



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Provázání leteckých taxonomií a typů událostí v modelu STAMP
Alignment of Aviation Safety Taxonomies and Event Types in STAMP

Bakalářská práce

Studijní program: Technika a technologie v dopravních spojích

Studijní obor: Letecká doprava

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

Ing. Kateřina Grötschelová

Johana Martinovská

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):

Johana Martinovská

Studijní program (obor/specializace) studenta:

bakalářský – LED – Letecká doprava

Název tématu (česky): **Provázání leteckých taxonomií a typů událostí v modelu STAMP**

Název tématu (anglicky): **Alignment of Aviation Safety Taxonomies and Event Types in STAMP**

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cíl práce: Vytvoření převodního systému provázání leteckých taxonomií a typů událostí v modelu STAMP, kterými lze reprezentovat řídicí strukturu a její části
- Analyzujte současné letecké taxonomie z pohledu typů událostí
- Analyzujte systémový přístup k bezpečnosti pomocí modelu STAMP a identifikujte využívané typy událostí
- Navrhněte převodní systém provázání leteckých taxonomií a typů událostí v modelu STAMP
- Dosažené výsledky vyhodnoťte



- Rozsah grafických prací: dle pokynů vedoucího 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 Ed., Montréal, Quebec, 2018.
Arlow, J. a Neustadt, I. UML 2 a unifikovaný proces vývoje aplikací: objektově orientovaná analýza a návrh prakticky. 2., Computer Press, 2007.
Leveson, N., Thomas, J. STPA Handbook, 2018.

Vedoucí bakalářské práce: **doc. Ing. Andrej Lališ, Ph.D.**
Ing. Kateřina Grötschelová

Datum zadání bakalářské práce: **8. října 2020**
(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

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



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

Potvrzuji převzetí zadání bakalářské práce.

Johana Martinovská
jméno a podpis studenta

V Praze dne..... 2. prosince 2021



Abstrakt

Bakalářská práce se věnuje taxonomii ECCAIRS a jejímu rozšíření, které by umožnilo, aby se v rámci povinného systému hlášení událostí v letectví mohli používat pokročilejší techniky pro šetření a klasifikaci událostí. Cílem mé bakalářské práce je vytvoření převodního systému taxonomie ECCAIRS a analýzy STAMP, které jsou schopné tohoto rozšíření. První část práce obsahuje popis současného stavu, jak pracují systémy pro sběr, zpracování a analýzu dat regionálních dozorových institucí, seznámení s bezpečnostní taxonomií ECCAIRS (typy událostí), vysvětlení modelu STAMP/STPA a zamyšlení nad limitacemi současného stavu. Dle těchto informací byl následně vytvořen převodní systém, který vznikl jako výsledek analýzy událostí dle modelu STAMP, který byl propojen UML modelem události za použití ECCAIRS taxonomie (typy událostí). Výsledkem práce je převodní systém, který byl ověřen a může sloužit jako základ pro převodní systém celé ECCAIRS taxonomie, který by byl přínosný pro letectví.

Klíčová slova: bezpečnost v letectví, ECCAIRS taxonomie, hlášení, STPA analýza, událost, UML model



Abstract

The bachelor thesis deals with the ECCAIRS taxonomy and its extension in a mandatory system of occurrence reports in aviation, which would allow to use advanced technology for occurrence investigation and classification. My bachelor thesis aims to create a conversion system of ECCAIRS taxonomy and STAMP analysis, that is capable of this extension. The first part of the thesis contains a description of the current state, how the systems for data collection, processing, and analysis of regional supervisory institutions works, acquaintance with ECCAIRS safety taxonomy (event types), an explanation of STAMP / STPA model, and reflections on current state limitations. According to this information, a conversion system was created as a result of an event analysis according to the STPA model, which was linked to the UML event model using the ECCAIRS taxonomy (event types). The result of this bachelor thesis is a conversion system that has been validated and can serve as a basis for the conversion system of the whole ECCAIRS taxonomy, which would be beneficial for aviation.

Keywords: aviation safety, ECCAIRS taxonomy, report, STPA analysis, occurrence, UML model



Poděkování

Tímto bych ráda poděkovala všem, kteří mi poskytli podklady pro vypracování této práce. Zvláště bych chtěla poděkovat panu docentu Lališovi a paní inženýrce Grötschelové za odborné vedení a konzultování bakalářské práce a za rady, které mi poskytovali za celou dobu studia. V neposlední řadě bych chtěla poděkovat i svým rodičům a blízkým za morální a materiální podporu, které se mi za celou dobu studia dostávalo.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Provázaní leteckých taxonomií a typů událostí v modelu STAMP vypracovala samostatně a použila 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 20. července 2022

Podpis



Obsah

Úvod.....	11
1. Regionální dozor nad leteckými organizacemi	12
1.1. ICAO – Mezinárodní organizace pro civilní letectví.....	12
1.2. EASA – Agentura Evropské unie pro bezpečnost letectví.....	13
1.3. ÚCL – Úřad pro civilní letectví.....	14
2. Systémy pro sběr, zpracování a analýzu dat regionálních dozorových institucí. 15	15
3. Bezpečnostní taxonomie – typy událostí	17
4. Systémový pohled na bezpečnost (model STAMP)	23
4.1. Aplikace STPA.....	24
5. Přehled vědecké literatury.....	29
6. Limitace současného stavu	30
7. Metodika.....	31
7.1. UML.....	31
7.2. ECCAIRS hlášení	33
8. Analýza nehod a incidentů pomocí STPA a ECCAIRS taxonomie	34
8.1. Událost 1 – kouř na palubě letadla.....	34
8.2. Událost 2 – únik paliva	39
8.3. Událost 3 – selhání tlaku v hlavní pneumatice	43
9. Provázání informací analyzovaných událostí.....	48
10. Výsledky	52
10.1. Spojitosti mezi STPA pojmy v událostech	52
10.2. Propojení ECCAIRS taxonomie a STPA pojmů v UML modelu.....	53



11. Validace	60
11.1. Událost 4 – pozemní srážka	60
11.2. Událost 5 – nepovolený vjezd na dráhu	64
11.3. Událost 6 – posun nákladu za letu	68
11.4. Zhodnocení událostí	72
12. Diskuse	74
Závěr	78
Seznam použité literatury	80



Seznam obrázků

Obrázek 1: SDCPS schéma	16
Obrázek 2: Ukázka větvení ECCAIRS taxonomie	22
Obrázek 3: Hierarchické modely	27
Obrázek 4: UML vazby	32
Obrázek 5: Řídící struktura – událost 1.....	35
Obrázek 6: Důležité informace z hlášení – událost 1	38
Obrázek 7: UML model události 1 - ECCAIRS taxonomie	40
Obrázek 8: Řídící struktura – událost 2.....	41
Obrázek 9: Důležité informace z hlášení – událost 2.....	42
Obrázek 10: UML model události 2 - ECCAIRS taxonomie.....	44
Obrázek 11: Řídící struktura – událost 3	45
Obrázek 12: Důležité informace z hlášení – událost 3	46
Obrázek 13: UML model události 3 - ECCAIRS taxonomie	47
Obrázek 14: Převodní systém taxonomie ECCAIRS a STPA v UML modelu	55
Obrázek 15: Řídící struktura – událost 4	61
Obrázek 16: Důležité informace z hlášení – událost 4	62
Obrázek 17: UML model události 4 - ECCAIRS taxonomie	63
Obrázek 18: Řídící struktura – událost 5	64
Obrázek 19: Důležité informace z hlášení – událost 5	66
Obrázek 20: UML model události 5 - ECCAIRS taxonomie	67



Obrázek 21: Řídící struktura – událost 6	69
Obrázek 22: Důležité informace z hlášení – událost 6	70
Obrázek 23: UML model události 6 - ECCAIRS taxonomie	71



Seznam tabulek

Tabulka 1: Porovnání typů událostí ECCAIRS a ICAO ADREP	18
Tabulka 2: Rozdíly taxonomií ECCAIRS a ICAO ADREP	19
Tabulka 3: Obecné ztráty	26
Tabulka 4: Obecné systémové nebezpečí	26
Tabulka 5: Ztráty a systémové nebezpečí – událost 1	36
Tabulka 6: Nebezpečné řídicí akce – událost 1	36
Tabulka 7: Ztrátové scénáře – událost 1	37
Tabulka 8: Ztráty a systémové nebezpečí – událost 2	41
Tabulka 9: Nebezpečné řídicí akce – událost 2	41
Tabulka 10: Ztrátové scénáře – událost 2	42
Tabulka 11: Ztráty a systémové nebezpečí – událost 3	45
Tabulka 12: Nebezpečné řídicí akce – událost 3	45
Tabulka 13: Ztrátové scénáře – událost 3	46
Tabulka 14: STPA pojmy – jednotlivé události	50
Tabulka 15: Legenda k převodnímu systému (obrázek 14)	56
Tabulka 16: ECCAIRS taxonomie – událost spojená s vybavením	58
Tabulka 17: ECCAIRS taxonomie – událost spojená s vybavením	59
Tabulka 18: Ztráty a systémové nebezpečí – událost 4	61
Tabulka 19: Nebezpečné řídicí akce – událost 4	61
Tabulka 20: Ztrátové scénáře – událost 4	62



Tabulka 21: Ztráty a systémové nebezpečí – událost 5	65
Tabulka 22: Nebezpečné řídicí akce – událost 5	65
Tabulka 23: Ztrátové scénáře – událost 5.....	65
Tabulka 24: Ztráty a systémové nebezpečí – událost 6.....	69
Tabulka 25: Nebezpečné řídicí akce – událost 6	69
Tabulka 26: Ztrátové scénáře – událost 6.....	70
Tabulka 27: Výsledky událostí.....	72



Seznam symbolů a zkratk

AAIB	Air Accidents Investigation Branch	-
CAST	Causal Analysis based on System Theory	-
EASA	European Union Aviation Safety Agency	Agentura Evropské unie pro bezpečnost letectví
ECCAIRS	European Co-ordination Center for Accident and Incident Reporting System	-
ECR	European Central Repository	-
EPAS	European Plan for Aviation Safety	-
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
RIT	Reduced Interface Taxonomy	-
ŘLP	Air Traffic Control	Řízení letového provozu
SDCPS	Safety Data Collection and Processing System	-



STAMP	System-Theoretic Accident Model and Process	-
STPA	System Theoretic Process Analysis	-
UML	Unified Modeling Language	-
ÚCL	Civil Aviation Authority	Úřad pro civilní letectví
ÚZPLN	Air Accidents Investigation Institute	Ústav pro odborné zjišťování příčin leteckých nehod



Úvod

Bezpečnost je alfa a omega letectví. Ačkoliv se letecká technika a letecké systémy vyvíjejí velice rychle, stále v letectví přetrvávají určité nedostatky, na kterých je třeba zapracovat. Hlavním problémem jsou nedostatky, se kterými nedokážeme počítat a hrají klíčovou roli při vzniku událostí. Mezi takové mezery v bezpečnosti patří například lidský faktor, který hraje roli u většiny událostí. Další překážkou jsou nedostatky systému. Toto můžeme chápat jako chybný systém jako celek anebo také jako funkční systém s vadnými komponenty, případně nedostatky mezi překrýváním a propojováním jednotlivých komponentů/podsystemů, ačkoliv systém jako celek se zdá bezchybný. Proto je na šetření událostí nutné využívat analýzu, která s těmito nedostatky dokáže počítat a předcházet vzniku událostí.

V této práci se bude pracovat se System Theoretic Process Analysis (STPA), která tyto problémy bere v potaz a dokáže je efektivně řešit. Práce by ale nemohla být kompletní, kdyby nezahrnovala i leteckou taxonomii, která se využívá pro vyplňování hlášení událostí – European Co-ordination Center for Accident and Incident Reporting System (ECCAIRS). Cílem této bakalářské práce je vytvoření převodního systému, který propojí taxonomii ECCAIRS a analýzu STPA pomocí modelovacího jazyku UML, který by mohl pomoci vylepšení bezpečnosti v letectví.



1. Regionální dozor nad leteckými organizacemi

1.1. ICAO – Mezinárodní organizace pro civilní letectví

ICAO¹ je letecká organizace vznikla v roce 1947. Má 193 členských států. Cílem je zajišťování bezpečnosti a spořádaného rozvoje mezinárodního civilního letectví. ICAO přispívá k rozvoji letectví, letišť a leteckých zařízení. Mimo jiné tato organizace celosvětově pomáhá s bezpečností a s podmínkami nutnými pro bezpečné, pravidelné a účinné fungování letecké dopravy. Dále zajišťuje rovné podmínky pro všechny státy provozující letecké služby, aby nedocházelo k diskriminaci států nebo leteckých subjektů. [1]

Mezi činnost ICAO patří kontrola současných a přijímání nových předpisů v rámci mezinárodní letecké přepravy. Podpora registrace mezinárodních smluv, tak zvané multilaterální letecké dohody, kde se jedná o vztah mezi více státy nebo státy a mezinárodními organizacemi. ICAO poskytuje odbornou pomoc při výstavbě letišť nebo jiné letecké infrastruktury. [1]

ICAO vydává mezinárodní standardy, doporučení a postupy. Tyto standardy se musí aplikovat a všechny členské země je musí dodržovat, pokud stát standardy nedodrží, hrozí sankce. V případě doporučení členové by se měly snažit o jejich plnění. Postupy slouží pro letecké operace, letové navigační služby nebo také postupy stanovují správné poskytování letových provozních služeb a provádění letů. [1]

ICAO vydalo 19 Annexů (19 příloh, které vznikly v rámci Chicagské úmluvy – Úmluva o mezinárodním civilním letectví²), jedná se o 19 leteckých oblastí, které obsahují podrobná pravidla týkající se provozu, na příklad: Způsobilost leteckého personálu (Annex 1), Pravidla létání (Annex 2), Provoz letadel (Annex 6), Letecká komunikační služba (Annex 10) nebo Zjišťování příčin leteckých nehod a incidentů (Annex 13). V České republice se setkáváme s českou obdobou, kde jsou tyto letecké předpisy označovány písmenem L (L1-L19³). [1]

¹ <https://www.icao.int/Pages/default.aspx>

² <https://www.zakonyprolidi.cz/cs/1947-147>

³ <https://aim.rlp.cz/predpisy/predpisy/index.htm>



1.2. EASA – Agentura Evropské unie pro bezpečnost letectví

EASA⁴ má celkem 32 členů, patří tam všem 27 členských států Evropské unie a k tomu navíc Island, Lichtenštejnsko, Norsko, Spojené království a Švýcarsko. Posledních 5 jmenovaných nemá hlasovací právo, jelikož nejsou členy Evropské unie. [2]

EASA spolupracuje s evropskými úřady pro civilní letectví. Mimo jejich spolupráci, musí EASA na úřady pro civilní letectví dohlížet a kontrolovat je. Mezi její hlavní aktivity a cíle patří dohled nad bezpečností v letectví. EASA také zajišťuje sjednocení předpisů, legislativy a certifikace, aby po celé Evropě platila stejná pravidla. Dále se snaží o prosazování mezinárodních a evropských bezpečnostních norem a spolupráci s jinými mezinárodními agenturami, jejichž cílem je zlepšení bezpečnosti. Mimo jiné schvaluje společnosti, které zajišťují konstrukci, výrobu nebo údržbu letadel a letadlových celků. Následně vydává osvědčení a certifikace letadlům a letadlovým celkům. EASA také vypracovává technická pravidla, předpisy a postupy, které se musí dodržovat a v případě, kdy zjistí, že tomu tak není, může daný subjekt sankcionovat. [2]

Všechny aktivity, které byly výše zmíněny, musí být samozřejmě i kontrolovány. EASA může vyslat například na vybrané letiště audit a zkontrolovat, zda je například bezpečnostní management vykonáván tak, jak je to v předpisech. Podobný audit může vykonávat i Úřad pro civilní letectví. U leteckých společností kontroluje stáří flotily, platnou kvalifikaci posádky či kvalifikovaný servis. Stejně kvalifikace kontroluje i u jiných leteckých subjektů. V případě, kdy odhalí nějaký přestupek, může zavést postih, pokutu nebo dokonce odebrat licenci⁵. [2,3]

V případě, kdy my jako obyčejní cestující nebudeme s něčím spokojeni a budeme si chtít stěžovat na leteckou společnost nebo budeme chtít nahlásit nějaké pochybení posádky, existuje pro nás jako cestující možnost nahlásit danou událost na stránkách EASA⁶ a ona dané pochybení může zkontrolovat. Samozřejmě záleží na vážnosti pochybení. [2]

⁴ <https://www.easa.europa.eu/light>

⁵ <https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1396857053904&uri=CELEX:32012R0646>

⁶ <https://aviationreporting.eu>



1.3. ÚCL – Úřad pro civilní letectví

Úřad pro civilní letectví⁷ v České republice spadá pod ministerstvo dopravy. Ministerstvo dopravy je státní orgán, který odpovídá za tvorbu státní politiky v oblasti dopravy. Ministerstvo dopravy má na starosti legislativu a zastupování v orgánech Evropské unie. Zároveň funguje jako odvolací orgán ve správním řízení proti rozhodnutí ÚCL. Úkolem úřadu pro civilní letectví je dozor nad letectvím v ČR, vydávání osvědčení, licencí a v případě pochybení může letecký subjekt sankcionovat. [3]

⁷ <https://www.caa.cz>



2. Systémy pro sběr, zpracování a analýzu dat regionálních dozorových institucí

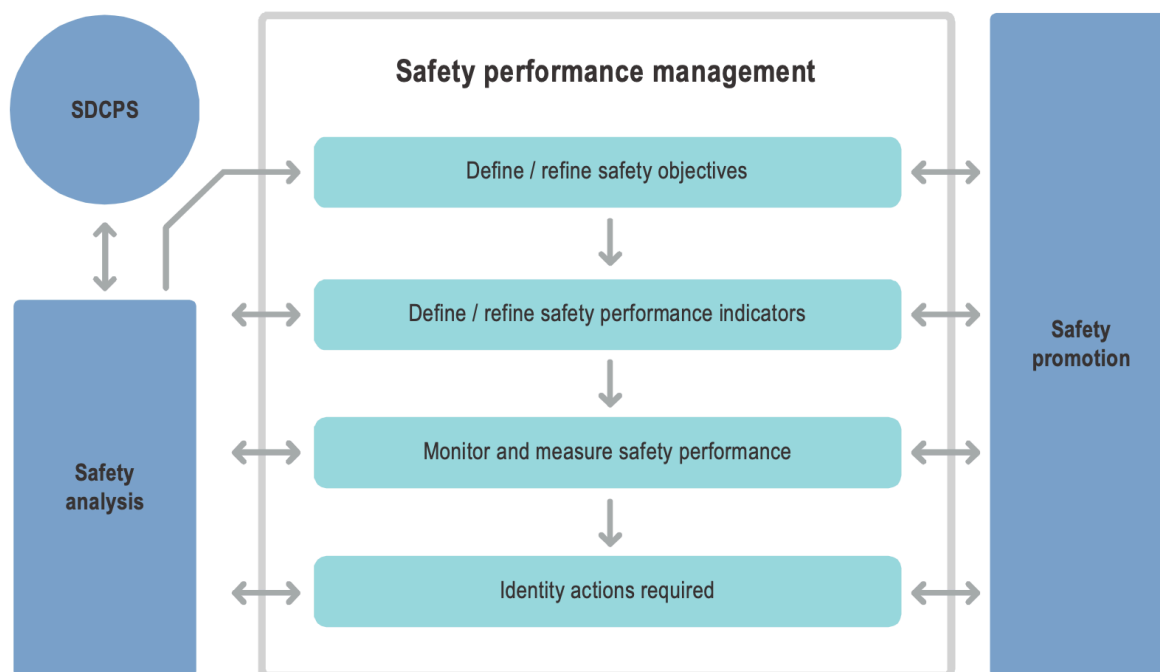
Sběr dat a následná jejich analýza je velice důležitá součást letectví. Výsledkem analýzy dat jsou informace o výkonnosti v bezpečnosti, případně, co je třeba vylepšit. Výsledná data jsou kritický ukazatel jak pro poskytovatele služeb, tak i pro organizace jako je ÚCL, EASA. [4]

Systém, který taková data sbírá a zpracovává je SDCPS (Safety Data Collection and Processing System). Tento systém získává interní a externí data od státu, který data sbírá od poskytovatelů služeb. Interní data jsou důvěrné informace státu a poskytovatelů služeb, které se týkají provozu, personálu a výkonnosti v bezpečnosti, které nejsou volně přístupné veřejnosti. Naopak externí data jsou volně dohledatelné. Stát, respektive ÚCL, je zodpovědný za to, aby data poskytovatelů služeb byla sbírána do SDCPS. Následně SDCPS tato data uloží, zpracuje a dále z těchto bezpečnostních dat vytvoří analýzu, která dá státu informace, kde hrozí nebezpečí a co je třeba vylepšit. Díky této analýze je možné zlepšit výkonnost v bezpečnosti daného státu. V případě, kdy úroveň bezpečnosti není taková, jak by měla odpovídat, je nutné, aby ÚCL použil své prostředky, které poskytovatelům služeb pomohou zvýšit úroveň bezpečnosti. Schéma, jak SDCPS funguje je ukázáno na obrázku 1. [4]

EASA Annual Safety Review je dokument rozdělen do několika kapitol, které pokrývají různá odvětví – obchodní leteckou dopravu, vrtulníky, bezmotorová letadla, provoz letiště a handlingu. Každá kapitola obsahuje portfolio bezpečnostních rizik. Dokument vydává každý rok EASA. Data získává z dostupných databází jako je EASA Occurrence Database a European Central Repository (ECR). Jedná se o databáze, kam jednotlivé státy hlásí události. Portfolio obsahuje přehled aktuálních bezpečnostních problémů, kde jsou označené rizikové oblasti, kterých se problém týká. Cílem je porozumět proč k událostem dochází a vytvořit postupy, které počty konkrétních událostí sníží. Bezpečnostní rizika jsou posuzována European Risk Classification Scheme, který odhaduje celkovou úroveň rizika daného bezpečnostního problému. [5]

EPAS (European Plan for Aviation Safety) je výsledkem analýzy z dat ECR, každý rok ho připravuje EASA. Tento evropský plán pro bezpečnost v letectví se zabývá tím, co je třeba

do budoucna vylepšit, aby se počty incidentů snížily a bezpečnost letectví zvýšila. Kromě přímých důvodů bere v potaz i skryté příčiny, které k nehodě vedly. [5]



Obrázek 1: SDCPS schéma [6]



3. Bezpečnostní taxonomie – typy událostí

Letecká taxonomie je soubor pojmů a jejich definicí, které se využívají při hlášení incidentů a nehod. Slouží k jejich jednotnému a přehlednému popisu.

Bezpečnostní letecká taxonomie se využívá k organizaci pojmů, které se v letectví používají. Vzhledem k složitému systému, jakým letectví je, je důležité mít pevně dané struktury taxonomie, které jsou přehledně uspořádány, aby mohly být správně použity. Ať už je bude používat expert při analýze nebo se bude jednat o vyplnění hlášení události. [7, 8]

Leteckých taxonomií existuje několik druhů. Dělí se podle toho, kdo je používá, jakým způsobem se s nimi dá pracovat anebo v jakém odvětví letectví jsou používány.

Mezi nejpoužívanější, komplexní taxonomie, které využívají experti na popis a kategorizaci událostí patří:

- ICAO ADREP – zahrnuje typy událostí s jejich popisem a klasifikací. Na základě této taxonomie vznikla taxonomie ECCAIRS.
- HEIDI – taxonomie slouží pro události spojené s řízením letového provozu, které by měly být ohlášeny. Jedná se o klasifikaci pojmů, které souvisejí s bezpečností řízení letového provozu. Využívá se, aby hlášení byly konzistentní po celé Evropě. Taxonomii navrhnul EUROCONTROL. [9]
- SM ICG Hazard Taxonomy – navržena mezinárodní spolupracující skupinou organizací (Safety Management International Collaboration Group), jejíž snahou je uplatnění taxonomie ve všech odvětvích letectví. Taxonomie je založena na 4 nebezpečích – technické, lidské, organizační a životní prostředí, které jsou vzájemně propojené. [10]
- ECCAIRS – taxonomie odvozená z ICAO ADREP taxonomie. Využívá ji systém ECCAIRS (European Co-ordination Center for Accident and Incident Reporting System), což je evropská digitální platforma, která slouží k hlášení nehod a incidentů. Tato data jsou dále sdílena, sbírána, analyzována a pomáhají k vylepšení bezpečnosti. ECCAIRS řídí EASA. [7]
- RIT (Reduced Interface Taxonomy) – jedná se o menší sadu pojmů než taxonomie ECCAIRS. Momentálně čítá přes 280 datových polí. Byla vytvořena k soustředění



se na hlášení povinných datových polí, které jsou definované v legislativě EU. K taxonomii RIT byl vytvořen souborový formát E5X, který umožňuje ověření dat před odesláním úřadu. [11]

Toto je krátký přehled taxonomií, se kterými se můžeme setkat. Pro svojí bakalářskou práci jsem si vybrala taxonomii ECCAIRS. Hlavním důvodem je, že taxonomie ECCAIRS se využívá k hlášení událostí v rámci Evropy. I na českých stránkách ÚZPLN jsou dvě možnosti – využití portálu ÚZPLN pro hlášení událostí nebo právě portál Aviation Safety Reporting, což je ECCAIRS portál pro hlášení událostí. Právě kvůli vysokému potenciálu ECCAIRS taxonomie jsem si ji zvolila pro svojí bakalářskou práci.

Pro porovnání jsem si vybrala ICAO ADREP taxonomii, která sloužila jako základ pro ECCAIRS taxonomii, protože mi přišlo zajímavé poukázat na rozdíly a podobnosti, které mezi taxonomiemi jsou.

Tabulka 1: Porovnání typů událostí ECCAIRS a ICAO ADREP

ECCAIRS	ICAO ADREP
Consequential Events (následná událost)	Consequential Events (následná událost)
Equipment (událost spojená s vybavením)	Aircraft/System/Component Related Event (událost související s letadlem/systémem/komponentem)
Operational (provozní typ události)	Aerodrome And Ground Aids Related Event (událost související s letištěm a pozemním vybavením)
	Air Navigation Services Related Event (událost související s letovými navigačními službami)
	Operation Of The Aircraft Related Event (událost související s provozem letadla)
	Events Related To Maintenance And Repair Of The Aircraft (událost související s údržbou a opravou letadla)
Personnel (události personálu)	Events Related To The Non-compliance With Regulations (událost související s nedodržováním předpisů)
Organisational (organizační typ události)	Civil Aviation Authority/Administration Related Event (událost související s úřadem pro civilní letectví (správa, administrativa))
Any Other Event (jiná událost)	An Event Other Than Listed Above (událost, která nebyla výše zmíněna)
Unknown (neznámá událost)	Unknown (Unknown) (neznámá událost)

V této tabulce (Tabulka 1) vidíme porovnání taxonomie ECCAIRS a ICAO ADREP. Vzhledem k tomu, že ECCAIRS vychází z taxonomie ICAO ADREP, můžeme si všimnout některých



podobností – *následná událost*. Kategorie se ale různě liší – počtem i názvy kategorií typů událostí. Při bližším prozkoumání taxonomie je jasné vidět, že taxonomie si je z velké části podobná, liší se převážně strukturou, kategorizací a názvy některých pojmů taxonomie. Barevné označení kategorií naznačuje, které kategorie si jsou nejvíce podobné, respektive jaké kategorie obsahují stejné/podobné pojmy taxonomie ECCAIRS a ICAO ADREP.

Nejzajímavější kategorie na porovnání je provozní typ události (*Operational*), která má kategorie, které jsou velice podobné ekvivalentním kategoriím ICAO ADREP s rozdílem, že jsou rozřazeny do podkategorií kvůli větší přehlednosti, například: *Aerodrome operations (letištní provoz)*, *Air navigation services (letové navigační služby)*, *Aircraft flight operations (letový provoz letadel)*, aircraft maintenance (údržba letadla).

Naopak rozdílnosti jsou zobrazeny v tabulce 2, kde můžeme vidět, že v obou taxonomiích existují pojmy, které v druhé chybí nebo jsou označeny jinak. Označení sloupců v tabulce L-0, L-1 a L-2 značí kategorie a podkategorie v taxonomii.

Tabulka 2: Rozdíly taxonomií ECCAIRS a ICAO ADREP

ECCAIRS				ICAO ADREP		
L-0	L-1	L-2	Popis události	L-0	L-1	L-2
Unknown (Neznámá událost)	Unknown (Neznámá událost)	-	-	Unknown (Neznámá událost)	Missing Aircraft (Pohřešované letadlo)	-
Consequential Events (Následná událost)	Flight Operation Outcome Event (Výsledek letové operace)	Undetermined (Neurčitý)	Missing Aircraft (Pohřešované letadlo)			
Consequential Events (Následná událost)	Flight Operation Outcome Event (Výsledek letové operace)	Outcome Events (Výsledek operace)	Abrupt Stop (Náhlé zastavení)	Consequential Events (Následná událost)	Abrupt Stop (Náhlé zastavení)	-
		Effect On Operations (Vliv na provoz)	Aircraft Return (Návrat letadla)		Aircraft Return (Návrat letadla)	-
		Emergency Situations (Nouzové situace)	Emergency Descent (Nouzový sestup)		Emergency Descent (Nouzový sestup)	-



ECCAIRS			ICAO ADREP		
L-0	L-1	L-2	L-0	L-1	L-2
Equipment (Událost spojená s vybavením)	4500 /4600	Maintenance Computer and Information System (Centrální počítačový a informační systém údržby)	Aircraft/System/Component Related Event (Typ události související s letadlem/systémem/komponentem)	4500	Maintenance Computer (Centrální počítač údržby)
	4500	Central Maintenance System (Centrální systém údržby)	-	-	-
	9500	Aircraft Special Purpose Equipment (Vybavení letadla pro zvláštní účely)	Aircraft/System/Component Related Event (Typ události související s letadlem/systémem/komponentem)	5100	Standard practices and structures (Standardní postupy a struktury)
	5800	Lighter-than-air/aerostat/Balloons/Airship specific (Specifikace pro letadla lehčí než vzduch, balony, vzducholodě)		1200	Servicing related event. (Události související se servisem)
	8400	Propulsion Augmentation (Zvýšení pohonu)		0600	Dimensions Area (Rozměry oblasti)
				0500	Time limits/maintenance check (Časové limity/kontrola údržby)
Aerodrome And ATM Equipment (Vybavení letiště a ŘLP)	ATM Surveillance Systems (ATM sledovací systémy)	Aerodrome and Ground Aids Related Event (Typ události související s letištěm a pozemním vybavením)	Air Traffic Management/Communication, Navigation and Surveillance serviceability related event (Událost týkající se provozuschopnosti řízení letového provozu/komunikace, navigace a dohledu)		



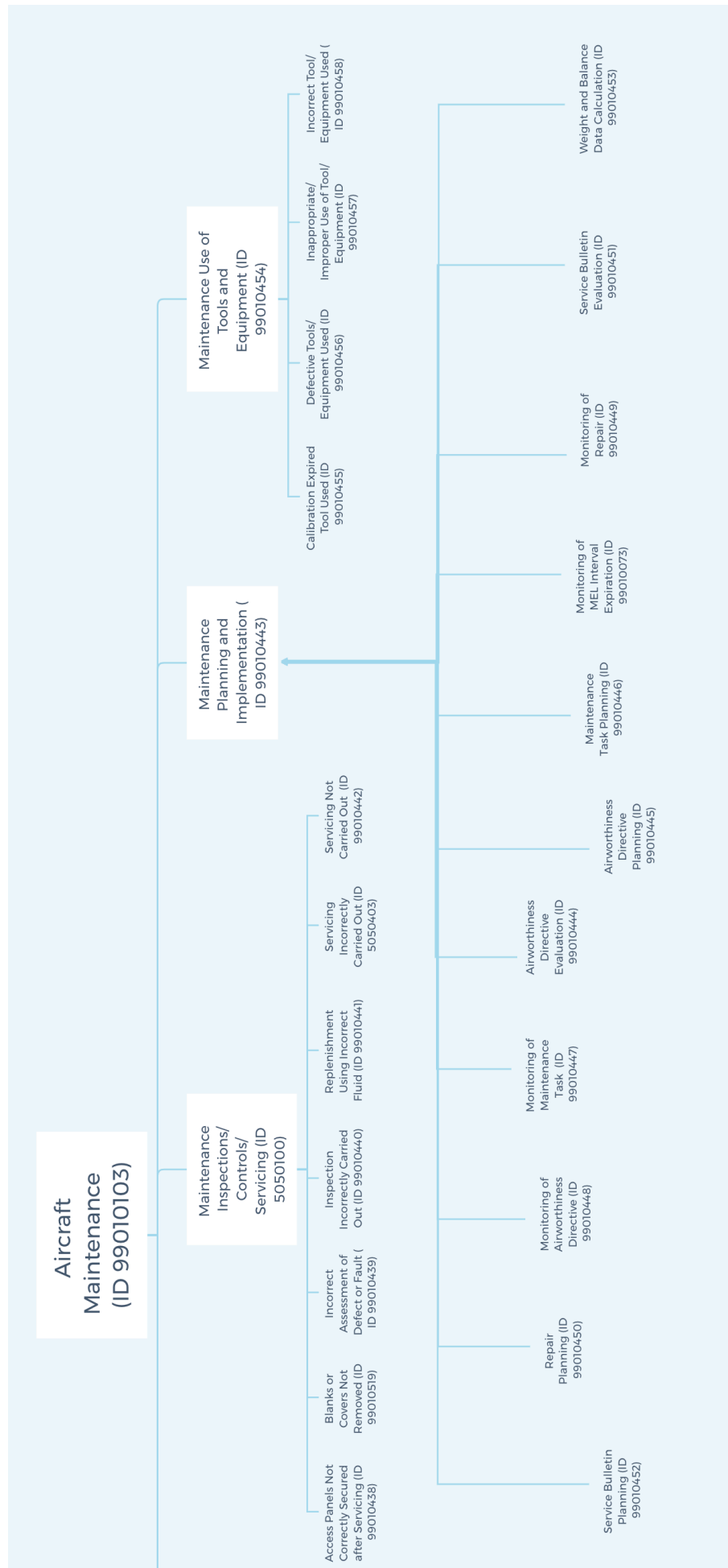
Pokud bychom chtěli nahlásit pohřešované letadlo, v taxonomii ECCAIRS tento pojem nalezneme v *následné události – výsledek letové operace – neurčený – pohřešované letadlo*. ICAO ADREP má pojem *pohřešované letadlo* pod *neznámá událost*.

Události jako *náhlé zastavení, návrat letadla* nebo *nouzový sestup* obě taxonomie řadí do kategorie *následná událost*, ale zatím co v taxonomii ICAO ADREP tento pojem najdeme přímo v této kategorii, taxonomie ECCAIRS tyto pojmy má zařazené v rámci různých podkategorií.

Dále v ECCAIRS nalezneme v kategorii události spojené s *vybavením* podkategorii *4500/4600 Centrální počítačový a informační systém údržby*, který se ale u ICAO ADREP liší – *4500 Centrální počítač údržby*. Zároveň v ECCAIRS existuje *4500 centrální systém údržby*, tento pojem má stejné číslo jako existuje v ICAO ADREP, ale má jiný název. [12, 13]

Další pojmy zobrazené v tabulce 2 z kategorie události spojené s *vybavením* označené čtyřčíslicím se vždy nacházejí buď v taxonomii ECCAIRS nebo ICAO ADREP.

Toto bylo krátké porovnání taxonomií ECCAIRS a ICAO ADREP. Na obrázku 2 je ukázka ECCAIRS taxonomie a jejího větvení. Jedná se o ukázku (nejedná se o celou taxonomii) provozního typu události (Operational). Kategorie provozní typ události (operational) se dále dělí na další kategorie. Na obrázku 2 je vidět ukázka podkategorie údržba letadel (Aircraft Maintenance), které se dále dělí na další podkategorie.



Obrázek 2: Ukázka větvení ECCAIRS taxonomie



4. Systémový pohled na bezpečnost (model STAMP)

STAMP (System-Theoretic Accident Model and Processes) poskytuje teoretický základ pro analýzu STPA (System Theoretic Process Analysis) a CAST (Causal Analysis based on System Theory). STAMP není přímo metoda, jedná se o model, který se skládá z předpokladů, proč nebo jak k nehodám dochází. Jedná se o alternativní model řetězových událostí, které na sebe navazují a podtrhují tradiční bezpečnostní techniky analýz. Výhodou STAMP je, že dokáže sjednotit a propojit do analýzy kauzální faktor jako je software, lidský faktor a lidské rozhodování, nové technologie atd, které se v současné době stávají větší hrozbou. [14]

Jedná se o model příčin nehod založený na systémové teorii. Posouvá tradiční model příčin nehod dále za řetězec přímo propojených poruch/závad jak událostí, tak poruch jednotlivých komponentů a zahrnuje komplexní procesy a nebezpečné interakce v systému mezi systémovými komponenty. [14]

STAMP pohlíží na bezpečnost jako na problém řízení systému, nikoliv jako na problém předcházení selhání komponentů. V modelu STAMP nejsou vynechány žádné příčiny, naopak jich je zahrnuto více a důraz je kladen na prosazení omezení systémového chování, nikoliv na předcházení selhání. [14]

Výhody využívání modelu STAMP jsou: jedná se o velice komplexní přístup, protože funguje od shora dolů, a ne od spodu nahoru. Myšleno hierarchicky od nejvyššího řídicího až po nejmenší řízené komponenty. Zahrnuje vše, od softwaru, organizace, lidského faktoru až po bezpečnostní kulturu. Z modelu systému se vytvoří řídicí struktura, ve které je hierarchicky zobrazeno, kdo co řídí. Zároveň zde nesmí chybět zpětná vazba. Efektivní řídicí struktura si bude prosazovat omezení na chování celého systému. Toto umožňuje vytvoření mnohem silnějších a lepších nástrojů, jako je STPA nebo CAST. [14]

STPA a CAST jsou dva nejrozšířenější nástroje modelu STAMP. [14]

STPA je proaktivní analýza, která dokáže zanalyzovat potenciál příčiny nehody již během vývoje systému, což znamená, že riziko může být buď úplně odstraněno nebo se alespoň může dostat pod kontrolu. [14]



CAST je reaktivní analýza, která zkoumá nehody či incidenty, ke kterým již došlo a identifikuje jejich příčiny. [14]

Důvod, proč jsem si z těchto dvou analýz zvolila STPA, a ne CAST je ten, že STPA je vhodnější analýza na řešení problematiky této práce. Pro vytvoření převodního systému taxonomie ECCAIRS je nutné mít analýzu, která dokáže pracovat s různými možnými událostmi, které mohou nastat. To je případ právě analýzy STPA, neboť dokáže nehodám předcházet tím, že se dá aplikovat na systém, který je teprve ve vývoji a může odhalit chyby systému, který ještě nebyl dokončen. Nebo v tomto případě dokáže pracovat s veškerými pojmy z taxonomie.

4.1. Aplikace STPA

Tato analýza má na rozdíl od starších, tradičních analýz zajišťování příčin incidentů nebo nehod spoustu výhod [14]:

- STPA předpokládá, že událost může být způsobena i nebezpečnými interakcemi mezi jednotlivými komponenty systému, ačkoliv systém jako takový funguje správně. Ostatní analýzy neberou tuto možnost v potaz.
- STPA zahrnuje do analýzy i software nebo lidský faktor, což zajišťuje všechny potenciální příčiny ztrát. To je velice důležité, vezmeme-li v potaz, že lidský faktor hraje roli v 70-80 % leteckých nehodách.
- Tato analýza je také schopná odhalit „neznámou příčinu typu události“ i ve velice komplexním systému jako je letectví. To je něco, co je pro klasické analýzy velice náročné. STPA je vhodná i na použití během vývoje procesu, protože dokáže odhalit potenciální chyby systému již při jeho vývoji a zamezit tak zbytečným ztrátám nebo je alespoň omezit.
- STPA předpokládá, že každý komponent funguje samostatně. Když se modeluje systém, každý komponent, subsystém je nezávislý. Při analýze se zkoumá, jak funguje daný komponent samostatně, s výjimkou bezprostředně předcházejících a následujících událostí. Komponenty se chovají stejně, jak v případě, kdy jsou zkoumány samostatně, tak i když jsou zkoumány, jak fungují v celku. Tradiční analýzy fungují na dekompozici. To znamená, že základní přístup je rozložení systému na komponenty a předpokládá se, že příčinou nehody byla porucha komponentu. Vypočítá se pravděpodobnost poruchy komponentu na každém



komponentu zvlášť a jako výsledek analýzy se kombinují předpoklady typů interakcí mezi komponenty které mohou nastat. STPA uvažuje ale i to, že problémem nemusí být jednotlivé komponenty jako takové, ale problém může nastat v systému jako v celku. Komplikované mohou být i přesahy mezi komponenty a subsystémy.

- STPA není analýza, která by se využívala jen v letectví, je vhodná pro jakýkoliv složitý, komplexní systém s pokročilou technologií, kde hrozí nějaké nebezpečí či ztráta. Uplatňuje se v automobilovém průmyslu, železniční dopravě, v chemickém průmyslu, v obranných systémech nebo může být použita i v systému jaderné elektrárny a další.
- STPA je také méně náročná co se týče času nebo prostředků než ostatní tradiční analýzy.
- STPA poskytuje dokumentaci systémových funkcí, které často nejsou součástí nebo chybí v komplexních systémech.
- Při vyhodnocení a porovnání s dalšími, tradičními analýzami, STPA dokázala najít stejné příčiny jako tradiční analýzy, dokonce jich našla i více, a to takové, které tradiční analýzy odhalit nedokázaly.

STPA analýza se skládá ze 4 kroků.

- 1) Nejprve si musíme určit systém, se kterým budeme pracovat, případně i prostředí, ve kterém se systém nachází. V prvním kroku je také důležité identifikovat si ztráty a systémové nebezpečí, které by v systému mohly nastat. Ztráty jsou více obecné než systémové nebezpečí, seznam ztrát z STPA je vidět v tabulce 3, které jsou dostačující pro události. Jde pouze o příklad ztrát, který může nastat v letectví. (Mají označení L – Loss). Systémové nebezpečí je už více specifické a záleží na jednotlivých událostech. V tabulce 4 můžeme vidět ukázkou systémových nebezpečí, nejedná se o všechny možnosti pro všechny systémy. V hranaté závorce je odkaz na ztráty, ke kterým vede dané systémové nebezpečí. (Značí se H – Hazard).



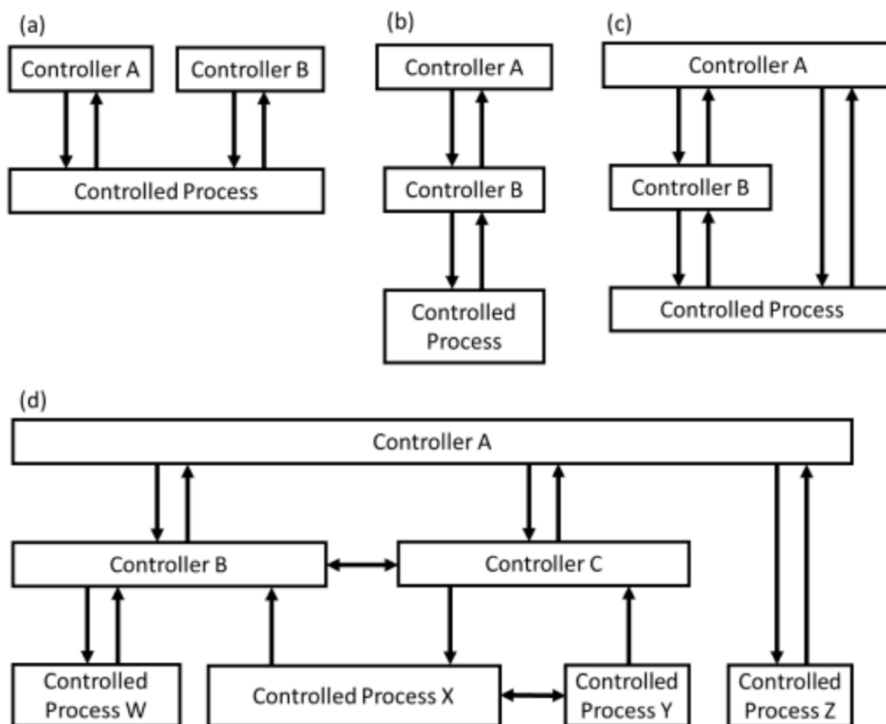
Tabulka 3: Obecné ztráty

Obecné ztráty
L-1: Ztráta života nebo zranění
L-2: Ztráta nebo poškození prostředku (letadla)
L-3: Ztráta nebo poškození předmětu mimo letadla
L-4: Ztráta mise (přeprava)
L-5: Ztráta spokojenosti zákazníka
L-6: Ztráta citlivých informací
L-7: Ztráta vůči životnímu prostředí

Tabulka 4: Obecné systémové nebezpečí

Obecné systémové nebezpečí
H-1: Letadlo poruší minimální standard rozestupů za letu. [L-1, L-2, L-4, L-5]
H-2: Ztracení integrity draku letadla. [L-1, L-2, L-4, L-5]
H-3: Letadlo opustí určenou dráhu, pojezdovou dráhu nebo odbavovací plochu. [L-1, L-2, L-5]
H-4: Letadlo se přiblíží příliš blízko k jiným objektům na zemi. [L-1, L-2, L-5]
H-5: Vozidlo/letadlo nedodrží bezpečnou vzdálenost od terénu a jiných překážek. [L-1, L-2, L-3, L-4]

- 2) Druhým krokem je model řídicí struktury. Jedná se o hierarchický model, který ukazuje, kdo je řídící. (V modelu bývá řídicích více. Může být model, kdy jeden řídící řídí dalšího řídicího nebo dva řídící řídí jeden stejný proces, jak je vidět na obrázku níže – obrázek 3 [14]. Řídící (Controller) řídí řízený proces (Controlled proces) pomocí řídicích akcí (Control action) a dostává zpětnou vazbu (Feedback), aby měl přehled o situaci a případně mohl zasáhnout, bylo by to nutné.



Obrázek 3: Hierarchické modely [15]

- 3) Ve třetím kroku je nutné identifikovat veškeré nebezpečné řídicí akce. Nebezpečná řídicí akce je ta řídicí akce, která v nejhorším případě povede k systémovému nebezpečí (které vede ke ztrátě). V tomto kroku je nutné si vypsát všechny řídicí akce z modelu a stanovit, v jakém kontextu povede řídicí akce k systémovému nebezpečí. Výsledek vypadá tak, že máme tabulku, kde nám vznikne nebezpečná řídicí akce podle toho, pokud řídicí akce nebude poskytnuta a způsobí systémové nebezpečí, pokud bude poskytnuta a způsobí systémové nebezpečí, bude-li poskytnuta brzy/pozdě nebo ve špatném pořadí, nebo bude řídicí akce zastavena příliš brzy/aplikace bude příliš dlouhá.

Nebezpečné řízení má jasně definovanou strukturu. Uspořádání není rozhodující, důležité je, aby nebezpečné řízení obsahovalo všechny části, které jsou:

- Zdroj – kdo poskytuje (nebezpečnou) řídicí akci. Řídicí akci poskytuje řídící.
- Typ – jedna ze 4 variant nebezpečného řízení – neposkytnutí způsobí systémové nebezpečí, poskytnutí způsobí systémové nebezpečí, poskytnutí příliš brzy/pozdě/ve špatném pořadí způsobuje systémové



nebezpečí, zastaveno příliš brzy/příliš dlouhá aplikace způsobí systémové nebezpečí.

- Řídící akce – řídící akce, která povede k systémovému nebezpečí.
 - Kontext – důležitá informace, která nám říká, kdy, jak nebo proč k systémovému nebezpečí dojde.
 - Odkaz k systémovému nebezpečí – tato informace nám řekne, k jakému systémovému nebezpečí nebezpečná řídící akce povede.
- 4) Posledním krokem je identifikace ztrátových scénářů. Zde uvažujeme, proč k nebezpečné řídící akci došlo a proč byly řídící akce, které vedly k systémovému nebezpečí provedeny/neprovedeny nebo provedeny špatně.



5. Přehled vědecké literatury

Tématu provázání leteckých taxonomií a typů událostí v modelu STAMP se prozatím nikdo nevěnoval.

Jak již bylo zmíněno výše, STPA není pouze analýza využívající se v letectví. Na příklad Technická univerzita Graz pracovala na tom, jaký vliv má lidský faktor na silniční bezpečnost v Rakousku a jak ji analýza STPA může vylepšit. [16]

STPA bylo také použito při analýze národních odpovědí na pandemii COVID-19. [17]

V letectví byla STPA analýza použita třeba v Číně (Air Force Engineering University, Xi'an), kde se analyzovala a hodnotila bezpečnost letu letadla na základě modelu IDAC-STPA. [18]

Další literatura se věnuje bezpečnosti a dohledem nad bezpečností.

Na příklad, rizikovým faktorům, které jsou brány jako základní bezpečnostní nástroj, v souladu s bezpečnostními předpisy a bezpečnostními standardy se zabývala fakulta Undang-Undang na technické univerzitě MARA, v Malajsii. [19]

Nebo implementaci a dalšímu rozvoji systému GASOS (Global Aviation Safety Oversight System), který uznává a monitoruje regionální organizace pro dohled nad bezpečností se věnoval A. A. Batalov v článku Global Aviation Safety Oversight System: Challenges and Opportunities for ICAO and its Member States. [20]



6. Limitace současného stavu

Vzhledem k náročnému a komplexnímu systému, kterým letectví je, je dáván velký důraz na bezpečnost. Bohužel, v současném systému stále existují skuliny, se kterým systém nedokáže počítat. Jako velký problém vidím lidský faktor, který je těžko předvídatelný a současné analýzy nepočítají se všemi možnostmi, které mohou nastat. Komplikací může být i složitost systému, protože současný systém nebere v potaz nebezpečné interakce mezi jednotlivými komponenty, pokud systém jako takový funguje správně.

Problémem může být pro někoho i složitost vyznat se v taxonomii a správně vyplnit hlášení. Určitě by se systém nahlašování událostí dal vylepšit tak, aby se podle vložených informací filtrovaly další kolonky, které je třeba vyplnit, a naopak ty kolonky, které s událostí nesouvisí by automaticky zmizely.

Pokud se někdy rozhodneme přečíst si hlášení události, může se stát, že v hlášení nebude jasně určená příčina. Respektive, byla zjištěna hlavní příčina, proč k události došlo, nikoliv jaké události k tomu vedly. A toto je klíčové, protože pokud nejsme schopni zjistit, co vedlo k události, nebudeme schopni jí příště zabránit. V hlášení ale často narazíme spíš na obecné pojmy jako „špatně provedená údržba“, ale už tam nebude napsané, proč byla špatně provedená, přitom možností je spousta – pracovník mohl být přepracovaný, v časové tísní, unavený, dostatečně neznal postupy. STPA analýza by tyto problémy z velké části dokázala odstranit a tyto důležité informace by v hlášení nechyběly. Navíc počítá s lidským faktorem i s neznámou příčinou. Bere na vědomí i nebezpečné interakce mezi komponenty. Dokonce dokáže odhalit i příčiny, které jiné analýzy odhalit nedokážou. Implementace STPA je poměrně jednoduchá a analýza STPA je časově méně náročná než ostatní analýzy.

Propojení taxonomie ECCAIRS s analýzou STPA by tyto problémy mohlo vyřešit, neboť převodní systém, kterému se tato práce věnuje, by usnadnil analýzu události, protože velkou část pojmů taxonomie dokážeme definovat jako ztrátu, systémové nebezpečí, řídicí akci, nebezpečnou řídicí akci, kauzální faktor. To znamená, že při nové události budeme jasně vědět, kde nastal problém – jaký kauzální faktor vedl ke vzniku nebezpečné řídicí akce, která vedla k systémovému nebezpečí, který potenciálně vedl ke ztrátě.



7. Metodika

Při tvoření praktické části jsem postupovala tak, že jsem si vybrala 6 událostí. Jako zdroj událostí jsem použila stránky ÚZPLN⁸ (Ústav pro odborné zjišťování příčin leteckých nehod) a AAIB⁹ (Air Accidents Investigation Branch). Díky dvěma různým zdrojům jsem mohla porovnat rozdíly závěrečných zpráv a zároveň jsem měla lepší výběr událostí, který byl třeba k co největšímu pokrytí rozsáhlé taxonomie.

Po nastudování hlášení události jsem následně vytvořila řídicí strukturu, kde jsem určila řídicí, řídicí akce, zpětné vazby, systém a postupovala jsem dle kroků STPA. To znamená – určení ztrát a systémového nebezpečí, vytvoření tabulky nebezpečných řídicích akcí, a nakonec vytvoření scénářů.

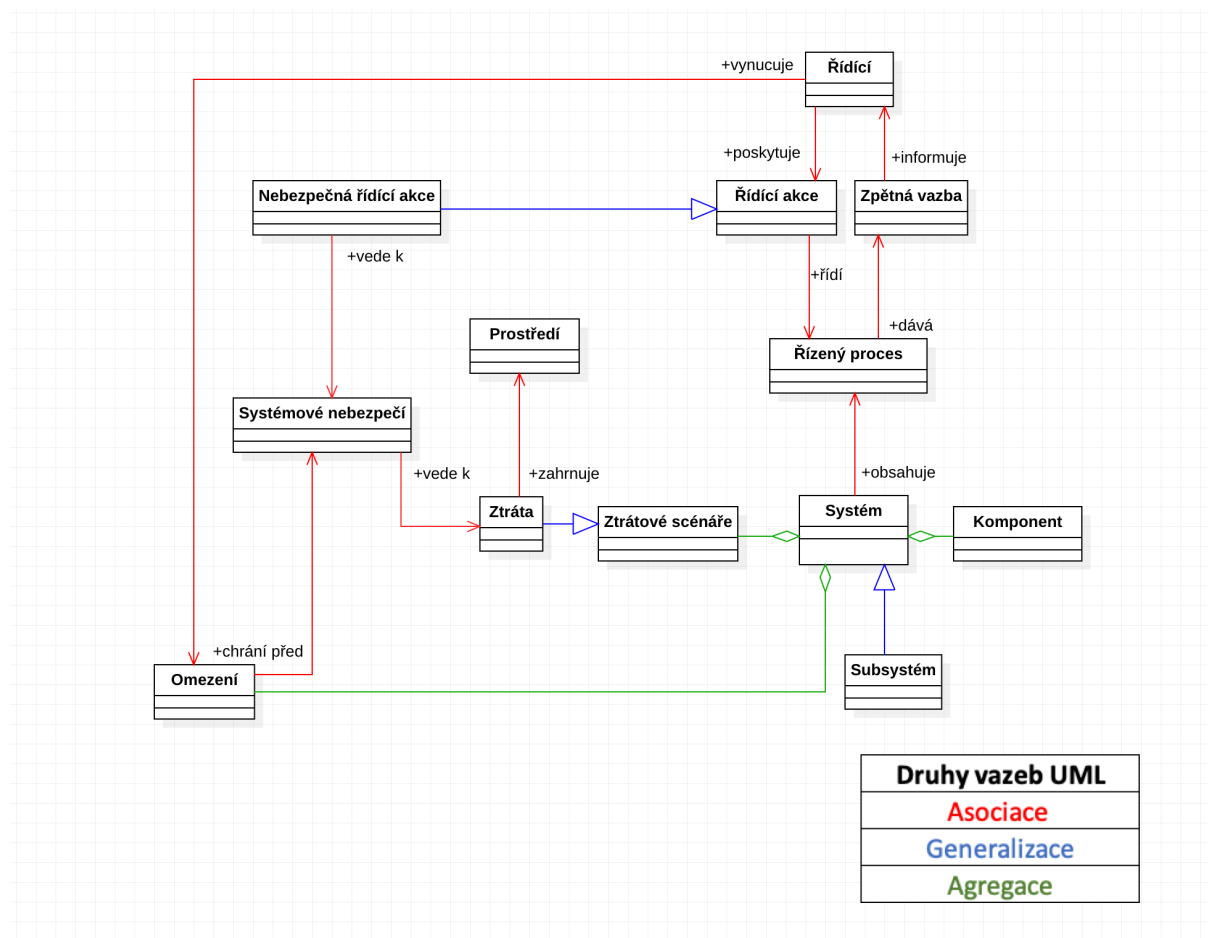
7.1. UML

Dalším krokem bylo vytvoření UML modelu události s použitím ECCAIRS taxonomie. UML (Unified Modeling Language) je modelovací jazyk, který nám díky svým funkcím dokáže namodelovat systém se všemi potřebnými informacemi, které při modelování události potřebujeme. Modelovacích jazyků existuje celá řada s různou řadou specializací. Výhodou UML jazyku je, že je univerzální, jednoduchý na modelování, nabízí několik druhů vazeb, které díky jasné definici zpřehledňují i složitější modely. Dále nabízí využití i stereotypu, který nám označuje význam nebo kategorii třídy. UML má i další, složitější funkce, které v této práci nebyly využity.

Systém namodelujeme tak, že využijeme diagram tříd. Třidu chápeme jako „box“ neboli objekt. Z objektů následně tvoříme celý systém. Třídy nám zobrazují řídicí, řídicí akce, systémové nebezpečí atd. U tříd také určíme stereotyp, který nám charakterizuje danou třídu, například: ztráta, událost, proces, předmět, osoba. Následně třídy propojíme jednou ze tří různých vazeb (UML nabízí celkem 7 vazeb, nám k modelování postačí 3), které se v UML používají. Tři vazby, se kterými se v této bakalářské práci setkáme jsou zobrazeny na obrázku 4. [21]

⁸ <https://uzpln.cz/zpravy-ln>

⁹ <https://www.gov.uk/aaib-reports>



Obrázek 4: UML vazby

Popis jednotlivých druhů vazeb UML [21]:

- Přímá asociace – vazba, která spojuje dvě třídy, které mohou existovat nezávisle na sobě. Směr šipky vazby nám specifikuje odkaz na druhou třídu, která může být doplněná o popis. Vazbu pak čteme jako – *Řídící poskytuje řídicí akce*. Nebo *zpětná vazba informuje řídící*.
- Generalizace – tato vazba označuje vztah mezi obecnou třídou s její konkrétnější třídou. (*Systém – subsystem*).
- Agregace – specifická vazba, která naznačuje vztah mezi třídami typu celek a jeho část, jak je vidět na obrázku 3 – *Komponent je součástí systému*.

Model byl tedy vytvořen za použití typů událostí taxonomie ECCAIRS (některé pojmy např.: letadlo, zaměstnanec řízení letového provozu (zaměstnanec ŘLP), vozidlo atd, byly



přidány pro přesnější a srozumitelnější popis události). Dále byly určeny (stejně jako v řídicí struktuře) STPA pojmy – ztráta, systémové nebezpečí, nebezpečná řídicí akce.

7.2. ECCAIRS hlášení

Jako poslední krok jsem vyplnila informace v ECCAIRS hlášení událostí, které souvisejí s typy událostí (damage, injuries, events). Hlášení se musí vyplňovat z několika důvodů. Nejprve, nám přesně popíše událost, ke které došlo. Toto jsou důležité informace nejen pro šetření události, ale také pro sbírání, sdílení a analýzu dat (kapitola 2), kde nám analýza řekne, kde hrozí největší nebezpečí, a co je třeba vylepšit. Díky takovým analýzám jsme schopni zvýšit výkonnost v bezpečnosti v letectví. Pro tuto práci je hlášení důležité, protože nám pomůže ve vytvoření převodního systému.



8. Analýza nehod a incidentů pomocí STPA a ECCAIRS taxonomie

V této kapitole budou detailně popsány a následně zanalyzovány tři události. Přesné kroky byly popsány v předešlé kapitole 7 -Metodika.

8.1. Událost 1 – kouř na palubě letadla

Průběh události

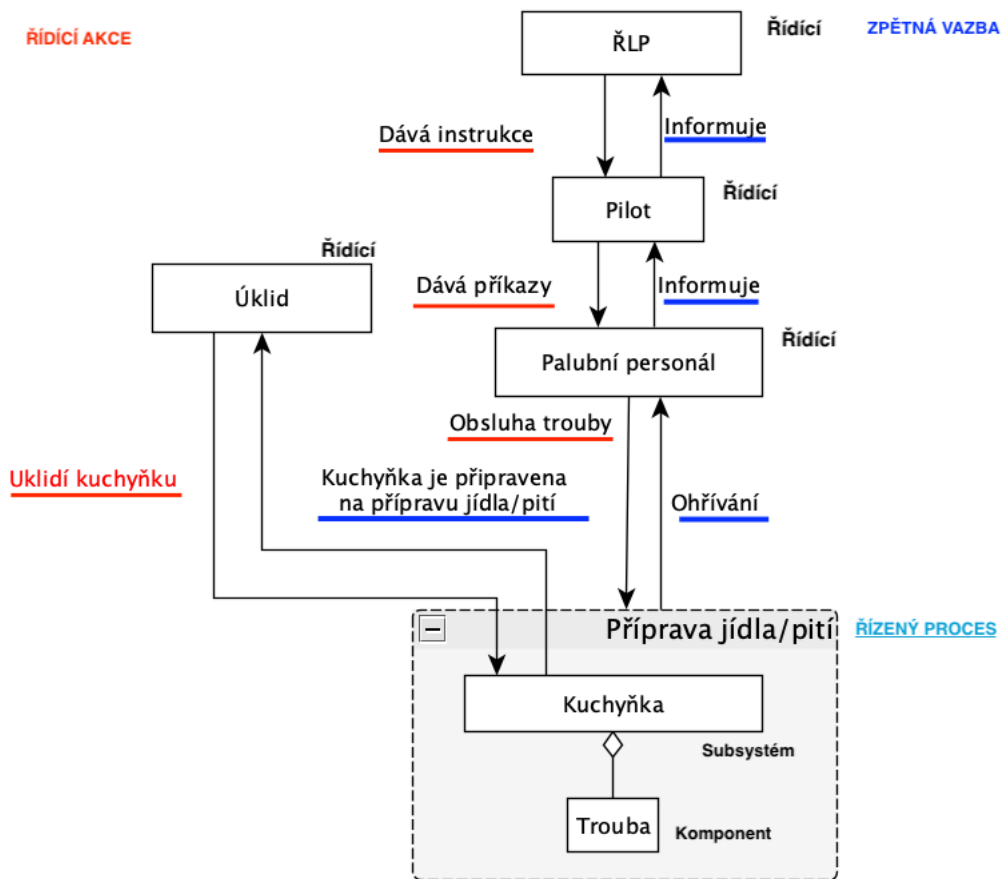
Událost se stala 8.července 2017 v 6:00. Během letu z Manchesteru (UK) do Girony (Španělsko) došlo k rozsáhlému kouři, který se šířil z trouby v kuchyňce během přípravy občerstvení. Palubní personál se snažil zasáhnout a kouř zastavit. Bohužel marně a muselo se nouzově přistát v Londýně – Gatwick. [22]

Po šetření bylo zjištěno, že trouby byly umyté nesprávným přípravkem, který nebyl určen pro trouby, což způsobilo kouř. [22]

Událost byla klasifikována jako vážný incident. Došlo k lehkému zranění tří členů palubní posádky. Z 204 cestujících nebyl nikdo zraněn. [22]

Řídící struktura události 1 dle modelu STAMP

Na obrázku 5 vidíme řídicí strukturu události 1 – kouř na palubě letadla. Řídící struktura (součást kroku 2 STPA) nám ukazuje hierarchickou řídicí strukturu modelu systému/události, která byla vytvořena podle hlášení a skládá se z řídicích akcí a zpětných vazeb. Vidíme zde všechny účastníky události – ŘLP, pilota, palubní personál a úklid. Díky této řídicí struktuře je jasné, kdo je řídicí, od koho dostává zpětné vazby, jaké zde probíhají řídicí akce, a co je řízený proces. Taková řídicí struktura nám pomůže zjistit, kde může vzniknout problém, a jak posílit systém. Červeně je zvýrazněná nebezpečná řídicí akce, která v této události vedla k systémovému nebezpečí (kouř na palubě letadla) a následně ke ztrátě (nouzové přistání, zranění, poškození letadla).



Obrázek 5: Řídící struktura – událost 1

V momentě, kdy máme model události, je nutné v rámci prvního kroku STPA ještě identifikovat ztráty a systémová nebezpečí. V této události došlo k systémovému nebezpečí H-1: Kouř na palubě letadla, který vedl ke ztrátám (ty byly zmíněny v obecných ztrátách – tabulka 3). toto systémové nebezpečí následně vedlo k těmto konkrétním ztrátám:

- L-1: Zranění 3 členů posádky
- L-2: Kouř poškodil letadlo
- L-4: Letadlo muselo nouzově přistát a nedoletělo do své plánované destinace

V tabulce 5 si všimneme, že systémové nebezpečí je označeno jako H-1: Kouř na palubě letadla [L-1, L-2, L-4], v hranaté závorce je odkaz na ztráty. Tento typ označení se využívá i v dalších krocích STPA.



Tabulka 5: Ztráty a systémové nebezpečí – událost 1

Kouř na palubě letadla – ztráty
L-1: Ztráta života nebo zranění
L-2: Ztráta nebo poškození prostředku (letadla)
L-4: Ztráta mise (přeprava)
Kouř na palubě letadla – systémové nebezpečí
H-1: Kouř na palubě letadla [L-1, L-2, L-4]

Třetím krokem STPA je určení nebezpečných řídicích akcí. Výše již bylo zmíněno (kapitola 2.4.), jak se nebezpečné řídicí akce tvoří. A níže vidíme tabulku 6 – tabulka nebezpečných řídicích akcí pro událost kouř na palubě letadla. Tabulka nebezpečných řídicích akcí není kompletní, jsou zde zobrazeny jen nebezpečné řídicí akce, které odpovídají úklidu kuchyňky. Kompletní tabulka nebezpečných řídicích akcí STPA musí zobrazovat veškeré řídicí a jejich řídicí akce, ale v této ukázce jsou důležité pouze nebezpečné řídicí akce, které se týkají úklidu kuchyňky.

V tabulce 6 je pak červeně zvýrazněná nebezpečná řídicí akce provedená pracovníkem úklidové společnosti, která v této události vedla k nebezpečí a následně ke ztrátě.

Pojem N/A (not applicable) znamená, že pole v tabulce nelze vyplnit.

Tabulka 6: Nebezpečné řídicí akce – událost 1

Řídicí akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Úklid kuchyňky	Pracovník úklidové společnosti neposkytne úklid kuchyňky (trouby) před letem. [H-1]	Pracovník úklidové společnosti poskytne úklid kuchyňky (trouby) špatným čisticím prostředkem před letem. [H-1]	Pracovník úklidové společnosti nedodrží postup a použije čisticí prostředky ve špatném pořadí/množství. [H-1]	N/A

Posledním čtvrtým krokem STPA je identifikace ztrátových scénářů. V tabulce 7, je znázorněná nebezpečná řídicí akce, která vedla k systémovému nebezpečí, které vedlo ke ztrátě. Z této nebezpečné řídicí akce potom byly vytvořeny 2 ztrátové scénáře.



Tabulka 7: Ztrátové scénáře – událost 1

Nebezpečná řídicí akce:	Pracovník úklidové společnosti poskytne úklid kuchyňky (trouby) špatným čisticím prostředkem před letem. [H-1]
Scénář 1:	Pracovník úklidové společnosti umyje troubu špatným čisticím prostředkem, protože nebyl dostatečně zkušený a vyškolený. Výsledkem byl vznik kouře na palubě a nutné nouzové přistání.
Scénář 2:	Pracovník úklidové společnosti umyje troubu špatným čisticím prostředkem, protože je v časové tísní a omylem si zamění čisticí tekutiny. Výsledkem byl vznik kouře na palubě a nutné nouzové přistání.

Důležité informace z hlášení události

Hlášení, které se musí vyplnit, pokud dojde k události, je velice komplexní a obsahuje spoustu důležitých informací – kdy a kde se událost stala, popis události, zda se jednalo o incident, vážný incident nebo nehodu, informace o poškození nebo zranění atd.

Vzhledem k tématu této bakalářské práce, zde budou zmíněny typy událostí, poškození a zranění. Ukázka hlášení je na obrázku 6. Typy událostí se zaznamenávají do kolonky EVENT, kde je na výběr ze všech typů událostí, které v taxonomii existují. Jak je zde ukázáno, do typů událostí spadá systémové nebezpečí, nebezpečná řídicí akce a kauzální faktor. Kromě hlášení tedy můžeme vidět i základní myšlenku převodního systému z STPA do ECCAIRS.

Zajímavé je, že poškození nebo zranění se v hlášení vyplňuje dvakrát – jednou v samostatné kolonce – DAMAGE/INJURIES, a dále informace o poškození/zranění nalezneme v kategorii *následné události*. Je to z toho důvodu, že informace o zranění nebo poškození leteckého vybavení (letadlo, letištní vybavení, navigační vybavení...) mají vliv na bezpečnost a je nutné mít tyto informace konkrétně poznamenané v hlášení. Tedy do kolonky EVENT se vyplní informace typ události, k jakému zranění/poškození došlo. Informace o zranění – vážnost zranění (žádné/malé/vážné/fatální) a počet zraněných osob (na palubě i na zemi) se vyplní samostatně do kolonky INJURIES. Informace o poškození se vyplní do kolonky DAMAGE pouze v případě, pokud dojde k poškození „třetí strany“, to znamená, pokud během události dojde k poškození



přímého účastníka, údaje o poškození se zadávají pouze do kolonky EVENT (Consequential event – následná událost).

DAMAGE Poškození - ZTRÁTA		
Third party damage:	<input type="text"/>	+
Object damaged:	<input type="text"/>	+
INJURIES Zranění - ZTRÁTA		
Injury level*:	<input type="text" value="Minor"/>	
	SERIOUS	MINOR
Total on ground	<input type="text" value="0"/>	<input type="text" value="0"/>
Total on aircraft	<input type="text" value="0"/>	<input type="text" value="3"/>
EVENTS Typ události - KAUZÁLNÍ FAKTOR		
Event type:	<input type="text" value="Personnel > Experience and Knowledge Events > Knowledge Events > Knowledge of Equipment or Aircraft"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > Standing > Standing : Other"/>	
EVENTS Typ události - NEBEZPEČNÁ ŘÍDÍCÍ AKCE		
Event type:	<input type="text" value="Operational > Aircraft Maintenance > Maintenance Use of Tools and Equipment > Inappropriate/Improper Use of Tool/Equipment"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > En-route > Cruise"/>	
EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ		
Event type:	<input type="text" value="Equipment > Aircraft General Explosions/Fire/Fumes/Smoke Events > Smoke > Smoke - Passenger Cabin"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > En-route > Cruise"/>	
EVENTS Typ události - ZTRÁTA		
Event type:	<input type="text" value="Consequential Events > Damage and Injuries Events > Medical and Injury > Impairment - Cabin Crew"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > En-route > Cruise"/>	
EVENTS Typ události - ZTRÁTA		
Event type:	<input type="text" value="Consequential Events > Flight Operations Outcome Events > Effect on Operations > Diversion - Medical Reasons"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > En-route > Cruise"/>	
EVENTS Typ události - ZTRÁTA		
Event type:	<input type="text" value="Consequential Events > Flight Operations Outcome Events > Emergency Situations > Forced Landing"/>	
Phase:	<input type="text" value="Powered Fixed-wing aircraft > En-route > Cruise"/>	

Obrázek 6: Důležité informace z hlášení – událost 1



Událost namodelovaná ECCAIRS taxonomií

Obrázek 7 zobrazuje událost namodelovanou v UML jazyce. Jak již bylo zmíněno v kapitole 7, tímto grafickým jazykem lze jednoduše namodelovat systém a potřebná data o systému.

Jednotlivé barvy v modelu na obrázku 7 naznačují rozdělení pojmů taxonomie ECCAIRS:

- Žlutá – následná událost
- Modrá – událost spojená s vybavením
- Zelená – události personálu
- Černá – provozní typ události
- Modré ohraničení třídy – kontextuální pojmy
- Červené ohraničení třídy – přidané pojmy

8.2. Událost 2 – únik paliva

Postup u druhé události byl stejný jako u události 1 – kouř na palubě letadla, proto jsou zde ukázány jen modely a tabulky, které jsou výsledkem shodného postupu, který byl již popsán v události 1.

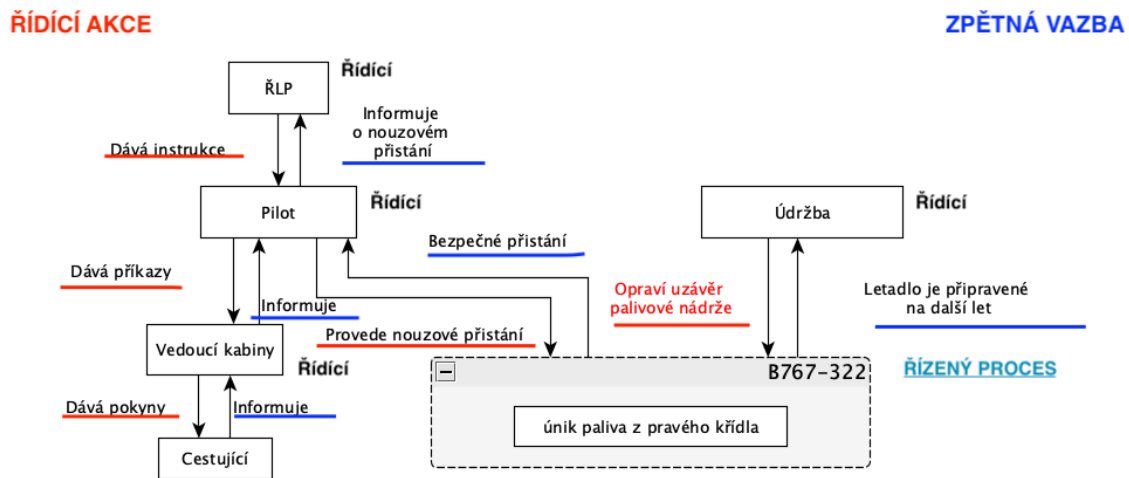
Průběh události

Událost se stala 12.července 2016 v 7:29 krátce po startu letu z Londýna Heathrow do Chicaga, když si cestující všiml, že z pravého křídla uniká palivo. Letadlo bylo nuceno nouzově přistát v Edinburghu. Druhý den, po opravě uzávěru nádrže odletěla pouze posádka. Během vzletu si všimla, že z pravého křídla opět uniká palivo. Letadlo opět přistálo v Edinburghu. [23]

Během rozsáhlejší údržby bylo zjištěno, že těsnění bylo pravděpodobně špatně nainstalováno a během provozu se postupně opotřebovávalo, a proto začalo docházet k úniku paliva. [23]

Událost byla klasifikována jako vážný incident. Nedošlo ke zranění jedenáctičlenné posádky, ani cestujících, kterých bylo 120. [23]

Řídící struktura události 2 dle modelu STAMP



Obrázek 8: Řídící struktura – událost 2

Tabulka 8: Ztráty a systémové nebezpečí – událost 2

Únik paliva – ztráty
L-2: Ztráta nebo poškození prostředku (letadla)
L-4: Ztráta mise (přeprava)
Únik paliva – systémové nebezpečí
H-1: Únik paliva [L-2, L-4]

Tabulka 9: Nebezpečné řídicí akce – událost 2

Řídící akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Oprava uzávěru palivové nádrže	Pracovník údržby neposkytne nutnou opravu palivové nádrže po nouzovém přistání. [H-1]	Pracovník údržby provede špatně nutnou opravu palivové nádrže po nouzovém přistání. [H-1]	Pracovník údržby provede opravu palivové nádrže ve špatném pořadí/ špatným zařízením/ prostředky. [H-1]	N/A



Tabulka 10: Ztrátové scénáře – událost 2

Nebezpečná řídicí akce:	Pracovník údržby provede špatně nutnou opravu palivové nádrže po nouzovém přistání. [H-1]
Scénář 1:	Pracovník údržby provede opravu uzávěru palivové nádrže po nouzovém přistání z důvodu úniku paliva. Nevšimne si ale, že problém není v uzávěru palivové nádrže, ale v těsnění, které bylo špatně instalováno a během provozu se opotřebovalo. V důsledku během následujícího letu došlo opět k úniku paliva a nouzovému přistání

Důležité informace z hlášení události

Na následujícím obrázku 9 je vidět informace o poškození a zranění – k žádnému nedošlo. Dále systémové nebezpečí a nebezpečná řídicí akce, které stejně jako v události

DAMAGE Poškození - ZTRÁTA

Third party damage: + Object damaged: +

INJURIES Zranění - ZTRÁTA

Injury level*: None

	SERIOUS	MINOR
Total on ground	<input type="text"/>	<input type="text"/>
Total on aircraft	<input type="text"/>	<input type="text"/>

EVENTS Typ události - KAUZÁLNÍ FAKTOR

Event type: Personnel > Situational Awareness and Sensory Events > Personnel Perception Events > Identification/Recognition

Phase: Powered Fixed-wing aircraft > Standing > Standing : Other

EVENTS Typ události - NEBEZPEČNÁ ŘÍDICÍ AKCE

Event type: Operational > Aircraft Maintenance > Maintenance Inspections/Controls/Service > Servicing Incorrectly Carried Out

Phase: Powered Fixed-wing aircraft > Standing > Standing : Other

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type: Equipment > 2800 Fuel System > 2801 Fuel Leak

Phase: Powered Fixed-wing aircraft > Take-off > Initial climb

EVENTS Typ události - ZTRÁTA

Event type: Consequential Events > Flight Operations Outcome Events > Emergency Situations > Mayday Fuel Declaration

Phase: Powered Fixed-wing aircraft > Take-off > Initial climb

EVENTS Typ události - ZTRÁTA

Event type: Consequential Events > Flight Operations Outcome Events > Emergency Situations > Declared Technical Emergency

Phase: Powered Fixed-wing aircraft > Take-off > Initial climb

EVENTS Typ události - ZTRÁTA

Obrázek 9: Důležité informace z hlášení – událost 2



kouř na palubě letadla spadá do kategorie události spojené s vybavením (equipment) a provozní *typ události (operational)*. Totožnou shodu najdeme i u kauzálního faktoru, který je opět v kategorii *události personálu (personnel)*. Poslední informací z hlášení je ztráta, která patří do *následných událostí (consequential events)*.

8.3. Událost 3 – selhání tlaku v hlavní pneumatice

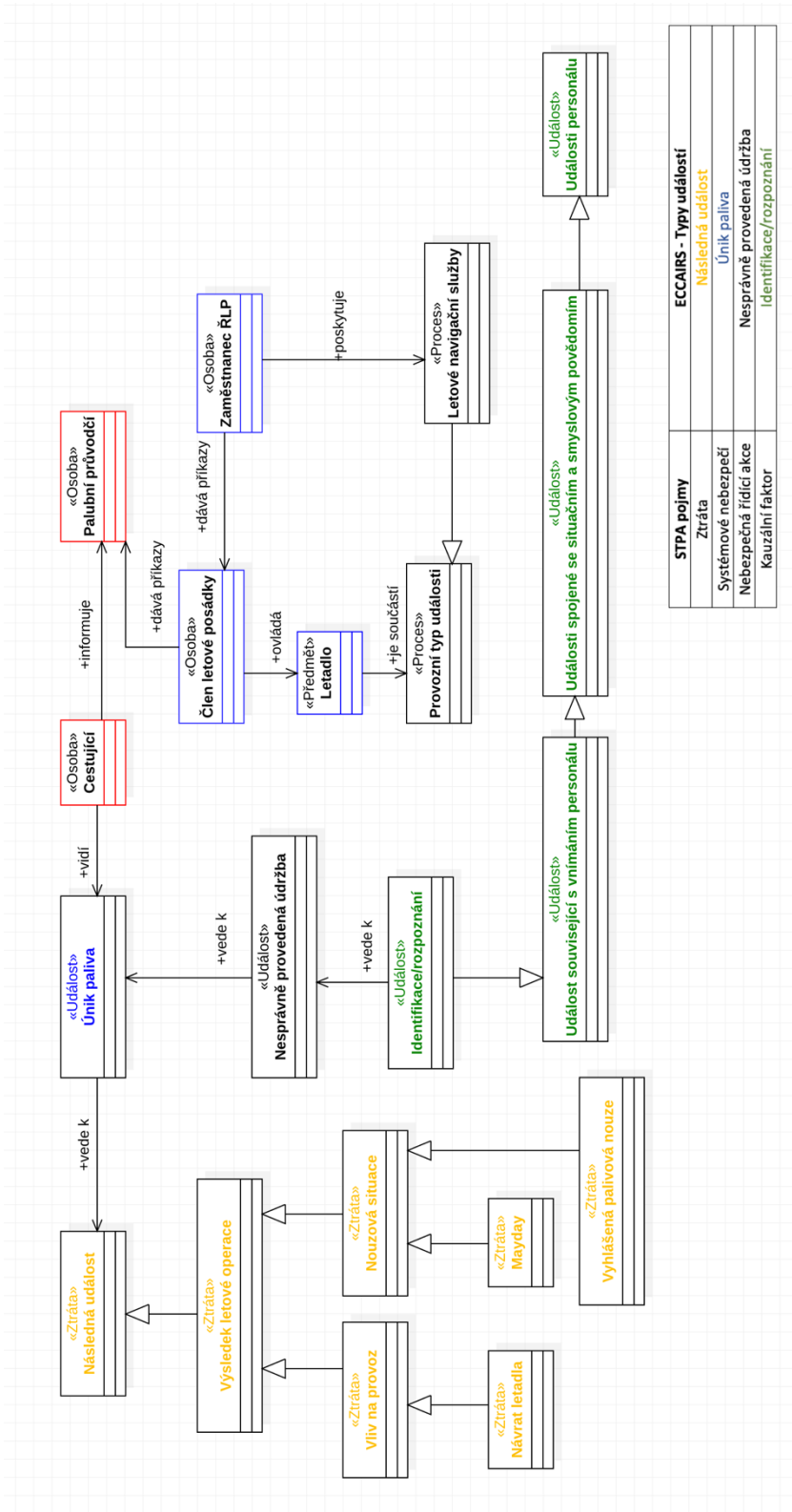
Průběh události

Událost se stala 15.února 2006 v 11:32. Během stoupání letu OK 650 z Prahy do Londýna Heathrow ohlásil pilot návrat a přistání v Praze z důvodu poškození křídla. Křídlo bylo poškozeno pneumatikou hlavního podvozku, která byla deformována. Na RWY 24 byly nalezeny zbytky, které odpovídaly poškození jedné pneumatiky. Pilot následně bezpečně přistál na RWY 13. [24]

Po šetření bylo zjištěno, že pneumatika byla zdeformovaná vlivem podhuštění, její přílišná deformace vedla ke vzniku šíření oddělení protektoru. Utržení částí gumy mělo za následek poškození křídla. [24]

Událost byla klasifikována jako incident. Ze 7členné posádky ani 84 cestujících nebyl nikdo zraněn. [24]

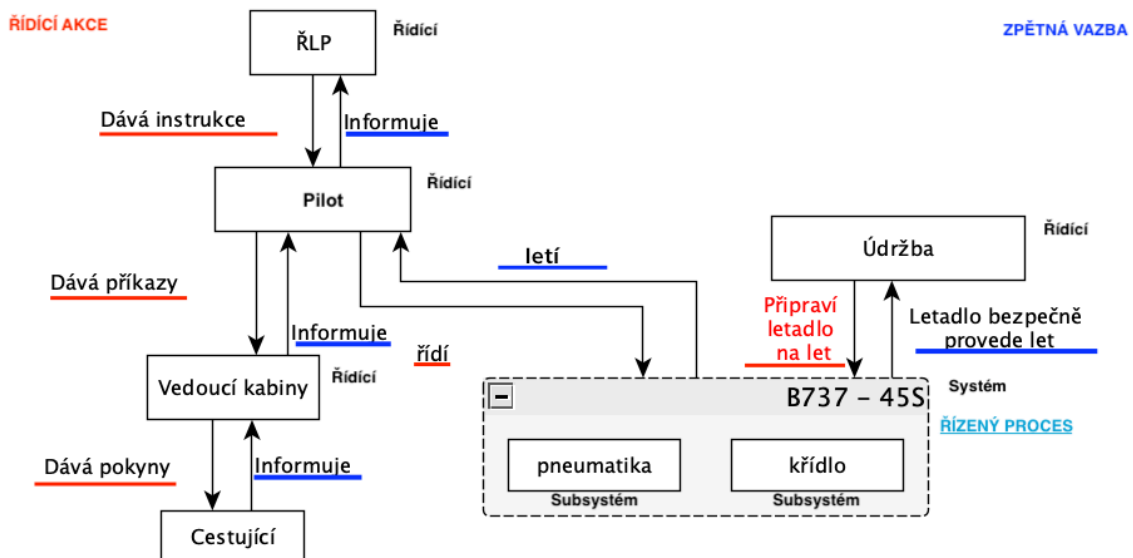
Událost namodelovaná ECCAIRS taxonomií



STPA pojmy	ECCAIRS - Typy událostí
Ztráta	Následná událost
Systémové nebezpečí	Únik paliva
Nebezpečná řídicí akce	Nesprávně provedená údržba
Kauzální faktor	Identifikace/rozpoznání

Obrázek 10: UML model události 2 – ECCAIRS taxonomie

Řídicí struktura události 3 dle modelu STAMP



Obrázek 11: Řídicí struktura – událost 3

Tabulka 11: Ztráty a systémové nebezpečí – událost 3

Porucha části systému – ztráty
L-2: Ztráta nebo poškození prostředku (letadla)
L-4: Ztráta mise (přeprava)
Porucha části systému – systémové nebezpečí
H-1: Selhání tlaku v hlavní pneumatice [L-2, L-4]

Tabulka 12: Nebezpečné řídicí akce – událost 3

Řídicí akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Připraví letadlo na let	Pracovník údržby neposkytne nutnou údržbu před letem. [H-2]	Pracovník údržby provede špatně vykonanou údržbu před letem. [H-2]	Pracovník údržby provede údržbu ve špatném pořadí, špatným zařízením/ prostředky. [H-2]	N/A



Tabulka 13: Ztrátové scénáře – událost 3

Nebezpečná řídicí akce:	Pracovník údržby provede špatně vykonanou údržbu před letem. [H-2]
Scénář 1:	Pracovník údržby nerozpoznal, že pneumatika je příliš zdeformovaná. Výsledkem bylo poškození křídla a nouzové přistání.
Scénář 2:	Pracovník údržby neměl dostatečnou znalost procedur, jeho špatně vykonaná údržba měla za následek deformaci pneumatiky, jejíž části poškodily křídlo. Výsledkem bylo poškození křídla a nouzové přistání.

Důležité informace z hlášení události

DAMAGE Poškození - ZTRÁTA

Third party damage: Object damaged:

INJURIES Zranění - ZTRÁTA

Injury level*:

Total on ground: **SERIOUS** **MINOR**

Total on aircraft:

EVENTS Typ události - KAUZÁLNÍ FAKTOR

Event type:

Phase:

EVENTS Typ události - NEBEZPEČNÁ ŘÍDICÍ AKCE

Event type:

Phase:

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type:

Phase:

EVENTS Typ události - ZTRÁTA

Event type:

Phase:

EVENTS Typ události - ZTRÁTA

Event type:

Phase:

EVENTS Typ události - ZTRÁTA

Event type:

Phase:

Obrázek 12: Důležité informace z hlášení – událost 3



9. Provázání informací analyzovaných událostí

Z modelů událostí, které jsou zobrazeny výše (8.1. Událost 1–8.3. Událost 3) jsou vidět jasné spojitosti.

Řídící akce nám na prvním modelu ukazují, jaké akce řídící vykonával, například řízení letového provozu (ŘLP) dává instrukce pilotovi nebo palubní personál obsluhuje troubu. Do hlášení se popisuje událost, musí se při tom ale vycházet z dané taxonomie. Typ události popisuje systémové nebezpečí, ztrátu, nebezpečnou řídící akci a kauzální faktor. Stejný popis typu události je možné vidět na obrázku 7, 10 nebo 13 – UML model události 1/2/3 – ECCAIRS taxonomie.

Můžeme si všimnout, že v taxonomii ztrátu najdeme vždy jako *následnou událost*, kde nalezneme informace o poškození letadla, výsledku letové operace – na příklad nouzové přistání nebo zranění, ke kterému během události došlo.

Kauzální faktor nalezneme v kategorii *události personálu*. Dá nám informace, například, že pracovníkovi chyběly důležité znalosti letadla nebo vybavení, nebo neodhadl situaci. Díky kauzálnímu faktoru zjistíme, jestli nebyl pracovník v časové tísní, zda nebyl unavený nebo pod vlivem návykových látek.

Systémové nebezpečí a nebezpečné řídící akce nalezneme téměř ve všech podkategoriích typů událostí. Jak je ale vidět v tabulce 14, nebezpečná řídící akce se nejčastěji objevuje v kategorii *provozní typ události (operational)*. Je to z toho důvodu, že v této kategorii jsou řídící akce, které popisují veškeré kroky, které jsou během letových akcí nutné – od letecké navigace, údržby letadel, letištní provoz nebo provoz během letu. V taxonomii jsou v podkategorii 2 a 3, tedy dvě kategorie s nejdetailnějším popisem události. Jsou zavedeny jako řídící akce a systém počítá s tím, že budou vykonávány. Nebezpečná řídící akce se z těchto řídících akcí stane v momentě, kdy kauzální faktor ovlivní bezpečnost této řídící akce. Na nebezpečnou řídící akci narazíme ale i v kategorii *události personálu*, kdy pracovník akci provede špatně nebo se špatně rozhodne kvůli špatnému odhadu/znalostem. Nebezpečná řídící akce následně vede k systémovému nebezpečí.



Systémové nebezpečí se nám nejčastěji objevuje dle výsledků zanalyzovaných událostí v kategorii *události spojené s vybavením (equipment)*. Otázkou je, zda by výsledky dopadly stejně, zanalyzovalo by se více událostí. Podíváme-li se zpět na tabulku 4 – ukázkou obecných systémových nebezpečí, tak téměř polovina z nich spadá do kategorie *provozní typ události (operational)*. Je proto nutné počítat s tím, že při zpracování více událostí by se výsledky mohly trochu lišit.

Můžeme si tedy představit jednoduchý sled událostí, kdy nám kauzální faktor ovlivní řídicí akci, ze které se stane nebezpečná řídicí akce, ta povede k systémovému nebezpečí a systémové nebezpečí vede ke ztrátě.

Z tabulky 14 je jasné, že se nám u událostí opakuje vzor, který platí pro všechny 3 události. Díky tomu můžeme rozřadit taxonomii:

- Ztráta = následná událost
- Systémové nebezpečí = událost spojená s vybavením
- Nebezpečná řídicí akce = provozní typ události
- Kauzální faktor = události personálu



Tabulka 14: STPA pojmy – jednotlivé události

STPA pojmy	Událost	ECCAIRS – typy událostí	ECCAIRS – kontextuální informace	Přidané pojmy	Hlášení
Řídící akce	Kouř na palubě letadla		Dává instrukce, dává příkazy	Obsluha trouby, úklid kuchyňky	
	Únik paliva		Dává instrukce, dává příkazy, řídí	Dává pokyny, oprava uzávěru palivové nádrže	
	Selhání tlaku v hlavní pneumatice		Dává instrukce, dává příkazy, řídí	Dává pokyny, připraví letadlo na let	
Řízený proces	Kouř na palubě letadla			Příprava jídla/pití	
	Únik paliva	Údržba – inspekce, kontroly, servis			
	Selhání tlaku v hlavní pneumatice	Údržba – inspekce, kontroly, servis			
Kauzální faktor	Kouř na palubě letadla				Event Type – Personnel > Knowledge of Equipment or Aircraft
	Únik paliva				Event Type - Personnel > Identification/Recognition
	Selhání tlaku v hlavní pneumatice				Event Type – Personnel – Knowledge of Procedures
Nebezpečná řídicí akce	Kouř na palubě letadla	Nevhodné/nesprávné použití přístroje/vybavení			Event Type – Operational> Inappropriate/Improper Use of Tool/Equipment
	Únik paliva	Nesprávně provedená údržba			Event Type – Operational> Servicing Incorrectly Carried Out
	Selhání tlaku v hlavní pneumatice	Nesprávně provedená údržba			Event Type - Operational > Inspection Incorrectly Carried Out



STPA pojmy	Událost	ECCAIRS – typy událostí	ECCAIRS – kontextuální informace	Přidané pojmy	Hlášení
Systémové nebezpečí	Kouř na palubě letadla	Kouř na palubě letadla			Event Type – Equipment> Smoke – Passenger Cabin
	Únik paliva	Únik paliva			Event Type – Equipment> Fuel Leak
	Selhání tlaku v hlavní pneumatice	Selhání tlaku v hlavní pneumatice			Event type – Equipment> Main Tyre Pressure Failure
Ztráta	Kouř na palubě letadla	Následná událost – zdravotní neschopnost (palubní průvodčí), nouzové přistání, odklon (zdravotní důvody)			Event Type – Consequential Events> Forced Landing, Diversion – Medical Reasons, Medical/Incapacitation – Cabin Crew, Damage, Injuries
	Únik paliva	Následná událost – návrat letadla, odklon – technické důvody, mayday, vyhlášená palivová nouze			Event Type – Consequential Events> Mayday Fuel Declaration, Aircraft Return, Declared Technical Emergency. Damage, Injuries
	Selhání tlaku v hlavní pneumatice	Následná událost – poškození uvolněného komponentu/konstrukce letadla, návrat letadla, vyhlášení technické nouze			Event Type – Consequential Events> Declared Technical Emergency, Aircraft Return, Loose/Shed Aircraft Structure/Component Damage. Damage, Injuries



10. Výsledky

V této kapitole budou zhodnoceny výstupy této práce. Cílem bylo navrhnout převodní systém taxonomie ECCAIRS a pojmů STPA. V kapitole 8 a 9 je ukázán postup, jak by takový převod měl vypadat. Viděli jsme rozebrání jednotlivých událostí dle modelu STPA, zadání události do hlášení, a nakonec vytvoření UML modelu za využití ECCAIRS taxonomie. V následujících kapitolách budou ukázány spojitosti mezi STPA pojmy v jednotlivých událostech, tedy krátké vysvětlení STPA pojmů a jak se nám objevovaly v událostech. Dále zde bude vidět ukázka převodního systému ECCAIRS taxonomie a STPA pojmů v UML modelu.

10.1. Spojitosti mezi STPA pojmy v událostech

Nebezpečná řídicí akce – nebezpečnou řídicí akci chápeme jako řídicí akci, která v nejhorším možném kontextu povede k systémovému nebezpečí. V modelovaných událostech vidíme nebezpečné řídicí akce jako špatně provedenou údržbu nebo použití špatného čisticího prostředku. Důležité je se podívat na kauzální faktor, proč k nebezpečné řídicí akci došlo. V případech těchto událostí se jednalo o rozptýlení, špatnou identifikaci/rozpoznání, znalost procedur nebo vybavení či letadla.

Systémové nebezpečí – jedná se o stav, kdy v nejhorším scénáři dojde ke ztrátě. V modelech událostí najdeme systémové nebezpečí jako poslední krok před ztrátou. V událostech systémové nebezpečí nalezneme jako: kouř na palubě letadla, únik paliva, selhání tlaku v hlavní pneumatice. Všechny tyto pojmy jsou dohledatelné v ECCAIRS taxonomii v typech událostí.

Ztráta – následná událost, zde nalezneme zranění, poškození letadla/infrastruktury/letištního vybavení. Důležité je zmínit, že při vyplňování hlášení je pro ztrátu kromě následných událostí je nutné vyplnit – zda se jednalo o nehodu, vážný incident, incident nebo jakoukoliv mimořádnou událost. Dále poškození třetí strany, pokud by se jednalo o poškození pouze na letadle, zaznamená se tato informace do typu událostí – následná událost. Informace o zranění je nutné vyplnit do samostatné kolonky v hlášení. Je nutné vědět, o jak vážné zranění se jednalo, ale také kolik lidí bylo zraněno. Tato informace se



dělí zvláště na posádku a cestující. Informace, zda došlo ke zranění, lze vyplnit i u typů událostí – následná událost, ale nezjistíme z ní, jak moc nebo kolik lidí bylo zraněno.

V tabulce 14 si můžeme všimnout, že se některé pojmy opakují. Například, ztráta je *následná událost* (v hlášení *consequential events*). Systémové nebezpečí nebo nebezpečná řídicí akce je nejčastěji k nalezení v kategoriích událost spojená s *vybavením* (*equipment*) nebo *provozní typ události* (*operational*).

10.2. Propojení ECCAIRS taxonomie a STPA pojmů v UML modelu

Jak již bylo zmíněno dříve (tabulka 1), taxonomie je rozdělená do 7 základních kategorií – následná událost, událost spojená s vybavením, provozní typ události, události personálu, organizační typ události, jiná událost, neznámá událost. Každá z těchto kategorií se dále člení do dalších podkategorií, které udávají detailnější typy událostí. Celkem jsou 4 podkategorie. V kategorii následná událost se veškeré události klasifikují jako ztráta. Události – jiná událost a neznámá událost nemají žádné jiné podkategorie. Zbývající kategorie typů událostí (*událost spojená s vybavením*, *provozní typ události*) v první a v druhé kategorii (*letový provoz letadel*, *letové navigační služby*, *události spojené s plněním úkolů personálu*) popisují řízený proces, případně řídicí akci. U nižších kategorií záleží na typu události, zda se jedná o řídicí akci nebo systémové nebezpečí, ale nalezneme zde i ztráty.

Na obrázku 14 vidíme ukázkou ECCAIRS taxonomie (legenda je v tabulce 15 pod obrázkem). Na rozdíl od obrázku 1, kde byla zobrazena taxonomie a její větvení na další podkategorie, zde na obrázku 13 si můžeme všimnout i dalších detailů, jak jsou spolu taxonomické pojmy propojené.

Zprvém, každý typ události má určený stereotyp, který nám událost popisuje. Například: *následnou událost* chápeme jako ztrátu, *navigace letadla* označuje proces, *pozemní srážka* je událost. Stereotyp nám naznačí funkci daného pojmu – *události personálu* – název kategorie, která popisuje události, ve kterých personál sehrál roli, na příklad, v čem udělal chybu nebo co na jeho akce mělo vliv.

Zadruhé, model je obohacen o vazby, které spojují různé druhy kategorií typů událostí. Příkladem je: *Událost spojená s komunikací posádky vede k odchylce od postupů ŘLP*



vede k střetu ve vzduchu. Tato vazba může být chápána, že řídicí akce *událost spojená s komunikací posádky*, pokud nebude provedena standardně, povede k systémovému nebezpečí *odchylka od postupů ŘLP*, které povede ke *střetu ve vzduchu*. Je nutné podotknout, že nejčastěji zmiňovaná vazba „vede k“ v modelu označuje potenciální kauzalitu, která může nastat v konkrétní události a spustí řetězec kauzální faktor -> nebezpečná řídicí akce -> systémové nebezpečí -> ztráta. Nejedná se o konkrétní příklad, který by zahrnoval všechny existující možnosti, které mohou reálně nastat. Vždy záleží na kauzálním faktoru. Podíváme-li se například *navigace letadla vede ke střetu ve vzduchu*, neznamena to, že pokaždé, kdy je vykonávána řídicí akce navigace letadla, dojde ke střetu ve vzduchu. Znamená to, že v konkrétní události tomu může tak být, protože během navigace může dojít k problému, který může vést ke střetu ve vzduchu. Proto by to nemělo být vnímáno jako jediná příčina. Vždy záleží i na kauzální příčině. Ke střetu ve vzduchu může vést i odchylka od postupů ŘLP anebo rovnou kombinace několika událostí současně. Vždy záleží na konkrétní události. Tento model (obrázek 13) má ukázat to, že taxonomie je daným způsobem seřazená, aby byla přehledná, ale pokud dojde k incidentu, většinou nejde o jednu událost. Jde o řetězec událostí, které se ovlivňují a z řídicí akce, která je součástí každého letu se může stát nebezpečná řídicí akce, která povede k systémovému nebezpečí, a to povede ke ztrátě.

Posledním přidaným údajem je barevné rozřazení na řídicí akce, systémové nebezpečí a ztráty. Mimo to má každá třída označení ID typu události, které je možné dohledat v tabulce typů událostí taxonomie ECCAIRS – jedná se o přílohu ECCAIRS Aviation v.4.1.0.6-at-390-Event-type-values.xlsx (příloha 1), která byla upravena tak, že všechny pojmy jsou barevně označené podle toho, do jaké spadají kategorie – ztráta, systémové nebezpečí, řídicí akce, systém, komponent, kromě sedmi hlavních kategorií taxonomie. Hlavní kategorie taxonomie nejde barevně rozřadit proto, že barevným označením určujeme, zda je pojem řídicí akce, systémové nebezpečí nebo ztráta, a to v tomhle případě nelze určit, neboť hlavní kategorie označuje desítky i stovky pojmů, jejichž označení se může lišit. Navíc u hlavní kategorie toto rozřazení nepotřebujeme, protože vždycky pracujeme s pojmy z detailnějších podkategorií.



Tabulka 15: Legenda k převodnímu systému (obrázek 14)

Řídící akce	Systémové nebezpečí	Ztráta
Události spojené s organizací a managementem	Události spojené se situačním a smyslovým povědomím	Pozemní srážka – vozidlo se zaparkovaným letadlem
Události spojené s plněním úkolů personálu	Události spojené s komunikací personálu	Střet ve vzduchu
Výroba letadel	Nedostatek komunikace	Srážka s ptáky/divokou zvěří
Údržba letadel	Nestandardní frazeologie	Pozemní srážka
Události spojené se zkušenostmi a znalostmi	Události spojené s nedodržováním předpisů	Pozemní srážka s budovou
Konstrukce letadla	Letištní zabezpečení	
Letištní operace	Nesprávný typ paliva	
Fyziologické události	Rozlití paliva během tankován	
Události související s organizační dokumentací a publikacemi	Téměř pozemní srážka – vlečné letadlo s předmětem	
Odmrazování letadla	Náhlý manévr	
Tankování letadla	Téměř srážka s pohybujícím se letadlem	
Kontrola divoké zvěře	Odchylna od postupů ŘLP	
Provoz letištních vozidel/vybavení	Nejasnosti posádky s volacím znakem	
Navigace letadla	Provozní problémy ŘLP	
Letové navigační služby	Selhání rádiové komunikace – jednosměrná	
Komunikace personálu ŘLP	Nevhodné povolení	
Letový provoz letadel	Rádiové rušení vzduch/země	
Události spojené s komunikací posádky	Porucha rádia vzduch/země (hardware)	
Komunikační vybavení letiště a ŘLP		
Vybavení letiště a ŘLP		

Speciální kategorie je *událost spojená s vybavením*, tyto pojmy lze kategorizovat jako řídicí akce, systémové nebezpečí, komponent, systém, některé pojmy je náročné určit, neboť název pojmu napovídá, že se jedná o komponent, v detailnějším popisu pojmu ale zjistíme, že se jedná o řídicí akci. Kategorie *událost spojená s vybavením* je nejpočetnější kategorií taxonomie a obsahuje vybavení letiště, řízení letového provozu i veškeré systémy letadla, proto je někdy těžké určit, zda se jedná o řídicí akci, systémové nebezpečí, komponent nebo systém, neboť některé kategorie slouží jen jako označení pro lepší přehlednost. Jak vidíme v tabulce 16, jedná se o ukázkou kabinového zařízení a vybavení. Modré pojmy (manuály, checklisty) bylo těžké zařadit, protože v porovnání



s dalšími komponenty (součástky, vedení, zařízení...) se jedná o odlišné věci, ale je nutné na tyto komponenty pohlížet jako něco, co sehraje důležitou roli v momentě, kdy je pilot bude potřebovat a v kokpitu budou chybět nebo budou poškozeny a nedaly by se použít, a proto na tyto pojmy pohlížíme jako na komponenty, které jsou nezbytnou součástí kokpitu.

Další ukázkou je kyslíkový systém v tabulce 17, kde můžeme vidět ukázkou opakující se taxonomie. Prvním (zeleným) pojmem kategorie 2 (*událost spojená s vybavením = kategorie 1*) je kyslíkový systém. Je označen jako řídicí akce z toho důvodu, že v definici je tento pojem popsán jako událost související s kyslíkovým systémem, tedy předpokládá se, že kyslíkový systém provádí nějaké akce. Druhý pojem – kyslíkový systém posádky (tentokrát fialový) je definován jako systém takový, tedy předpokládáme, že se při modelování využije jako systém, který přestal fungovat, nebo kde mohlo dojít k poškození. Následné dva pojmy (oranžové) již znázorňují systémové nebezpečí, kdy kyslíkový systém nepracuje tak, jak má. Další řádek znázorňuje kyslíkový systém cestujících, pojem se trochu liší, ale zařazení v taxonomii (kategorie) i v STPA pojmech (systém, systémové nebezpečí) je stejné. Problém je v tom, že tento pojem je v této tabulce identifikovaný jako systémové nebezpečí, ale dal by se identifikovat i jako selhání komponentu. A toto je problém ECCAIRS taxonomie, jelikož je velice subjektivní a relativní a každý tento pojem může chápat trochu jinak podle toho v jaké události se použije. Pojmů s podobným problémem je více a nejedná se pouze o systémové nebezpečí. Například pojem *pozemní srážka*, který se objevuje v následné kapitole, lze klasifikovat jako systémové nebezpečí, ale v jiné události by se tento pojem dal klasifikovat jako ztráta. Taxonomii chybí zjednodušení, který by tento problém dokázalo vyřešit. Převodní systém by teoreticky mohl tyto „problematické“ pojmy vyřešit databází, kde by se ukládaly události s konkrétními příklady, kde daný pojem figuroval jako selhávající komponent/systémové nebezpečí/ztráta a pomohl by tak identifikaci pojmu v jiné události.



Tabulka 16: ECCAIRS taxonomie – událost spojená s vybavením

Kategorie 1 typu události	Podkategorie 2 typu události	Podkategorie 3 typu události	Kategorie	ID	Podkategorie 4 typu události	STPA pojmy
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2500 Cabin Equipment/Furnishing	2	1250000	2500 Cabin Equipment/Furnishing	Řídící akce
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2510 Flight Compartment Equipment	3	1251000	2510 Flight Compartment Equipment	Řídící akce
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2510 Flight Compartment Equipment	4	99010796	2511 Flight Crew Documentation – Approach Charts	Komponent
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2510 Flight Compartment Equipment	4	99010797	2511 Flight Crew Documentation – Checklists	Komponent
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2510 Flight Compartment Equipment	4	99010798	2511 Flight Crew Documentation – Company Ops Manuals	Komponent
Equipment (událost spojená s vybavením)	2500 Cabin Equipment/Furnishing (Kabinové zařízení a vybavení)	2510 Flight Compartment Equipment	4	99010799	2511 Flight Crew Documentation – Emergency Checklists	Komponent



Tabulka 17: ECCAIRS taxonomie – událost spojená s vybavením

Kategorie 1 typu události	Podkategorie 2 typu události	Podkategorie 3 typu události	Kategorie	ID	Podkategorie 4 typu události	STPA pojmy
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3500 Oxygen System	2	1350000	3500 Oxygen System	Řídící akce
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3510 Crew Oxygen System	3	99011088	3510 Crew Oxygen System	Systém
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3510 Crew Oxygen System	4	99011091	3510 Crew Oxygen System Erroneous Operation	Systémové nebezpečí
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3510 Crew Oxygen System	4	99011092	3510 Crew Oxygen System Loss or Unavailability	Systémové nebezpečí
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3520 Passenger Oxygen System	3	99011089	3520 Passenger Oxygen System	Systém
Equipment (událost spojená s vybavením)	3500 Oxygen System (Kyslíkový systém)	3520 Passenger Oxygen System	4	99011093	3520 Passenger Oxygen System Erroneous Operation	Systémové nebezpečí



11. Validace

V této kapitole budu ověřovat provázání informací analyzovaných událostí. Půjde o ověření převodního systému, který vychází z analýzy předchozích událostí. Toto ověření by mělo správnost převodního systému ověřit nebo vyvrátit. Události byly vybrány tak, aby byla použita co možná největší část taxonomie a neopakovaly se stejné pojmy ve více událostech.

Postup je stejný jako u předchozích událostí, který byl detailně popsán u události 1, proto zde budou ukázány pouze modely a tabulky, které jsou dostačující pro ukázání výsledku.

11.1. Událost 4 – pozemní srážka

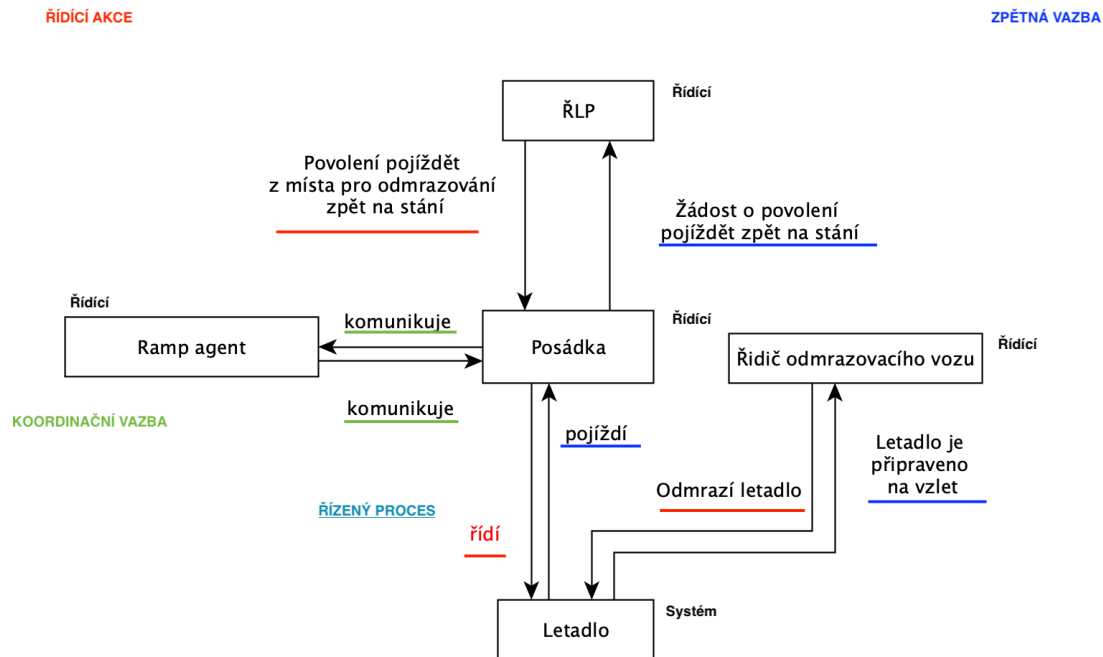
Průběh události

Událost se stala 17.12.2010 v Praze na letišti Ruzyně, kdy posádka požádala ŘLP o povolení zpět na stání z odmrazovacího místa z důvodu zdržení jejího odletu kvůli provádění zimní údržby na dráze. Posádka začala pojíždět z odmrazovacího místa bez koordinace s ramp agentem. V průběhu pojíždění došlo ke střetnutí levého wingletu CL-600 s košem odmrazovacího zařízení. [25]

Během šetření bylo zjištěno, že příčina této letecké nehody bylo selhání lidského činitele, jelikož nedošlo ke koordinaci posádky s ramp agentem. [25]

Událost byla klasifikována jako letecká nehoda. Nedošlo ke zranění posádky ani jiných účastníků přítomných při této události. Byl poškozen levý winglet, letadlo nebylo dále schopno letu. [25]

Řídicí struktura události 4 dle modelu STAMP



Obrázek 15: Řídicí struktura – událost 4

Tabulka 18: Ztráty a systémové nebezpečí – událost 4

Pozemní srážka – ztráty
L-2: Ztráta nebo poškození letadla
L-4: Ztráta mise
Pozemní srážka – systémové nebezpečí
H-1: Pozemní srážka s vozidlem/vybavením [L-2, L-4]

Tabulka 19: Nebezpečné řídicí akce – událost 4

Řídicí akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Řídí	N/A	Posádka řídí letadlo bez povolení ŘLP. [H-1]	Posádka řídí letadlo příliš brzy/ pozdě, vykoná příkazy ŘLP ve špatném pořadí. [H-1]	N/A



Tabulka 20: Ztrátové scénáře – událost 4

Nebezpečná řídicí akce:	Posádka řídí letadlo bez povolení ŘLP. [H-1]
Scénář 1:	Posádka dostatečně nekomunikovala pohyb po ploše s ramp agentem. Rozjela se z odmrazovacího místa zpět na stání. V důsledku toho došlo ke střetnutí levého wingletu s košem odmrazovacího zařízení.

Důležité informace z hlášení události

DAMAGE Poškození - ZTRÁTA

Third party damage: + Object damaged: +

INJURIES Zranění - ZTRÁTA

Injury level*: ×

	SERIOUS	MINOR
Total on ground	<input type="text"/>	<input type="text"/>
Total on aircraft	<input type="text"/>	<input type="text"/>

EVENTS Typ události - KAUZÁLNÍ FAKTOR

Event type: ×

Phase: ×

EVENTS Typ události - NEBEZPEČNÁ ŘÍDICÍ AKCE

Event type: ×

Phase: ×

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type: ×

Phase: ×

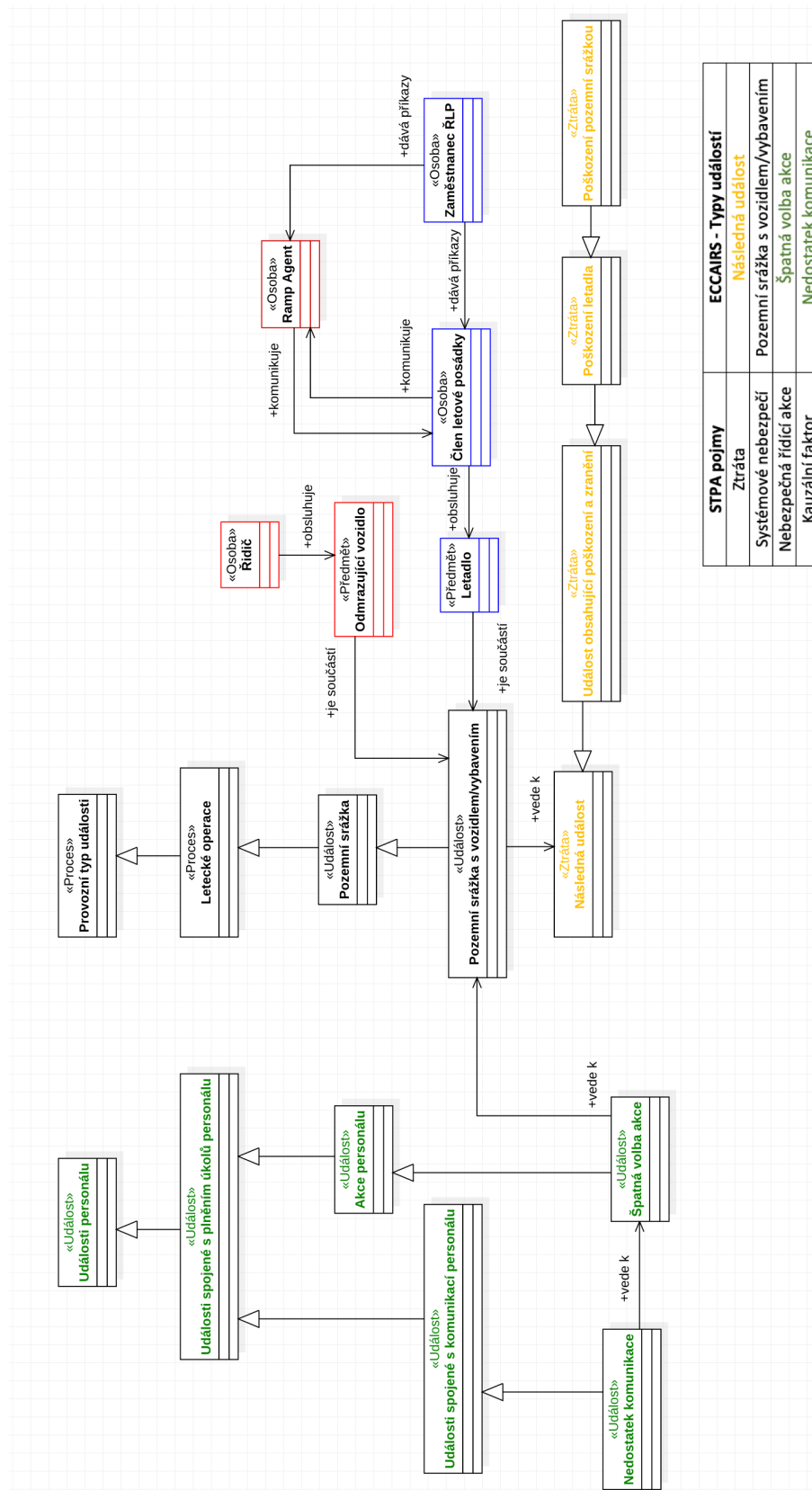
EVENTS Typ události - ZTRÁTA

Event type: ×

Phase: ×

Obrázek 16: Důležité informace z hlášení – událost 4

Událost namodelovaná ECCAIRS taxonomií



STPA pojmy	ECCAIRS - Typy událostí
Ztráta	Následná událost
Systémové nebezpečí	Pozemní srážka s vozidlem/vybavením
Nebezpečná řídicí akce	Špatná volba akce
Kauzální faktor	Nedostatek komunikace

Obrázek 17: UML model události 4 – ECCAIRS taxonomie

11.2. Událost 5 – nepovolený vjezd na dráhu

Průběh události

Událost se stala 4.10.2010 v Praze na letišti Ruzyně, kdy posádka letounu B 737-800 (TVS1038) dostala od ŘLP povolení k pojíždění na vyčkávací místo do blízkosti dráhy 13 a vyčkávat. Druhý letoun (NAX3580) získal od ŘLP povolení na krátké finále na dráhu 13. Posádka (TVS1038) ale vstoupila na dráhu bez povolení. ŘLP proto musel vydat letadlu (NAX3580) pokyn k provedení nezdařeného přiblížení. Mezi letadly byl snížen vertikální rozestup na 70 % a horizontální rozestup na 66 %. [26]

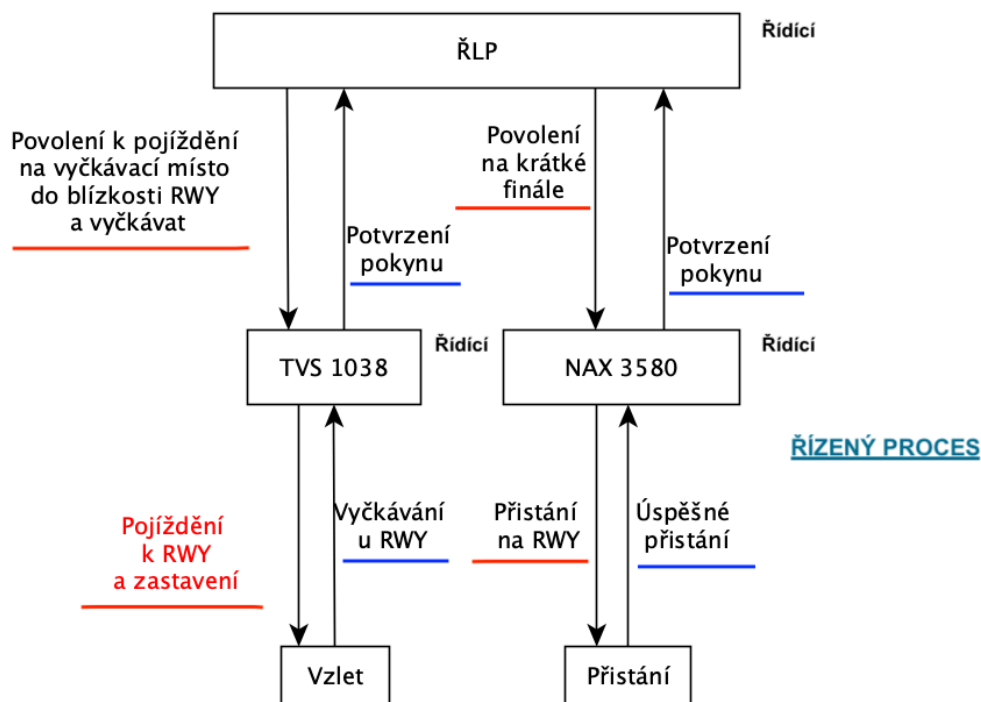
Během šetření bylo zjištěno, že příčina tohoto incidentu bylo selhání lidského činitele, kdy posádka (TVS1038) nedodržela instrukce ŘLP. [26]

Událost byla klasifikována jako vážný incident. Během incidentu nedošlo ke zranění ani žádnému poškození. [26]

Řídicí struktura události 5 dle modelu STAMP

ŘÍDÍCÍ AKCE

ZPĚTNÁ VAZBA



Obrázek 18: Řídicí struktura – událost 5



Tabulka 21: Ztráty a systémové nebezpečí – událost 5

Nepovolený vjezd na dráhu – ztráty
L-4: Ztráta mise (přeprava)
Nepovolený vjezd na dráhu – systémové nebezpečí
H-1: Vjezd letadla na dráhu bez povolení [L-4]

Tabulka 22: Nebezpečné řídicí akce – událost 5

Řídicí akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Pilot vjede na dráhu	Pilot vjede na dráhu bez povolení ŘLP. [H-1]	N/A	Pilot vjede na dráhu příliš brzy/ pozdě. [H-1]	N/A

Tabulka 23: Ztrátové scénáře – událost 5

Nebezpečná řídicí akce:	Pilot vjede na dráhu bez povolení ŘLP. [H-1]
Scénář 1:	Pilot se nedržel instrukcí vydané ŘLP. Bez povolení vjel na dráhu, snížil minimální rozestup s NAX 3580, který měl povolení na krátké finále. V důsledku toho byl snížen minimální rozestup a NAX 3580 nemohl přistát.



Důležité informace z hlášení události

DAMAGE Poškození - ZTRÁTA

Third party damage: + Object damaged: +

INJURIES Zranění - ZTRÁTA

Injury level*: × ▾

	SERIOUS	MINOR
Total on ground	<input type="text" value="0"/>	<input type="text" value="0"/>
Total on aircraft	<input type="text" value="0"/>	<input type="text" value="0"/>

EVENTS Typ události - KAUZÁLNÍ FAKTOR

Event type: ×

Phase: ×

EVENTS Typ události - NEBEZPEČNÁ ŘÍDÍCÍ AKCE

Event type: ×

Phase: ×

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type: ×

Phase: ×

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type: ×

Phase: ×

EVENTS Typ události - ZTRÁTA

Event type: ×

Phase: ×

Obrázek 19: Důležité informace z hlášení – událost 5



11.3. Událost 6 – posun nákladu za letu

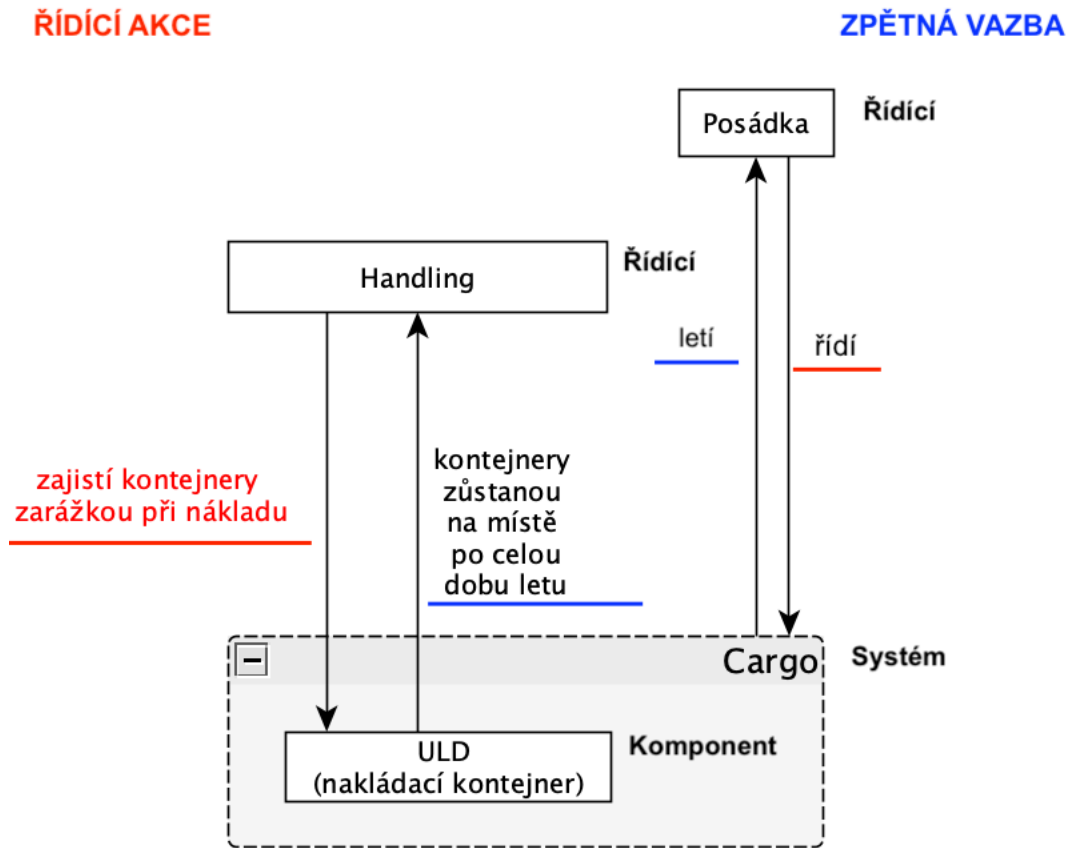
Průběh události

Událost se stala 16.dubna 2021 v 6:30. Proběhl let z East Midlands do Guernsey, kde došlo k vyložení nákladu (2 nákladové kontejnery z 5), zbylý náklad byl přemístěn do pozic C1, C3 a C5 a letadlo odletělo do Jersey. Během vzletu piloti zaslechli nepatrné zadunění, zbytek letu pokračoval bez jakýkoliv obtíží nebo odlišností. Během přistání piloti zaslechli hlasité bouchnutí. Následně při kontrole nákladu bylo zjištěno, že došlo k přesunutí nákladu z pozice C3 do C2. [27]

Po šetření bylo zjištěno, že nakladač byl pravděpodobně nedostatečně zaškolen, protože nevěděl, že má kontejnery zajišťovat zarážkou při nákladu, kterou nechal mezi C3 a C4 v dolní poloze. Náklad se tedy během letu pohyboval v prostorech C3-C4-C3-C2, tento pohyb poškodil zarážky a kolejnice mezi C2 a C3. Dále bylo zjištěno, že v provozních postupech neexistoval požadavek na kontrolu jednotlivých zarážek při nakládání nákladu. [27]

Událost byla klasifikována jako vážný incident. Na letadle nedošlo k jinému poškození. Z dvoučlenné posádky nebyl nikdo zraněn. [27]

Řídící struktura události 6 dle modelu STAMP



Obrázek 21: Řídící struktura – událost 6

Tabulka 24: Ztráty a systémové nebezpečí – událost 6

Posun nákladu za letu – ztráty
L-2: Ztráta nebo poškození prostředku (letadla)
Posun nákladu za letu – systémové nebezpečí
H-1: Posun nákladu za letu

Tabulka 25: Nebezpečné řídicí akce – událost 6

Řídící akce	Neposkytnutí způsobí systémové nebezpečí	Poskytnutí způsobí systémové nebezpečí	Příliš brzy/ pozdě, ve špatném pořadí	Zastaveno příliš brzy/ příliš dlouhá aplikace
Zajistí kontejnery zarážkou při náběhu	Pracovník handlingu nezajistí kontejner zarážkou při náběhu nákladu. [H-1]	N/A	Pracovník handlingu zajistí kontejner zarážkou ve špatném pořadí (nedostatečně). [H-1]	N/A



Tabulka 26: Ztrátové scénáře – událost 6

Nebezpečná řídicí akce:	Pracovník handlingu nezajistí kontejnery zarážkou při nakládání nákladu. [H-1]
Scénář 1:	Pracovník handlingu nezajistil při nákladu kontejnery zarážkou, neboť nebyl dostatečně proškolen. Výsledkem byl pohyb nákladu při letu, což způsobilo poškození zarážky a kolejnice mezi C2 a C3.

Důležité informace z hlášení události

DAMAGE Poškození - ZTRÁTA

Third party damage: + Object damaged: +

INJURIES Zranění - ZTRÁTA

Injury level*: ×

	SERIOUS	MINOR
Total on ground	<input type="text"/>	<input type="text"/>
Total on aircraft	<input type="text"/>	<input type="text"/>

EVENTS Typ události - KAUZÁLNÍ FAKTOR

Event type: ×

Phase: ×

EVENTS Typ události - NEBEZPEČNÁ ŘÍDÍCÍ AKCE

Event type: ×

Phase: ×

EVENTS Typ události - SYSTÉMOVÉ NEBEZPEČÍ

Event type: ×

Phase: ×

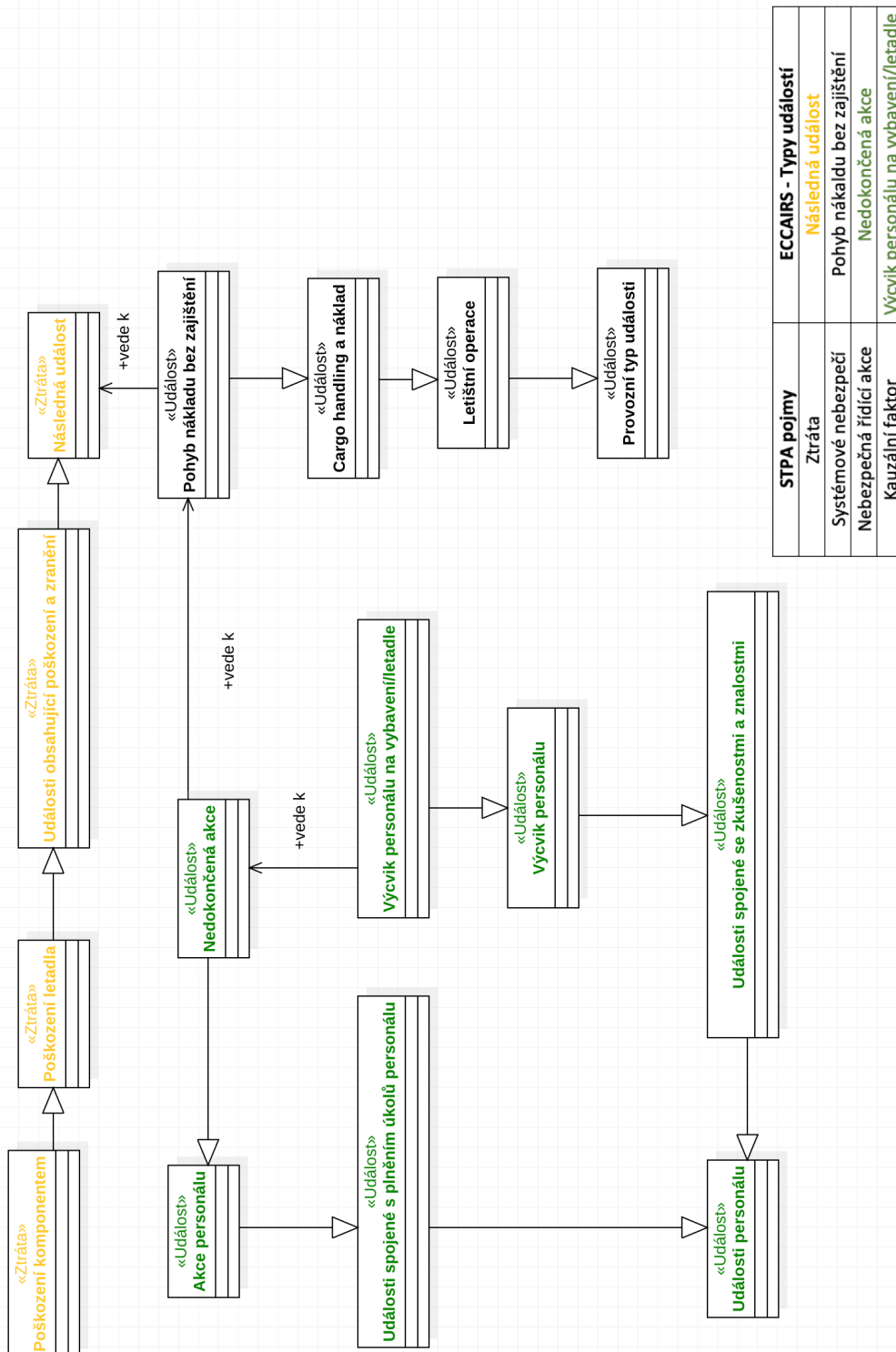
EVENTS Typ události - ZTRÁTA

Event type: ×

Phase: ×

Obrázek 22: Důležité informace z hlášení – událost 6

Událost namodelovaná ECCAIRS taxonomií



STPA pojmy	ECCAIRS - Typy událostí
Ztráta	Následná událost
Systémové nebezpečí	Pohyb nákladu bez zajištění
Nebezpečná řídicí akce	Nedokončená akce
Kauzální faktor	Výcvik personálu na vybavení/letadle

Obrázek 23: UML model události 6 – ECCAIRS taxonomie



11.4. Zhodnocení událostí

Převodní systém vznikl tak, že jsem nejdříve zpracovala 3 události, které jsou detailně popsány v kapitole 8. Následně jsem hledala spojitosti mezi nimi, to znamená opakující se pojmy v taxonomii, kterou můžeme vidět v tabulce 14. Tyto výsledky mi pomohly při anotaci celé ECCAIRS taxonomie ((ECCAIRS Aviation v.4.1.0.6-at-390- Event-type-values) – příloha 1). Dále jsem zpracovala další 3 události, které jsou výše (kapitola 11.1., 11.2. a 11.3.) a jejich hlavním cílem bylo ověření převodního systému.

Podíváme-li se na událost 4, událost 5 a událost 6 a porovnáme je s předešlými událostmi (1-3), zjistíme, že některé pojmy se nám opakují a potvrzují převodní systém, ale objevují se zde i menší nesrovnalosti. Pro větší přehlednost jsem výsledky zapsala do tabulky 27.

Tabulka 27: Výsledky událostí

	Kauzální faktor	Nebezpečná řídicí akce	Systémové nebezpečí	Ztráta
Událost 1	Události personálu	Provozní typ události	Události spojené s vybavením	Následná událost
Událost 2	Události personálu	Provozní typ události	Událost spojená s vybavením	Následná událost
Událost 3	Události personálu	Provozní typ události	Událost spojená s vybavením	Následná událost
Událost 4	Události personálu	Události personálu	Provozní typ události	Následná událost
Událost 5	Události personálu	Provozní typ události	Provozní typ události	Následná událost
Událost 6	Události personálu	Události personálu	Provozní typ události	Následná událost

Události 4, 5 a 6 potvrdily, že kategorie taxonomie *následná událost* bude vždy ztráta a kategorie *události personálu* ve všech případech označuje kauzální faktor.



Rozdílem je systémové nebezpečí, které v prvních třech událostech spadalo do kategorie *událost spojená s vybavením*, zatímco v událostech 4-6 bylo v kategorii *provozní typ události*. Můžeme tedy předpokládat, že systémové nebezpečí se nám z velké většiny bude objevovat v jedné z těchto dvou kategorií.

Nebezpečná řídicí akce byla během validace převodního systému jednou potvrzena událostí 5, naopak se lišila událostí 4 a 6, kde nebezpečná řídicí akce byla nalezena v kategorii *události personálu*.

Zhodnotíme-li tyto výstupy, vidíme, že navržený převodní systém funguje, ale mohou nastat události, které se budou lehce lišit. S počtem pojmů, které taxonomie čítá (± 3100 pojmů) ani nemůžeme předpokládat, že každá kategorie bude jasně definovat jeden pojem STPA a nebude docházet k žádným iregularitám. Těchto 6 událostí ukazuje, jaké kategorie jsme schopni určit, o jaký pojem/pojmy STPA se jedná a jaké kategorie obsahují nejvíce pojmů STPA. Po zhodnocení je možné říci, že převodní systém funguje a je schopen zařadit minimálně 2/3 pojmů taxonomie.



12. Diskuse

Bezpečnostní taxonomie ECCAIRS je momentálně strukturovaná tak, že veškeré pojmy typů událostí jsou definované jako událost – *události personálu, událost spojená s vybavením, událost související s palivovým systémem*, což na první pohled může být trochu zavádějící, protože je pro nás jednodušší si představit personál, vybavení, palivový systém. Ale není reálné taxonomii modifikovat, když byla záměrně navrhnutá právě na typy událostí.

Taxonomie by se ale dala zjednodušit a zpřehlednit tak, že by se na UML modely daly navázat pojmy objektů, které by sloužily jako filtr. Pokud bychom do filtru při hledání zadali pojem jako například: posádka, vybavení, palivový systém, filtr by nám zobrazil události s těmito pojmy spojené, například:

- Posádka -> události spojené s posádkou
- Řízení letového provozu -> události, kde ŘLP sehrálo roli
- Palivový systém -> události spojené s palivovým systémem
- Křídlo -> události související s křídlem
- Znalosti -> události, kde znalost personálu měla vliv na výsledek události

Tato funkce by musela fungovat lépe než dosavadní filtr v ECCAIRS hlášení, který vyhledá přesně to, co zadáme. Příkladem je slovo „wing“, které při zadání, zobrazí jakékoli slovo obsahující „wing“, tedy kromě křídla, které hledáme, se nám zobrazí i slova jako „following“ nebo „towing“. Hlavní výhodou od dosavadního filtru by bylo propojení s STPA. Takže při zadání pojmu „znalosti“ by se nám zobrazily veškeré události, kde znalost personálu měla vliv na výsledek letové operace a zároveň by všechny zobrazené události byly klasifikované jako kauzální faktor, nebezpečná řídicí akce, systémové nebezpečí, ztráta. Tato funkce by umožnila zpřehlednění taxonomie a zjednodušení vyplňování hlášení.

V roce 2020 byla vydána nová verze ECCAIRS 2. V porovnání s předchozí verzí existují malé odlišnosti.

Dříve šlo v hlášení zadat více (až 3 typy událostí), nyní lze v online verzi vybrat pouze jeden typ události. Nemyslím si, že je to posun správným směrem, protože incident je



většinou složen z více typů událostí – nalezneme tam řídicí akce, nebezpečné řídicí akce, řízené procesy, ale i nebezpečí nebo ztrátu. Proto nelze vybrat jen jeden typ události, který by ji dostatečně popsal.

Na druhou stranu, je možné, že tato úprava byla myšlena jako ulehčení pro toho, kdo bude hlášení vyplňovat, protože stačí označit pouze jeden typ události, co se stalo. Další detaily, proč k události došlo, se řeší až během analýzy události, nikoliv během vyplňování hlášení. Navíc, některé například technické problémy jsou zjištěny až během vyšetřování, takže tyto informace, *proč* k události došlo ani ten, kdo bude hlášení vyplňovat, vědět nemůže.

Problém, který byl v předchozí verzi a přetrvává i ve verzi nové, je nedostatečná funkčnost off-line hlášení. Tady sice možnost vyplnit až 3 typy událostí zpočátku zůstala, v průběhu psaní této práce, ale došlo k dalším úpravám a tato možnost byla stejně jako u online hlášení zrušena. V off-line verzi je ale větší problém a to ten, že jde rozkliknout jen hlavní kategorie – *následná událost, neznámá událost, jiná událost, provozní typ události, události personálu, organizační typ události, události spojené s vybavením*. Pokud bychom chtěli najít konkrétnější událost, například, že došlo k požáru, tak nemáme možnost, jak do hlášení tuto informaci zadat. Další problém je ten, že po pracovním vyplnění off-line hlášení a jeho uložení po jeho znovuotevření většina informací, které byly do hlášení vyplněny, budou chybět, proto by bylo dobré, kdyby u off-line hlášení došlo k úpravě, která by tyto problémy eliminovala.

V rámci analýzy STPA narazíme na systémové omezení (system level constraints), které můžeme chápat jako požadavek na chování systému, které řídicí v rámci svých rozhodnutí prosazuje, neboť řídicí nesmí tento požadavek porušit. Systémové omezení nám tedy upřesňuje podmínky, jak by se měl systém chovat, aby bylo předcházeno systémovým nebezpečím. Neznamená to ale, že jedno omezení se dá uplatnit pouze na jedno systémové nebezpečí. Reálně jedno omezení je uplatnitelné na jedno nebo více systémových nebezpečí, stejně jako jedno systémové nebezpečí je uplatnitelné na jednu nebo více ztrát. Zajímavé ale je, že v rámci ECCAIRS taxonomie, kde se setkáváme s řídicími akcemi, systémovými nebezpečími nebo ztrátami, omezení v ECCAIRS taxonomii obsaženo není. V ECCAIRS taxonomii existuje kategorie organizační typ události (organisational), která popisuje události, kdy, již došlo k porušení předpisů,



nedodržení postupů, špatně vyplněné nebo chybějící letecké dokumentaci nebo nezachování nutné pauzy personálu, což je následek nedodržení těchto systémových omezení. Veškeré postupy, pravidla a omezení již existují a letecký personál se jimi musí řídit. Otázkou je, zda by do hlášení tato informace nešla zařadit, pokud by k jejímu porušení došlo a jakým způsobem by se zadávala. Zda by šlo o otevřené pole, kam by osoba vyplňující hlášení mohla napsat, jaké omezení bylo porušeno nebo by šlo o pole, které by nabízelo několik možností. Nebo kombinace obou variant. Já osobně si myslím, že tato informace by byla užitečná, a pokud by pole obsahovalo seznam omezení na výběr, tato informace by byla jednoduchá na vyplnění, protože by šlo jen o vybrání jedné z možností. Na druhou stranu, si nedokážu představit, o jak rozsáhlý seznam omezení by se jednalo, zda by stačilo mít na výběr 10 možností nebo by šlo o seznam podobající se typům událostí, kde je 7 hlavních kategorií, které se rozdělují na podkategorie a čítají velký počet pojmů.

Výsledky této práce pro mě byly překvapivé, neočekávala jsem, že nalezneme tolik spojitostí. Výhody převodního systému jsou, že je velice jednoduchý, není časově náročný a je částečně předvídatelný – jsme schopni odhadnout z taxonomie ztrátu, systémové nebezpečí, nebezpečnou řídicí akci či kauzální faktor.

Zároveň jsem při práci narazila na dvě hlavní nevýhody – zaprvé, se jedná o malý vzorek událostí, se kterým jsem pracovala, a proto nelze 100 % zaručit přesnost převodního systému. Zároveň není možné v tomto rozsahu zpracovat například 100 různých událostí, které by nám dávaly přesnější výsledky převodního systému. Druhou nevýhodou je, že ačkoliv jsem se snažila vybírat události s co nejodlišnější taxonomií, aby se neopakovaly stejné pojmy, stále chybí velká část taxonomie, která nebyla vůbec zpracována, a můžeme tedy jen předpovídat její zařazení. Na druhou stranu, jak již bylo zmíněno výše, některé pojmy jsou lehce zařaditelné.

Tento převodní systém vznikl tak, že byly vybrány události, které se následně zpracovaly. Je nutné si uvědomit, že v této bakalářské práci šlo pouze o vyzkoušení, zda převodní systém bude fungovat, neboť STPA je proaktivní analýza, která se využívá tak, že dokáže zjistit potenciální příčinu incidentu ještě předtím, než k incidentu dojde. Jedna z možností, jak by tento převodní systém mohl být využitelný v letecké dopravě, je využití EASA Annual Safety Review, které nám dává aktuální přehled bezpečnostních problémů. Převodní systém by se tedy dal využít tak, že by se vybrala jedna z rizikových



oblastí, kterou EASA Annual Safety Review popisuje, zanalyzovala by se, zjistilo by se, proč k událostem v této oblasti dochází a následně by bylo možné použít opatření, které jsou nutné zavést pro snížení rizika vzniku události v dané rizikové oblasti.



Závěr

Tato bakalářská práce se soustředila na vytvoření převodního systému ECCAIRS taxonomie a analýzy STPA. Jak již bylo zmíněno, v současném systému letecké bezpečnosti, existují mezery, které mohou ohrozit bezpečnost, protože systém s nimi nedokáže počítat. Příkladem je nepředpověditelný lidský faktor nebo nebezpečná interakce mezi jednotlivými komponenty správně fungujícího systému.

V této práci se setkáme s převodním systémem, který by mohl tuto situaci vylepšit. Jde o propojení ECCAIRS taxonomie s STPA analýzou za použití UML. Jako důkaz, že převodní systém funguje, zde bylo ukázáno 6 událostí, které byly nejprve popsány a dle kroků STPA zanalyzovány. To znamená: představení systému, vypracování řídicí struktury, určení ztrát a systémových nebezpečí, vypracování tabulky nebezpečných řídicích akcí, zpracování ztrátových scénářů. Dalším krokem bylo vyplnění hlášení, kde se pracovalo s ECCAIRS taxonomií. Vyplňování hlášení je klíčové. Musí se vyplnit, když dojde k události. Následně se událost zanalyzuje a data z této analýzy nám potom řeknou, co je třeba vylepšit, aby k podobným událostem nedocházelo. Posledním krokem bylo namodelování UML modelu události za použití ECCAIRS taxonomie. V těchto modelech můžeme vidět nejen to, jak událost vypadala, ale i jednotlivé vazby mezi taxonomií, a zároveň i určení STPA pojmů. Následně byly události porovnány.

Z těchto výsledků můžeme určit ztráty, systémové nebezpečí, nebezpečné řídicí akce a řídicí akce z ECCAIRS taxonomie. Například, v kategorii *následná událost* určíme všechny typy událostí jako ztrátu. Neznamená to ale, že by se v jiných kategoriích taxonomie ztráty nenacházely. Naopak systémové nebezpečí nelze jednoznačně určit, z šesti analyzovaných událostí se nacházelo v kategoriích *události spojené s vybavením* nebo *provozní typ události*.

I tak jsou ale výsledky pozitivní, neboť ukazují, že převodní systém funguje, a že existují možnosti, jak s taxonomií dál pracovat, aby se práce s taxonomií co nejvíce zjednodušila a zároveň jsme získali co nejvíce informací – navázání pojmů na UML model.

Limitace mojí práce jsou, že není možné zanalyzovat veškeré typy událostí, alespoň v rámci této bakalářské práce. Určitě by bylo velice užitečné zkusit podobným způsobem zanalyzovat více než jen 6 událostí a získat výsledky, které by dokázaly odhalit další



odlišnosti nebo naopak potvrdit již zjištěné podobnosti v převodním systému. Výsledky z dalších událostí by rozšířily převodní systém a také by mohly odhalit nepřesnosti v převodním systému, se kterými se nedá na obecné rovině počítat a výrazně se liší od mých výsledků. V případě, že by takový převodní systém byl vytvořen, troufám si říct, že by bylo možné ho začít aktivně používat. V budoucnu by tyto výsledky mohly sloužit jako základ pro převodní systém celé taxonomie, jelikož prozatímni výsledky jsou pozitivní a ukazují, že převodní systém v tomto provedení dokáže fungovat a dávat nám uspokojivé výsledky.



Seznam použité literatury

1. ICAO [online]. [cit. 2022-07-24]. Dostupné z: <https://www.icao.int/about-icao/Pages/default.aspx>
2. EASA [online]. [cit. 2022-07-24]. Dostupné z: <https://www.easa.europa.eu/light/easa>
3. ZMEŠKALOVÁ, Adéla. Legislativa a provozní předpisy: Mezinárodní organizace zabývající se civilním letectvím. 2020. Výukový materiál. České Vysoké Učení Technické.
4. Doc 9859, Safety Management Manual. Fourth Edition. Canada: INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2018. ISBN 978-92-9258-552-5.
5. EASA ANNUAL SAFETY REVIEW 2019. 13. EASA, 2019. ISSN 2314-9272.
6. Safety Performance Management Process. In: DOC 9859: Safety Management Manual. 4. ICAO, 2018, s. 4-2. ISBN 978-92-9258-552-5.
7. ECCAIRS 2. ECCAIRS: Aviation Reporting [online]. [cit. 2021-11-05]. Dostupné z: <https://aviationreporting.eu>
8. ICAO Taxonomy [online]. [cit. 2022-07-24]. Dostupné z: <https://www.icao.int/safety/airnavigation/aig/pages/taxonomy.aspx>
9. HEIDI taxonomy [online]. EUROCONTROL, 2009 [cit. 2022-03-19]. Dostupné z: <https://www.eurocontrol.int/publication/esarr-2-reporting-and-assessment-safety-occurrences-atm>
10. STOJIC, Slobodan, Peter VITTEK, Vladimír PLOS a Andrej LALIŠ. Taxonomies and their role in the aviation Safety Management Systems [online]. eXclusive e-JOURNAL [cit. 2022-08-03]. ISSN 1339-4509. Dostupné z: <https://exclusivееjournal.sk/files/1-2015/7-vittek.pdf>
11. ECCAIRS 2: RIT [online]. EASA, 2020 [cit. 2022-03-25]. Dostupné z: <https://aviationreporting.eu/en/ElectronicReporting>
12. ECCAIRS Aviation v.4.1.0.6-at-390: Event-type-values.xlsx
13. ADREP Taxonomy. ICAO [online]. [cit. 2021-11-05]. Dostupné z: [https://www.icao.int/safety/airnavigation/AIG/Documents/ADREP%20Taxonomy/ECCAIRS%20Aviation%201.3.0.12%20\(VL%20for%20AttrID%20%20390%20-%20Events\).pdf](https://www.icao.int/safety/airnavigation/AIG/Documents/ADREP%20Taxonomy/ECCAIRS%20Aviation%201.3.0.12%20(VL%20for%20AttrID%20%20390%20-%20Events).pdf)
14. LEVESON, Nancy a Johny P. THOMAS. STPA HANDBOOK. March 2018.
15. LEVESON, Nancy G. a John P. THOMAS. Different Types of Control Structures. March 2018. STPA Handbook, 2018.



16. KRAUT, M. a I.V. KOGLBAUER. STPA-based analysis of the process involved in enforcing road safety in Austria [online]. Vehicle Safety Institute, Institute of Engineering and Business Informatics (Graz University of Technology), June 2021 [cit. 2021-11-28]. ISSN 2313576X. Dostupné z: doi:10.3390/safety7020034
17. CHEN, S., S. KHASTGIR a P. JENNINGS. Analyzing National Responses to COVID-19 Pandemic using STPA [online]. WMG, University of Warwick, United Kingdom, June 2021 [cit. 2021-11-28]. ISSN 09257535. Dostupné z: doi:10.1016/j.ssci.2021.105195
18. WANG, Y., Y. SUN a C. LI. Aircraft flight safety analysis and evaluation based on IDAC-STPA model. Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics Pages [online]. Equipment Management and UAV Engineering College, Air Force Engineering University, Xi'an, 710051, China, May 2019, 41(5), 1056-1062 [cit. 2021-11-28]. ISSN 1001506X. Dostupné z: doi:10.3969/j.issn.1001-506X.2019.05.18
19. ZAINUDIN, A.H., N.A. HASMIN, A.W. DHIHNY a R.M. SHAH. Aviation safety management: Minimizing the deleterious effect of an aviation disaster. International journal of engineering and technology (UAE) [online]. Science Publishing Corporation, 2018, 2018, 4(7), 35-42 [cit. 2022-03-25]. ISSN 2227524X.
20. BATALOV, Alexander A. Global Aviation Safety Oversight System: Challenges and Opportunities for ICAO and Its Member States. Air and Space Law [online]. Kluwer Law International, 2021, 46(1), 99-118 [cit. 2022-05-19]. ISSN 09273379. Dostupné z: <https://kluwerlawonline.com/journalarticle/Air+and+Space+Law/46.1/AILA202105>
21. The Unified Modeling Language. The Unified Modeling Language [online]. 2009 [cit. 2021-11-29]. Dostupné z: <https://www.uml-diagrams.org>
22. AAIB investigation to Boeing 757-28A, G-OOBC. In: AAIB Bulletin [online]. 2018, March 2018, s. 121-122 [cit. 2021-11-29]. Dostupné z: https://assets.publishing.service.gov.uk/media/5a82efefe5274a2e8ab5a1bf/Boeing_757-28A_G-OOBC_03-18.pdf
23. AAIB investigation to Boeing 767-322, N642UA [online]. In: . AAIB Bulletin, 2016, November 2016, s. 51-52 [cit. 2021-11-29]. Dostupné z: https://assets.publishing.service.gov.uk/media/57ff8ee140f0b67138000012/Boeing_767-322_N642UA_11-16.pdf



24. ÚZPLN – ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin incidentu letadla B 737-45S poznávací značky OK-FGR na letišti Praha-Ruzyně 15.2.2006. In: ÚZPLN [online]. Praha, 2006, s. 1-9 [cit. 2021-11-29]. Dostupné z: <https://uzpln.cz/incident/209>
25. ÚZPLN – ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin letecké nehody pozemního střetnutí letounu CL-600 poznávací značky D-ACPE s košem odmrazovacího vozu na odmrazovacím místě dne 17.12.2010 na letišti Praha/Ruzyně [online]. In: . Praha, 2011, Květen 2011, s. 1-9 [cit. 2021-11-29]. Dostupné z: <https://uzpln.cz/incident/131>
26. ÚZPLN – ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin incidentu nedovoleného vjezdu na aktivní RWY 13 letounem B737-800 poznávací značky OK-TVP dne 4.10.2010 na letišti Praha /Ruzyně [online]. In: . Praha, 2011, Květen 2011, s. 1-8 [cit. 2021-11-29]. Dostupné z: <https://uzpln.cz/incident/129>
27. AAIB investigation to ATR 72-211, G-CLNK: In-flight load shift, Guernsey Airport, 16 April 2021 [online]. In: . AAIB Buletin, 2022, February 2022, s. 53-57 [cit. 2022-07-25]. Dostupné z: <https://www.gov.uk/aaib-reports/aaib-investigation-to-atr-72-211-g-clnk>