ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Hodnocení bezpečnosti rozšířeného provozu minimálních posádek

Safety assessment of the Extended Minimum-Crew Operations

Diplomová práce

Studijní program: Technika a technologie v dopravě a spojích

Studijní obor: Provoz a řízení letecké dopravy

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

Bc. Pavel Mikule

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. Pavel Mikule

Studijní program (obor/specializace) studenta:

navazující magisterský – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Hodnocení bezpečnosti rozšířeného provozu minimálních posádek**

Název tématu (anglicky): Safety Assessment of the Extended Minimum-Crew Operations

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je provedení bezpečnostní studie konceptu „Extended Minimum-Crew Operations (eMCO)" zaměřeného na provoz minimálních posádek v komerční letecké dopravě.
- Analyzujte dostupné metody bezpečnostního inženýrství.
- Analyzujte koncept Extended Minimum-Crew Operations (eMCO).
- Proveďte bezpečnostní studii konceptu eMCO s pomocí moderních nástrojů bezpečnostního inženýrství.
- Stanovte bezpečnostní doporučení pro zajištění bezpečnosti konceptu eMCO.
- Dosažené výsledky vyhodnoťte a ověřte.

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, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N. a Thomas. J. STPA Handbook, 2018.

Vedoucí diplomové práce: **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. Pavel Mikule
jméno a podpis studenta

V Praze dne 15. července 2022

Abstrakt

Cílem této diplomové práce je zhodnocení bezpečnosti Rozšířeného provozu minimálních posádek pomocí moderní nástrojů bezpečnostního inženýrství. V teoretické části je popsán vývoj automatizace v letectví, současné trendy, projekty a limitace tohoto odvětví. Dále jsou zde popsány jednotlivé koncepty provozu, jejich výhody a nevýhody. V metodické části práce jsou pak stručně popsány bezpečnostní modely a metody, které byly v rámci práce využity. Dále je zde popsán princip práce s jednotlivými metodami. V rámci praktické části jsou pak analyzovány z pohledu bezpečnosti jednotlivé koncepty Rozšířeného provozu minimálních posádek. V závěru jsou stanoveny bezpečnostní požadavky pro jednotlivé koncepty a zhodnocena jejich bezpečnost.

Klíčová slova: automatizace, bezpečnostní požadavky, letadlo, posouzení bezpečnosti, systém

Abstract

The aim of this diploma thesis is to evaluate the safety of Extended Minimum Crew Operatins using modern safety engineering tools. The theoretical part of this thesis presents the evolution in aircraft automation, current trends, projects and limitations in this field. Also proposed concepts of operation, their advantages and disadvantages are described in this part. In the methodological part of this thesis, used safety engineering models and methods are briefly described, including the working principles. In the practical part, the analysis are conducted on the concepts. In the end, safety requirements are derived and safety of concepts evaluated.

Keywords: aircraft, automation, safety assessment, safety requirements, system

Poděkování

Tímto bych chtěl poděkovat doc. Ing. Andreji Lališovi, Ph. D. za jeho cenné rady, ochotu a konzultace, které mi v rámci psaní diplomové práce poskytl. Dále bych chtěl také poděkovat svým blízkým a celé rodině za neustávající podporu v rámci celého studia.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou/diplomovou práci s názvem Název práce vypracoval/a samostatně a použil/a k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské/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. Pavel Mikule

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

ATTOL	Airbus Autonomous Take–Off and Landing
BAC	British Aircraft Corporation
CAST	Causal Analysis based on STAMP
CRC	Crew Rest Compartment
CRM	Crew Resource Management
eMCO	Extended Minimum-Crew Operations
FL	Flight Level
GATP	Ground Airline Transport Pilot
GPS	Global Positiong system
HTA	Hierarchical Task Analysis
ILS	Instrument Landing System
LCD	Liquid Crystal Display
PR	Pilot Resting
SiPO	Single Pilot Operations
SRM	STPA Informed Risk Matrix
STPA	System-Theoretic Processes Analysis
STAMP	Systems theoretic accident model and process
TCAS	Traffic Collision Avoidance Systém
VPA	Virtual Pilot Assistant

Úvod

Civilní letectví, vyjma období pandemie, zažívá stabilní růst již několik desetiletí. Zvyšují se nejen počty odbavených a přepravených cestujících, ale i množství přepraveného nákladu či pošty. S tím je úzce spjatá větší hustota provozu a tím pádem větší vytížení vzdušných prostorů. Dalším výsledkem tohoto trendu jsou personální požadavky. Se vzrůstající hustotou provozu je nutné zajistit dostatek personálu na jeho obsluhu. V oblasti letových posádek má tento problém v podstatě 2 řešení. Prvním je přijímání velkého množství nového personálu. Tím druhým řešením, kterého je především využíváno, je v ohledu na technologické možnosti doby snižování počtu pilotů nutných k obsluze letadla.

Avšak ke snižování počtu členů posádky je nutné přistupovat zodpovědně. U Každé takto výrazné změny v letectví musí totiž být prokázána její bezpečnost, která je dozorována kontrolními orgány. Bezpečnost celého provozu je ostatně prioritou letecké dopravy a letecká doprava je v oblasti bezpečnosti na vrcholu pomyslné pyramidy jednotlivých druhů dopravy. Tudíž v rámci nového systému dochází k pravidelnému hodnocení z pohledu bezpečnosti. Moderní metody bezpečnosti pak již umožňují zhodnocení i v průběhu vývoje systému, bez znalosti jakýchkoliv dat a informací z provozu systému. To umožňuje poskytnout cenné informace pro designéry a snižuje doby nutné pro testování před zavedením do provozu. V odborné literatuře se pak hovoří o proaktivním přístupu k bezpečnosti.

Jedním z kroků v rámci snižování počtu pilotů v kokpitu je i implementace Rozšířeného provozu minimálních posádek. Let v hladině s jedním pilotem v kokpitu v je vhodným předchůdcem pro implementaci jednopilotního provozu obchodní letecké dopravy, a to především z důvodu, že let v hladině je z méně kritických fází letu a je tak logickým krokem v rámci zavádění. Tudíž po prokázání tohoto konceptu je množné na vývoj dále navázat a rozšířit tento koncept do všech fází letu. A právě předběžné zhodnocení bezpečnosti systému letu v hladině s jedním pilotem v kokpitu je předmětem této práce. Cílem práce je tedy zhodnotit jednotlivé koncepty a stanovit bezpečnostní doporučení, která by měla být implementována do systému pro zachování úrovně bezpečnosti.

1. Současný stav

Tato kapitola se zabývá zhodnocením současného stavu v letectví z pohledu automatizace. V Kapitole 1.1 jsou uvedeny informace týkající se zavádění, vývoje a současného stavu automatizace v letadlech. Dále jsou zde uvedeny některé projekty, které udávají směr vývoje letectví do budoucna, a v neposlední řadě jsou v této kapitole taktéž uvedeny limitace současného stavu automatizace v letectví. V kapitole 1.1 je pak popsán systém provozu s jedním pilotem v kokpitu (Single Pilot Operations – SiPO) a jeho podčást Rozšířený provoz minimálních posádek (Extended Minimum Crew Operations – eMCO). V kapitole 1.2 je pak uvedena dostupná literatura zabývající se problematikou SiPO, potažmo eMCO.

1.1 Automatizace v letadlech

Jako je tomu v každém odvětví, i v letectví dochází k progresivnímu vývoji. Tento vývoj probíhá ve všech odvětvích letectví, avšak vývoj automatizace v letadlech je nejlépe viditelný v samotných kokpitech. Počátek rozmachu letecké dopravy se datuje již od 20. let 20. století, avšak vývoj obchodní letecké dopravy byl záhy téměř zastaven druhou světovou válkou. Po válce došlo k rapidnímu rozmachu letectví do civilní sféry a lidé tak mohli začít cestovat s dříve nevídaným komfortem na nepředstavitelné vzdálenosti. Letadla samotná se však od těch, která je možné spatřit na obloze nyní, výrazně lišila. Dalším výrazným krokem, který umožnil vývoj letectví, byla deregulace letecké dopravy. Ta probíhala od poloviny 70. let na území Ameriky a následně v průběhu 80. let i v Evropě. Deregulace otevřela volný trh v letectví a umožnila tak nástup nových dopravců, snížení cen letenek a dalších důležitých náležitostí, které dříve bránili vývoji. [1]

1.1.1 Vývoj

Vývoj automatizace v letadlech se přímo váže na vývoj letectví. Po skončení druhé světové války bylo využíváno hlavně bývalých vojenských letounů, které byly upraveny pro použití v civilní letecké dopravě. Jako příklad může být uveden letoun Lockheed Constellation, který lze považovat za prvopočátek v oblasti automatizace

v letadle. Letoun totiž ve své původní variantě není vybaven žádnou automatizací. Letoun byl obsluhován pěti členy letové posádky. Těmi byli dva piloti, navigátor, palubní inženýr a radista. Kokpit letounu (Obrázek 1) je vybaven pouze mechanickými či elektrickými ovládacími prvky a ukazateli letových údajů budíkového typu. [2]

Obrázek 1: Původní kokpit letounu Lockheed Constellation. Převzato z [3]

Automatizace v letadlech je úzce spojená právě s velikostí letové posádky, která je potřebná pro obsluhu letadla. Příkladem postupné automatizace na palubě může být legendární letoun Aérospatiale – BAC Concorde. Kokpit tohoto letounu je považován za jeden z nejsložitějších v dějinách lidstva (Obrázek 2). Avšak počet členů letové posádky je výrazně nižší než u výše zmíněného letounu. Concorde byl operován pouze třemi členy letové posádky, a to dvěma piloty a palubním inženýrem. K redukci členů posádky mohlo být přistoupeno právě díky automatizaci v kokpitu. Přestože většina přístrojů v kokpitu byla zobrazena stále formou budíků, Concorde disponoval na svoji dobu převratnými technologiemi. Mezi systémy, které dopomohly k odstranění dvou členů posádky a převedení jejich povinností na zbylé členy, se řadí například na svoji dobu převratný

systém autopilota i s automatickým ovládáním tahu motorů, inerční navigační systém, palubní protisrážkový systém (Traffic Collision Avoidance System – TCAS), meteorologický radar a další. [4]

Obrázek 2: Pohled do kokpitu Concorde. Převzato z [5]

1.1.2 Současnost

V dnešní době je ale i tak převratný letoun, jako je Concorde, technologicky překonán a stal se již pouze mementem v historii. Současný stav automatizace kokpitu je možné sledovat na jednom z nejmodernějších letadel obchodní letecké dopravy, a to na letounu Airbus A350. Počet členů posádky se dále snížil na dva členy, piloty. Ti mají k dispozici moderní systémy a vybavení, které snižují jejich pracovní zatížení pro zachování bezpečného provozu. Kokpit (Obrázek 3) se výrazně liší od těch, které byly zmíněny výše v textu. Současnými trendy jsou dotykové displeje z tekutých krystalů (Liquid Crystal Display – LCD) s vysokým rozlišením, které umožňují pilotům zobrazení veškerých

informací potřebných k letu i změny v zobrazovaných informacích na základě fáze letu. [6]

Obrázek 3: Kokpit letounu Airbus A350. Převzato z [7]

Automatizace na palubě moderních letadel je velice rozšířená a má mnoho nesporných výhod. Hlavním cílem automatizace je již výše zmíněná bezpečnost provozu. Míra automatizace je úzce spjatá s každou další přicházející generací letadla, což umožňuje přesun předešlých generací od velkých dopravců k menším, do méně vyspělých zemí, kde je takto zvyšována úroveň bezpečnosti provozu. Dalším aspektem je technická spolehlivost, kdy jsou počítače mnohem spolehlivější, levnější a lehčí než mechanické přístroje, které často nahrazují. Využitím počítačů je také možné zajistit redundanci jednotlivých systémů. Automatizace taktéž umožňuje ovládání letadla v nestabilních polohách a je využívána v oblasti aerodynamické výkonnosti letadla a snižování spotřeby paliva. [8]

Moderní letadla jsou již standartně vybavena systémem autopilota, automatického ovládání tahu motorů, managementu letu a dalšími vysoce automatizovanými systémy. Cílem tohoto vybavení je odebrání povinnosti manuálního řízení letadla pro pilota letícího tak, aby mohl své kapacity věnovat zvyšování situačního povědomí či řešení nastalých situací za letu. V současné době se dá funkčnost autopilota rozdělit do dvou skupin, a to zvolené vedení a řízené vedení. V případě zvoleného vedení se jedná o dosažení cíle, zvoleného posádkou na příslušném ovládacím panelu, za pomocí autopilota. V druhém případě se jedná o vedení letadla po zadaném letovém plánu díky vstupům od systému managementu letu. [8, 9]

1.1.3 Airbus UpNext

Airbus UpNext je součástí letadlového výrobce Airbus S.A.S. a zabývá se inovacemi a budoucností letecké dopravy. Hlavními úkoly tohoto oddělení je identifikace trendů letecké dopravy ve světě, vývoj a prokazování vhodných konceptů a vývoj aplikací pro technologie zaváděné do reálného provozu.

1.1.3.1 Airbus Autonomous Take–Off and Landing (ATTOL)

Airbus Autonomní pojíždění, vzlet a přistání (ATTOL) je projekt zaměřený na autonomní řízení letadla v kritických fázích letu. Technologický demonstrátor tohoto projektu, Letoun Aribus A350 (Obrázek 4), vybavený potřebnými technologiemi a senzory vykonal vůbec první cyklus autonomního pojíždění, vzletu a přistání. Výraznou odlišností tohoto projektu je pak fakt, že dané autonomní procesy nejsou závislé na žádné vnější infrastruktuře, jako je systém přesného přístrojového přiblížení (Instrument Landing System – ILS) nebo globální polohový systém (Global Positioning System – GPS). Letadlo se tak pohybuje v prostoru výhradně díky senzorům a systémům na palubě. V průběhu projektu, jehož letová část trvala dva roky, bylo provedeno kolem 500 letů, z nichž 450 bylo určeno ke sběru dat a úpravě algoritmů. Cílem projektu je zjistit, jak algoritmizace a strojové učení mohou umožnit pilotům soustředit se na jiné aspekty jejich práce, jako je strategické rozhodování a management mise. Dalším z cílů bylo právě dokázání možnosti operování pouze na základě palubních systémů, což může vést k výrazným úsporám na infrastruktuře. Výstupem úspěšného projektu jsou pak data, která může Airbus využívat v rámci dalšího vývoje letadel. [10, 11]

Obrázek 4: Technologický demonstrátor s dodatečným senzory v přední části letounu. Převzato z [12]

1.1.3.2 Airbus Dragonfly

Airbus Dragonfly je další z projektů Airbus UpNext, který v jisté míře navazuje na výše zmíněný projekt. Název projektu Vážka není náhodný. V tomto projektu je využito biologicky inspirovaného inženýrství. Vážka totiž disponuje 360° zorným polem a schopností identifikace orientačních bodů, které pak využívá k určení hranice teritoria, což byla inspirace pro vytvoření systému, který bude schopný sledovat svoje okolí a bezpečně se v něm pohybovat. [12]

Cílem je zkonstruování takového systému, který bude zaměřen na snižování rizika nouzových operací. Systém by měl disponovat kontinuálním sledováním parametrů důležitých pro bezpečnost. Mezi ně patří sledování okolního prostoru letadla, sledování stavu posádky a další. Poté, například při neschopnosti pilotů vykonávat svoji práci, tento systém problém identifikuje a je schopný provést bezpečné přistání letadla na vhodném letišti. Systém pak při rozhodování bere v potaz nejrůznější provozní podmínky, které by mohly ohrozit bezpečnost letu, a zvolí nejvhodnější trajektorii k dosažení letiště. Projekt počítá s faktory jako je počasí, provoz, vojenské prostory, množství paliva a další.

V průběhu celé operace pak projekt počítá s komunikací letadla s řízením letového provozu. Princip autonomního přistání je pak shodný s projektem ATTOL, kdy je tedy veškeré potřebné vybavení dostupné na palubě. Navíc díky senzorům a algoritmům by mohlo docházet například ke snižování minim při přiblížení na přistání. Další funkcionalitou tohoto projektu je asistence při pojíždění, kdy je například počítáno s přenosem hlasových instrukcí pro pojíždění v reálném čase do grafické podoby, pro lepší orientaci pilotů. [12]

1.1.4 Boeing Aurora

Centrem pro inovace v letectví pro největšího výrobce letadel v Americe je právě Aurora Flight Sciences. Tato společnost se zabývá, jako její protějšek v Evropě, inovacemi, designem a prokazováním využitelnosti nových technologií v letectví.

1.1.4.1 Projekt Centaur

Centaur je volitelně pilotovatelná letecká platforma, na které Aurora demonstruje a testuje své technologie. Jedná se o dvoumotorový letoun všeobecného letectví, který je vybaven systémy, které umožňují jak klasické ovládání pilotem, tak ovládání na dálku z pozemní stanice i autonomní let. Platforma je pak využívána pro testování technologií jako například autonomní vedení, navigace a ovládání, což je projekt obdobný s projektem Dragonfly. [13]

1.1.5 Limitiace

Jako každá inovace i automatizace v letadlech má své limitace. Přestože automatizace výrazně zvyšuje bezpečnost letectví, je nutné ji využívat obezřetně a brát v potaz veškerá její úskalí. Hlavní z těchto úskalí zde budou zmíněna.

Zásadní problém spojený se zvyšující se mírou automatizace vzniká na rozhraní pilot – automatizace. To zahrnuje například nepochopení systému pilotem. Tím je myšleno, že pilot nemá dostatečné znalosti o složitém automatizačním systému, což může v konečném důsledku vést k provedení nesprávných akcí a snížení bezpečnosti. Další limitací je přílišné věnování pozornosti automatizaci. Posádka se může řídit pokyny od automatizace a kompletně opomenout základní letové parametry jako je úhel náklonu, úhel stoupání/klesání a zatáčení. Důležité je také adresovat, že s přibývající

automatizací ubývá možností pro piloty manuálně řídit letadlo, což vede k degradaci této základní dovednosti. Dále je také nutno zmínit riziko, kdy automatizace vydává v dané situaci nejasné či nevhodné signály, které vedou pouze k prohloubení problému. Za zmínku stojí podobnost s limitacemi jednotlivých konceptů SiPO, které jsou uvedeny dole v textu. [8]

Všechny výše zmíněné problémy pak vychází z několika principů implementace automatizace. Jedním z nich je takzvaný paradox automatizace. Tento paradox spočívá v tom, že s přibývající automatizací, která člověku usnadňuje práci, zároveň člověku vznikají nové povinnosti, pokud by měl v systému efektivně pracovat. Dalším z negativních dopadů automatizace je fakt, že při nízké zátěži automatizace zátěž ještě snižuje, což může vést ke ztrátě ostražitosti a situačního povědomí, avšak v situacích s vysokou zátěží automatizace poskytováním velkého množství informací a dat danou situaci nadále zhoršuje. Toto jsou principiální limitace automatizace.

Problémem, který je nyní nutné vyřešit je stav, kdy dva piloti na palubě + automatizace se rovná vyšší úrovni bezpečnosti, avšak jeden pilot + automatizace představuje významné bezpečnostní riziko. [14, 15]

1.1 Single Pilot Operations

Již od konce 50. let 20. století dochází v oblasti obchodní letecké dopravy k systematickému snižování počtu členů posádky. Koncept provozu s jedním pilotem v kokpitu (Single Pilot Operations – SiPO) je tak logickým a velmi lukrativním vývojovým krokem, ke kterému obchodní letecká doprava směřuje. Provoz obchodní letecké dopravy s pouze jedním pilotem v pilotní kabině je výhodný zejména pro samotné aerolinie, které tak budou mít možnost snížit náklady na posádky a flexibilněji se vyrovnat s nedostatkem pilotů, který v blízké budoucnosti hrozí. [16]

Vize konceptu SiPO spočívá v provedení letu obchodní letecké dopravy jedním pilotem, a to včetně jeho kritických fází. Právě absence druhého člena posádky je největší výzvou tohoto konceptu, a proto je nutné jeho nahrazení věnovat velkou pozornost, aby nedošlo ke snížení bezpečnosti provozu v žádném ohledu.

1.1.1 Bezpečnostní výzvy SiPO

V rámci konceptu již bylo adresováno několik oblastí, které jsou v rámci provozu klíčové a představují hlavní výzvy pro bezpečné zavedení konceptu do provozu. V následující části budou některé oblasti stručně zmíněny.

Jak již bylo zmíněno výše, absence druhého pilota v kokpitu představuje velký krok do neznáma. Zaniká tím totiž možnost křížové kontroly mezi pilotem a druhým pilotem. Proto je nutné ji v rámci SiPO nějakým způsobem nahradit. Tyto způsoby jsou podrobně rozebrány kapitolách 1.1.2 až 1.1.6. Dalším, velice důležitým faktorem, který bude v jedno pilotním provozu ovlivněn je management zdrojů posádky (Crew resource management - CRM). CRM je nedílnou součástí každého více pilotního letu a nelze ho opomíjet. V Tabulka 1 jsou uvedeny výsledné hodnoty získané experimentem prováděným na pilotech s využitím simulátoru, který porovnával právě jednotlivé druhy provozu SiPO z pohledu CRM. Popisované režimy SiPO v rámci experimentu jsou: standartní složení posádky – SSP, jeden pilot a operátor pozemní stanice, kteří disponují spojením pouze pomocí verbální komunikace – JPAK a jeden pilot a operátor pozemní stanice, kteří disponují navíc ještě kamerovým záznamem z kokpitu letounu – JPAVK. Hodnoty uvedené v tabulce jsou vypočteny pomocí analýzy rozptylu (Analysis of variance – ANOVA) z dat získaných od respondentů, kteří dané oblasti hodnotili na 9bodové stupnici. [17]

Tabulka 1: Porovnání režimů SiPO z pohledu CRM. Upraveno z [17]

Hodnocená oblast	SSP	JPAK	JPAVK
Bezpečnost letu	7,70	6,89	6,83
Koordinace posádky	7,14	6,56	6,50
Rozhodovací procesy	7,35	6,85	6,50
Povědomí	8,26	6,88	6,86
Komunikace	7,71	7,24	7,15
Porovnání konfigurací	8,58	5,89	6,78

Z Tabulka 1 je patrné, že standartní složení posádky, což je pilot a druhý pilot na palubě letadla, dosahuje nejlepších výsledků ve všech oblastech. Zbylé dva režimy se překvapivě v několika oblastech příliš neliší. Je nutné podotknout, že i režimy JPAK

a JPAVK získali kladná hodnocení, ne však tak vysoká, jako SSP. Z toho plyne, že je nutné této problematice stále věnovat pozornost a čas, aby se režimy SiPO dostaly na stejné či lepší hodnoty než hodnoty se standartním rozložením posádky.

Další výzvou je degradace schopností pilota se zvyšující se automatizací v kokpitu. V dnešní době je průměrný čas, kdy pilot manuálně řídí letadlo, přibližně 7 minut u letadel Boeing, a dokonce polovina u letadel Airbus. Právě s příchodem SiPO by mohlo docházet ještě ke snižování tohoto času z důvodu většího počtu povinností pilota. V tomto případě by bylo nutné zajišťovat dostatečnou kvalitu schopností pilota například pomocí simulátorů. [17]

Další v pořadí je problém výcviku druhých pilotů. Výcvik druhých pilotů totiž probíhá v dnešní době právě pod dohledem zkušeného kapitána. Druhý pilot tak získává dodatečné znalosti o letadle, vedení v rámci rozhodování v kokpitu nebo například praktické poznatky z provozních postupů společnosti. V případě SiPO by tak bylo nutné najít jiné řešení pro výcvik druhých pilotů. Jako jedna z možností se nabízí audiovizuální záznamy z kokpitu, které by mohly být přehrávány v rámci výcviku. [17]

Největší překážkou konceptu SiPO je bezesporu náhlá nezpůsobilost pilota k letu. To je stav, kdy pilot není z jakýchkoliv důvodů dále schopen aktivně řídit letadlo a je nutný zásah jiné osoby či automatizace. Tento stav nastává v letecké dopravě průměrně jednou za měsíc. Přestože se jedná o největší překážku provozu SiPO, Mayers et al. tvrdí, že není neřešitelná. [17]

1.1.2 SiPO – Pilot bez dodatečné podpory

Jedná se o nejjednodušší a také nejlevnější koncept, kdy dojde pouze k odstranění druhého pilota, ale celkový koncept provozu zůstane nezměněn. S odebráním pilota se výrazně zvýší pracovní zatížení pilota letícího. S narůstajícím pracovním zatížením se zvyšuje i riziko selhání, které může překročit únosnou mez stanovenou pro leteckou dopravu.

Dalším problémem tohoto řešení je nemožnost převzetí kontroly nad letadlem v případě zdravotní či jiné indispozice pilota. Tyto dvě překážky tak z této varianty dělají spíše jen

teoretické řešení, které by v praxi jistě mělo svůj význam, avšak nebude možné zajistit jeho bezpečnost a jeho zavedení do provozu je tedy velice nepravděpodobné. [17]

1.1.3 SiPO – Pilot a palubní personál jako záložní pilot

Tento koncept je založen na pilotovi v kokpitu, který by mohl být v určitých případech doplněn či nahrazen členem palubního personálu letadla. Mezi členy palubního personálu se řadí letečtí maršálové, stevardi a piloti letící jako pasažéři. Stejně jako i jiné koncepty, tak i tento má své překážky. Jako příklady lze uvést systém otevírání dveří do kokpitu po událostech 11. září, dostupnost palubního personálu na jednotlivých letech atd. Pomineme-li již zmíněné překážky, využitelnost tohoto konceptu výrazně klesá s faktem, že členové palubního personálu určení k vykonávání funkce záložního pilota musí disponovat velice podobnými či dokonce stejnými schopnostmi jako samotný pilot, což samozřejmě zahrnuje i pilotní výcvik. Tento požadavek pak vylučuje hlavní dvě výhody provozu SiPO, což je snížení nákladů a vyřešení problému nedostatku pilotů. [17]

1.1.4 SiPO – Pilot a vyspělý automatizační systém na palubě

Po odstranění druhého pilota z kokpitu letadla dochází ke kritickému zvýšení pracovní zátěže na pilota letícího. Tato varianta tak počítá se zavedením softwarového prostředku, který přebere některé funkce druhého pilota a sníží tak pracovní zatížení na přijatelné minimum. Dle Harrise [18] by se neměl druhý pilot pouze nahradit softwarovým prostředkem, ale mělo by dojít k celkovému přehodnocení role pilota a vyvinout vylepšený systém ovládání letadla. Hlavní nevýhodou tohoto konceptu je konflikt mezi člověkem a automatizací. Pro vyřešení tohoto problému bude nutné vyvinout metody rozeznávání konfliktu mezi dvěma subjekty. Se snížením počtu pilotů se taktéž sníží i situační povědomí pilota, které by měli zvyšovat funkce v rámci automatizačního systému. Jedná se například o funkce zobrazení pojezdového systému letiště na průhledovém displeji, rozeznávání hlasu, syntetický hlas nebo například hlasové či vizuální navádění pilota při orientaci v kokpitu a ovládání letadla. Příkladem může být systém zobrazený na Obrázek 5. Na obrázku je možné vidět letoun při přiblížení na přistání, kdy se pilotovi v zorném poli pomocí multifunkčních brýlí zobrazuje stav kontrolního seznamu relevantního pro danou část letu. V dolní části obrázku je možné vidět šipku odkazující na ovládací prvek relevantní pro dokončení seznamu, který

je mimo zorné pole. V případě, že by se tento prvek nacházel v zorném poli pilota, byl by prvek samotný zvýrazněn. Největší překážkou tohoto řešení je samotný vývoj systému. Dle Harrise je vyvinutí takového systému velice náročné a v dnešní době s dnešními technologiemi, finančně neekonomické. [17, 19]

Obrázek 5: Zorné pole pilota při používání vizuálních prostředků. Převzato z [19]

1.1.5 SiPO – Pilot a pozemní člen týmu nahrazující druhého pilota

Tato varianta počítá se zřízením pozemního kontrolního centra, které by bylo v režii aerolinie. V tomto centru by bylo několik operátorů, kteří jsou definováni jako pozemní dopravní piloti (Ground-Based Airline Transport Pilot – GATP). Každý z těchto pozemních pilotů by mohl mít v jeden okamžik na starosti až 12 letadel dané letecké společnosti. Pozemní stanice by měly disponovat systémy umožňujícími kontrolu a ovládání letadla přes datalink. Jedním z navrhovaných systémů je Virtuální pilot asistent (Virtual Pilot Assistant System – VPA). Tento systém by pak umožňoval převedení kontroly nad letadlem pozemnímu pilotovi v případě nutnosti opuštění kokpitu, například

z fyziologických důvodů. Nutno však podotknout, že primární funkcí pozemního pilota by nebylo samotné ovládání letadla, nýbrž pouze kontrola stavu letu. Dále by pozemní pilot také mohl monitorovat zdravotní stav pilota a v případě nezpůsobilosti k letu, převzít řízení. Avšak i toto řešení, které je považováno za nejperspektivnější, má své slabé stránky. Jednou z nich je zmatek v kokpitu, který byl v rámci studií zaznamenán. Jde především o neznalost jednotlivých kompetencí, snížené situační povědomí a chybějící neverbální komunikaci mezi piloty. [17]

1.1.6 SiPO – Pilot s podporou složitého distribuovaného týmu

Tento koncept je založený na rozdělení podpory pro letadlo do několika částí. V kokpitu by byla instalována dodatečná automatizace, která by zastupovala druhého pilota. V kabině pro cestující by se nacházel velitel kabiny cestujících, jak je tomu i v dnešní době, který by řešil potíže s pasažéry a potíže v kabině pro pasažéry. Dále by bylo využíváno pilotů letadel letících v blízkosti, kteří by mohli sloužit jako podpora při vyhýbání se počasí, při checklistech nebo například v nouzových situacích. Dalším členem týmu by byl pozemní personál, který by řešil potíže například v rámci příletu na letiště, či odletu z něj. Populárním je řešení podobné tomu, se kterým je možné se setkat v lodní dopravě. Každé letiště by mělo své pozemní pracovníky, kteří by se starali o bezpečné přílety a odlety letadel. Tito pracovníci by měli rozsáhlé znalosti daného letitě, ze kterých by mohli piloti profitovat. [17]

Změny pracovního vytížení jednotlivých variant získané pomocí Kognitivní pracovní analýzy jsou pak uvedeny v Tabulka 2. Tabulka zobrazuje varianty, kterými jsou současný stav, varianta A, odpovídající konceptu uvedenému v kapitole 1.1.2, varianta B, kde je aplikováno zrcadlení systémů pro monitorování ze země, varianta C, odpovídající kapitole 1.1.5 a varianta D, která taktéž odpovídá kapitole 1.1.5 s využitím zrcadlení systémů. Pod tímto termínem se rozumí systém, který na zemi věrně replikuje vstupy pilota a naopak. [20]

Tabulka 2: Vytížení při jednotlivých variantách. Upraveno z [20]

Vytížení/Varianty	Současnost	A	B	C	D
Pilot letící	90	217	217	90	90
Pilot monitorující/Pilot na zemi	160	-	-	160	160
Letadlová automatizace	143	143	143	143	143
Zrcadlení systémů	-	-	143	-	143

1.1.7 Extended minimum crew operation – eMCO

Koncept SiPO je však až finálním výsledkem snahy o redukci posádek v obchodní letecké dopravě. Za mezistupeň k provozu SiPO je považován Rozšířený provoz minimálních posádek (Extended minimum crew operation – eMCO), dříve známé také jako Reduced crew operation – RCO. Princip provozu eMCO se poměrně zásadně liší od SiPO. Jedná se o provoz, kdy se v letadle nachází dva piloti stejně jako nyní. V průběhu kritických fází letu, kterými jsou především vzlet a přistání, ale také například průlet prostorem s vysokým vytížením, odlet z letiště a prvotní fáze stoupání nebo klesání a přílet by byli oba piloti v pilotní kabině a let probíhal podle pravidel, která známe dnes. Avšak v případě, že by letadlo bylo mimo kritické fáze letu (nejvhodnější je let v hladině), nastane významný rozdíl. Jeden z pilotů, označovaný jako pilot odpočívající (pilot resting – PR) by se neměl podílet na řízení letadla a v rámci zvyšování efektivity využití posádek by tento pilot odpočíval, potažmo spal. Koncept pracuje se dvěma možnostmi, a to s odpočinkem pilota v pilotní kabině, či kabině pro cestující a odpočinkem mimo kabinu v prostorách k tomu určených. [21–24]

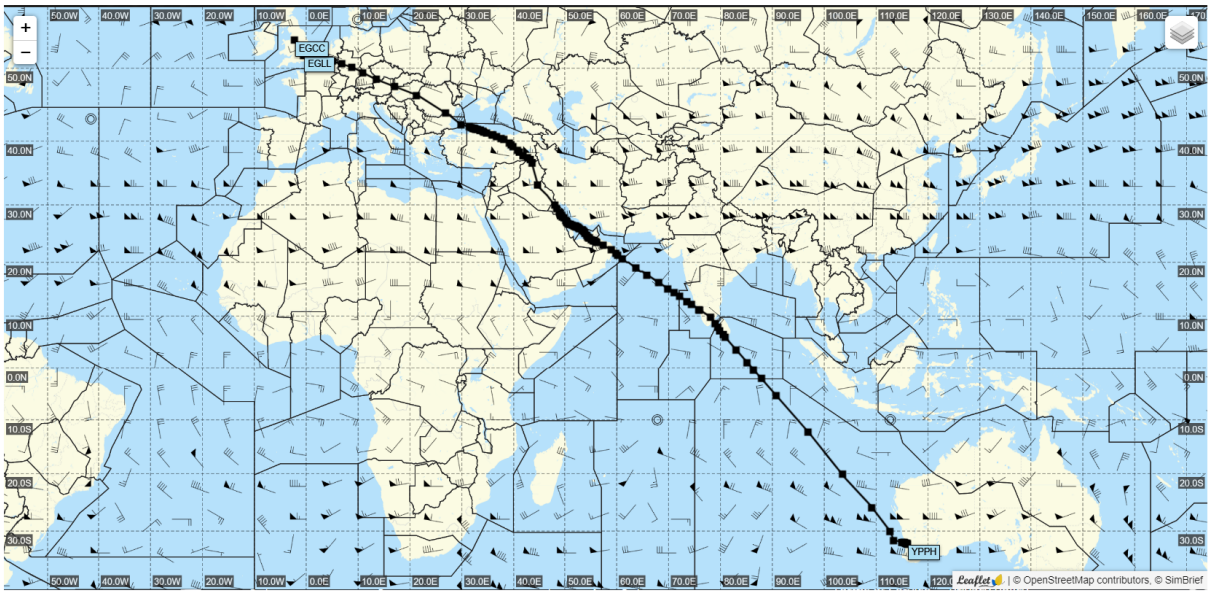
Pokud by se PR nacházel v pilotní kabině či v kabině pro cestující, bylo by nutné ho pro kvalitní odpočinek oddělit od všech vnějších vjemů. Řešením tohoto problému by byla například protihluková sluchátka a maska na oči. Tato možnost odpočinku by se nejspíše týkala především letadel na střední tratě, viz Boeing 737 či Airbus A320 family, kde se nenachází oddělení pro odpočinek posádek (Crew rest compartment – CRC). Na palubách většiny dálkových letadel, která budou nejvíce benefitovat z provozu eMCO, se však CRC nachází, a tudíž by se nabízela možnost odpočinku mimo kabinu, právě v CRC. [21–24]

Parametry samotného odpočinku zatím nebyly přesně stanoveny, ale dá se předpokládat, že se bude jednat o výrazně delší časové intervaly, než se kterými je možné se setkat nyní v rámci odpočinku posádek. V současné době jsou totiž intervaly odpočinku časově omezeny, aby nedocházelo ke spánkové setrvačnosti. Tento druh odpočinku však nelze využít v plánování posádek a slouží pouze ke zlepšení schopností posádky.

1.1.7.1 Příklad letu eMCO

Protože ještě neexistuje jednotný a jasný koncept provozu eMCO, bude v této části uveden příklad dálkového letu v rámci provozu eMCO. Tento příklad je z části představa autora o dané problematice a slouží pouze k lepšímu pochopení problematiky. Nejedná se tedy o finální verzi konceptu ani o verzi, která bude analyzována v rámci praktické části.

Jako let vhodný pro demonstraci konceptu eMCO byl zvolen let QF9 společnosti Qantas, který směřuje z Austrálie, města Perth do Evropy, Londýna. Let je pravidelně operován letounem Boeing 787−900, který je svým vybavením ideálním kandidátem pro provoz eMCO. Na Obrázek 6 je možné vidět přibližnou trasu letu. Doba letu je 17 hodin a 45 minut. Z dat dostupných na portálu Flightradar24 je možné stanovit, že průměrná doba pro dosažení cestovní hladiny, která se pro tento let pohybuje okolo FL380, je přibližně 40 minut. Průměrná doba od zahájení klesání, do přistání je 30 minut. Jednoduchým a přibližným výpočtem je možné zjistit celkový čas letu v hladině, který je asi 16 hodin 35 minut. Je nutné také počítat s dobou nutnou pro předání povinností a brífink před zahájením a po skončení jednopilotní části letu a další situace, kdy musí být v kokpitu oba piloti. Tudíž vychází přibližně 13 až 14 hodin, při kterých může probíhat odpočinek. [25]



Obrázek 6: Trasa letu QF9. Převzato z [26]

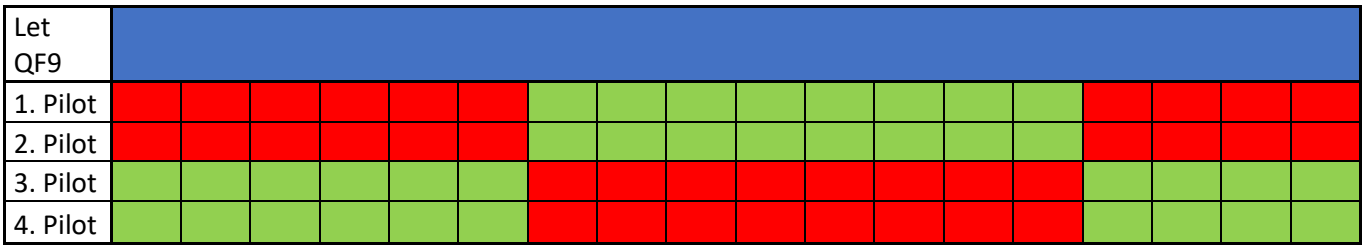
Z legislativy upravující pracovní dobu a odpočinek pro létající personál je jasné, že pro tento let je maximální pracovní doba letové posádky 13 hodin, to je však doba od nástupu pilota do práce do ukončení letu. Maximální čas, při kterém může pilot aktivně řídit letadlo je legislativně stanoven na 10 hodin v případě dvoupilotní posádky a 8 hodin v případě jednopilotní posádky. Protože eMCO je ve své podstatě jednopilotní provoz, bude nadále počítáno s limitem 8 hodin. Z toho jasně plyne, že tento let nemůže v současné době vykonat letová posádka ve složení dvou pilotů. Je běžnou praxí, že se na takové lety nasazují četnější posádky, například v počtu 4 až 5 pilotů v závislosti na délce letu, kdy se na palubě nachází jeden kapitán a daný počet prvních důstojníků (ne nutně hodnostně, nýbrž funkcí). Taktéž je možné ve výše zmíněném dokumentu nalézt dobu odpočinku, kterou je nutné po takovém letu dodržet. Doba odpočinku v destinaci zvoleného letu je 14 hodin. [27, 28]

V rámci samotného odpočinku se nabízí následující. Ve vhodném okamžiku po vzletu by se PR odebral do CRC, kde by započal odpočinek spolu s již odpočívajícími dalšími členy posádky. V kokpitu letadla by zůstal pouze jeden pilot dohlížející na bezpečnost letu. Protože doba letu přesahuje 8 hodin, musí v průběhu letu dojít i k výměně pilota letícího. K tomu by mělo v ideálním případě dojít takovým způsobem, aby se byl pilot letící – kapitán schopen vrátit do kokpitu letadla pro kritické fáze letu. Výsledkem odpočinku by mohla být redukce pilotů na daný let se zachováním doby odpočinku po

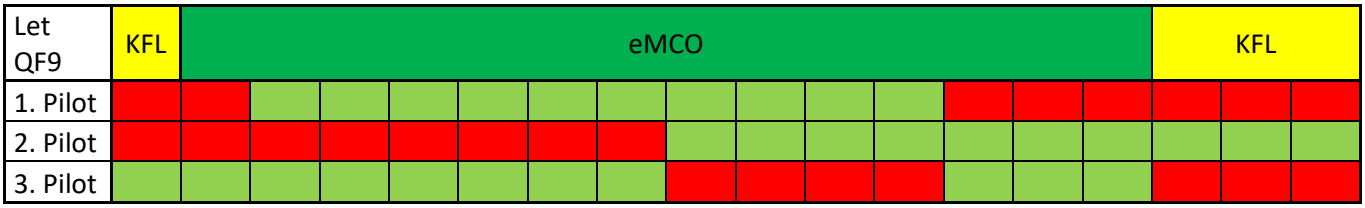
letu, či zkrácení doby odpočinku po letu se zachovaným počtem pilotů. V některých případech může docházet i ke kombinaci těchto dvou řešení. Všechny tyto varianty výrazně zvyšují využitelnost letových posádek. Srovnání současného řešení posádek a možného řešení eMCO na dlouhých letech je uvedeno v Tabulka 3 a

Tabulka 4. Červeně je v tabulce vyznačena doba, kdy daný člověk vykonává svoji funkci a zeleně doba, kdy odpočívá. Jeden sloupec tabulky značí 1 hodinu. Zkratkou KFL jsou označeny kritické fáze letu.

Tabulka 3: Střídání pilotů v současné době



Tabulka 4: Návrh řešení v rámci eMCO



Ze srovnání obou tabulek je na první pohled patrné, že v tomto případě by díky konceptu eMCO mohlo dojít ke snížení počtu pilotů ze 4 na 3, což je pro aerolinie významná úspora. Je nutné podotknout, že tento příklad byl vytvořen na základě současné legislativy, upravující maximální doby letu, která může být v rámci zavádění eMCO změněna ve prospěch tohoto konceptu. Z dalšího zkoumání lze stanovit, že pokud by byl odpočinek v rámci provozu eMCO považován za stejně kvalitní jako odpočinek mimo službu (některé studie s tímto počítají), bylo by možné zkrátit některým členům posádky, viz. 2. pilot, dobu odpočinku o dobu strávenou odpočinkem v letadle (v tomto případě 10

hodin) a umožnit tak zaměstnavateli například dřívější let tohoto člověka zpět v rámci jiné posádky.

1.2 Dostupná literatura

Protože se nacházíme v rané fázi vývoje systémů eMCO a SiPO je množství dostupné relevantní literatury poněkud malé. Avšak i přesto je možné najít dostatek referencí pro zhotovení této práce. V této části práce jsou zmíněné ty, které jsou dle autora nejrelevantnější. Jedním ze stěžejních dokumentů je článek *Single Pilot Operations IN Commercial Cockpits: Background, Challenges, and Options* [17]. Tato publikace nastiňuje vývoj provozu s jedním pilotem v kokpitu, dále vysvětluje benefity a úskalí SiPO, zobrazuje koncepty, jak by mohl provoz SiPO vypadat a v neposlední řadě taktéž dává doporučení v oblastech budoucí implementace. Podobný je z velké části i článek *Wearable Technologies as a Path to Single-Pilot Part 121 Operations* [19], který navrhuje možnosti, jak vyřešit problém zvyšujícího se pracovního zatížení pilota po odstranění druhého člena posádky. V práci jsou prezentovány jednotlivé možnosti, jako například multifukční brýle, jejich vlastnosti a princip fungování. Dále je zde i prezentována vize letadla budoucnosti, které je vhodné pro provoz SiPO. [17, 19]

Dalším dostupným článkem je *Progressing Toward Airliners' Reduced-Crew Operations: A Systematic Literature Review* [21]. V této práci se nachází přehled dostupné literatury pro daná klíčová slova (SiPO, RCO) a následně jsou zde uvedeny oblasti, které prozatím brzdí implementaci těchto systémů. Jako příklad může být uvedena neschopnost pilota k letu či s tím související nutnost kontroly zdravotního stavu letové posádky. [21]

Dalším, neméně důležitým, je dokument vydaný Agenturou Evropské unie pro bezpečnost v letectví (European Union Aviation Safety Agency – EASA). Jedná se o dokument *Horizon Europe Project: Extended Minimum Crew Operations – Single Pilot Operations – Safety risk assessment framework* [22]. V tomto dokumentu se nachází technické specifikace systémů eMCO a SiPO. [22]
Jednotlivé publikace se tedy zabývají limitacemi současného stavu, které jsou uvedeny v kapitole 1.1.5. Navrhují řešení daných problémů, stanovují koncepty provozu a vyhodnocují jejich využitelnost a proveditelnost. Stejně tak cílem této práce je díky bezpečnostní analýze systému eMCO přispět k vývoji tohoto systému a stanovit oblasti,

kterým je nutné při designu systému věnovat vyšší míru pozornosti a zajistit tak především bezpečný proces implementace a provozu tohoto, pro letectví významného, systému.

2 Metodika

V této části práce je uvedena metodika práce v rámci praktické části. V kapitole 2.1 jsou uvedeny informace ohledně databáze metod, která je využívána k nalezení vhodné metody bezpečnosti. Dále se zde nachází i popis, jak bylo s databází pracováno. V kapitole 2.2 je pak uvedena stěžejní analýza této práce a to STPA. V této kapitole jsou nastíněny všechny náležitosti analýzy a taktéž je popsána práce s analýzou. Poslední kapitolou je kapitola 2.3, která se věnuje způsobům zhodnocení rizika a jejich využití v rámci této práce.

2.1 Databáze metod bezpečnosti

Databáze metod bezpečnosti je dokument vytvořený Nizozemským centrem pro letectví a kosmonautiku. Tento dokument byl vytvořen v kooperaci s několika subjekty z celého světa a poskytuje aktuální seznam dostupných metod bezpečnosti. V současné době je v dokumentu zahrnuto 866 bezpečnostních metod. Lze však předpokládat, že toto číslo se bude nadále zvětšovat v dalších aktualizacích materiálu. [29]

Dokument se skládá ze tří hlavních částí. První částí je samotný přehled bezpečnostních metod, pak následuje část se statistikami, a nakonec veškeré zdroje a prameny. [29]

2.1.1 Přehled bezpečnostních metod

V této části dokumentu jsou, jak již bylo zmíněno výše, uvedeny bezpečnostní metody. Metody jsou zobrazeny formou tabulky, kdy každá z metod je náležitě popsána. K popisu je využito celkem jedenácti atributů, které budou v této části rozebrány na referenční metodě. Na Obrázek 7 a Obrázek 8 je uvedena jedna zmíněná metoda společně s legendou.

Id	Method name	For-mat	Pur-pose	Year	Aim/Description	Remarks
784.	STPA (Systems Theoretic Process Analysis)	Tab	Mit	2008	STPA is a qualitative hazard analysis technique that assumes that accidents occur not simply because of component failures, but because constraints on component behavior are inadequately enforced. It is used to identify instances of inadequate control that could lead to the presence of hazards, to identify safety-related constraints necessary to ensure acceptable risk, and to gain insight into about how those constraints may be violated. This information can be used to control, eliminate, and mitigate hazards in the system design and operation. STPA can be applied to existing designs, or in a proactive way to help guide the design and system development.	STPA is based on STAMP and was developed by Nancy Leveson and co-authors.

Obrázek 7: Referenční metoda, část 1. Převzato z [29]

Safety assessment stage								Domains	Application					References
1	2	3	4	5	6	7	8		Hw	Sw	Hu	Pr	Or	
		3	4		6			avionics, ATM, aviation, oil&gas, defence, space, rail, food	x	x	x	x	x	• [Leveson, 2011] • [Thomas & Leveson, 2011]

Obrázek 8: Referenční metoda, část 2. Převzato z [29]

Prvním atributem každé metody je identifikátor. Každá z metod má jedinečný identifikátor, tudíž může být využit k vyhledání jednotlivých metod a jednodušší orientaci v dokumentu. Identifikátorem referenční metody je číslo 784. Dalším atributem je jméno dané metody společně s využívanou zkratkou. Po jméně metody následuje formát, ve kterém je metoda napsána. Formáty využité v tomto dokumentu jsou uvedeny v Tabulka 5. [29]

Tabulka 5: Formáty využité v dokumentu. Upraveno z [29]

Zkratka	Popis formátu
Gen	Obecný princip, či teorie, než specifická metoda
Step	Krokový přístup, či technika. Taktéž metody se specifickým postupem
Tab	Statický přístup s podporou tabulek, kontrolních seznamů a dotazníků

Stat	Statický přístup či model s grafickou podporou
Dyn	Dynamický model s grafickou podporou. Často na matematické bázi
Math	Matematická formulace s minimální nebo žádnou grafickou podporou
Int	Rámec nebo integrovaná metoda skládající se z více metod
Dat	Databázový nástroj, či nástroj uchování dat
Min	Nástroj analýzy, či získávání dat
RTS	Simulace v reálném čase
FTS	Simulace ve zrychleném čase

Dalším atributem je účel dané metody. Účel metody udává v jisté míře, k čemu by daná metoda měla být využita a jaké výsledky je možné očekávat. V dokumentu je využito několik kategorií účelu, které jsou přehledně uvedeny v Tabulka 6.

Tabulka 6: Účely využité v dokumentu. Upraveno z [29]

Zkratka	Popis účelu
Mod	Tvorba modelu
Par	Posouzení hodnoty parametru (pravděpodobnost lidské chyby atd.)
HRA	Analýza spolehlivosti lidského faktoru či analýza lidského pochybení
HFA	Analýza lidského faktoru (mimo spolehlivosti, například chování, situační povědomí atd.)
Task	Analýza úkolu člověka
Trai	Technika výcviku nebo metoda pro analýzu výcviku
Des	Technika designu (tvorba/zajištění bezpečného designu)
Dec	Rozhodovací procesy
SwD	Analýza závislosti softwaru nebo technika testování softwaru
HwD	Analýza závislosti hardwaru (spolehlivost, udržovatelnost, dostupnost atd.)
OpR	Analýza rizika operace či bezpečnostně kritického scénáře
Org	Posouzení organizace, bezpečnostního managementu nebo bezpečnostní kultury
Dat	Uchovávání dat a sdílení informací
Mit	Zmírnění rizika

HzI	Identifikace nebezpečí, příčin, problémů
HzA	Identifikace a analýza frekvence a/nebo závažnosti nebezpečí, příčin, problémů
CoI	Analýza rizika kolize, převážně mezi letadly
VaI	Analýza validace, verifikace, zaujatosti
Ret	Retrospektivní analýza nehody nebo události

Dalším atributem je rok zveřejnění dané metody. Poté následuje stručný popis dané metody, který by měl čtenáři danou metodu přiblížit. V případě zájmu jsou pak v posledním atributu, v referencích, uvedeny kompletní dokumenty o dané metodě. Dalším atributem jsou poznámky k dané metodě. Poté následuje rozmezí posouzení bezpečnosti, ve kterém je možné a vhodné danou metodu využít. Rozčlenění vychází z obecného posouzení bezpečnosti, které je uvedeno v Programu bezpečnostního posouzení 15 (SAP-15 - Safety Assessment Program 15). Rozčlenění je uvedeno v Tabulka 7. [29]

Tabulka 7: Rozčlenění využité v dokumentu. Upraveno z [29]

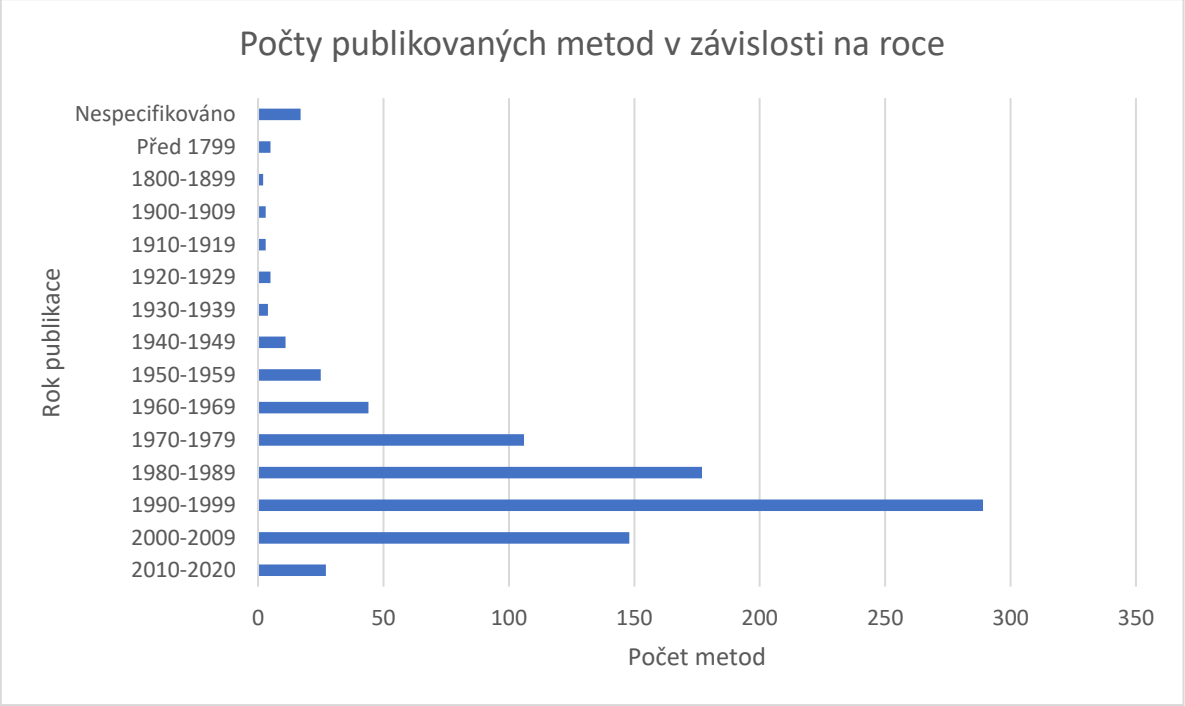
Číslo fáze	Popis fáze
1	Určení rozsahu posouzení
2	Nastudování normálního provozu
3	Identifikace nebezpečí
4	Začlenění nebezpečí do rámce rizik
5	Vyhodnocení rizika
6	Identifikace potenciálních zmírňujících opatření pro snížení rizika
7	Monitorování a ověření bezpečnosti
8	Čerpání znalostí ze zpětné vazby

Dalším atributem je doména metody. Jedná se o výčet domén (například letectví, chemický průmysl, jaderný průmysl), ve kterých byla daná metoda využita. Podtržené domény jsou pro danou metodu nejvhodnější. Pokud je předpoklad, že je daná metoda použitelná v některé z domén, avšak nebyl nalezen žádný příklad tohoto použití, je tato

doména uvedena v závorkách. Dalším atributem každé metody je aplikovatelnost metody. V tomto atributu je uvedeno, zda je metoda vhodná pro použití v oblasti hardware, software, člověk, procedury nebo organizace. [29]

2.1.2 Ostatní části

Ve zbylé části dokumentu se pak nachází statistiky a reference. V části se nachází několik grafů a tabulek, které seskupují jednotlivé metody dle různých kritérií. Z těchto statistik je pak možné vyčíst mnoho zajímavých informací týkajících se metod bezpečnosti. Jako jeden příklad může být uvedena například statistika metod podle roku publikování, viz. Graf 1.



Graf 1: Počty publikovaných metod v závislosti na roce. Upraveno z [29]

Z Graf 1 je patné, že k významnějšímu vývoji metod začalo docházet až po příchodu první průmyslové revoluce, což je logické, vzhledem k faktu, že s příchodem průmyslové revoluce byly do provozu zařazovány velké a často velice nebezpečné stroje. Z toho plynuly mnohem častější nehody a úrazy a bylo tak nutné zajistit vyšší bezpečnost, převážně pak na pracovišti. S nabýváním dalších zkušeností v této oblasti a s větším kladením důrazu na bezpečnost pak počty publikovaných metod výrazně rostly.

Poslední částí dokumentu jsou pak, výše zmíněné reference a odkazy na jednotlivé metody, modely a principy.

2.1.3 Práce s databází

Stěžejním krokem celé práce je zhotovení bezpečnostní studie na dané téma pomocí moderních metod bezpečnostního inženýrství. A právě v problematice analýzy a výběru některé z dostupných metod bylo využito databáze metod bezpečnosti. Vzhledem k faktu, že je databáze pravidelně aktualizována a obsahuje tak komplexní soubor starších i nových inovativních metod se toto řešení jeví jako velice výhodné. Proces výběru je založen na splnění předem určených požadavků, které by měla daná metoda splňovat. Tyto požadavky jsou pak porovnány s atributy jednotlivých metod a na základě shodnosti s nejvíce požadavky je zvolena daná metoda bezpečnostního inženýrství.

Prvním požadavkem je možnost využití metody proaktivně. Protože se námi analyzovaný systém nachází ve fázi raného designu nejsou k dispozici provozní informace o systému eMCO, které by bylo možné využít pro některou z retrospektivních metod. Dalším požadavkem je vhodnost metody pro daný systém. Vzhledem ke komplexnosti zadaného systému je nevhodné využití jakékoliv jiné metody než metody systémové. To znamená, že daná metoda je vhodná pro použití ve všech aspektech systému, jmenovitě hardware, software, lidský činitel, procedury a organizace. Při využití jiné, než systémové metody by mohlo dojít například k opomenutí některých nebezpečí. Posledním z hlavních rozhodujících atributů je doména, pro kterou již byla metoda využita nebo pro kterou je metoda vhodná. V tomto případě je cíleno na metody z domén letectví, či letadlo. Výsledkem zhodnocení je volba metody bezpečnostního inženýrství, v tomto případě STPA (System-Theoretic Process Analysis). Tato metoda splňuje všechny požadavky zadání i požadavky zadané autorem. Za zmínku stojí, že v rámci hledání vhodné metody bylo identifikováno několik metod, které splňovaly většinu kritérií. Mezi nimi byly například metody CAST (Causal Analysis based on STAMP) a O&SHA (Operating and Support Hazard Analysis). Ani jedna z těchto zmíněných metod však plně neodpovídá požadavkům. CAST z důvodu, že se jedná o retrospektivní metodu a O&SHA z důvodu, že se nejedná o systémovou metodu, protože nezahrnuje odvětví organizace.

2.2 STPA (System-Theoretic Process Analysis)

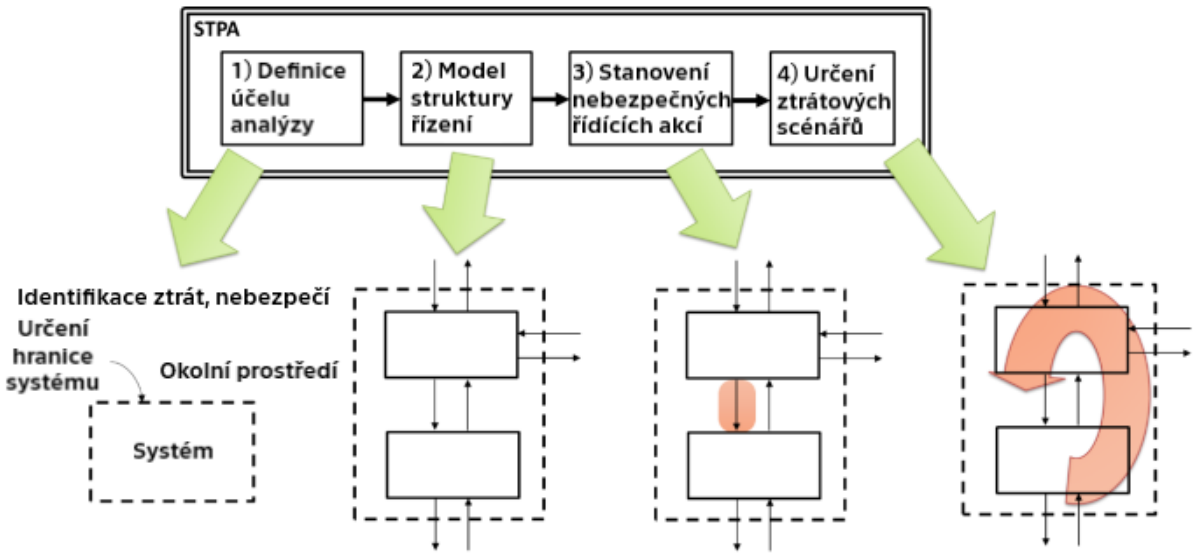
Každá metodika v oblasti bezpečnosti musí být založena na některém z teoretických základů. Nejinak je tomu i v případě STPA. Tato metodika je založená na modelu System-Theoretic Accident Model and Processes (STAMP). STAMP je model založený na systémové teorii. Tato teorie je odlišná od všech svých předchůdců tím, že se systémem zabývá jako celkem, namísto rozdělení systému na jednotlivé části a řešení po částech. Z toho také vychází známé tvrzení systémové teorie, že celek je více než suma všech částí. To je možné si vyložit tak, že některé vlastnosti systému jsou viditelné pouze tehdy, pokud je na systém nahlíženo jako na celek. To znamená, že některé vlastnosti vznikají interakcí mezi jednotlivými částmi systému. Spolu se staršími přístupy k bezpečnosti, jako je modelování lineárních řetězců událostí, které je podmnožinu STAMP, je tak možné vytvářet komplexní metody, které mohou obsahovat výsledky starších metod jako podmnožinu. [30]

STPA je tedy nástroj využívající model STAMP. Jedná se o proaktivní bezpečnostní metodu, což znamená, že tato metoda je využívána pro zjištění možných příčin nehod ještě před samotným uvedením systému do provozu. Cílem je tedy eliminace nebo kontrola nebezpečí ještě před začátkem provozního života systému. STPA je systémovou metodou a je tak vhodná pro složité systémy, kde starší metody často nachází své limity. [31]

2.2.1 Postup STPA

Metodika STPA je důkladně vysvětlena v dokumentu STPA Handbook, tudíž zde budou pouze obecně zmíněny hlavní body analýzy, viz. Obrázek 9. Prvním krokem je určení účelu analýzy, do čehož spadá určení zúčastněných stran, ze kterých mohou být odvozeny ztráty. Ztráty jsou stavy, které jsou pro některou ze zúčastněných stran nepřípustné. Dalším krokem je pak identifikace samotného systému. V tomto kroku je stanovena a popsána komplexnost systému, vymezena hranice systému a zvolena rozlišovací úroveň vhodná pro danou analýzu, na což pak navazuje určení systémových nebezpečí. To jsou stavy systému, které spolu s nejhoršími environmentálními podmínkami vedou na ztráty. Poslední částí prvního kroku je určení systémových

omezení. To jsou stavy systému, které musí být dodrženy, aby nedošlo k nebezpečí, které může vést ke ztrátě. [31]



Obrázek 9: Základní přehled metody STPA. Upraveno z [31]

Dalším krokem analýzy je vytvoření struktury řízení daného systému. Jedná se o hierarchický model, který se skládá z řídících a řízených prvků. Tyto prvky jsou propojeny pomocí vazeb, a to pomocí řídících akcí, které vedou od řídících prvků k řízeným a zpětných vazeb, které spojují řízené prvky s řídícími. Systém je tedy graficky modelován a vazby mezi prvky jsou popsány. Ve struktuře řízení je nutné zachovat hierarchické zobrazení, což znamená, že prvky s nejvyšší autoritou by měly být ve vrchní části modelu a poté níže prvky s klesající autoritou. [31]

Dalším krokem analýzy je identifikace nebezpečných řídících akcí. Nebezpečná řídící akce je taková akce, která v určitém kontextu a za nejhorších environmentálních podmínek vyústí v nebezpečí. Metoda STPA pracuje s tvrzením, že řídící akce se mohou stát nebezpečnými 4 způsoby. Tyto způsoby jsou uvedeny níže. [31]

- Neprovedení řídící akce způsobuje nebezpečí
- Provedení řídící akce způsobuje nebezpečí
- Provedení řídící akce příliš brzy, příliš pozdě, ve špatném pořadí
- Ukončení řídící akce příliš brzy, aplikování řídící akce příliš dlouho

Po stanovení řídících akcí je dalším krokem identifikace omezení řídících prvků. Jedná se o překlad nebezpečných řídících akcí do formy omezení podobně, jako tomu bylo v prvním kroku analýzy. [31]

Posledním krokem analýzy je určení ztrátových scénářů. Ztrátové scénáře popisují kauzální faktory vedoucí k nebezpečným řídícím akcím a nebezpečí. Metoda v oblasti určování těchto scénářů pracuje s teorií, že tyto scénáře vznikají především nebezpečným chováním řídícího prvku nebo nedostatečnou zpětnou vazbou a informacemi. Tímto krokem je pak celá analýza dokončena. Výsledky analýzy lze použít například k identifikaci doporučení designu, tvorbě požadavků nebo například k vytvoření efektivnějšího managementu bezpečnosti. [31]

2.2.2 Využití STPA a systémové teorie

Jak již bylo zmíněno nahoře, pro samotnou bezpečnostní analýzu je zvolena metoda STPA. Práce s analýzou je vykonána v souladu s dokumenty *STPA Handbook* [31] a *Engineering a Safer World* [30]. Druhá ze zmíněných publikací je využívána převážně z důvodu, že se autor snaží o vytvoření komplexní analýzy bezpečnosti systému, který v současné době existuje pouze jako koncept a ovlivnit tak další vývoj konceptu, nejen o provedení STPA. Proto je využívána kapitola 10 publikace *Engineering a Safer World*, která je věnovaná integrování bezpečnosti do systémového inženýrství. V této kapitole je pak popsáno několik aspektů, které tvoří komplexní zhodnocení bezpečnosti systému. Pro práci stěžejní je pak systémová bezpečnost a lidský činitel integrovaný do typického procesu systémového inženýrství. Zásadní kroky tohoto procesu, které jsou relevantní pro tuto práci jsou uvedeny níže.

- Stanovení cílů systému
- Identifikace omezení, jak může být cíle dosaženo
- Výběr architektury systému
- Identifikace environmentálních předpokladů
- Tvorba konceptu provozu
- Provedení předběžné analýzy úkolů operátora
- Provedení STPA

Některé z těchto bodů obsahují ještě další podbody, které mohou být dohledány ve zmíněné publikaci. [30]

Body, které potřebují další komentář zde budou zmíněny. V rámci Identifikace omezení, jak může být cíle dosaženo je nutné stanovit nejen bezpečnostní omezení, ale také omezení, která se týkají dalších vlastností návrhu systému. To jsou omezení, která nemají dopad na bezpečnost a často vychází právě z principu daného systému. Dále to mohou být například omezení zadaná zadavatelem. To mohou být například omezení dané požadovanou efektivitou od konečného systému a další. [30]

Stanovení environmentálních předpokladů je důležité pro jasné určení podmínek, ve kterých je systém analyzován. Podmínky se mohou v průběhu času měnit, což by mělo vyústit v kontrolu analýzy a ověření správnosti. [30]

Koncept provozu je v tomto případě vytvořen na základě dostupné literatury a odpovídá tak současným možnostem. Provedení předběžné analýzy úkolů operátora zajistí zdokumentování principu fungování člověka v systému. Výstup analýzy slouží i pro kontrolu úplnosti následné analýzy, v tomto případě STPA. V rámci této práce bylo využito Hierarchické analýzy úkolů (Hierarchical Task Analysis – HTA). HTA je využito, protože se jedná o jednu z nejlepších úkolových metod současnosti a taktéž protože je možné ji využít na analýzu jakéhokoliv úkolu. [32, 33]

Provedení samotné analýzy STPA je pak rozděleno do dvou iterací. To znamená, že systém je v rámci první iterace posuzován abstraktně a v následující iteraci se tento systém dále konkretizuje. Ve druhé iteraci jsou pak zohledněny jednotlivé vhodné varianty provozu uvedené v tomto dokumentu, což znamená, že druhá iterace analýzy obsahuje několik analýz. Cílem tohoto rozčlenění je přehlednost analýzy a co možná nejpřesnější a správné zhodnocení systému z pohledu bezpečnosti.

2.3 Zhodnocení rizika

V této kapitole práce jsou uvedeny základní informace a popis standartní matice rizik (Kapitola 2.3.1), dále je v kapitole 2.3.2 uvedena Matice rizik založená na STPA (STPA Informed Risk Matrix – SRM), kde jsou uvedeny taktéž základní informace a kroky

postupu hodnocení. Taktéž jsou v této kapitole uvedeny výhody této matice a popsána práce s maticí v rámci praktické části diplomové práce.

2.3.1 Standartní matice rizik

Standartní matice rizik je velmi rozšířeným nástrojem pro analýzu rizika, který se začleňuje do procesu managementu rizika. Analýza rizika je prováděna ve velkém množství odvětví, například v průmyslu, obraně, dopravě a dalších. Proto byla matice pro každé z těchto odvětví upravena, aby co nejlépe splňovala požadavky dané oblasti. Za standartní matici rizik používanou v civilním letectví je považována matice představená v dokumentu *ICAO Safety Management Manual Doc 9859* [34]. Protože ale v rámci této práce byla využita Matice rizik založená na STPA, která je odvozená z matice rizik upravené pro potřeby resortu obrany, bude zde popsána právě standartní matice rizik určená pro odvětví obrany (Tabulka 8).

Principem využití standartní matice rizik je ohodnocení každého z identifikovaných nebezpečí na škále pravděpodobnosti a závažnosti. Každá ze škál a hodnoty, kterých nabývají jsou přesně stanoveny právě v dokumentu *MIL – STD – 882E* [35]. Za zmínku ale stojí dvě možnosti ohodnocení pravděpodobnosti. Prvním přístupem ke stanovení pravděpodobnosti výskytu nebezpečí je kvantitativní přístup. Ten je založen na číselném ohodnocení pravděpodobnosti. Kvantitativní ohodnocení je tedy číslo, které vyjadřuje počet selhání dělený jednotkou času. Jako jednotka času může být využito například očekávané délky životnosti, počtu letových hodin atd. Tento přístup je autory preferován a měl by být využit, pokud to dostupná data a zkušenost analytika umožňují. Druhým přístupem je kvalitativní přístup. To je přístup, kdy je pravděpodobnost hodnocena pomocí 6-bodové stupnice, kdy každý element má stanovenou pravděpodobnost pomocí slovní definice. Na analytikovi je, aby vybral ohodnocení nejlépe vystihující danou pravděpodobnost. [35, 36]

Tabulka 8: Matice rizik MIL - STD - 882E. Upraveno z [35]

Matice rizik				
Závažnost Pravděpodobnost	Katastrofická (1)	Kritická (2)	Okrajová (3)	Zanedbatelná (4)
Častá (A)	Vysoké	Vysoké	Závažné	Střední
Pravděpodobná (B)	Vysoké	Vysoké	Závažné	Střední
Občasná (C)	Vysoké	Závažné	Střední	Nízké
Mizivá (D)	Závažné	Střední	Střední	Nízké
Nepravděpodobná (E)	Střední	Střední	Střední	Nízké
Eliminovaná (F)	Eliminováno			

2.3.2 Matice rizik založená na STPA

Matice rizik založená na STPA (STPA Informed Risk Matrix – SRM) je modifikací vytvořenou v rámci diplomové práce *A System-Theoretic Approach to Risk Analysis* [36], která využívá standartní matici rizik MIL – STD – 882E (Tabulka 8). Přestože, jak již bylo zmíněno výše v textu, se jedná o matici vytvořenou pro potřeby resortu obrany, sami autoři stanovili, že je tento nástroj vhodný pro využití mimo odvětví obrany a že jeho použití mimo toto odvětví nemá žádné limitace. [36]

SRM je vytvořená tak, aby umožňovala zhodnocení rizika z výstupů analýzy STPA. Metodika obsahuje dva možné přístupy, jak dojít k zhodnocení rizika, a to přístup založený na ztrátových (kauzálních) scénářích a přístup založený na nebezpečí. [36]

Hlavní odlišností od standartní matice rizik MIL – STD – 882E je princip práce s pravděpodobností. V rámci SRM je stanovena nová veličina, nazvaná Škála účinnosti zmírnění (Mitigation Effectiveness Score – MES). Díky této veličině je pak možné se oprostit od klasického určování pravděpodobnosti, kdy daný jev nastane a je možné

přímo zmírňovat riziko. MES nabývá 5 možných hodnot (Tabulka 9), které odpovídají Úrovni zmírnění (Mitigation level). Za povšimnutí stojí, že v popisu zmírnění je využíváno termínu kauzální faktor. Důvodem je, že v rámci přístupu založeném na ztrátových scénářích je riziko identifikováno právě ze ztrátových (kauzálních) scénářů. V případě přístupu založeném na nebezpečí je tento termín nahrazen sub – nebezpečím. [36]

Tabulka 9: Škála účinnosti zmírnění. Upraveno z [36]

Úroveň zmírnění	Popis zmírnění	Škála účinnosti zmírnění
Eliminováno	Kauzální faktory mohou být eliminovány přes design nebo vhodnou kombinací zmírnění níže	ELIM
Snížení designovým řešením	Výskyt kauzálních faktorů může být omezen nebo kontrolován skrze design	3
Odhalení s reakcí	Kauzální faktor může být odhalen a pro zmírnění musí být provedena akce	2
Trénink a procedury	Kauzální faktor může být zmírněn dodatečným výcvikem a procedurami	1
Žádná	Žádné zmírnění neexistuje nebo není využito	0

Dále je v matici využíváno Kombinované škály účinnosti zmírnění (Combined Mitigation Effectiveness Score – CMES). Právě CMES je v SRM náhradou za standartní stanovení pravděpodobnosti. Tato veličina udává důsledek kombinace jednotlivých zmírnění. Při určování CMES je však nutné brát v potaz několik předpokladů. Nejdůležitějším z nich je, že aplikace více zmírnění se stejnou hodnotou nemá kvantitativní dopad na konečné CMES. V rámci určování zmírnění je tak důležitější kvalita, nikoliv kvantita. Přestože několik zmírnění stejné úrovně má jistě ve výsledku pozitivní dopad, snahou kvantifikace těchto zmírnění je možné se dostat na úroveň pouhého číselného odhadu pravděpodobnosti. V ideálním případě jsou tedy na každý kauzální faktor aplikovány všechny úrovně zmírnění (1–3). Hodnota CMES je pak vypočítána jako součet unikátních hodnot Škály účinnosti zmírnění. Další předpoklady jsou uvedeny v dokumentu. [36]

Druhou hodnotou, jako je tomu i v rámci standartní matice rizik je závažnost. V kontextu SRM je závažnost rozdělena na Závažnost před zmírněním (Pre – Mitigation Severity – PMS) a Potenciální závažnost po zmírnění (Post – Potential Mitigation Severity – PPMS). Obě veličiny využívají standartní škály závažnosti. Nejdříve se stanovuje PMS, což je hodnota závažnosti rizika před aplikací jakéhokoliv zmírnění. Následně je stanovena PPMS, která zhodnocuje dopad jednotlivých zmírnění na závažnost. A konečně Kombinovaná potenciální závažnost po zmírnění (Combined Post – Potential Mitigation Severity – CPMS). Výpočet CPMS je uveden v rovnici níže. Jedinou výjimkou pro výpočet CPMS je, že pokud je riziko eliminováno (ELIM ve sloupci MES), CPMS odpovídá hodnotě 4, nezávisle na ostatních hodnotách PPMS. Následně jsou pak získané hodnoty CMES a CPMS zaneseny do tabulky SRM (Tabulka 10). [36]

$$Pro\ N = počet\ zmírnění$$

$$CPMS = \frac{\sum_1^N PPMS}{N}\ (zaokrouhlit\ dolů\ na\ nejbližší\ celé\ číslo) \quad (1)$$

Tabulka 10: Matice rizik založená na STPA. Upraveno z [36]

Všechny ztrátové (kauzální) scénáře					
Minimálně [A]	0				
Trochu [B]	1				
Přiměřeně [C]	2-3				
Velmi [D]	4-5				
Mimořádně [E]	6				
Eliminováno [F]	N/A				
CMES		1	2	3	4
	CPMS	katastrofická	Kritická	Okrajová	Zanedbatelná

2.3.2.1 Využití SRM

V rámci této práce bylo rozhodnuto pro využití SRM kvůli specifikaci bezpečnostních doporučení. Po dokončení analýzy STPA je tedy nutné stanovit bezpečnostní doporučení pro provoz tak, aby byla zachována či zlepšena úroveň bezpečnosti systému eMCO vůči současnému provozu.

SRM je svojí využitelností v návaznosti na STPA pak ideálním nástrojem pro zhodnocení a kategorizaci rizika. Dalším důvodem podporujícím využití této matice je již zmiňovaná absence stanovení pravděpodobnosti. Protože stanovení pravděpodobnosti je velmi závislé na odbornosti analytika a dostupných datech, byla nahrazením toho kroku do jisté míry zajištěna objektivita vykonané analýzy. V grafické podobě je pak možné si lépe vizualizovat jednotlivá rizika a odvození bezpečnostních doporučení je taktéž jednodušší a objektivnější. SRM byla tedy využita pro stanovení bezpečnostních doporučení v rámci každé iterace analýzy STPA.

2.3.2.2 Přístup k SRM

Jak již bylo zmíněno nahoře v textu, existují dva rozdílné přístupy ke kvantifikaci a prioritizaci výsledků STPA. V rámci této práce byl využit, z důvodů uvedených níže v textu, pouze přístup založený na ztrátových (kauzálních) scénářích, proto zde bude popsán pouze tento přístup.

Možnost přímého využití ztrátových (kauzálních) scénářů pro sestavení SRM existuje díky samotné struktuře ztrátových scénářů. Standartní matice rizik využívá ke stanovení rizika logiku „pokud – pak“, kterou je možné interpretovat i do ztrátových scénářů. Definice ztrátových scénářů je: „Popis kauzálních faktorů, které mohou vést k nebezpečné řídící akci a nebezpečí“. Pokud se pak využije logika uvedená výše, kauzální faktory odpovídají části „pokud“ a nebezpečí části „pak“. Díky tomu je možné ztrátové scénáře přímo využít v rámci zhodnocení rizika. [36]

Značnou výhodou tohoto přístupu je využívání samotných scénářů. Díky nim je totiž možné zachytit riziko mnohem více komplexně než u jiných přístupů. Je totiž možné zachytit i rizika, která vznikají interakcí mezi jednotlivými prvky systému. Analýza tak není omezená pouze na spolehlivost jednotlivých prvků. To umožňuje identifikace rizik,

která by mohla zůstat bez povšimnutí a poté, v rámci provozu, způsobit nedozírné následky. [36]

3 Výsledky

V této části práce jsou uvedeny jednotlivé výsledky získané v rámci praktické části práce. Kapitola 3.1 obsahuje výsledky práce, které byly získány ještě před započetím samotné analýzy STPA. Kapitola 3.2 pak obsahuje výsledky metody STPA, které jsou rozděleny na několik částí. V kapitole 3.2.1 jsou uvedeny výsledky 1. iterace analýzy, v kapitole 3.2.2 výsledky 2. iterace s vyspělým automatizačním systémem na palubě, v kapitole 3.2.3 výsledky 2. iterace s pozemním členem týmu nahrazujícím druhého pilota, a nakonec v kapitole výsledky 2. iterace se složitým distribuovaným týmem.

3.1 Práce předcházející analýzu STPA

Jak již bylo zmíněno v metodické části práce, systém eMCO je posuzován dle moderních postupů bezpečnostního inženýrství popsaných v publikaci *Engineering a Safer World* [30]. Před samotnou analýzou STPA bylo tedy provedeno ještě několik dalších kroků, jejichž výsledky jsou v této části prezentovány.

Prvním krokem bylo stanovení cíle, kterého by měl posuzovaný systém dosáhnout. Cíl systému byl zvolen autorem a formulován jako:

Let v hladině s jedním pilotem v kokpitu.

Pro stanovení cíle bylo využito i tendru EASA pro zhotovení bezpečnostní studie pro systém eMCO, který již byl v rámci této práce zmíněn. Přestože autor nebyl vybrán pro zhodnocení bezpečnosti v rámci tendru, snaží se v rámci této práce o nezávislé posouzení s výsledky prezentovanými dříve než v případě tendru. Většina výsledků tendru pak navíc nebude veřejně přístupná.

Dalším krokem bylo stanovení omezení, jak může být cíle dosaženo. V tomto kroku byly identifikovány zúčastněné subjekty, ze kterých pak vychází identifikace nepřijatelných ztrát (Tabulka 11). V rámci bezpečnostních analýz je pak běžnou praxí stanovení zúčastněných subjektů, které poté identifikují z jejich perspektivy nepřijatelné ztráty a ty jsou zapracovány do studie. V případě této práce ale byla identifikace zúčastněných

subjektů i nepřijatelných ztrát provedena autorem. Pod pojmem regulační orgán je pak možné si představit subjekt zajišťující dohled nad civilním letectvím z pohledu bezpečnosti. Tento subjekt je v rámci studie kritický, protože jeho požadavek je pro provoz letecké dopravy nejdůležitější a není možné bez splnění tohoto požadavku systém provozovat.

Tabulka 11: Identifikované nepřijatelné ztráty

Zúčastněný subjekt – cíl	Nepřijatelná ztráta
Regulační orgán – udržení úrovně bezpečnosti	Z1: Zranění nebo smrt člověka
	Z2: Poškození nebo zničení letadla

Dále bylo v tomto kroku identifikováno systémové nebezpečí. To bylo pro zachování abstrakce a splnění požadavku na systémovost formulováno následovně:

Letadlo není řízeno v rámci letu eMCO.

Poté následovalo určení bezpečnostních a ostatních omezení systému. Pro systém eMCO byla identifikována následující bezpečnostní systémová omezení (BO):

BO1: Letadlo musí být řízeno v rámci letu eMCO

a ostatní systémová omezení (OSO):

OSO1: Fáze letu v hladině musí být v jakýkoliv okamžik zvládnutelná pouze jedním pilotem

OSO2: Ekologičnost provozu musí být na vyšší nebo stejné úrovni, jak je tomu v současnosti

OSO3: Celková ekonomická náročnost projektu musí být přijatelná

Zde je také vhodné okomentovat původ těchto omezení, zvláště pak OSO2. Zbylé 2 omezení plynou přímo z konceptu SiPO/eMCO a jeho reálné využitelnosti v provozu. OSO2 je pak odvozeno ze zásad EASA v oblasti vývoje nových systémů v letectví.

Dalším krokem pak bylo zvolení architektury systému. V tomto případě bylo rozhodováno na základě dostupných informací o systému a stavu implementace systému do reálného provozu. Protože analyzovaný systém nemá konkrétní designová řešení a zatím existuje pouze ve formě návrhu, bylo zvoleno využití předběžné analýzy nebezpečí (Preliminary hazard analysis). Zde je vhodné taktéž podotknout, že výsledky prezentované do tohoto bodu jsou takzvaně systémové, což znamená, že se vztahují na analyzovaný systém jako celek, a tudíž se v rámci iterací nemění. Tyto výsledky jsou tedy společné pro všechny iterace a koncepty. Avšak v rámci každé bezpečnostní analýzy bylo ověřeno, zda jsou dané výsledky platné.

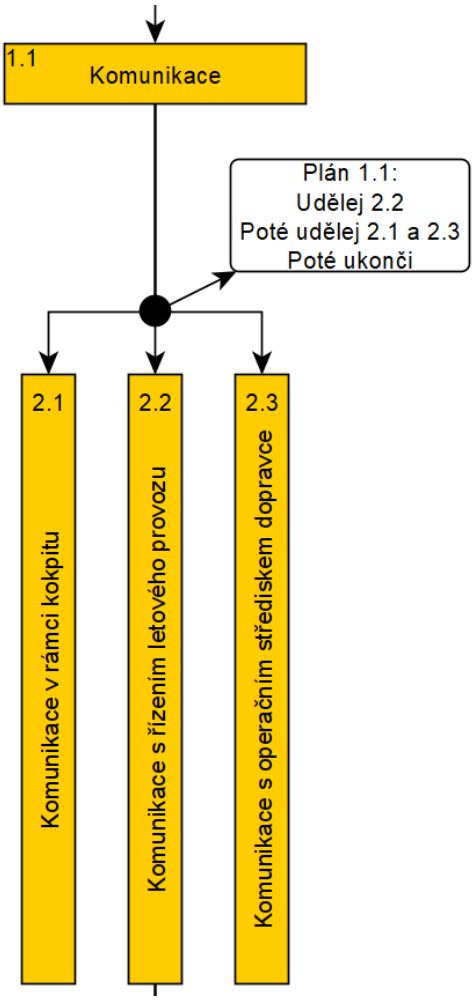
Po určení architektury systému byly stanoveny environmentální předpoklady pro analyzovaný systém. Ty byly stanoveny na základě znalosti systému autorem a navázány na jednotlivé iterace. Předpoklady se v rámci iterací liší, a to především kvůli různé míře abstrakce a kvůli jednotlivým konceptům, se kterými se uvažovalo. Ilustrace environmentálních předpokladů pro první iteraci je uvedena níže (Tabulka 12), kompletní seznamy předpokladů všech analýz jsou pak uvedeny v rámci přílohy 1. Je vhodné také uvést, že v rámci environmentálních předpokladů je uvedeno i několik předpokladů týkajících se samotného systému. Tyto předpoklady se nachází ve spodní části a jsou napsány kurzívou. Díky stanovení environmentálních předpokladů pak bylo možné si lépe představit systém jako součást provozu a dále s ním pracovat. Dále je možné díky předpokladům například i stanovit rozsah následujících prací, například omezením se na určité situace. Toho bylo využito i v rámci této práce, kdy bylo autorem stanoveno omezení pouze na normální provoz, viz jeden z předpokladů. Nouzové situace byly tedy vyloučeny. Toto rozhodnutí bylo učiněno především kvůli rozsahu práce, kdy by obsažení těchto situací rozsah práce zněkolikanásobilo.

Tabulka 12: Ilustrace environmentálních předpokladů

Environmentální předpoklady 1. iterace
Koncept provozu není k dispozici ve fázi první iterace
Okolní provoz tvořen letadly v režimu eMCO i letadly ve standartním režimu
Absence stanovení konkrétních přístrojů v systému
Analýza se týká pouze normálního provozu, nebere v potaz zvláštní situace

Jak již bylo zmíněno, koncept provozu nebyl v rámci první iterace k dispozici, tudíž bylo využito a nadále pracováno s abstraktním modelem obchodní letecké dopravy, který zahrnuje všechny potřebné vazby. Tento model byl vytvořen autorem na základě obecné znalosti obchodní letecké dopravy. Model je pak prezentován v rámci výsledků analýzy STPA.

Následovalo vykonání předběžné analýzy úkolů operátora. K tomuto úkolu byla zvolena Hierarchická analýza úkolů, a to z důvodů zmíněných v metodické části práce. Výsledkem je pak hierarchický model zobrazující úkoly operátora, jehož ilustrativní část je uvedena na Obrázek 10. Analýza byla provedena na základě elementárního leteckého pravidla stanovujícího úkoly pilota za letu (Letět, navigovat, komunikovat). Toto pravidlo bylo pak upraveno pro potřeby letu v hladině, kdy navigace ve smyslu ladění pozemních zařízení a dalších činností v podstatě neprobíhá a byla tedy nahrazena činností monitorování. Monitorování letu je totiž nejvýraznější částí každého letu v hladině. Jednotlivé úkoly potřebné ke splnění cíle na vyšší úrovni pak byly prioritizovány a zaznamenány v rámci plánů pomocí jednoduché výrokové logiky analýzy. Kompletní analýza včetně textové části je uvedena v rámci Přílohy 2. Analýza HTA byla taktéž využívána v rámci všech iterací.



Obrázek 10: Ilustrativní část HTA

3.2 Výsledky bezpečnostní analýzy

V této podkapitole jsou prezentovány výsledky získané pomocí STPA a navazujících metod v rámci jednotlivých iterací a navrhovaných provozních řešení. Prezentované výsledky v této části nemusí být kompletní. Kompletní výsledky jsou uvedeny v rámci příloh a to následovně. Výsledky první iterace jsou obsahem Přílohy 3, druhé iterace s vyspělým automatizačním systémem na palubě jsou v rámci Přílohy 4, druhé iterace s pozemním členem týmu nahrazujícím druhého pilota jsou uvedeny v Příloze 5 a výsledky druhé iterace s podporou složitého distribuovaného týmu se nachází v Příloze 6.

3.2.1 1. iterace

V rámci prvního kroku STPA bylo provedeno zhodnocení nepřijatelných ztrát a systémových nebezpečí, která byla stanovena v práci předcházející analýzu. K ověření bylo využito také diagramu zobrazujícího hranice analyzovaného systému (Obrázek 11). Bylo stanoveno, že ztráty a nebezpečí odpovídají potřebám práce, a tudíž byly tyto výsledky využity. Pouze došlo ke změně zápisu, aby výsledky odpovídaly syntaxi STPA. Výstupem prvního kroku analýzy jsou tedy ztráty:

Z1: Zranění nebo smrt člověka

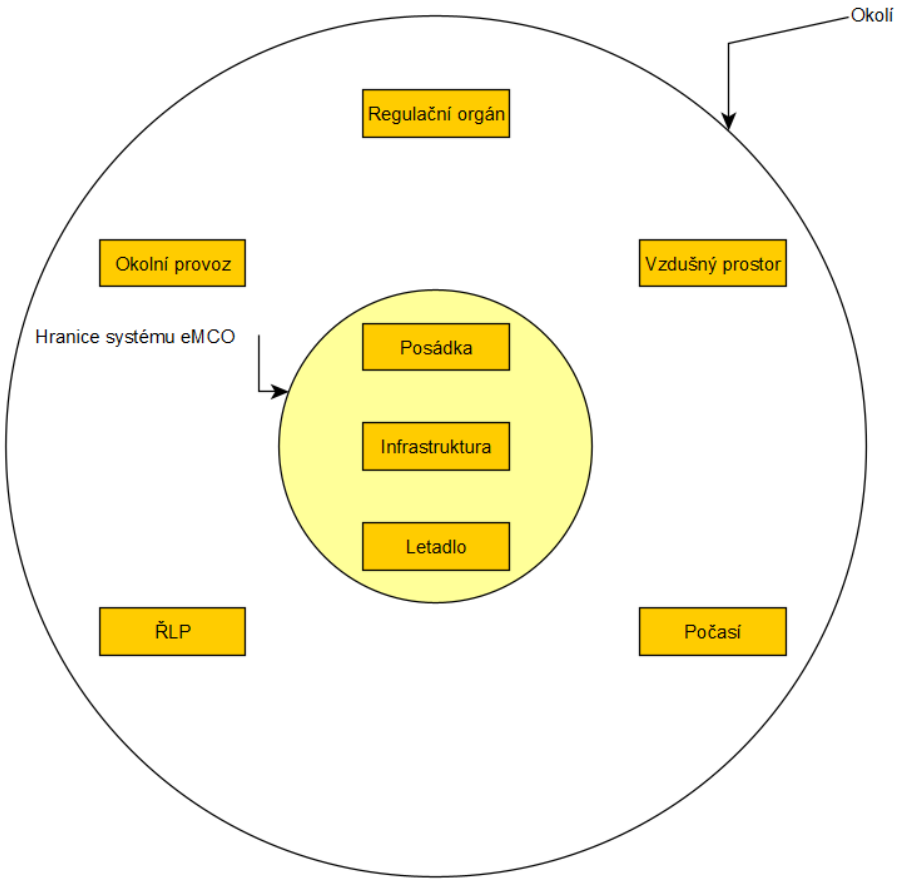
Z2: Poškození nebo zničení letadla

a stanovená systémová nebezpečí:

SN1: Letadlo není řízeno v rámci letu eMCO [Z1, Z2]

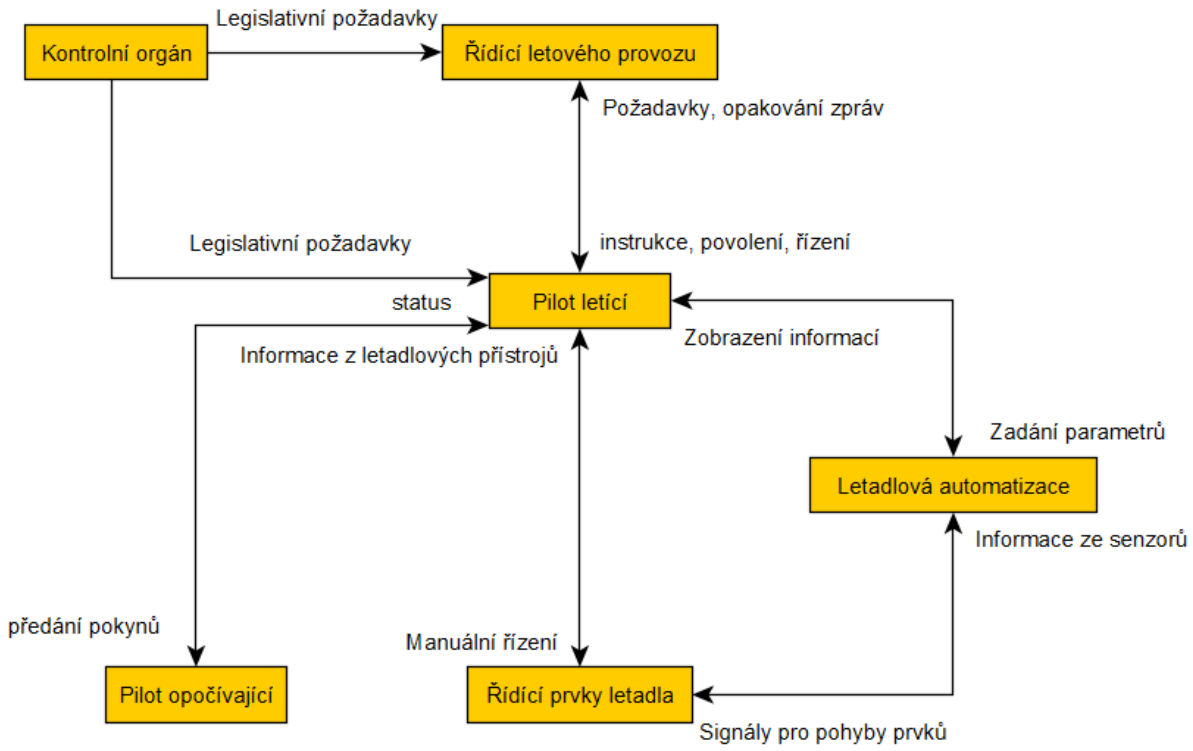
a následně odvozená systémová bezpečnostní omezení:

BO1: Letadlo musí být řízeno v rámci letu eMCO [SN1]



Obrázek 11: Diagram hranice systému

Dalším krokem bylo vytvoření modelu struktury řízení (Obrázek 12). Model vychází ze získaných informací o systému a ze stanovených environmentálních předpokladů. Stěžejním bylo v rámci první iterace zachování vysoké míry abstrakce, aby na ni mohly být navázány iterace další. Dostatečná míra abstrakce pak byla zajištěna absencí jakéhokoliv konceptu provozu a konkrétních letadlových systémů. Model pak připomíná spíše klasický dvoupilotní provoz pouze s rozdělením pilotů na letícího a odpočívajícího a vytváří tak prostor pro konkretizaci v rámci dalších iterací. Za zmínku také stojí vazba mezi letadlovou automatizací a řídícími prvky letadla. V tomto případě se jedná o vazbu typu aktuátor – řízený proces, tudíž se z této vazby neodvozují nebezpečné řídící akce.



Obrázek 12: Řídící struktura 1. iterace

Následně pak byly v souladu s principy STPA stanoveny nebezpečné řídící akce, které vychází ze struktury řízení. V této iteraci bylo stanoveno 10 nebezpečných řídících akcí. Ilustrace je uvedena v Tabulka 13. Z nebezpečných řídících akcí pak byly formulovány omezení řídících prvků podle syntaxe STPA. Vygenerovaná omezení pak mají následující charakter:

O1: Pilot musí manuálně řídit, pokud je autopilot vypnutý [NŘA1]

O2: Pilot musí manuálně řídit letadlo na požadované úrovni [NŘA2]

Tabulka 13: Ilustrace nebezpečných řídících akcí. 1. iterace

Řídící akce	Neprovedení způsobuje nebezpečí	Provedení způsobuje nebezpečí	Příliš brzy, příliš pozdě, ve špatném pořadí	Ukončení příliš brzy, aplikování příliš dlouho

Manuální řízení	NŘA1: Pilot manuálně neřídí, když autopilot je vypnutý [SN1]	NŘA2: Pilot manuálně řídí letadlo, avšak na nižší než požadované úrovni [SN1]		
Zadávání parametrů	NŘA3: Pilot nezadá parametry, když je to potřeba [SN1]	NŘA4: Pilot zadá chybné parametry [SN1]		

Finálním krokem STPA bylo stanovení ztrátových scénářů. Ty byly generovány v souladu se všemi dostupnými informacemi a stanovenými předpoklady. Pro nebezpečné řídící akce této iterace bylo vygenerováno 19 ztrátových scénářů. Příkladem mohou být ztrátové scénáře nebezpečné řídící akce 1, které jsou:

ZS1: Při letu v hladině může letadlo vlétnout do turbulence, následkem které dojde k odpojení autopilota, čehož si pilot, který je přetížen nemusí všimnout [NŘA1]

ZS2: Při letu může dojít ke zvýšení pracovního zatížení na pilota, který s přesvědčením, že ovládá jiné systémy letadla, odpojí autopilota a následnou signalizaci zamění za jinou [NŘA1].

3.2.1.1 SRM

Po dokončení STPA bylo pro stanovení bezpečnostních doporučení využito SRM. V rámci SRM bylo identifikováno několik desítek navrhovaných zmírnění, která tvoří jádro SRM. Jednalo se o stanovení již stávajících zmírnění i o identifikaci nových zmírnění. Stávající zmírnění jsou uvedena v matici, protože závažnost jednotlivých scénářů je hodnocena v situaci bez jakéhokoliv zmírnění, tudíž i bez zmírnění, která jsou v dnešní době již implementována. Ilustrace části s ohodnocením jednotlivých scénářů je uvedena v Tabulka 14.

Tabulka 14: Ilustrace ohodnocení scénářů. 1. iterace

Ztrátový scénář	PMS	NZ ID	Navrhované zmírnění	MES	CMES	PPMS	CPMS
ZS1	1	NZ01	Schopnost autopilota řídit letadlo v turbulenci	3	6	4	1
		NZ02	Indikace odpojení autopilota	2		1	
		NZ03	Schopnost predikování turbulence	2		1	
		NZ04	Zajištění schopnosti křížové kontroly a případné upozornění	2		1	
		NZ05	Školení pilotů v oblasti rozložení pozornosti při letu	1		1	

Po ohodnocení jednotlivých scénářů na škálách CMES a CPMS je pak možné scénáře promítnout do Matice rizik založené na STPA. Výsledná matice rizik je uvedena v Tabulka 15. Je nutné podotknout, že dané scénáře jsou v matici rizik zobrazeny již po aplikaci navrhovaných zmírnění. Za povšimnutí pak stojí ZS16. V případě tohoto scénáře se v rámci matice rizik založené na STPA nepodařilo stanovit dostatek zmírnění pro přesun z oranžové zóny. Avšak díky uplatnění principů popsaných v rámci metodické části práce bylo dostatečné úrovně bezpečnosti zajištěno vyšším počtem zmírnění v jednotlivých MES.

Tabulka 15: Výsledná matice rizik založená na STPA. 1. iterace

Všechny ztrátové (kauzální) scénáře					
Minimálně [A]	0				
Trochu [B]	1				
Přiměřeně [C]	2-3			ZS8, ZS15	
Velmi [D]	4-5	ZS16	ZS6, ZS10, ZS11	ZS12	ZS14
Mimořádně [E]	6	ZS1, ZS9	ZS1, ZS2, ZS4, ZS5, ZS7		
Eliminováno [F]	N/A	ZS3, ZS13, ZS17, ZS18, ZS19			
CMES		1	2	3	4
	CPMS	katastrofická	Kritická	Okrajová	Zanedbatelná

Z matice a předem odvedené práce bylo pak možné stanovit jednotlivá bezpečnostní doporučení vztahující se na systém. V rámci stanovování bylo nutné dbát na přesnou a výstižnou formulaci jednotlivých doporučení, aby nemohlo dojít k jinému výkladu. Dalším důležitým aspektem stanovování bylo zachování požadované míry abstrakce, aby odpovídala abstrakci celého systému. V neposlední řadě bylo nutné uvědomění si funkce autora, jakožto bezpečnostního inženýra a neobsahovat v rámci bezpečnostních doporučení, jak jich bude dosaženo, nýbrž jen čeho by mělo být dosaženo. Výsledná bezpečnostní doporučení jsou pak platná i pro následující iterace, kde může docházet k jejich specifikaci. V první iteraci bylo stanoveno 9 bezpečnostních doporučení, která jsou uvedena v Seznam 1.

Seznam 1: Bezpečnostní doporučení 1. iterace

Bezpečnostní doporučení
•Snížení pracovního zatížení na pilota automatizací vhodných úkonů •Zajištění způsobu validace úkonů prováděných na palubě letadla v režimu eMCO •Zajištění dostatečné materiálové podpory (kontrolní seznamy, operační postupy atd.) pro posádky v režimu eMCO •Zajištění vyšší úrovně audiovizuální komunikace mezi letadlem a posádkou, než je nynějším standardem •Zajištění dostatečných kapacit a efektivity systému řízení letového provozu •Zajištění jednoznačné odpovědnosti za provedené činnosti a nadřazenosti pilota letícího nad odpočívajícím pilotem v režimu eMCO •Zajištění efektivního a jednoznačného způsobu komunikace mezi pilotem letícím a pilotem odpočívajícím •Zajištění jednoznačné a správné legislativní základny •Udržení informovanosti všech zainteresovaných subjektů

Zde je vhodné také podotknout, že výsledky první iterace byly zhodnoceny a na jejich základě bylo rozhodnuto o obsahu následující iterace. V rámci teoretické části bylo zmíněno několik možných konceptů provozu. Avšak zde, po získání výsledků, je možné některé z nich vyloučit. Prvním konceptem, který byl vyloučen je koncept, kdy je pouze odebrán druhý pilot, který je popsán v kapitole 1.1.2. Toto rozhodnutí bylo učiněno na základě bezpečnostních doporučení první iterace, které jasně stanovují dodatečné akce pro zajištění bezpečnosti. Druhým vyloučeným konceptem je i ten popsaný v kapitole 1.1.3. V tomto případě tak bylo rozhodnuto také na základě bezpečnostních doporučení, ale především na základě ostatních systémových omezení, zvláště pak OSO3, kdy tato možnost počítá s výcvikem palubního personálu na úroveň pilota, což je v rozporu s tímto omezením.

3.2.2 2. iterace – pilot a vyspělý automatizační systém na palubě

Dalším krokem práce bylo zhotovení druhé iterace analýzy na jednotlivé vhodné koncepty provozu. Kompletní výsledky popsané v této kapitole jsou pak uvedeny v rámci přílohy 4. Jak již bylo zmíněno dříve cílem 2. iterace je zpřesnění iterace první a konkretizování jejich výsledků. Systémové výsledky se nemění, protože se jedná o stále stejný systém. Což znamená, že úvodní kroky metody STPA byly převzaty z 1. iterace

a pouze posouzeny, zda – li postačují pro tuto iteraci. Po posouzení byly tedy znovu použity tyto systémové výsledky:

Z1: Zranění nebo smrt člověka

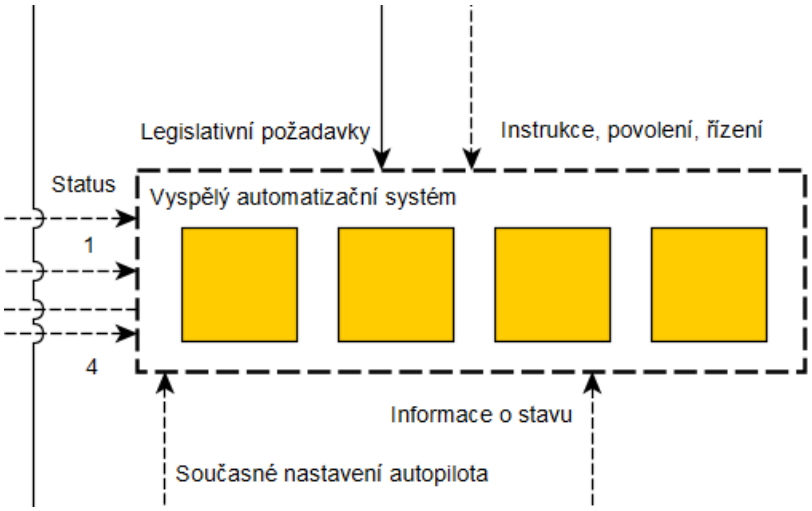
Z2: Poškození nebo zničení letadla

SN1: Letadlo není řízeno v rámci letu eMCO [Z1, Z2]

BO1: Letadlo musí být řízeno v rámci eMCO [SN1]

Poté byla zkompletována řídící struktura. Ke stanovení řídící struktury bylo využito dostupné literatury, avšak ne všechny vazby systému již byly popsány. Tudíž se v rámci řídící struktury objevují vazby, které byly stanoveny na základě úsudku autora s ohledem na funkčnost celého systému. Tyto vazby jsou pak v rámci struktury vyznačeny čárkovaně. Oproti první iteraci došlo ke zpřesnění modelu v částech, které byly autorem vyhodnoceny jako stěžejní, což ostatně bylo i cílem druhé iterace.

Za zmínku stojí také samotný vyspělý automatizační systém. Ten v době tvorby analýzy nebyl nijak definován. Tudíž se autor rozhodl pro zobrazení vyspělého automatizačního systému jako abstraktního subsystému. To znamená, že se v rámci struktury neobjevují jednotlivé komponenty subsystému, ale subsystém interaguje s okolím jako celek. V pozdějších fázích vývoje pak bude možné tento subsystém dospecifikovat. Abstraktní subsystém je v rámci struktury ohraničen přerušovanou čarou (Obrázek 13). Taktéž bylo autorem rozhodnuto o poloze vyspělého automatizačního systému v rámci struktury. Po zhodnocení povahy subsystému, principu možné činnosti a dalších faktorů bylo rozhodnuto, že subsystém bude autoritou pod pilotem a nad letadlem. A to především z důvodu, že vyspělý automatizační systém by měl sloužit jako podpora pro pilota, tudíž s nižší autoritou a zároveň by měl být schopen ovlivnit ostatní systémy letadla. Za zmínku také stojí stanovení vztahu mezi systémem managementu letu a automatizací. V tomto případě bylo na základě podobných faktorů jako výše rozhodnuto o vztahu podřízenosti systému managementu letu vůči vyspělému automatizačnímu systému.



Obrázek 13: Zobrazení vyspělého automatizačního systému v rámci řídící struktury

Po stanovení řídící struktury byly identifikovány nebezpečné řídící akce. V tomto kroku stojí za komentář hned několik věcí. Samotné stanovování NŘA již bylo prováděno v souladu s první iterací. Tudíž NŘA, které byly shodné v obou iteracích již ve druhé iteraci nejsou zaznamenány.

Dále byly v rámci struktury identifikovány vazby typu aktuátor – řízený proces. Například ve vazbě mezi systémem managementu letu a autopilotem. Zásadní bylo v těchto případech uvědomění, zdali prvek aktivně řídí, či pouze slouží jako databáze pro poskytování informací.

V neposlední řadě je nutné zmínit řídící akci: *Změna frekvence, výběr aktivního komunikačního zařízení*. Stanovení této řídící akce totiž vedlo k nutnosti odvození nového systémového dílčího nebezpečí. Toto je krok, který metoda STPA umožňuje a je velkou výhodou této metody. Odvozené nebezpečné řídící akce totiž v tomto případě nevedou přímo na systémové nebezpečí. Tudíž bylo v rámci této řídící akce odvozeno dílčí nebezpečí podřízené již stanovenému nebezpečí. Toto nebezpečí bylo definováno jako:

SN1.1: Letadlo není ve spojení v rámci letu eMCO

Dále pak bylo z dílčího nebezpečí odvozeno bezpečnostní omezení:

BO1.1: Letadlo musí být ve spojení v rámci letu eMCO

Po zhodnocení veškerých vazeb bylo tedy v rámci struktury identifikováno 24 nebezpečných řídících akcí (Tabulka 16).

Tabulka 16: Ilustrace nebezpečných řídících akcí. 2. iterace – vyspělý automatizační systém

Řídící akce	Neprovedení způsobuje nebezpečí	Provedení způsobuje nebezpečí	Příliš brzy, příliš pozdě, ve špatném pořadí	Ukončení příliš brzy, aplikování příliš dlouho
Zadávání parametrů	NŘA1: Vyspělý automatizační systém nezadává parametry, přestože je to vyžadováno [SN1]	NŘA2: Vyspělý automatizační systém zadá parametry, které neodpovídají požadavkům [SN1]	NŘA3: Vyspělý automatizační systém zadává parametry do nesprávných atributů letu [SN1]	

Z každé nebezpečné řídící akce bylo následně vygenerováno omezení řídících prvků. Jejich ilustrace je níže:

O1: Vyspělý automatizační systém musí zadávat parametry, pokud je to vyžadováno [NŘA1]

O2: Vyspělý automatizační systém musí zadat parametry, které odpovídají požadavkům [NŘA2]

O3: Vyspělý automatizační systém musí zadávat parametry do správných atributů letu [NŘA3]

Na základě nebezpečných řídících akcí pak byly generovány ztrátové scénáře. V rámci této iterace bylo vygenerováno 38 scénářů. Ilustrace je uvedena níže:

ZS1: Automatizační systém trpí designovou chybou, která vyvstane za určitých předpokladů [NŘA1]

ZS2: V rámci letu dojde k výboji elektrické energie, například následkem úderu bleskem, což způsobí nesprávnou funkčnost softwaru [NŘA1]

3.2.2.1 SRM

Následně byly jednotlivé ztrátové scénáře ohodnoceny na škálách PMS, MES, CMES, PPMS a CPMS, jako tomu bylo v případě 1. iterace. Ilustrace ohodnocení scénáře je uvedena v Tabulka 17.

Tabulka 17: ilustrace ohodnocení ztrátových scénářů. 2. iterace – vyspělý automatizační systém

Ztrátový scénář	PMS	NZ ID	Navrhované zmírnění	MES	CMES	PPMS	CPMS
ZS1	2	NZ01	Vybavení záložním systémem jiné architektury	3	6	4	3
		NZ02	Rozsáhlé testování systému	2		2	
		NZ03	Schopnost pilota odhalit chybu softwaru a adekvátně reagovat	1		3	

Po ohodnocení scénářů následovalo zobrazení scénářů v matici rizik (Tabulka 18).

Tabulka 18: Výsledná matice rizik založená na STPA. 2. iterace – vyspělý automatizační systém

Všechny ztrátové (kauzální) scénáře					
Minimálně [A]	0				
Trochu [B]	1				
Přiměřeně [C]	2-3				
Velmi [D]	4-5		ZS18, ZS31	ZS2, ZS3, ZS16, ZS17,	ZS23

				ZS33, ZS34, ZS36, ZS38	
Mimořádně [E]	6		ZS9, ZS30	ZS1, ZS4, ZS5, ZS12, ZS13, ZS14, ZS15, ZS32, ZS35, ZS37	ZS24, ZS28, ZS29
Eliminováno [F]	N/A	ZS6, ZS7, ZS8, ZS10, ZS11, ZS19, ZS20, ZS21, ZS22, ZS25, ZS26, ZS27			
CMES		1	2	3	4
	CPMS	katastrofická	Kritická	Okrajová	Zanedbatelná

Po zhodnocení komplexních výsledků práce v 2. iteraci pro vyspělý automatizační systém pak bylo stanoveno 12 bezpečnostních doporučení (Seznam 2). Zde je nutné podotknout, že platí taktéž bezpečnostní doporučení první iterace. Za komentář pak stojí bezpečnostní doporučení: *Zajištění aktivit pro pilota tak, aby byla udržena minimální úroveň pozornosti.* Toto doporučení vychází z několika scénářů a jeví se jako zásadní pro zajištění bezpečnosti provozu. V rámci tohoto konceptu totiž nemá pilot letící k dispozici nikoho v pilotní kabině, kdo by mu mohl dělat společnost v případě velmi nízkého vytížení. Tato role by pak musela být přiřazena s největší pravděpodobností právě vyspělému automatizačnímu systému. Protože se jedná o velice zajímavou myšlenku, autor ji věnoval nějaký čas, přestože návrh konkrétních řešení není cílem této práce. Z pohledu autora tak připadá v úvahu například periodické provádění činností požadovaných vyspělým automatizačním systémem. Tím je myšleno, že automatizační systém rozpozná situaci a pilotovi zadá úkoly, například propočet paliva, projití plánované tratě a další činnosti pro udržení míry pozornosti.

Seznam 2: Bezpečnostní doporučení. 2. iterace – vyspělý automatizační systém

Bezpečnostní doporučení
•Zajištění redundance a schopnosti fungování vyspělého automatizačního systému ze záložních zdrojů •Zajištění spolehlivosti vykonání úkolů definovaných pro automatizaci •Zajištění, v rámci designu systému, znalosti vyspělého automatizačního systému veškerých možných kombinací vstupů od operátora •Zajištění, v rámci designu systému, schopnosti vyspělého automatizačního systému správně reagovat na kritické situace z pohledu bezpečnosti •Zajištění co nevyšší míry shodnosti vyspělého automatizačního systému se současnou logikou automatizace a vykonávání úkonů na palubě •Zajištění schopnosti vyspělého automatizačního systému oboustranné komunikace na několika úrovních, minimálně pak na hlasové a datové úrovni •Jednoznačné definování úkolů vyspělého automatizačního systému, které se v rámci eMCO nemění •Zajištění vhodného rozhraní mezi pilotem a vyspělým automatizačním systémem pro snadné ovládání ve stížených podmínkách •Zajištění absolutní znalosti vyspělého automatizačního systému piloty a řídícími letového provozu •Zajištění minimálního růstu povinností pro řídící letového provozu •Zajištění, že posádky létající eMCO vnímají automatizaci na palubě pozitivně •Zajištění aktivit pro pilota tak, aby byla udržena minimální úroveň pozornosti

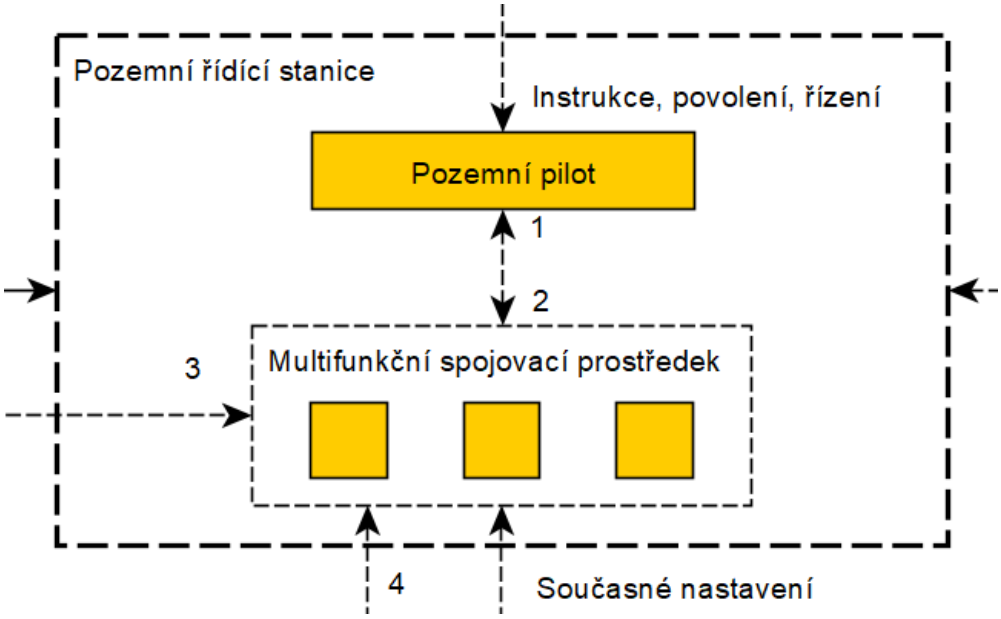
3.2.3 2. iterace – pozemní člen týmu nahrazující druhého pilota

Dalším zhodnoceným konceptem byl koncept pilota a pozemního člena týmu nahrazujícího druhého pilota. Stejně tak jako tomu bylo v předchozích případech i nyní zde bude popsána pouze část výsledků. Kompletní výsledky této kapitoly jsou uvedeny v příloze 5. Analýza tohoto konceptu byla zhotovena jak na základě 1. iterace, tak ale byla použita i již vykonaná varianta 2. iterace.

Princip analýzy byl stejný jako v případě předchozích. Tudíž prvním krokem bylo zhodnocení systémových výsledků, zda – li jsou vhodné. Po zhodnocení byly tedy stanoveny ztráty, systémová nebezpečí, bezpečnostní omezení a ostatní systémová omezení shodné s první iterací.

Dalším krokem pak bylo stanovení řídící struktury. V tomto případě autor vycházel především z již hotové 2. iterace s vyspělým automatizačním systémem. Řídící struktura byla předělána tak, aby odpovídala konceptu provozu. Za zmínku stojí samotná pozemní

řídící stanice. Stejně jako tomu bylo i u vyspělého automatizačního systému, není prozatím jasně stanovený design ani princip fungování tohoto prvku. Tudíž byla pozemní stanice popsána s jistou mírou abstrakce (Obrázek 14). Taktéž byly na základě zajištění fungování systému stanoveny autorem některé vazby. Ty jsou ve struktuře zobrazeny přerušovanou čarou. Zde je nutné taktéž podotknout, že se v rámci řídící struktury objevují vazby, které jsou shodné s předchozími iteracemi. Tyto vazby již nejsou obsahem analýzy, především z důvodu snížení rozsahu.



Obrázek 14: Zobrazení pozemní řídící stanice v rámci řídící struktury

Dalším krokem analýzy bylo stanovení nebezpečných řídících akcí. V tomto případě bylo stanoveno 11 unikátních nebezpečných řídících akcí. Za zmínku stojí, že v případě pozemní řídící stanice byly všechny nebezpečné řídící akce odvozeny z vazby mezi pozemním pilotem a multifunkčním spojovacím prostředkem. Autorem totiž bylo stanoveno, že vazby mezi spojovacím prostředkem a dalšími prvky systému jsou již pouze vazby pro přenos informace, nikoliv řídící akce. Ilustrace nebezpečných řídících akcí je uvedena v Tabulka 19.

Tabulka 19: Ilustrace nebezpečných řídících akcí. 2. iterace – pozemní člen týmu

Řídící akce	Neprovedení způsobuje nebezpečí	Provedení způsobuje nebezpečí	Příliš brzy, příliš pozdě, ve špatném pořadí	Ukončení příliš brzy, aplikování příliš dlouho
Instrukce (obsahuje instrukce, povolení, řízení)	NŘA1: Řídící pozemnímu pilotovi nepředá instrukce, když je to žádoucí [SN1]	NŘA2: Řídící předá pozemnímu pilotovi instrukce, jejichž vykonání v daný okamžik způsobí nebezpečí [SN1]		

Po stanovení nebezpečných řídících akcí bylo provedeno odvození omezení řídících prvků, jejichž ilustrace je uvedena níže:

O1: Řídící musí pozemnímu pilotovi předat instrukce, pokud je to žádoucí [NŘA1]

O2: Řídící nesmí pozemnímu pilotovi předat instrukce, jejichž vykonání způsobí v daný okamžik nebezpečí [NŘA2]

Poté již následovalo generování ztrátových scénářů. V tomto případě bylo vygenerováno 23 scénářů. Ilustrace je uvedena zde:

ZS1: Řídící je vytížený řízením ostatního provozu a opomene své povinnosti vůči zájmovému letadlu [NŘA1]

ZS2: V rámci provozu nastane situace, kdy řídící neví, z důvodu neznalosti systému, že má danou informaci poskytnout pozemnímu pilotovi [NŘA1]

3.2.3.1 SRM

Následně byly výstupy analýzy, a to ztrátové scénáře, STPA zhodnocena dle metody SRM. Ilustrace ohodnocení je uvedena v Tabulka 20.

Tabulka 20: Ilustrace zhodnocení ztrátových scénářů. 2. iterace – pozemní člen týmu jako druhý pilot

Ztrátový scénář	PMS	NZ ID	Navrhované zmírnění	MES	CMES	PPMS	CPMS
ZS1	2	NZ01	Vhodná sektorizace vzdušného provozu	3	6	2	2
		NZ02	Detekce a upozornění řídícího ohledně povinností vůči letadlu	2		3	
		NZ03	Procedury ohledně žádostí pilota o asistenci	1		2	
		NZ04	Výcvik řídících v oblasti rozložení pozornosti	1		2	

Následně byly scénáře vyneseny do matice rizik založené na STPA (Tabulka 21). Taktéž v tomto případě se podařilo všechny scénáře přesunout do žluté zóny. Což v rámci SRM znamená přijatelné riziko.

Tabulka 21: Výsledná matice rizik založená na STPA. 2. iterace – pozemní člen týmu nahrazující druhého pilota

Všechny ztrátové (kauzální) scénáře					
Minimálně [A]	0				
Trochu [B]	1				
Přiměřeně [C]	2-3				
Velmi [D]	4-5		ZS9, ZS12, ZS13, ZS14,	ZS10, ZS15,	

			ZS16, ZS20, ZS21, ZS22, ZS23	ZS18, ZS19	
Mimořádně [E]	6	ZS6	ZS1, ZS3, ZS4, ZS8, ZS17	ZS5	
Eliminováno [F]	N/A	ZS2, ZS7, ZS11			
CMES		1	2	3	4
	CPMS	katastrofická	Kritická	Okrajová	Zanedbatelná

Ze získaných výsledků dosavadní práce pak byly stanoveny bezpečnostní požadavky. V rámci tohoto konceptu bylo stanoveno 11 unikátních bezpečnostních doporučení pro zachování úrovně bezpečnosti (Seznam 3). Zde je vhodné podotknout, že je nutné brát v potaz jak bezpečnostní požadavky stanovené v rámci první iterace, tak i v rámci druhé iterace s vyspělým automatizačním systémem na palubě.

Seznam 3: Bezpečnostní doporučení. 2. iterace – pozemní člen týmu jako náhrada druhého pilota

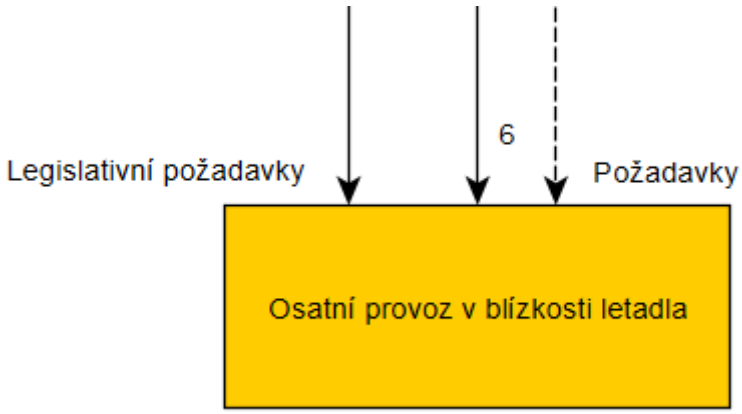
Bezpečnostní doporučení

- Zajištění co možná nejnižšího nárustu požadavků na řídící letového provozu
- Zajištění kontroly a validace úkonů prováděných na pozemním stanovišti
- Zajištění vhodného rozhraní mezi pozemním pilotem a letadlem pro efektivní a jednoduchou interakci
- Jednoznačné stanovení využití verbální komunikace mezi piloty
- Jednoznačné určení úkonů, které je možné provádět z pozemní stanice
- Zajištění, že pozemní pilot má přesné informace o činnostech pilota v letadle a naopak
- Zajištění, že počet letadel v kompetenci pozemní stanice bude v každé situaci zvládnutelný
- Zajištění rovnoměrného rozložení pozornosti pozemního pilota mezi letadla v kompetenci
- Zajištění jednoznačného způsobu identifikace (ke stávajícím způsobům) letadel v kompetenci
- Zajištění schopnosti multifunkčního komunikačního prostředku prioritizace požadavků
- Zajištění, v rámci multifunkčního komunikační prostředku, jednoznačného zobrazení prioritních zpráv

3.2.4 2. iterace – pilot s podporou složitého distribuovaného týmu

Posledním analyzovaným konceptem byla varianta s pilotem s podporou složitého distribuovaného týmu. V rámci prvního kroku STPA byly znovu využity výsledky 1. iterace, které zde již nebudou prezentovány.

Druhým úkolem bylo stanovení řídící struktury. V tomto kroku bylo učiněno několik důležitých rozhodnutí. Řídící struktura je založena na řídící struktuře 2. iterace s vyspělým automatizačním systémem, protože navrhovaný koncept taktéž počítá s dodatečným automatizačním systémem na palubě. Koncept taktéž obsahuje pozemní stanici, avšak v této práci byl ze systému vyloučen. Pozemní stanice totiž v rámci tohoto konceptu je centralizovaná a funguje pouze pro asistenci při příletu a odletu z letiště. Vzhledem k tomu, že systém eMCO počítá pouze s jednopilotním letem v hladině, byl tento prvek systému autorem vyloučen. Tudíž řídící struktura je totožná se strukturou pro vyspělý automatizační systém, pouze s tím rozdílem, že v tomto konceptu dochází i ke spolupráci mezi jednotlivými letadly v prostoru (Obrázek 15). Tato spolupráce je pak převážně koordinačního charakteru, tudíž bližší specifikace v době tvorby práce nedávala smysl.



Obrázek 15: Zobrazení okolního provozu v rámci řídící struktury

Z řídící struktury byly následně stanoveny nebezpečné řídící akce. V tomto případě byly stanoveny 3 unikátní nebezpečné řídící akce (Tabulka 22). Počet stanovených NŘA je poměrně malý, a to především z důvodů zmíněných výše v textu a faktu, že tak jako tomu

bylo v předchozím konceptu, nebyly znovu zaznamenány řídící akce, které byly analyzovány v předešlé analýze.

Tabulka 22: Stanovené nebezpečné řídící akce. 2. – složitý distribuovaný systém

Řídící akce	Neprovedení způsobuje nebezpečí	Provedení způsobuje nebezpečí	Příliš brzy, příliš pozdě, ve špatném pořadí	Ukončení příliš brzy, aplikování příliš dlouho
Požadavky	NŘA1: Pilot letící nezadá požadavky na okolní provoz, když je to žádoucí [SN1]	NŘA2: Pilot letící zadá nesprávné požadavky na okolní provoz [SN1]		
		NŘA3: Pilot letící zadá takové požadavky (množství, kvalita) okolnímu provozu, že způsobí nebezpečí [SN1]		

Na základě NŘA pak byly vygenerována omezení řídících prvků, jejichž ilustrace je uvedena níže:

O1: Pilot letící musí zadat požadavky na okolní provoz, pokud je to žádoucí [NŘA1]

O2: Pilot letící musí zadat správné požadavky na okolní provoz [NŘA2]

Dalším krokem bylo stanovení ztrátových scénářů. V tomto případě bylo stanoveno 5 ztrátových scénářů, ilustrovaných níže:

ZS1: Pilot neví, na jaké komunikační úrovni se s letadlem spojit [NŘA1]

ZS2: Pilot si myslí, že je schopen danou situaci vyřešit sám a není mu třeba asistence [NŘA1]

3.2.4.1 SRM

Výsledky STPA pak byly zpracovány v rámci SRM. Ilustrace ohodnocení scénářů je uvedena v Tabulka 23.

Tabulka 23: Ilustrace ohodnocení ztrátových scénářů. 2. iterace – složitý distribuovaný systém

Ztrátový scénář	PMS	NZ ID	Navrhované zmírnění	MES	CMES	PPMS	CPMS
ZS1	2	NZ01	Automatické přednastavení vhodných frekvencí	3	4	2	2
		NZ02	Stanovení procedur v oblasti komunikace s okolním provozem	1		2	

Výsledky ohodnocení pak byly vyneseny do matice SRM (Tabulka 24). I v tomto případě se podařilo pomocí navrhovaných zmírnění přesunout všechny ztrátové scénáře do žluté, z hlediska bezpečnosti přijatelné, části matice.

Tabulka 24: Výsledná matice rizik založená na STPA. 2. iterace – složitý distribuovaný systém

Všechny ztrátové (kauzální) scénáře					
Minimálně [A]	0				
Trochu [B]	1				
Přiměřeně [C]	2-3				
Velmi [D]	4-5		ZS1, ZS3, ZS4		
Mimořádně [E]	6		ZS2, ZS5		
Eliminováno [F]	N/A				
CMES		1	2	3	4
	CPMS	katastrofická	Kritická	Okrajová	Zanedbatelná

Poté byly na základě výsledků stanoveny 2 unikátní doporučení pro bezpečnou implementaci (Seznam 4). Tak jako tomu bylo v předešlých případech, je nutné brát v potaz bezpečnostní doporučení stanovená v rámci 1. iterace a 2. iterace s vyspělým automatizačním systémem.

Seznam 4: Bezpečnostní doporučení. 2. iterace – pilot s podporou složitého distribuovaného týmu

Bezpečnostní doporučení
•Zajištění, že požadavky na okolní provoz jsou jasně definovány, co se týče charakteru, množství a jejich využití •Zajištění, že proces asistence nevyústí v nebezpečí u asistujícího letadla

3.3 Diskuze výsledků

Cílem této diplomové práce bylo zhodnocení a stanovení bezpečnostních doporučení systému eMCO. Tohoto cíle bylo v rámci práce dosaženo a v této části jsou diskutovány jednotlivé výsledky.

Samotnou bezpečnostní analýzu však předcházelo několik neméně důležitých kroků v souladu s publikací *Engineering a Safer World* [30], která byla využívána v průběhu celé praktické části. Tyto kroky a jejich výsledky dopomohly k jasnému vymezení a pochopení systému autorem. Za komentář stojí využití Hierarchické analýzy úkolů operátora. Této analýzy bylo využito pro vizualizaci práce v kokpitu při letu v hladině a taktéž sloužila jako kontrolní vstup do následné analýzy STPA. Na základě Hierarchické analýzy úkolů operátora byla totiž možná zpětná kontrola, zda – li nebyly opomenuty některé vazby v rámci řídící struktury STPA. Zde je nutné podotknout, že v rámci této analýzy byla zachována jistá míra abstrakce, nikoliv však kvůli nedostatku dostupných informací, nýbrž kvůli navazujícím činnostem, které nevyžadovaly konkretizaci. Validitu této analýzy úkolů lze stanovit na základě dostupných pramenů, které se touto problematikou již zabývaly. Mezi ně patří například *Commercial Airline Single-Pilot Operations: System Design and Pathways to Certification* [37]. Ze srovnání je možné stanovit, že obě provedené analýzy se svými výsledky ve značné části shodují a tudíž je možné považovat provedenou analýzu za validní.

Následujícím významným krokem bylo provedení bezpečnostní analýzy. Vhodná metoda byla zvolena z databáze metod [29] po slnění parametrů plynoucích ze systému a stavu jeho implementace do provozu. Tím byla zajištěna vhodnost dané metody. Po zvolení metody bylo rozhodnuto k rozdělení práce s metodou na iterace, což metoda STPA umožňuje. Díky iteračnímu rozdělení bylo zajištěno, že nebudou opomenuty některé části systému, jako by k tomu mohlo dojít při snaze bezpečnostního posouzení v rámci jedné iterace. V rámci druhé iterace pak bylo provedeno zhodnocení v rámci jednotlivých vhodných konceptů. Jako vhodné koncepty k posouzení byly vybrány ty, které byly v souladu s bezpečnostními doporučeními a systémovými výsledky 1. iterace analýzy. Na tomto základě byly vyloučeny varianta, kde je počítáno pouze s odstraněním druhého pilota bez náhrady a varianta, která počítá s náhradou druhého pilota členem

palubního personálu. Jednotlivé analýzy pak byly vykonány v souladu s příručkou *STPA Handbook* [31].

Dále bylo využito matice rizik založené na STPA. Tento krok byl vykonán kvůli, z pohledu autora, jednoduššímu stanovování bezpečnostních doporučení, a to především díky vizualizaci jednotlivých scénářů v matici rizik a nutnosti stanovení zmírňujících opatření. Matice rizik založená na STPA byla z ostatních matic rizik vybrána kvůli faktu, že je přímo vázána na analýzu STPA a taktéž absentuje stanovování pravděpodobnosti, což je veličina, která je z pohledu autora velice závislá na dostupných datech a subjektivním vnímaní analytika. To má pak negativní dopad na objektivitu výsledků. Využitím SRM byla tedy zajištěna objektivita při zhodnocení rizika jednotlivých scénářů. Celý proces SRM byl vykonán na základě publikace *A System-Theoretic Approach to Risk Analysis* [36], která poskytuje podrobný popis postupu.

Na základě výstupů z prací popsaných v předešlých odstavcích byla stanovena bezpečnostní doporučení, což bylo cílem této práce. Možnosti validace na základě porovnání jsou však v současné době omezené z důvodu absence studie bezpečnosti zabývající se stejnou problematikou. Jedinou vhodnou možností bylo kontaktování autorů některé z publikací, což by vyžadovalo přeložení práce do anglického jazyka s nejistou zpětnou vazbou, proto byl tento krok s ohledem na časovou náročnost a prioritu vykonání vlastní studie vynechán. V dohledné době však bude možné využít výsledky zadaného tendru EASA na tuto problematiku. Ovšem za předpokladu, že budou výsledky zveřejněny. V současné době je tak možné pouze validovat postup vykonání studie, který byl popsán v textu výše a na tomto základu stanovit validitu práce. Protože byla práce vykonána v souladu se systémovou teorií a dle moderních a ověřených metod bezpečnosti, které jsou vhodné pro použití v tomto odvětví a na tento typ problémů, je možné tvrdit, že výsledky práce jsou validní.

Z výsledků získaných z jednotlivých analýz je pak možné stanovit, že při dodržení prezentovaných bezpečnostních doporučení jsou všechny analyzované koncepty bezpečné pro implementaci do provozu. Zde je nutné podotknout, že toto tvrzení platí pro současný stav a omezení práce. V rámci dalšího designu a specifikace systému je pak nutné brát v potaz aktuální bezpečnostní doporučení.

Na tuto práci by pak bylo vhodné navázat dalšími studiemi v souladu s vývojem, konkretizací a odhalováním nových trendů tohoto systému. Jako navrhovaný cíl konkretizace je v rámci přílohy 7 uvedena analýza úkolů operátora pro ovládání autopilota přes panel Glareshield. Jedná se pouze o zlomek úkolů, které pilot v rámci letu v hladině plní a slouží pouze pro vizualizaci míry konkretizace, do které je nutné se dostat pro komplexní zhodnocení bezpečnosti. Schéma je založeno na kokpitu letounu Airbus A350. Konkrétní design kokpitu však může být v budoucnu rozdílný, tudíž toto schéma nelze brát jako závazné.

Mezi jednotlivými analyzovanými koncepty pak bylo identifikováno několik faktorů, které poukazují na vhodnost využití daného konceptu. Jako nejvhodnější se v současné době jeví koncept s využitím vyspělého automatizačního systému. A to z tohoto důvodu. V této variantě se totiž nevyskytují dodatečné nebezpečné řídící akce ze vztahu člověk -> člověk. Ty byly z pohledu autora v rámci vyhodnocování a zmírňování nejnáročnější na zpracování, tudíž i jejich reálná implementace může být komplikovaná. Většina nebezpečných řídících akcí je pak spojená se samotným automatizačním systémem. V tomto případě je pak bezpečná implementace závislá převážně na technické vyspělosti daných systémů. Tudíž pokud je techniky a ekonomicky možné systém s takovýmito požadavky zkonstruovat, jeví se tato varianta jako nejjednodušší pro zajištění bezpečnosti. Avšak v rámci dalších prací může dojít k identifikaci požadavků, které vyspělý automatizační systém nebude schopen splnit a od této varianty se bude muset upustit.

4 Závěr

Tato diplomová práce se zabývá zhodnocením bezpečnosti systému eMCO. Cílem práce bylo stanovení bezpečnostní doporučení a zhodnocení bezpečnosti systému eMCO. K dosažení cíle bylo nejdříve nutné zhodnotit současný stav problematiky, to jak z pohledu automatizace v letectví, tak z pohledu snižování počtu pilotů v kokpitu. Na základě zhodnocení současného stavu byly vybrány metody ke zhodnocení bezpečnosti vhodné pro tento systém a jeho vývojovou fázi. Tyto metody, konkrétně HTA, STPA

a SRM pak byly využity ke stanovení bezpečnostních doporučení a následnému zhodnocení bezpečnosti. Výsledky práce pak byly validovány dle dostupných možností.

Již zmíněná validace je limitací této práce, protože výsledky práce nebyly validovány v potřebném rozsahu, a tak nemůže být jejich správnost jednoznačně zaručena. Dalším limitem této práce je určitě její rozsah. Práce totiž analyzuje pouze normální provoz a neuvažuje nouzové či jiné zvláštní situace. Asi největší limitací této práce je fakt, že zhodnocení bezpečnosti bylo provedeno v rané fázi vývoje systému, kdy jsou k dispozici pouze koncepty a návrhy systému, nikoliv technická řešení. Tudíž se může následující vývoj ubírat k rozdílným, novým, technickým řešením, což může mít výrazný vliv na další posouzení z pohledu bezpečnosti. S tím se pojí i fakt, že při dodatečné specifikaci systému by mělo dojít k revalidaci studie a jejich výsledků.

Přínosem práce je určitě samotné provedení studie bezpečnosti. Dle dostupných informací se totiž v současné době jedná o jedinou práci, která se zabývá touto problematikou. Tudíž může sloužit jako základní práce pro ty následující. Díky této práci je také možné již v rané části vývoje stanovit bezpečnostní požadavky, které je nutné do systému zakomponovat. Tyto informace, v tak raném stádiu vývoje, mohou výrazně snížit či dokonce eliminovat ekonomické dopady zásahů do systému v pozdějších fázích vývoje a zajistit vyšší úroveň bezpečnosti v rámci celého vývoje a implementace systému.

V rámci budoucích prací by bylo vhodné dokončit tuto práci zahrnutím nouzových a jiných zvláštních situací do analýzy. Dále pak na tuto práci navázat dalšími studiemi v souladu s vývojem, konkretizací a odhalováním nových trendů tohoto systému. Jako navrhovaný cíl konkretizace je v rámci přílohy 7 uvedena analýza úkolů operátora pro ovládání autopilota přes panel Glareshield. Jedná se pouze o zlomek úkolů, které pilot v rámci letu v hladině plní a slouží pouze pro vizualizaci míry konkretizace, do které je nutné se dostat pro komplexní zhodnocení bezpečnosti. Schéma je založeno na kokpitu letounu Airbus A350. Konkrétní design kokpitu však může být v budoucnu rozdílný, tudíž toto schéma nelze brát jako závazné.

Zdroje

[1] KAJTMAN, Jan a Vlastimil MELICHAR. DEREGULACE A LIBERALIZACE LETECKÉ DOPRAVY. nedatováno.

[2] C-121C Super Constellation. *Air Mobility Command Museum* [online]. [vid. 2023-04-27]. Dostupné z: http://amcmuseum.org/at-the-museum/aircraft/c-121c-constellation/

[3] *Cockpit_of_a_Lockheed_L-1049_G_Super_Constellation_(D-ALEM).JPG (3663×2680)* [online]. [vid. 2023-04-27]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/2/29/Cockpit_of_a_Lockheed_L-1049_G_Super_Constellation_%28D-ALEM%29.JPG

[4] Heritage Concorde. *heritage-concorde* [online]. [vid. 2023-04-27]. Dostupné z: https://www.heritageconcorde.com

[5] *ConcordeCockpitSinsheim.jpg (2272×1704)* [online]. [vid. 2023-04-27]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/8/8c/ConcordeCockpitSinsheim.jpg

[6] *Cockpits | Airbus* [online]. 16. červen 2021 [vid. 2023-04-27]. Dostupné z: https://www.airbus.com/en/products-services/commercial-aircraft/cockpits

[7] *VIDEO: Airbus A350-1000 British Airways I Cockpit Tour | flyRosta.com* [online]. [vid. 2023-04-27]. Dostupné z: https://flyrosta.com/ba-a350-cockpit-tour/

[8] EASA Automation Policy: Bridging design and training principles. 2013.

[9] *Optimum_Use_Of_Automation_1.pdf* [online]. [vid. 2023-04-27]. Dostupné z: https://www.smartcockpit.com/docs/Optimum_Use_Of_Automation_1.pdf

[10] *Airbus concludes ATTOL with fully autonomous flight tests | Airbus* [online]. 28. říjen 2021 [vid. 2023-04-27]. Dostupné z: https://www.airbus.com/en/newsroom/press-releases/2020-06-airbus-concludes-attol-with-fully-autonomous-flight-tests

[11] *Is autonomy the future of aerial mobility? | Airbus* [online]. 10. září 2021 [vid. 2023-04-27]. Dostupné z: https://www.airbus.com/en/newsroom/stories/2020-01-is-autonomy-the-future-of-aerial-mobility

[12] *Could the humble dragonfly help pilots during flight? | Airbus* [online]. 6. leden 2023 [vid. 2023-04-27]. Dostupné z: https://www.airbus.com/en/newsroom/stories/2023-01-could-the-humble-dragonfly-help-pilots-during-flight

[13] ADMINISTRATOR, Aurora. Advanced and Unmanned Aircraft. *Aurora Flight Sciences* [online]. [vid. 2023-04-27]. Dostupné z: https://www.aurora.aero/advanced-and-unmanned-aircraft/

[14] CHIALASTRI, Antonio. Automation in aviation. In: Florian KONGOLI, ed. *Automation* [online]. B.m.: InTech, 2012 [vid. 2023-04-27]. ISBN 978-953-51-0685-2. Dostupné z: doi:10.5772/49949

[15] EVJEMO, Tor Erik a S. JOHNSEN. Lessons Learned from Increased Automation in Aviation: The Paradox Related to the High Degree of Safety and Implications for Future Research. In: [online]. 2019, s. 3076–3083. Dostupné z: doi:10.3850/978-981-11-2724-3_0925-cd

[16] VU, Kim-Phuong L., Joel LACHTER, Vernol BATTISTE a Thomas Z. STRYBEL. Single Pilot Operations in Domestic Commercial Aviation. *Human Factors* [online]. 2018, **60**(6), 755–762. ISSN 0018-7208. Dostupné z: doi:10.1177/0018720818791372

[17] MYERS, Paul L. a Arnold W. STARR. Single Pilot Operations IN Commercial Cockpits: Background, Challenges, and Options. *Journal of Intelligent & Robotic Systems* [online]. 2021, **102**(1), 19. ISSN 1573-0409. Dostupné z: doi:10.1007/s10846-021-01371-9

[18] HARRIS, Don, Neville A. STANTON a Alison STARR. Spot the difference: Operational event sequence diagrams as a formal method for work allocation in the development of single-pilot operations for commercial aircraft. *Ergonomics* [online]. 2015, **58**(11), 1773–1791. ISSN 0014-0139. Dostupné z: doi:10.1080/00140139.2015.1044574

[19] MOEHLE, Robert a Jason CLAUSS. Wearable Technologies as a Path to Single-Pilot Part 121 Operations. *SAE International Journal of Aerospace* [online]. 2015, **8**(1), 81–88. ISSN 1946-3855, 1946-3901. Dostupné z: doi:10.4271/2015-01-2440

[20] STANTON, Neville A., Don HARRIS a Alison STARR. The future flight deck: Modelling dual, single and distributed crewing options. *Applied Ergonomics* [online]. 2016, **53**, Transport in the 21st Century: The Application of Human Factors to Future User Needs, 331–342. ISSN 0003-6870. Dostupné z: doi:10.1016/j.apergo.2015.06.019

[21] SCHMID, Daniela a Neville A. STANTON. Progressing Toward Airliners' Reduced-Crew Operations: A Systematic Literature Review. *The International Journal of Aerospace Psychology* [online]. 2020, **30**(1–2), 1–24. ISSN 2472-1840. Dostupné z: doi:10.1080/24721840.2019.1696196

[22] eMCO-SiPO - Extended Minimum Crew Operations – Single Pilot Operations – Safety Risk Assessment Framework. *EASA* [online]. [vid. 2023-04-27]. Dostupné z: https://www.easa.europa.eu/en/research-projects/emco-sipo-extended-minimum-crew-operations-single-pilot-operations-safety-risk

[23] *The Human and the concepts of Extended Minimum Crew Operations and Single Pilot Operations* [online]. [vid. 2023-04-27]. Dostupné z: https://www.eurocockpit.be/positions-publications/human-and-concepts-extended-minimum-crew-operations-and-single-pilot

[24] BAILEY, Randall E., Lynda J. KRAMER, Kellie D. KENNEDY, Chad L. STEPHENS a Timothy J. ETHERINGTON. An assessment of reduced crew and single pilot operations in commercial transport aircraft operations. In: *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*: *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)* [online]. St. Petersburg, FL: IEEE, 2017, s. 1–15 [vid. 2023-04-27]. ISBN 978-1-5386-0365-9. Dostupné z: doi:10.1109/DASC.2017.8101988

[25] FLIGHTRADAR24. Live Flight Tracker - Real-Time Flight Tracker Map. *Flightradar24* [online]. [vid. 2023-04-27]. Dostupné z: https://www.flightradar24.com/data/flights/qf9

[26] *SimBrief - Dispatch* [online]. [vid. 2023-04-27]. Dostupné z: https://dispatch.simbrief.com/home

[27] *EASA FTL 2016: Flight and Duty Time Limitations and Rest Requirements* [online]. B.m.: EASA, Kolín nad Rýnem, Německo. 24. duben 2017. Dostupné z: https://understandingeasa2016ftl.files.wordpress.com/2017/04/easa-combined-ftl-2017.pdf

[28] CS FTL.1.205 Flight Duty Period (FDP). *Understanding EASA ORO.FTL 2016* [online]. 3. březen 2014 [vid. 2023-04-27]. Dostupné z: https://understandingeasa2016ftl.wordpress.com/easa-ftl/cs-ftl/cs-ftl-1-205-flight-duty-period-fdp/

[29] EVERDIJ, Mariken H C, Henk A P BLOM, Michael ALLOCCO, David BUSH, Mete ÇELIKTIN, Barry KIRWAN, Patrick MANA, Jochen MICKEL, Keith SLATER, Brian SMITH a Oliver STRÄTER. Safety Methods Database, Version 1.2. 2020.

[30] LEVESON, Nancy G. *Engineering a Safer World: Systems Thinking Applied to Safety* [online]. Massachusetts, USA: Aeronautics and Astronautics and Engineering Systems Division, Massachusetts Institute of Technology, 2012 [vid. 2023-04-27]. Dostupné z: doi:10.7551/mitpress/8179.001.0001

[31] LEVESON, Nancy a John THOMAS. STPA Handbook. 2018.

[32] SKŘEHOT, Petr. Hierarchical Task Analysis. nedatováno.

[33] STANTON, Neville. Hierarchical task analysis: Developments, applications, and extensions. *Applied ergonomics* [online]. 2006, **37**, 55–79. Dostupné z: doi:10.1016/j.apergo.2005.06.003

[34] *ICAO, Doc. 9859: Safety management manual, 4th Ed.* [online]. B.m.: Montréal, Quebec. 2018. Dostupné z: https://skybrary.aero/sites/default/files/bookshelf/5863.pdf

[35] *Standard practice, System safety, MIL-STD-882E* [online]. B.m.: Department of defence, Virginia, USA. 2012. Dostupné z: https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf

[36] GREGORIAN, Dro J a Sam M YOO. A System-Theoretic Approach to Risk Analysis. 2021.

[37] LIM, Yixiang, Vincent BASSIEN-CAPSA, Subramanian RAMASAMY, Jing LIU a Roberto SABATINI. Commercial Airline Single-Pilot Operations: System Design and Pathways to Certification. *IEEE Aerospace and Electronic Systems Magazine* [online]. 2017, **32**, 4–21. Dostupné z: doi:10.1109/MAES.2017.160175