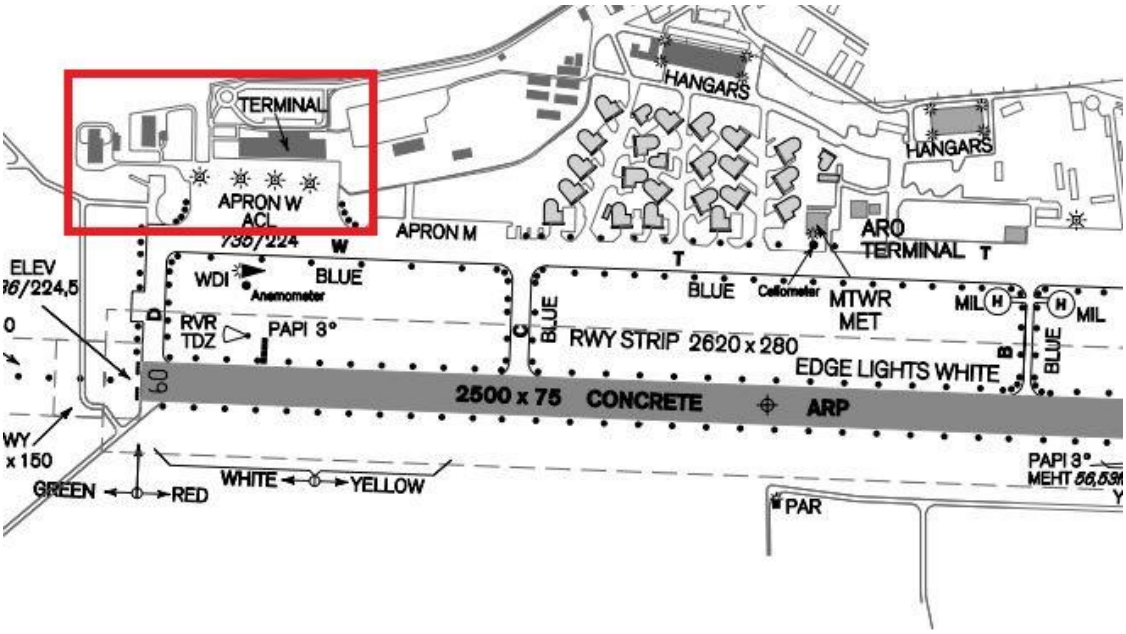
Přesné a spolehlivé údaje jsou zásadní pro efektivní hodnocení rizik a rozhodování v rámci SMS. Organizace se však mohou potýkat s problémy při shromažďování, analýze a interpretaci údajů, což může ohrozit přesnost a účinnost SMS. Mnoho organizací používá vedle SMS více systémů řízení, jako je řízení kvality nebo environmentální řízení. Integrace těchto systémů může být náročná, což může vést ke zdvojování úsilí, nekonzistentním procesům a potenciálním mezerám v řízení bezpečnosti.

8. Letiště Pardubice

Letiště Pardubice se nachází ve Východních Čechách přibližně 4 km jihozápadně od středu města Pardubice. Má status vojenského mezinárodního veřejného letiště s povoleným provozem civilních letadel. Dále má statut letiště „OPEN SKIES“ (Otevřeného nebe) pro ČR. Disponuje jednou vzletovou a přistávací dráhou o délce 2 500 metrů a šířce 75 metrů. Provozovatelem letiště je Armáda České republiky, konkrétně Správa letiště Pardubice, která se taktéž řadí mezi uživatele letiště. Dalšími subjekty působícími na letišti jsou Centrum leteckého výcviku s.p. Pardubice (CLV) a společnost East Bohemian Airport a.s. (EBA), kteří se řadí mezi civilní uživatele. [25]

8.1 Civilní část letiště

Provoz civilní části letiště má na starost společnost East Bohemian Airport a.s. (EBA). Působí pouze v západní části letiště a přístup bez omezení má pouze na odbavovací plochu WEST, jak je znázorněno na Obrázku 7. Pokud je potřeba zajistit služby v jiné části letiště, je třeba již koordinace s Armádou ČR a její povolení. [25]



Obrázek 7: Apron WEST (upraveno z [26])

Civilní uživatel letiště poskytuje níže uvedené služby a činnosti: [25]

- Odbavení cestujících a nákladu
- Služby posádkám letadel
- Technická obsluha letadel
- Navádění letadel
- Tankování letadel
- Údržba provozních budov

Pro odbavení civilních letadel disponuje pardubické letiště třemi průjezdnými stojánkami pro menší typy letadel a poté třemi otočnými stáními pro letadla kategorie C a vyšší. [26]

8.2 SMS Letiště Pardubice

Jelikož je zavedení systému pro řízení provozní bezpečnost dané zákonem, má i civilní uživatel letiště zavedený SMS pro výkon svých činností. Safety Management System splňuje všechny požadavky dané předpisy a obsahuje všechny prvky, které jsou zmíněny v kapitole 2.2.1. popisující jednotlivé složky (komponenty) SMS.

V současnosti se připravuje transformace tohoto systému, protože ve stávajícím stavu je SMS nastaven na pokrytí celého letiště a dá se tak považovat za letištní SMS. Tento stav však nevyhovuje provozovateli civilní části, jelikož aktuální SMS obsahuje velké množství prvků, jejichž činnost tento provozovatel nemůže ovlivnit. Jedná se například o údržbu provozních ploch, naváděcích světel apod. Z těchto důvodů je nutná aktivní spolupráce mezi provozovatelem civilní části letiště a armádou, která má na starosti provozní plochy letiště, řízení letového a pozemního provozu a další. Kvůli zvýšené potřebě koordinace byl zaveden výkonný orgán, který sdružuje zástupce jak civilní části, tak armády. V rámci tohoto orgánu dochází k projednávání bezpečnostních cílů na následující období, předkládají se navrhované úpravy a přijímá se například i návrh rozpočtu vyčleněného pro zajištění bezpečnosti na letišti. Nastavení současného SMS se odráží například i v plánování vnitřních auditů, kdy je nutné podle aktuálního SMS auditovat i oblasti, které podléhají kontrole armády a nelze tak jejich audit provést, protože tyto oblasti musí auditovat armáda, přičemž neumožnuje se jich účastnit. Cílem probíhající transformace je tak kromě vytvoření aktualizovaného systému pro řízení provozní bezpečnosti

odpovídajícího novodobým trendům i jeho přizpůsobení pouze činnostem provozovatele civilní části letiště. Z letištního SMS se tak stane „uživatelský“ SMS, který bude zahrnovat pouze ty činnosti, které této uživatel využívající letiště pro své účely přímo vykonává a které jsou uvedeny v kapitole 8.1.

Popis aktuálního SMS lze provést pomocí struktury jeho komponent:

Bezpečnostní politika a cíle

Bezpečnostní oddělení v Pardubicích nedisponuje širokou škálou zaměstnanců, což odpovídá hustotě provozu, která doposud rovněž nebyla vysoká. V rámci organizace jsou definovány odpovědnosti za bezpečnost, kdy hlavní slovo má manažer bezpečnosti. V rámci bezpečnostní politiky a cílů je ustanoven i kontrolní orgán, který projednává bezpečnostní cíle všech účastníků provozu letiště na následující období. V rámci orgánu se předkládají navrhované úpravy a přijímá se například i návrh rozpočtu vyčleněného pro zajištění bezpečnosti na letišti. Prohlášení o bezpečnostní politice je k dispozici na webových stránkách letiště. Organizace klade důraz na vedení podrobné dokumentace a soulad s veškerými předpisy související s provozem civilní části letiště.

Řízení bezpečnostních rizik

K identifikaci nebezpečí organizace nevyužívá žádné bezpečnostní analýzy. Pokud je třeba, využívá se k tomuto účelu setkání všech stran, které mají s aktuálně řešeným problémem spojitost. Výsledem tohoto setkání jsou bezpečnostní opatření nebo návrhy upravených postupů organizace. Rizika jsou ohodnocována na základě matice ICAO hodnocení rizik. Podstatným zdrojem dat pro identifikaci nebezpečí je systém hlášení událostí, který nabízí zaměstnancům tři způsoby, jakými mohou událost nahlásit.

Zajištění bezpečnosti

Měření bezpečnosti probíhá v podobě inspekcí, které se například často realizují při technickém odbavení letadla. Dále jsou v rámci organizace prováděny bezpečnostní audity, které zahrnují i oblasti, které má na starost výhradně armáda a je tedy nutné ji tyto konkrétní audity podstoupit, přičemž společnost EBA jakožto provozovatel civilní části bude seznámena s výsledky těchto auditů. Organizace má rovněž zavedené indikátory bezpečnosti, které jsou však spíše reaktivní a sledují již vzniklé události.

Podpora bezpečnosti

Bezpečnostní oddělení ve spolupráci s vedoucími pracovníky jednotlivých oddělení zajišťuje školení pro všechny zaměstnance. Informace, které zazní na těchto školení si zaměstnanci musí zapisovat do poznámek, jelikož následně neexistují materiály, do kterých by bylo možno nahlédnout a dané informace si připomenout. V rámci komunikace bezpečnosti je snaha vše podstatné zaměstnancům vysvětlit již při školení, přičemž problematika bezpečnosti je následně rozebírána pouze v případech, kdy dojde k jejímu ohrožení.

9. Analýza systému pomocí STPA

Bezpečnostní analýza systému byla provedena pomocí metody STPA. Z důvodu rozsáhlé analýzy jsou v některých následujících podkapitolách uvedeny pouze její části pro celkovou přehlednost práce. Kompletní analýza je poté uvedena v přílohách práce.

9.1 Stanovení účelu analýzy

Důležitým aspektem prvního kroku analýzy je stanovit si hranice analyzovaného systému. Hranice systému je nutné si stanovit hned v prvním kroku z toho důvodu, aby bylo jasně určeno, které prvky systému budou do analýzy zahrnuty a které nikoliv. Pokud by k takovému kroku nedošlo, zbytečně by to vytvářelo analýzu složitější a mohlo by dojít ke zkreslení kontrolní struktury systému. Analyzovaným systémem bude v tomto případě organizace provozující civilní část letiště. Takto definovaný systém bude v sobě zahrnovat všechny prvky a činnosti, které společnost EBA jakožto provozovatel vykonává a které jsou zmíněny v kapitole 8.1.

Následuje určení ztrát (Tabulka 2), které mohou být důsledkem nebezpečí způsobeného nevhodným provedením řídící akce. Těmto ztrátám se v systému snažíme vyhnout. Mezi ztráty se řadí vše, o co lze v systému přijít. Při odbavení letadla může dojít ke zraněním cestujících nebo pracovníků stejně jako může dojít k poškození letadla nebo odbavovací techniky. Neméně významnou ztrátou je bezesporu i časová ztráta, jelikož každé zpoždění je v letectví drahá záležitost a často způsobí další komplikace spojené s leteckým provozem. V systému taktéž může dojít i ke ztrátě relevantních bezpečnostních dat, pokud nebude funkční systém bezpečnostního hlášení apod.

V prvním kroku analýzy je dále nutné stanovit systémová nebezpečí, ke kterým by mohlo dojít na úrovni celého systému (Tabulka 3). Identifikovány byly čtyři hlavních nebezpečí (H1 až H4). Součástí definice každého nebezpečí je i jeho odkaz na ztráty, ke kterém v případě výskytu toho nebezpečí může dojít.

Tabulka 2: Systémové ztráty [tvorba autora]

#	Definice ztráty	Dodatečný popis ztráty
L-1	Zranění či úmrtí	Týká se zaměstnanců i cestujících
L-2	Poškození techniky	Zahrnuje odbavovací techniku, letadla a další technické nástroje včetně software
L-3	Finanční ztráta	Důsledek oprav, penalizací za zpoždění apod.
L-4	Časová ztráta	Např. zpoždění odletu letadla
L-5	Ztráta dat	Veškerá data související s provozem
L-6	Environmentální ztráta	Únik provozních kapalin, zplodin atd.
L-7	Fluktuace pracovníků	Odchody do jiného zaměstnání, ukončení poměru kvůli fyzické námaze apod.

Tabulka 3: Systémová nebezpečí [tvorba autora]

H-1	Postupy organizace nejsou revidovány a neodpovídají bezpečnostním předpisům. [L-2, L-3, L-4, L-6, L-7]
H-2	Personál letiště nedostává/nemá potřebné informace pro výkon své činnosti. [L-1, L-2, L-3, L-4, L-6, L-7]
H-3	Činnosti jsou vykonávány technikou a nástroji ve stavu neumožňujícím bezpečné provedení těchto činností. [L-1, L-2, L-3, L-4, L-5, L-6]
H-4	Činnosti jsou vykonávány nezpůsobilým anebo v nedostatečném počtu zastoupeným personálem. [L-1, L-2, L-3, L-4, L-5, L-6, L-7]

V prvním kroku analýzy je jako poslední úkon stanovení bezpečnostních omezení nebezpečí, které zobrazuje Tabulka 4. Jsou to obecná systémová omezení, kde v podstatě jde o negování systémových nebezpečí tak, aby bylo jasné, že k těmto nebezpečím v systému nesmí dojít. Opět je zde zachována návaznost ve formě odkazování na systémová nebezpečí v hranatých závorkách. V tomto systému tedy musí být činnosti vykonávány technikou a nástroji v takovém stavu, který umožní bezpečné provedení činností s nimi spojených a nedojde tak k různým ztrátám napříč systémem. Dále musí být všechny procesy a postupy organizace pod neustálou kontrolou, aby mohla být včas identifikována nebezpečí a následně navržena bezpečnostní opatření v případě zjištění, že aktuální postupy svým provedením mohou způsobovat ztráty. V neposlední řadě je taktéž důležité, aby všechny činnosti, které organizace provádí, byly vykonávány personálem, který je k těmto činnostem zaškolený, má všechny potřebné informace i během pracovního výkonu a je rovněž způsobilý pro výkon dané činnosti (např. zdravotně).

Tabulka 4: Systémová omezení [tvorba autora]

SC-1	Postupy organizace musí být revidovány a musí odpovídat bezpečnostním předpisům organizace. [H-1]
SC-2	Personál letiště musí dostávat/mít potřebné informace pro výkon své činnosti. [H-2]
SC-3	Činnosti musí být vykonávány technikou a nástroji v takovém stavu, který umožňuje bezpečné provedení těchto činností. [H-3]
SC-4	Činnosti musí být vykonávány způsobilým a v dostatečném počtu zastoupeným personálem. [H-4]

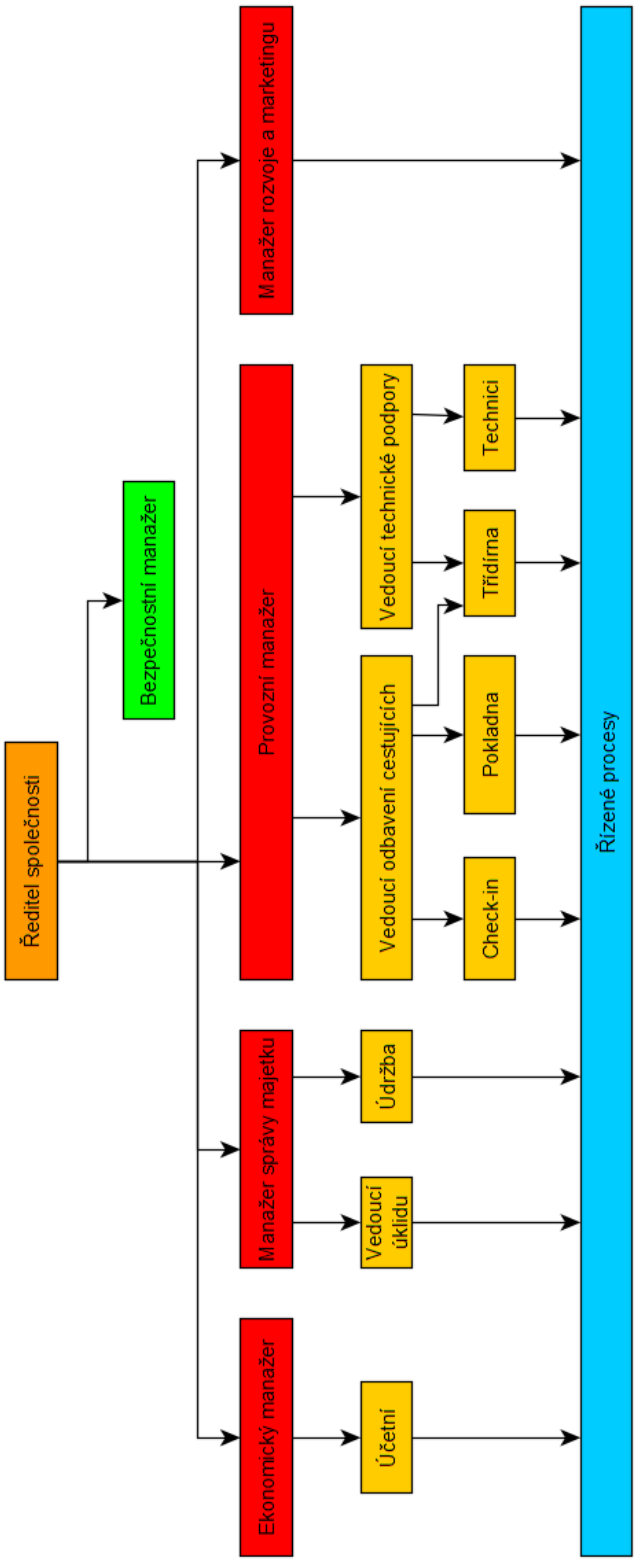
9.2 Modelování struktury systému

Ve druhém kroku analýzy se modeluje řídící sktruktura systému. Pro vytvoření této struktury je nutné znát všechny řídicí prvky, které se nacházejí v systému, a které řídicí činnosti tyto prvky provádí. V tomto kroku jsou do analýzy uváženy pouze řídicí prvky, které mohou ovlivnit provozní bezpečnost organizace.

Řídicí prvky:

- Ředitel společnosti
- Bezpečnostní manažer
- Provozní manažer
- Vedoucí směny odbavení
- Vedoucí směny technické podpory
- Technici
- Pracovníci třídírny
- Údržbář

Pro přehlednost řídicí sktruktury je přiloženo zjednodušené schéma znázorňující strukturu zaměstnanců v rámci hierarchie společnosti (Obrázek 8). Znázornění řídicích smyček zde nebylo nutné, protože řídicí činnosti řídicích prvků a zpětné vazby jsou pro některé kontroléry uvedeny v Tabulce 5 a pro všechny zbylé řídicí prvky podílející se na zajištění bezpečnosti, jejich řídicí činnosti, zpětné vazby, koordinační vazby a popisy činností, které řídicí prvky provádí na vlastní zodpovědnost, jsou uvedeny v tabulce v Příloze 1 na konci této práce. Aby byla zachována čitelnost schématu řídicí struktury, nejsou v něm uvedeny zpětné a koordinační vazby. Ze stejného důvodu jsou ve schématu vynechány vazby mezi bezpečnostním manažerem a ostatními zaměstnanci. Schéma znázorňuje všechny řídicí prvky napříč celou organizací, aby bylo schopné poskytnout komplexní přehled o zaměstnanecké struktuře. Pro účely analýzy však nejsou v potaz brány veškeré řídicí prvky, pouze ty, které mohou ovlivnit bezpečnost. Dále tak již analýza nepočítá například s řídicími prvky „Účetní“ nebo „Manažer rozvoje a marketingu“.



Obrázek 8: Hierarchie společnosti [tvorba autora]

Tabulka 5: Řídicí činnosti [tvorba autora]

Řídicí prvek	Řídicí činnost	Zpětná vazba
Provozní manažer	• Stanovuje postupy pro bezpečnou manipulaci s pozemní odbavovací technikou • Stanovuje postupy pro manipulaci s pohonnými hmotami • Navrhuje bezpečnostní opatření	• Nahlašuje bezpečnostní nedostatky • Pravidelně informuje o stavu odbavení
Safety manažer	• Zajišťuje bezpečnostní školení • Zahajuje a účastní se šetření interních událostí • Vydává bezpečnostní doporučení • Vytváří nápravná opatření	• Vydává pravidelné zprávy o bezpečnostní výkonnosti • Předkládá bezpečnostní cíle vedení organizace
Vedoucí směny technické podpory	• Dohlíží nad dodržováním postupů při odbavení letadla • Plánuje směny podřízených pracovníků • Provádí navádění letadel	• Vznáší požadavky pro zajištění bezpečnosti při odbavení (navýšení počtu pracovníků atd.) • Hlášení bezpečnostních událostí
Technici	• Plnění letadla pohonnými hmotami • Catering • Přistavení/odstavení schodů, pásového dopravníku • Catering • Doplnění vody • Toalety • Připojení/odpojení pozemního zdroje • Údržba pozemní techniky	• Provedení/neprovedení činností uvedených ve druhém sloupci • Hlášení bezpečnostních událostí

9.3 Identifikace nebezpečného řízení

Třetí krok analýzy je založený na identifikaci potenciálně nebezpečného řízení v systému. Nebezpečné řízení (UCA – Unsafe control action) je takové řízení, které může vést k nebezpečí, které následně může zapříčinit ztrátu v systému. V Tabulce 6 je vždy uvedeno, pro jakou řídicí činnost se nebezpečné řízení stanovuje. Dále jsou jednotlivé UCA rozřazeny do kategorií podle typu nebezpečného řízení. Každé UCA musí obsahovat stručný kontext a u každého typu nebezpečného řízení je na závěr uveden odkaz na nebezpečí, které může nastat jako důsledek tohoto řízení.

V Tabulce 6 je uvedeno pouze několik příkladů, kompletní tabulka, ve které je zpracován třetí krok analýzy a všechna UCA jsou řádně očíslována kvůli orientaci v dokumentu, je připojena k práci v Příloze 2. Nejčastěji identifikovaným nebezpečným řízením je řízení spadající do první a druhé kategorie, tedy že řídicí činnost nebyla vůbec provedena nebo byla provedena nevhodným způsobem způsobující nebezpečí. Naopak poslední kategorie („Řídicí činnost trvá moc dlouho, nebo byla zastavena příliš brzy“) v systému nebyla vůbec identifikována. V tabulce níže jsou všechna nebezpečná řízení označena písmenem „X“ nahrazující číslo, jelikož se jedná o výběr konkrétních UCA z většího množství identifikovaných UCA z Přílohy 2, ve které je vždy identifikován alespoň jeden příklad nebezpečného řízení pro každou řídicí činnost.

Tabulka 6: Nebezpečné řízení [tvorba autora]

Řídicí činnost	**Neprovedení řídicí činnosti povede k nebezpečí**	**Řídicí činnost je provedena nevhodným způsobem vedoucí k nebezpečí**	**Řídicí činnost je provedena příliš pozdě, brzo, nebo ve špatném pořadí**	**Řídicí činnost trvá moc dlouho, nebo byla zastavena příliš brzy**
Manipulace s odbavovací technikou		UCA-X1: Technici či jiná obsluha manipulační techniky nedodrží stanovenou rychlost manipulace při odbavení letadla [H-3]	UCA-X2: Technici či jiná obsluha přistaví manipulační techniku k letadlu ve špatném pořadí a naruší tak stanovenou bezpečnou vzdálenost [H-3]	
Zajištění bezpečnostního školení	UCA-X3: Bezpečnostní manažer nezajistí školení pro zaměstnance před nástupem do služby [H-2, H-4]	UCA-X4: Bezpečnostní manažer zajistí školení pouze pro některé zaměstnance před nástupem do služby [H-2, H-4]	UCA-X5: Bezpečnostní manažer zajistí školení pro zaměstnance až po proběhlé události [H-2, H-4]	
Plánování směn podřízených pracovníků	UCA-X6: Vedoucí směny nenaplánuje podřízené pracovníky na směny [H-4]	UCA-X7: Vedoucí směny naplánuje nízký počet podřízených pracovníků na směny [H-4]		
Stanovení postupů pro bezpečnou manipulaci s pozemní odbavovací technikou	UCA-X8: Provozní manažer nestanoví provozní postupy pro manipulaci s odb. technikou [H-1, H-2, H-3]	UCA-X9: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou neodpovídající funkcím této techniky [H-1, H-2, H-3]	UCA-X10: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou až v závislosti na probíhajícím provozu [H-1, H-2, H-3]	

9.4 Identifikace scénářů

Posledním krokem STPA analýzy je identifikace scénářů ztrát. Tyto scénáře dokreslí celkový pohled na vznik nebezpečného řízení a pomohou celkový kontext situací, proč by mohlo dojít k systémovým nebezpečím stanoveným v prvním kroku analýzy. Každý scénář musí obsahovat odkaz na nebezpečný způsob provedení řídicí činnosti, odkaz na nebezpečí, které může dané UCA způsobit a také musí obsahovat stručný popis toho, z jakého důvodu by mohla být řídicí činnost provedena nebezpečným způsobem. Níže je uveden výčet několika scénářů vztahujících se k identifikovaným případům nebezpečného řízení stanovených v předchozím kroku analýzy. Kompletní seznam scénářů je uveden v Příloze 3 této práce.

UCA-X1:

Scénář 1: Technici či jiná obsluha manipulační techniky nedodrží stanovenou rychlost manipulace při odbavení letadla [UCA-X1], protože si již nepamatují informace z dopravního řádu, a mohli by tak způsobit poškození techniky určené k odbavení letadla. [H-3]

UCA-X4:

Scénář 1: Bezpečnostní manažer z důvodu neúplné databáze zaměstnanců zajistí školení pouze pro některé zaměstnance před jejich nástupem do služby [UCA-X4] a zapříčiní tak fakt, že zaměstnanci nebudou mít k dispozici všechny informace pro výkon pracovního poměru [H-2] nebo budou činnosti vykonávány nedostatečným počtem pracovníků [H-4], jelikož bude třeba zbylé pracovníky dodatečně proškolit.

UCA-X9:

Scénář 1: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou, které však neodpovídají konkrétnímu typu a funkcím této techniky [UCA-X9], jelikož nedisponoval při tvorbě všemi technickými parametry vztahujícím se k této technice. Tímto může dojít k nesprávnému použití techniky při odbavování [H-1].

9.5 Využití výstupů analýzy v kontextu letiště Pardubice

Provedená analýza má v konečném důsledku více možností využití v rámci SMS letiště Pardubice. Dá se využít jako:

a) Vstup pro tvorbu nástrojů určených k zajištění provozní bezpečnosti
b) Podklad k rozhodování o zavedení bezpečnostních analýz v systému
c) Nástroj demonstrující možnosti systémového a proaktivního přístupu

Metodika STPA a její názorné provedení v této práci prokazuje praktické využití bezpečnostních metod v SMS, obzvláště pak v oblasti řízení bezpečnostních rizik. Podstatou všech bezpečnostních metod je především prevence vzniku incidentů, nehod a zranění. Identifikováním potenciálních nebezpečí a zavedením vhodných bezpečnostních opatření se snižuje riziko nehod a chrání se osoby před újmou. Mohou rovněž z dlouhodobého hlediska vést k úsporám nákladů. Předcházením nehodám, zraněním a škodám na majetku se organizace mohou vyhnout lékařským výdajům, pojistným událostem, právním sporům a nutnosti oprav nebo výměn. Bezpečnější pracovní prostředí jako důsledek provádění bezpečnostních metod navíc snižuje absenci a fluktuaci, což vede ke zvýšení produktivity a snížení nákladů na nábor zaměstnanců. Pomocí výstupů z analýzy lze rovněž určit prioritní problémy, které organizaci ovlivňují nejvíce a které jsou z hlediska bezpečnosti nejzávažnější. Poté lze systematicky postupovat až k méně závažným problémům. Určení priorit se ovšem může lišit u různých organizací. Konkrétně metoda STPA k tomu navíc přidává i relativně ještě nový, systémový přístup, který umožnuje analyzovat systém jako celek se zahrnutím lidského faktoru i čistě technických komponentů najednou. Letiště Pardubice v aktuální podobě SMS nevyužívá žádné bezpečnostní metody, veškeré otázky týkající se bezpečnosti společně řeší a analyzují zástupci všech zúčastněných stran při společných sezeních, pokud je tomu třeba.

Dalším příkladem využití systémového přístupu, potažmo bezpečnostních metod analyzujících celý systém je jejich možné použití jako zdroj bezpečnostních dat pro zlepšení SMS pomocí návrhu nových nástrojů. Tento postup byl využit i v této práci, kdy následující kapitoly popisují návrh zcela nových nástrojů nebo výrazně upravených, které jsou aktuálně součástí letištního SMS v Pardubicích.

10. Návrh technických nástrojů a postupů

Při návrhu nových nástrojů nebo úpravě těch stávajících bylo pracováno zejména s výstupy STPA analýzy a jejich porovnáním se skutečností, a také s faktem, že letištní systém pro řízení provozní bezpečnosti v Pardubicích prochází výraznější obměnou, kdy se transformuje z letištní verze na uživatelské SMS, jelikož provozovatel civilní části má na starosti pouze část celkového provozu na letišti a zbytek nemůže výrazněji ovlivnit.

Analýza poskytuje podklad pro tvorbu nástrojů spadajících pod různé komponenty SMS, zejména scénáře ztrát poskytují cenné informace o tom, jakým způsobem by mohlo dojít ke ztrátám v systému, jelikož spojují nebezpečně řízení a možné důvody, proč k tomuto řízení došlo, se systémovým nebezpečím, které nebezpečné řízení způsobuje. Často se v těchto scénářích opakuje například absence hlášení nebo chybějící znalosti zaměstnanců. V rámci bezpečnostní analýzy jsou stanovena celkem čtyři systémová omezení, která musí být v rámci systému aplikována. Aby byly procesy revidovány a odpovídaly bezpečnostním předpisům, musí mít bezpečností oddělení data a podklady, ze kterých vyvodí bezpečnostní opatření a zajistí tak, že procesy a postupy organizace budou odpovídat bezpečnostním předpisům. Zmíněná data poskytne například funkční systém hlášení, který představuje důležitou zpětnou vazbu od zaměstnanců a podstatný zdroj dat pro bezpečnostní oddělení, které následně tyto data využívá k identifikaci nebezpečí a návrhu bezpečnostních opatření. Systémová nebezpečí, že zaměstnanci nebudou způsobilí pro výkon práce či nebudou disponovat všemi potřebnými znalostmi je třeba vyřešit prostředky, které tomuto nebezpečí zamezí či alespoň sníží pravděpodobnost jeho výskytu. V tomto případě se jedná zejména o školení pracovníků. I s přihlédnutím ke struktuře zaměstnanců a důležitosti lidského faktoru, kdy naprostá většina činností je v rámci organizace prováděna pomocí zaměstnanců a bez většího využití počítačových technologií, byla proto vybrána tvorba nástrojů, které spadají zejména do komponent „Zajištění bezpečnosti“, „Propagace bezpečnosti“ a „Řízení bezpečnostních rizik“, ve kterých se v rámci SMS řeší výcvik zaměstnanců, hlášení událostí nebo například sledování výkonnosti v bezpečnosti

systému a struktura registru nebezpečí. Taktéž jsou navržené nástroje uzpůsobeny pouze pro ty činnosti, které vykonává provozovatel civilní části. Ve výsledku navržené vzájemné propojení nástrojů ovlivňuje celý systém pro řízení provozní bezpečnosti. Práce se věnuje návrhu několika nástrojů, které spadají do výše zmíněných oblastí. Dle výstupů z analýzy se ovšem dají najít i další oblasti a nástroje, které mohou být předmětem úprav. Dalo by se uvažovat o nástroji, který by strukturovaně řešil plánování a sestavování bezpečnostních auditů a inspekcí, nebo by například mohlo dojít k úpravám procesu školení zaměstnanců. Jedná se však o poměrně komplexní záležitosti, které by vyžadovaly řádné ozkoušení v provozu.

Pro znázornění vztahů mezi jednotlivými navrhovanými nástroji byl využit modelovací jazyk UML. Jazyk UML (Unified Modeling Language, unifikovaný modelovací jazyk) je univerzální jazyk pro vizuální modelování systémů, který nabízí přehledné znázornění celku a jednotlivých jeho částí. [29]

UML diagramy jsou tvořeny pomocí objektů, tříd a relací, které objekty a třídy propojují.

Objekt

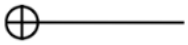
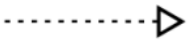
Objekt je považován za soudržný balíček dat a funkcí. Každý objekt je instancí určité třídy, která definuje společnou množinu rysů (atributů, operací a metod), které jsou vlastní všem instancím dané třídy. [29]

Třídy

Třída je definovaná jako deskriptor množiny objektů, které sdílejí stejné atributy, operace, metody, relace a chování. [29] Třídu by jinými slovy bylo možné popsat jako šablonu objektů, která určuje strukturu všech objektů příslušící k dané třídě.

Relace

Relace umožňuje ukázat na modelu, jaký je vztah mezi dvěma předměty (objekty, třídami). [29] Typy používaných relací v jazyce UML jsou na Obrázku 9.

Typ relace	Syntaxe UML zdroj cíl	Stručný popis
Závislost (Dependency)		Změna v určitém předmětu ovlivňuje význam závislého předmětu.
Asociace (Association)		Popis množiny spojení mezi objekty.
Agregace (Aggregation)		Cílový prvek je součástí zdrojového prvku
Kompozice (Composition)		Silnější forma agregace (má více omezení)
Ochranná nádoba (Containment)		Zdrojový prvek obsahuje cílový prvek
Zobecnění (Generalization)		Jeden prvek je specializací jiného prvku a lze jej nahradit obecnějším (univerzálnějším) prvkem.
Realizace (Realization)		Asociace mezi klasifikátory, kde jeden klasifikátor určuje dohodu, jejíž uskutečnění zaručuje druhý klasifikátor

Obrázek 9: Druhy relací [29]

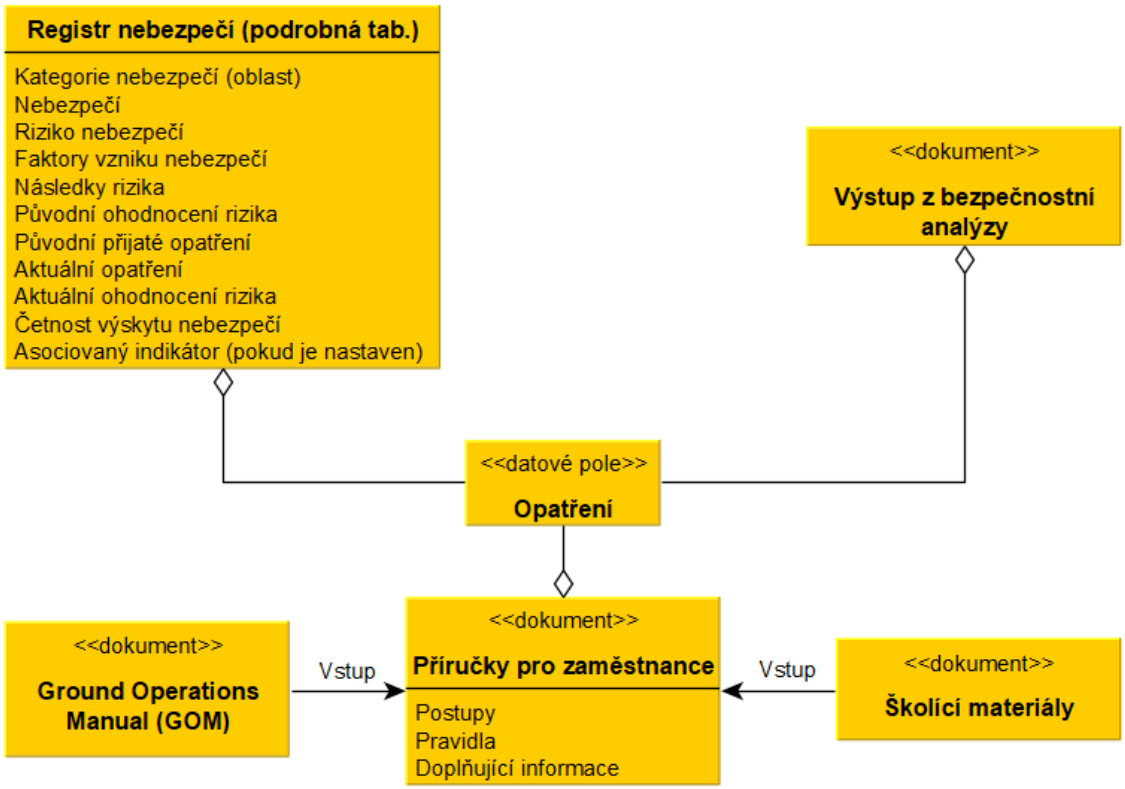
10.1 Příručka pro zaměstnance

Vzdělávání vlastních zaměstnanců patří mezi nejdůležitější pilíře zajišťující bezpečnost v organizaci. Bez odpovídajícího vzdělávání nemohou pracovníci vykonávat své pracovní povinnosti a pokud nejsou dostatečně poučeni o pracovních postupech a pravidlech, mohou ohrozit nejen sebe, ale i své kolegy. Na letišti v Pardubicích jsou v rámci SMS na pravidelné bázi školeni všichni zaměstnanci včetně vedoucích pracovníků. Školení jsou zaměřena na všechny činnosti, které daný zaměstnanec vykonává, případně bude vykonávat, pokud se jedná o vstupní školení budoucího zaměstnance. Školení zaměstnanců je v případě pardubického letiště (přesněji jeho civilní části) velice důležité i z toho důvodu, že jeho zaměstnanecká struktura odpovídá provozu letadel. V minulých letech bývalo zvykem, že většina leteckého provozu se odehrávala během letní sezóny a v zimním období byl civilní provoz na letišti minimální nebo žádný. Z tohoto důvodu provozovatel civilní části letiště využívá velké množství

brigádníků na různých pracovních pozicích, pro které jde často o první zkušenost s letectvím. Tyto brigádníci jsou zaměstnáni pouze v období vyššího provozu a v době provozního útlumu si letiště drží pouze stálé zaměstnance.

Školení probíhá každý rok, většinou před zahájením letní sezóny. Analýza STPA provedená na činnosti, které provozovatel civilní části vykonává, však identifikovala, že mezi časté důvody nevhodného řízení může mimo jiné patřit i fakt, že zaměstnanci už neví, či už si přesně nepamatují, jak danou činnost správně a podle předpisů provést. Na školeních zazní velké množství informací, čísel a pravidel a může se stát, že postupem času si už zaměstnanci nebudou vše pamatovat a budou se při pracovním výkonu řídit vlastními postupy. Tento fakt je navíc umocněn v případě, kdy zaměstnanec v zaměstnání delší čas nebyl a nemá tak postupy společnosti zažité, nebo v případě, kdy zaměstnanec vykonává více podobných zaměstnání, avšak postupy se v těchto zaměstnáních liší a může tak dojít ke zmatení.

Výše zmíněné důvody jsou společně s výstupy bezpečnostní analýzy (viz například systémová nebezpečí) dostatečným argumentem pro vytvoření tzv. příruček pro zaměstnance, které doposud nejsou na letišti zavedeny. Jedná se o nástroj, který je možné okamžitě zavést bez větších zásahů do systému a který se stane důležitým informačním zdrojem pro zaměstnance. Společná příručka pro všechny pracovníky by nebyla efektivní, jelikož by obsahovala velké množství informací, které by nebyly relevantní pro všechny zaměstnance a spíše by odrazovala od četby z důvodu zdlouhavého vyhledávání. Lépe se tedy jeví vytvoření sady příruček, které by byly určeny konkrétním skupinám zaměstnanců podle toho, jaké činnosti provádí. Příručky by byly tvořeny primárně ze školících materiálů, doplněných o informace z Ground Operations Manual (GOM) a obsahovaly by všechny nutné postupy a pravidla (Obrázek 10) tak, aby příručky obsahovaly všechny potřebné informace. Přínos takto nastavených příruček tkví taktéž v jejich možné okamžité aktualizaci v případě nově identifikovaných nedostatků a nebezpečí, v jejichž důsledku by došlo k zavedení nových nápravných opatření.



Obrázek 10: Zdroje dat pro tvorbu příruček [tvorba autora]

Pro ilustraci byla vytvořena příručka pro zaměstnance třídírny. V této konkrétní příručce jsou uvedeny všechny informace nutné ke správnému a bezpečnému provedení všech činností, které zajišťují zaměstnanci třídírny zavazadel. Kvůli obsahu interních informací je v této práci uvedena pouze jedna kapitola z této příručky, konkrétně na Obrázku 11. Obsahuje informace týkající se úkonů předcházející příletu letadla, přičemž zahrnuje informace ze školících materiálů, z GOMu (například časový údaj přistavení techniky před příletem) a obsahuje i informace převzaté z výstupů analýzy STPA (například zkouška brzd pro zamezení samovolnému rozjezdu odbavovací techniky). Realizaci příručky předcházela konzultace s vedením společnosti a průzkum mezi zaměstnanci, který vyvolal kladný ohlas na vznik tohoto nástroje.

5 Před příletem letadla

Přistavení odbavovací techniky

- Všechna odbavovací technika musí být připravena na odbavovací ploše s dostatečným časovým předstihem před příjezdem letadla na určenou stojánku.
  - **RYANAIR** – 5 minut před příletem
- Během přistavování se provede **zkouška brzd** vozidla, aby se ověřila jejich funkčnost a vozidlo se případně vyřadilo z provozu.
- Odbavovací technika musí být po jejím přistavení **zajištěna proti pohybu**, aby se zabránilo jejímu samovolnému rozjezdu a případné kolizi.
  - Zavazadlový tahač se zajišťuje ruční brzdou.
- Provede se kontrola, zdali nedošlo k vypadnutí zavazadel z přistavených zavazadlových vozíků.

Obrázek 3: Ohraničení stojánky

- **Technika nikdy nesmí žádnou svojí částí zasahovat do stání** ohraničeného červenou nepřerušovanou čarou (Obrázek 3, modrá šipka). Hrozilo by pak narušení bezpečné vzdálenosti od letadla.

FOD Check (Foreign object debris Check)

- Jedná se o kontrolu přítomnosti cizích předmětů na odbavovací ploše (Obrázek 4).
- Provádí se **před příletem a poté i před odletem** letadla, aby se předešlo nasátí těchto předmětů do motorů.

Obrázek 11: Příručka pro zaměstnance třídírny [tvorba autora]

10.2 Sada indikátorů bezpečnosti

Z provedené bezpečnostní analýzy pomocí proaktivní metody STPA lze sestavit kompletní sadu indikátorů bezpečnosti sledující bezpečnostní výkonnost organizace. ICAO v Safety Management Manuálu (ICAO doc. 9859), doporučuje všem provozovatelům, aby v rámci svého SMS měli vytvořenou sadu indikátorů, které budou zastoupeny reaktivními i proaktivními typy. Pro sestavení sady indikátorů se mohou použít všechny čtyři kroky analýzy, ať už to je stanovení účelu analýzy, kde jsou sepsána systémová nebezpečí, na která by indikátory měly včas upozornit, stejně tak lze využít i například scénáře ztrát, kde je naopak dodán i kontext ke způsobům nebezpečného řízení, respektive možné důvody, proč k nebezpečnému řízení došlo, které taktéž usnadní identifikaci indikátorů pro systém provozovatele civilní části letiště Pardubice.

Z prvního kroku STPA analýzy vyplývá, že v rámci systému nesmí nastat situace, kdy činnosti probíhají pomocí menšího počtu zaměstnanců, než je žádoucí (systémové nebezpečí označené H-4). K tomuto může v Pardubicích opravdu dojít vzhledem k zaměstnanecké struktuře, kdy velké procento pracovníků tvoří brigádníci. Proaktivní indikátor nastavený na tento problém by mohl být definován takto:

„Počet/procento případů, kdy byl počet pracovníků odbavení nižší, než je stanovené minimum.“

Obdobně by se mohl nastavit indikátor bezpečnosti sledující stav odbavovací techniky, jelikož na letišti v Pardubicích je vzhledem k nízkému objemu provozu civilních letadel v minulých letech odpovídající nízký počet pozemní techniky. V případě navýšení letového provozu, které bude významné již v roce 2023, by špatný technický stav již tak nízkého počtu techniky mohl způsobit nemalé problémy v odbavovacím procesu. Reaktivní indikátory se mohou vytvářet například podle identifikovaných systémových ztrát. Tento typ poskytuje statistický pohled na bezpečnostní výkonost systému, tudíž indikátory nastavené na sledování systémových ztrát tomu plně odpovídají. Příkladem reaktivního indikátoru sledující systémové ztráty by mohl být:

„Počet incidentů souvisejících s odbavením letadla.“

Důležité je také stanovení přiměřeného počtu indikátorů, které budou poskytovat dostatečný vhled do bezpečnostní výkonnosti systému, zároveň budou měřitelné a nebude jich příliš mnoho, poněvadž by to spíše způsobovalo problémy s kontrolou správnosti velkého množství údajů. Na letišti v Pardubicích je momentálně nastavená sada devíti indikátorů bezpečnosti, ve které převažuje reaktivní typ indikátorů. Konkrétní znění indikátorů není v této práci kvůli citlivosti informací uvedeno. Pro budoucí vývoj by však bylo vhodné zavést i proaktivní indikátory bezpečnosti, které by na rozdíl od jejich reaktivních protějšků dokázaly upozornit včas na možný výskyt nebezpečí v organizaci ještě před tím, než by ve skutečnosti nastala. V Tabulce 7 je navržena sada indikátorů bezpečnosti kombinující reaktivní i proaktivní typy indikátorů navržených pomocí výstupů STPA analýzy společně s definovanými zdroji dat. U všech indikátorů se předpokládá, že by byly sledovány po období jednoho roku, což je u indikátorů standardní doba, po které se záznamy vyhodnocují a stanovuje se další postup.

Tabulka 7: Sada indikátorů bezpečnosti [tvorba autora]

Druh indikátoru	**Definice indikátoru**	**Zdroj dat**
Proaktivní	Počet/procento případů, kdy byl počet pracovníků odbavení nižší, než je stanovené minimum	Databáze plánování směn zaměstnanců
	Počet odbavovací techniky ve vyhovujícím technickém stavu umožňujícím bezpečné provedení činnosti	Denní záznamy techniky
	Procento proškolených zaměstnanců	Databáze zaměstnanců
	Poměr plánovaných a neplánovaných auditů a inspekcí	Dokument plánující vnitřní audity a inspekce
Reaktivní	Počet událostí souvisejících s činnostmi organizace	Systém bezpečnostního hlášení, inspekce
	Počet poranění osob souvisejících s činnostmi organizace	Kniha úrazů
	Počet nově přijatých bezpečnostních opatření	Registr nebezpečí
	Počet bezpečnostních hlášení pracovníků	Systém bezpečnostního hlášení

Další postup s nastavenými indikátory představuje nastavení bezpečnostních cílů. Jedná se rozhodnutí jednotlivce (bezpečnostního manažera) nebo skupiny lidí, kteří si stanoví cíle pro následující období a nastavené indikátory budou sloužit k ověření toho, zda bylo cílů dosaženo nebo je zapotřebí dalších úprav systému, jelikož indikátory zaznamenaly větší než přípustný počet naměřených hodnot (nebo hodnoty mimo definovaný interval).

Použití indikátorů:

1) *„Počet/procento případů, kdy byl počet pracovníků odbavení nižší, než je stanovené minimum“*

Jelikož je v Pardubicích velké množství brigádníků, může nastat situace, kdy nebude na směně dostatek lidí pro výkon zaměstnání (systémové nebezpečí H-4), což by byl výrazný problém z hlediska bezpečnosti, kdy by méně zaměstnanců muselo dělat více činností pod větším tlakem způsobeným například časovým omezením trvání činnosti. V tomto případě by se definovaly požadavky na minimální počet zaměstnanců a indikátor by zaznamenával případy, kdy takového počtu dosaženo nebylo. Pokud by záznamy indikátoru překonávaly stanovené cíle související s počtem pracovníků, muselo by dojít k navýšení počtu zaměstnanců.

2) *„Počet bezpečnostních hlášení pracovníků“*

Hlášení událostí kromě auditů a inspekcí představuje hlavní zdroj dat pro bezpečnostní oddělení na letišti v Pardubicích, což je označeno i v STPA analýze jako častý feedback od zaměstnanců. Za předpokladu, že se nastaví funkční systém hlášení je možné nastavit indikátor, který bude sledovat počet hlášení zaměstnanců. Pokud tento indikátor zaznamená větší množství hlášení, než je pro bezpečnostního manažera přípustné (zde se naráží na problematiku toho, co je vlastně přípustné), muselo by dojít k prošetření problematických oblastí, které byly nahlášeny, jelikož navržená opatření zřejmě nefungují tak, jak by měla.

3) *„Počet odbavovací techniky ve vyhovujícím technickém stavu umožňujícím bezpečné provedení činnosti“*

Tento indikátor souvisí se systémovým nebezpečím H3. Díky tomu, že dříve nebyl v Pardubicích velký provoz civilních letadel je na letišti odpovídající nízký počet odbavovací techniky. S nárustem provozu a současným výpadek techniky by letiště nebylo schopné odbavovat. Musí se tedy pečlivě hlídat, zda je všechna technika v pořádku.

4) *„Procento proškolených zaměstnanců“*

Indikátor odkazuje na systémová nebezpečí H2 i H4, přičemž i z odborných konzultací se zástupci letiště vyplynulo, že se může stát, že činnost bude vykonávat zaměstnanec k tomu neproškolený. U tohoto indikátoru nejspíš nejde nastavit jiný cíl než 100 % s tím, že jakmile indikátor klesne pod tuto hodnotu, bude muset dojít k nápravným opatřením v procesu školení tak, aby k podobné situaci v budoucnu už nedošlo.

5) *„Poměr plánovaných a neplánovaných auditů a inspekcí“*

Indikátor odkazuje na systémové nebezpečí H1, tedy že procesy a postupy organizace nebudou odpovídat bezpečnostním předpisům. V případě vzrůstajícího počtu hlášení je možné jako nápravné opatření či ověření problematických oblastí provést neplánovaný audit. Pokud indikátor zaznamená nepoměr ve prospěch neplánovaných auditů, znamená to nejspíš, že opatření a postupy bezpečnostním předpisům neodpovídají a je zapotřebí je revidovat.

6) *„Počet událostí souvisejících s činnostmi organizace“*

Tento indikátor odkazuje na systémové ztráty bez rozlišení na konkrétní typy incidentů. V současném SMS je zavedeno několik indikátorů sledujících různé typy událostí, ale většinou nic nezaznamenají, tudíž se nabízí sloučení více indikátorů do jednoho. Slouží jako statický údaj pro přehled o bezpečnostní výkonnosti v organizaci.

7) *„Počet poranění osob souvisejících s činnostmi organizace“*

Tento indikátor stejně jako předchozí odkazuje na systémovou ztrátu – konkrétně na poranění osob. Cílová hodnota by měla být 0 (takto je nastaven i v současném SMS), v případě zaznamenání by měla být stanovena nápravná opatření.

8) *„Počet nově přijatých bezpečnostních opatření“*

Indikátor sledující počet přijatých opatření poskytuje skrze tento počet pohled na (ne)účinnost opatření, kdy méně záznamů může značit účinnost opatření a že procesy jsou z hlediska bezpečnosti nastavené správně, ale i dokazuje, že jsou procesy revidovány, jelikož zaznamenaná opatření jsou důkazem aktivity vyvinuté bezpečnostním oddělením s cílem zajištění bezpečnosti.

10.3 Systém hlášení událostí

Hlášení událostí představuje jeden z nejdůležitějších zdrojů bezpečnostních dat, které má bezpečnostní oddělení organizace k dispozici. Důkazem toho je i provedená bezpečnostní analýza, která identifikovala, že absence hlášení událostí od zaměstnanců společnosti může vést k výskytu systémových nebezpečí. Aktuální podoba systému hlášení bezpečnostních událostí reflektuje nastavení SMS na celé letiště, což je pro probíhající transformaci SMS rovněž nežádoucí. Cílem tohoto návrhu je vznik nástroje, respektive návrh kompletního procesu hlášení, který bude zaměřen pouze na potřeby a činnosti společnosti provozující civilní část letiště, protože i kdyby se stala například událost na pojížděcí dráze letiště (vyjma případů navádění letadel), bude tuto událost šetřit armáda.

Prvotní podmínkou pro nastavení systému hlášení je školení zaměstnanců zaměřené na hlášení událostí v organizaci. Je nezbytné zaměstnance poučit o způsobech hlášení a druzích hlášení (povinné x dobrovolné). Letiště Pardubice se v tomto případě rozhodlo, že nebude po zaměstnancích vyžadovat rozlišování událostí spadajících do povinného či dobrovolného systému hlášení, místo toho pracovníky instruuje, aby hlásili, pokud možno vše, co jim přijde v nepořádku nebo co bezprostředně ohrožuje bezpečnost. Zde však může nastat problém, že zaměstnanci nedokáží rozlišit, zda daná událost ovlivňuje bezpečnost či nikoliv a ve výsledku ji nenahlásí. Z tohoto důvodu je součástí navrhovaných příruček pro zaměstnance kapitola zaměřená pouze na hlášení událostí, ve které jsou specifikovány způsoby hlášení i co se má hlásit společně s uvedenými příklady.

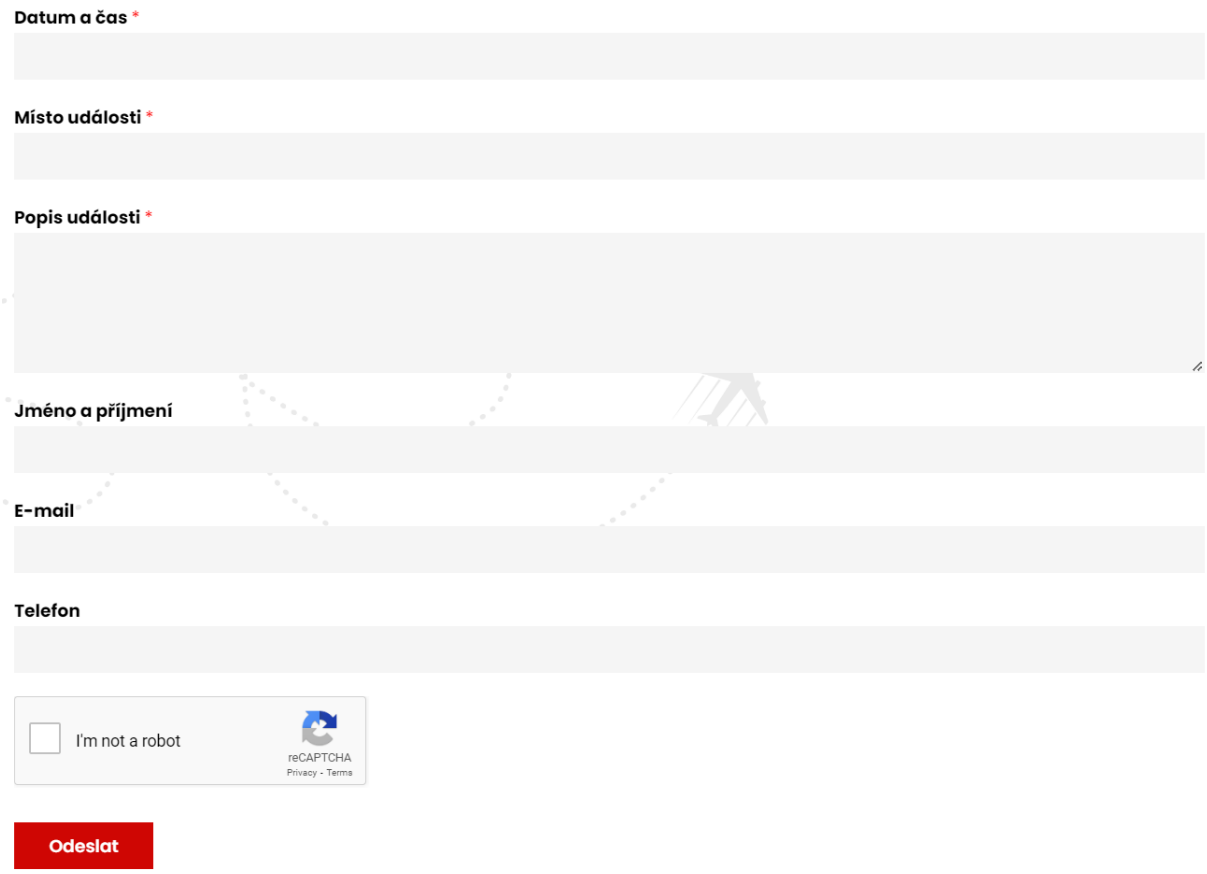
Dalším krokem je vytvoření webového portálu, který bude sdružovat všechny druhy hlášení událostí a bude také poskytovat informace o tom, jak vyplňovat hlásící formuláře apod. Z hlediska poskytování informací by byl obsah informací velmi podobný kapitole z příruček pro zaměstnance zaměřené na bezpečnostní hlášení. V současném stavu se na webových stránkách nachází jednoduchý formulář pro hlášení na jednom místě a podrobný formulář ke stažení nebo online vyplnění se nachází v jiné sekci webových stránek. Tento způsob se jeví neprakticky a v návrhu systému hlášení událostí je počítáno s tím, že všechny způsoby hlášení budou umístěny v jedné dedikované webové sekci, jejíž součástí bude rovněž podrobný popis způsobu vyplňování a odevzdávání

hlásících formulářů. Tento návrh je podpořen zpětnou vazbou od zaměstnanců, kdy jako odpověď na to, proč nevyužívají systém hlášení, uváděli jako důvod to, že ani neví, kde takové formuláře najdou a tím pádem se spokojí pouze s tím, že daný problém nahlásí svému vedoucímu.

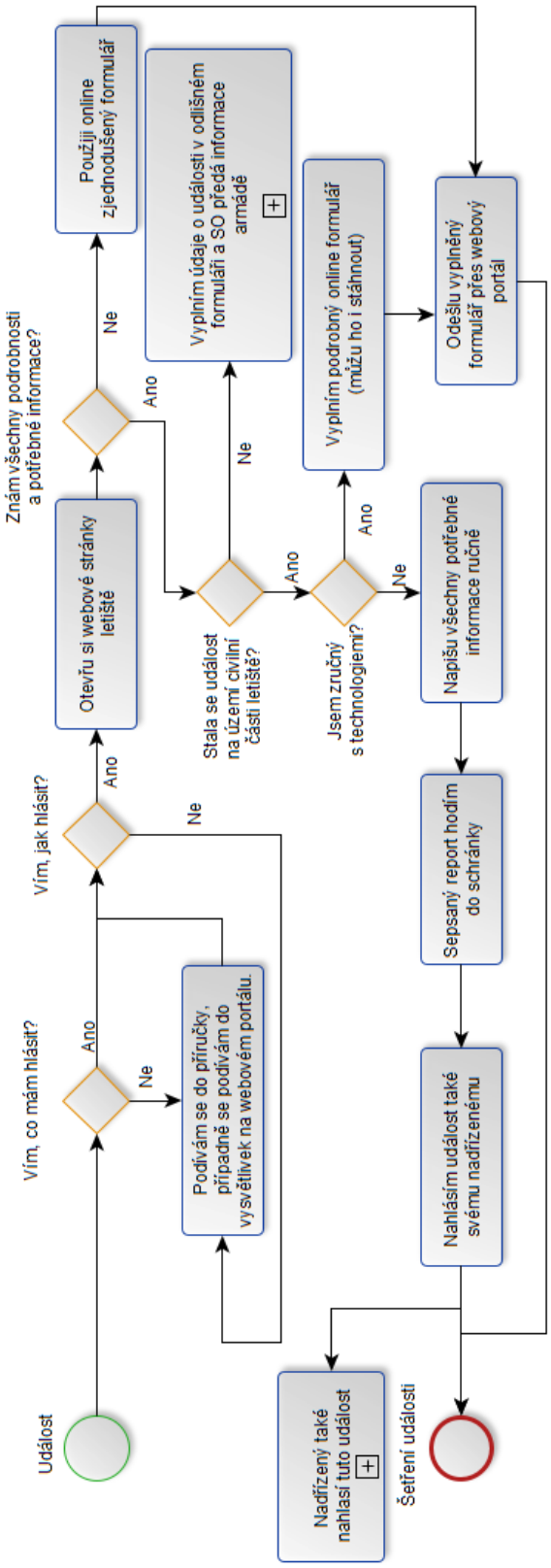
Stávající způsoby hlášení jsou zastoupeny jednoduchým formulářem (Obrázek 12), podrobným formulářem, který je možné vyplnit online, nebo vytisknout a vyplnit ručně, a poslední způsob je ručně sepsané hlášení, které následně zaměstnanci vhodí do určené schránky u administrativní budovy na letišti. Všechny zmíněné způsoby umožňují anonymizaci. Postrádána je však už informace, kdy mají zaměstnanci využít ten který způsob hlášení. V návrhu nástroje je počítáno s tím, že jednoduchý formulář by měl být využit v případě, kdy zaměstnanci neznají všechny podrobnosti o události a nebyli by schopni vyplnit podrobný formulář. Pokud by však znali podrobnosti o události (například v případě, že byli jejími přímými účastníky), byli by odkazování na vyplnění podrobného formuláře, který by poskytl dostatek informací pro bezpečnostní oddělení. Logiku rozhodování znázorňuje Obrázek 13. V rámci systému hlášení by toto mělo být ošetřeno způsobem, že si zaměstnanec vybere ze dvou možností – zná všechny informace a tím pádem ho systém odkáže na vyplnění podrobného formuláře. V tomto případě se však v návrhu počítá s výraznou proměnou tohoto formuláře. Současná verze formuláře, která je znázorněna na Obrázku 14 odpovídá nastavenému SMS a připomíná spíše formulář určený na hlášení událostí související s letovým provozem. Revidovaný formulář (Obrázek 15) by byl zaměřen pouze na činnosti, které zajišťuje provozovatel civilní části letiště. Jeho struktura byla při návrhu inspirována metodou STPA, kdy byly analyzovány všechny možné výstupy (nevhodné řízení, scénáře, ztráty apod.), které tato metoda poskytuje a dle toho byl strukturován i tento formulář. Pro ilustraci je navrhovaný formulář i vyplněn, přičemž všechny vyplněné informace byly vymyšleny pouze pro účely této práce a nepopisují skutečnou událost. Navrhovaný formulář kombinuje kolonky, kde by se pouze vybíralo z nabízených možností a pole, kde je nutné informace vypsat. Tímto by se sjednotil výstup z bezpečnostních metod a ze systému hlášení s cílem rychlejšího zpracování dat a řízení bezpečnostních rizik.

Pokud by zaměstnanec neznal všechny potřebné informace pro vyplnění podrobného formuláře, systém by ho odkázal na vyplnění jednoduchého formuláře, který zajistí, že událost bude přinejmenším zaznamenána. Tento formulář samozřejmě nepřinese

bezpečnostnímu oddělení všechny nutné informace k řádnému prošetření události, představuje však přijatelnou alternativu ke složitějšímu formuláři, protože se může stát, že pokud zaměstnanci nebudou mít všechny informace a tím pádem nebudou vědět, co mají do podrobného formuláře vyplnit, mohlo by v případě absence jednoduchého formuláře dojít k situaci, že zaměstnanci danou událost nenahlásí jen kvůli tomu, že nevěděli, co mají ve formuláři vyplnit. K tomu zůstane samozřejmě i možnost podat hlášení pomocí ručně psaného reportu. Důležité však je, aby všechny informace o hlášení, druhy hlášení a způsoby podání byly dostupné na jednom místě a byly vysvětlené tak, aby zaměstnanci přesně věděli, co mají vyplnit a jaký formulář mají použít. V návrhu je počítáno i s možností hlášení událostí mimo působnost provozovatele civilní části (části letiště pod kontrolou armády), kdy by v rámci formuláře bylo specifikováno, že se nejedná o činnosti spojené s civilní částí a bylo by popsáno, kde přesně se daná událost na letišti stala. Tento formulář by pak oddělení bezpečnosti předalo armádě.



Obrázek 12: Jednoduchý formulář [27]



Obrázek 13: Schéma využití formulářů [tvorba autora]

Hlášení události v civilním letectví

Druh hlášení: Povinné ☐ Dobrovolné ☐ Anexovaná letadla ☐

Datum události:	**Místní čas události:**	**Letiště:**	**Místo na letišti:** *Místo, kde došlo k události* Vyber místo
Číslo letu:	**Typ letadla:**	**Poznávací značka:**	**Provozovatel letadla:**
Letiště odletu:	**Letiště určení:**	**Posádka - počet:**	**Cestující - počet:**

Popis události:

Popište prosím a co možná nejpřesnější zaznamenejte průběh události. Uveďte maximum informací, které jsou Vám k danému letu a/nebo události známy (např. poškození letadla /techniky, zranění/úmrtí osob, náklad - druh/DGR, množství LPH v letadle apod.). ***Každá sdělená informace je důležitá!***

Jméno a příjmení oznamovatele: *Nepovinný údaj.*	**Telefonní číslo:** *Nepovinný údaj.*	**E-mail:** *Nepovinný údaj.*

Vyplněný formulář odešlete na adresu safety@airport-pardubice.cz

Obrázek 14: Aktuální podrobný formulář [28]

Vymezení události			
Datum události: *10. února 2023*	**Čas události:** *13:15*	**Činnost:** *Technické odbavení letadla*	**Bližší specifikace činnosti:** *Odmrazování*
Popis události			
Popis toho, co se stalo: *Během odmrazování letadla před jeho odletem natekla odmrazovací kapalina do pravé motorové gondoly.*			
Příčiny vzniku události: *Byla zvolena špatná pozice odmrazovacího vozu vůči letadlu.*		**Následky události:** (včetně zranění osob, poškození techniky apod.) *Výpary v kabině cestujících.*	
Doplňující informace			
Další informace: (místo, letadlo, číslo letu apod.) *Stojánka W5, letadlo A320, registrace HA-XXX*		**Druh hlášení:** (zaškrtněte) *Povinné / nepovinné*	
Kontaktní údaje (nepovinné)			
Jméno a příjmení: *Jan Novák*		**Telefonní číslo:** *123456789*	**E-mail:** *j.novak@seznam.cz*

Obrázek 15: Aktualizovaný formulář [tvorba autora]

Výše navržený formulář se tedy plně zaměřuje na činnosti, které vykonává provozovatel civilní části letiště a vede zaměstnance pro vyplnění podstatných informací o události, které budou následně zpracovány bezpečnostním oddělením.

10.4 Dotazníky

Hlášení událostí je nezbytný informační zdroj pro vytváření nápravných opatření a dalších kroků souvisejících se zajištěním provozní bezpečnosti. Existuje však možnost, že tímto nástrojem nebudou zachyceny všechny problémy vyskytující se v organizaci. Jako alternativa doplňující systém hlášení událostí se jeví využití dotazníků zaměřených

na různé oblasti podle toho, jaké informace bezpečnostní oddělení aktuálně potřebuje pro vytvoření si přehledu o bezpečnostní situaci. Výstupy z těchto dotazníků nebudou mít stejnou váhu jako z hlásících systémů, ale mohou informovat o skrytých nebezpečích, která nemusí být na první pohled vidět.

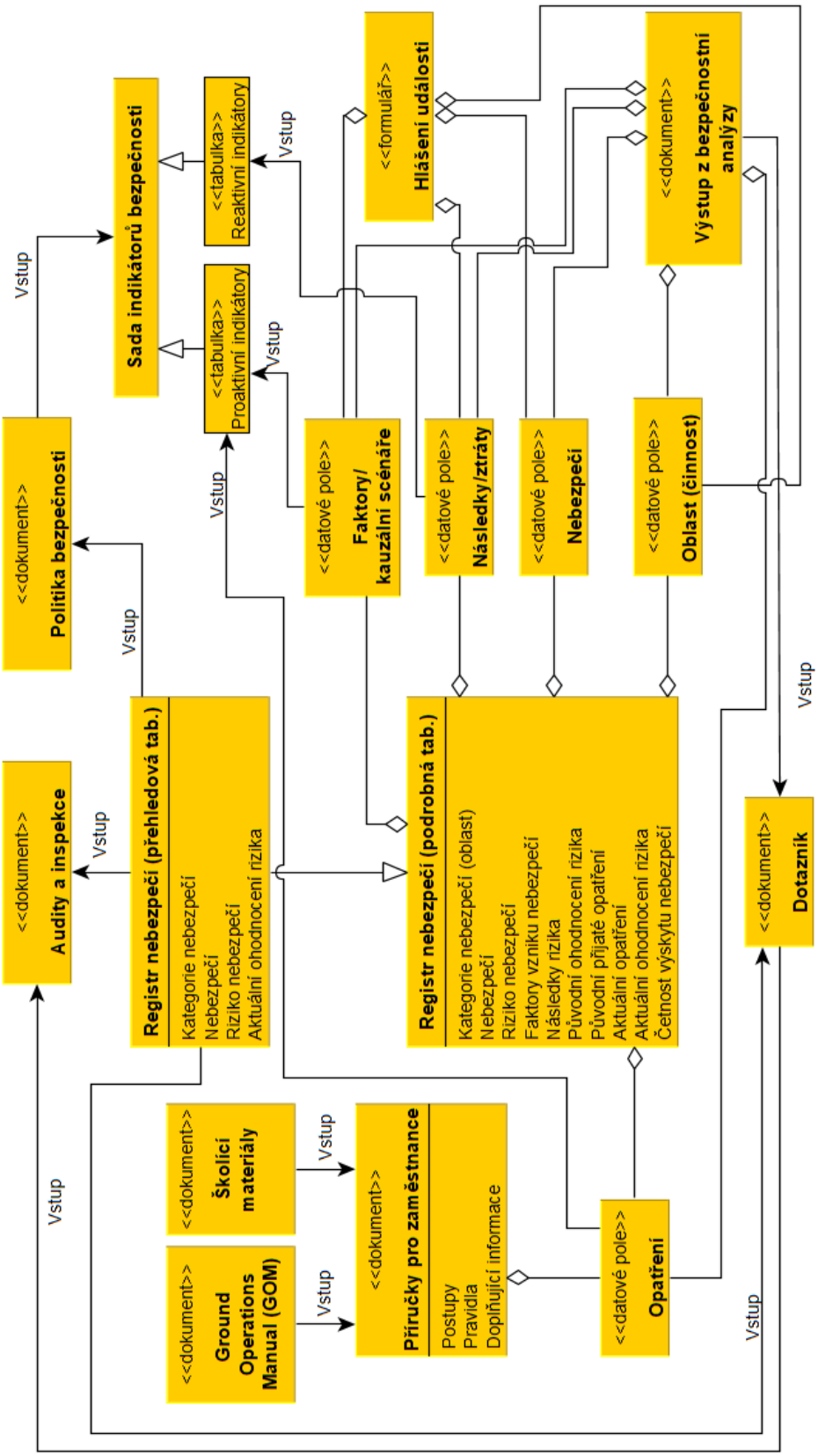
Dotazníky mohou být obecného charakteru, aby maximálně pokryly všechny zaměstnanecké pozice, nebo mohou být konkrétněji zaměřeny na oblast, kterou označila analýza za problematickou. Příkladem tedy může být dotazník konkrétně zaměřený na hlášení událostí. Při tvorbě dotazníku by měly převažovat otázky, které musí být definovány tak, aby nutily respondenty volit mezi nabízenými odpověďmi. Tyto otázky pak mohou být doplněny o ty, které vyžadují písemnou odpověď. Podstatné je také strukturování otázek a odpovědí způsobem, kdy je z hlediska přínosu pro bezpečnost lepší volit konkrétní odpovědi místo obecných typu „Ano“ a „Ne“. Některé otázky lze pojmout formou testu, kdy nabízené možnosti odpovědi ověří, zda zaměstnanci znají či neznají postupy a pravidla organizace a podle výsledků lze následně určit opatření či provést mimořádné školení. Nezbytnou součástí každého dotazníku by taktéž měla být informace o důvodu a následném využití daného dotazníků, aby zaměstnanci byli srozuměni s tím, proč se po nich chce vyplnění dotazníku.

Příklady otázek zaměřené na systém hlášení událostí:

1. *Popište, jak postupujete v případě, kdy se stane nějaká událost během výkonu služby:*
   Odpověď:
2. *Kterou z následujících událostí byste zařadil(a) do systému dobrovolného hlášení?*
   a) Vyjetí ze vzletové, přistávací nebo pojezdové dráhy
   b) Poškození letadla zařízením na pozemní odbavování
   c) Neprovedení popříletové kontroly letadla
   d) Natankování znečištěného nebo nesprávného paliva
3. *Máte nějaké připomínky ke stávajícímu systému bezpečnostního hlášení?*
   Odpověď:
4. *Který z následujících způsobů hlášení v případě potřeby využíváte?*
   a) Jednoduchý formulář *b) Podrobný formulář*
   c) Ručně psané hlášení *d) Hlášení nadřízenému*

10.5 Propojení navrhovaných nástrojů

Všechny výše zmíněné nástroje je nutné zakomponovat do safety management systému, aby nástroje byly efektivní z hlediska zajištění provozní bezpečnosti a aby výstupy z těchto nástrojů mohly být využity v dalších částech SMS. Toto vzájemné propojení nejlépe znázorňuje Obrázek 16. Výstupy z bezpečnostních analýz a ze systémů hlášení událostí se jednak zpracují v registru nebezpečí, mohou však být rovnou využity při tvorbě a úpravě dalších nástrojů, které jsou součástí SMS. Příkladem může být identifikace faktorů a kauzálních scénářů události, které kromě zaznamenání v registru mohou být okamžitě využity k tvorbě proaktivních indikátorů bezpečnosti. Samotný registr nebezpečí, který je v návrhu lehce pozměněný oproti stávajícímu o několik aspektů (následky, faktory a předchozí opatření), slouží jako propojovací nástroj zbylých navržených nástrojů a je v navrhovaném systému rozdělen na dvě tabulky, kde hlavní tabulka (Tabulka 8) bude obsahovat všechna důležitá a relevantní data týkající se identifikovaných nebezpečí a druhá, přehledová tabulka (Tabulka 9), bude poskytovat okamžitý přehled o stavu identifikovaných nebezpečí, bude z ní na první pohled patrné, která oblast systému aktuálně vyžaduje největší pozornost a lze ji využít i pro plánování vnitřních auditů a inspekcí v organizaci. Identifikované nebezpečí zaznamenané v tabulce je pouze ilustrační. Ke stejnému účelu mohou být využity rovněž výstupy z dotazníků. Jako zdroj dat pro skládání dotazníků mohou opět posloužit výstupy z bezpečnostních analýz či záznamy z registru nebezpečí. Součástí systému jsou taktéž příručky pro zaměstnance, které jsou primárně tvořeny na základě školících materiálů, případně údajů z GOM. Tyto příručky však nabízejí možnost okamžité aktualizace o nově přijatá bezpečnostní opatření, která jsou navržena z dat registru nebezpečí nebo přímo v rámci výstupů bezpečnostních analýz. Přehledová tabulka registru i její podrobnější varianta dále může posloužit jako zdroj dat pro tvorbu bezpečnostních cílů na následující období společně s tvorbou sady indikátorů bezpečnosti, které budou zaznamenávat, zdali bylo těchto cílů dosaženo či nikoliv.



Obrázek 16: Schéma propojení nástrojů [tvorba autora]

Příručky pro zaměstnance

Vstup: Příručky tvořeny ze školících materiálů, GOM doplněné o přijatá bezpečnostní opatření

Indikátory bezpečnosti

Vstup: Indikátory lze sestavit v závislosti na identifikovaných nebezpečích, faktorech a ztrátách, nebo například dle navrhovaných opatření a stanovených bezpečnostních cílů

Hlášení událostí

Výstup: Identifikace nebezpečí, faktorů, kauzálních scénářů, následků, ztrát a problematických oblastí systému

Dotazníky

Vstup: Problematické oblasti identifikované v registru nebezpečí nebo s pomocí bezpečnostních analýz

Výstup: Výsledky dotazníků mohou pomoci například ke stanovení programu vnitřních auditů a inspekcí

Registr nebezpečí

Vstup: Identifikace nebezpečí, faktorů, kauzálních scénářů, následků, ztrát a problematických oblastí systému

Výstup: Bezpečnostní opatření navržená v závislosti na výsledcích risk managementu s využitím dat v registru, podklady pro plánování auditů a inspekcí, data pro stanovení bezpečnostních cílů na další období

Výstupy z bezpečnostních analýz:

Výstup: Identifikace nebezpečí, faktorů, kauzálních scénářů, následků, ztrát a problematických oblastí systému

Tabulka 8: Podrobná tabulka registru [tvorba autora]

Kategorie nebezpečí	Nebezpečí	Riziko	Faktory vzniku nebezpečí	Následky nebezpečí	Původní ohodnocení rizika	Původní opatření	Současné bezpečnostní opatření	Současné ohodnocení rizika	Četnost
Technické odbavení	Nedodržení bezpečné vzdálenosti při manipulaci s odb. technikou	Střet s letadlem nebo jinou odbavovací technikou	Nedodržení dopravního řádu – překročení rychlostních limitů	Poškození techniky, zranění	3C/3B	Nebylo stanoveno	Snížení rychlosti manipulace s technikou během odbavení	1C / 1B	1

Tabulka 9: Přehledová tabulka registru [tvorba autora]

Nebezpečí	Kategorie nebezpečí	Riziko	Ohodnocení rizika
Nedodržení bezpečné vzdálenosti při manipulaci s odb. technikou	A, B	Střet s letadlem nebo jinou odbavovací technikou	3C/3B

Jednotlivé nástroje jsou navrhovány takovým způsobem, aby odpovídaly činnostem organizace, ale také aby podporovaly tok informací (bezpečnostních dat) napříč systémem pro řízení provozní bezpečnosti s cílem sjednotit a pokud možno zefektivnit proces řízení rizik. Názornou ukázkou je návrh příručky pro zaměstnance obsahující kapitolu vysvětlující zaměstnancům, jak funguje systém hlášení, co mají při hlášení vyplnit a jaké události mají hlásit. Ty samé informace by pak měly být i na samotném webovém portálu hlášení událostí, tudíž proces hlášení by pak měl být pro zaměstnance jednodušší. V rámci formuláře hlášení událostí jsou zaměstnanci vedeni k vyplnění konkrétních informací o události jako jsou například následky či příčiny události, které i přes to, že budou identifikovány subjektivně dle pohledu zaměstnanců, mohou proces zpracování události a identifikace nebezpečí zrychlit. Všechny tyto informace ze systému hlášení následně budou zapsány do registru nebezpečí, který ve výsledku poskytne strukturovaný přehled o všech identifikovaných nebezpečích v systému a poskytne manažerovi bezpečnosti okamžitý přehled o problematických oblastech v organizaci. V rámci řízení rizik budou v registru nebezpečí stanovena nápravná opatření, která se po schválení mohou v podstatě okamžitě zanést do příruček pro zaměstnance a tím se tok informací dostane zpět k příručce.

Organizace společně s transformací aktuálního SMS přechází na sdílená webová uložiště (MS Sharepoint), což představuje další možnosti aplikace navržených nástrojů, kdy příručky nemusí být pouze ve fyzické formě přímo na pracovišti, ale mohou být dostupné online stejně jako například systém hlášení a formuláře, které zaměstnanci vyplňují, mohou býti k dispozici v online uložišti na jednom místě, ze kterého by tyto formuláře šli odesílat přímo bezpečnostnímu oddělení ke zpracování.

11. Diskuze výsledků

Práce nabízí ucelený pohled na aktuální stav v oblasti řízení bezpečnosti v letecké dopravě, zejména pak poskytuje detailní popis fungování systému pro řízení provozní bezpečnosti (SMS), který byl pro tento účel zaveden v organizacích nejen v leteckém odvětví. Postup řešení práce byl založen na analýze teoretických informací týkajících se popisu Safety Management Systému, jeho konkrétní podobě na letišti v Pardubicích a analýze systémového přístupu k bezpečnosti, což bylo podpořeno praktickou aplikací metody STPA využívající tento přístup. Bezpečnostní analýza byla aplikována na systém představující činnosti prováděné provozovatelem civilní části letiště Pardubice – společností EBA. Lze se domnívat, že tento předložený výzkum nabízí nové unikátní poznatky využitelné pro další výzkum v dynamickém prostředí odvětví bezpečnosti v civilním letectví. Z práce je patrné, že systém pro řízení provozní bezpečnosti patří mezi vůbec nejdůležitější pilíře letectví, ve kterém je bezpečnost vždy na prvním místě a jenž indikuje důležitost přínosů této diplomové práce.

Model STAMP využívající systémový přístup je postaven na pevných teoretických základech a poskytuje nový pohled na systém ve smyslu jeho kontrolní struktury a hierarchie. Otázkou zůstává, jestli jsou letecké organizace schopné implementovat nový systémový přístup v praxi. Jedná se stále o relativně nový přístup, v současnosti mnoho společností spíše klade důraz na kvalitní a efektivní identifikování nebezpečí a řízení rizik spojených s již vzniklou nehodou, přičemž analyzují jednotlivé subjekty, které mohly ke vzniku události přispět, ale už k tomu nepřidávají celkový pohled na kontext systému jako celku. Jak totiž tvrdí i výše zmíněná systémová teorie – selhání systému je důsledek špatného řízení a špatné kooperace komponent systému, nikoliv pouze selhání jeho jednotek. V případě nového systémového přístupu je důležité si uvědomit, jak systém a jeho jednotlivé části nebo subsystémy fungují. Pokud porozumíme systému, budeme schopni určit způsoby interakce tohoto systému s jeho okolním prostředím a budeme snadněji umět identifikovat, jak by takový systém měl fungovat, aby dosáhl žádoucích výsledků. V dnešní době jsou systémy komplexnější a více vzájemně propojené, než tomu bývalo dříve. Metoda STPA, která byla použita v této práci, dokáže takové systémy zpracovat tak, že se můžeme podívat na jednotlivé části a procesy v systému z pohledu řídicích činností a identifikovat zde potenciální

systémové nebezpečí, nebezpečné řízení a ztráty, kterým se snažíme pomocí vhodného a zároveň efektivního návrhu systému zabránit.

Při řízení provozní bezpečnosti stále převažuje spíše reaktivní přístup k bezpečnosti. Hodnocení bezpečnosti je prováděno až na základě bezpečnostních událostí, kdy z dat a informací dostupných o těchto událostech jsou navržena bezpečnostní opatření mající za úkol podobným nehodám v budoucnu zabránit. Tento přístup už v dnešní době přestává být v některých odvětvích, zejména v letectví, dostačující a přesvědčit firmy, aby začaly řídit bezpečnost ve svém systému proaktivním způsobem, když mají ověřený svůj stávající systém řízení bezpečnosti, není tak jednoduché, jak se na první pohled může zdát. Provedená bezpečnostní analýza vytvořená pomocí metody STPA v této práci demonstruje proaktivní přístup k řízení bezpečnosti. Pomocí této metody se podařilo identifikovat systémová nebezpečí, množství nebezpečného řízení i scénářů ztrát. Nejedná se přitom o výčet toho, co se už v minulosti stalo, nýbrž o to, co vše se může v rámci systému, který je v civilní části letiště Pardubice, stát.

Díky provedení bezpečnostní analýzy bylo poté možné navrhnout postupy, nové nástroje či upravit nástroje stávající. Při tomto návrhu byl rovněž zohledněn i stav aktuálně nastaveného systému SMS, který se nachází na letišti v Pardubicích. Jako příklad se dají uvést současné komunikační kanály, které sice umožňují hlášení událostí na letišti, ale zaměstnanci je z různých důvodů nevyužívají v plné míře. Indikátory jsou zavedené podle SMM ICAO, v této chvíli ale prozatím nejsou stanoveny proaktivní indikátory, díky čemuž má SMS menší kontrolu nad provozní bezpečností, než by potenciálně mohl mít. Dále tyto indikátory nejsou přímo propojené na registr nebezpečí, což dělá náročným proces jejich správy. V současnosti jeho sestavení spíše odpovídá letištnímu systému, kdy SMS a jeho komponenty pokrývají všechny procesy a postupy, které se provádí v rámci celého letiště, ať už se jedná o údržbu dráhového systému, světel, nebo řízení letového provozu. V Pardubicích se ovšem nachází vojenské letiště s povoleným civilním provozem a vše, co se netýká civilního provozu, má na starost armáda, která se řídí armádními předpisy a která k bezpečnosti přistupuje pomocí svých systémů. Z toho vyplývá, že aktuální SMS, který spravuje provozovatel civilní části, je zbytečně robustný, protože pokrývá oblasti, které společnost EBA ve výsledku nemůže ovlivnit. Návrh nástrojů, které popisuje tato práce, počítá s aktuálně probíhající transformací SMS, kdy cílem je navrhnout takový SMS, který bude pokrývat pouze ty

činnosti a oblasti, které vykonává provozovatel civilní části letiště a jejichž průběh může ovlivňovat. Práce se v závislosti na výsledcích STPA analýzy a jejich porovnání se skutečným stavem zaměřila na vybrané komponenty SMS, konkrétně na „Zajištění bezpečnosti" a „Podporu bezpečnosti" s tím, že některé nástroje svými funkcemi ovlivňují i zbylé komponenty SMS. Navrženo nebo upraveno bylo celkem pět nástrojů, přičemž i provedená bezpečnostní analýza pomocí metody STPA by se dala považovat za nástroj, jelikož na letišti v Pardubicích nejsou v rámci SMS využívány žádné bezpečnostní metody pro identifikaci nebezpečí. Navržena byla příručka pro zaměstnance, konkrétně pro ilustraci byla vytvořena příručka pro zaměstnance třídírny. Jedná se o nástroj, který poskytne zaměstnancům podporu při výkonu služby v případě, že si budou chtít ověřit informace týkajících se jejich zaměstnání nebo si například nebudou pamatovat všechny důležité úkony, jelikož dlouho v zaměstnání nebyli. Tento případ může v Pardubicích nastat poměrně často, jelikož je zde zaměstnáno velké procento brigádníků, jenž nepracují pouze na letišti. Často se v jejich případě navíc jedná o jejich první zkušenosti s letectvím a provedený průzkum mezi zaměstnanci potvrdil, že by příručku shrnující všechny potřebné a podstatné informace na pracovišti uvítali. Dále se práce věnovala návrhu sady reaktivních a proaktivních indikátorů bezpečnosti. V dnešní době se může u některých organizací vyskytnout problém nevhodně nastavených indikátorů. Často je takový problém způsoben tím, že organizace nemusí vědět, jaká data jsou pro její systém relevantní a která data má sledovat, aby dokázala vyhodnotit úroveň bezpečnosti. V Pardubicích jsou v současnosti využívány pouze reaktivní indikátory, které se snadněji navrhují, opomíjí se však proaktivní indikátory bezpečnosti, jejichž přínos práce popisuje. Z výsledků STPA analýzy bylo možné navrhnout sadu indikátorů, která by pokrývala celé portfolio organizace a jenž by kombinovala reaktivní indikátory sledující systémové ztráty a proaktivní, které by sledovali stav systému a včas upozornily na jeho odchylky. Zejména proaktivní indikátory byly konzultovány s bezpečnostním manažerem, který je uznal za přínosné s výhledem jejich zavedení. Dále se práce zaměřila na systém hlášení, který, stejně jako SMS, je v současnosti pojat spíše obecně a na letový provoz. Činnosti probíhající v civilní části však nemusí probíhat pouze za přítomnosti letadla, tudíž došlo k návrhu nového formuláře hlášení i úpravě procesu hlášení, kdy byl opět brán zřetel na průzkum mezi zaměstnanci. V něm bylo často zmíněno, že systém hlášení nevyužívají, jelikož si neví rady s vyplňováním. Tento neduh je v návrhu řešen pomocí dedikované kapitoly

v příručce a vytvořením webového portálu s obsáhlými informacemi o tom, jak a co hlásit. Společně se systémem hlášení návrh počítá i zavedením dotazníků, které představují na první pohled sice primitivní nástroj, ale v případě nefunkčního systému hlášení můžou i odpovědi z dotazníku poskytnout relevantní zpětnou vazbu pro bezpečnostní oddělení.

U všech nástrojů je počítáno s tím, že nejlepší způsob, jak vyzkoušet jejich přínos, je skrze využití v reálném provozu. Jelikož však bylo letiště v době psaní práce uzavřeno pro veškerý provoz, nebylo možné tyto nástroje v praxi ověřit. Jako validace se tedy bere zpětná vazba od zaměstnanců a konzultace s bezpečnostním oddělením společně s provedenou bezpečnostní analýzou pomocí metody STPA, která je celosvětově uznávaná a podpořená výsledky. Navrhované nástroje zaměstnanci ohodnotili jako zlepšení současného stavu a označili je jako nástroje, které by měly řešit identifikované nedostatky v oblastech, na které se zaměřují. U všech nástrojů ale zazněl i podstatný argument, že nejlépe se validita dokáže při jejich zavedení do ostrého provozu.

12. Závěr

Cílem této práce bylo vytvoření návrhu technických nástrojů a postupů pro systém řízení provozní bezpečnosti (SMS) provozovatele civilní části letiště Pardubice. Pro dosažení tohoto cíle bylo nejprve nutné analyzovat současný způsob řízení provozní bezpečnosti v organizacích. Pochopení funkce systému řízení provozní bezpečnosti, který se stará o bezpečnost organizace pomocí propojených bezpečnostních nástrojů jako je sběr a monitorování dat, identifikace nebezpečí a řízení bezpečnostních rizik, bylo včetně rozklíčování funkcí jednotlivých komponent SMS nutné pro dokončení této práce. Provedena byla analýza nedostatků a limitací současného systému pro řízení provozní bezpečnosti, přičemž pro eliminace a potlačení těchto nedostatků bylo určeno použití nového systémového přístupu k řízení bezpečnosti. K tomu bylo nutné nastudovat vhodnou literaturu týkající se systémového přístupu, neboť se jedná o poměrně nový bezpečnostní přístup, který některé letecké organizace doposud vůbec neaplikovaly na procesy ve svých systémech.

Následně byl prostudován model STAMP z důvodu využívání výše zmíněného systémového přístupu. Stejně tak byla popsána metoda, která vychází z tohoto modelu, nazývaná STPA. Kromě této metody využívá model STAMP i metoda CAST, ale vzhledem k charakteru této práce byla použita první uvedená metoda. V práci byl k analýze použit systém, který reprezentoval činnosti vykonávající provozovatel civilní části letiště Pardubice. Jednalo se o konkrétní systém, který v sobě zahrnoval jednotlivé procesy skutečné organizace. Následovalo provedení STPA analýzy na tento systém, která byla vytvořena podle STPA Manuálu. Jelikož je skutečný systém poměrně obsáhlý, byl zvolen obecnější pohled, který zobecňoval některé dílčí procesy. Díky tomu se podařilo vytvořit komplexní analýzu, jejíž jednotlivé kroky jsou lehce pochopitelné a které pomohly při identifikaci nebezpečí, nebezpečného řízení a ztrát v systému. Výstupy z této analýzy jsou subjektivní a nemusí pokrývat všechny možné situace, které mohou v systému nastat.

V závislosti na provedené analýze a s přihlédnutím k nastavení aktuálního SMS pokrývajícího celé letiště byly vytvořeny postupy a nové nástroje, případně byly upraveny nástroje stávající. Tyto nástroje jsou uzpůsobeny pro budoucí SMS pokrývající

pouze ty činnosti, které vykonává provozovatel civilní části letiště. Vytvořené či upravené nástroje budou ve výsledku mít celkový efekt na provozní bezpečnosti. Nástroje nabízejí praktická řešení pro zlepšení bezpečnostních postupů, zlepšení schopností řízení rizik a podporu proaktivní kultury bezpečnosti na letišti Pardubice. Výsledky této práce mohou sloužit jako cenná reference pro další letiště a organizace, které usilují o zlepšení svých systémů řízení bezpečnosti prostřednictvím proaktivního a systémového přístupu. Stejně tak mohou příklady navrhovaných nástrojů tvořit podklad pro další práce na obdobné téma. Zde se například nabízí vývoj systémů řízení rizik, zejména způsob hodnocení, kde se aktuálně zkoumá, jak lze k hodnocení rizik přistupovat.

Jako největší limitace práce je považována absence možnosti navržené nástroje vyzkoušet v praxi. Tato možnost zůstala nevyužita, jelikož v době finalizace návrhů nástrojů bylo letiště uzavřeno a nebylo tak možné vyzkoušet efektivitu a účinnost nástrojů v provozu. Díky zavedení nástrojů do provozu by pak bylo možné o nově nabyté poznatky nástroje upravit, aby byla jejich funkčnost více podpořena.

Seznam použité literatury

[1] MINISTERSTVO DOPRAVY ČR. Předpis L19. Řízení bezpečnosti. 2013 [online]. [Cit. 2023-04-01]. Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm

[2] ICAO doc.9859, Safety Management Manual (SMM) Fourth Edition. Montreal, 2018. [Cit. 2023-04-02]. ISBN 978-92-9249-214-4.

[3] GHARIBI V, Mokarami H, Cousins R, Jahangiri M, Eskandari D. Excessive Daytime Sleepiness and Safety Performance: Comparing Proactive and Reactive Approaches. Int J Occup Environ Med. 2020 [online]. [Cit. 2023-04-05]. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7205513/

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

[5] STOLZER, A.J., Halford, C., & Goglia, J.J. Implementing Safety Management Systems in Aviation (1st ed.). Routledge. 2011. ISBN 978-13-1558-798-1.

[6] KRUML Lukáš, J. Novotný. Controlling a metoda neustálého zlepšování. Univerzita Pardubice [online]. [Cit. 2023-04-05]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/67437/Controlling%20a%20Neust%c3%a1l%c3%a9%20zlep%c5%a1ov%c3%a1n%c3%ad.pdf?sequence=1&isAllowed=y

[7] MALIŠ, Michael. Systém bezpečnostního managementu v letectví [online]. Ostrava, 2011 [Cit. 2023-04-06]. Diplomová práce. Technická univerzita Ostrava, Fakulta strojní. Vedoucí práce prof. Ing. Rudolf Volner, Ph.D. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/87992/MAL434_FS_N2301_2301T003_40_2011.pdf?sequence=1&isAllowed=y

[8] What is Safety Management System (SMS)? | SafetyCulture. SafetyCulture: Easy Inspection Solution – Get Started for Free [online]. Copyright © 2023 [Cit. 2023-04-09]. Dostupné z: https://safetyculture.com/topics/safety-management-system/

[9] CHAKIB Mohamed. Safety Management System. International Civil Aviation Organization (ICAO). Cairo, 2018 [online]. [Cit. 2023-04-09] Dostupné z: https://www.icao.int/MID/Documents/2018/Aerodrome%20SMS%20Workshop/M1-1-SMS_Aerodrome_Hazard%20Identfication.pdf

[10] LEVESON, Nancy G. CAST HANDBOOK: How to Learn More from Incidents and Accidents. [online]. 2019. [Cit. 2023-04-10] Available from: http://sunnyday.mit.edu/CASTHandbook.pdf

[11] INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). Annex 13 – Aircraft Accident and Incident Investigation. 11th edition. Montreal, Quebec: International Civil Aviation Organization, 2016. ISBN 978-92-9249-968-6.

[12] Nařízení Komise (EU) č. 139/2014. In: *EUR-Lex Access to European Union law* [online]. [Cit. 2023-04-12]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014R0139

[13] Nařízení Evropského parlamentu a Rady (EU) č. 376/2014. In: *EUR-Lex Access to European Union law* [online]. [Cit. 2023-04-12]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0376

[14] Prováděcí nařízení Komise (EU) 2015/1018. In: *EUR-Lex Access to European Union law* [online]. [Cit. 2023-04-12]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R1018

[15] Easy Access Rules | EASA Copyright © [Cit. 2023-04-12]. Dostupné z: https://www.easa.europa.eu/en/document-library/easy-access-rules

[16] Acceptable Means of Compliance (AMC) and Guidance Material (GM) | EASA. [online]. Copyright © [Cit. 2023-04-12]. Dostupné z: https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials

[17] LEVESON, Nancy. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. [Cit. 2023-04-13] ISBN 978-0-262-01662-9.

[18] HANÁKOVÁ L. a kolektiv. Metodika pro zefektivnění analýzy a řízení rizik s využitím konceptuálního modelování. Výzkumný projekt TA ČR [online]. [Cit. 2023-04-13]. Dostupné z: mdcr.cz/getattachment/Dokumenty/Veda-a-vyzkum/Certifikovane-metodiky/Letecka-doprava/Metodika-pro-zefektivneni-analyzy-a-rizeni-rizik-s/Metodika-pro-zefektivneni-analyzy-a-rizeni-rizik-s-vyuzitim-konceptualniho-modelovani.PDF.aspx

[19] SONG, Yao. Applying system-theoretic accident model and processes (STAMP) to hazard analysis. McMaster University 2012 [online]. [Cit. 2023-04-15]. Dostupné z: https://macsphere.mcmaster.ca/bitstream/11375/11867/1/fulltext.pdf

[20] LEVESON, Nancy G. a John P. THOMAS. STPA handbook [online]. [Cit. 2023-04-13]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[21] SULAMAN, S., Beer, A., Felderer, M. et al. Comparison of the FMEA and STPA safety analysis methods–a case study. Software Qual. 2019 [online]. [Cit. 2023-04-15]. Dostupné z: https://link.springer.com/article/10.1007/s11219-017-9396-0

[22] SUN, L., Li, Y., and Zio, E. Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems. 2021 [online]. [Cit. 2023-04-15]. Dostupné z: https://asmedigitalcollection.asme.org/risk/article-abstract/8/3/031104/1115198/Comparison-of-the-HAZOP-FMEA-FRAM-and-STPA-Methods

[23] SABALIAUSKAITE, G., Lin S. L., Jin C. Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model. Singapore University of Technology and Design 2018 [online]. [Cit. 2023-04-15]. Dostupné z: http://personales.upv.es/thinkmind/dl/journals/sec/sec_v11_n12_2018/sec_v11_n12_2018_13.pdf

[24] PLIOTSIAS, A., Nektarios K. Using STPA in the Evaluation of Fighter Pilots Training Programs. [online]. [Cit. 2023-04-15]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877705815038618

[25] O nás | slp.army.cz. slp.army.cz [online]. Copyright © 2004 [Cit. 2023-04-18]. Dostupné z: https://slp.army.cz/o-nas

[26] Aerodrome chart – ICAO Pardubice. AIM | Air Navigation Services of the CR [online]. Copyright © [Cit. 2023-05-05]. Dostupné z: https://aim.rlp.cz/ais_data/aip/data/valid/a2-pd-adc.pdf

[27] Safety hlášení – Letiště Pardubice. Letiště Pardubice – Létejte pohodlně z letiště Pardubice [online]. [Cit. 2023-05-05]. Dostupné z: https://www.airport-pardubice.cz/safety-hlaseni/

[28] Ke stažení – Letiště Pardubice. Letiště Pardubice – Létejte pohodlně z letiště Pardubice [online]. [Cit. 2023-05-05]. Dostupné z: https://www.airport-pardubice.cz/ke-stazeni/

[29] Jim Arlow and Illa Neustadt. UML 2 a unifikovaný proces vývoje aplikací. Computer Press, Brno, 2011. ISBN: 978-80-251-1503-9.

Přílohy

Příloha 1 – Řídicí činnosti

Role	Řídicí činnost	Zpětná vazba	Vlastní zodpovědnost	Koordinace
Ředitel společnosti	A) Schvaluje bezpečnostní opatření a cíle		A) Musí si zachovat přehled o aktuálním dění ve společnosti	
Provozní manažer	A) Provádí pravidelné kontroly a inspekce B) Stanovuje postupy pro bezpečnou manipulaci s pozemní odbavovací technikou C) Stanovuje postupy pro manipulaci s pohonnými hmotami	A) Nahlašuje bezpečnostní nedostatky B) Pravidelně informuje o stavu odbavení	A) Vedení a aktualizace provozní dokumentace k provozním hmotám B) Vedení a aktualizace provozní dokumentace k provozování pozemní odbavovací techniky	A) Tvorba provozních postupů, identifikace rizik a návrh provozních opatření (společně s bezpečnostním manažerem)
Bezpečnostní manažer	A) Zajišťuje bezpečnostní školení B) Zahajuje a účastní se šetření interních událostí C) Vydává bezpečnostní doporučení D) Vytváří nápravná opatření	A) Vydává pravidelné zprávy o bezpečnostní výkonnosti B) Předkládá bezpečnostní cíle vedení organizace	A) Identifikuje nebezpečí B) Analyzuje rizika C) Zajišťuje a udržuje dokumentace k řízení bezpečnosti D) Řídí a zpracovává systém bezpečnostních hlášení	A) Tvorba provozních postupů, identifikace rizik a návrh provozních opatření (společně se provozním manažerem) B) Kooperace se zástupcem armády
Vedoucí odbavení cestujících a letadel	A) Řídí odbavovací činnosti B) Dohlíží nad dodržováním pracovních dob	A) Vznáší požadavky pro zajištění bezpečnosti při odbavení (navýšení počtu pracovníků atd.) B) Nahlašuje vzniklé incidenty během odbavení C) Předává statistické údaje	A) Sleduje platnost všech certifikací B) Udržuje databáze a všechny podpůrné softwarové programy C) Zajišťuje zpracování statistických přehledů a údajů	A) Předává provozně letové informace

Vedoucí technické podpory	A) Dohlíží nad dodržováním postupů při odbavení letadla B) Plánuje směny podřízených pracovníků C) Provádí navádění letadel	A) Vznáší požadavky pro zajištění bezpečnosti při odbavení (navýšení počtu pracovníků atd.) B) Hlášení bezpečnostních událostí	A) Sleduje termíny revizí B) Hlídá platnosti certifikací a školení C) Zajišťuje dostupnost pracovních pomůcek D) Hlídá stav pozemní techniky	
Technici	A) Manipulace s pozemní odbavovací technikou B) Údržba pozemní techniky	A) Provedení/neprovedení činností uvedených v prvním sloupci B) Hlášení bezpečnostních událostí		A) Spolupráce při odbavení s pracovníky třídírny
Pracovníci třídírny	A) Nakládka/vykládka zavazadel B) Manipulaci s pozemní odbavovací technikou C) Manipulace s dalšími nástroji odbavení (kužely, špalky, schůdky pro paliváře)	A) Provedení/neprovedení činností uvedených v prvním sloupci B) Hlášení bezpečnostních událostí		A) Spolupráce při odbavení s techniky B) Spolupráce s vedoucím odbavení
Údržbář	A) Údržba budov a okolních ploch B) Údržba systémů a techniky odbavení (pásový dopravník atd.)	A) Podává zprávy o aktuálním stavu infrastruktury a budov společně s navrhovanými úpravami		A) Spolupráce s techniky

Příloha 2 – Nebezpečné řízení (identifikováno alespoň jedno ke každé řídicí činnosti)

Řídicí činnost	Neprovedení řídicí činnosti povede k nebezpečí	Řídicí činnost je provedena nevhodným způsobem vedoucí k nebezpečí	Řídicí činnost je provedena příliš pozdě, brzo, nebo ve špatném pořadí	Řídicí činnost trvá moc dlouho, nebo byla zastavena příliš brzy
Schválení bezpečnostních opatření a cílů	UCA-1: Ředitel společnosti neschválí bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera [H-1, H-3, H-4]	UCA-2: Ředitel společnosti schválí pouze některá bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera [H-1, H-3, H-4]	UCA-3: Ředitel společnosti schválí bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera až poté, co se stane událost [H-1, H-3, H-4]	
Provádění pravidelných kontrol a inspekcí	UCA-4: Provozní manažer neprovede pravidelnou kontrolu či inspekce [H-1, H-3, H-4]	UCA-5: Provozní manažer při kontrole či inspekci nebude dostatečně důkladný [H-1, H-3, H-4]	UCA-6: Provozní manažer provede kontrolu či inspekce až poté, co se stane událost [H-1, H-3, H-4]	
Stanovení postupů pro bezpečnou manipulaci s pozemní odbavovací technikou	UCA-7: Provozní manažer nestanoví provozní postupy pro manipulaci s odb. technikou [H-1, H-2, H-3]	UCA-8: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou neodpovídající funkcím této techniky [H-1, H-2, H-3]	UCA-9: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou až v závislosti na probíhajícím provozu [H-1, H-2, H-3]	
Stanovení postupů pro manipulaci s pohonnými hmotami	UCA-10: Provozní manažer nestanoví provozní postupy pro manipulaci s pohonnými hmotami [H-1, H-2, H-3]	UCA-11: Provozní manažer stanoví provozní postupy pro manipulaci s pohonnými hmotami odpovídající jiným než používaným druhům této techniky [H-1, H-2, H-3]	UCA-12: Provozní manažer stanoví provozní postupy pro manipulaci s pohonnými hmotami až v závislosti na probíhajícím provozu [H-1, H-2, H-3]	
Zajištění bezpečnostního školení	UCA-13: Bezpečnostní manažer nezajistí školení pro zaměstnance před nástupem do služby [H-2, H-4]	UCA-14: Bezpečnostní manažer zajistí školení pouze pro některé zaměstnance před nástupem do služby [H-2, H-4]	UCA-15: Bezpečnostní manažer zajistí školení pro zaměstnance až po proběhlé události [H-2, H-4]	

Šetření interních událostí	UCA-16: Bezpečnostní manažer neprovede šetření události po jejím vzniku [H-1]	UCA-17: Bezpečnostní manažer provede šetření vzniklé události, které však neodhalí veškeré bezpečnostní hrozby [H-1]	UCA-18: Bezpečnostní manažer provede šetření události, až po jejím opakovaném vzniku [H-1]	
Vydávání bezpečnostních doporučení	UCA-19: Bezpečnostní manažer nevydá bezpečnostní doporučení po proběhlém šetření [H-1, H-2]	UCA-20: Bezpečnostní manažer vydá nekompletní bezpečnostní doporučení po proběhlém šetření [H-1, H-2]	UCA-21: Bezpečnostní manažer vydá bezpečnostní doporučení až po opakovaném vzniku události [H-1, H-2]	
Vytváření nápravná opatření	UCA-22: Bezpečnostní manažer nenavrhne nápravná opatření po proběhlém šetření [H-1, H-2]	UCA-23: Bezpečnostní manažer navrhne nápravná opatření pouze pro některá identifikovaná nebezpečí [H-1, H-2] UCA-24: Bezpečnostní manažer navrhne neefektivní nápravná opatření pro identifikovaná nebezpečí [H-1, H-2]	UCA-25: Bezpečnostní manažer vytvoří nápravná opatření až po opakovaném vzniku nebezpečí [H-1, H-2]	
Řízení odbavovacích činností	UCA-26: Vedoucí odbavení neřídí odbavovací činnosti před přistavením letadla [H-2]			
Dohled nad dodržováním pracovních dob	UCA-27: Vedoucí odbavení nedohlíží na dodržování pracovních dob zaměstnanců při výkonu práce [H-1, H-2, H-3, H-4]			
Dohled nad dodržováním postupů při odbavení	UCA-28: Vedoucí technické podpory nedohlíží na dodržování postupů při odbavení letadla [H-1, H-2, H-3, H-4]			
Plánování směn podřízených pracovníků	UCA-29: Vedoucí technické podpory nenaplánuje podřízené	UCA-30: Vedoucí technické podpory naplánuje nízký počet		

	pracovníky na směny [H-4]	podřízených pracovníků na směny [H-4]		
Navádění letadel		UCA-31: Vedoucí technické podpory navede letadlo mimo předepsané místo zastavení [H-1]		
Údržba pozemní techniky	UCA-32: Technici neprovedou v případě potřeby údržbu pozemní odbavovací techniky před zahájením směny [H-3]	UCA-33: Technici provedou v případě potřeby údržbu pozemní odbavovací techniky, která však nevyřeší poruchy této techniky [H-3]	UCA-34: Technici provedou údržbu pozemní odbavovací techniky po vzniklém incidentu [H-3]	
Nakládka/vykládka zavazadel		UCA-35: Pracovníci třídírny provedou nakládku / vykládku do jednotlivých cargo holdů v nesprávném pořadí [H-1, H-3]		
Manipulace s odbavovací technikou		UCA-36: Technici či jiná obsluha manipulační techniky nedodrží stanovenou rychlost manipulace při odbavení letadla [H-3]	UCA-37: Technici či jiná obsluha přistaví manipulační techniku k letadlu ve špatném pořadí a naruší tak stanovenou bezpečnou vzdálenost [H-3]	
Manipulace s dalšími nástroji odbavení	UCA-38: Pracovníci třídírny nerozmístí podpůrné nástroje odbavení (kužely, špalky, ...) na určená místa při odbavení letadla [H-1, H-3]	UCA-39: Pracovníci třídírny rozmístí při odbavení letadla podpůrné nástroje odbavení (kužely, špalky, ...) na neodpovídající místa k tomu určená [H-1, H-3]	UCA-40: Pracovníci třídírny rozmístí podpůrné nástroje odbavení (kužely, špalky, ...) na odpovídající místa k tomu určená až po započatí odbavení [H-1, H-3]	
Kontrola a údržba budov a okolních ploch	UCA-41: Údržbář neprovede kontrolu a údržbu budov a ploch před zahájením směny [H-1, H-3]			
Kontrola a údržba systémů a techniky odbavení (pásový dopravník atd.)	UCA-42: Údržbář neprovede kontrolu a údržbu systémů a techniky odbavení před zahájením směny [H-1, H-3]			

Příloha 3 – Scénáře ztrát (alespoň jeden scénář pro každé nebezpečné řízení)

UCA-1:

Scénář 1: Ředitel společnosti neschválí bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera [UCA-1], jelikož mu žádné bezpečnostní opatření či cíle nebyly předloženy. Následkem toho může být využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-2

Scénář 1: Ředitel společnosti schválí pouze některá bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera [UCA-2], protože na pokrytí všech nemá vymezený dostatečný finanční rozpočet. Následkem toho může být využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-3

Scénář 1: Ředitel společnosti schválí bezpečnostní opatření a cíle, které jsou mu předkládány od bezpečnostního manažera až poté, co se stane událost [UCA-3], jelikož do vypuknutí události inspekce neodhalily žádné nebezpečí, která by danou událost mohla způsobit. Tímto bylo zapříčiněno využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-4

Scénář 1: Provozní manažer neprovede pravidelnou kontrolu či inspekce [UCA-4] z důvodu absence hlášení poukazujícího na jakýkoliv problém. Následkem toho může být využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-5

Scénář 1: Provozní manažer při kontrole či inspekci nebude dostatečně důkladný [UCA-5], jelikož nedostal nedisponoval všemi nutnými podklady a materiály k provedení těchto inspekcí. Následkem toho může být využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-6

Scénář 1: Provozní manažer z důvodu absence dat (například ze systému hlášení) provede kontrolu či inspekce až poté, co se stane událost [UCA-6]. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů[H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo například nenavýšení počtu potřebných zaměstnanců [H-4].

UCA-7

Scénář 1: Provozní manažer nestanoví provozní postupy pro manipulaci s odb. technikou [UCA-7], jelikož to nepovažoval za nutné z důvodu jasné obsluhy této techniky. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-8:

Scénář 1: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou, které však neodpovídají konkrétnímu typu a funkcím této techniky [UCA-8], jelikož nedisponoval při tvorbě všemi technickými parametry vztahujícím se k této technice. Tímto může dojít k nesprávnému použití techniky při odbavování [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-9

Scénář 1: Provozní manažer stanoví provozní postupy pro manipulaci s odb. technikou až v závislosti na probíhajícím provozu [UCA-9], protože předpokládal bezproblémový provoz bez nutnosti stanovení postupů. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-10

Scénář 1: Provozní manažer nestanoví provozní postupy pro manipulaci s pohonnými hmotami [UCA-10], jelikož to nepovažoval za nutné z důvodu jasné obsluhy této techniky. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-11

Scénář 1: Provozní manažer stanoví provozní postupy pro manipulaci s pohonnými hmotami odpovídající jiným než používaným druhům této techniky [UCA-11], jelikož neměl dostatek informací o odlišnostech jednotlivých druhů pohonných hmot. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-12

Scénář 1: Provozní manažer stanoví provozní postupy pro manipulaci s pohonnými hmotami až v závislosti na probíhajícím provozu [UCA-12], jelikož to nepovažoval za prioritní z důvodu jasné obsluhy této techniky a upřednostnil zpracování jiných postupů. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1], používání techniky v nevyhovujícím technickém stavu [H-3], nebo by zaměstnanci mohli postrádat informace pro provedení postupů s pomocí této techniky [H-2].

UCA-13

Scénář 1: Bezpečnostní manažer nezajistí školení pro zaměstnance před nástupem do služby [UCA-13], jelikož nemá vytvořené školící materiály. Zapříčiní tak fakt, že zaměstnanci nebudou mít k dispozici všechny informace pro výkon pracovního poměru [H-2] nebo budou činnosti vykonávány nedostatečným počtem pracovníků [H-4], jelikož bude třeba zbylé pracovníky dodatečně proškolit.

UCA-14:

Scénář 1: Bezpečnostní manažer z důvodu neúplné databáze zaměstnanců zajistí školení pouze pro některé zaměstnance před jejich nástupem do služby [UCA-14] a zapříčiní tak fakt, že zaměstnanci nebudou mít k dispozici všechny informace pro výkon pracovního poměru [H-2] nebo budou činnosti vykonávány nedostatečným počtem pracovníků [H-4], jelikož bude třeba zbylé pracovníky dodatečně proškolit.

UCA-15

Scénář 1: Bezpečnostní manažer zajistí školení pro zaměstnance až po proběhlé události [UCA-15], jelikož nepovažoval za nutné zaměstnance proškolit. Zapříčinil tak fakt, že zaměstnanci neměli k dispozici všechny informace pro výkon pracovního poměru [H-2] nebo nebyly činnosti vykonávány způsobilým personálem pro výkon dané činnosti [H-4].

UCA-16

Scénář 1: Bezpečnostní manažer neprovede šetření události po jejím vzniku [UCA-16], protože daná událost mu nebyla nahlášena. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1].

UCA-17

Scénář 1: Bezpečnostní manažer provede šetření vzniklé události, které však neodhalí veškeré bezpečnostní hrozby [UCA-17], jelikož neprovedl kompletní analýzu události. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1].

UCA-18

Scénář 1: Bezpečnostní manažer provede šetření události, až po jejím opakovaném vzniku [UCA-18], jelikož do té doby mu nebyla tato událost hlášena nebo protože to nepovažoval za nutné. Tímto bylo zapříčiněno využívání nebezpečných postupů [H-1].

UCA-19

Scénář 1: Bezpečnostní manažer nevydá bezpečnostní doporučení po proběhlém šetření [UCA-19], protože žádné důvody pro vydání doporučení neshledal. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-20

Scénář 1: Bezpečnostní manažer vydá nekompletní bezpečnostní doporučení po proběhlém šetření [UCA-20], jelikož zatím nedefinoval zbylé způsoby provedení opatření. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-21

Scénář 1: Bezpečnostní manažer vydá bezpečnostní doporučení až po opakovaném vzniku události [UCA-21], jelikož do té doby mu nebyl známý žádný problém, kvůli kterému bylo nutné vytvořit bezpečnostní doporučení. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-22

Scénář 1: Bezpečnostní manažer nenavrhne nápravná opatření po proběhlém šetření [UCA-22], jelikož není například z finančního hlediska možné tato opatření navrhnout. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-23

Scénář 1: Bezpečnostní manažer navrhne nápravná opatření pouze pro některá identifikovaná nebezpečí [UCA-23], jelikož zatím nedefinoval zbylá nápravná opatření. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-24

Scénář 1: Bezpečnostní manažer navrhne neefektivní nápravná opatření pro identifikovaná nebezpečí [UCA-24], jelikož neměl dostatek podpůrných dat ke stanovení efektivních opatření. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-25

Scénář 1: Bezpečnostní manažer vytvoří nápravná opatření až po opakovaném vzniku nebezpečí [UCA-25], jelikož do té doby neidentifikoval žádné nebezpečí, kvůli kterému bylo nutné vytvořit nápravné opatření. Tímto by mohlo být zapříčiněno využívání nebezpečných postupů [H-1] a zaměstnanci by nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-26

Scénář 1: Vedoucí odbavení kvůli zaneprázdněnosti (časové, jiné záležitosti týkající se provozu) neřídí odbavovací činnosti před přistavením letadla [UCA-26]. Hrozí tak, že by zaměstnanci nemuseli mít všechny potřebné informace pro výkon činnosti [H-2].

UCA-27

Scénář 1: Vedoucí odbavení nedohlíží na dodržování pracovních dob zaměstnanců při výkonu práce [UCA-27], protože nefunguje systém sledující docházku zaměstnanců a plánování směn. Tímto může způsobit nedodržení postupů [H-1], poškození techniky, jelikož nikdo zaměstnanci mohou pociťovat únavu [H-3] a neuhlídá ani pohyb nezpůsobilých zaměstnanců při odbavení [H-4].

UCA-28

Scénář 1: Vedoucí technické podpory nedohlíží na dodržování postupů při odbavení letadla [UCA-28], protože musí suplovat za chybějící zaměstnance (například při vykládce/nakládce). Tímto může způsobit nedodržení postupů [H-1], absenci distribuce informací [H-2], poškození techniky, jelikož nikdo nebude dohlížet na její používání [H-3] a neuhlídá ani pohyb nezpůsobilých zaměstnanců při odbavení [H-4].

UCA-29

Scénář 1: Vedoucí technické podpory nenaplánuje podřízené pracovníky na směny [UCA-29], jelikož nemá dostatek vycvičených zaměstnanců. Způsobí tak, že činnosti organizace nebudou vykonávány dostatečným počtem zaměstnanců [H-4].

UCA-30

Scénář 1: Vedoucí technické podpory naplánuje nízký počet podřízených pracovníků na směny [UCA-30], jelikož nemá dostatek vycvičených zaměstnanců. Způsobí tak, že činnosti organizace nebudou vykonávány dostatečným počtem zaměstnanců [H-4].

UCA-31

Scénář 1: Vedoucí technické podpory navede letadlo mimo předepsané místo zastavení [UCA-31], jelikož bylo vodorovné značení na odbavovací ploše špatně čitelné (například kvůli stojaté vodě po dešti). Letadlo mimo svoji standardní pozici donutí zaměstnance porušit postupy organizace při odbavení [H-1].

UCA-32

Scénář 1: Technici neprovedou v případě potřeby údržbu pozemní odbavovací techniky před zahájením směny [UCA-32], protože v technických knihách není veden žádný záznam o problémech. Mohou tak způsobit, že při odbavení bude použita technika ve špatném technickém stavu [H-3].

UCA-33

Scénář 1: Technici provedou v případě potřeby údržbu pozemní odbavovací techniky, která však nevyřeší poruchy této techniky [UCA-33], jelikož neměli potřebné znalosti pro opravu této techniky. Mohou tak způsobit, že při odbavení bude použita technika v přetrvávajícím špatném technickém stavu [H-3].

UCA-34

Scénář 1: Technici provedou údržbu pozemní odbavovací techniky po vzniklém incidentu [UCA-34], protože do té doby považovali závady a poškození techniky za zanedbatelné a neohrožující bezpečnost. Způsobili tak, že při odbavení byla použita technika v přetrvávajícím špatném technickém stavu [H-3].

UCA-35

Scénář 1: Pracovníci třídírny provedou nakládku / vykládku do jednotlivých cargo holdů v nesprávném pořadí [UCA-35], protože neměli instrukce, v jakém pořadí mají tyto holdy naložit / vyložit. Při odbavení tak byly použity nebezpečné postupy [H-1], které by mohly poškodit i techniku [H-3].

UCA-36:

Scénář 1: Technici či jiná obsluha manipulační techniky nedodrží stanovenou rychlost manipulace při odbavení letadla [UCA-36], protože si již nepamatují informace z dopravního řádu, a mohli by tak způsobit poškození techniky určené k odbavení letadla. [H-3]

UCA-37

Scénář 1: Technici či jiná obsluha přistaví manipulační techniku k letadlu ve špatném pořadí a naruší tak stanovenou bezpečnou vzdálenost [UCA-37], protože spěchali, aby zkrátili zpoždění. Mohli by tak způsobit poškození techniky určené k odbavení letadla. [H-3]

UCA-38

Scénář 1: Pracovníci třídírny nerozmístí podpůrné nástroje odbavení (kužely, špalky, …) na určená místa při odbavení letadla [UCA-38], protože už neví, kam přesně by je měli umístit (dlouho například nebyli v zaměstnání). Důsledkem toho by tak mohlo dojít k porušení postupů [H-1] a poškození techniky, která by nedodržela bezpečnostní perimetry [H-3].

UCA-39

Scénář 1: Pracovníci třídírny rozmístí při odbavení letadla podpůrné nástroje odbavení (kužely, špalky, …) na neodpovídající místa k tomu určená [UCA-39], protože už neví, kam přesně by je měli umístit (dlouho například nebyli v zaměstnání). Důsledkem toho by tak mohlo dojít k porušení postupů [H-1] a poškození techniky, která by nedodržela bezpečnostní perimetry [H-3].

UCA-40

Scénář 1: Pracovníci třídírny rozmístí podpůrné nástroje odbavení (kužely, špalky, …) na odpovídající místa k tomu určená až po započatí odbavení [UCA-40], protože je na pracovišti málo zaměstnanců a nestihli udělat více činností včas. Důsledkem toho by tak mohlo dojít k porušení postupů [H-1] a poškození techniky, která by nedodržela bezpečnostní perimetry [H-3].

UCA-41

Scénář 1: Údržbář neprovede kontrolu a údržbu budov a ploch před zahájením směny [UCA-41], protože mu nejsou hlášeny žádné problémy. Důsledkem toho by tak mohlo dojít k porušení postupů [H-1] a poškození techniky, se kterou by se manipulovalo na neudržovaných plochách [H-3].

UCA-42

Scénář 1: Údržbář neprovede kontrolu a údržbu systémů a techniky odbavení před zahájením směny [UCA-42], protože mu nejsou hlášeny žádné problémy nebo není momentálně k dispozici. Důsledkem toho by tak mohlo dojít k porušení postupů [H-1] nebo k provedení odbavení s technikou v nevyhovujícím technickém stavu H-3].