ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Ověření hypotézy v modelu spojení znalosti ze safety studií s daty z provozu

Bakalářská práce

Studijní program: Technika a technologie v dopravě a spojích

Studijní obor: Profesionální pilot

Vedoucí práce: Ing. Markéta Šedivá Kafková
Ing. Slobodan Stojić, Ph.D

Viacheslav Yakovenko

Praha 2022

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

K621.....Ústav letecké dopravy

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Viacheslav Yakovenko

Studijní program (obor/specializace) studenta:

bakalářský –PIL– Profesionální pilot

Název tématu (česky): **Ověření hypotézy v modelu spojení znalosti ze safety studií s daty z provozu**

Název tématu (anglicky): **Hypothesis Verification Using the Model of Integrated Safety Knowledge**

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je komparace výsledků současného přístupu k vyhodnocování dat a vyhodnocení pomocí modelu integrace znalosti z bezpečnostních studií s daty o bezpečnosti z provozu se zaměřením na takové procesy, ve kterých je kontrolním prvkem člověk.
- Popište stávající způsoby řízení provozní bezpečnosti
- Popište model integrace znalosti z bezpečnostních studií s daty o bezpečnosti provozu
- Proveďte výběr a analýzu bezpečnostních informací z oblasti provozu letiště a navrhněte vlastní bezpečnostní hypotézy
- Vyberte a zpracujte vzorek dat
- Proveďte komparaci výsledků

ČVUT FD

Rozsah grafických prací: dle pokynů vedoucího bakalářské práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: ICAO, Doc. 9859: Safety Management Manual, 4th Edition, Montréal, Quebec, 2018.
Leveson, N., Thomas, J. STPA Handbook, 2018.
Dekker, S. The Field Guide to Understanding ´Human Error´. Ashgate, 2014.

Vedoucí bakalářské práce: **Ing. Markéta Šedivá Kafková**
Ing. Slobodan Stojić, Ph.D.

Datum zadání bakalářské práce: **8. října 2021**
(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 bakalářské práce: **8. srpna 2022**
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

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L. S.

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

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Viacheslav Yakovenko
jméno a podpis studenta

V Praze dne 8. října 2021

Poděkování

Děkuji vedoucí své práce za neustálé poskytování rad a konzultací při psaní této práce. Dále bych chtěl poděkovat společnosti inAero, konkrétně Pavlu Pačesovi a Pavlu Brodskému za poskytnutí simulátoru a dat z něj. V neposlední řadě chci poděkovat své rodině a přátelům, kteří mě celou dobu podporovali.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem „Ověření hypotézy v modelu spojení znalosti ze safety studií s daty z provozu“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské 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 8. srpna 2022 .....

Podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Ověření hypotézy v modelu spojení znalosti ze safety studií s daty z provozu

Bakalářská práce

srpen 2022

Viacheslav Yakovenko

Abstrakt

Tato práce řeší model integrace dat, jehož základem je aplikace metodiky Active STPA. Bude provedena simulace dat, aby bylo na jejich příkladu ilustrováno, jak přesně lze provést integraci dat pro každý krok Active STPA a ukáže se, jak datová integrace dokáže spustit tuto analýzu. Práce se zaměřuje na výběr takových procesů, ve kterých je řídícím prvkem člověk (provozní pracovník). Dále bude provedena analýza modelu integrace dat a porovnání výsledků současného přístupu a přístupu integračního na základě teoretické rešerše a analýzy výsledků.

Klíčová slova

STAMP, STPA, Active STPA, provozní bezpečnost, systém řízení bezpečnosti, prediktivní prístup, proaktivní přístup, přistání letadla, integrace dat.

CZECH TECHNICAL UNIVERSITY IN PRAGUT

Faculty of transportation sciences

Hypothesis Verification Using the Model of Integrated Safety Knowledge

Bachelor's thesis

August 2022

Viacheslav Yakovenko

Abstract

This work solves the data integration model, the basis of which is the application of the Active STPA methodology. A data simulation will be performed to exemplify exactly how data integration can be done for each step of Active STPA and to show how data integration can trigger this analysis. The work focuses on the selection of such processes in which the controlling element is a person (operational worker). Furthermore, an analysis of the data integration model and a comparison of the results of the current approach and the integrative approach will be carried out on the basis of theoretical research and analysis of the results.

Keywords

STAMP, STPA, Active STPA, operational safety, safety management system, predictive approach, proaktive approach, aircraft landing, data integration.

Obsah

Seznam použitých zkratek

A-1 – Assumption	Předpoklad
ADGS – Aircraft Docking Guidance System	Naváděcí systém pro dokování letadla
AGL – Above Ground Level	Nad úrovní terénu
AMSL – Above Mean Sea Level	Nad střední hladinou moře
ATC – Air Traffic Control	Řízení letového provozu
DME – Distance Measuring Equipment	Zařízení pro měření vzdálenosti
EASA – European Union Aviation Safety Agency	Agentura Evropské unie pro bezpečnost letectví
FNPT – Flight and Navigation Procedures Trainer	Trenér letových a navigačních postupů
FSTD – Flight Simulator Training Devices	Výcviková zařízení na letových simulátorech
GS – Ground speed	Pozemní rychlost
H-1 – Hazard	Nebezpečí
IAS – Indicated Airspeed	Indikovaná rychlost
ICAO – International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
ILS – Instrument Landing System	Přístrojový přistávací systém
L-1 – Loss	Ztráta
MCC – Multi Crew Cooperation	Výcvik vícečlenné posádky
MLW – Maximum Landing Weight	Maximální přistávací hmotnost
SC-1 – Safety constraint	Bezpečnostní omezení
SMM – Safety Management Manual	Manuál řízení bezpečnosti
SMS – Safety Management System	Systém řízení bezpečnosti
SSP – State Safety Programme	Státní bezpečnostní program

STAMP – Systems Theoretic Accident Modeling and Processes

	Systémové teoretické modelování nehod a procesy
STPA – System-Theoretic Process Analysis	Systémově teoretická procesní analýza
TAS – True Airspeed	Skutečná rychlost
UDP – User Data Protocol	Protokol uživatelských dat
UML – Unified Modeling Language	Unifikovaný Modelovací Jazyk
VHF - Very high frequency	Velmi krátké vlny
VKV - Velmi krátké vlny	
VOR - VHF Omnidirectional Radio Range	VKV všesměrový radiomaják

1 Úvod

Bezpečnost letového provozu je jedno z důležitých témat v letectví, Kontinuálně dochází k revizi stávajících a navrhování nových pravidel, pravidelně se konají konference pro podporu bezpečnosti a je věnována velká pozornosti a úsilí tomu, aby došlo k dosažení stanovených cílů. Přestože během historie letectví došlo k mnoho násobnému zvýšení bezpečnosti letů, pokračuje vládní Agentura Evropské unie pro bezpečnost letectví EASA ve vytváření nových plánů k podpoře zvýšení bezpečnosti letecké dopravy. [1] [2]

Hlavním cílem mé práce je porovnání dvou modelů k vyhodnocování dat: současného a vyhodnocení pomocí modelu integrace znalostí z bezpečnostních studií s daty o bezpečnosti z provozu. V práci se zaměřím na takové procesy, ve kterých je řídicím prvkem člověk – provozní pracovník.

Pro bezpečnost v letectví je samozřejmě důležité s každým nebezpečím předem pracovat a nereagovat na něj až poté, kdy způsobí nějakou škodu. Proto jsou v současné době v letectví hlavními přístupy prediktivní a proaktivní, a nikoli reaktivní, kde se nehoda musela nejprvé stát, a teprve potom se rozhodlo, jaké korekce pro zvýšení bezpečnosti zavést. Na vlastním příkladu využití dat dle metodiky integrace ukáži, jak může nový přístup podpořit proaktivní způsob analýzy dat a prediktivně pracovat se systémem pro zajištění bezpečnostních trendů.

Téma této bakalářské práce jsem si vybral s ohledem na můj zájem o analýzu dat, práci s nimi a vyvozování závěrů z těchto údajů. V práci bude provedena simulace dat, na jejichž základě bude provedena další analýza. Data budou generována pomocí programu X-plane; na základě těchto dat budou vytvořeny indikátory, které budou dále aplikovány jako způsob spuštění analýzy Active STPA.

2 Stávající způsoby řízení provozní bezpečnosti

Vysoká úroveň bezpečnosti v letectví je zajišťována pomocí systému řízení provozní bezpečnosti, tzv. Safety Management System, krátce SMS.

2.1 Systém řízení provozní bezpečnosti

Safety Management System je systematický přístup k řízení provozní bezpečnosti, zahrnující nezbytné organizační struktury, odpovědnosti, zásady a postupy pro řízení bezpečnosti. SMS se skládá z:

- Identifikace nebezpečí;
- procesu vývoje a prosazování pravidel pro udržení bezpečnosti na přijatelné úrovni;
- neustálého sledování a vyhodnocování úrovně bezpečnosti. [3] [4]

Safety Management System se skládá ze tří metod: proaktivní, prediktivní a reaktivní metody.

Reaktivní přístup řídí bezpečnost tak, že zavádí reakce na nežádoucí incidenty nebo události. Jedná se o jeden z nejjednodušších přístupů k provedení potřebných akcí, protože tyto akce se provádějí poté, co k události došlo a proto jsou již k dispozici všechna potřebná data. Významnou nevýhodou tohoto přístupu je, že k incidentu či nehodě musí nejprve dojít, než začněme přemýšlet o tom, co s tím můžeme udělat.

Proaktivní přístup se soustředí na řízení rizik v předstihu, tedy před realizací nežádoucí události. Zahrnuje vytváření manuálů, které mají pomoci vyhnout se chybám. Snahou při použití této metody je předvídat události, které se mohou stát a předvídat, co se děje v systému, na základě již známých dat a událostí. Například pokud vidíme, že se počet incidentů zvýšil, pak s tímto přístupem můžeme předejít možné nežádoucí události dříve, než k němu dojde.

Prediktivní přístup znamená hledání příčin poruchy, analýzu dat ze senzorů, řídících jednotek a dalších zdrojů dat, budování řetězce událostí, které mohou vést k nějakému incidentu. Predikce se realizuje ve využívání a analyzování dat, na jejichž základě můžeme vyvodit závěry o určitých oblastech bezpečnosti a aplikovat potřebná bezpečnostní opatření k jejich zlepšení.

2.1.1 ICAO Doc. 9859

ICAO Document 9859, nebo Safety Management Manuál (zkráceně SMM) je dokument vydaný Mezinárodní organizací pro civilní letectví ICAO. Jeho hlavním účelem je poskytovat pravidla

a doporučení pro zajištění a udržení požadované úrovně provozní bezpečnosti v organizaci. Mimo jiné prosazuje přechod na hodnocení provozní bezpečnosti založené na výkonu. [5]

Výhody řízení bezpečnosti jsou:

- Posílená kultura bezpečnosti;
- Rozhodování založené na bezpečnostních datech;
- Optimalizace prostředků;
- Úspora nákladů;
- Zvýšení příjmů.

2.1.2 Státní bezpečnostní program

Státní bezpečnostní program (State safety programme, zkráceně SSP) je integrovaný soubor předpisů a činností zaměřených na zlepšení bezpečnosti. Jde o systém řízení pro správu bezpečnosti státem. [6]

Každý stát má svůj vlastní bezpečnostní program, který je vytvořen v souladu se SMM tak, aby jak stát, tak i jednotlivé organizace, mohly sledovat úroveň bezpečnosti v různých směrech a stanovovat konkrétní cíle včetně časových rámců pro tyto cíle, analyzovat trendy a výsledky jejich práce a na základě těchto výsledků vyvodit závěry o přijatých opatřeních (ke zvýšení bezpečnosti). [5] [6]

Pojem provozní bezpečnost označuje stav, při kterém rizika spojená s leteckými činnostmi, které souvisejí s provozem letadel, jsou snížena a řízena na přijatelné úrovni.

SSP poskytuje prostředky pro kombinaci normativních postupů a přístupů založených na výkonu k:

1. Tvorbě bezpečnostních pravidel na základě analýz leteckých systémů;

2. Rozvoji bezpečnostní politiky na základě identifikace nebezpečí a řízení bezpečnostních rizik;

3. Bezpečnostnímu dohledu se zaměřením na oblasti významných bezpečnostních problémů nebo vyšších bezpečnostních rizik.

2.1.3 Současný přístup využití dat

Dle doporučení Safety Management Manuálu od ICAO je žádoucí přistupovat k rozhodování při řízení bezpečnosti na základě dat. [5] Kvalitní analýza dat nám poskytne relevatní obraz o aktuálním stavu úrovně provozní bezpečnosti v řízeném systému. Při řízení rizik se tak můžeme

informovaně rozhodovat a zajistit potřebnou rovnováhu mezi zajištěním bezpečného systému (ve smyslu zabránění ztrátám) a ekonomickým fungováním systému (ve smyslu zabránění bankrotu). Do tohoto pohledu přináší stanovení indikátorů bezpečnosti vymezení hranic bezpečnostního prostoru, v rámci kterého se snaží subjekt fungovat a zároveň včas indikovat možné překročení určených hranic.

Jak bylo řečeno, bezpečnostní indikátory poskytují obraz o reálném stavu bezpečnosti a při jasném definování jejich vazby na provozní postupy poskytují zpětnou vazbu o účinnosti zavedených zmírňujících opatření, či mohou poukázat na v systému se vyskytující provozní odchylku.

Dle SMM je předpokladem pro hladké zavedení indikátorů fungující systém řízení provozní bezpečnosti. Ten mimo jiné zajišťuje sběr dat v podobě výstupů z bezpečnostních auditů, výsledků inspekcí z provozu, výstupů z bezpečnostních průzkumů či záznamů z dobrovolného a povinného systému hlášení.

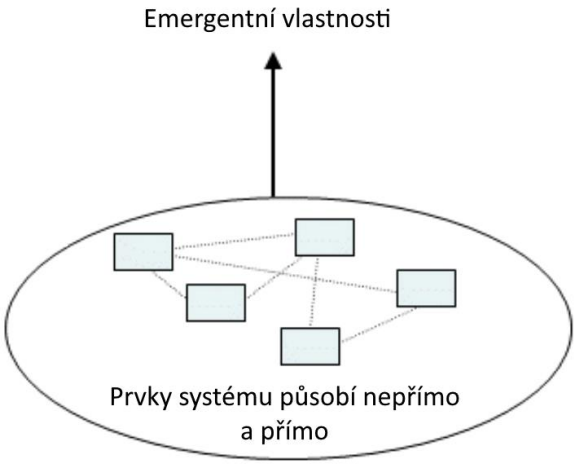
Indikátory se dle SMM dělí na reaktivní a proaktivní. Nejvýraznějším zástupcem a vhodným příkladem reaktivního indikátoru je počet leteckých nehod. Reaktivní indikátory reagují na realizaci nežádoucí události, tedy nabývají hodnot až po vzniku nehody nebo incidentu. Proaktivní indikátory slouží pro monitorování kritických míst provozních procesů ve smyslu předcházení potenciální nehodě. Proaktivní indikátory vyžadují zajištění dostatečného množství provozních dat.

2.2 Modely a metody analýzy dat a nehod

2.2.1 Systémová teorie

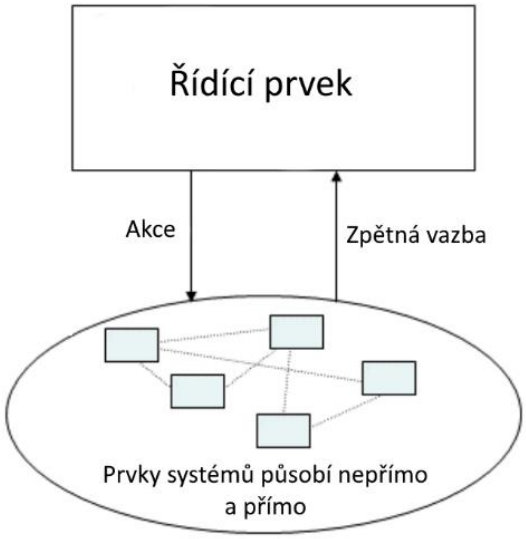
Systémová teorie byla vytvořena po druhé světové válce jako způsob, jak se vypořádat se složitějšími systémy, které se začaly objevovat. V takových systémech jsou prvky a jejich interakce odděleny pro jejich další analýzu, protože tyto prvky spolu mohou interagovat nejzřejmějšími způsoby. [8] [9]

Primárním zájmem jsou emergentní vlastnosti, což jsou vlastnosti, které nejsou v součtu jednotlivých složek, ale „projevují se“, když složky interagují. Mezi těmito vlastnostmi může být například bezpečnost, zabezpečení, udržitelnost a provozuschopnost (viz Obrázek 1).



Obrázek 1 - Vzhled emergentních vlastností [8]

Vzhledem k tomu, že tyto vlastnosti pocházejí z chování prvků a jejich interakce, má smysl zde umístit řídící prvek, která bude tyto vlastnosti spravovat. Řídící prvek zajišťuje řízení systému a přijímání zpětné vazby o stavu systému (viz Obrázek 2). [8]



Obrázek 2 - Řídící prvek v systému [8]

2.2.2 STAMP model

Chceme-li vytvořit model integrace dat, musíte jej nejprve postavit na modelu, který bude vhodný pro další analýzu. Pro tyto účely použijeme model STAMP.

STAMP (Systems Theoretic Accident Model and Processes) je model nehod založený na systémové teorii. Zahrnuje tři základní komponenty: omezení, hierarchické úrovně řízení a procesní smyčky. Tento model pracuje s reprezentací systému dle teorie zpětnovazebního

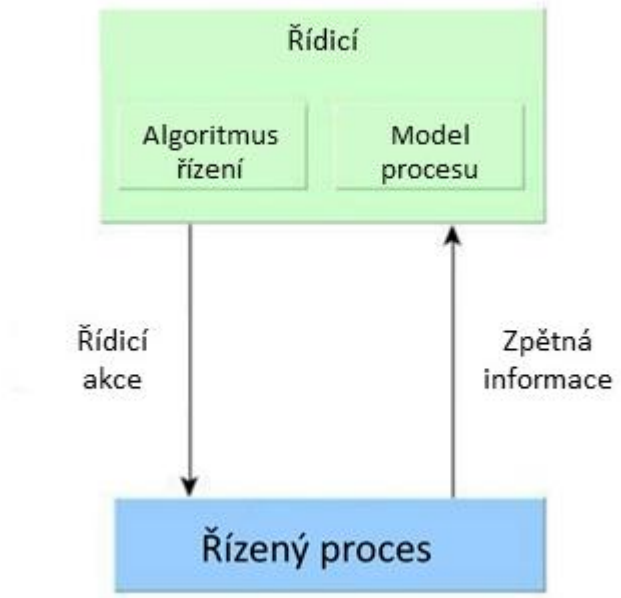
řízení, dále se snaží nahlížet na bezpečnost z pohledu vzájemné interakce prvků v rámci systému a hledá spíš problém v přímé interakci než v prvcích samotných. V tomto modelu se nehody zkoumají z hlediska toho, proč zavedené kontroly nezabránily nebo nezjistily nebezpečí a proč tyto kontroly nebyly adekvátní k prosazování bezpečnostních omezení systému. Jinými slovy, při vytváření celého modelu založeného na nějakém procesu dojde k selhání celého systému, když je zpětná vazba systému nesprávná. [10] [11]

Výhody tohoto modelu jsou:

- tento model je použitelný pro složité a rozsáhlé systémy, protože přístup tohoto modelu je shora dolů;
- zahrnuje software, lidi, organizaci a kulturu jako faktory nehod;
- umožňuje vytvářet výkonnější analytické nástroje, jako například analýzu STPA (System-Theoretic Process Analysis). [8]

Řídící smyčka je jedním z důležitých prvků systému STAMP. S jeho pomocí můžeme popsat procesy, které se v systému vyskytují, a vytvořit logická spojení nezbytná k jejich vysvětlení.

Jednoduchá řídící smyčka se skládá z řídicího (anglicky označován jako Controller) a řízeného procesu (anglicky označován jako Controlled process). Řídicí pomocí algoritmu řízení provádí řídicí akce v rámci řízeného procesu, a získává zpětné informace o novém stavu procesu, který vznikl právě v důsledku akcí s tímto procesem (viz Obrázek 3). [12] [13]



Obrázek 3 - STAMP model a jeho součásti [12]

Takovým systémem je například letadlo (viz Obrázek 4). Pilot (řídicí) řídí pomocí k tomu určených ovladačů letadlo v rámci řízeného procesu „změna polohy letadla v prostoru“ dle svého záměru tak, aby mohl pokračovat v bezpečném udržování letu. Zároveň pilot získává zpětnou informaci o aktuálním stavu pomocí senzorů (konkrétně např. sleduje aktuální výšku letadla nad Zemí po provedeném stoupání). Jakmile pilot přestane ovládat letadlo, letadlo již nebude moci letět dříve plánovanou trasu.

Cílem v tomto modelů je zaměřená výška a celková poloha letadla, a omezení jsou omezení letadla a povolení od ATC.

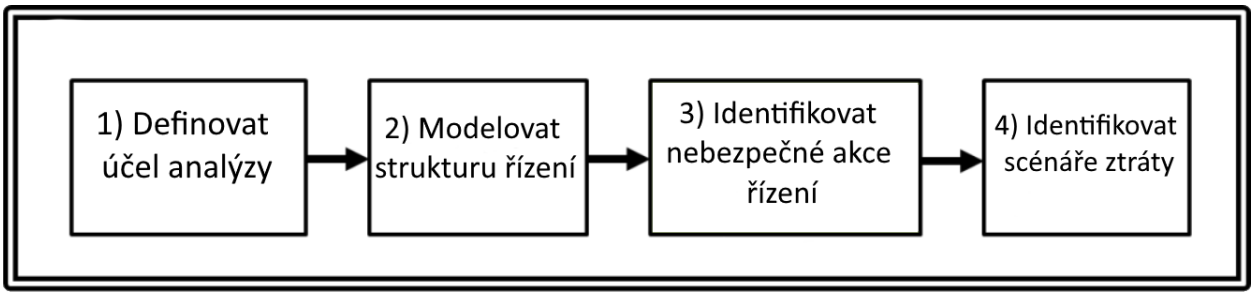
Obrázek 4 - Applikace modelu STAMP na letadlo [12]

2.2.3 STPA analýza

STPA (System-Theoretic Process Analysis) je technika analýzy rizik založená na rozšířeném modelu příčiny nehody. Kromě selhání komponent STPA předpokládá, že nehody mohou být způsobeny také nebezpečnými interakcemi komponentů systému, z nichž by žádný nemusel selhat. [8]

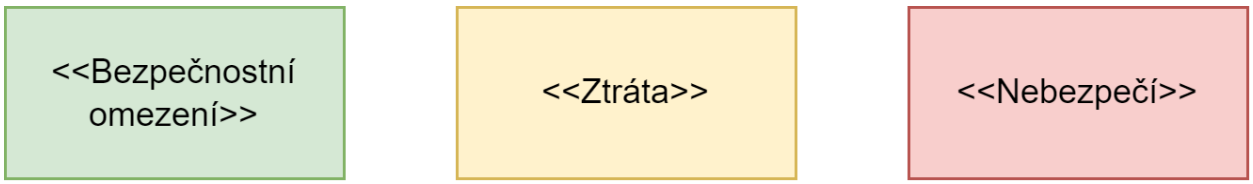
Tuto analýzu lze určit pomocí 4 jednoduchých kroků:

1. Definovat cíl analýzy;
2. Modelovat strukturu řízení;
3. Identifikovat nebezpečné akce řízení;
4. Identifikovat možný vývoj ztrát (viz Obrázek 5).



Obrázek 5 - STPA analýza [7]

Abychom mohli určit účel analýzy, musíme definovat 3 typy prvků, se kterými budeme dále pracovat v následujících krocích: Ztráty (anglicky „losses“), nebezpečí (anglicky „hazards“) a omezení (anglicky „constraints“) (viz Obrázek 6).



Obrázek 6 - Grafické znázornění prvků analýzy [7]

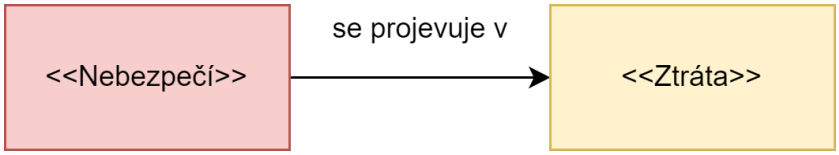
Ztráta je jeden z nejdůležitějších prvků, který lze definovat jako něco, co je pro daný systém cenné, něco, co nechceme ztratit, poškodit nebo nad tím ztratit kontrolu. Celá analýza bude postavena na tom, že chceme předcházet ztrátám, tudíž správná definice ztrát od samého počátku pomůže určit zbytek elementů analýzy.

Pro správnou definici ztrát je třeba nejprve identifikovat strany v systému (piloti, pozemní personál, cestující), poté určit jejich cíle a hodnoty (bezpečnost, poskytování dopravních služeb, finanční zisk) a převést je do ztrát (ztráty resp. poškození letadla či zavazadel, ztráta lidských životů, ztráta provozuschopnosti dráhy apod.).

Abychom mohli dále definovat nebezpečí, musíme nejprve definovat systém, v rámci kterého budeme tato nebezpečí hledat. Nejlepším způsobem, jak definovat tento systém je přesněji vymezit hranice tohoto systému a zahrnout do tohoto systému všechny prvky, nad kterými existuje alespoň částečná kontrola. Vzhledem k tomu, že cílem celé analýzy je snížit nebo zcela předejít následkům jakékoliv nehody, je nutné nejprve vytvořit model, nad kterým má operátor kontrolu. To je přesně to, v čem je rozdíl mezi ztrátou a nebezpečím: v případě ztráty nemůže mít operátor nad prvkem vůbec kontrolu.

Každá nejistota může vést k několika ztrátám současně. Interakce ztráta – nebezpečí, jak lze vidět na obrázku číslo 7, jsou tedy zapsány v následujícím tvaru.

H-1: Nebezpečí číslo 1 [L-1, L-2, L-3].

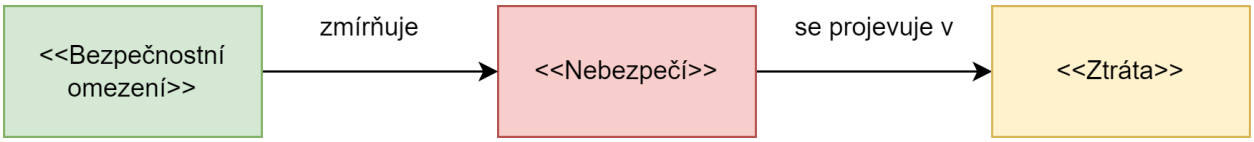


Obrázek 7 - Vazba mezi ztrátou a nebezpečím [autor]

Nebezpečí jako takové by mělo být stavem určitého prvku, nikoli prvkem samotným a k definování nebezpečí v systému by měl být vždy použit scénář nejhoršího případu, který může nastat, protože každé nebezpečí může, ale nemusí vést ke ztrátě.

Při identifikaci nebezpečí je také nutné zaměřit se na to, který proces nebo situace může vést ke konkrétní ztrátě a poté na základě tohoto procesu identifikovat nové nebezpečí.

Omezení na úrovni systému specifikují systémové podmínky nebo chování, které je třeba splnit, aby se předešlo nebezpečí (a předešlo se ztrátám). Jinými slovy, omezení na úrovni systému je tedy v našem systému výchozím bodem, ze kterého může jít systém do nebezpečí a následně až do ztráty (viz Obrázek 8).



Obrázek 8 - Interakce mezi ztrátou, nebezpečím a bezpečnostním omezením [autor]

V modelu může z jednoho bezpečnostního omezení vyplývat více nebezpečí a z každého nebezpečí může vyplývat více ztrát. Pochopení tohoto aspektu je při analýze důležité, protože pomůže vykreslit souvislosti mezi prvky a zaměřit více pozornosti na interakci těchto prvků.

Dále musíme modelovat strukturu řízení. Tato struktura bude v našem případě představovat celý systém, se kterým pracujeme. Na základě řídících smyček postavíme celý model, jak je naznačeno na obrázku číslo 3.

Poté, co sestavíme celý model, bude potřeba definovat nebezpečné kontrolní akce, se kterými bude možné určit scénáře nebezpečné ztráty.

2.2.4 Active STPA

Vzhledem k tomu, že se svět neustále mění a ke změnám dochází i v každém systému v rámci jeho provozování, vzniká potřeba aktualizovat analýzu STPA v kontextu takovýchto změn. Řešení přináší metodika v disertační práci Dioga Silvy Castilha pod názvem Active STPA. [7]

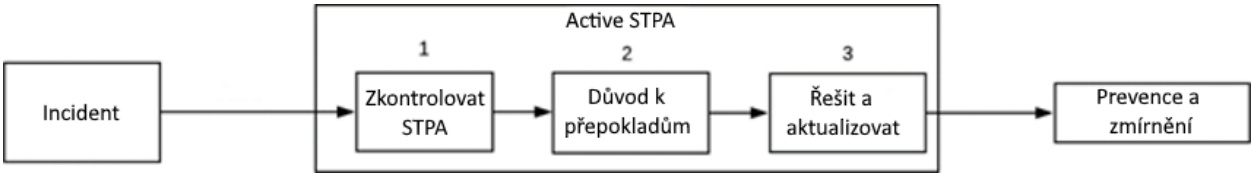
Active STPA využívá data k přizpůsobování a upravování modelu měnícím se vnějším a vnitřním podmínkám. Potřeba vylepšit již existující analýzu se objevila z toho důvodu, že původní model po svém vytvoření dále neprocházel žádnou úpravou, což vytvářelo prostor pro skryté chyby v případě, že byla analýza původně vytvořena nepřesně nebo chybně či pokud došlo k nezáměrným změnám v systému. Tento přístup posouvá analýzu na novou proaktivní úroveň. [7]

Ke vzniku metodiky Active STPA přispěla také řada problémů s předchozí analýzou. Některé z hlavních problémů STPA analýzy, které samotná analýza nedokázala určit ani opravit, jsou:

- Analýza byla původně udělána špatně;
- Analýza nebyla provedena kompletně;
- Změny, které se objevily v průběhu času a ovlivnily analýzu, zrušily platnost předpokladů vložených do STPA.

Active STPA tedy odstraňuje tyto problémy a umožňuje najít chybějící prvky v analýze, a tedy správně identifikovat a předcházet problémům dříve, než k nim dojde.

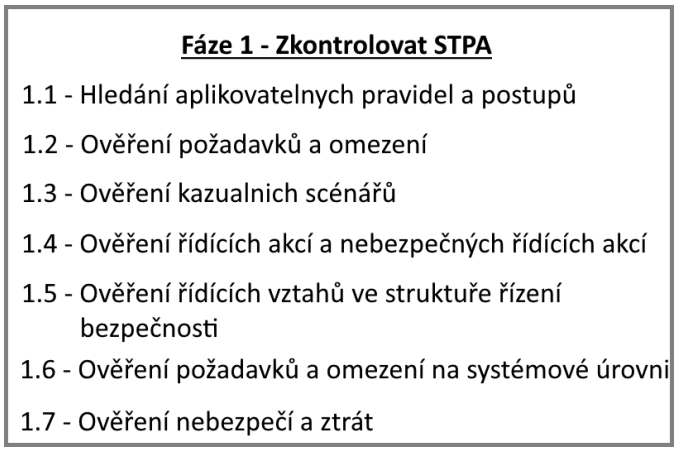
Tato analýza se skládá ze tří fází: STPA analýza, Analýza modelu a trendů, Řešení a aktualizace (viz Obrázek 9).



Obrázek 9 - 3 fáze Active STPA [13]

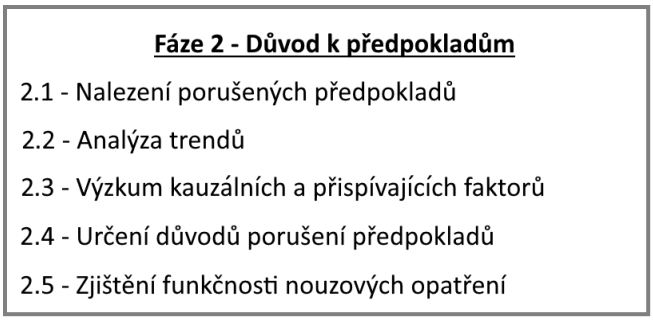
Jak je vidět na obrázku, do celého bloku Active STPA vstupuje incident a vystupuje reakce v podobě určité prevence před další realizací takového incidentu. V této metodice funguje incident jako výchozí bod pro celou analýzu. To znamená, že nejprve dojde k nějakému incidentu, aby byla následně provedena analýza Active STPA. Skutečnost, že k incidentu došlo, znamená, že stávající model STPA není kompletní a je třeba ho aktualizovat.

Během první fáze provádíme kontrolu stávajícího stavu dotčené části analýzy STPA, krok za krokem, jak uvádí Obrázek 10).



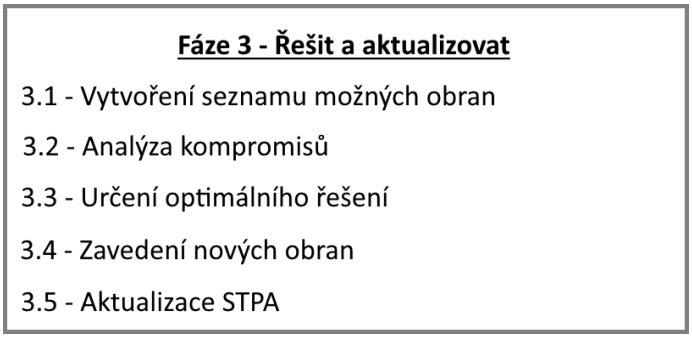
Obrázek 10 - První fáze Active STPA [13]

Během druhé fáze již začínáme reflektivně analyzovat náš model, abychom pochopili, zda skutečně funguje nebo zda při plánování modelu došlo k chybě. Je nutné identifikovat porušené předpoklady, analyzovat trendy, pokusit se odhalit možné faktory ovlivňující model a určit důvod nefunkčních nebo nesprávných předpokladů, pokud existují (viz Obrázek 11).



Obrázek 11 - Druhá fáze Active STPA [13]

Během třetí fáze využíváme výsledky získané během druhé fáze a začínáme analyzovat klady a zápory integrace nových změn do existující analýzy, vybíráme nejoptimálnější řešení a aktualizujeme STPA analýzu (viz Obrázek 12).



Obrázek 12 - Třetí fáze Active STPA [13]

Po provedení celé analýzy získáme jako výstup potřebné prevence a zmírňující opatření, které je dále potřeba aplikovat pro zlepšení bezpečnosti tohoto systému.

3 Model integrace znalosti z bezpečnostních studií s daty o bezpečnosti provozu

Abychom mohli správně vizualizovat model STAMP, můžeme použít ontologii UML, která nám pomůže určit prvky v modelu a vztahy mezi nimi. V této práci budou části UML ontologie použity pouze jako způsob vizualizace prvků a jejich vzájemné interakce, nicméně všechna tato schémata neposkytují architekturu UML, na jejímž základě by mohla být vytvořena aplikace.

3.1 UML diagramy

UML (Unified Modeling Language) - je standardizovaný modelovací jazyk sestávající z integrované sady diagramů pomocí kterého můžeme schematicky znázornit celý systém nebo model a vzájemné působení všech prvků tohoto modelu. Grafické znázornění modelu pomocí diagramů pomáhá vidět celý model najednou, bez nutnosti hlubokého porozumění každému z prvků a co je pro STPA analýzu důležitější, kromě prvků samotných pomáhá věnovat pozornost jejich vzájemné interakci. [14] [15]

Každý diagram se skládá z prvků a vztahů mezi těmito prvky. UML poskytuje rozsáhlou sadu prvků a vztahů, se kterými lze pracovat a popisovat tak systémy jakékoli složitosti. V této práci budou rozebrány pouze ty vztahy a prvky, které budou dále použity. [16]

3.1.1 Prvky

Prvky jsou součástí systému, který chceme popsat. Prvek může být jakýkoliv předmět nebo část předmětu: osoba, nástroj, senzor, proces, jev a tak dále (viz Obrázek 13).

Obrázek 13 - Příklady různých prvků [autor]

V diagramu je prvek označen v obdélníku, ve kterém je napsáno, o jaký prvek se jedná.

Pokud chceme specifikovat, že daný prvek má nějaké chování nebo vlastnosti, pak takový prvek implementuje rozhraní (angl. interface). V tomto případě je blok rozdělen na dvě části a v horní části je určeno, které rozhraní tento prvek implementuje (viz Obrázek 14).

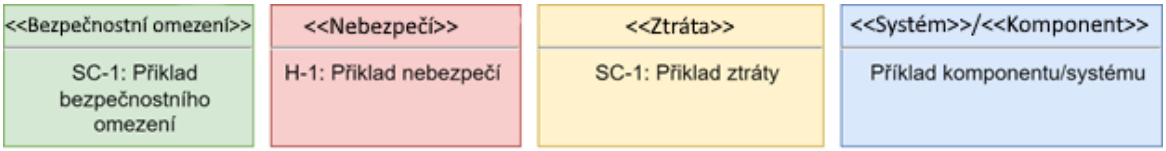
Obrázek 14 - Schematické znázornění prvku, který implementuje rozhraní [autor]

V modelování UML jsou rozhraní prvky modelu, které definují sady operací, které musí implementovat jiné prvky modelu. Prvek implementačního modelu realizuje rozhraní přepsáním každé z operací, jež rozhraní deklaruje. Jinými slovy, pro lepší pochopení modelu, pokud chceme popsat nebo vysvětlit obecné vlastnosti prvku, můžeme specifikovat, které rozhraní implementuje (viz Obrázek 15). [17]

Obrázek 15 - Příklad prvku, který implementuje rozhraní [autor]

Příklad prvku, který implementuje rozhraní: letadlo je dopravní prostředek. To znamená, že máme rozhraní dopravní prostředek, které popisuje chování prvku: tímto prvkem lze pohybovat, může mu být doplněno palivo, může být opravován, můžeme pomocí něj převážet náklad a tak podobně To znamená, že letadlo je již implementací tohoto prvku, protože letadlo je schopno vykonávat všechny funkce uvedené v rozhraní, abychom jej nazvali dopravním prostředkem. Stejně tak může být za dopravní prostředek považováno auto nebo loď, z důvodu schopnosti pohybu a přepravy nákladu, avšak místo vzduchu využívají zem či vodu. Toto je hlavní koncept a myšlenka v rozhraní: popisujeme chování, které je tomuto objektu vlastní, ale jeho implementace pro nás není důležitá. V našem příkladu by to vypadalo takto: pro nás je důležité, že tento objekt je dopravní prostředek, ale je nám jedno, zda se bude pohybovat vzduchem, vodou nebo po zemi.

Na obrázku číslo 16 můžete vidět, jaké prvky budou dále použity k vytvoření a popisu modelu STPA analýzy. Navzdory tomu, že UML diagramy nedefinují žádné barevné označení prvků, bylo rozhodnuto při označování prvků použít barvy, které napomáhají pochopení a vnímání výsledného modelu.

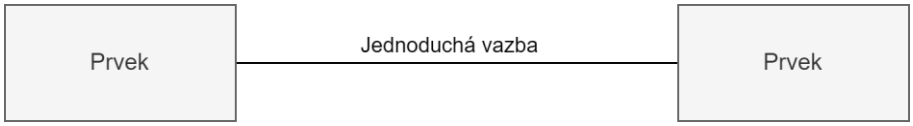


Obrázek 16 - Příklady prvků, které budou použití při vytváření modelu STPA analýzy [autor]

3.1.2 Vazby

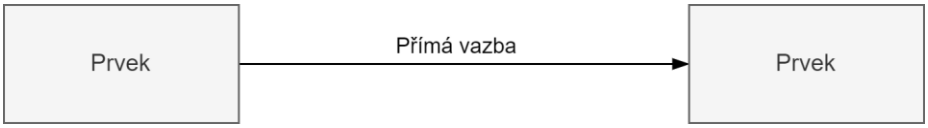
Vazby jsou prvky diagramů UML, které propojují různé prvky v tabulce a ukazují jejich vzájemnou interakci. Vazby jsou čáry mezi prvky, které mohou vypadat jako jednoduchá přímka, stejně jako šipka nebo přímka s nějakým symbolem/označením, které nese nějaký význam. Stejně jako v předchozí části budu v této práci zvažovat pouze ty vazby, které budou použity níže. [18]

Jednoduchá asociace (anglicky Simple Association) je nejzákladnější vazba mezi prvky. Asociace znamená jakýkoli typ vztahu nebo spojení mezi elementy. To znamená, že pokud mají prvky alespoň nějakou souvislost, pak lze mezi nimi nakreslit přímku, která bude naznačovat jednoduchou asociaci (viz Obrázek 17).



Obrázek 17 - Označení jednoduché vazby [autor]

Přímá asociace (anglický Directed Association) je asociace, která naznačuje silný vztah mezi prvky. Označuje se šipkou od jednoho objektu k druhému (viz Obrázek 18).



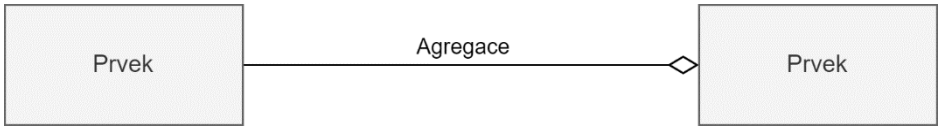
Obrázek 18 - Označení přímé asociace [autor]

Při navrhování modelu použijeme přímou asociaci, pokud chceme zobrazit nějakou posloupnost prvků nebo událostí: tato asociace bude indikovat, který prvek má z kterého vycházet.

Dále bude použita generalizace. Generalizace umožňuje určit, zda je některý prvek přesnější specifikací nějakého obecného prvku. Například pomocí tohoto spojení můžete označit, že rádiovýškoměr je pálubní přístroj (viz Obrázek 19).

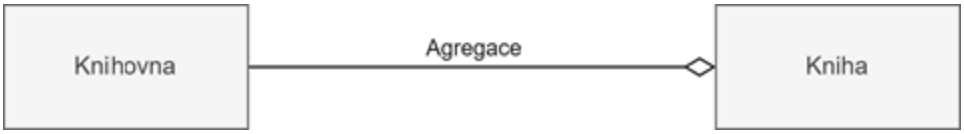
Obrázek 19 - Příklad generalizace [autor]

Poslední vztah, který se bude používat, je agregace (anglicky aggregation). Agregace se bude používat k označení prvků, které jsou součástí nějakého prvku nebo systému. Schematické označení přímky s kosočtvercem na konci, přičemž kosočtverec musí být umístěn u prvku, který je podčástí druhého prvku (viz Obrázek 20).



Obrázek 20 - Označení agregace [autor]

Můžete si vzít například knihovnu a knihu. Vzhledem k tomu, že v knihovně je mnoho knih, bude prvek „kniha“ součástí prvku „knihovna“ a vztah mezi nimi bude vypadat takto (viz Obrázek 21):

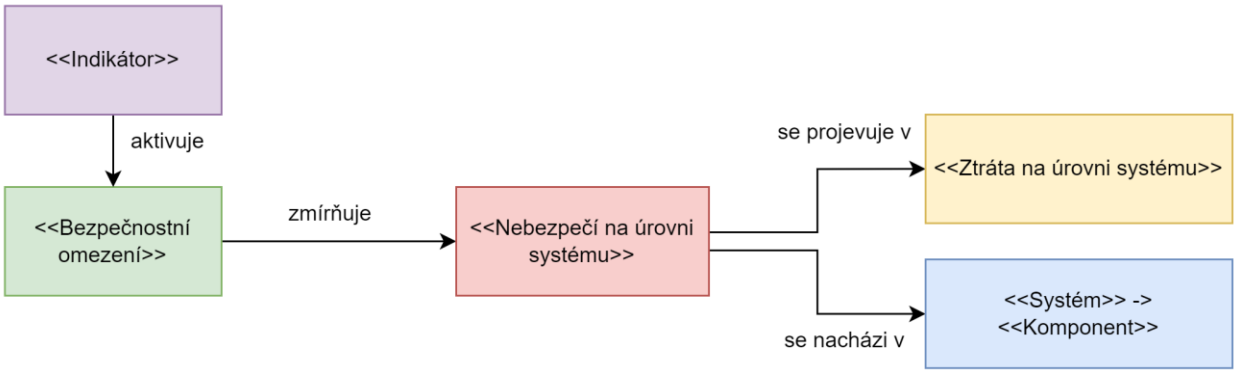


Obrázek 21 - Příklad agregace [autor]

3.2 Model integrace

Pokud máme data z provozu a STPA analýzu založenou na STAMP modelu, musíme definovat sadu pravidel, kterými se budeme řídit, abychom vytvořili logickou a srozumitelnou integraci dat. V této práci je hlavním zdrojem pro integrační model metodika Active STPA s tím rozdílem, že mou snahou je posunout práci s daty do možnosti jejich neustálé integrace namísto částečně reaktivního způsobu iniciace analýzy realizací incidentu. [7] Neustálá integrace se realizuje při sběru a vyhodnocování dat, samotná analýza neprobíhá neustále, ale zachováním iniciace. Mou ambicí je nicméně doplnit jednotlivé kroky analýzy Active STPA o pohled na možnou podporu díky průběné práci s daty.

Po vytvoření modelu STAMP dostaneme schematicky následující model (viz Obrázek 22):



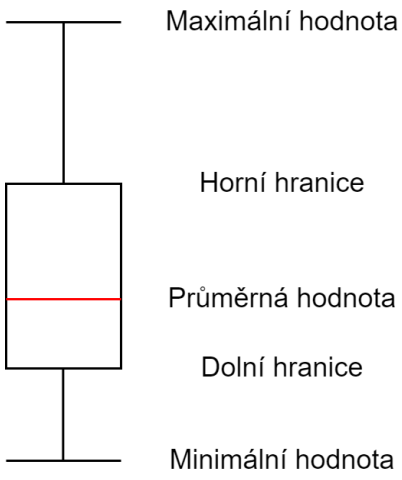
Obrázek 22 - Příklad modelu STAMP [19]

Bezpečnostní omezení a jeho indikátor jsou výchozí body, se kterými budeme pracovat na další integraci dat. [19]

V modelu lze definovat několik bezpečnostních omezení, z nichž každé je doprovázeno seznamem indikátorů, pomocí kterých lze toto bezpečnostní omezení sledovat.

Indikátor je prvek v systému, který je přiřazen k bezpečnostnímu omezení za účelem sledování, zda bylo toto omezení porušeno. Indikátor se skládá ze souboru dat, průměru a hodnoty maximální odchylky pro tato data. Indikátor bude při dosažení určité hodnoty spouštěčem analýzy Active STPA a právě pomocí indikátoru můžeme navázat kontinuální integraci dat do tohoto modelu. V současném přístupu je takovým ukazatelem incident, respektive hlášení o incidentu.

Soubor dat může být soubor jakýchkoliv měřitelných parametrů: rychlost, nadmořská výška, sklon, zrychlení, použitá délka dráhy při přistání a podobně.



Obrázek 23 - Schematické znázornění hodnot indikatorů [autor]

Poté jsou tato data analyzována a je uvedena jejich ideální hodnota. Tato hodnota představuje hodnotu, na kterou by měl měřený proces v dané sekundě měření směřovat, aby se minimalizovaly šance na nebezpečný výskyt.

Na konci je stanoven parametr maximální odchylky, který nám signalizuje aktivaci indikátoru, pokud se údaj o tuto hodnotu liší od průměrné hodnoty. Jinými slovy, indikátor se aktivuje, pokud odchylka od normy překročí předem stanovené limity. Jinými slovy, indikátor je v našem modelu pravidlo, které neustále analyzuje data a aktivuje se, pokud data překročí určitou hranici. (viz Obrázek 23).

Pro další zlepšení nástroje pro integraci dat by bylo možné definovat jeden nebo více horních a dolních mezí, přičemž by každá z nich měla svojí důležitost: pokud je například odchylka v některém parametru 5 %, systém zobrazí varování, což nevyžaduje žádné akce, ale již

upozorňuje na to, že se v systému něco děje. Pokud je však odchylka 10% nebo více, pak se indikátor aktivuje.

V praktické části práci pro jednoduchost použita pouze jedna hranice.

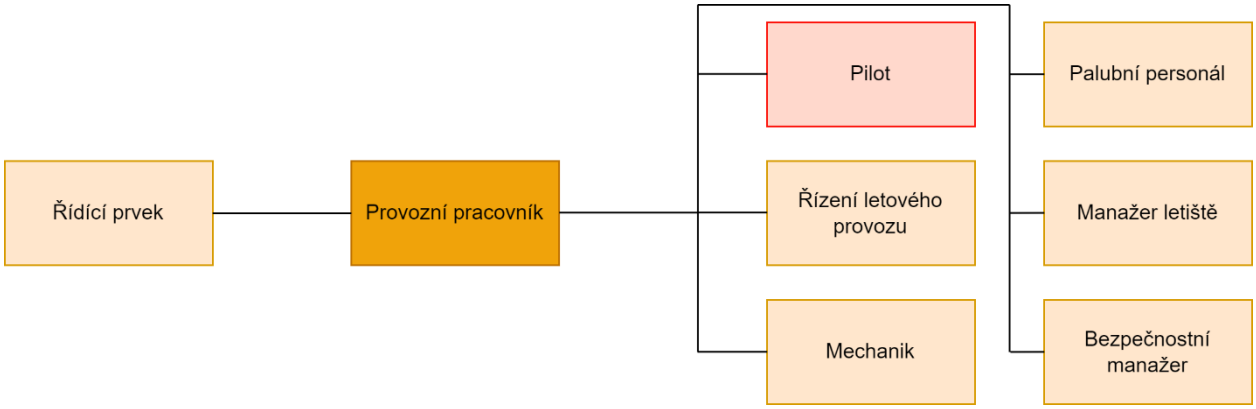
4 Výběr procesu a tvorba modelu pro následnou analýzu

Výběr řízeného procesu byl omezen zadáním, podle kterého by měl řídicím takového procesu být člověk – provozní pracovník.

4.1 Pracovník v leteckém provozu

V prostředí letiště pracuje mnoho lidí, z nichž každý plní svůj úkol, čímž je delegován jako řídicí do určitého množství jím řízených procesů. Pro přesnou a správnou integraci dat potřebujete zaměstnance, kolem kterého se shromažďuje obrovské množství dat, a následně zvolit kontrolní proces, který má dostatek prostoru pro zlepšení v rámci bezpečnosti.

Obrázek 24 uvádí některé možnosti, které by mohly být použity pro stavbu modelu. Vzhledem k tomu, že data budeme simulovat, a k analýze pilota je dostupných dat mnohem více, než například ve vztahu k manažeru letiště, bylo rozhodnuto zvolit pilota. V tomto ohledu bude vybrán i proces, ve kterém je pilot přítomen a který nejvíce souvisí s bezpečností na letišti.



Obrázek 24 - Varianty provozního pracovníka [autor]

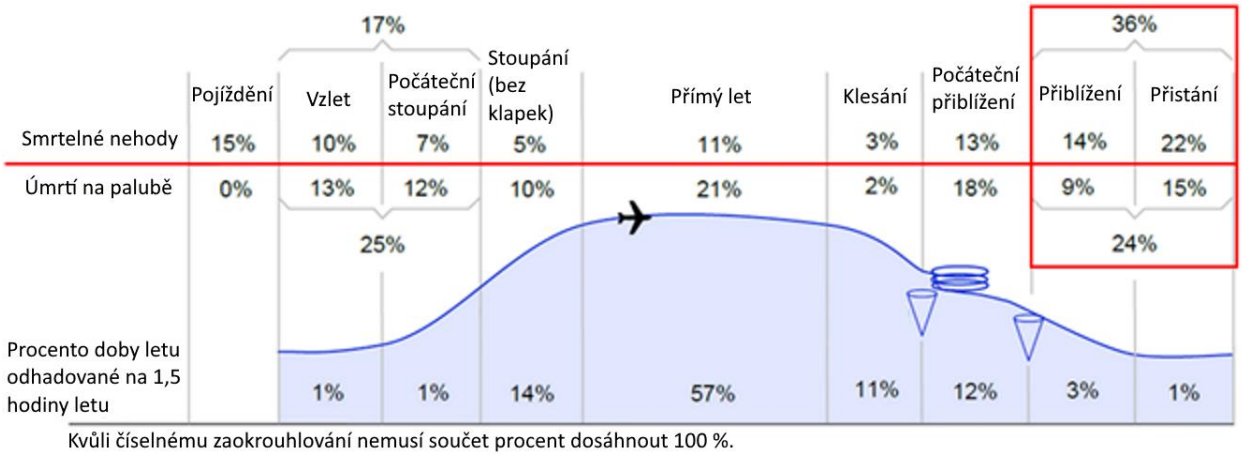
4.1.1 Lidský faktor

Jedním z hlavních bodů, proč by měl být model datové integrace testován včetně procesů, kde řídícím prvkem je člověk, je lidský faktor. Faktem je to, že byl integrační model testován na systému ADGS, kde jsou všechna data obecně měřitelná a lze je analyzovat. To však neznamená, že tento model bude fungovat i s lidským faktorem, protože se měří mnohem hůře a výzkum lidského faktoru stále probíhá. [20]

Lidský faktor tvoří přibližně 80 % všech nehod, a proto je jeho studium důležitou složkou letecké bezpečnosti v letectví. [21] [22]

4.1.2 Výběr řízeného procesu

Pokud vezmeme v úvahu různé fáze letu letadla, uvidíme, že k většině nehod dochází ve fázi přiblížení a přistání letadla (viz Obrázek 25). [23]



Obrázek 25 - Procento smrtelných nehod a úmrtí na palubě - komerční proudová flotila 2001 - 2010 (Boeing) (volný překlad) [23]

Proto bylo rozhodnuto zvolit proces, se kterým budeme dále pracovat – proces přiblížení a přistání letadla. Proces je vhodný pro ilustraci neustálého toku dat, protože letecká společnost má větší možnosti dat k dispozici – na letišti takto kontinuální sběr dat není možný. Také z toho důvodu byla pozornost posunuta k procesu priblížení, protože samotné letiště a jeho infrastruktura přímo ovlivňují samotný proces takovými prvky, jako je radionavigační zařízení letiště, cizí předměty na dráze a pokyny z řízení vzdušného prostoru.

4.2 Vytvoření modelu STAMP

Jakmile máme vybrán řídící prvek a proces, který bude řídit, můžeme začít vytvářet model STAMP. Pro vytvoření modelu budeme postupně přidávat prvky, které jsou ovlivněny pilotem, a prvky, které jsou ovlivněny samotným procesem přistání, dokud nedostaneme kompletní řídící smyčku. Tento STAMP model uvádí Příloha A.

Nad každou vazbou je seznam parametrů, které se předávají z prvku na prvek. Stejně jako seznam parametrů však může být celkový model mnohem větší a některé prvky lze rozdělit na několik podprvků, ale z důvodu praktičnosti byl model popsán pouze v nezbytné míře.

4.3 Definice systému s ontologií STAMP

Popsaný systém spoléhá především na pilota a jeho jednání, nicméně na systém mají vliv i další prvky jako samotný letoun, další letouny a řízení letového provozu.

4.3.1 Ztráty

V tomto systému byly identifikovány následující ztráty:

- L-1: Poškození letadla v důsledku kolize s letištní infrastrukturou;
- L-2: Uzavření drahy z důvodu poškození letadla na dráze a poškození dráhy;
- L-3: Poškozená radiová infrastruktura na letišti v důsledku srážky letadel;
- L-4: Zranění posádky a cestujících.

4.3.2 Nebezpečí

Dále byla identifikována nebezpečí na úrovni systému:

- H-1: Nestabilizované přiblížení [L-1, L-2, L-4]
- H-2: Výjetí za práh dráhy [L-1, L-3, L-4]
- H-3: Překročení maximální přistávací hmotnosti [L-2, L-3, L-4]

4.3.3 Bezpečnostní omezení

Potom byla definována bezpečnostní omezení:

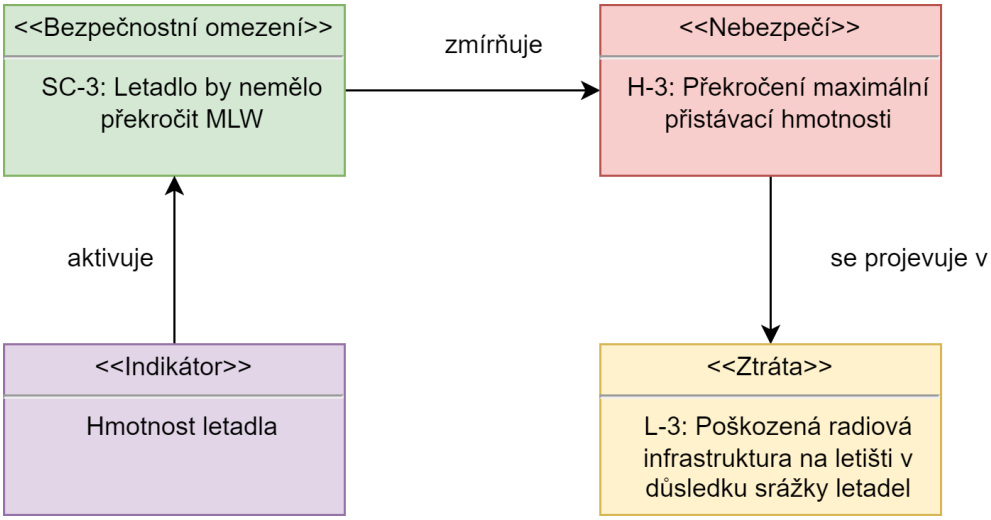
- SC-1: Letadlo by mělo byt stabilizované na přiblížení;
- SC-2: Letadlo by mělo zastavit na dráze ;
- SC-3: Letadlo by nemělo překročit MLW.

4.3.4 Předpoklady

Na konci, k vytvoření schématu, byly definovány tyto předpoklady:

- A-1: Letoun bude vyhovovat z hlediska výkonu pro přistání na tomto letišti
- A-2: Letová posádka bude certifikována pro přiblížení a bude mít dostatečný výcvik
- A-3: Letadlo bude stabilizováno během přiblížení
- A-4: Letová posádka bude z přístrojů informována o poloze letadla

Na základě výše definovaných bodů bylo vytvořeno následující schéma, kterou uvádí Příloha B, Příklad tohoto schéma pro jedno bezpečnostní omezení je na obrázku číslo 26.



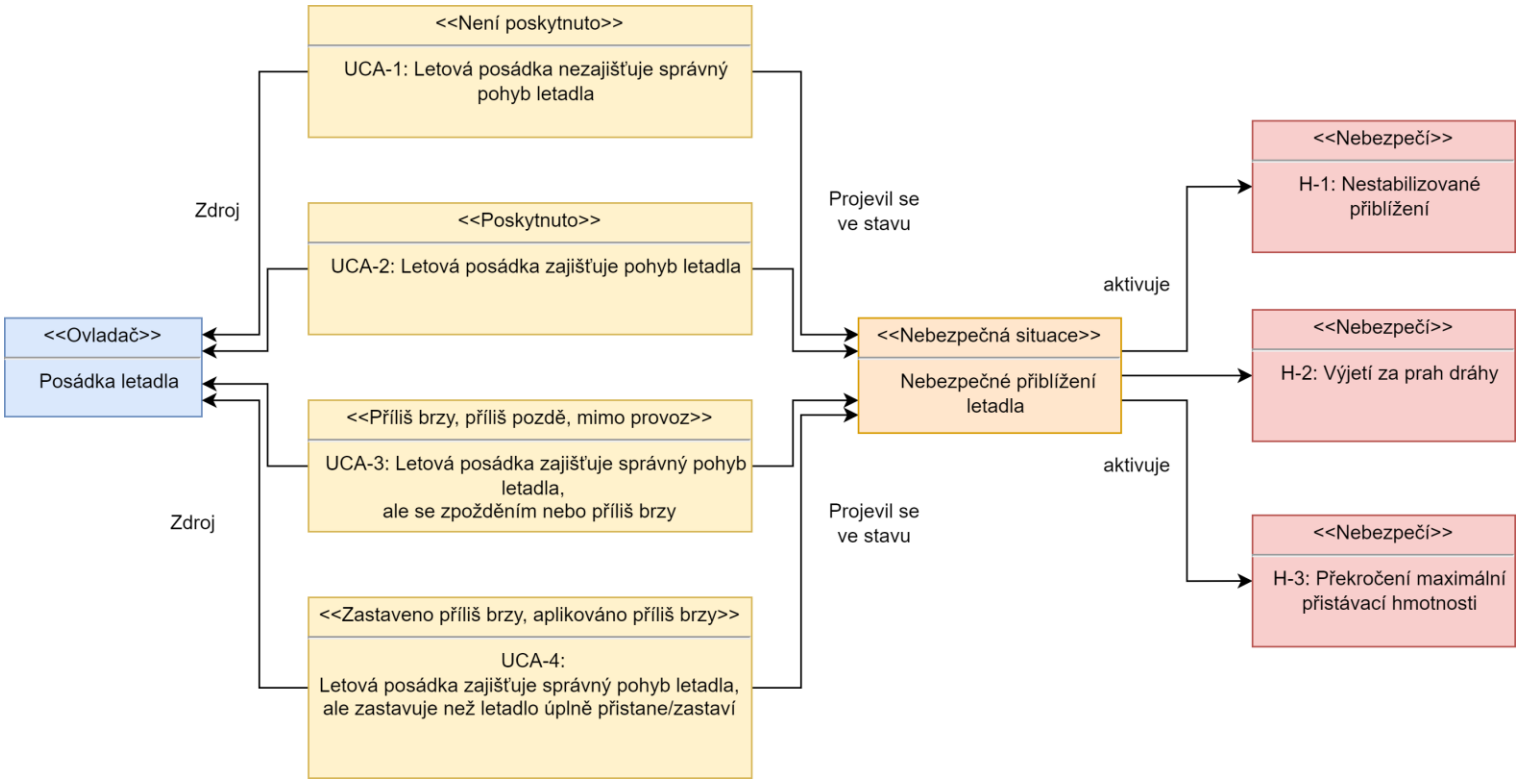
Obrázek 26 - Část systému s ontologií STAMP [autor]

4.4 Bezpečnostní řídicí struktura

Dalším krokem je definování a vytvořit bezpečnostní řídicí struktury. Tento model bude klasickým modelem STAMP, který byl popsán dříve, ale s označením vztahů mezi prvky. V tomto případě model ukáže tři vztahy: informační vztah, zpětnovazební vztah a akční vztah. Bezpečnostní řídicí strukturu uvádí Příloha C.

4.5 Nebezpečné kontrolní akce

Posledním modelem, který má být definován, je model nebezpečné kontrolní akce (viz Obrázek 27):



Obrázek 27 - Nebezpečné kontrolní akce [autor]

5 Návrh bezpečnostních hypotéz

Hypotéza je přesné testovatelné prohlášení o tom, co se očekává a co bude výsledkem studie. [24]

Byly identifikovány celkem dvě hypotézy:

- Způsob neustálé integrace dat bude fungovat i v takových procesech, ve kterých je kontrolním prvkem člověk.
- Neustálá integrace dat v porovnání s současným přístupem pomůže rychleji a spolehlivěji odhalit skryté hrozby a problémy v rámci bezpečnostního modelu.

První hypotéza má otestovat cíl této práce. Druhá hypotéza, pokud se první potvrdí, bude muset také naznačovat, že tato metoda je v některých aspektech výhodná ve srovnání s současným přístupem.

6 Zpracování dat

Manuální zpracování dat může být při zpracování velkého množství dat poměrně časově náročné a neefektivní. Napsání programu pro zpracování dat umožní vytvořit architekturu aplikace, kterou lze korigovat v závislosti na formátu a taxonomii dat, formě, ve které se data čtou a zapisují, a usnadní a zrychlí práci s daty obecně. Dále bude uvedeno, jaká data budou analyzována, jak vypadají a co bylo použito k napsání programu.

6.1 Software

Jako software pro zpracování dat a grafů byly použity dva jazyky: Python a Java. Pomocí Pythonu bylo možné sestavovat, podepisovat a zobrazovat grafy založené na již napsané knihovně matplotlib a Java byla použita jako nástroj pro čtení a zpracování dat a také jako doplněk k již napsané knihovně pro pohodlnější práci s grafy a daty.

Aby bylo možné pracovat se dvěma jazyky a vzájemně je integrovat, mělo být původně možné použít Jython - knihovnu, která poskytuje možnost používat implementace Pythonu v Javě, nicméně vzhledem k stále probíhajícímu vývoji tohoto jazyka (Jython), a jeho nedokonalostem, byla nalezena další knihovna, která zjednodušila integraci mezi oběma jazyky: matplotlib4j, která byla později v projektu použita pro práci s daty. [25] [26]

Napsal jsem Java program, který je schopen číst data ze souboru, kategorizovat je (rychlost, výška atd.) a zobrazovat na obrazovce jeden nebo více grafů spolu se všemi přednastavenými parametry, jako je průměrná hodnota nebo limity tohoto indikátoru. Na základě těchto grafů tak bude možné analyzovat, zda je daný indikátor aktivován nebo ne.

6.2 Data

Původně bylo plánováno použít údaje od letiště pro obecnou analýzu, ale vzhledem k tomu, že tyto údaje jsou pro letiště citlivé a některé z nich jsou považovány za obchodní tajemství, které nepodléhají zveřejnění, a aby bylo možné zobrazit práci programu na dříve popsaném modelu STAMP bylo rozhodnuto použít data z simulátoru k zobrazení integračních dat. Proces přiblížení a přistání byl zvolen proto, že se týká bezpečnosti na letišti a je nejnebezpečnější částí letu. [23]

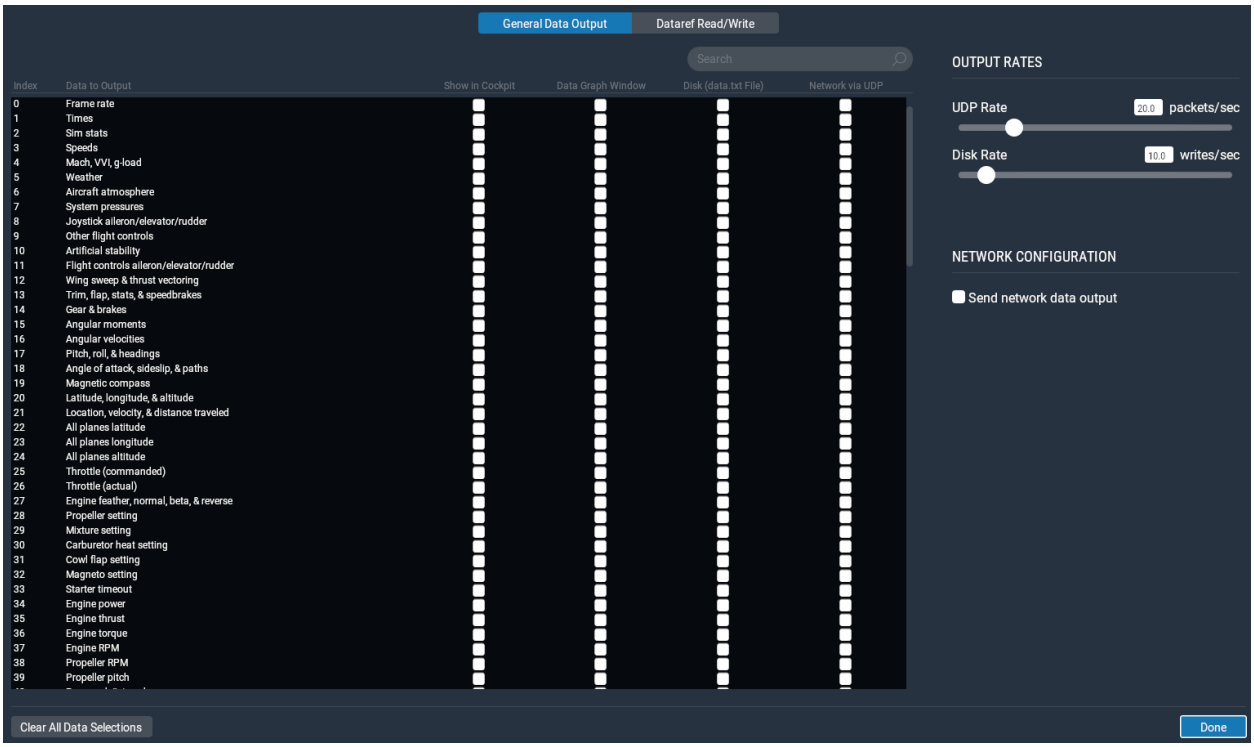
Simulátor, který byl použit pro analýzu je certifikovaný FSTD Generix TurboProp FNPT II MCC, od společnosti inAero, který představuje simulátor dvoumotorového letadla L410. Software tohoto

simulátoru je program X-Plane 11 (dále jen X-Plane), který generoval data, která budou dále analyzována (viz Obrázek 28). [27] [28]

Obrázek 28 - Kokpit simulátoru letadla L410 [autor]

Během letu je X-Plane schopen generovat letová data a buď je zapisovat do souboru, nebo je odesílat na vzdálený server prostřednictvím protokolu UDP. Pro jednoduchost řešení a absenci nutnosti neustále posílat data na server byla zvolena první možnost.

Záznam dat probíhá během letu a X-Plane ukládá vybraná letová data do souboru s názvem Data.txt. Pro úsporu zdrojů X-Plane umožňuje přesně vybrat, jaká data chcete uložit a frekvenci ukládání dat; jinými slovy, kolikrát za sekundu chceme změřit a uložit všechny parametry letadla (viz Obrázek 29).



Obrázek 29 - Okno nastavení výstupu dat X-Plane [autor]

Celkem je k dispozici 136 datových sad, přičemž každá sada může obsahovat více parametrů. [29] Například sada číslo 1 „Čas“ poskytuje parametry jako například:

- Reálný čas – čas na počítači, na kterém byl simulátor spuštěn;
- Aktuální čas – čas aktuálního letu v letadle;
- Celkový čas – jak dlouho byl simulátor zapnutý;
- Čas na časovači;
- Místní čas - čas s úpravou časového pásma podle toho, ve kterém časovém pásmu se letadlo nachází;
- Čas zulu;
- Celkový počet hodin nalétaných tímto letadlem

6.2.1 Datový formát

Pro další práci s daty je důležité pochopit, v jakém formátu jsou data zaznamenána.

Obrázek číslo 30 ukazuje příklad dat z datové sady č. 1 – “Čas“. Pokaždé, když je datová skupina přidána nebo odebrána z nastavení simulátoru, X-Plane vygeneruje se nový řádek skládající se z názvů těch datových skupin, které byly zahrnuty do položky souboru. Každý sloupec představuje sadu dat, která se zaznamená během letu.

_real,_time	_totl,_time	missn,_time	timer,_time	_zulu,_time	local,_time	hobbs,_time
89.30979	0.05025	0.05025	0.00000	15.86001	11.86001	1.32445
89.77206	0.10050	0.10050	0.00000	15.86003	11.86003	1.32446
91.97385	1.08355	1.08355	0.00000	15.86030	11.86030	1.32474
92.97134	2.08103	2.08103	0.00000	15.86058	11.86058	1.32501
93.96864	3.07833	3.07833	0.00000	15.86086	11.86086	1.32529
94.96663	4.07632	4.07632	0.00000	15.86113	11.86113	1.32557
95.96151	5.07120	5.07120	0.00000	15.86141	11.86141	1.32585
96.96357	6.07326	6.07326	0.00000	15.86169	11.86169	1.32612
97.96244	7.07213	7.07213	0.00000	15.86196	11.86196	1.32640
98.96006	8.06975	8.06975	0.00000	15.86224	11.86224	1.32668

Obrázek 30 - Soubor "Data.txt" otevřen v textovém editoru [autor]

V tomto příkladu byla frekvence měření zvolena jednou za sekundu a ze sloupce missn,_time (zrkátka z angl. „Mission time“), každý další řádek je přibližně o 1 sekundu delší než předchozí. První dva řádky se vždy měří mnohem rychleji, protože je to součást kalibrační sekvence simulátoru a časový rozdíl mezi dvěma nejbližšími řádky ve sloupci missn,_time není přesně 1, protože se jedná o chybu a nepřesnost počítače. Za účelem minimalizace této chyby a zvýšení přesnosti dat bude hodnota měření nastavena na 10krát za sekundu. (Simulátor umožňuje vybrat až 100 měření za sekundu, ale pozdější zpracování dat by s takovou přesností trvalo mnohem déle).

Protože sloupec missn,_time zobrazuje čas daného letu, lze jej použít k identifikaci dvou různých letů: každý nový let se tento sloupec začne počítat od nuly (viz Obrázek 31).

_real,_time	_totl,_time	missn,_time	timer,_time	_zulu,_time	local,_time	hobbs,_time
549.69281	457.77203	457.77203	0.00000	15.98716	11.98716	1.45160
550.68585	458.76508	458.76508	0.00000	15.98744	11.98744	1.45187
551.67755	459.75681	459.75681	0.00000	15.98771	11.98771	1.45215
552.67383	460.75308	460.75308	0.00000	15.98799	11.98799	1.45242
553.67267	461.75192	461.75192	0.00000	15.98826	11.98826	1.45270
571.81549	462.45514	0.04371	0.00000	15.98846	11.98846	1.45290
572.81195	463.45163	1.04020	0.00000	15.98874	11.98874	1.45317
573.80786	464.44751	2.03607	0.00000	15.98901	11.98901	1.45345
574.80322	465.44287	3.03146	0.00000	15.98929	11.98929	1.45373
575.79504	466.43469	4.02328	0.00000	15.98956	11.98956	1.45400
576.79364	467.43332	5.02190	0.00000	15.98984	11.98984	1.45428

Obrázek 31 - Jak vypadá začátek nového letu v datovém souboru [autor]

V programu lze tento rozdíl sledovat a pokaždé, když k takovému přechodu času na nulu dojde, lze jej zaznamenat jako nový let.

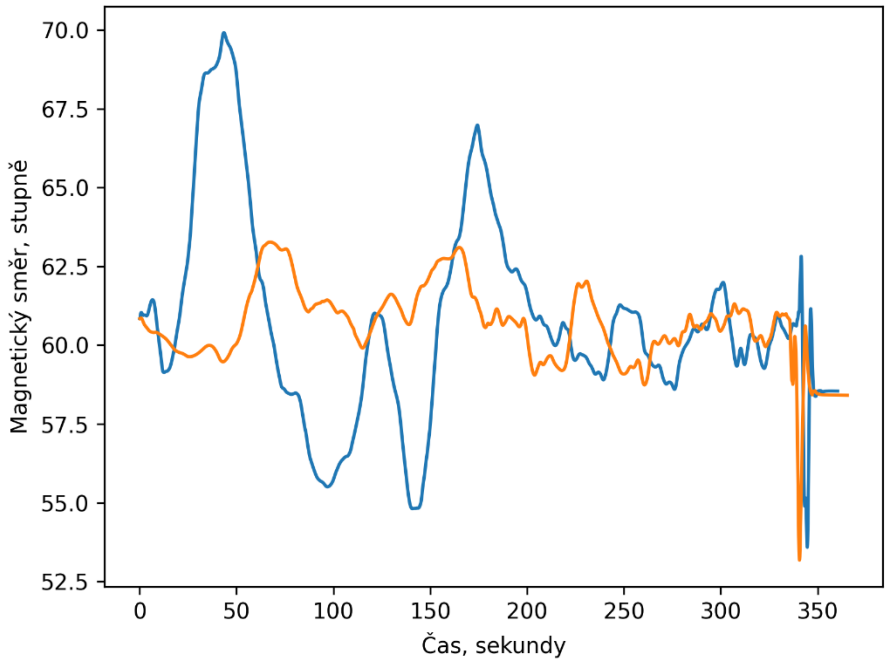
6.2.2 Shromážděná data

Jak již bylo zmíněno dříve, data budou zaznamenávána 10krát za sekundu. Ze 136 dostupných datových souborů bylo vybráno 15, které zahrnují celkem 82 parametrů, z nichž hlavními parametry jsou:

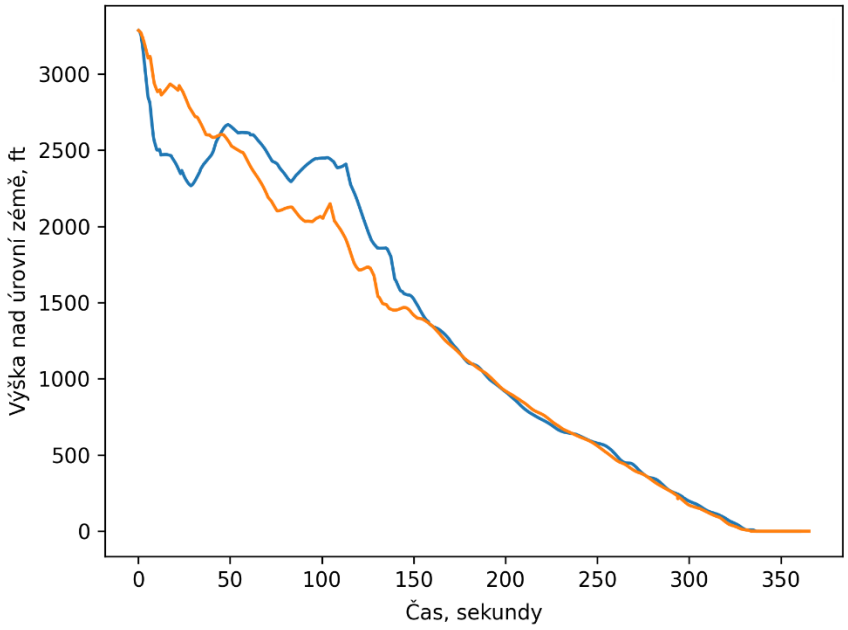
- Čas
- Rychlost
    - IAS
    - TAS
    - GS
- Vertikální rychlost
- Výchylka řízení
- Vyvážení
- Pozice klapek
- Náklon a úhlová rychlost
- Výška
    - AGL
    - AMSL
- Vzdálenost od radionavigačního zařízení
- Odchylka od radionavigačního zařízení ve stupních

6.3 Grafy

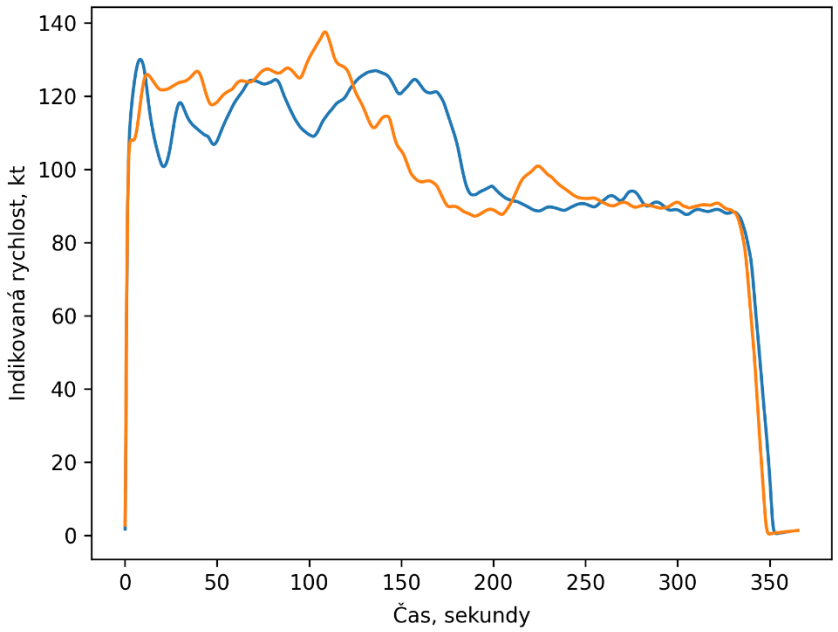
Pro prvotní představu o možnostech měření dat byly provedeny dva počáteční simulované lety v podobě dvou ILS přiblížení na dráhu 06 na letišti LKPR. První let je označen modře a druhý žlutě. Na následujících grafech můžeme pozorovat, že kolísání magnetického směru (viz Graf 1) a výšky (viz Graf 2) během druhého letu je mnohem menší, což naznačuje, že při druhém letu si pilot na simulátor lépe zvykl. Na grafu rychlosti můžeme pozorovat, že v mezičase 150 až 200 sekund došlo k otevření klapek do pozice 42 stupňů, což vedlo ke stabilizaci rychlosti kolem 90 - 95 uzlů (viz Graf 3).



Graf 1 - Magnetický směr při přistání [autor]



Graf 2 - Výška nad úrovní země při přistání [autor]



Graf 3 - Indikovaná rychlost při přistání [autor]

6.4 Integrace dat

6.4.1 Indikátory

Pro vybraný proces přistání letadla byly stanoveny následující indikátory stabilizovaného přiblížení, jinými slovy - indikátory pro bezpečnostní omezení SC-1 – „Letadlo by mělo být stabilizované na přiblížení“:

- Vertikální a horizontální odchylka od ILS by neměla být větší než 0,5 stupně (1 bod na přístroji letadla);
- Magnetický kurz se nesmí lišit o více než 5 stupňů od směru dráhy;
- Vertikální rychlost nesmí překročit 1000 stop za minutu v absolutních hodnotách;
- Sklon letadla nesmí v absolutní hodnotě překročit 10 stupňů;
- Náklon letadla nesmí v absolutní hodnotě překročit 5 stupňů;
- Rychlost s plně otevřenými klapkami musí být mezi Vref - 5 a Vref + 10 uzlů rychlosti (84 uzlů pro plně otevřené klapky) ;
- Nemělo by docházet k žádným náhlým pohybům letadla.

Pro bezpečnostní omezení SC-2 – “Letadlo by mělo zastavit na dráze” byly stanoveny tyto indikátory:

- Vertikální rychlost nesmí překročit 1000 stop za minutu v absolutních hodnotách;
- Vertikální odchylka od ILS by neměla být větší než 0,5 stupně (1 bod na přístroji letadla);
- Rychlost s plně otevřenými klapkami musí být mezi Vref - 5 a Vref + 10 uzlů rychlosti (84 uzlů pro plně otevřené klapky) ;
- Hmotnost letadla by neměla překročit MLW.

Pro bezpečnostní omezení SC-3 – “Letadlo by nemělo překročit MLW” byl stanoven jeden indikátor: Hmotnost letadla by neměla překročit MLW.

Je potřeba zmínit, že tyto parametry byly zvoleny pro nejlepší grafické znázornění integrace dat. V praxi by měl byt použit dokument ICAO 8168. Vzhledem k tomu, že toto letadlo má přistávací rychlost 84 uzlů, patří do kategorie A, což znamená, že jej lze nastavit pro rychlostní limity 70-100 uzlů a pro vertikální rychlost - 394 - 655 stop za minutu. [30] [31] [32]

Hranice pro jednotlivé indikátory je z velké části záležitostí nastavení koncovým uživatele. Díky neustálé integraci dat lze upravovat parametr hranice pro každý indikátor podle toho, v jakém přesném okamžiku je hranice nejčastěji překročena. Pokud není překročena nastavená hranice

ukazatele, lze ji postupně snižovat a naopak, pokud je tato hranice neustále porušována, pak ji lze zkalibrovat na hodnotu méně citlivou na změny.

V této práci bude zvažována aktivace indikátoru, pokud průměrná hodnota parametru překročila limit, nebo určité procento letů z celkového počtu tuto hodnotu překročilo. Je také možné sledovat trendy indikátorů, zda aktuální trend bude překračovat limit nebo ne, nicméně taková práce s trendy vyžaduje velké množství dat, které je obtížné v rámci simulace dat vytvořit.

Dle původního záměru získat reálná data z provozu od letecké společnosti jsem předpokládal, že analyzovaný typ letounu bude vyžadovat délku přistání srovnatelnou s délkou dráhy použité pro přistání. V takovém případě by bylo možné analyzovat bezpečnostní omezení SC-2 a SC-3 podrobněji, ale protože analyzovaný model letadla byl pouze jeden a konfigurace každého letu před přistáním byla stejná, nebudou tato bezpečnostní omezení později v práci rozebírána.

6.4.2 Simulovaná situace

Abychom mohli ilustrovat, jaké indikátory lze v modelu integrace použít, jak fungují a jak s nimi pracovat, musíte je analyzovat na konkrétním procesu. Bylo rozhodnuto, že zkoumaným procesem bude přistání letadla na dráze 06 na letišti LKPR z bodu ve vzdálenosti 10 námořních mil ve výšce 4000 stop AMSL. V tomto bodě je letadlo pod úrovni ILS glideslope, takže jakmile začne let na simulátoru, pilot má nějaký čas na to, aby se vyrovnal a začal klesat. Tato simulace byla spuštěna s viditelností větší než 10 km, bez mraků a bez větru, čímž se v analýze eliminoval faktor počasí. Letoun byl ve vyváženém stavu, klapky byly v poloze 0 stupňů a kola podvozku vysunuta a upevněna. Simulace začala při cestovní rychlosti 135 uzlů a celkové hmotnosti letadla 6000 kilogramů, palivové nádrže byly plné.

Toto letadlo má 2 konfigurace klapek: 18 stupňů a 42 stupňů. Pro proces přistání byla stanovena následující konfigurace: otevření prvních vztlakových klapek ve vzdálenosti 5 námořních mil od DME PH, druhých vztlakových klapek ve vzdálenosti 2 námořních mil od DME PH.

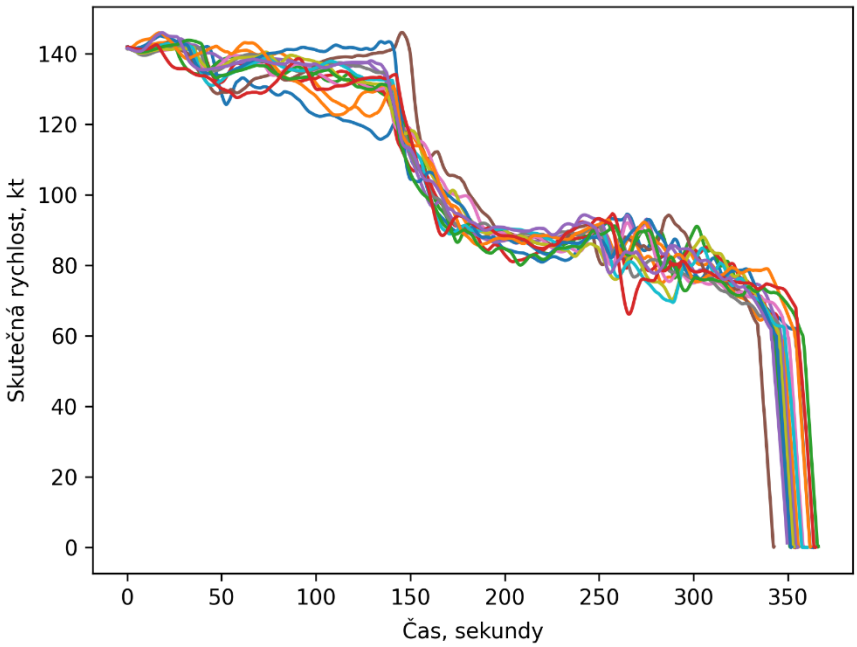
Veškerá konfigurace a limity byly nastaveny podle letové příručky letadla. [30]

V této konfiguraci bylo provedeno celkem 20 přistání za účelem přesného stanovení průměrných hodnot.

6.4.3 Analýza dat

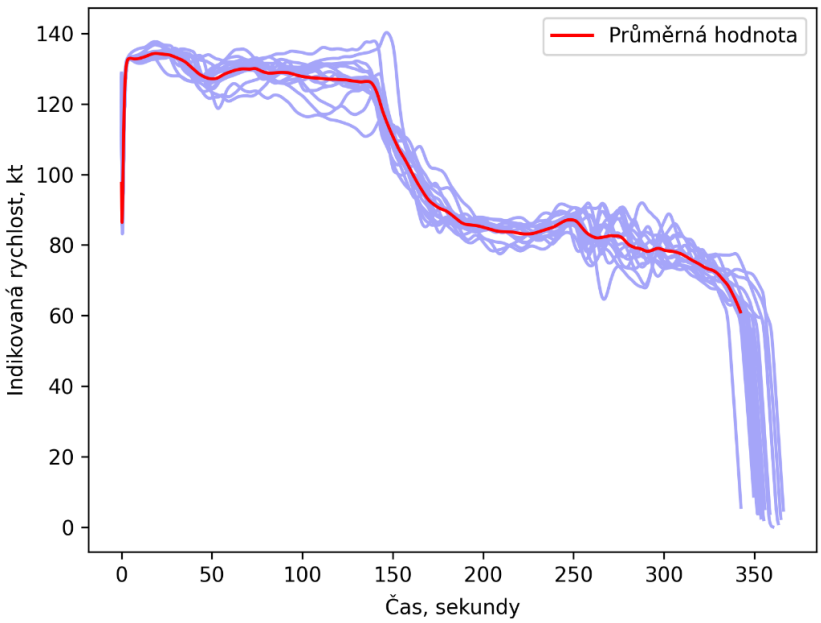
Aby bylo možné určit, jak budou indikátory aktivovány, je nutné stanovit logické pravidlo, podle kterého bude možné zvážit, zda je indikátor aktivován.

Následující graf (viz Graf 4) ukazuje rychlosti letu každého letadla z realizovaných simulovaných letů. Přestože tento graf poskytuje informace o výsledcích měření procesu, nestačí to na práci s indikátory a určení, zda mělo dojít k jejich aktivaci. Za účelem práce s indikátory je třeba nejprve vypočítat průměrnou hodnotu pro průběh všech simulovaných letů a s tou dále pracovat



Graf 4 - Skutečná rychlost všech letů během přistání [autor]

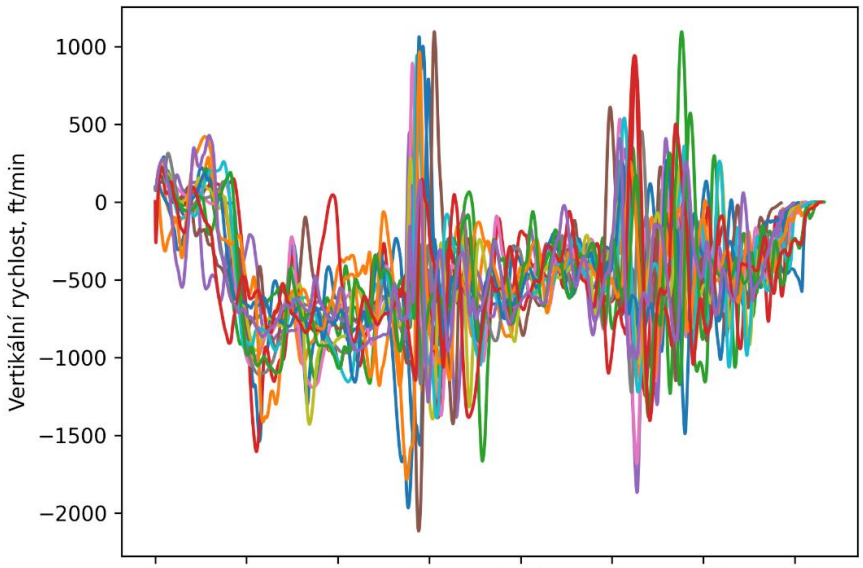
V následujícím grafu (viz Graf 5) jsou jednotlivé průběhy rychlosti každého ze simulovaných letů zobrazena světle fialovou barvou a jejich průměrná hodnota průběhu rychlosti je zobrazena červenou barvou. Je třeba věnovat pozornost tomu, že průměr není započítán na konci grafu, protože se počítá pouze tehdy, jsou-li všechny lety dostupné pro zadané časové období. Jinými slovy, pokud jeden z letů skončil dříve než ostatní, průměrná hodnota se dále nepočítá.



Graf 5 - Průměrná indikovaná rychlost všech letů [autor]

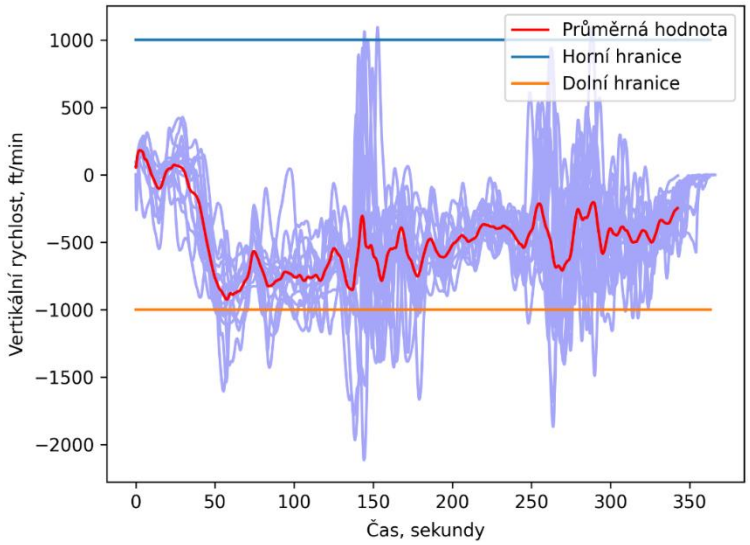
Musíme také věnovat pozornost tomu, že tento graf byl vytvořen na základě času: osa x udává, kolik sekund let letadla trvá (proměnná X-Plane - TOTAL_TIME - celkový čas). Při reálném letu se sledovaná událost samozřejmě neděje vždy ve stejnou dobu a je třeba na to pamatovat patřičou korekcí.

Příklad: Vertikální rychlost letadla během prvního letu v konkrétní sekundě byla 1000 stop za minutu, zatímco průměrná rychlost druhého letu byla -1000 stop za minutu. Průměrná vertikální rychlost bude 0 stop za minutu, ačkoli vertikální rychlost prvního i druhého letu může být rozhodující pro aktivaci nějakého z indikátorů (viz Graf 6).



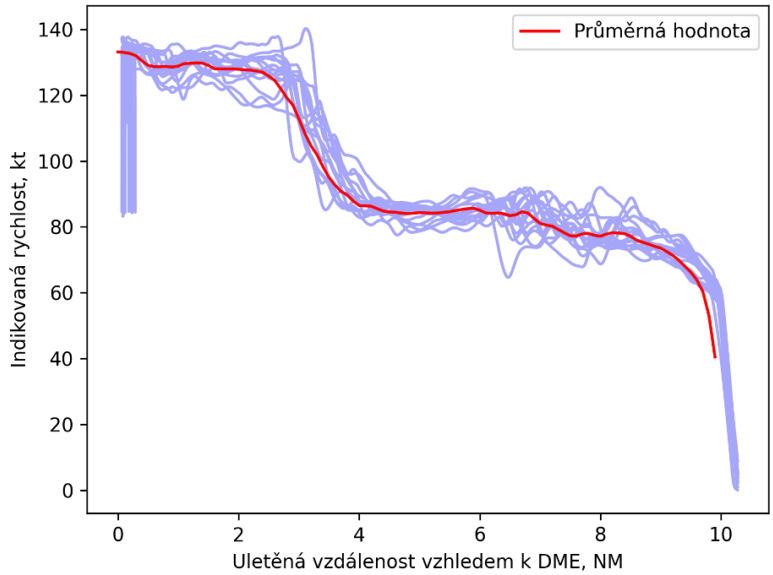
Graf 6 - Vertikální rychlost všech letů během přistání [autor]

Na grafu je vidět, že vertikální rychlosti mezi 140 a 160 sekundami překračují odchylky vertikální rychlosti absolutní hodnoty 1000 stop za minutu. Spočítáme-li průměrnou hodnotu, bude vidět, že je v rámci stanovených hodnot, i když jednotlivé lety tyto hodnoty překročili (viz Graf 7).



Graf 7 - Průměrná vertikální rychlost všech letů [autor]

Také na grafu číslo 5 ke konci osy x (čas) se rychlost každého letu snižuje v různých časech, ačkoli každé letadlo se stejnou počáteční konfigurací přistává a snižuje rychlost přibližně ve stejné vzdálenosti od DME PH. Pokud uděláme graf vzhledem ke vzdálenosti od DME, a ne vzhledem k času, pak uvidíme, že rychlost všech letů současně klesá, což naznačuje, že pomocí tohoto grafu lze některé faktory určit více přesně (viz Graf 8).

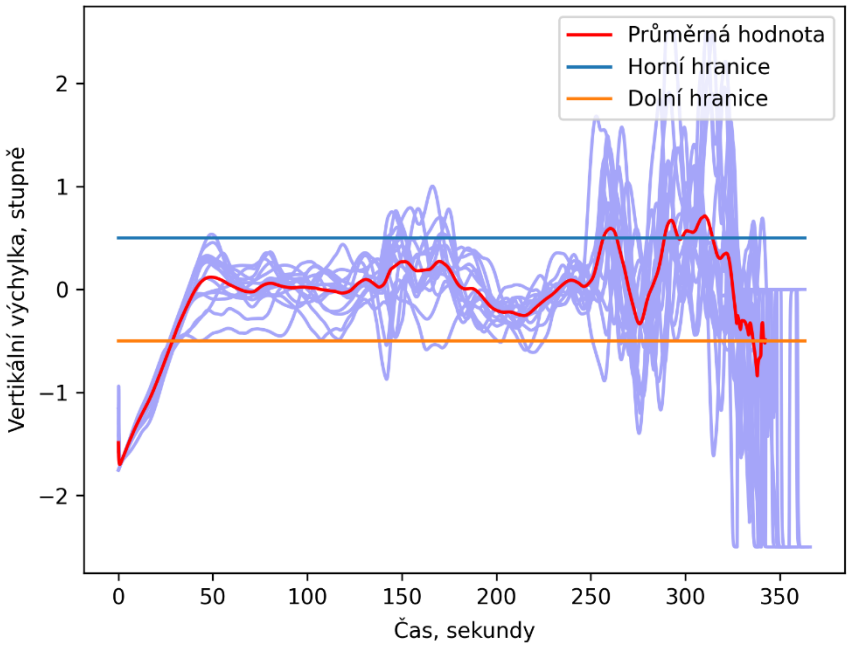


Graf 8 - Průměrná indikovaná rychlost všech letů ve vztahu ke vzdálenosti od DME [autor]

Dále v práci budou grafy používat osu, která více odráží odchylku průměrné hodnoty.

Dále se budeme zabývat grafy souvisejícími s každým z výše uvedených indikatorů.

Protože každý let začal pod rovinou ILS, graf začíná na -1,5 stupni a postupně dosáhuje požadované úrovně. Dále lze pozorovat dva hlavní časové intervaly, kdy odchylky překročí stanovené limity: přibližně po 150 až 260 sekundách. Tyto odchylky jsou spojeny s otevřením vztlakových klapek pro vzlet a vztlakových klapek pro přistání. V dalších grafech bude podobný trend pozorován v překračování stanovených limitů v určitých časových intervalech (viz Graf 9).



Graf 9 - Vertikální odchylka od ILS glideslope [autor]

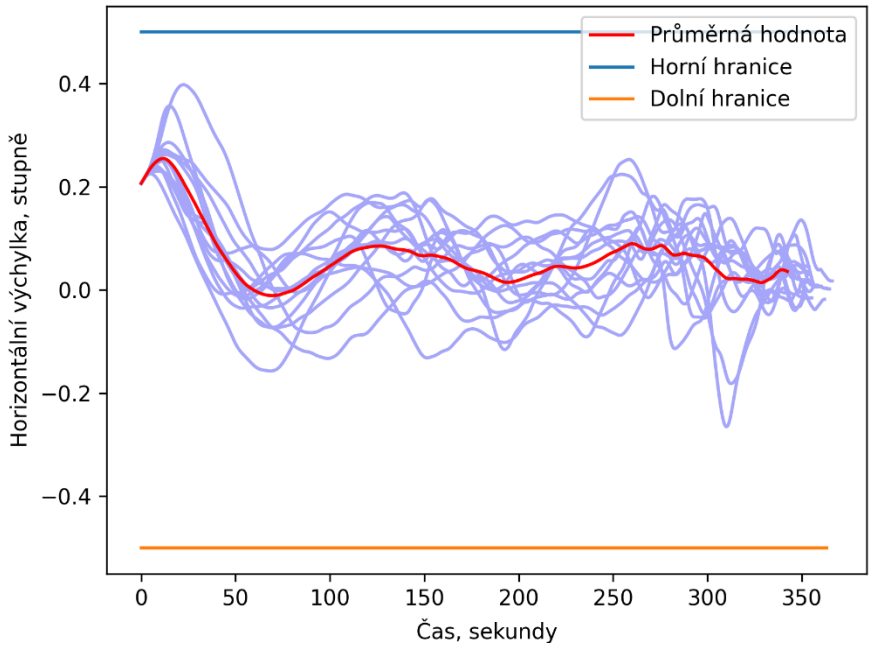
V prvním uvažovaném intervalu se průměrná hodnota pohybovala v požadovaných mezích, jednotlivé lety však tuto hranici překračovaly. Teoreticky lze jako indikátory označit nejen překročení průměrné hodnoty, ale také kvantifikací kolik letů překročilo stanovený limit a kolikrát každý let překročil daný limit, v praxi však tato metoda vyžaduje mnohem více dat a letů pro analýzu, aby bylo možné na základě těchto ukazatelů provést přesné výpočty a vyvodit správné závěry.

Ve druhém časovém intervalu je situace mírně odlišná. Vzhledem k tomu, že pilot je již mnohem blíže k dráze, stejné odchylky, které byly v prvním časovém intervalu, mají mnohem větší amplitudu. Po otevření vztlakových klapek pro přistání je vidět, že letoun nejprve vzlétne nad horní nastavenou mez, pak se pokusí vrátit zpět do požadované roviny. Dále průměrná hodnota opět překračuje horní hranici, což ukazuje na možné zvýšení rychlosti v důsledku klesání, a tato

rychlost zase zvedá letoun nahoru. V důsledku toho vidíme výkyvy na grafu, které je obtížné sladit, protože jsou v těsné blízkosti pásma. V případě takových odchylek při skutečném letu by pilot musel znovu kroužit.

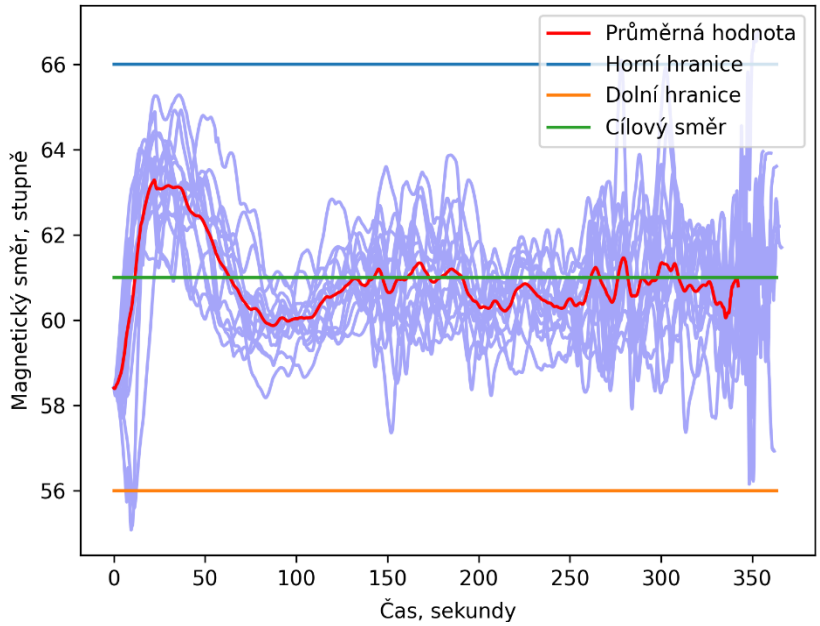
Na konci se průměrná hodnota dostane pod spodní hranici, ale to je již způsobeno tím, že jakmile letadlo přestane chytat signál z ILS, simulátor zaznamená do dat maximální zápornou hodnotu, v tomto případě , -2,5 stupně. Proto lze toto chování pozorovat při každém letu.

V případě horizontální odchylky je vše v pořádku. Po celou dobu letu horizontální odchylka nepřekročila stanovené limity. Jediné, čemu můžeme věnovat pozornost, je začátek grafu: nejprve se hodnota trochu zvýší, pak se vyrovná na požadovanou úroveň. Bylo to z důvodu nepřesnosti výchozí polohy letadla, aby se pilot sám mohl vrátit do požadovaného kurzu a pokračovat v letu (viz Graf 10).



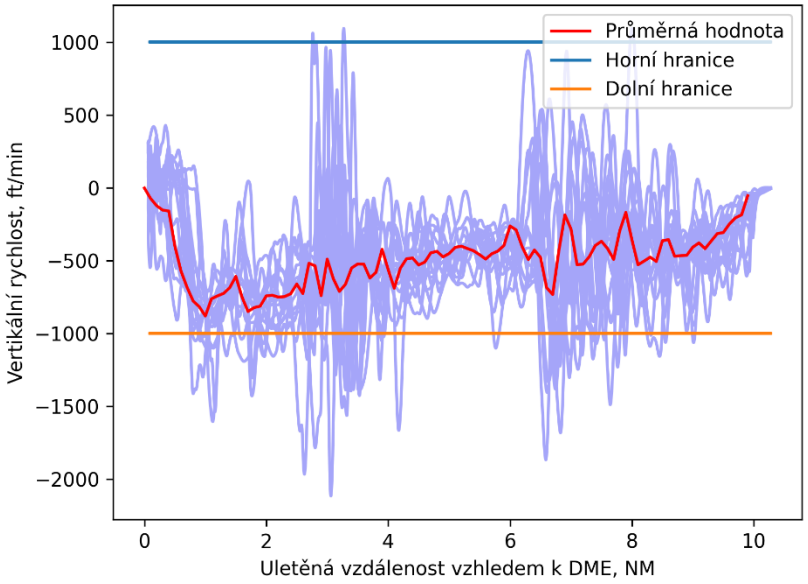
Graf 10 - Horizontální odchylka od ILS glidepath [autor]

Přesně stejné chování lze pozorovat v případě magnetického směru. Zelená barva na grafu označuje magnetický směr dráhy- 61 stupňů, pro relativní srovnání, kde by měla být průměrná hodnota (viz Graf 11).



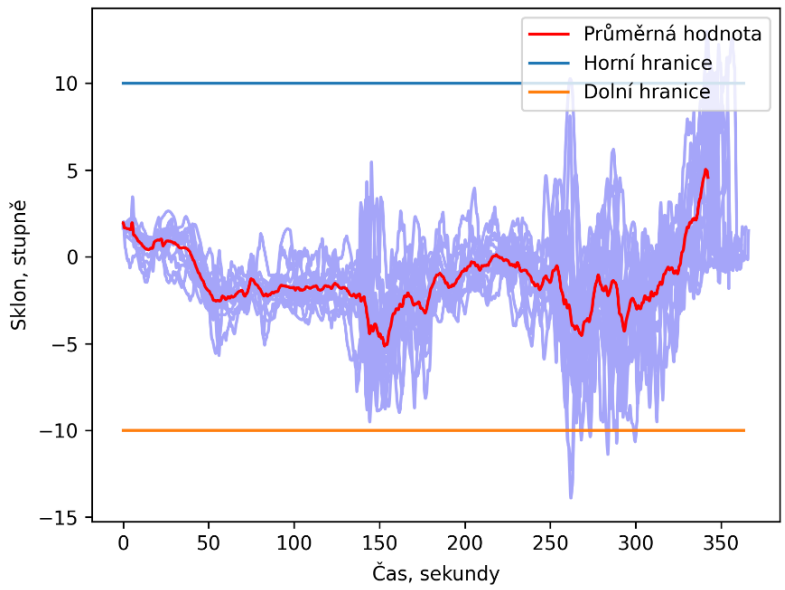
Graf 12 - Průměrný magnetický směr všech letů [autor]

Nyní se podíváme na graf vertikální rychlosti, ale pouze ve vztahu k DME. Již od začátku grafu je vidět, že průměrná hodnota klesá dolů, což souvisí se zahájením klesání. Na celém grafu není mnoho překročení horní hranice, ale mnohem více překročení lze pozorovat ve srovnání s dolní hranicí (viz Graf 12).

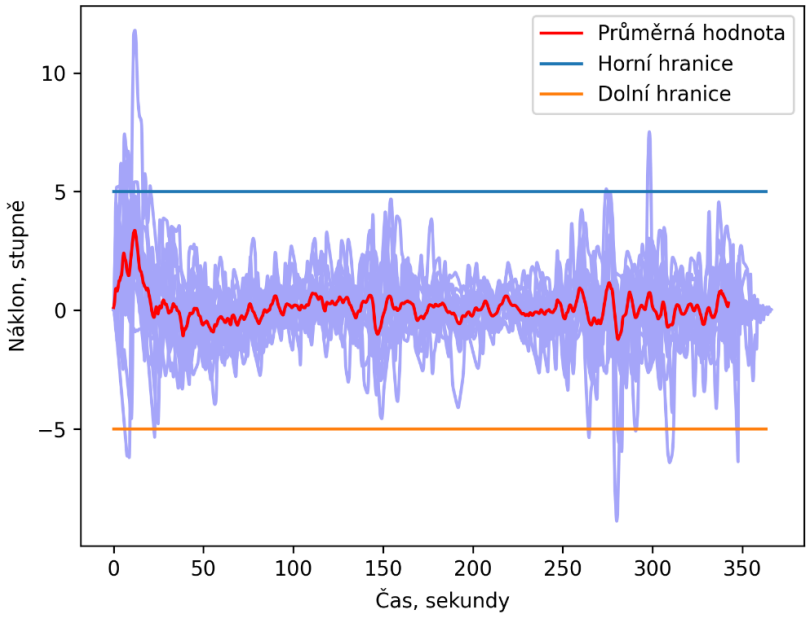


Graf 11 - Průměrná vertikální rychlost všech letů vzhledem k vzdálenosti od DME [autor]

Na grafech sklonu a náklonu jsou odchylky, které překročily hranice,ale jde o jednotlivé lety. Změny náklonu na začátku jsou spojeny s vyrovnáním do požadované dráhy a změny sklonu na konci jsou spojeny s vyrovnáním letadla před přistáním na dráhu. Všechny nadměrné odchylky samozřejmě závisí přímo na hranicích samotných, které by měly být nastaveny v souladu s požadovanými cíli a citlivostí každého grafu na odchylku (viz Graf 13, Graf 14).

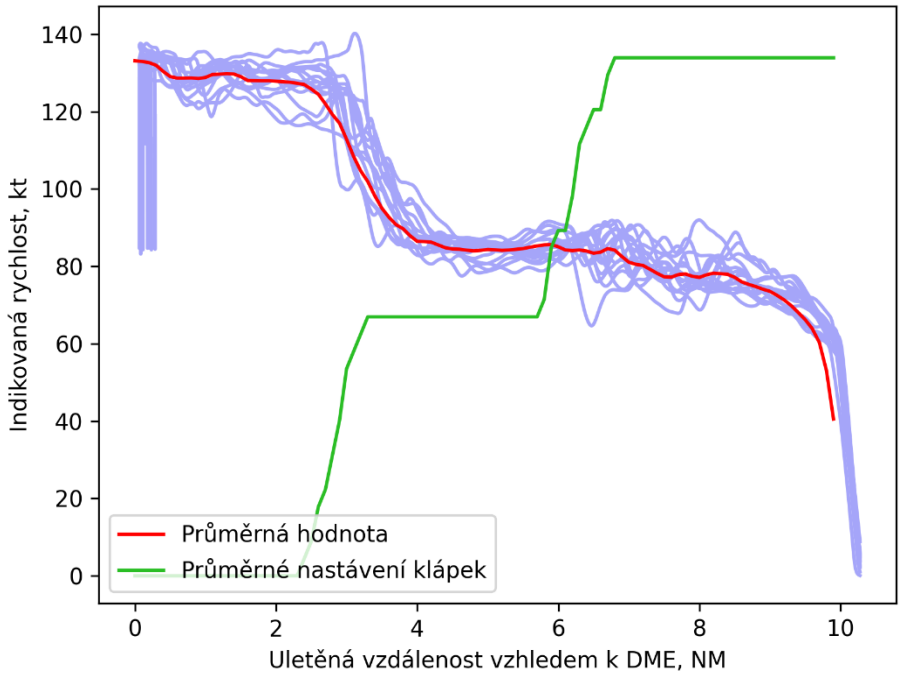


Graf 14 - Průměrný sklon všech letů [autor]



Graf 13 - Průměrný náklon všech letů [autor]

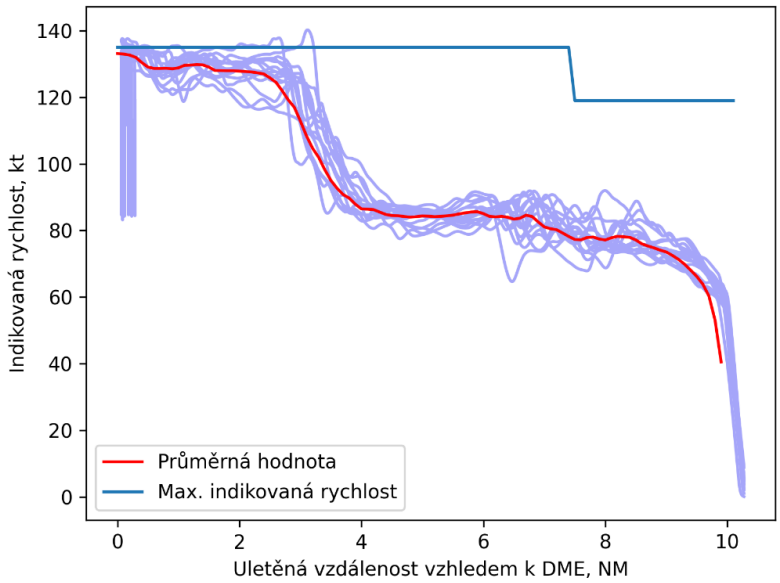
Následující graf ukazuje rychlost spolu s nastavením klapkek. Data vztlakových klapek zaznamenává simulátor v následujícím tvaru: 0 pro zavřenou polohu klapek, 0.5 pro vzletové klapky a 1 pro klapky na přistání. Tento graf byl zvětšen na graf rychlosti, aby bylo možné lépe ukázat, kde a v jakém okamžiku byly klapky použity. Pomocí grafu tedy můžeme vysvětlit pokles rychlosti z přibližně 135 na 85 uzlů (viz Graf 15).



Graf 15 - Indikovaná rychlost a nastavení klapek [autor]

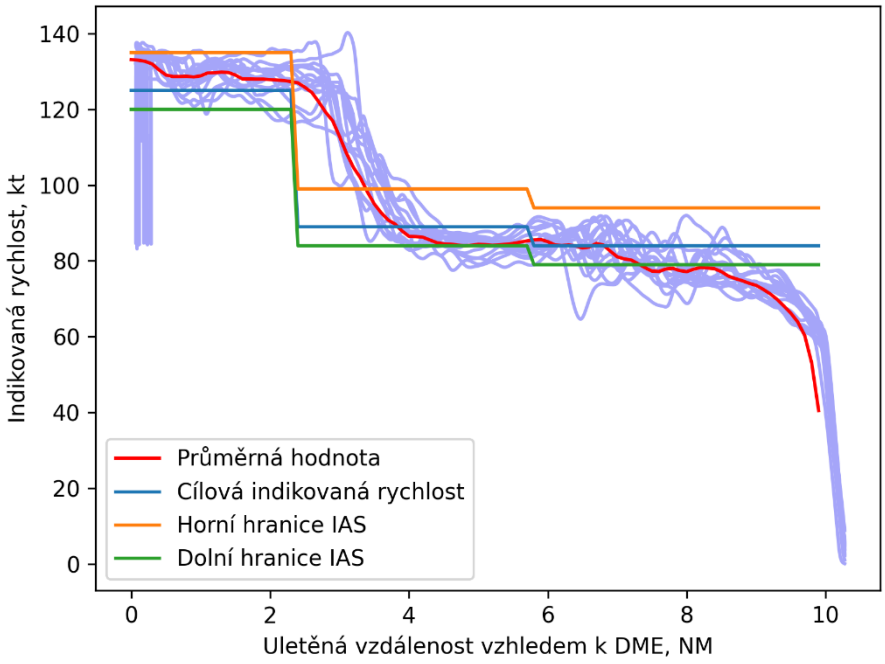
Znáte-li konfiguraci klapek, můžete na základě údajů v letové příručce nastavit maximální rychlostní limity pro kontrolu překročení limitů.

Vzhledem k tomu, že letoun zahajuje let s již vysunutým podvozkem, byl stanoven limit 135 uzlů pro konfiguraci uzavřené klapky a vzletové klapky a 119 uzlů pro konfiguraci přistání. Z grafu je patrné, že v některých případech při otevření vztlakových klapek pro vzlet překročila rychlost maximální nastavenou rychlost, což může být způsobeno úpravou výšky letadla (viz Graf 16).



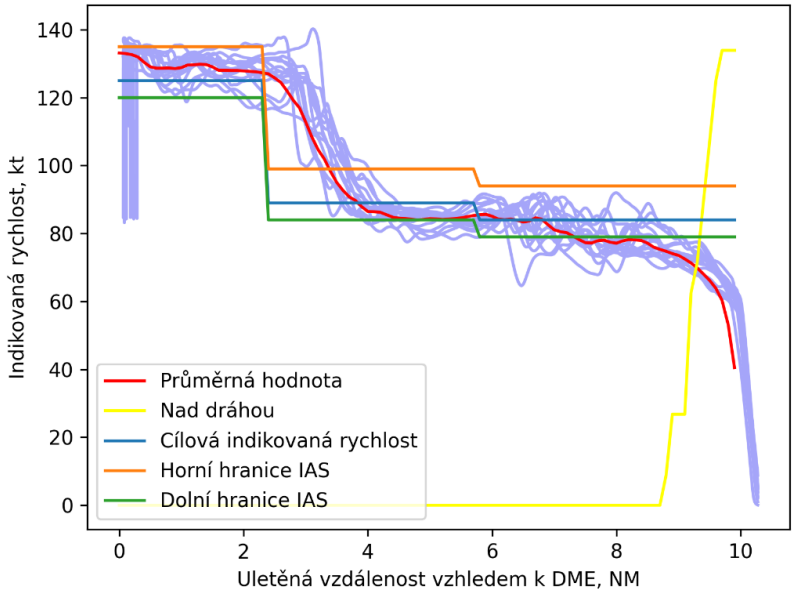
Graf 17 - Indikovaná rychlost a max. indikovaná rychlost na základě konfigurace letadla [autor]

Nyní lze sestavit úplně stejný graf, pouze pro konečnou rychlost přiblížení - V_{ref}, což je 125 uzlů bez klapek, 89 uzlů s klapkami a 84 uzlů bez klapek. Tento graf ukazuje, že před otevřením posledních vztlakových klapek klesá průměrná rychlost pod minimální mez, což naznačuje, že se pilot snaží s předstihem zpomalit letadlo, aby snížil vliv otevření posledních vztlakových klapek na správnou výšku letu (viz Graf 17).



Graf 16 - Indikovaná rychlost a grafy Vref, Vref+10 kt., Vref-5 kt [autor]

Na konci grafu také rychlost klesá pod minimální hranici. Protože však v tomto okamžiku již pilot může vyrovnávat letadlo, aby zpomalilo, bylo by správné uvést na grafu ještě jeden parametr, který by indikoval, zda je letadlo nad dráhou nebo ne (viz Graf 18).

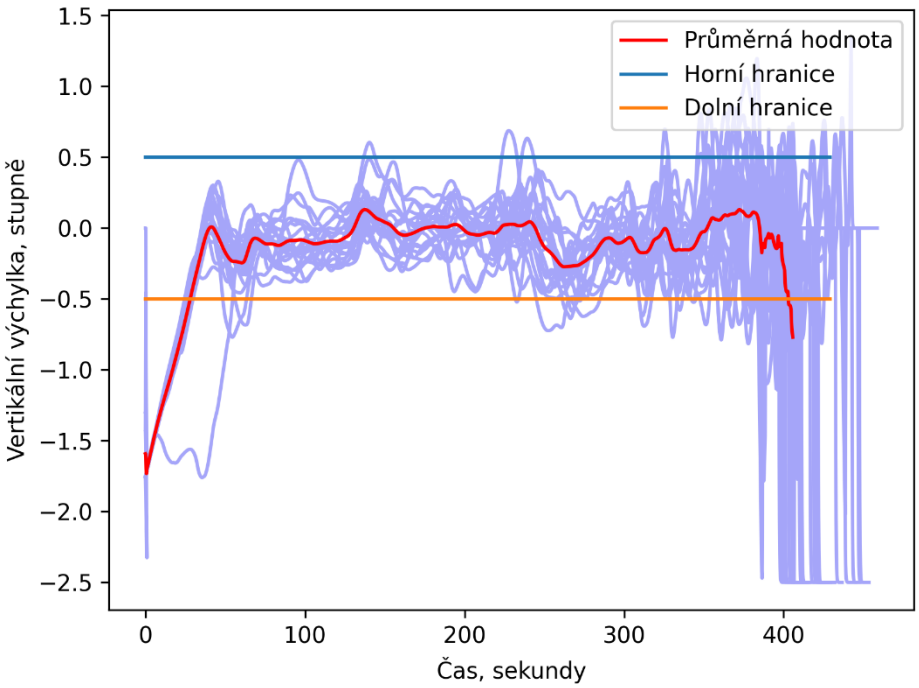


Graf 18 - Indikovaná rychlost a grafy Vref, Vref+10 kt., Vref-5 kt, a označení letadla nad dráhou [autor]

Tento parametr je zapsán jako logická jednička a má tedy 2 hodnoty: 0 nebo 1. Na grafu byl také pro lepší vizualizaci zaznamenán na svou maximální rychlost a své maximální hodnoty dosahuje postupně, protože graf ukazuje průměr hodnot všech letů.

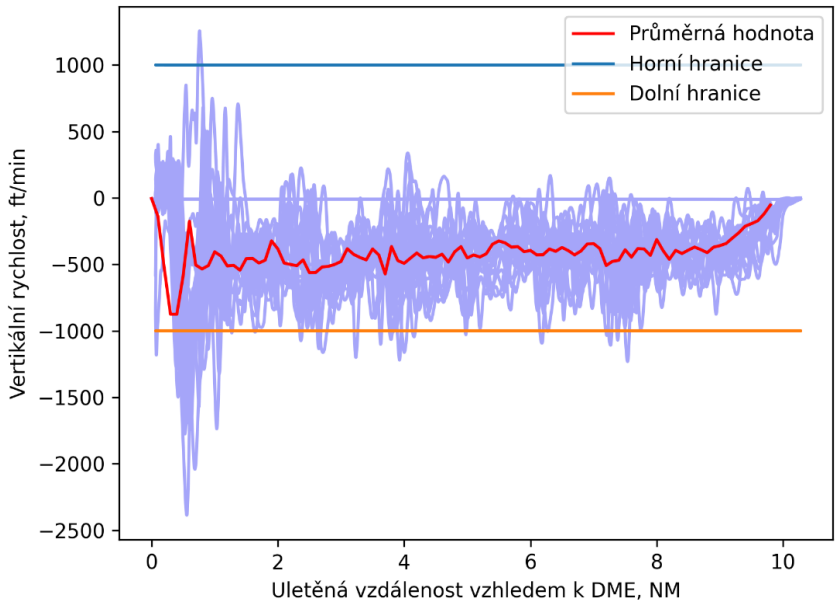
Dva hlavní indikátory, které byly aktivovány během analýzy, jsou vertikální rychlost a vertikální odchylka od ILS. Na základě toho, že tyto 2 indikátory byly aktivovány, bylo stanoveno, že to bylo způsobeno nedostatkem času a vzdálenosti na stabilizaci letadla během přiblížení. K tomu byla přijata zmírňující opatření: klapky by se měly otevřít dříve, aby bylo více času na stabilizaci letadla. Dále bylo provedeno 20 letů s přesně stejnou počáteční konfigurací, ale byly otevřeny první klapky ve vzdálenosti 8 námořních mil od DME PH a druhé klapky ve vzdálenosti 4 námořních mil od DME. Další analýza těchto letů pomůže pochopit, zda naše preventivní opatření pomohlo zlepšit bezpečnost celého systému.

Při porovnání tohoto grafu s grafem číslo 9 ukazuje tento graf, že průměrná hodnota vertikální odchylky již nepřekračuje stanovené limity, nicméně ke konci grafu je pozorováno, že při některých letech bylo letadlo stále nad, resp. pod stanoveným limitem. To znamená, že ačkoli zavedené změny pravidel pomohly v průměru lépe stabilizovat letadlo při přistání, stále existuje prostor pro další vylepšení (viz Graf 19).



Graf 20 - Vertikální odchylka od ILS glideslope po úpravě pravidel otevírání klapek [autor]

Podobnou situaci lze pozorovat u vertikální rychlosti. Počáteční kolísání vertikální rychlosti je způsobeno tím, že letoun začal klesat přibližně ve vzdálenosti 9 námořních mil a okamžitě došlo k otevření klapek ve výšce 8 námořních mil, což si vyžádalo reakci letounu v podobě překročení stanovených limitů. Po další analýze grafu je však průměrná hodnota v mezích a pouze některé lety překračují spodní hranici vertikální rychlosti (viz Graf 20).



Graf 19 - Průměrná vertikální rychlost všech letů po úpravě pravidel otevírání klapek [autor]

Analýza zbytku grafů a parametrů neodhalila žádné změny, tudiž nebudou v práci dále rozebrány.

6.4.4 Statistické ověření

Abychom potvrdili správnost výše uvedených oprav letadla na přiblížení, je možné statisticky potvrdit zlepšení analyzovaných parametrů. K tomu musíme nastavit indikátory, pomocí kterých určíme, jak stabilní je let, například:

- Kolikrát každý let překročil stanovenou hranici;
- Jaké procento letů překročilo stanovenou hranici alespoň jednou;
- Jak dlouho bylo letadlo mimo stanovenou hranici;
- Jaká je odchylka průměrné hodnoty od požadované hodnoty (například rychlosti letadla);
- Jak velká je směrodatná odchylka každého letu.

Dále bude zvážen a analyzován poslední bod na příkladu vertikální rychlosti a vertikální odchylky od ILS, avšak zbytek indikátorů lze analyzovat stejným způsobem. Všechny dále specifikované příkazy a všechny analýzy budou provedeny v Matlabu.

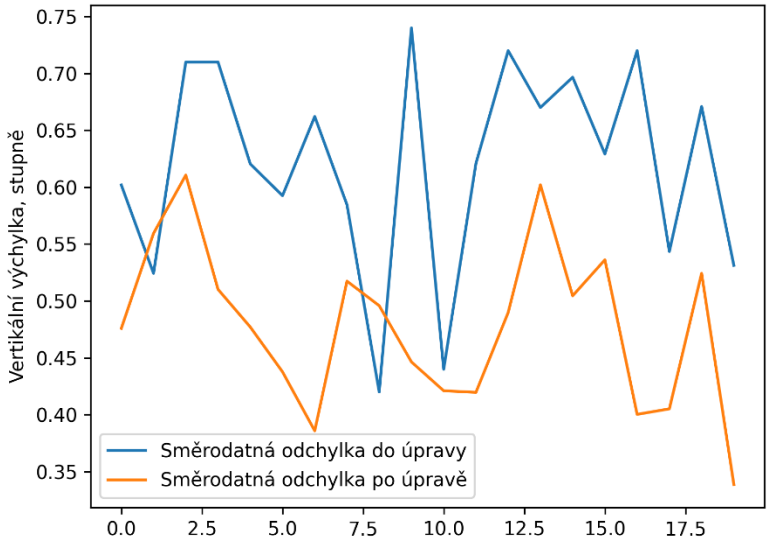
Pro začátek byla pro každý ze 40 uskutečněných letů vypočtena směrodatná odchylka (viz Obrázek 32).

```
notCorrectedData = [0.6 0.52 0.69 0.71  0.62 0.59 0.66 0.58 0.42 0.74
                    0.44 0.62 0.72 0.67 0.70 0.63 0.72 0.54 0.67 0.53];
   correctedData = [0.47 0.55 0.61 0.51 0.47 0.43 0.38 0.51 0.49 0.44
                    0.42 0.41 0.48 0.60 0.50 0.53 0.40 0.40 0.52 0.33];
```

Obrázek 32 - Snímek obrazovky z Matlabu: Směrodatná odchylka vertikální odchylky letadla od ILS před a po korekci zavedené do postupů při přistání [autor]

Poznámka: pro snazší a srozumitelnější vizualizaci byla data zaznamenaná v této tabulce zaokrouhlena na 2 desetinná místa, protože skutečná data vypsala hodnoty s 20 a více desetinnými místy.

Dále, abychom určili, který příkaz chceme použít k analýze dat, musíme nejprve analyzovat obě datové sady pro normální rozdělení pomocí příkazu adtest(x), který představuje Andersonův-Darlingův test. Pokud je p-hodnota alespoň z jednoho testu menší než 0.05, bude třeba použít Mann-Whitneyův test, jinak bude vhodné použít dvouvýběrový t-test – příkaz `ttest2(x)` (viz Graf 21).



Graf 21 - Grafické zobrazení směrodatných odchylek vertikálních odchylek letadla od ILS [autor]

p - hodnoty obou testů vyšly 1 a 0.3027, což znamená, že můžeme říci, že nezamítáme předpoklad normality dat, a můžeme použít dvouvýběrový t-test.

Předpokládáme, že po opravě pravidel pro přistání letadla je rozptyl dat menší než dříve. Pokud tedy v testu nejprve zadáme proměnnou *correctedData* a poté proměnnou *notCorrectedData*, budeme muset použít pravostranný test ke kontrole našeho původního tvrzení.

Test ukázal p-hodnotu 1, která je větší než 0.05, což znamená, že rozptyl v datech po opravě pravidel přistání je skutečně menší, což ukazuje na stabilnější let.

Nyní otestujme naši hypotézu o stabilnějším přiblížení na vertikální rychlosti letadla (viz Obrázek 33).

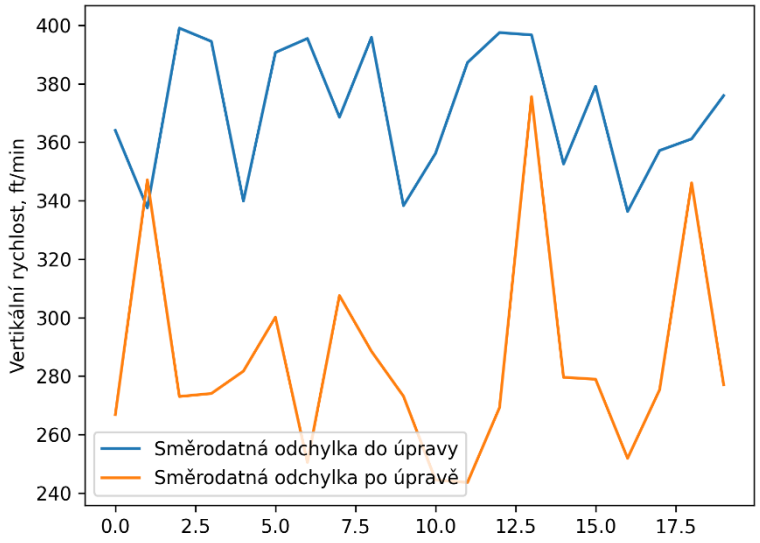
```
notCorrectedData = [364.03 337.53 399.02 394.48 339.88 390.68 395.47 368.56 395.88 338.28
                    356.15 387.25 397.49 396.69 352.54 379.13 336.30 357.16 361.13 375.94];
   correctedData = [266.83 347.11 273.01 274.04 281.68 300.14 250.48 307.54 288.46 273.10
                    244.47 243.62 269.22 375.57 279.57 278.92 251.87 275.31 346.09 277.05];
```

Obrázek 33 - Snímek obrazovky z Matlabu: Směrodatná odchylka vertikální rychlosti letadla před a po korekci zavedené do postupů při přistání [autor]

Poznámka: pro snazší a srozumitelnější vizualizaci byla data zaznamenaná v této tabulce zaokrouhlena na 2 desetinná místa, protože skutečná data vypsala hodnoty s 20 a více desetinnými místy.

Při provedení Anderson-Darlingova testu p - hodnoty obou testů vyšly 0.003 a 0.0501, což znamená, že tentokrát zamítáme předpoklad normality dat, a musíme použít Mann-Whitneyův test.

Mann-Whitneyův test ukázal p-hodnotu 1, která je větší než 0.05, což znamená, že rozptyl v datech po opravě pravidel přistání je skutečně menší, což ukazuje na stabilnější let (viz Graf 22).



Graf 22 - Grafické zobrazení směrodatných odchylek vertikální rychlosti letadla [autor]

7 Aplikace Active STPA analýzy

V předchozí kapitole jsem na vzorku dat ilustroval, jakým způsobem pracovat s daty z běžného provozu a jak v navrženém modelu neustálé integrace dat pracovat s indikátory jako spouštěči analýzy Active STPA. Při následné realizaci všech kroků Active STPA po jejím spuštění dojde k aktualizaci původní prediktivní analýzy STPA, čímž posouváme bezpečnostní přístup na novou úroveň. [7]

Ačkoliv těžiště této práce leží v návrhu práce s daty jako spouštěči analýzy při jejich kontinuálním toku z každého realizovaného procesu, pro řízení bezpečnosti je důležité následně realizovat všechny kroky Active STPA.

V této kapitole projdu následné kroky analýzy Active STPA po jejím spuštění při překročení indikátoru. Jednotlivé odstavce popíší kroky analýzy z teoretického pohledu i jak by měly vypadat při realizaci do praxe. Postupně bude popsána celá integrace dat do původní prediktivní studie.

7.1 1. krok - Kontrola STPA analýzy

7.1.1 Hledání aplikovatelných pravidel a postupů

Prvním krokem při revizi STPA analýzy je nutné určit dotčená místa v systému. Při hledání možného zdroje problémů věnujeme pozornost tomu, jaká pravidla a postupy měly zajistit bezpečnost v oblasti kontrolované překročeným indikátorem a zda vůbec takové postupy existují. Pokud postupy pro zajištění bezpečnosti existují, je třeba zjistit, z jakého důvodu nebyly efektivní.

Pokud má dojít k rozšíření sady indikátorů o nový, je třeba jej propojit s příslušným bezpečnostním omezení.

V našem příkladu lze všechny indikátory, které se používají pro bezpečnostní omezení číslo 1 (viz Příloha B), propojit s kontrolními postupy, které piloti dělají před a během procesu přiblížení. V případě aktivace indikátorů je potřeba zkoumat, zda řídicí, tedy piloti, dodrželi všechny kontrolní postupy, a případně je dále analyzovat po stránce efektivity.

Výstupem by mělo být určení neúčinných opatření, nebo opatření, která chyběla v původní STPA analýze. Nekompletnost původní STPA analýzy lze vysvětlit chybou v původní studii, či změnou v systému realizovanou v době po dokončení STPA analýzy.

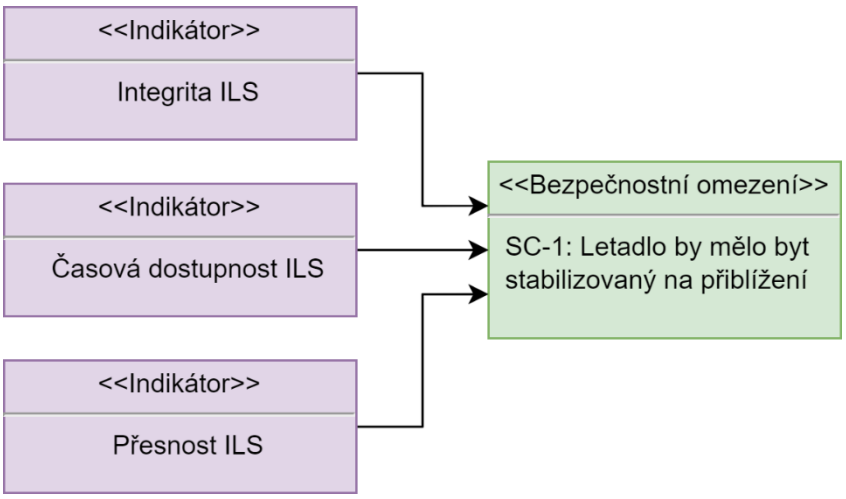
7.1.2 Ověření požadavků a omezení

Cílem použití STPA analýzy je identifikovat bezpečnostní omezení, která vstupují do systému jako omezení, která mají zabránit danému nebezpečí a jak by mohla být porušena. Výstupem má být označení neúčinných a doplnění chybějících omezení.

Při integraci dat jsou každému bezpečnostnímu omezení přiřazeny indikátory, které mají ilustrovat, zda je toto bezpečnostní omezení porušováno či nikoli. Integrace dat může pomoci, pokud jsou aktivovány indikátory pro bezpečnostní omezení, ale dále nevede k porušení bezpečnostních omezení u žádného letu. V takovém případě to může znamenat, že samotná bezpečnostní omezení nebo indikátory byly vytvořeny chybně. Stejně tak lze uvažovat i o opačné situaci: pokud dojde například k porušení bezpečnostního omezení, ke kterému nejsou přiřazeny aktivované indikátory, pak to znamená, že problém může být jak v indikátorech samotných, tak

v jejich vztahu k bezpečnostnímu omezení, které by mělo být zváženo při dalším řešení systémových změn.¨

Praktickou aplikací tohoto kroku v řešeném příkladu pro případ přistání letadla závisí informace o poloze letadla od ILS nejen na přístrojích samotného letadla, ale také na provozuschopnosti tohoto systému jako součásti infrastruktury letišť, které by mělo být neustále monitorováno. Díky tomu, že se objeví nový prvek, se v systému objeví nové indikátory a okamžitě pochopíme, že bezpečnostní omezení spojené s novým prvkem již není dostačující a bude vyžadovat aktualizaci v následujících krocích. V našem příkladu by takovými indikátory mohla být dostupnost, přesnost a integrita ILS (viz Obrázek 34).



Obrázek 34 - Nové indikátory systému objevené jako výsledek Active STPA [autor]

Zajímavostí tohoto příkladu je skutečnost, že přidaný prvek je součástí infrastruktury letiště a je to právě letiště, které musí zajistit správný provoz tohoto prvku pro zajištění bezpečnosti.

7.1.3 Ověření kazuálních scénářů

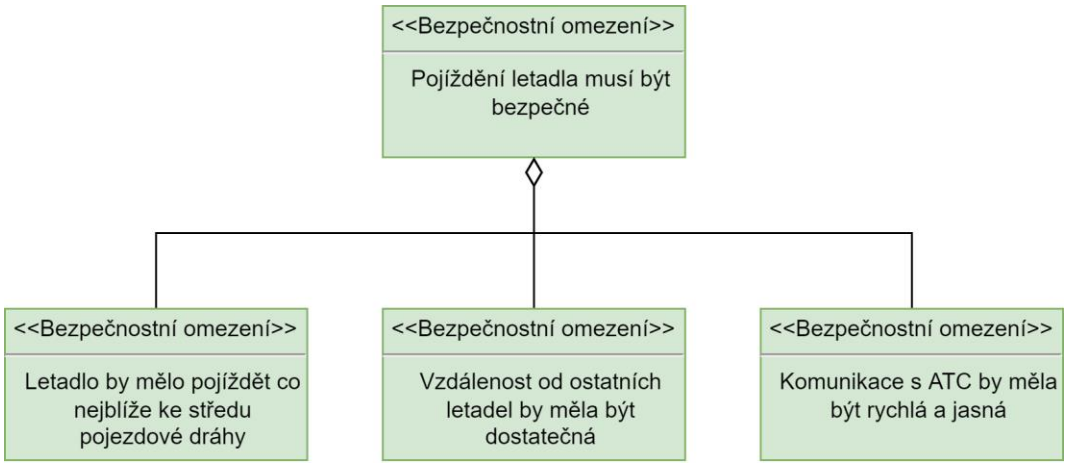
V tomto kroku analýzy dochází k revizi kauzálních scénářů. Pokud se v současném stavu systému objevuje nová nebezpečná řídicí akce, studujeme, z jakého důvodu takový scénář v původní studii chyběl. Dle charakteru kroku lze usuzovat, že tato část analýzy se výrazněji uplatní, pokud je analýza Active STPA spuštěna jako reakce na konkrétní incident.

Zajímavou úvahou je potřebná míra detailu při stanovování kauzálních scénářů. Při obecné kontrole scénářů představených v analýze bude přirozené pokusit se vytvořit univerzální scénář, který by pokrýval všechny procesy. Například proces přistání letadla jako celek je poměrně velký a zahrnuje množství podprocesů. Pro nás by to znamenalo, že všechny dostupné indikátory přiřadíme pouze jednomu scénáři, což ztěžuje další podrobnější analýzu, protože by bylo obtížné

sledovat, co přesně porušení procesu obnáší. Integrace dat nám umožňuje věnovat pozornost všem scénářům, pokud jde o to, kolik indikátorů je celkově přiřazeno danému bezpečnostnímu omezení. Pokud existuje pouze jeden ukazatel, pak takový proces může být součástí nějakého jiného procesu, ale pokud má jeden proces mnoho ukazatelů, je vhodné rozdělit je do podprocesů.

Jako příklad můžeme analyzovat proces pojíždění letadla po přistání. Nejjednodušším přístupem by bylo vytvořit jedno bezpečnostní omezení, které pokryje celý proces, jako „Pojíždění letadla musí být bezpečné“. Takové bezpečnostní omezení však zahrnuje spoustu elementů, jako řídicí vstupují do procesu a samotná posádka letadla, tak dále posádky jiných pojíždějících letadel, dispečeři řízení letového prostoru koordinující daný sektor pro pojíždění, pracovníci letištní složky kontrolující provozuschopnost dráhy a další letištní infrastruktury; kromě těchto řídicích v podobě lidského činitele dále také prvky jako samotná letištní infrastruktura, technologie a další.

V tomto případě integrace dat pomůže pochopit, že takové bezpečnostní omezení je vhodné rozdělit do několika přesnějších, protože danému bezpečnostnímu omezení bylo přiřazeno velké množství parametrů. Pokud je takové bezpečnostní omezení rozloženo na přesnější, jako například „Letadlo musí pojíždět co nejblíže ke středu pojezdové dráhy“, „Vzdálenost od ostatních letadel by měla být dostatečná“, „Vzdálenost od letištních objektů by měla být dostatečná“ a „Komunikace s ATC by měla být rychlá a jasná", pak bude mnohem snazší vytvořit ochrany pro každé z těchto bezpečnostních omezení v následujících krocích analýzy (viz Obrázek 35).

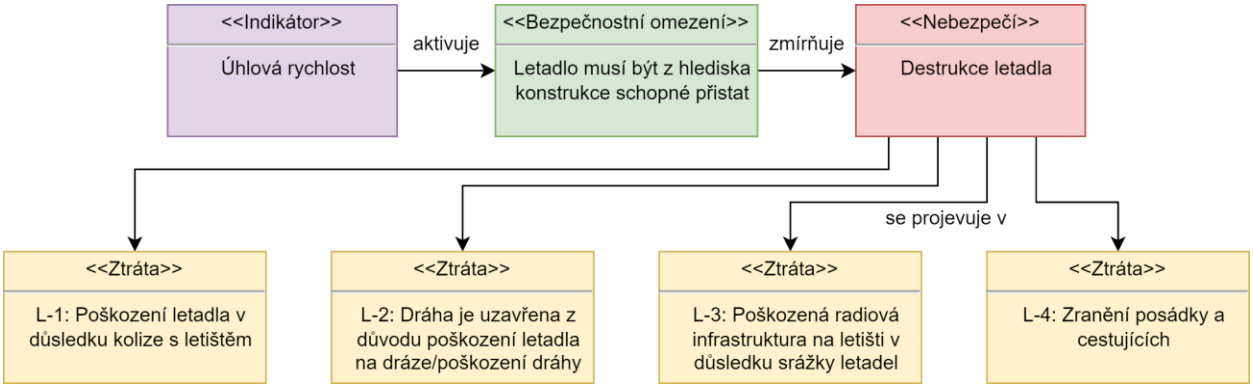


Obrázek 35 - Rozdělení obecného bezpečnostního omezení na přesnější [autor]

Jednou z možných kontrol, zda byly vytvořeny všechny možné scénáře, je zohlednit vazby s indikátory, konkrétně se zaměřit na nezapojené indikátory. Pokud se měří nějaký indikátor, který však není konkrétně navázán, pak pokud si představíme aktivaci tohoto indikátoru, můžete

pochopit, k jakému scénáři může realizace vést, a podle toho navrhnout nový scénář pro doplnění analýzy.

Jedním z takových parametrů v prováděné analýze je úhlová rychlost. Překročení tohoto parametru může vést k trvalé deformaci křídel letadla, což může mít velmi kritický vliv na proces přistání letadla. Takové události jsou často ignorovány z důvodu velmi nízké pravděpodobnosti, nicméně v případě integrace dat bude tvorba nových indikátorů v budoucnu fungovat automaticky, takže je nutné provést jejich doplnění do analýzy (viz Obrázek 36).



Obrázek 36 - Objevení nového bezpečnostního omezení kvůli nepoužítému indikátoru [autor]

Můžeme také vytvořit indikátory založené na existujících indikátorech, což nám umožní lépe předvídat možnosti výskytu jakékoli nejistoty v systému. Přestože jsou všechny ukazatele nejčastěji nahlíženy ve vztahu k času, v některých situacích může být užitečné uvažovat ve vztahu k jiné veličině, podle toho, ke kterému parametru chceme tento proces relativně sledovat. Tímto způsobem lze sledovat parametry vzhledem k nadmořské výšce nebo vzdálenosti od radionavigačních zařízení (viz Graf 8, Graf 12).

7.1.4 Ověření řídících akcí a nebezpečných řídících akcí

Tento krok analýzy se zaměřuje na řídicí prvky v systému a jejich zodpovědnosti v rámci daných řídicích akcí, dále pak na vzájemné vazby mezi prvky a jejich dopady na systém.

Vzhledem k obrovskému množství parametrů je velmi obtížné celý model neustále udržovat, proto je vždy celý proces popsán např. stoupání nebo klesání. Takový proces lze snadno popsat, nicméně v případě porušení bezpečnostních omezení bude obtížné s takovou definicí procesu dále pracovat při hledání konkrétnější příčiny. Není možné změřit všechna data v kokpitu letadla, například jak je uvedeno v dizertační práci o Active STPA, pokud pilot nejprve změnit výšku sedadla a opraví ji až při konečném přiblížení, pak se může jednat o nebezpečnou akci. [7] Pokud se však k popisu procesu přistupuje z hlediska integrace dat, pak se zvažování všech konečných

nebezpečných akcí stává zcela reálným vzhledem k tomu, že každá nebezpečná akce je uložena v důsledku aktivace určitých indikátorů, a možná v určitém pořadí. Chceme-li to provést, musíme věnovat pozornost tomu, kdy přesně jsou indikátory procesu aktivovány, a ptát se, proč došlo k jejich aktivaci. Pokud by obecný scénář vypadal takto: pilot vyrovnal výšku sedadla, to vedlo k prudkému pohybu v kokpitu a nárazu na řízení letadla a odchylce od ILS, pak by bylo možné tento vzorec zjištěných odchylek vysledovat obráceně. Pro bezpečnostního manažera by tok přidání nového procesu vypadal takto:

- ➔ Proč byl indikátor aktivovan? Protože pilot omylem dotkl nebo se opřel o ovládání letadla.
- ➔ Proč se to stálo? Pilot letěl v hladině, s konstantní rychlosti, nebyly zjištěny žádné další indikátory, takže se dá předpokládat, že se tak stalo náhodou.
- ➔ Co mohlo k tomu přivést? Uprava výšky sedadla během přiblížení.

Ačkoliv nelze měřit a pokrýt všechny parametry (např. výšku sedadla), dle mého názoru v budoucnu by při potřebném vývoji a podpoře takové aplikace bylo možné pokrýt zhruba 70-80 procent všech možných situaci.

Aby bylo možné vytvořit základ pro tento krok nebo v této fázi umožnit integraci dat, která podpoří další identifikaci možných nebezpečných řídicích akcí, je vhodné nejprve přemýšlet o tom, jaké další možné parametry o letu by mohly být užitečné, a na základě toho pokračovat v analýze.

Automatické navrhování nápadů z programu ohledně porušených řídících smyček však může způsobit, že sám manažer situaci nezvažuje, ale prostě se spoléhá na výsledky programu. V takovém případě bude nutné ujasnit si správný způsob použití takového programu, kdy nejprve bude muset manažer dojít k vlastním závěrům, podívat se na závěry programu, porovnat a pochopit, proč neměl závěry, které program obdržel, a naopak. Program tak lze pravidelně doplňovat a rozšiřovat jeho funkčnost o znalosti a dovednosti manažera.

Pro vytvoření objektivní databáze pro program je také nutné využít a doplnit znalosti několika bezpečnostních manažerů, což by mohlo výrazně zvýšit efektivitu programu.

7.1.5 Ověření řídících vztahů ve struktuře řízení bezpečnosti

V tomto kroku analyzujeme všechny řídicí prvky v našem systému a provedeme rovněž analýzu z pohledu hierarchie řízení. Možná pomoc při integraci může záviset na tom, zda jsou pro řídící prvky k dispozici nějaká data pro jeho elementy. Na procesu přistání letadla máme potřebné parametry: proces přistání letadla, pro který máme ukazatele výšky, rychlosti letadla a další parametry, dále máme údaje o odchylkách při řízení letadla v každé z os . V programu je tedy

možné napsat test, který by prověřil, zda takové spojení u každého letu funguje či nikoliv. Během analýzy je však nezbytné prověřit všechny úrovně řízení a tam, kde je to relevantní zjistit, zda k odchylce dochází vlivem řízení posádkou letadla, nebo vlivem řízení dispečerem řízení letového provozu, respektive následováním pokynů z této úrovně řízení.

Příkladem takového jednoduchého testu může být, že když se letadlo nakloní, očekáváme, že se změní jeho magnetický směr, nebo když letadlo otevře klapky, pak se zpomalí.

7.1.6 Ověření požadavků a omezení na systémové úrovni

Z pohledu bezpečnosti je klíčové ošetřit důležité změny v systému, ke kterým došlo až po provedení původní bezpečnostní studie. Porušení požadavků a omezení na systémové úrovni by pravděpodobně vedlo ke ztrátě.

Častým důvodem k přehodnocení bezpečnostního omezení je přidání nového prvku do systému, kterým by v našem procesu přistání letadla mohlo být nové vybavení v letadle. K integraci dat v této části lze využít metadata, jinými slovy, data o datech. Příkladem metadat mohou být informace o tom, kdy se konkrétní data objevila, kolik z nich a jak se používají v modelu integrace dat. [33] Nové prvky v systému nejčastěji vedou k vytvoření nových indikátorů. Pro pochopení relevance vytvořených omezení na úrovni systému je možné se podívat na to, jak dlouho byly některé prvky přidány do obecné analýzy, kdy byly přidány indikátory a s jakým časovým rozdílem. Je tedy možné vyhodnotit systém na úrovni těch dostupných dat, ke kterým byl přístup dříve a ke kterým je přístup teď, a na základě toho vyvozovat závěry o relevanci prvků v celkovém systému. Protože Active STPA přináší neustálé přizpůsobování analýzy stávajícím podmínkám, parametry a ukazatele, které lze použít, by měly byt přizpůsobený stejným způsobem.

7.1.7 Ověření nebezpečí a ztrár

V této fázi můžeme integrovaná data použít také k nalezení skrytých nebo dosud nezjištěných nebezpečí a ztrát. K tomu je třeba se podívat na data a přemýšlet, co by se mohlo stát, kdyby byl některý z indikátorů aktivován z důvodu překročení povolené hodnoty. Úvaha pokračuje vyvozením, co by pro systém znamenala aktivace více indikátorů současně. Kombinace těchto parametrů lze volit tak, aby se vytvořilo co nejvíce možných scénářů ztrát a nebezpečí. Například ve zde řešené analýze nebyla původně uvažována úhlová rychlost náklonu letadla. K systému lze rovnou dodat, že při překročení této hodnoty může dojít k vysokému zatížení křídla (příklad nebezpečí), což pak může vést k deformaci křídla (ztrátě). Vzhledem k tomu, že nebyly využity

všechny zaznamenané parametry z letů, je možné projít všechny nepoužívané parametry a na jejich základě vytvořit nové nebezpečí a hrozby na systémové úrovni.

7.2 2. krok - Důvod porušení předpokladů

7.2.1 Nalezení porušených předpokladů

Základním cílem této části analýzy je zjistit, proč řídicí prvek porušil stanovené postupy. Jakékoli předpoklady nejčastěji představují nějaké tvrzení, na jehož základě byl postaven další model. Pro integraci dat v této fázi je nutné ke každému předpokladu ve fázi tvorby STPA analýzy přiřadit nějaké logické pravidlo, které by bylo možné pomocí programu popsat a které by odráželo naše očekávání od systému, a jak vidíme chování systému jako celku. Například při přistání, v případě destabilizace letadla a zvýšení rychlosti letadla, můžeme určit, že budeme očekávat buď zvýšení výchylky kormidla ze strany pilota, aby se kompenzoval dodatečný vztlak generovaný letadlem, popř. zvýšení výšky samotného letadla. V případě, že nebylo následováno žádné z předem stanovených pravidel, lze tvrdit, že byly vytvořené předpoklady porušeny. V takových případech je důležité pochopit, proč k porušení došlo. Je možné, že vytvořená pravidla nebyla správná a vyžadují úpravy. Na datech lze snadno pozorovat, zda k porušení dochází opakovaně.

7.2.2 Analýza trendů

Analýza trendů je část, kde je integrace dat velmi vhodná a její realizace bude mít zásadní přínos. Dobře napsaný program bude na vyžádaní schopen okamžitě zobrazit všechny podobné incidenty na obrazovce se všemi potřebnými údaji, které pomohou zjistit, proč došlo ke konkrétnímu incidentu. Hlavní výhodou datové integrace je to, že zatímco současný přístup zohlední staré podobné incidenty až poté, co k aktuálnímu incidentu již došlo, integrace dat do zabezpečení okamžitě identifikuje jakékoli porušení parametrů a předem upozorní na možné trendy. Například: pokud se během přistání letadla postupně prodlužuje požadovaná délka pro úplné zastavení, může to již znamenat, že v systému existuje nějaká hrozba, kterou je třeba detekovat a je třeba vytvořit potřebné ochrany, které realizaci hrozby zabrání. Jedním takovým příkladem by bylo postupné nahromadění pryže na dráze, které snižuje účinnost brzd letadla.

7.2.3 Výzkum kazuálních a přispívajících faktorů

Vzhledem k tomu, že všechny složité systémy mají mnoho faktorů, tento krok implikuje zahrnutí všech faktorů do analýzy. Základem je, že analyzujeme vazby mezi konkrétní nebezpečnou kontrolní akcí a kauzálními faktory a hodnotíme možný vliv kauzálních a přispívajících faktorů.

Protože shromážděná data jsou koncentrovanější při přesnější a podrobnější analýze interních procesů, je obtížné zohlednit externí procesy využívající data. Na příkladu tohoto kroku můžete pochopit, proč mluvíme o integraci dat, spíše než o absolutním či výhradním použití samotných dat pro veškeré rozhodování. Člověk se svou expertní znalostí a schopností rozhodování musí brát v úvahu různé vnější faktory, jako je srážka s ptáky nebo dronem při přistání. Přestože by později v programu bylo možné tyto vnější faktory přidat do celkové analýzy, program v dané prezentaci nebude schopen vnější faktory vymýšlet a navrhovat sám.

7.2.4 Určení důvodů porušení předpokladů

Program také nebude schopen identifikovat důvod porušení předpokladů, respektive nesprávné předpoklady a tento úkol zůstává pouze na bezpečnostním expertovi. Jak bylo zmíněno v odstavci 7.2.1, popsaná pravidla lze vytvořit a přidat do systému, což pomůže zjistit, které předpoklady byly chybné, ale nedokáže odpovědět na otázku, proč došlo k porušení předpokladů. Pokud byla pravidla zapsaná v programu původně vytvořena nesprávně, zobrazí se nesprávný výsledek. Na tomto příkladu je patrné, že i přes to, že obecně může datová integrace hodně pomoci, v některých krocích bez řádné kontroly a korekce pravidel taková integrace programu a dat jako celek mnoho nepřinese.

7.2.5 Zjištění funkčnosti nouzových opatření

V této části analýzy zkoumáme, zda dříve zavedená nouzová opatření správně reagují a plní takn svůj účel, tedy zabraňují nehodám, či alespoň zmírňují následky při vzniku nehody. Vzhledem k charakteru tohoto kroku se lépe alanyzuje v případě reaktivního využití analýzy. V případě obecné kontroly spolehlivosti systému a zjištění funkčnosti nouzvých opatření může integrace dat pomoci pouze při dlouhém, pečlivém a intenzivním používání a integraci do systému jako celku. Pomocí dat by bylo možné okamžitě předvídat nástup jakýchkoli trendů a i poté reagovat na narušení bezpečnosti v systému, to však skutečně pomůže pouze tehdy, budete-li datovou integraci neustále aktualizovat a pracovat s ní. Stejně jako se samotná analýza STPA bez patřičných aktualizací časem stává irelevantní vzhledem k realizaci změn v systému, může být zastaralý i program, který dříve poskytoval určitou obecnou spolehlivost systému, ale v budoucnu bez podpory není schopen tuto spolehlivost udržet na stejné úrovni jako dříve.

7.3 3. krok - Řešit a aktualizovat

7.3.1 Vytvoření seznamu možných obran

Cílem této části analýzy je zvýšit úroveň provozní bezpečnosti v systému. Vytvoření seznamu možných obran je výchozím bodem pro výběr konkrétních obran vhodných pro implementaci v rámci dalšího rozhodování. Množství možných obran často závisí na složitosti řešeného systému.

Za přítomnosti datové integrace do seznamu možných obran okamžitě můžeme přidat nová pravidla do analýzy dat. Pokud došlo k nějakému incidentu, který program nebyl schopen detekovat, pak má smysl tomu věnovat pozornost, protože program v tomto případě funguje jako další vrstva ochrany v celém systému.

7.3.2 Analýza kompromisů

V tomto kroku dochází k posuzování pozitivního i negativního vlivu možných obran na celkový systém a hodnocení pro výběr nejvhodnějšího řešení pro implementaci.

Při analýze možných kompromisů za ochranu v případě integrace dat s původně správně vytvořenou aplikační architekturou by vytvoření nové ochranné vrstvy v programu mělo vyžadovat minimální finanční a časové náklady. Pokud jde o vytváření nových indikátorů nebo pravidel v rámci programu pro další zajištění bezpečnosti systému, pak by takové procesy měly být prováděny rychle a rozhodnutí o přijetí takových opatření by nemělo znamenat obrovské náklady, ale pokud se vytvoří složitější vzorec, může být zapotřebí mnohem více zdrojů. V takovém případě musí bezpečnostní manažer tento problém řešit přímo s osobou, která pracuje na softwarové části datové integrace.

7.3.3 Určení optimálního řešení

Ze seznamu možných obran jako výstupu předchozích dvou kroků je třeba vybrat jednu nebo více obran a implementovat je do systému včetně nově vzniklých požadavků a omezení. Vzhledem k potřebné rovnováze mezi úrovní provozní bezpečnosti a finanční udržitelností subjektu podnikání je často součástí rozhodování cost-benefit analýza.

Volba optimálního řešení leží na bezpečnostním manažerovi, integrace dat mu s tím může výrazně pomoci. Pokud například integrace dat najde v systému více problémů se zabezpečením, může software hodnotit každý problém na základě toho, jak často se problém vyskytoval v minulosti a jak závažný je. S tímto posouzením problémů zjištěných integrací dat bude možné

okamžitě označit, který z nich představuje větší bezpečnostní riziko, což pomůže při výběru nejlepšího řešení.

7.3.4 Zavedení nových obran

V tomto kroku dochází k implementaci dříve zvolené obrany. Výhodu integrace dat můžeme vidět spíše při následném sledování chování obrany v systému, než přímo v tomto kroku.

7.3.5 Aktualizace STPA

S ohledem na celkový cíl analýzy, tedy zajištění stále se zdokonalujícího procesu řízení provozní bezpečnosti, je analýza zakončena implementací všech vzniklých aktualizací a změn do modelu analýzy STPA.

Při aktualizaci obecného modelu STPA je nutné opravit samotný program integrace dat v souladu se zavedenými úpravami. Bez řádné a trvalé podpory pro metodu integrace dat může být tato metoda zastaralá a přestane být relevantní pro analýzu a systém jako celek.

8. Shnutí výsledků a srovnání přístupů práce s daty

Bezpečnost v letectví nestojí na místě a neustále se vyvíjí. Jedním z kroků ve vývoji obecného přístupu k bezpečnosti je vytvoření modelu analýzy STPA a následně analýzy Active STPA. Hlavní výhodou Active STPA jsou dodatečné kroky, které umožňují znovu prozkoumat celou analýzu za účelem její aktualizace v souladu s neustále se měnícím systémem, pro který je tato analýza určena. Tím dochází k integraci znalosti z bezpečnostní studie s daty z provozu, kdy bezpečnostní studie je díky datům z provozu v průběhu času akualizována.

Ačkoliv řízení bezpečnosti již v současné době pracuje s takzvanými reaktivními a proaktivními indikátory, překročení takové hranice je spouštěčem pro řízení rizik dle systému řízení bezpečnosti dané společnosti. V tomto přístupu také nedochází k další práci s původní safety studií, která standardně slouží jen při zavádění nového systému či změny, ale dále není metodicky aktualizována.

Přístup využívající integrační model je oproti současnému přístupu práce s indikátory dle ICAO Safety Management Manuálu efektivnější, protože poskytuje jasnou metodiku, jak postupovat v případě aktivace bezpečnostního indikátoru a využívá výhod spojení proaktivní a prediktivní metody řízení bezpečnosti.

V rámci vlastního přístupu v této bakalářské práci jsem se pokusil změnit práci s daty a zvýšit tím efektivitu integračního modelu. Dle mého názoru existuje v současné metodice limitace, kdy kroky analýzy Active STPA začínají až na základě nějakého incidentu, který musí nastat. A i když samotná analýza STPA vytváří proaktivní omezení a snaží se předvídat jakoukoli nežádoucí událost, kroky Active STPA začínají pouze v případě, že došlo k incidentu. Právě tato část má funkci reaktivní bezpečnosti, ve které se snažíme opravit naši analýzu až poté, co se něco stane. Pravidelné procházení celé analýzy by také nebylo vhodným řešením, protože s tímto přístupem neexistuje žádný ukazatel a pro bezpečnostního inženýra se to může změnit v rutinní práci, při které neprojde celou analýzou pokaždé, a není jisté, jestli je s ní už něco v nepořádku, nebo ne.

Pro pochopení modelu integrace dat provedeme SWOT analýzu. SWOT analýza je technika strategického plánování a řízení, která pomáhá identifikovat silné stránky, slabé stránky, příležitosti a hrozby související s nějakým modelem anebo procesem (viz Obrázek 37). [34]

Obrázek 37 - SWOT analýza modelu integrace dat [autor]

Způsob integrace dat je dobrým krokem ke zlepšení zabezpečení, ale ne vždy prvním, protože závisí přímo na datech, což nemůže být. Výsledkem analýzy bylo naznačeno, že model lze aplikovat jak v procesech provozní oblasti letiště, tak v procesech, ve kterých je řídícím prvkem člověk.

8 Závěr

Bezpečnost v letectví je stav, při kterém v procesech souvisejících s provozem letadel rizika zranění osob nebo poškození majetku jsou snížena a řízena na přijatelné úrovni. Postavit první letadla a provést na nich první lety bylo pro lidstvo obrovským krokem. Protože lidské tělo ze své podstaty nebylo původně určeno k létání, velkou otázkou před inženýry a dalšími specialisty bylo, jak tento problém vyřešit a jak zajistit bezpečnost letů a letadel. Zpočátku byly hlavním zájmem o bezpečnost letectví technické aspekty letadla. Během „Technické éry“ byly výsledky katastrof především technické chyby, nepřesnosti a poruchy letadel, které vedly ke katastrofě. Poté, co se inženýrům na celém světě podařilo pochopit, jak správně vyrobit a udržovat letadlo tak, aby se minimalizovala možnost technické poruchy, přišla „éra lidského faktoru“, během níž byl následkem katastrofy jenom člověk, i když byl pod vlivem nějaké organizace. Když se ukázalo, že lidské chování, které vedlo ke katastrofě, bylo někdy i důsledkem něčeho zvenčí, začala „éra organizační“, ve které se kvůli bezpečnosti začali věnovat nejen pilotovi, ale celé společnosti, která obsluhuje toto letadlo, a jak společnost ovlivňuje chování a rozhodnutí pilotů. A nyní nastala „éra společného systému“, kdy pro zajištění bezpečnosti je nutné se zaměřit nejen na prvky systému, ale také na vzájemné působení těchto prvků.

V souvislosti s nutností hledat problém nejen v prvcích systému, ale i ve vazbách mezi těmito prvky, vznikl model STAMP. Díky kompetentnímu a správnému vytvoření tohoto modelu můžeme získat jasnou představu o tom, jaké prvky jsou v systému, jak se vzájemně ovlivňují, a získat kruhy zpětné vazby, se kterými dokáže pochopit, jak selkhani jednoho elementu přišli k selkhani celého systému. Taková analýza založená na modelu STAMP se nazývá STPA analýza. Tato analýza umožňuje na systémové úrovni určit rizika, ztráty a bezpečnostní omezení, které lze následně sestavit do společného modelu a následně s ním pracovat.

Aby bylo možné proaktivně pracovat s STPA analýzou, je nutná integrace s daty. S neustálou integrací dat dokážeme analyzovat nejen simulovanou situaci, ale i samotnou STPA analýzu, takže v případě chybně vytvořené analýzy v ní identifikujeme chyby a přidáme změny do již existující analýzy. Tato analýza se nazývá Active STPA, protože závěry takové analýzy se v případě potřeby okamžitě použijí k přehodnocení modelu analýzy, což snižuje pravděpodobnost chyb v modelu samotném.

Model neustále integrace dat byl již testován na modelu ADGS a výsledky ukázaly, že integraci dat lze použít pro automatizované modely. Dalším logickým krokem by bylo otestovat integraci dat v procesu, kde by řídícím prvkem byl člověk. Proces přistání letadla byl zvolen, protože

současně poskytuje velké množství parametrů pro analýzu a je jednou z nejnebezpečnějších částí letu z hlediska procenta leteckých nehod dle fáze letu.

V praktické části této práce bylo ukázáno, jak lze provést integraci dat při přistání letadla, a také bylo ukázáno, jak pracovat s indikátory a jak sledovat, zda změny zavedené do systému nějak ovlivnily výsledky .Za přínos považuji napsání programu, který dokáže analyzovat data, stejně jako naznačení obecného přístupu k tomu, jak by měla integrace dat probíhat, a to na konkrétním příkladu. Tento přístup umožňuje, v závislosti na taxonomii poskytnutých nebo zaznamenaných dat, napsat program, který by mohl nezávisle upozornit osobu na porušení jakýchkoli ukazatelů, čímž uvolní čas pouze na analýzu správného výkonu samotného programu, ukazování správnosti indikatorů a činit rozhodnutí ke zvýšení celkové bezpečnosti. Také v případě počítačového kódu je schopen okamžitě zpracovávat data ze všech letů, čímž je dalším krokem k prediktivnímu přístupu k bezpečnosti v letectví.

Bylo také naznačeno, že model integrace dat lze použít v procesech, ve kterých je řídícím prvkem člověk. Nejdůležitější při takové integraci je identifikovat všechna možná data, která na této osobě mohou záviset a která je schopna přímo ovlivnit. Ve formě dat tak získáme představu o chování člověka v daném okamžiku a na základě toho jej můžeme analyzovat. Samozřejmě není možné reprezentovat všechny proměnné ve formě parametrů a dat, jako je například nálada člověka nebo jeho úroveň stresu, nicméně již existující parametry mohou být příležitostí pro další výzkum dalších proměnných, které nelze vyjádřit pomocí čísel a dat obecně.

Hlavním rozdílem modelu integrace dat do Active STPA je, že indikátory používáme jako spouštěče, které se aktivují na základě neustálého sledování dat. To znamená, že takový přístup, se správnou definicí parametrů indikátorů, je schopen určit narušení v rámci systému mnohem dříve, než dojde k jakémukoli incidentu, zatímco současný přístup k přehodnocení obecné analýzy čeká, až k incidentu dojde, a pouze pak začne analyzovat, proč žádná ze zavedených obran nepomohla incident zastavit. Pomocí datové integrace lze tedy Active STPA posunout na novou úroveň, která je schopna se okamžitě analyzovat a kontrolovat, jakmile jsou v ní data použita, což umožňuje udržovat celkový systém neustále v závislosti na změnách v systému a jeho relevanci.

V budoucnu může být tato práce použita jako základ pro napsání programu, který by analyzoval data ze skutečné letecké společnosti, aby ukázal, že takový přístup je nebo není potřeba pro bezpečnost letectví. Bylo by také možné vymyslet nejen algoritmus, ale celou umělou inteligenci,

která by byla schopna samostatně vytvářet indikátory a pracovat s nimi na základě existujících dat.

Závěrem lze konstantovat, že jednotlivá tvrzení uvedená v odstavci číslo 5 byla potvrzena jako výsledek této práce.

9 Bibliografie

1. Allianz. *Aviation Risk Report 2020. Safety and the state of the Nation.* Munich, Germany : Allianz Global Corporate, 2019.

2. Agency, European Union Aviation Safety. *The Europlan for Aviation Safety (EPAS 2020-2024).* 2019.

3. Úřad pro civilní letectví, Ministerstvo dopravy ČR. *Letecký předpis L 19 Řízení bezpečnosti.* 2013. 166/2013-220-LPR/1.

4. ICAO. *ICAO State Safety Programme. Aerodrome Safety Management System (SMS).* Mexico : autor neznámý, 2014.

5. Organization, International Civil Aviation. *Doc 9859, Safety Management Manual.* 2017.

6. State Safety Programme (SSP). *SKY brary.* [Online] [Citace: 17. duben 2022.] https://skybrary.aero/articles/state-safety-programme-ssp.

7. Castilho, Diogo Silvia. *Active STPA: Integration of Hazard Analysis into a Safety Management System Framework.* 2019.

8. Nancy G. Leveson, John P. Thomas. *STPA Handbook.* 2018.

9. Introduction to Systems Theory in Social Work. *Online MSW Programs.* [Online] 2U, Inc, červenec 2020. [Citace: 28. duben 2022.] https://www.onlinemswprograms.com/social-work/theories/systems-theory-social-work/.

10. Hanan Altabbakh, M. A. *STAMP – Holistic system safety approach or just another risk model?* 2014.

11. Hanáková Lenka, Ing., Lališ Andrej Ing., Ph.D, Stojić Slobodan Ing., Ph.D., Kafková Markéta, Ing. *Metodika pro zefektivnění analýzy a řízení rizik s využitím konceptuálního modelování.*

12. Whiteley-Safety. *5 min. Intro to: STAMP (Systems Theoretic Accident Model & Processes).* 2016.

13. Guskova, N. *Konceptualizace vybraných částí modelu bezpečnosti STAMP.* Praha : autor neznámý, 2018.

14. Amit. All You Need to Know About UML Diagrams: Types and 5+ Examples. *Tallyfy.* [Online] 2018. [Citace: 8. květěn 2022.] https://tallyfy.com/uml-

diagram/#:~:text=A%20UML%20diagram%20is%20a,document%20information%20about%20the%20system..

15. Nishadha. UML Diagram Types Guide: Learn About All Types of UML Diagrams with Examples. *Creately.* [Online] 10. září 2021. [Citace: 2022. květen 2022.] https://creately.com/blog/diagrams/uml-diagram-types-examples/.

16. Paradigm, Visual. What is Unified Modeling Language (UML)? *Visual Paradigm.* [Online] [Citace: 8. květen 2022.] https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/.

17. IBM. Interfaces. *IBM.* [Online] 02. 03 2021. [Citace: 14. červen 2022.] https://www.ibm.com/docs/en/rational-soft-arch/9.7.0?topic=diagrams-interfaces.

18. Greg. UML class diagram arrow types: explanations and examples. *gleek.io.* [Online] 20. duben 2021. [Citace: 14. červen 2022.] https://www.gleek.io/blog/class-diagram-arrows.html.

19. Andrej Lalis, Slobodan Stojic, Oldrich Stumbauer, Marketa Sediva Kafkova. *Systemic Integration of safety studies with operational safety data in the aviation.* Praha : autor neznámý, 2020.

20. P. Turner, A. Kushniruk, C. Nohr. Are We There Yet? Human Factors Knowledge and Health Information Technology – the Challenges of Implementation and Impact. *National Library of Medicine.* [Online] 26. srpen 2017. [Citace: 30. červen 2022.] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6239238/.

21. VAŇOUREK, Bc. JIŘÍ. *Lidský faktor v letectví.* Brno : VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2009.

22. Agency, European Union Aviation Safety. *ANNUAL SAFETY REVIEW 2020.* 2020. 978-92-9210-222-7/2314-9272.

23. Jackman, Frank. Flight Safety Foundation. *flightsafety.org.* [Online] 4. listopad 2014. [Citace: 30. červen 2022.] https://flightsafety.org/asw-article/nearly-half-of-commercial-jet-accidents-occur-during-final-approach-landing/#:~:text=Approximately%2014%20percent%20of%20the,initial%20approach%20and%203%20percent.

24. McLeod, Saul. What is a hypothesis? *SimplyPsychology.* [Online] 16. prosinec 2021. [Citace: 30. červen 2022.] https://www.simplypsychology.org/what-is-a-hypotheses.html.

25. What is Jython? *Jython.* [Online] [Citace: 11. červenec 2022.] https://www.jython.org/.

26. sh0nk. Github repository sh0nk/matplotlib4j. *Github.* [Online] [Citace: 11. červenec 2022.] https://github.com/sh0nk/matplotlib4j.

27. Pavel Pačes, Pavel Brodský. Let L-410 simulator. *inAero.* [Online] [Citace: 11. červenec 2022.] https://www.l410simulator.cz/.

28. Pačes, Pavel. inAero. *pacespavel.net.* [Online] [Citace: 11. červenec 2022.] http://www.pacespavel.net/inaero.php.

29. X-Plane. Datarefs for X-Plane 1150. *X-Plane developer.* [Online] 7. květen 2020. [Citace: 19. červenec 2022.] https://developer.x-plane.com/datarefs/.

30. LET, a.s. Airplane flight manual for the L 410 UVP - E20. *x-plane.hu.* [Online] 13. květen 1998. [Citace: 19. červenec 2022.] https://x-plane.hu/L-410/download/L410%20Flight%20Manual.pdf.

31. Foundation, Flight Safety. Approach and landing Accident Reduction - Stabilized Approach. *Flight safety.* [Online] srpen 2000. [Citace: 19. červenec 2022.] https://flightsafety.org/wp-content/uploads/2016/09/alar_bn7-1stablizedappr.pdf.

32. Organization, International Civil Aviation. *Aircraft Operations Doc 8168 OPS/611, Procedures for Air Navigation Services.* 2006.

33. Kranz, Garry. Metadata. *WhatIs.* [Online] [Citace: 6. srpen 2022.] https://www.techtarget.com/whatis/definition/metadata.

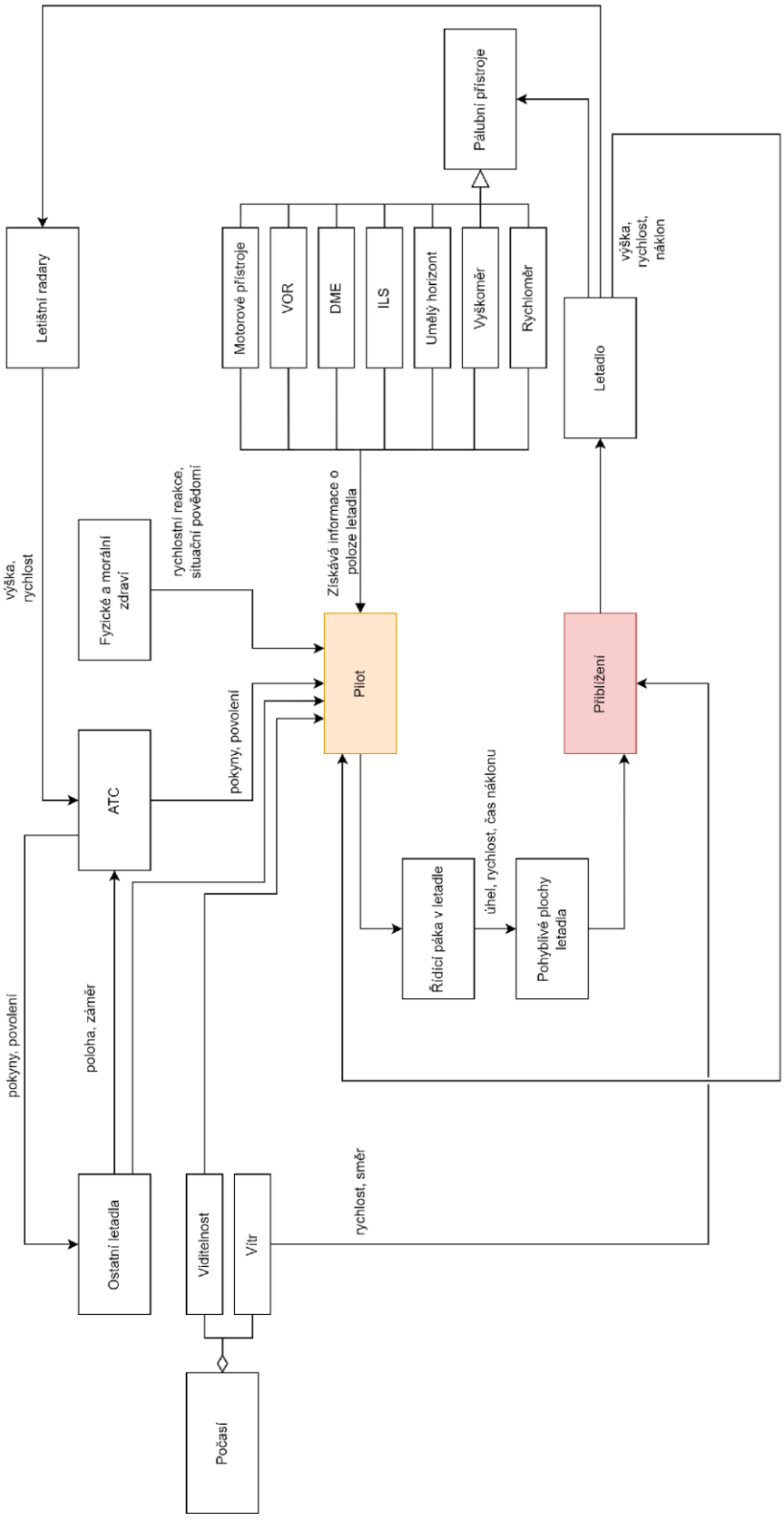
34. Kenton, Will. Strength, Weakness, Opportunity, and Threat (SWOT) Analysis. *Investopedia.* [Online] 28. květěn 2022. [Citace: 4. srpen 2022.] https://www.investopedia.com/terms/s/swot.asp.

10 Seznam obrázků

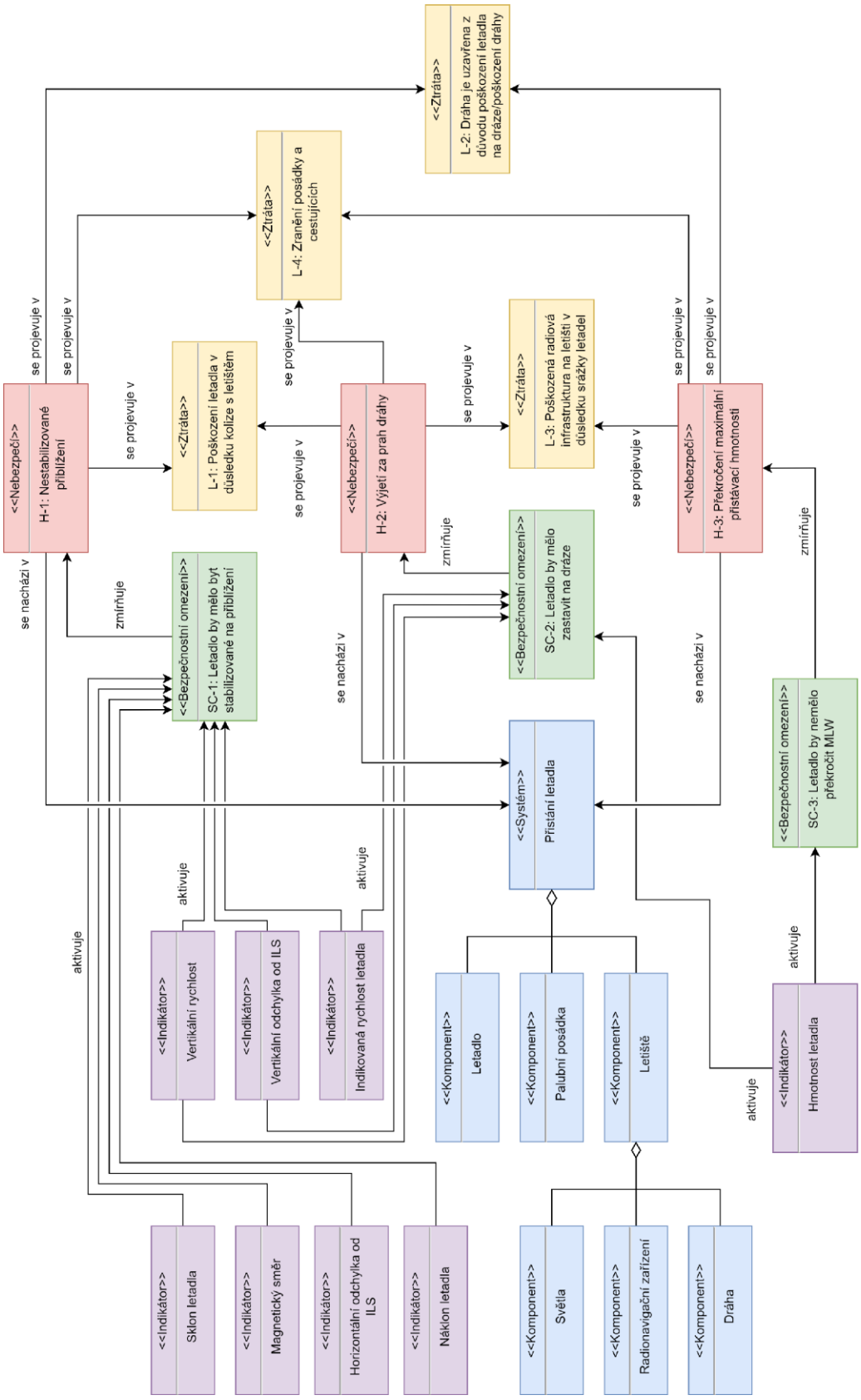
11 Seznam grafů

12 Seznam příloh

Příloha A - STAMP model procesu přistání pilota [autor]



Příloha B - Definice systému s ontologií STAMP [autor]



Příloha C - Bezpečnostní řídicí struktura [autor]