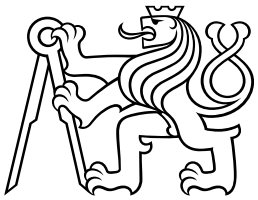


ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Pavel Smíšovský

SYSTÉM PRO INTEGRACI STUDIÍ BEZPEČNOSTI S DATY O BEZPEČNOSTI Z LETECKÉHO PROVOZU

Bakalářská práce

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):

Pavel Smíšovský

Studijní program (obor/specializace) studenta:

bakalářský –LED– Letecká doprava

Název tématu (česky): **Systém pro integraci studií bezpečnosti s daty o bezpečnosti z leteckého provozu**

Název tématu (anglicky): **System for Integration of Safety Studies Knowledge With Aviation Safety Data**

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je vypracovat návrh architektury softwarového nástroje, který zvýší použitelnost modelu integrace znalosti z bezpečnostních studií s daty o bezpečnosti provozu v praxi.
- Popište metodiku integrace znalosti z bezpečnostních studií s daty o bezpečnosti provozu
- Definujte základní prvky nutné pro tvorbu nástroje
- Navrhněte architekturu softwarového nástroje
- Prezentujte vlastní návrh na vybrané sadě dat
- Zhodnoťte možnosti integrace do SMS mezinárodního civilního letiště

Rozsah grafických prací: dle pokynů vedoucího bakalářské práce

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

Seznam odborné literatury: ICAO, Doc. 9859: Safety Management Manual, 4th Edition, Montréal, Quebec, 2018.
Pribyl, P., Přibyl, O. Effective Decision Support System Based on Statistical Tools, 2016.

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

Datum zadání bakalářské práce: **8. října 2021**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **8. srpna 2022**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

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

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

Potvrzuji převzetí zadání bakalářské práce.

Pavel Smíšovský
jméno a podpis studenta

V Praze dne ..... 8. října 2021

Poděkování

Na tomto místě bych rád poděkoval všem, kteří mi jakýmkoliv způsobem pomohli vypracovat tuto bakalářskou práci. Velké poděkování patří zaměstnancům oddělení řízení kvality, safety a procesů Letiště Praha, a. s., kteří mi poskytli podklady pro její vypracování a ochotně její průběh konzultovali. Zejména zde děkuji Ing. Oldřichu Štumbauerovi za konstruktivní připomínky. Zvláště bych pak rád poděkoval Ing. Markétě Šedivé Kafkové za odborné vedení bakalářské práce a za konzultace, s nimiž mi vždy vyšla vstříc. V neposlední řadě je mou milou povinností poděkovat rodičům, blízkým a přátelům za podporu, které se mi od nich dostávalo po celou dobu studia.

Prohlášení

Předkládám tímto k posouzení a obhajobě bakalářskou práci, zpracovanou na závěr studia na Fakultě dopravní ČVUT v Praze.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

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

V Chlumci nad Cidlinou dne 8. srpna 2022 ……

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

SYSTÉM PRO INTEGRACI STUDIÍ BEZPEČNOSTI S DATY O BEZPEČNOSTI Z LETECKÉHO PROVOZU

bakalářská práce

srpen 2022

Pavel Smíšovský

ABSTRAKT

Cílem bakalářské práce je návrh architektury softwaru, který by zvýšil použitelnost metody integrace proaktivní a prediktivní metody řízení provozní bezpečnosti v prostředí mezinárodního civilního letiště v praxi, tedy metody integrace bezpečnostních studií s provozními daty. První část práce je zaměřena na teoretickou rešerši, zejména různé modely, analýzy, legislativu a normy související s tématem letišť a řízením provozní bezpečnosti. Ve druhé části byla podle zásad modelu STAMP a analýzy Active STPA navržena architektura budoucího softwarového nástroje. Nakonec byl návrh prezentován na sadě dat získané z letiště a proběhla diskuse nad implementací tohoto nástroje do prostředí řízení provozní bezpečnosti na mezinárodním civilním letišti.

KLÍČOVÁ SLOVA

STAMP, STPA, Active STPA, provozní bezpečnost, letiště, architektura softwaru, SMS, proaktivní přístup, prediktivní přístup

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

SYSTEM FOR INTEGRATION OF SAFETY STUDIES KNOWLEDGE WITH AVIATION SAFETY DATA

bachelor thesis

August 2022

Pavel Smíšovský

ABSTRACT

The aim of the bachelor thesis is to design a software architecture that would increase the applicability of the method of integration of proactive and predictive methods of safety management in the environment of an international civil airport in practice, i.e. the method of integration of safety studies with operational safety data. The first part of the thesis focuses on theoretical research, in particular various models, analyses, legislation and standards related to the topic of airports and safety management. In the second part, according to the principles of the STAMP model and the Active STPA analysis, the architecture of the future software tool was designed. Finally, the proposal was presented on a dataset obtained from the airport and a discussion was held on the implementation of this tool in an operational safety management environment at an international civil airport.

KEYWORDS

STAMP, STPA, Active STPA, safety, airport, software architecture, SMS, proactive method, predictive method

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

AIM	Aeronautical Information Management Letecká informační služba
ATS	Air Traffic Services Letové provozní služby
CAST	Causal Analysis based on Systems Theory Kauzální analýza založená na teorii systémů
CNS	Communication, Navigation, Surveillance Komunikační, navigační a přehledové (systémy)
ČVUT	České vysoké učení technické v Praze
EASA	European Union Aviation Safety Agency Agentura Evropské unie pro bezpečnost letectví
FMEA	Failure Mode and Effects Analysis Analýza způsobů a důsledků poruch
FTA	Fault Tree Analysis Analýza stromu poruchových stavů
FOD	Foreign Object Debris/Damage Úlomky cizích předmětů / Poškození cizím předmětem
ICAO	International Civil Aviation Organization Mezinárodní organizace pro civilní letectví
LKPR	Letiště Praha-Ruzyně
MCAS	Manoeuvring Characteristics Augmentation System Systém pro zlepšení řídicích vlastností
NASA	National Aeronautics and Space Administration Národní úřad pro letectví a vesmír
ŘLP	Řízení letového provozu
SRM	Safety Risk Management Řízení bezpečnostních rizik
SMM	Safety Management Manual Příručka řízení bezpečnosti
SMS	Safety Management System Systém řízení bezpečnosti
SSP	State Safety Programme Státní program bezpečnosti
STAMP	Systems-Theoretic Accident Model and Processes Systémověteoretický model nehod a procesů

STPA	Systems-Theoretic Process Analysis Systémověteoretická analýza procesů
UCA	Unsafe Control Action Nebezpečná řídicí akce
ÚCL	Úřad pro civilní letectví České republiky
UFO	Unified Foundational Ontology Sjednocená základní ontologie

1 ÚVOD

Letectví se s otázkou provozní bezpečnosti potýkalo od svých prvopočátků. S postupným rozmachem aviatiky, růstem letadel a zvyšujícími se počty přepravovaných osob však bylo nutné začít se dívat na bezpečnostní hledisko komplexněji. Zároveň se letectví přesunulo ze stavu, kdy nejčastěji docházelo k technickým závadám, do doby, kdy se nejslabším článkem systému stal člověk. Nejjednodušší reaktivní přístup, řešící nedostatky až po jednotlivých selháních prvků, již přestal odpovídat požadavkům odborníků i široké veřejnosti. Proto se postupně začaly uplatňovat přístupy proaktivní a prediktivní. Ty významnou měrou posunuly bezpečnost moderního letectví k dnešnímu stavu.

Ačkoliv se jednalo o markantní průlom, stále byly tyto dva pohledy na problematiku bezpečnosti používány odděleně. Ze znalosti systémové analýzy však víme, že „celek je víc než souhrn jeho částí“, jak myšlenku ve 4. století před naším letopočtem formuloval řecký filozof Aristotelés, a proto vznikla myšlenka tyto dva pohledy na bezpečnost propojit, aby se ještě více využilo jejich výhod. Jeden z integračních projektů vznikl i na Fakultě dopravní ČVUT (České vysoké učení technické v Praze) v roce 2019 pod názvem „Konceptuální model integrace znalosti z bezpečnostních studií s daty o bezpečnosti z provozu“. Ze světového hlediska je nutné zmínit hlavně disertační práci Dioga Silvy Castilha pod názvem Active STPA (Systems-Theoretic Process Analysis), jejíž výstupy budou klíčové i pro tuto bakalářskou práci.

Překážkou na cestě plnohodnotného uplatnění takových projektů v SMS (Safety Management System) je jejich teoretičnost a absence softwarového řešení, které by letišti coby koncovému uživateli usnadnilo práci s těmito modely. Tato bakalářská práce právě tyto nedostatky řeší. Jejím hlavním cílem je navrhnout architekturu softwarového nástroje, který by zvýšil použitelnost modelu integrace v praxi. Návrh architektury softwaru přitom bude postaven na poznatcích z analýzy Active STPA. Použitelnost a výhody architektury i případného budoucího softwarového řešení budou poté prezentovány na reálné sadě provozních dat z letiště. Nakonec proběhne diskuse nad zavedením takového nástroje do SMS mezinárodního civilního letiště.

2 LEGISLATIVA

Provozní bezpečností v oblasti mezinárodního civilního letectví se zabývá 19. příloha Úmluvy o civilním letectví (také Chicagská úmluva). V praxi je tento dokument znám jako Annex 19. Do českého práva se převádí předpisem L 19 „Řízení bezpečnosti“, který je povinnou součástí AIM (Aeronautical Information Management) a vydává jej Ministerstvo dopravy České republiky skrze Řízení letového provozu, s. p. Dalším, neméně důležitým prvkem v oblasti řízení provozní bezpečnosti je Dokument 9859, který vydala Mezinárodní organizace pro civilní letectví ICAO (International Civil Aviation Organization). Na území Evropské unie se o bezpečnost letectví stará EASA (European Union Aviation Safety Agency) skrze vydávaná nařízení.

2.1 Annex 19

Poslední příloha Chicagské úmluvy nese název Safety Management, tedy řízení provozní bezpečnosti. V současné době je v platnosti její druhé vydání, aktualizace annexu proběhla v roce 2016. Do oblasti provozní bezpečnosti zavádí tzv. SSP (State Safety Programme), což je z definice „integrovaná sada nařízení a aktivit zaměřených na provozní bezpečnost“, a SMS, tedy *„systematický přístup k řízení bezpečnosti zahrnující nezbytné organizační struktury, odpovědnosti, zásady a postupy“* [1]. Kromě výše zmíněného přesně definuje i další pojmy, jako je např. nehoda, incident, vážné zranění aj. [2]

Podle Annexu 19 mají státy zajistit zřízení SSP, jehož struktura bude odpovídat systému letectví a jeho úrovni v daném státě. Do tohoto programu je nutné implementovat všechny potřebné požadavky, funkce a aktivity, aby mohl být nejen zřízen, ale také nadále udržován. Důležitou součástí SSP jsou též postupy plánování, organizace, řízení programu a jeho neustálé zlepšování. [2]

Co se týče SMS, annex uvádí, které organizace by ho povinně měly zavést. Jedná se o výcvikové organizace, provozovatele komerčních letadel, organizace provádějící údržbu, organizace zodpovědné za návrh a výrobce letadel, provozovatele ATS (Air Traffic Services) a provozovatele letišť. Jednotlivé státy přitom tento seznam mohou rozšířit. [2]

Systémem pro řízení provozní bezpečnosti se zabývá i druhý dodatek Annexu 19. Ačkoliv stále odkazuje na detailnější Dokument 9859, sám podává některá doporučení v oblasti provozní bezpečnosti. Celkem je zde zmíněno dvanáct pilířů implementace SMS, přičemž je lze rozdělit do následujících čtyř kategorií:

1) stanovení bezpečnostních zásad a cílů,
2) řízení bezpečnostních rizik,
3) zajištění bezpečnosti,
4) prosazování bezpečnosti. [2]

2.2 L 19

Letecký předpis L 19 „Řízení bezpečnosti“, vydaný v roce 2013, je jeden z devatenácti leteckých předpisů, kterými jsou annexy převedeny do českého práva. Jejich návrh připravuje ÚCL (Úřad pro civilní letectví České republiky) podle standardů ICAO. [3]

Podobně jako v Annexu 19 jsou i zde vypsány informace pro zřízení SSP a SMS s poznámkou, že detailní informace jsou uvedeny v Dokumentu 9859. V předpisu L 19 se již však objevují konkrétnější požadavky na zřízení SMS jednotlivými, výše zmíněnými organizacemi. Tyto minimální požadavky jsou:

1) identifikace rizik,
2) plánovaný postup zavádění nutných opatření,
3) ustanovení o monitorování řízení bezpečnosti. [1]

SMS pro provozovatele mezinárodních civilních letišť musí být přijatelný pro ÚCL. [1]

2.3 Dokument 9859

SMM (Safety Management Manual), známý pod názvem Doc 9859 nebo Dokument 9859, je součástí dokumentů PANS (Procedures for Air Navigation Services), vydávaných ICAO. SMM upřesňuje požadavky na řízení provozní bezpečnosti v letectví. Je rozdělený do devíti kapitol, v nichž řeší provozní bezpečnost jako takovou, sběr dat o bezpečnosti, jejich vyhodnocování a ochranu, SPS i SMS. V obecné části přístup k provozní bezpečnosti v prostředí mezinárodního civilního letectví rozděluje na čtyři období, a to:

1) technické,
2) lidského faktoru,
3) organizační,
4) celkového systému.

Problémem dnešní letecké bezpečnosti podle manuálu není apriori selhání technické části nebo člověka, jak tomu bylo v minulosti, nýbrž omezený pohled na velmi komplexní oblast mezinárodního civilního letectví. Proto Dokument 9859 ve svých doporučeních upřednostňuje proaktivní přístup a zároveň integraci všech různých organizací, které se podílejí na provozní bezpečnosti v letectví nebo na ni jakýmkoliv způsobem mají vliv. [4]

Jelikož se tato bakalářská práce zabývá oblastí provozní bezpečnosti v civilním letectví, je nutné na tomto místě zmínit problematiku rizika a nebezpečí, definovat je, a vysvětlit tak rozdíl mezi nimi. Nebezpečí (hazard) je „stav nebo objekt, který může potenciálně způsobit incident či nehodu nebo k nim přispět“. Oproti tomu riziko (risk) je *„předpovídaná pravděpodobnost a závažnost následků nebo výsledků nebezpečí“* [1]. [4]

2.3.1 Řízení bezpečnostních rizik

Klíčovou součástí řízení provozní bezpečnosti je SRM (Safety Risk Management). Tento nástroj v sobě zahrnuje identifikaci, vyhodnocení, zmírnění, příp. přijetí bezpečnostních rizik. V oblasti identifikace rizik dokument zmiňuje dvě metody: reaktivní a proaktivní. Také podotýká, že rizika mohou být objevena analýzou bezpečnostních dat a předpovědí vývoje těchto rizik. Tato (třetí) možnost se nazývá prediktivní. Blíže se pohledům na provozní bezpečnost věnuje 3. kapitola této práce (viz Bezpečnostní přístupy). [4]

Důležitým aspektem vyhodnocování závažnosti rizik je pravděpodobnost, že dojde k naplnění tohoto rizika v podobě incidentu či nehody. Při rozhodování o pravděpodobnosti určitého jevu je nutné zvážit všechny možné faktory, které jej ovlivňují. Pomoci může historická zkušenost, funkce podobných komponent systému, časový průběh použití prvku a v neposlední řadě také vazby zkoumaného prvku na ostatní části systému. Ačkoliv je záležitost bezpečnostní pravděpodobnosti do určité míry subjektivní, s rozhodováním o zařazení do určité kategorie může pomoci následující tabulka (Tab. 1), kde je pravděpodobnost rozdělena do pěti kategorií. Nejvyšší pravděpodobnost je v tabulce uvedena pod číslem pět, nejnižší pod číslem 1. [4]

Aby se co nejvíce snížil subjektivní lidský faktor na rozhodování při hodnocení pravděpodobnosti rizika, používá LKPR (letiště Praha-Ruzyně) místo pravděpodobnosti hodnocení ve formě frekvence výskytu daného jevu na letišti za jeden kalendářní rok. Do kategorie velmi vysoká spadají události s roční frekvencí deset a více, na druhé straně tabulky jsou takové události, u kterých je pravděpodobnost, že nastanou, prakticky mizivá, a to nejen na ruzyňském letišti, nýbrž i na ostatních podobných letištích. [5]

Tab. 1: Tabulka pravděpodobnosti rizik [4] [5]

Pravděpodobnost	Frekvence výskytu na LKPR (za rok)	Hodnota
Velmi vysoká	10 a více	5
Vysoká	2–9	4
Střední	1	3
Nízká	Bez výskytu zde či na podobném letišti	2
Velmi nízká	Téměř nemyslitelná	1

Dalším, neméně důležitým ukazatelem bezpečnosti je závažnost rizik. Závažnost rizik se určuje jako pravděpodobný rozsah škod, které by vznikly konkrétní událostí. Do problematiky závažnosti se promítají jak materiální škody, tak zranění či usmrcení osob přímo související s danou událostí. Pro objektivnější vyhodnocení závažnosti rizika je součástí Dokumentu 9859 i tabulka závažnosti rizik (Tab. 2). Rizika řadí od písmena A (nejzávažnější) až po E (nejméně závažná). [4]

Podobně jako u pravděpodobnosti rizik se i u závažnosti LKPR snaží o konkrétnější rozdělení do jednotlivých kategorií, aby byla subjektivita lidského rozhodování v co nejvyšší možné míře snížena. Jak to doporučuje Dokument 9859, hledí se na ztráty na životech či zranění, dále na škody na majetku a v neposlední řadě také na finanční vyjádření škod. V nejvyšší kategorii rizik se pohybují takové nehody, které mají za následek spoustu obětí na životech, letecká technika při bych byla prakticky ztracena a celková ztráta vyjádřená v českých korunách převyšuje hodnotu deseti milionů. Naopak na druhé straně tabulky se nacházejí incidenty, které se obejdou bez jakýchkoliv zranění či poškození techniky a celková ztráty ohodnocená finančními prostředky nepřevyšuje deset tisíc korun českých. [5]

Tab. 2: Tabulka závažnosti rizik [4] [5]

Závažnost	Zdravotní dopady	Škody na technice	Ztráta [Kč]	Hodnota
Katastrofická	Mnohonásobná úmrtí	Celková ztráta	> 10 mil.	A
Nebezpečná	Jednotky mrtvých	Zásadní poškození	do 10 mil.	B
Velká	Těžká zranění	Střední poškození	do 1 mil.	C
Malá	Lehká zranění	Drobné poškození	do 100 tis.	D
Nepatrná	Bez zranění	Bez poškození	do 10 tis.	E

Abychom mohli efektivně vyhodnotit dané riziko, musíme oba výše zmíněné aspekty bezpečnosti (tedy pravděpodobnost a závažnost) spojit do jedné tabulky, respektive matice (Tab. 3), přičemž v řádcích se nachází rozdělení pravděpodobnosti, sloupce jsou dělené podle závažnosti rizika. Označení buněk matice je spojení kódového čísla pravděpodobnosti s kódovým písmenem závažnosti.

Tab. 3: Matice bezpečnostních rizik [4]

Bezpečnostní riziko		Závažnost				
Pravděpodobnost		Katastrofická A	Nebezpečná B	Velká C	Malá D	Nepatrná E
Velmi vysoká	5	5A	5B	5C	5D	5E
Vysoká	4	4A	4B	4C	4D	4E
Střední	3	3A	3B	3C	3D	3E
Nízká	2	2A	2B	2C	2D	2E
Velmi nízká	1	1A	1B	1C	1D	1E

Dokument 9859 také stanovuje, jaká míra bezpečnostního rizika je pro letectví přijatelná, a to následovně:

1) nepřijatelná (5A, 5B, 5C, 4A, 4B a 3A),
2) tolerovatelná (5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C a 1A),
3) přijatelná (3E, 2D, 2E, 1B, 1C, 1D a 1E).

Pakliže je riziko identifikováno jako nepřijatelné, musejí být ihned provedeny takové úpravy, aby bylo zmírněno, případně je nutné problémovou činnost, z níž riziko pramení, pozastavit. Buňky označené žlutou barvou představují rizika, která mohou být za určitých okolností tolerována, ale budou vyžadovat schválení příslušného orgánu, respektive odpovědné osoby. Pokud riziko spadá do zelené, přijatelné kategorie, není třeba činit žádná opatření. [4] [5]

2.4 Nařízení Evropské komise č. 139/2014

Nařízení Evropské komise č. 139/2014 z 12. února 2014 je *„nařízení, kterým se stanoví požadavky a správní postupy týkající se letišť podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008“* [6]. Z pohledu letiště se zabývá podmínkami, které je nutné splnit, aby získalo osvědčení, případně aby mu bylo prodlouženo, a dalšími pravidly, jež musejí být za provozu letišť splněna. [6]

Řízení provozní bezpečnosti se nařízení dotýká v několika oblastech. Například uvádí, že členské státy mají zajistit sledování okolí letišť za účelem zajištění bezpečnosti a omezení rizik souvisejících se:

1) stavbami v okolí letiště,
2) používáním světel, která by mohla piloty oslnit nebo je mást,
3) výskytem divoké zvěře,
4) zdroji elektromagnetických vln, které by mohly rušit nebo ovlivňovat CNS (Communication, Navigation, Surveillance) systémy. [6]

Podobně jako jiné dokumenty zabývající se provozní bezpečností požaduje i toto nařízení Evropské komise zřízení systému řízení provozní bezpečnosti. Tento systém by měl být zřízen příslušným úřadem (v ČR ÚCL) a měl by zahrnovat zdokumentované postupy v rámci organizace, dostatek kvalifikovaného personálu a odpovídajícího zařízení pro plnění povinností. Pro účely vyhodnocení bezpečnosti a správného fungování úřadu je nutné vytvořit systém vedení záznamů, kde lze činnost úřadu zpětně dohledat. [6]

Z pohledu letišť a jejich provozovatelů jsou v nařízení uvedeny požadavky, které musejí být splněny, zejména předložení platné dokumentace a schválených postupů. Po dobu provozu letiště provozovatel zodpovídá za jeho bezpečnost. Musí tedy dodržovat všechny schválené postupy a případné neshody okamžitě vyřešit a vytvořit nápravná opatření. Jakékoliv mimořádné události, které vedly k nehodě či vážnému incidentu nebo které obecně ohrozily provoz na letišti, musí provozovatel hlásit ÚCL, a to do 72 hodin od zjištění daných okolností. Provozovatel letiště je také zodpovědný za zřízení systému řízení bezpečnost, vytvoření letištní příručky a systému bezpečnostních hlášení, dále správu leteckých dat a zajištění bezpečného leteckého provozu na letišti, jmenovitě zřízením záchranných a hasičských služeb, monitorováním pohybu divoce žijících zvířat, stanovením postupů pro letištní personál nebo dohlížením na překážkové plochy a ochranná pásma letiště. [6]

3 BEZPEČNOSTNÍ PŘÍSTUPY

Podle posloupnosti akcí odstraňujících nedostatky systému a pohledu na bezpečnost rozlišujeme tři základní bezpečnostní přístupy používané v prostředí mezinárodního civilního letiště: reaktivní, proaktivní a prediktivní.

3.1 Reaktivní

Jedná se o starší způsob pohledu na bezpečnost, který lze ale za určitých okolností využít i v současnosti. Jak je z názvu patrné, tento přístup reaguje na událost (incident nebo nehodu), jež proběhla v minulosti. Pokud by vše fungovalo v souladu s předpoklady systému, žádná událost by se nestala. Incident nebo nehoda je proto indikátor chybného, respektive nedokonalého fungování systému. Reaktivním pohledem lze odhalit rizika, jež vedla nebo by v budoucnu mohla vést k problémům nebo úplné ztrátě funkčnosti systému. [4]

Výhodou tohoto pohledu je jeho relativní jednoduchost, jež byla uplatňována hlavně v zárodcích aviatiky. Reaktivní metodou bylo například zjištěno, po sérii nehod letounu de Havilland Comet, že hranatá konstrukce letadlových okének špatně rozkládá tlak. Od té doby se konstruují okénka oválná. Ačkoliv je reaktivní pohled na bezpečnost spjat spíše s obdobím technických faktorů, i dnes jej můžeme využít. Nevýhoda tohoto přístupu není v něm samotném, nýbrž v okolnostech, za kterých je použitelný: musí nastat incident nebo nehoda, kterým však nejlépe chceme úplně předcházet. Z novějších nehod řešených právě reaktivním pohledem lze zmínit softwarovou chybu v systému MCAS (Manoeuvring Characteristics Augmentation System) u letounů typu Boeing B737 MAX.

Jak již však bylo naznačeno v úvodu, kvůli vysokému vytížení letišť a celého leteckého prostoru ve druhé polovině 20. století tento pohled samotný přestal stačit stále se zpřísňujícím podmínkám pro bezpečný letecký provoz. Cílem všech zúčastněných subjektů je totiž odhalit nebezpečí ukrytá v systému ještě dříve, než přerostou v událost.

3.2 Proaktivní

Proaktivní přístup posouvá práci s bezpečností na vyšší úroveň, jelikož již pracuje s pohledem do budoucnosti, aktivně a intencionálně hledá takové nedostatky systému, které by mohly přerůst v selhání některých prvků nebo částí systému, a snaží se tyto nedostatky zmírnit či úplně eliminovat. Jeho práce spočívá v analýze jednotlivých komponent a procesů systému a zjišťování, jestli by v něm nemohlo dojít k incidentu nebo nehodě. Tímto přístupem lze zabránit události, která ještě nenastala. [4]

Jako příklad v oblasti provozní bezpečnosti na mezinárodním civilním letišti můžeme uvést systém odstraňování FOD (Foreign Object Debris/Damage). Zaměstnanci letiště pohybující se na provozních plochách jsou poučeni o důležitosti sběru FOD a jejich odevzdávání do vyznačených nádob, které by ideálně měly být rozmístěné po celém areálu letiště. V případě výskytu nežádoucích objektů na dráze a v jejím okolí hrozí nasátí do motoru, což může způsobit velice závažný incident. V minulosti FOD na dráze způsobilo například nehodu nadzvukového dopravního letounu Concorde. Proto dnes již existují různé systémy skenování povrchu dráhy, které včas na nežádoucí objekty upozorní. Dále také platí povinnost posádek na tyto objekty upozorňovat řídící letového provozu. [6]

3.3 Prediktivní

Prediktivní metoda se neobjevuje v Dokumentu 9859 jako základní pohled na bezpečnost, nýbrž jako typ analýzy. Stále častěji se však s tímto přístupem setkáváme v prostředí řízení provozní bezpečnosti mezinárodního civilního letiště, proto je záhodno se prediktivnímu pohledu na bezpečnost nevyhnout.

Prediktivní metoda je založena na predikci, tj. předpovídání situace v budoucnosti. Děje se tak prostřednictvím různých studií a auditů, jejichž cílem je upozornit na chybnou část nebo takový prvek, který by se eventuálně mohl stát nebezpečným pro funkci systému. Své místo má prediktivní přístup například tehdy, když letiště posuzuje, jestli dané rozšíření s sebou nepřinese do oblasti SMS závažnější problém, respektive jaké problémy by mohly do budoucna nastat. Vždy také přijde na scénu, pokud chce letiště nižší kategorie přijímat letadla vyšší kategorie. Typicky se jedná o lety Airbusu A380 (tedy letadla kódového značení F) na ruzyňské letiště, které je však schválené pouze pod kódovým značením 4E. [4] [6] [7]

4 MODEL INTEGRACE

Původním záměrem této bakalářské práce bylo navazovat na model integrace studií bezpečnosti s daty o bezpečnosti z leteckého provozu. V roce 2019 totiž vznikl na Ústavu letecké dopravy Fakulty dopravní ČVUT v Praze projekt s názvem „Konceptuální model integrace znalosti z bezpečnostních studií s daty o bezpečnosti z provozu“. Cílem tohoto projektu, na kterém spolupracuje univerzita se společností Letiště Praha, a. s., bylo navrhnout model, který by propojoval proaktivní a prediktivní přístup k bezpečnosti. Každý způsob totiž skýtá určitá pozitiva, nicméně jejich spojením je možné dosáhnout ještě lepších výsledků. Tyto dva pohledy na bezpečnost jsou však stále používány odděleně, což limituje jejich plnohodnotné využití v praxi. Model integrace je založen na logice STAMP (Systems-Theoretic Accident Model and Processes). Autoři tohoto modelu zmiňují, že myšlenka integrace bezpečnostních studií s provozními daty je už částečně shrnutá v STPA, kde jsou využívány proaktivní indikátory založené na předpokladech systému. Pro další práci s provozními daty je důležitá znalost této fundamentální analýzy. [8]

Během řešení této bakalářské práce bylo zjištěno, že další integrací bezpečnostních studií s provozními daty a fungováním v rámci SMS se zabývá disertační práce Dioga Silvy Castilha pod názvem Active STPA. Systém analýzy, popsaný v této disertační práci, je rozčleněn do tří částí a každá z nich je pak ještě dále rozdělena na několik kroků. Pro návrh architektury softwaru, který by měl využívat přínosy metody integrace, je tento stav ideální, neboť na něj lze architektonicky jednoduše navázat. Pro další práci s tímto tématem tedy bylo rozhodnuto, že metodu integrace studií bezpečnosti s provozními daty, na niž se bude navazovat návrhem architektury softwarového nástroje, poskytne disertační práce pod názvem Active STPA. Základem analýzy, modelem STAMP, se bude zabývat následující kapitola (5). V ní bude také popsána zmíněná disertační práce Active STPA (5.4) a původní analýza STPA (5.3), jež je nutná pro spuštění Active STPA. [9]

5 STAMP

S nástupem složitějších systémů, jejichž nefunkčnost či porucha by měla výrazný dopad na společnost a zároveň by mohla být velmi drahá (tj. jaderná energetika, petrochemický průmysl, kosmonautika, letectví aj.), nastala potřeba zaměřit se na bezpečnost takových systémů, a to nejlépe ještě předtím, než budou uvedeny v činnost. Kvůli komplexitě těchto systémů a nutné vysoké míře provozní bezpečnosti bylo nutné vytvořit bezpečnostní modely, které by simulovaly fungování procesů v rámci systému a upozornily by na případné závady dříve, než by mohly způsobit incident či nehodu.

Mezi nejznámější bezpečnostní modely patří Reasonův model, známý také jako „model švýcarského sýra“, společností NASA (National Aeronautics and Space Administration) vyvinutý model FMEA (Failure Mode and Effects Analysis), dále FTA (Fault Tree Analysis), SHELL a mnoho dalších. Každý z těchto modelů pak na bezpečnost nahlíží různými aspekty, a proto se hodí do specifických oblastí. Některé starší modely už také byly nahrazeny novějšími. Vzhledem k tomu, že tato bakalářská práce navazuje na disertační práci Dioga Silvy Castilha pod názvem Active STPA, kde se používá model STAMP, bude i zde tento bezpečnostní model představen a v průběhu řešení bakalářské práce využíván.

STAMP je jeden z bezpečnostních modelů, který na začátku 21. století vyvinula Nancy Levesonová. Podhoubím pro jeho vznik se stalo zastarávání předešlých modelů (většinou nebyly schopné zohledňovat nelineární vazbu prvků – např. zpětnou vazbu) a zároveň absence takového modelu, který by podal lepší a méně subjektivní zprávu o tom, proč se stávají nehody a jak jim zabránit. STAMP zavádí nový přístup v oblasti zkoumání nehod. Ty jsou dle popisu modelu způsobené vnějšími vlivy, chybami vnitřních prvků systému nebo jejich špatnou interakcí. Na nehodu je zde nahlíženo jako na selhání kontrolních prvků, které nezajistily, aby se nehodě předešlo. Cílem je pak zjistit, jak k tomuto selhání mohlo dojít. Vadný prvek, případně celá část systému (tedy ta část, která nehodu zapříčinila) je důkladně zanalyzována: proč selhala konstrukce a proč právě v tomto místě, z jakého důvodu byl konkrétní prvek vybrán, jestli se jeho chybě nedokázalo předejít, případně jak jí zabránit do budoucna. [8]

5.1 Omezení systému

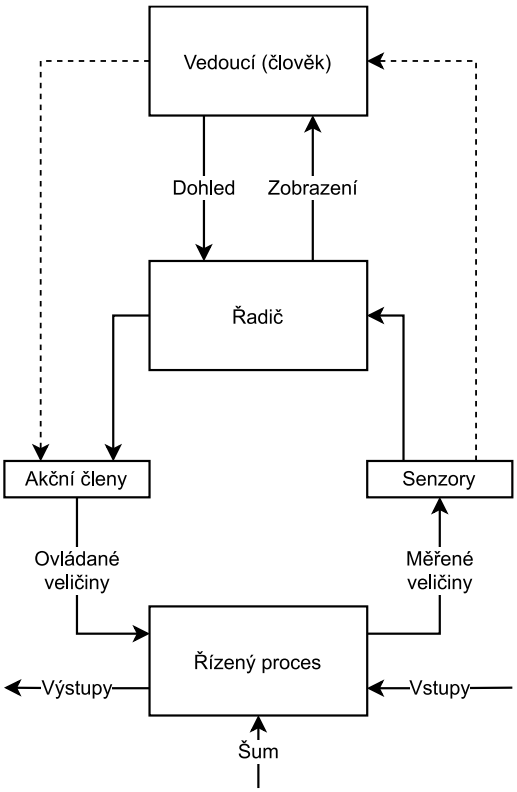
Model pracuje s novým pohledem na chybu systému. Základním pojmem přitom není událost, nýbrž omezení. Aby systém vždy správně fungoval, musí být řádně omezen. V opačném případě, kdy jsou omezení příliš benevolentní, dochází k nehodám. Zvláště důležitá je tato poučka v dnešním světě, v němž možnosti informatiky odsunuly hranice toho, co dříve bylo považováno za nemožné. Najednou tedy pracujeme v mnohem širším a liberálnějším prostředí, kde však daleko více musíme dbát na to, abychom systému nastavili řádná omezení,

respektive vytvořili pravidla pro takové fungování systému, kdy kontrolní orgán může systém dostatečně omezit. Tyto okolnosti mohou být o to obtížnější, že současné systémy nezřídkakdy přesahují hranice lidského intelektu. Omezení modelu STAMP, tedy řízení jednotlivých prvků systému a jejich interakcí, je znázorněno a vysvětleno v kapitole 5.2. [10]

Pro exaktnější pochopení tématu omezení systému přidejme ještě definici z příručky analýzy STPA: „Omezení na systémové úrovni upřesňuje podmínky nebo chování systému, které musejí být uspokojeny pro zabránění rizikům.“ [11]

5.2 Řídicí smyčka

Na rozdíl od jiných bezpečnostních modelů, jež při analyzování daný systém rozebírají na menší části, model STAMP nabízí nové řešení v podobě řízení ovlivněného adaptivní zpětnou vazbou. Toto zpětnovazební řízení je v souladu s dnešním pojetím řízení systému, kdy řídicí prvek (např. člověk) není přímo spojen s řízeným prvkem, a tak od něj nezískává základní parametry odezvy, jako sílu reakce, kmity, zvukové projevy aj. Řídicí prvky člověk ovlivňuje pouze nepřímo, což s sebou nese některé výhody (možnost ovládat systém z větší dálky), ale také nevýhody (již zmíněná absence přímé odezvy). Základním kamenem analýzy modelu STAMP v souladu s výše uvedenými pravidly nepřímého zpětnovazebního řízení je řídicí smyčka (viz Obr. 1). Díky ní lze lépe porozumět tomu, co se v systému děje a jak odpovídá na jednotlivé podněty, tedy vstupní prvky, které do procesu přicházejí. [10]

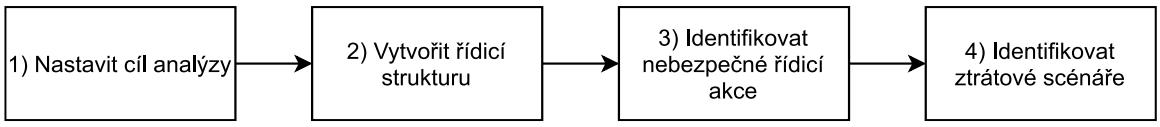


Obr. 1: Řídicí smyčka (vytvořeno podle [5])

5.3 STPA

STPA je metoda analýzy rizik založená na modelu STAMP. V základě již zahrnuje propojení analýzy rizik s provozními daty o bezpečnosti. Podobně jako základní model STAMP zdůrazňuje potřebu holistického řešení provozní bezpečnosti. Rozdíl mezi STAMP a STPA je v jejich funkci. STAMP totiž není považován za analytický nástroj, nýbrž pouze za teoretický model bezpečnosti. Pro plné využití tohoto modelu je nutné použít nástroje na něm založené, např. STPA nebo CAST (Causal Analysis based on Systems Theory). CAST představuje nástroj reaktivního přístupu k provozní bezpečnosti, a proto je v této bakalářské práci upřednostněna analýza STPA, která pohlíží na bezpečnost proaktivně. [10] [11]

Součástí příručky STPA je detailní návod, jak provést analýzu pomocí tohoto přístupu založeném na modelu bezpečnosti STAMP. Tato analýza se skládá ze čtyř základních kroků uvedených na Obr. 2. V příručce je ke každému kroku uveden i jeho podrobný popis.



Obr. 2: Kroky analýzy STPA (přeloženo z [9])

5.3.1 Nastavit cíl analýzy

Prvním krokem analýzy STPA je, podobně jako u dalších typů analýz, definovat její cíl, respektive účel. Tento krok se skládá ze čtyř částí:

1) identifikovat ztráty,
2) identifikovat nebezpečí na systémové úrovni,
3) identifikovat omezení na systémové úrovni,
4) upřesnit nebezpečí (volitelné). [11]

Ztráty, kterým chceme předejít, mohou být materiální či finanční podoby, ale zahrnují také zranění, ztráty lidských životů, dopad na životní prostředí nebo jiné situace, které jsou nepříjemné pro zúčastněné strany. Tyto ztráty musejí být v této části analýzy identifikovány a mohou být zároveň seřazeny podle jejich závažnosti nebo důležitosti pro systém. [11]

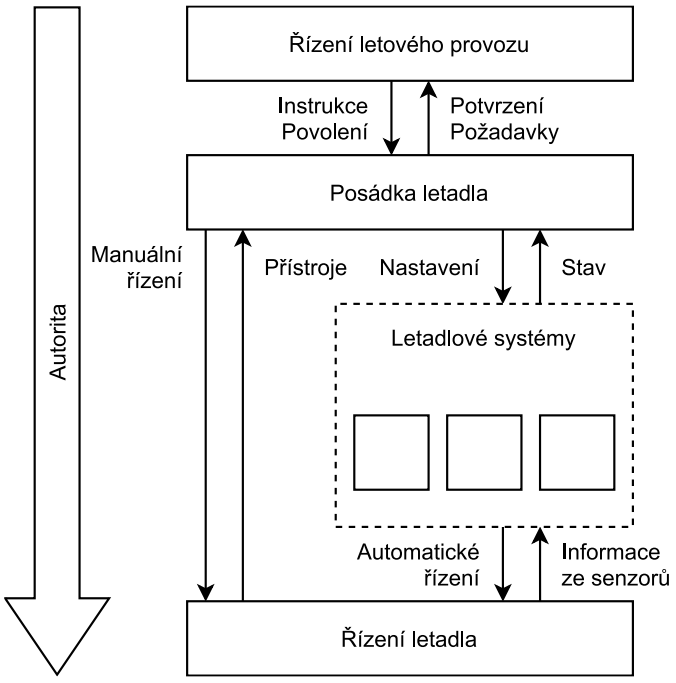
„Nebezpečí je stav systému nebo stav podmínek, které spolu s konkrétním nejhorším stavem okolního prostředí povedou ke ztrátě.“ Abychom nebezpečí mohli identifikovat, musíme nejdříve stanovit, co považujeme za sledovaný systém, a co za okolí. Následuje vypsání všech možných nebezpečí, tedy nebezpečných stavů systému, které by při určité konfiguraci mohly vést ke ztrátě. Zároveň k těmto nebezpečím přiřazujeme ztráty z předešlého kroku. [11]

Tématu omezení systému se podrobněji věnuje kapitola 5.1, kde je také uvedená jeho definice. Tento krok úzce navazuje na identifikaci nebezpečí, jelikož přesně víme, která omezení máme aplikovat, aby byla nebezpečí odstraněna nebo zmírněna, případně byly zmírněny jejich následky. Vlastně se jedná o negaci nebezpečí. Pokud jsme například v předchozím kroku identifikovali jako nebezpečí nedodržení rozstupů mezi letadly, omezením by bylo dodržování předepsaných rozstupů. [11]

Posledním, volitelným krokem první části analýzy STPA je upřesnění nebezpečí. Příručka STPA uvádí jako příklad nebezpečí, že se letadlo dostane do blízkosti dalších objektů na zemi, což můžeme upřesnit např. tím, že letadlo dostatečně nebrzdilo. [11]

5.3.2 Vytvořit řídicí strukturu

Řídicí strukturu systému lze chápat jako vazby mezi prvky systému, které jsou namodelované pomocí řídicích smyček (viz kapitolu 5.2). Řídicí smyčka jako taková představuje řízení procesu vedoucím. V rámci řídicí smyčky mohou nastat chybové situace: vedoucí se může rozhodovat na základě pocitů, které nekorespondují s realitou, detektory mohou do systému posílat chybná data aj. Pomocí dalších kroků se STPA snaží tyto situace nalézt. Jak může vypadat konkrétní řídicí struktura v oblasti mezinárodního civilního letectví, ukazuje Obr. 3. Zároveň je na obrázku i uvedena hierarchie systému, od nejvyšší autority – ŘLP (řízení letového provozu) – až po letadlo, které samo o sobě o ničem nerozhoduje, pouze podává informace vyšším autoritám. Pro přehlednější zobrazení hierarchie je zvolen systém vertikálního rozlišení. [11]



Obr. 3: Ukázka řídicí struktury v letectví (přeloženo z [9])

5.3.3 Identifikovat nebezpečné řídicí akce

Ve třetím kroku dochází k určení takových řídicích akcí, které by mohly vést ke ztrátám definovaným v prvním kroku. Nebezpečná řídicí akce je v příručce STPA definována jako „řídicí akce, která v určité situaci a nejhorších podmínkách okolního prostředí povede k nebezpečí“. Účelem tohoto kroku je nastavit omezení systému (viz kapitolu 5.1). Obecně lze nebezpečné řídicí akce rozlišit podle čtyř kritérií:

1) absence řídicí akce vede k nebezpečí,
2) použití řídicí akce vede k nebezpečí,
3) použití bezpečné řídicí akce, avšak brzy, pozdě nebo ve špatném pořadí,
4) řídicí akce trvá moc dlouho nebo příliš krátce (pro kontinuální řídicí akce). [11]

5.3.4 Identifikovat ztrátové scénáře

Na konci analýzy STPA přichází čas na odhalení ztrátových scénářů, tj. důvodů (příčin), proč by se v systému mohly objevit nebezpečné řídicí akce. V potaz musíme brát dva druhy těchto scénářů, a to:

1) proč by v systému mohla proběhnout nebezpečná řídicí akce (chyba v řídicím prvku, chybné algoritmy, chybné vstupy, nesprávný model aj.),
2) proč by řídicí akce nemusely být vykonány správně nebo proč by nemusely být vykonány vůbec (špatné vazby mezi prvky nebo chybné řídicí akce). [11]

5.4 Active STPA

Myšlenka analýzy Active STPA je zachycena v disertační práci Dioga Silvy Castilha z Massachusettského technologického institutu. Práce byla vedena přímo autorkou výše zmíněného modelu STAMP. Jejím cílem bylo integrovat analýzu nebezpečí do SMS pomocí použití metody Active STPA, tedy aktivní verze analýzy STPA. Tato metoda využívá data z provozní bezpečnosti (např. systém dobrovolného hlášení) k určení vývoje stavu bezpečnosti. Na rozdíl od běžně používané praxe se tedy jedná o nástroj nikoliv reaktivního, nýbrž proaktivního pohledu na provozní bezpečnost. Výstupem z této analýzy je sada obranných opatření k prevenci a zmírnění bezpečnostních rizik, která budou prosazovat požadavky a omezení generované analýzou STPA. [9]

Rozdíl mezi STPA a Active STPA je v použití provozních dat. Zmíněná disertační práce poznamenává, že bezpečnost v klíčových oblastech nemůže záviset na zkušenostech několika zainteresovaných lidí. Právě proto do systému vstupuje tvrdý, exaktní faktor, kterým jsou provozní data. Aktivní STPA analýza byla zkonstruována proto, aby pomocí trendu vývoje provozní bezpečnosti neustále aktualizovala STPA. [9]

Pro použití Active STPA potřebuje zmíněná organizace projít následující kroky:

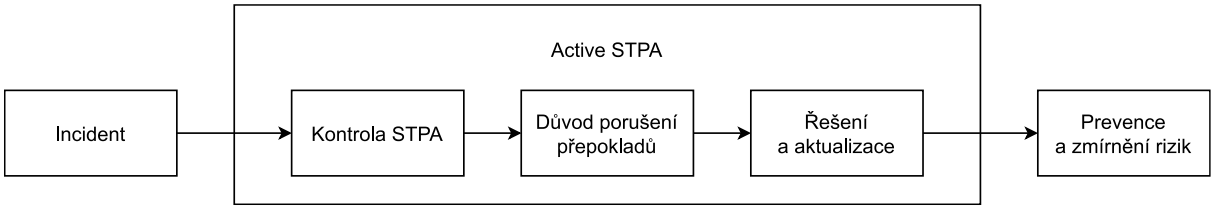
1) vytvořit STPA nebo použít již existující,
2) zavést opatření doporučená STPA,
3) nasbírat provozní data,
4) použít analýzu Active STPA. [9]

Analýza Active STPA tedy pracuje na principu zlepšení, zpřesnění a aktualizování původní analýzy STPA, a to na základě incidentu, respektive provozních dat. Pro její použití je nutné nejprve projít analýzu STPA nebo použít nějakou existující, na kterou lze navazovat analýzou Active STPA.

Samotná analýza Active STPA se pak skládá ze tří základních kroků, a to:

1) kontroly základní STPA,
2) důvodu porušení předpokladů,
3) řešení a aktualizace. [9]

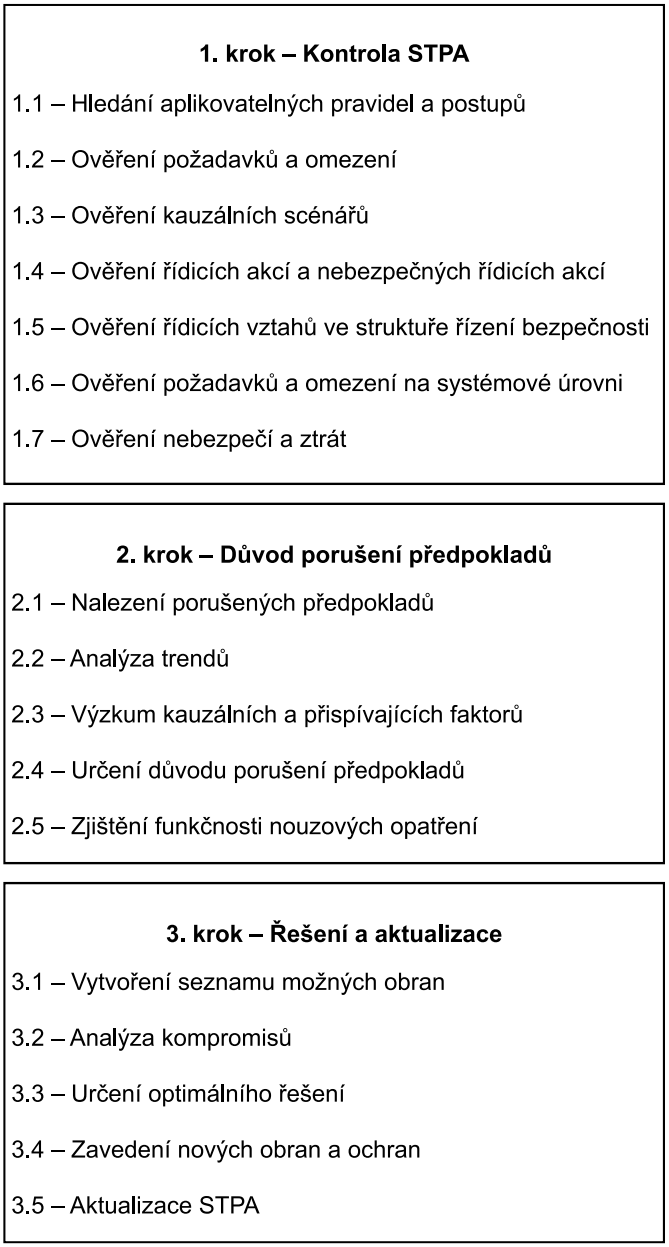
Výstupem z analýzy Active STPA je prevence vzniku rizik a jejich zmírnění. Celý proces (tedy vstupy, samotná analýza Active STPA a výstupy) je pro lepší představivost graficky znázorněn na Obr. 4. Informace z této části budou použity při návrhu architektury softwaru. [9]



Obr. 4: Stručný diagram analýzy Active STPA (přeloženo z [10])

Z obrázku je patrné, že do systému bude vstupovat nějaký incident, respektive provozní data (např. rychlost letadel při vyjíždění z dráhy na rychloodbočku). V rámci systému pro integraci studií bezpečnosti s daty o bezpečnosti z leteckého provozu budou postupně řešeny kroky analýzy Active STPA. Výstupem pak budou informace o nebezpečných řídicích akcích a opatřeních k prevenci a zmírnění rizik. Předpokládá se jak určité textové, tak i grafické znázornění.

V následující části se budeme konkrétněji věnovat analýzy Active STPA a jejím třem krokům, z nichž se skládá. Představeny byly výše, nyní budou podrobně rozebrány. Pro lepší představivost je opět přiloženo grafické znázornění (viz Obr. 5).



Obr. 5: Kroky analýzy Active STPA (přeloženo z [10])

5.4.1 1. krok – Kontrola STPA

Hledání aplikovatelných pravidel a postupů: Na začátku analýzy Active STPA se zjišťuje, jakým způsobem jsou pravidla provozu a provozní postupy komunikovány směrem od řízení společnosti k řídicím prvkům skrze dokumenty, manuály atd. Pokud je v tomto kroku zjištěno, že se ve společnosti uplatňuje postup, který měl zabránit onomu incidentu, přichází na řadu úvaha, proč tento postup nezafungoval. Ze všech důvodů pro tuto nefunkčnost zmiňme konflikt s jinými postupy, nákladnost či nedostatek času pro zavedení. [9]

Ověření požadavků a omezení: V tomto kroku se ověřují původní požadavky a omezení, které byly do systému vneseny původní analýzou STPA. Vzhledem k časovému intervalu mezi poslední analýzou však již tyto kroky nemusejí stačit nebo nemusejí být aktivně prosazovány (provozní odchylka). Zjišťuje se také, jestli v systému již neexistují omezení, která měla zamezit incidentu. Pokud ne, jsou vytvořena a zjišťuje se, proč nebyla vytvořena dříve; pokud ano, postupuje se na další fázi prvního kroku. [9]

Ověření kauzálních scénářů: Ve čtvrtém kroku analýzy STPA (viz kapitolu 5.3.4) jsou zkoumány nebezpečné řídicí akce a to, jak k nim může dojít. Pokud nebyla identifikována taková řídicí akce, která vedla k incidentu, je nutné vyšetřit příčiny před přesunem k další fázi analýzy Active STPA. Disertační práce ohledně použití Active STPA se také zabývá nutností určitých kompromisů v této fázi. Na jedné straně totiž můžeme abstraktnějšími scénáři obsáhnout obecnější omezení, která však nebudou dostatečně specifická na bezpečné uplatnění v praxi. Na straně druhé můžeme zkoumat konkrétnější scénáře, kterých však bude daleko více, a existuje tak větší riziko, že některý přehlédneme. Na tuto fázi navazuje část třetího kroku analýzy Active STPA. [9]

Ověření řídicích akcí a nebezpečných řídicích akcí: V této části analýza Active STPA zjišťuje, zda řídicí akce účastnící se incidentu koresponduje s některou nebezpečnou řídicí akcí identifikovanou v rámci původní analýzy STPA. Ať už je výsledek tohoto zjištění jakýkoliv, v této fázi by se měly prověřit předpoklady fungování systému, zejména je důležité revidovat zodpovědnosti každého řídicího prvku systému a jeho vazby na ostatní prvky. [9]

Ověření řídicích vztahů ve struktuře řízení bezpečnosti: V každém systému se objevují řídicí prvky na různých úrovních, tedy hierarchicky vyšší (srov. ŘLP na Obr. 3), a hierarchicky nižší (srov. letadlové systémy na témže obrázku). Bezpečnostní analytik musí v tomto kroku vzít v potaz obě tyto úrovně a identifikovat všechny příslušné řídicí smyčky. Pro lepší pochopení je tato fáze uvedena na konkrétním příkladu z praxe, kdy letadlo letělo na přiblížení vyšší rychlostí, než je obvyklé. Jako první se nabízí chyba posádky, nicméně musí se také prozkoumat, jaké pokyny dostala posádka od ŘLP. Nebezpečné řídicí akce na nižších úrovních jsou totiž běžně způsobeny řídicími akcemi z vyšších úrovní nebo také špatnou kooperací prvků na stejné úrovni. Nedostatečné řízení prvků může indikovat změnu systému po původní analýze STPA. V tomto případě je nutné znovu zmapovat strukturu systému. [9]

Ověření požadavků a omezení na systémové úrovni: Omezení a požadavky na vyšších hierarchických úrovních vycházejí přímo z nebezpečí v systému. Toto může být problém při důležitých změnách systému, které byly provedeny až po původní analýze STPA. Úplnost požadavků a omezení na vyšších úrovních systému je klíčová pro bezpečnost celého systému, neboť jejich porušení může vést ke ztrátě. [9]

Ověření nebezpečí a ztrát: Konečná fáze prvního kroku analýzy Active STPA vede bezpečnostního analytika k nalezení chybějících ztrát, nebezpečí a požadavků a omezení na systémové úrovni, což navazuje na předchozí fáze analýzy. Absence ztráty nebo nebezpečí je však v této fázi celkem vzácná. [9]

5.4.2 2. krok – Důvod porušení předpokladů

Nalezení porušených předpokladů: Při posuzování porušení předpokladů je důležité zjistit, proč řídicí prvek porušil postup nebo spíše zásadu. Dále je nutné vzít na vědomí, že jednoduché obvinění člověka z nedodržování postupů je velmi krátkozraké. Naopak musíme pochopit, co jej k tomu vedlo, tzn. dívat se na systém holistickým přístupem. Pokud jsou předpoklady porušovány opakovaně, je to znamení, že přijatá opatření nejsou efektivní, a tento fakt se musí zohlednit v následujícím kroku analýzy. [9]

Analýza trendů: Pokud dojde k události, nemusí to nutně znamenat, že předpoklady systému jsou chybné. Za incidentem totiž může stát úplná náhoda, a tento incident pak bude ojedinělou událostí, která se nebude opakovat. Na druhou stranu se může analýzou dat zjistit, že se zde objevují určité trendy, které by měly být prošetřeny. Příkladem z disertační práce je střet letadla s ptákem ve fázi přiblížení na přistání. Vyšetřením dat lze například zjistit, že v tomto místě vzrostlo množství ptactva, a tudíž se bude jednat o trend v oblasti bezpečnosti. [9]

Výzkum kauzálních a přispívajících faktorů: K nebezpečné řídicí akci vede vždy jeden nebo více kauzálních faktorů. Tyto faktory mohou být tříděny a posuzuje se jejich vliv, pokud by se měly opakovat v jiných situacích. [9]

Určení důvodu porušení předpokladů: Jak již bylo uvedeno v jedné z předchozích fází, spíše než stanovením viny za událost se provozní bezpečnost zabývá otázkou, co daný prvek systému vedlo k jeho rozhodnutí. Je možné, že předpoklady, které byly stanoveny, platí pro obvyklý stav systému, avšak nelze je použít pro vzácné situace. Ve společnostech bývají často z chyb viněni zaměstnanci. Ačkoliv tento pohled může přinést krátkodobé zlepšení situace, z dlouhodobějšího hlediska se jedná o nesystémové řešení. Je nutné přiznat chybu na úrovni celého systému. Analýza Active STPA může pomoci prosazovat systémová opatření, případně identifikovat mezery v bezpečnostních postupech společnosti. [9]

Zjištění funkčnosti nouzových opatření: Jelikož by systém neměl spoléhat pouze na omezení, potřebuje také nějaká nouzová opatření, která zareagují v případě, že předpoklady selžou. Může se jednat například o redundanci zařízení – když se jedno porouchá, stále je ještě v záloze druhé. Tato nouzová opatření mají buď úplně zabraňovat nehodám, nebo alespoň zmírnit jejich následky. V této fázi analýzy Active STPA se sleduje, jestli byla taková opatření zavedena a jestli zareagovala, případně musejí být vytvořena nová. [9]

5.4.3 3. krok – Řešení a aktualizace

Vytvoření seznamu možných obran: První fáze třetího kroku zjišťuje, jak udělat systém lepší, bezpečnější. V jednodušších systémech se může nabízet jen jedno řešení, kdežto ve složitějších jich bude patrně více. Tato řešení pak můžeme rozdělit na taková, která do stávajících postupů zasáhnou méně, a taková, která budou vyžadovat důkladnější implementaci a vyšší vynaložené prostředky. Toto rozdělení pak bude nápomocno při rozhodování o zavedení jednotlivých opatření v další fázi. [9]

Analýza kompromisů: Jelikož se v předchozí fázi řešení rozdělovala podle složitosti jejich implementace, nyní je čas na posouzení jejich hlavních výhod a nevýhod, a to podle metod již přijatých organizací. Hodnotí se, jak by jednotlivá opatření byla přijímána ve společnosti a jaký by byl jejich dopad. Zejména u řešení, která vyžadují větší zásah do struktury společnosti, je nutné velmi důkladně prozkoumat jejich vliv. [9]

Určení optimálního řešení: Ze všech uvažovaných řešení, která byla stanovena v předchozích fázích, se vybere alespoň jedno, přičemž se nesmí zapomenout na nové požadavky a omezení, které toto řešení přináší do systému. Dále je nutné rozhodnout, do jaké míry bude zajištěna rovnováha prevence a zmírnění rizik. Nejbezpečnější je sice vsadit vše na prevenci, nicméně tento krok je pro společnost velmi nákladný, a tudíž neefektivní. Levnější je zmírnění rizik, tento pohled ale zase popírá proaktivní přístup k bezpečnosti. [9]

Zavedení nových obran a ochran: Řešení, které bylo vybráno a u kterého byl vyloučen střet s jinými pravidly, je připravené pro zavedení. Očekává se, že více změn bude čekat dokumenty na nižší úrovni, např. manuály. U každé změny musí být jasné, kdo je zodpovědný za její zavedení a dokdy se tak má učinit. Protože je bezpečnost společnosti velmi komplexní, není dostačující jen rozeslat změny v opatřeních zaměstnancům. Naopak je nutné, aby se s těmito novými opatřeními všichni sžili, čehož se dosahuje těmito kroky:

1) školení (předávání informací zaměstnancům),
2) plánování (myslí se plánování budoucích akcí, při němž jsou vyjasněny nesrovnalosti nebo nedorozumění),
3) nastavení (zapamatování procesů při různých situacích, checklisty),
4) provoz (použití jasných zvukových, hmatových nebo vizuálních signálů v provozu). [9]

Aktualizace STPA: Na úplném konci analýzy Active STPA se zpětně zahrnují vzešlé předpoklady a všechny nové prvky systému. Mění se bezpečnostní požadavky a omezení. Ačkoliv se analýza Active STPA snaží nalézt všechna slabá místa systému, je nutné mít na vědomí, že ani v této fázi nemusí být jejich seznam kompletní nebo že zavedená opatření nemusejí být dostačující. Zejména se jedná o latentní chyby, které se v systému dlouho neprojevují. Tato analýza tak musí být stále se zdokonalujícím procesem. [9]

5.5 UFO

Ontologie (z řeckého *óntos*, tj. jsoucí, a *logía*, tj. dějové jméno od *légó* – sbírám, čtu, mluvím) je ve filozofii podle Akademického slovníku cizích slov *„učení o bytí, o jeho nejobecnějších určeních a pojmech“*. [12] Slovník spisovného jazyka českého pak toto heslo shrnuje do jednoduchého *„nauka o jsoucnu“*. [12] Do češtiny měl tento termín proniknout v 19. století. [13]

Tato věda nebo obor filozofie se tedy zabývá bytím, existencí, jsoucnem. Popularizována byla filozofy v 18. století, do oblasti výpočetní technologie, softwarové architektury a modelů se ontologie dostala v druhé polovině 20. století, přičemž větší pozornost na ni byla upřena po roce 2000. [14]

UFO (Unified Foundational Ontology) je ontologie vyvinutá italským vědcem Giancarlem Guizzardim v roce 2006 v rámci disertační práce na nizozemské univerzitě Twente. Pro vybrané části modelu STAMP ji v roce 2018 využila studentka Fakulty dopravní ČVUT Natalia Guskova ve své bakalářské práci s tématem „Konceptualizace vybraných částí modelu bezpečnosti STAMP“. V ní je primárně podrobena studiu řídicí smyčka a analýza STPA, která se jako základ objevuje i v tomto dokumentu. [14] [15]

Ačkoliv se tato bakalářská práce primárně nezabývá programováním určitého softwaru založeného na modelu bezpečnosti STAMP, mohou informace z předchozího výzkumu na Fakultě dopravní ČVUT pomoci při pochopení návrhu architektury potřebného softwarového nástroje, zejména při vytváření jednotlivých prvků systému. Ontologie také může pomoci s modelováním vazeb na původní analýzu STPA a rozhodně by měla být zohledněna v budoucnu při programování softwarového nástroje založeného na architektuře popsané v této bakalářské práci. Jelikož je tato ontologie unifikovaná, zaručuje bezproblémovou návaznost jednotlivých softwarů, zde například STPA a Active STPA. Pokud má být uplatněna ontologie právě v případě nástroje popsaného v této bakalářské práci, bude však nutné některé části UFO ještě domodelovat. Například se jedná o spouštěcí indikátory, které nejsou v UFO dosud zohledněny.

6 DEFINICE

V návrhu architektury softwaru i v budoucím softwarovém nástroji budou používány termíny ze slovníku modelu STAMP. Jelikož se v drtivé většině jedná o abstraktní slova, jejichž význam nemusí být hned zpočátku uživateli zcela zřejmý, je záhodno je v této části vysvětlit. Je plánováno tyto vysvětlivky též zahrnout do samotného softwarového nástroje, a to do konkrétních kroků, v nichž budou tyto termíny používány. Pro lepší představivost je také plánováno vždy uvést příklad, na kterém se uživateli použití těchto termínů osvětlí. Tyto příklady by pocházely přímo z reálného řešení Active STPA v této bakalářské práci (viz kapitolu 8).

Kauzální scénář (Causal Scenario)

Cesta modelem systému, na jejímž konci se nachází nebezpečná řídicí akce.

Nebezpečí (Hazard)

Stav nebo objekt, který může potenciálně způsobit incident či nehodu nebo k nim přispět. [4]

Nebezpečná řídicí akce (Unsafe Control Action)

Řídicí akce, která v daném kontextu a nejhorším možném prostředí povede k nebezpečí. [11]

Nouzové opatření (Contingency Protection)

Opatření zavedené za účelem zabránění ztrátám nebo jejich zmírnění.

Obrana (Defense)

Konkrétní zmírňující opatření, preventivní kontrola nebo nápravné opatření zavedené za účelem zabránit naplnění nebezpečí nebo jeho eskalaci. [4]

Omezení na systémové úrovni (System-Level Constraint)

Omezení specifikuje podmínky nebo chování systému, které musejí být splněny, aby se předešlo nebezpečí (a nakonec i ztrátám). [11]

Omezení řídicího prvku (Controller Constraint)

Omezení specifikuje chování řídicího prvku, které musí být splněno, aby se zabránilo nebezpečným řídicím akcím. [11]

Postup (Procedure)

Pravidlo uplatňované ve společnosti.

Provozní data (Safety Data)

Definovaný soubor faktů nebo soubor bezpečnostních hodnot shromážděných z různých zdrojů souvisejících s letectvím, který se používá k udržení nebo zvýšení bezpečnosti. [4]

Předpoklad (Assumption)

Co je přijímáno za pravdu bez otázek a důkazů. [16]

Riziko (Risk)

L 19: *„Předpovídaná pravděpodobnost a závažnost následků nebo výsledků nebezpečí.“* [1]

STPA: Riziko je definováno z hlediska účinnosti řídicích prvků používaných k prosazování bezpečného chování systému, tj. konstrukce a fungování bezpečnostní řídicí struktury. [11]

Řídicí akce (Control Action)

Orientovaná vazba směrem od řídicího prvku, která zajišťuje řízení procesu.

Ztráta (Loss)

Ztráta zahrnuje něco, co má pro zúčastněné strany hodnotu. Ztráty mohou zahrnovat ztrátu lidského života nebo zranění lidí, škody na majetku, znečištění životního prostředí, ztrátu poslání, ztrátu pověsti, ztrátu nebo únik citlivých informací nebo jakoukoli jinou ztrátu, která je pro zúčastněné strany nepřijatelná. [11]

Ztrátový scénář (Loss Scenario)

Ztrátový scénář popisuje kauzální faktory, které mohou vést k nebezpečné řídicí akci a k nebezpečím. [11]

Zmírnění rizik (Risk Mitigation)

Proces začlenění obranných, preventivních řídicích akcí nebo nápravných opatření ke snížení závažnosti nebo pravděpodobnost předpokládaného následku nebezpečí. [4]

7 ARCHITEKTURA SOFTWARU

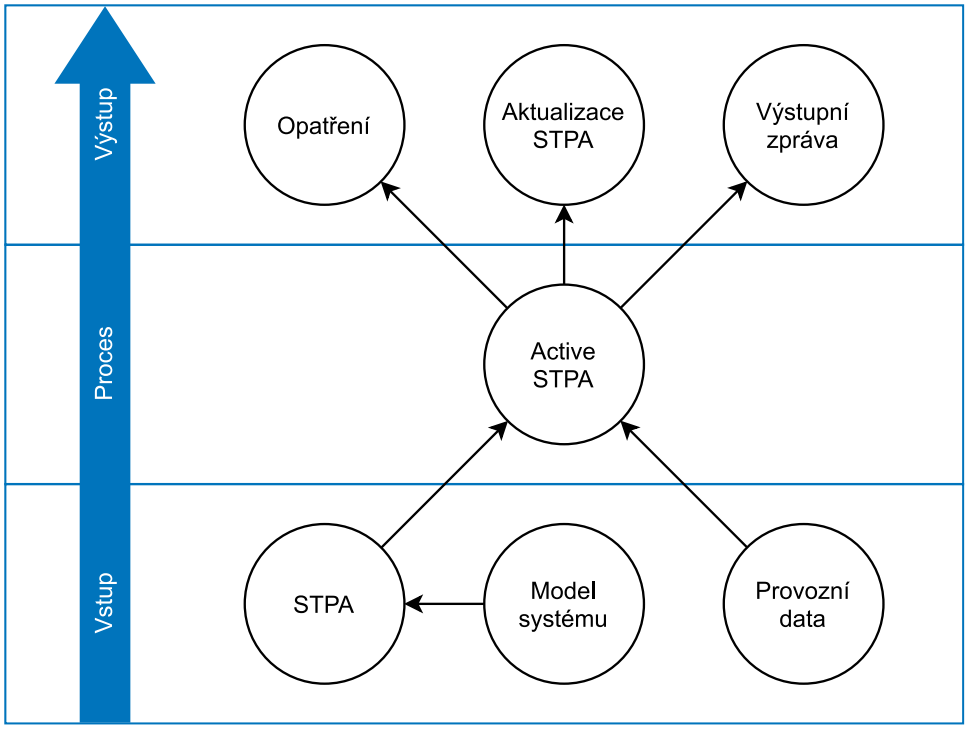
Vzhledem k tomu, že tento obor je relativně mladý (ve větší míře se pozornost na něj byla upřena v 70. letech 20. století), neexistuje zatím jednotná definice toho, co to vlastně softwarová architektura je. Každý zdroj nabízí svůj pohled na věc. Etymologicky se význam slova architektura posunuje z oblasti stavebního průmyslu do oblasti výpočetní techniky, jeho smysl pro konkrétní obor nicméně zůstává téměř stejný. Architekturou u stavebnictví rozumíme to, jak dům vypadá zvenčí, jakých je tvarů, zároveň i vnitřní uspořádání, tj. jak jsou situovány místnosti, ale nesmí zde chybět ani plány elektrických rozvodů, vodovodního potrubí, rozmístění světel atd. Architektura v sobě tedy zahrnuje nejen obecný pohled na dům, nýbrž i detaily v různé rozlišovací úrovni neboli podrobnosti, přičemž všechny prvky je nutné považovat za úzce vzájemně propojené a systém brát jako celek. Analogicky tato pravidla můžeme převést na architekturu softwaru. [17] [18]

Pokud bychom se nespokojili s analogií předchozího zdroje, existuje spousta dalších vysvětlení architektury softwaru. Například kniha Document Software Architectures z roku 2011 nabízí hned několik definic toho, co se může rozumět pod tímto pojmem, jedním dechem ale dodává, že již v roce vydání těchto definic existuje přes 150 a jejich počet s největší pravděpodobností za předešlé roky ještě vzrostl. Některé jsou jednodušší a intuitivní, jiné si dávají za cíl přesně specifikovat, o co se v dané problematice jedná, a vyjmenovávají všechny prvky, které se na architektuře softwaru podílejí. Jelikož je architektura softwaru pro tuto bakalářskou práci a komplexní oblast provozní bezpečnosti na mezinárodním civilním letišti klíčová, uveďme alespoň pár definic pro lepší porozumění tohoto pojmu. [19]

- „Architektura softwaru = {prvky, forma, zdůvodnění}. (…) Architektura softwaru je soubor architektonických (…) prvků, které mají určitou formu.“ [18]
- Architektura softwaru je „struktura komponentů programu/systému, jejich vzájemné vazby a principy a pokyny řídící jejich uspořádání a vývoj v čase“. [20]
- „Architektura je souhrn významných rozhodnutí ohledně organizace softwarového systému, výběr strukturních prvků a jejich rozhraní, ze kterých je systém složen, společně s jejich chováním určeným spoluprací těchto prvků, skládání těchto (…) prvků do větších podsystémů a architektonický styl, který tuto organizaci provází – tyto prvky, jejich rozhraní, spolupráce a kompozice.“ [21]
- Architektura softwaru je „fundamentální organizace systému ztělesněného v jeho komponentech, jejich vztahy vůči sobě navzájem a ke svému okolí a principy provázející uspořádání a vývoj“. [22]

Pro účely této bakalářské práce budeme architekturu softwaru chápat jako souhrn prvků systému, jejich vazby na ostatní prvky a okolí (včetně datových toků, které na těchto vazbách probíhají) a pravidla fungování tohoto systému.

Při návrhu architektury softwaru budeme postupovat „shora dolů“, tedy nejdříve bude vytvořen celkový model architektury softwarového nástroje, který však bude obecný, a dále se jednotlivé prvky budou konkretizovat, až vznikne konečná podoba architektury. Z nejobecnějšího hlediska lze architekturu daného nástroje rozdělit do tří částí: vstupní, procesní a výstupní (viz Obr. 6). Do vstupní části budou spadat všechny takové prvky, jež budou následujícím částem systému poskytovat data či informace dodané uživatelem. V procesní části softwaru dojde k jejich zpracování podle zásad modelu STAMP, respektive analýzy Active STPA, a to tak, že jednotlivé prvky (části Active STPA) budou spolupracovat s uživatelem, budou mu klást otázky a získávat od něj odezvu. Výstupní část nakonec poskytne uživateli vyhodnocení procesu – v prvé řadě aktualizaci STPA, dále nová opatření zaznamenaná do SMS a také průvodní zprávu.



Obr. 6: Obecná architektura softwaru [vlastní tvorba]

Obecně byla tedy architektura softwaru navržena. V dalším kroku dojde ke specifikaci jednotlivých prvků systému, zejména prostřední, procesní části. Tato část bude velmi úzce navazovat na disertační práci zabývající se analýzou Active STPA, kde jsou rozepsané jednotlivé kroky, co se v nich zjišťuje (tzn. co potřebujeme získat od uživatele, respektive od vstupních prvků) a jaký je jejich výstup.

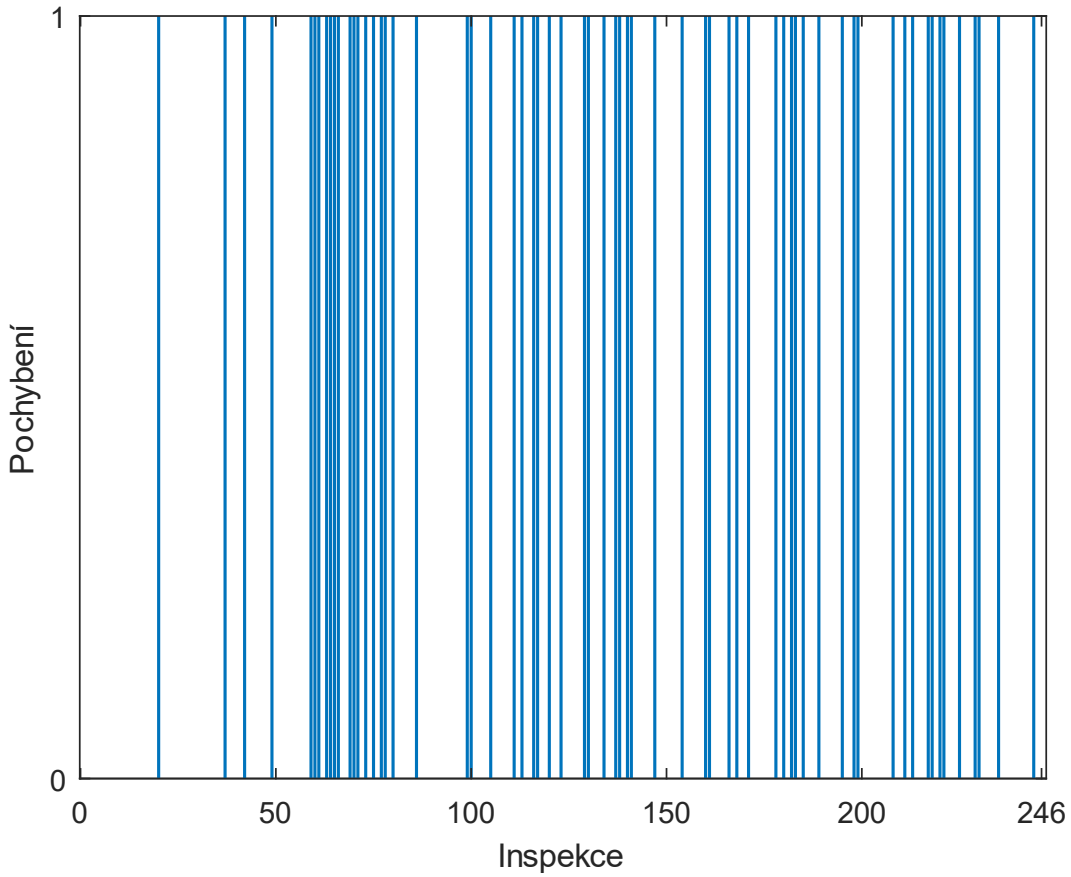
7.1 Spuštění analýzy

Jelikož se tato bakalářská práce zabývá možností integrace studií bezpečnosti s provozními daty, je důležité na tomto místě rozhodnout, co povede ke spuštění samotné analýzy Active STPA. Jak bylo naznačeno na obecném návrhu architektury (Obr. 6), na vstupu figurují provozní data. To je však celkem široký pojem. Za data z provozu můžeme považovat nejen údaje zaznamenané v rámci automatického měření, nýbrž i incidenty, závěry inspekcí či informace poskytnuté systémem povinného a dobrovolného hlášení. V případě „lidských" dat, jako jsou inspekce nebo hlášení, může být analýza spuštěna už při zjištění nedostatků. Zejména v části automatického měření dat však potřebujeme stanovit metodu, která by poukázala na trend v oblasti provozní bezpečnosti.

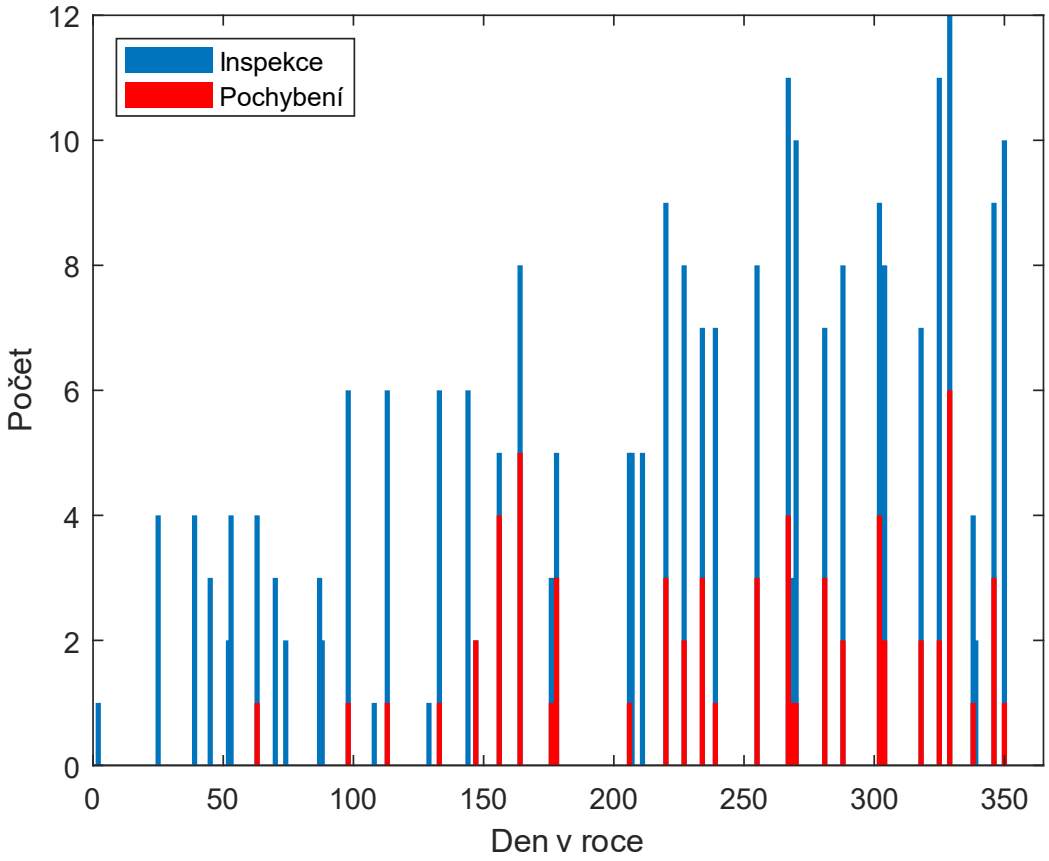
Zřejmě nejjednodušší metoda je sledování průměru či mediánu určité hodnoty. Může se jednat například o rychlost letadel na přistání, rychlost opouštění dráhy, počet letadel využívajících danou odbočku a další. Pokud nastane v těchto datech změna, kupříkladu se zvýší průměrná rychlost opouštění dráhy, může se jednat o určitý trend v oblasti provozní bezpečnosti, který indikuje, že v systému došlo k nějaké změně. Možné je také průměr s mediánem porovnávat.

Další možností, jak rychle analyzovat bezpečností data, je sledování odchylek od průměru či mediánu. Bezpečnostní analytik může nastavit procentuální hranici odchylky, při jejímž překročení bude na tuto skutečnost upozorněn. Systémovým řešením je sledování směrodatné odchylky. Taková analýza nám říká, jak moc se od sebe jednotlivé hodnoty v souboru dat liší. Pokud směrodatná odchylka vzroste, bude to znak, že přiblížení každého letadla se od sebe začíná více a více lišit, což může, podobně jako u předchozího příkladu, ukazovat na změny v systému.

Oddělení řízení kvality, safety a procesů společnosti Letiště Praha, a. s. laskavě poskytlo data z inspekcí pozemního odbavení za rok 2019. Z důvodu jejich anonymizace však na přání poskytovatele dat není tento zdroj uveden v seznamu referencí. Zde je alespoň vhodné zmínit, že jeho data využívají i následující grafy. Pro tuto bakalářskou práci jsou důležité závěry ze sledování pohybu pásových dopravníků. Bezpečnostní inspektoři se zaměřují na dodržování předpisů a správné provádění jednotlivých úkonů. Při porušení pravidel pohybu pásového dopravníku kolem letadla je toto pochybení zaznamenáno (viz Obr. 7). Inspekce poté byly softwarově pomocí kontingenčních tabulek sdruženy po jednotlivých dnech. Výsledek lze vidět na Obr. 8, kde na ose x jsou znázorněny jednotlivé dny v roce a na ose y počet inspekcí (modře) a počet nalezených pochybení (červeně). Zřetelně je tak vidět poměr mezi těmito dvěma sledovanými údaji, což bude přesněji znázorněno na dalších grafech.

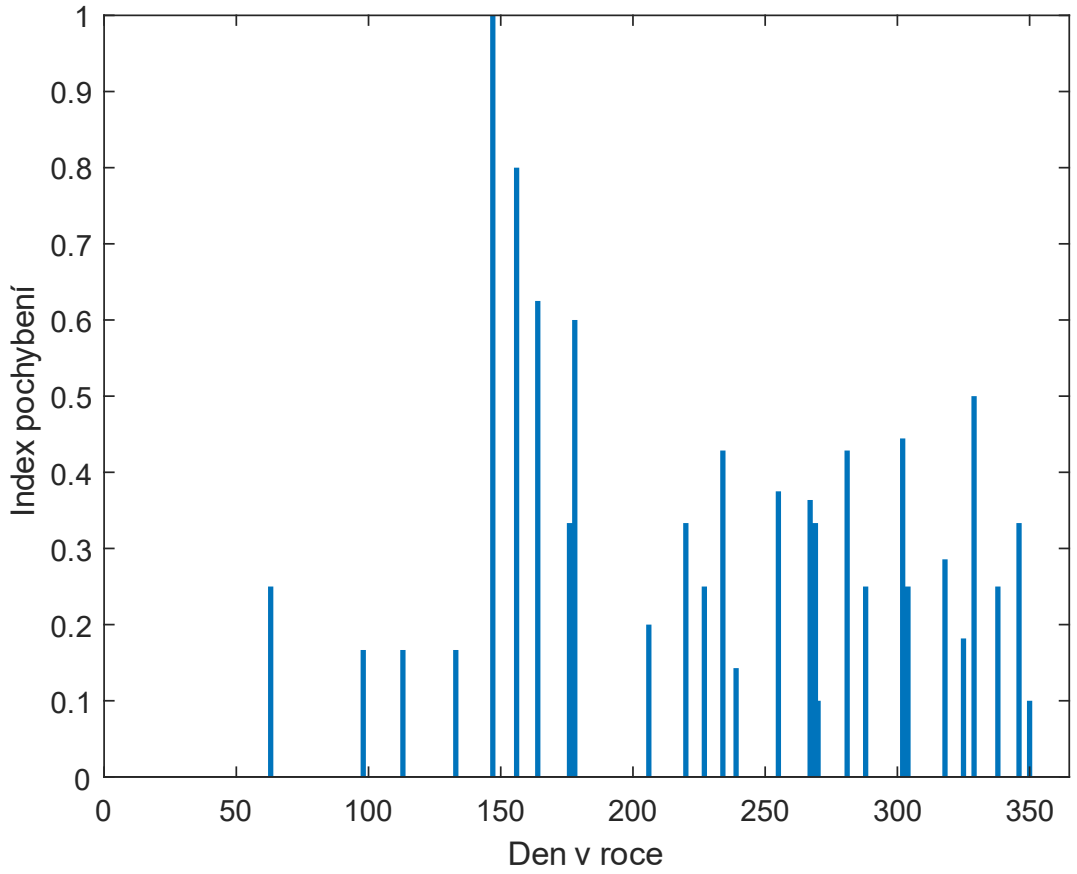


Obr. 7: Pochybení nalezená při jednotlivých inspekcích [podle dat z inspekcí]



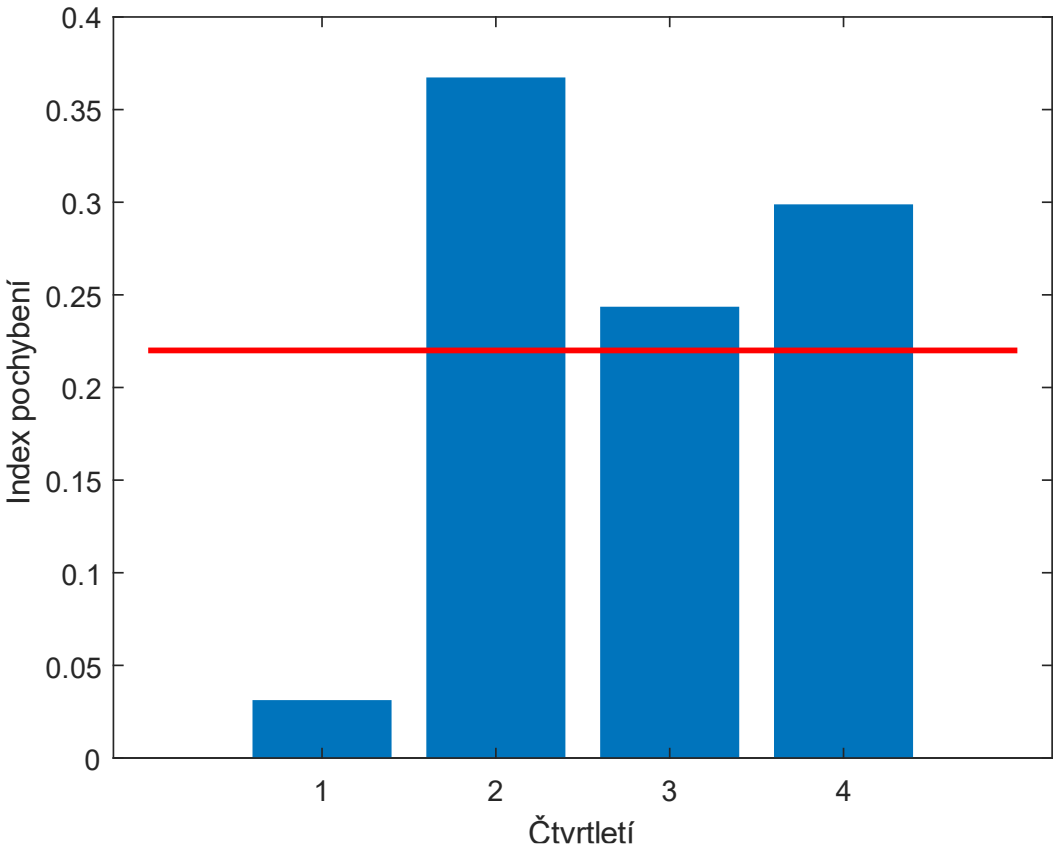
Obr. 8: Počty inspekcí (modře) a pochybení (červeně) za jednotlivé dny v roce [podle dat z inspekcí]

Jak je znázorněno v grafu na Obr. 8, v jeden den může být provedeno i více inspekcí, a proto je důležité nedívat se pouze na počty nalezených porušení, nýbrž na jejich relativní vyjádření. To získáme tak, že počet inspekcí, které nalezly pochybení, vydělíme celkovým počtem inspekcí za daný den (viz Obr. 9). Je však důležité mít na paměti, že v některé dny inspekce vůbec neprobíhaly. Tento graf by tedy měl sloužit pouze jako doplněk k předchozímu (Obr. 8).



Obr. 9: Relativní vyjádření pochybení [podle dat z inspekcí]

Zavádějící by také bylo dívat se na data pouze z jednoho dne. Důležitý je celkový trend dat. Nejčastěji letiště sleduje data za dvanáct předchozích měsíců či od začátku kalendářního roku. Pro co nejvyšší kompatibilitu se stávajícím systémem řízení provozní bezpečnosti na ruzyňském letišti a uživatelskou přívětivost je navrženo sledovat průměrnou hodnotu relativního počtu pochybení za předešlých dvanáct měsíců a při překročení stanovené hodnoty spustit analýzu Active STPA. Je však doporučeno vyhodnocení provádět častěji, a to jednou za půl nebo čtvrt roku (viz Obr. 10). Vzhledem k tomu, že v jeden den může být provedeno více inspekcí, jedná se o vážený průměr, kde váhu představuje počet provedených inspekcí. Tuto hodnotu lze spočítat tak, že počet inspekcí za dané období, které nalezly pochybení, vydělíme celkovým počtem inspekcí za dané období. Na Obr. 10 je vidět i jedna z možných hraničních hodnot pro spuštění analýzy, a sice 0,22. Ta byla stanovena jako vážený průměr ze sady dat, z níž bylo odstraněno pět dní s nejvyšším indexem (20 inspekcí) a sedm dní s nejnižším indexem (21 inspekcí). Tento průměr (0,228) pak byl zaokrouhlen dolů na setiny.



Obr. 10: Index pochybení za jednotlivá čtvrtletí s možnou hraniční hodnotou [podle dat z inspekcí]

Jak je z grafu vidět, již ve druhém čtvrtletí by podle této hranice měla být analýza spuštěna. Kromě prvního čtvrtletí všechna ostatní překročila danou hodnotu. Na tento datový trend z roku 2019 bezprostředně navazuje incident v kapitole 8 z ledna roku 2020. Je zde tedy vidět, že zvýšená míra porušených předpisů, které byly nalezeny v rámci inspekcí, svědčí o chybném stavu systému, jenž nahrává nechtěným událostem v provozu. Ideálně by měla být hranice určena z dat za předešlý rok a stanovena uživatelem podle metod letiště.

Pro systémovější přístup by bylo nutné použít data z více roků a sledovat ještě dlouhodobější trend, protože data z jednoho roku nemusejí nutně vypovídat o stavu systému (srov. pandemie koronaviru v roce 2020). Po každém roce by pak bylo záhodno stanovovat novou hranici spuštění analýzy, která by se v souladu se zvyšující se úrovní bezpečnosti měla snižovat. Také je doporučeno provádět inspekce častěji a ve větším počtu, aby byl pro počty pohybů na letišti (např. 154 777 za rok 2019) zajištěn dostatečný reprezentativní vzorek. [23]

Z důvodu vysoké různorodosti provozních dat sbíraných na letišti není možné spolehlivě určit, že bude tato metoda určení hranice spuštění analýzy Active STPA vyhovovat i dalším kategoriím. Každopádně je doporučeno, aby letiště pro spuštění analýzy používalo indikátory, s nimiž má již zkušenosti, tj. například počet nepovolených vjezdů na dráhu přepočítaný na celkový počet pohybů na letišti.

7.2 Krok 1.1: Hledání aplikovatelných pravidel a postupů

V této části začíná samotná architektura softwaru (pokud nepočítáme vstupní parametry). Kromě této popisné části je pro lepší představivost k dispozici ještě přehled navržené architektury softwaru, a sice v přílohách 1–3. Kroky od 1.1 do 1.7 lze nalézt v příloze 1, druhá část se nachází v příloze 2 a závěrečná v příloze 3.

Do architektury softwaru nejdříve vstupuje z analýzy STPA množina uplatňovaných postupů. Uživatel označí postupy, které se účastnily incidentu. Zároveň bude mít možnost:

1) označit neúčinné postupy,
2) doplnit postupy, které v původní analýze STPA chyběly.

V prvním případě systém uživatele povede na řešení problému nefunkčních postupů. Analýza Active STPA nabízí dva druhy řešení, a to upravení pravidel nebo prosazování obran. Aby systém mohl vyhodnotit, jak má v daném případě postupovat a co zlepšit, bude uživatel muset vybrat důvod proti použití obranných opatření. Disertační práce jich nabízí pět, jmenovitě (i s doporučenými opatřeními):

1) obrana je příliš nákladná (prioritizovat zvýšení úrovně obrany),
2) nebyl čas na implementaci všech obran (prioritizovat zvýšení úrovně obrany),
3) doporučená obrana není proveditelná (revize postupů),
4) obrana koliduje s existujícím postupem (revize postupů),
5) výsledky analýzy nebyly komunikovány správným subjektům (zlepšit komunikaci v rámci SMS). [9]

Pokud bude uživatel přidávat nové postupy, informace o nich dále poputuje do kroku 3.5, kde dojde k aktualizaci analýzy STPA. Pakliže mu systém doporučí zavedení obranných mechanismů, bude tato informace uživateli k dispozici v kroku 3.1, kdy se právě obrany navrhují.

V druhém případě, kdy postupy v analýze STPA úplně chyběly, bude uživatel tyto postupy doplňovat. Zároveň zvolí důvod, proč chyběly:

1) analýza STPA nebyla kompletní,
2) systém se od poslední analýzy STPA změnil. [9]

Informace o chybějících postupech se softwarovým nástrojem dostane do části 3.5, kde dojde k aktualizaci analýzy STPA.

7.3 Krok 1.2: Ověření požadavků a omezení

Do této fáze vstupuje z původní analýzy STPA množina všech omezení (řídicích prvků). Uživatel nejdříve označí omezení, která měla zabránit nebezpečí a následně bude moci (podobně jako u předchozího kroku):

1) doplnit chybějící omezení,
2) označit neúčinná omezení.

Pokud budou chybět omezení, uživatel je přidá a vybere jeden z důvodů, proč nebyla původní analýza STPA kompletní:

1) nedostatek času na provedení STPA,
2) omezené informace o systému,
3) nedostatečné zkušenosti bezpečnostního analytika,
4) účelové vytvoření analýzy pouze pro splnění požadavků,
5) přílišná komplexnost systému,
6) nedostatečné zohlednění vazeb s okolím. [9]

Nová omezení se dostanou datovým tokem do části 3.5, kde dojde k jejich přidání do knihovny STPA, a tak k aktualizaci samotné analýzy.

Pro případ neúčinných omezení má uživatel následující možnosti:

1) systém je zatížen provozní odchylkou (je vyžadováno důslednější prosazování postupů nebo vytvoření nových omezení),
2) model řídicího procesu již není platný,
3) do procesu vstupuje zpoždění,
4) předpoklady systému již nejsou platné. [9]

V případě, že v reálném provozu nejsou dodržovány postupy nebo je záhodno vytvořit nová omezení (provozní pravidla), je nutné tuto skutečnost promítnout do systému SMS. V obou případech je nutné dbát na bezkonfliktnost opatření. Pokud nejsou již platné systémové předpoklady, uživatel dostane tuto informaci v části architektury, která se jimi zabývá (2.1). Jelikož se ve třetí části přidávají obrany, které mají prosazovat omezení přidaná analýzou STPA, dodá se do kroku 3.1 informace o vybraných omezeních. Když uživatel v této fázi provede nějaké změny v modelu systému nebo pravidlech jeho fungování, informace se samozřejmě automaticky dostanou do aktualizačního kroku (3.5).

7.4 Krok 1.3: Ověření kauzálních scénářů

V této fázi architektura softwaru zjišťuje, jak dochází k nebezpečné řídicí akci. Kauzální scénáře, které byly identifikovány původní analýzou STPA jsou porovnávány s nastalým scénářem vedoucím k incidentu. Pokud některé kauzální scénáře chybějí, je nutné před přesunem k dalšímu kroku zjistit důvody, proč tyto scénáře v analýze STPA chyběly.

Jak již bylo uvedeno v popisu analýzy Active STPA, disertační práce zmiňuje, že bezpečnostní analytik má v této části obtížný úkol s nutností činit jisté kompromisy. Abychom v rámci analýzy dosáhli specifičtějších, a tudíž efektivnějších omezení, musíme scénáře co nejvíce konkretizovat. Na druhou stranu však konkrétnějších scénářů bude logicky daleko více, a existuje tedy vyšší šance, že se na některý zapomene. [9]

Důvody pro absenci kauzálních scénářů v původní analýze STPA mohou být stejné jako u omezení. Jedná se o důvody, proč nebyla analýza kompletní, konkrétně:

1) nedostatek času na provedení STPA,
2) omezené informace o systému,
3) nedostatečné zkušenosti bezpečnostního analytika,
4) účelové vytvoření analýzy pouze pro splnění požadavků,
5) přílišná komplexnost systému,
6) nedostatečné zohlednění vazeb s okolím. [9]

Studium kauzálních scénářů bude pokračovat v dalším kroku, kde bude nápomocno při zkoumání řídicích akcí a nebezpečných řídicích akcí.

7.5 Krok 1.4: Ověření řídicích akcí a nebezpečných řídicích akcí

Nyní uživatel zvolí, zda řídicí akce, která se účastnila incidentu, koresponduje s některou nebezpečnou řídicí akcí z původní analýzy STPA. Pokud ne, je uživatelem přidána a ten zároveň označí kategorii nebezpečné řídicí akce podle rozdělení uvedeného v příručce STPA:

1) nevykonání řídicí akce způsobuje nebezpečí,
2) vykonání řídicí akce způsobuje nebezpečí,
3) řídicí akce byla vykonána brzy, pozdě nebo ve špatném pořadí,
4) kontinuální akce trvala příliš krátce nebo příliš dlouze. [11]

Na řídicí akce existují dva pohledy. První je takový, že všechny, které mají týž výsledek, považujeme za jednu. Takovým způsobem pak můžeme v další části analýzy lépe najít omezení na systémové úrovni. Pokud však chceme sestavit omezení na nižší systémové úrovni a zapracovat je do dokumentů taktéž nižší úrovně, musejí se nebezpečné řídicí akce konkretizovat. [9]

Nebezpečné řídicí akce z tohoto kroku budou přecházet do dalších kroků, kde pomohou najít další řídicí akce na jiných úrovních a stanovit omezení na systémové úrovni. Pokud zároveň uživatel najde novou nebezpečnou řídicí akci a kategorizuje ji, bude o ni automaticky ve fázi 3.5 obohacena knihovna analýzy STPA.

7.6 Krok 1.5: Ověření řídicích vztahů ve struktuře řízení bezpečnosti

V tomto kroku uživatel prověří nebezpečné řídicí akce z hlediska řízení bezpečnosti na vyšších hierarchických úrovních. Pokud totiž systém dovolil vzniknout události, jedná se o chybu prvků řízení na hierarchicky vyšších úrovních, které omezeními měly zajistit bezpečné a efektivní fungování systému. Zároveň chyby, které vyvstávají na nižších hierarchických úrovních, jsou ovlivněny řídicími akcemi hierarchicky vyšších prvků nebo nedostatečnou spoluprací prvků na stejné úrovni. [9]

Uživatel se v této části tedy zaměří na okolí již objevené nebezpečné řídicí akce a identifikuje všechny prvky, které pracovaly správně, respektive vybere ty, které se na nebezpečné řídicí akci z minulého kroky podílely. Tím také zvolí hierarchickou úroveň vzniku nebezpečné řídicí akce. Poté se uživatel zaměří na zodpovědnosti jednotlivých řídicích prvků a zjistí, jestli se od poslední analýzy STPA nezměnily. Pokud ano, je nutné prověřit jejich dopad na celý systém.

Nebezpečné řídicí akce na různých hierarchických úrovních pomohou v předposledním kroku první části analýzy Active STPA revidovat omezení na systémové úrovni, respektive stanovit nová omezení. Pokud také uživatel najde v tomto místě další nebezpečné řídicí akce, vazby v architektuře předají tuto informaci na konec analýzy, kde dochází k její aktualizaci. V případě že je z hlediska řídicích prvků nutné nebo žádoucí aktualizovat zodpovědnosti jednotlivých prvků v oblasti SMS, uživatel tak provede pomocí vazby z této úrovně do SMS.

7.7 Krok 1.6: Ověření požadavků a omezení na systémové úrovni

Následuje krok, ve kterém uživatel zhodnotí systémová omezení, jejich funkčnost, porušení a navržení nových. Do této fáze analýzy Active STPA budou vstupovat všechna systémová omezení, která byla v rámci systému identifikována původní analýzou STPA. S vyhodnocením problematiky systémových omezení budou uživateli pomáhat výstupy z předchozích částí analýzy, zejména se jedná o nebezpečné řídicí akce, jejich kategorizaci a zařazení do hierarchie systému. Na tyto nebezpečné řídicí akce musejí bezprostředně reagovat omezení na systémové úrovni, která jim mají zabránit. Přidaná systémová omezení poputují do fáze 3.5, a aktualizují tak knihovnu analýzy STPA.

7.8 Krok 1.7: Ověření nebezpečí a ztrát

Úkolem uživatele v tomto kroku je znovu projít nebezpečí a ztráty, které jsou součástí systému z původní analýzy STPA. Pomocí znalosti z předchozích kroků (nebezpečné řídicí akce) uživatel zhodnotí, jestli je seznam nebezpečí a ztrát kompletní, nebo jestli je nutné nějaké položky přidat. Pokud ano, je informace o nich předána aktualizační fázi 3.5, která má za úkol aktualizovat knihovnu analýzy STPA. Tím je první část analýzy Active STPA ukončena. Informace o nových nebezpečích a ztrátách budou využívány v části 2.5, v níž uživatel přidává nouzová opatření. Taktéž se datovou vazbou dostanou do fáze 3.1, kde pomohou vytvořit seznam možných obran.

7.9 Krok 2.1: Nalezení porušených předpokladů

Uživatel se v tomto kroku dostává do důležité fáze, kdy z předpokladů, které uživatel přidal v rámci původní analýzy STPA, vybírá ty porušené. Porušení či porušování předpokladů je známka určité změny v systému, kterou se uživatel snaží odhalit a podchytit. Kromě označení porušených předpokladů se v tomto kroku přidávají i chybějící předpoklady na systém. Zde uživatel také zvolí, jestli jsou předpoklady porušovány opakovaně. To by totiž byla známka toho, že tyto předpoklady nejsou správné nebo zavedená opatření nejsou účinná. Poznatky z této fáze budou uživateli ještě nápomocny při určování důvodu porušení předpokladů.

7.10 Krok 2.2: Analýza trendů

Softwarový nástroj bude v této fázi instruovat uživatele, aby zanalyzoval data o bezpečnosti z leteckého provozu. V případě, že se události bude týkat více souborů dat, projde uživatel všechna taková data, která by mohla podat zprávu o trendu v oblasti provozní bezpečnosti. Uživatel poté zvolí, jestli data trend vykazují. Pokud ano, popíše, o jaký trend se jedná (kategorizace) a zvolí, jakým směrem se ubírá (klasifikace): zda jde o setrvalý trend, roste či klesá. Podobně jako u předchozího kroku budou i zde znalosti použity při určování důvodu porušení předpokladů.

7.11 Krok 2.3: Výzkum kauzálních a přispívajících faktorů

K nehodě či incidentu zřídkakdy vede pouze jeden chybný krok. V oblasti mezinárodního civilního letectví je událost většinou souhra několika přispívajících faktorů. Tyto faktory zde uživatel vyjmenuje a zároveň ohodnotí jejich závažnosti pro proběhnuvší incident či událost, které by se eventuálně mohly stát i za jiných podmínek. Hodnocení kauzálních a přispívajících faktorů bude provedeno na škále 1–5, kde 1 znamená nejnižší závažnost a 5 nejvyšší, podobně jako je tomu u hodnocení závažnosti rizik v Tab. 2. I zde budou závěry ohledně faktorů použity pro vyhodnocení porušení předpokladů.

7.12 Krok 2.4: Určení důvodu porušení předpokladů

Na tomto místě, kdy má uživatel za sebou kroky týkající se porušených předpokladů, analýzy provozních dat a výskytu trendů a nakonec i zhodnocení závažnosti kauzálních a přispívajících faktorů, je načase rozhodnout, zda tyto všechny indicie vedou na chybný předpoklad, nebo se opravdu jen jedná o ojedinělou událost, které není třeba věnovat přílišnou pozornost. S tím mu mohou pomoci i poznatky z předchozího kroku architektury, konkrétně fáze 1.2, kde uživatel vybíral důvod neúčinných omezení a kde jeden z důvodů byl, že předpoklady systému již nejsou platné. Pokud uživatel rozhodne, že předpoklady na systém jsou opravdu chybné, lze očekávat, že bude chtít nastavit nové, platné předpoklady. Zároveň přidá důvod, proč byl původní předpoklad porušen:

1) předpoklad byl od začátku chybný,
2) předpoklad platil pouze pro specifické situace,
3) systém se od stanovení původního předpokladu změnil.

7.13 Krok 2.5: Zjištění funkčnosti nouzových opatření

V poslední fázi druhého kroku uživatel posuzuje, zda existovala nouzová opatření, která měla zabránit ztrátám nebo je alespoň zmírnit. V tom mu pomáhají poznatky z fáze 1.7, v níž došlo k aktualizaci seznamu možných ztrát. V případě, že taková opatření existovala, uživatel zvolí, jestli byla účinná. Pakliže se zjistí, že účinná nebyla, je nutné vypátrat, proč opatření, která byla za tímto účelem zavedena, selhala. Uživatel zvolí jednu z následujících možností:

1) nouzová opatření nezareagovala,
2) nouzová opatření byla slabá vzhledem k intenzitě události,
3) nouzová opatření neměla správný účinek.

Uživatel také bude moci přidat nová, funkční opatření. V případě, že pro oblast problému zatím neexistují žádná nouzová opatření, je záhodno, aby je uživatel přidal. Je ale také možné, že je z nějakého důvodu nelze zavést. Pak musí uživatel přidat komentář ohledně toho, proč tato opatření nemohou být implementována do provozu. Konkrétně se může jednat o následující možnosti:

1) nouzová opatření jsou příliš nákladná,
2) nouzová opatření jsou v konfliktu s jinými prvky systému,
3) neexistují nebo nejsou k dispozici nouzová opatření, která by byla v dané situaci použitelná.

7.14 Krok 3.1: Vytvoření seznamu možných obran

Úkolem úplně prvního kroku analýzy Active STPA bylo získat od uživatele zpětnou vazbu ohledně postupů v systému. Uživatel také volil, proč nebyly použity obrany nebo se o nich neuvažuje do budoucna. Z tohoto kroku (1.1) povede tok dat právě sem, protože zde uživatel bude přidávat nové obranné mechanismy. Uživatel zde také využije znalosti z fáze 1.7, v níž přidal nová nebezpečí. V prvé řadě budou navrženy jednotlivé obranné mechanismy. V tomto místě je také uživatel rozdělí podle náročnosti následovně: ke každé položce přidá ohodnocení náročnosti zavedení na škále 1–5, přičemž čím vyšší číslo, tím vyšší je náročnost zavedení takové obrany. Proces bude přirozeně pokračovat v další fázi.

7.15 Krok 3.2: Analýza kompromisů

Z minulého kroku má již uživatel předpřipravenou množinu možných obran. V nynější fázi ke každé položce přidá několik kladů a záporů souvisejících se zavedením daného opatření. To mu v dalších fázích pomůže s rozhodováním o zavedení obran. Dalším parametrem, který bude k jednotlivým obranám přiřazovat, je vliv na systém. Ačkoliv je možné, že zavedená obrana nebude mít nejmenší vliv na ostatní prvky, může se stát také opak. V tom případě je nutné detailně zdokumentovat, co se musí v systému změnit, aby obrana byla systémem a společností přijata, a jak zabránit rozvinutí případných negativ jednotlivých obran.

7.16 Krok 3.3: Určení optimálního řešení

Uživatel se nyní nachází ve fázi, kdy již poměrně detailně zanalyzoval zavedení potenciálních obran do systému. Nyní důkladně zhodnotí všechna předpokládaná negativa a pozitiva a dopady na systém a rozhodne o tom, která obrana bude do systému vložena. Může jich být samozřejmě i více, je však nutné dbát na to, aby nebyly v konfliktu s již stávající architekturou systému ani spolu navzájem. Po schválení určité obrany přichází také na řadu shrnutí nutných změn v SMS. Tyto dva pilíře se posouvají do dalšího kroku, kde dojde k jejich implementaci.

7.17 Krok 3.4: Zavedení nových obran a ochran

Nyní se analýza Active STPA přesouvá do provozní oblasti. Systém obranných opatření, která uživatel navrhl výše, je připraven k použití. Protože je však letectví vysoce kritickou oblastí, je nutné před ostrým zavedením do provozu tyto obrany řádně a důkladně vyzkoušet. Zkoumá se, jestli opatření nemají na systém nežádoucí vliv, a v druhé řadě se sleduje, zda opatření splňují svůj účel a pomáhají zvyšování provozní bezpečnosti. Pokud se v této fázi nevyskytne žádná chyba, aktualizuje se dokumentace společnosti a prosadí se změny. Na zavedení nových opatření se přitom musí dát veliký důraz. Nestačí jen publikovat nové manuály a oběžníky oznámit zaměstnancům, že došlo ke změně. Je nutné seznámit je s nimi, naučit je v souladu s nimi pracovat, poučit je o důležitosti daného opatření a v konečném důsledku také vyžadovat dodržování platných pravidel. To však neplatí jen pro tento krok. K jakýmkoliv změnám, které jsou provedeny v rámci tohoto nástroje a zavádí se do SMS, musí být přistupováno s touž důsledností. Ani po zavedení změn ale tato fáze nekončí. Změny v systému musejí být pod drobnohledem, musejí být podrobeny neustálému pozorování a vyhodnocování jejich účinnosti a vlivu na systém.

7.18 Krok 3.5: Aktualizace STPA

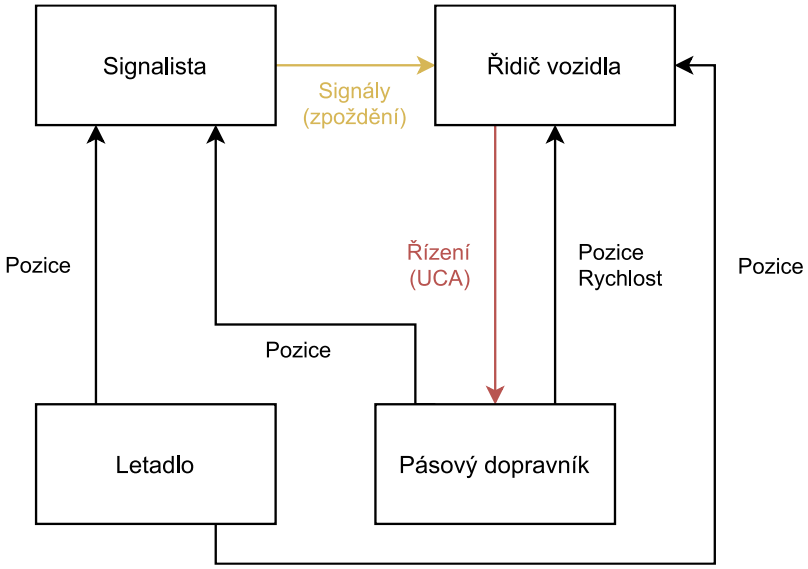
Poslední krok finalizuje analýzu Active STPA přidáním všech nových skutečností, které se během provádění uživatele softwarovým prostředím vyskytly. Mohou to být změny v systému, jež nebyly zaznamenány nebo zcela nová pravidla pro fungování systému, nová bezpečnostní opatření, postupy atd. Již během procesu uživatel přidal do SMS a STPA nové skutečnosti. V této fázi dojde k rekapitulaci práce bezpečnostního analytika. Nástroj by na konci měl uživatele znovu upozornit na změny, které byly v systému provedeny. Tímto dvojitým ověřením se sníží pravděpodobnost zavedení nechtěného nebo nesprávného opatření.

7.19 Výstup

Podle obecného návrhu architektury softwaru (kapitola 7) z procesní fáze vystupuje množina opatření, soubor pro aktualizaci knihovny STPA a závěrečná zpráva. Opatřením a aktualizaci byla věnována pozornost již v posledním kroku návrhu architektury (tj. 3.5), nyní zbývá jen v krátkosti popsat závěrečnou zprávu. Bude možné vytisknout jak kompletní, tak zkrácenou verzi. Jak již názvy napovídají, budou se lišit v úrovni podrobnosti zobrazovaných informací. Úplná zpráva bude obsahovat veškerou aktivitu uživatele, zkrácená pouze informace potřebné pro oddělení řízení kvality, safety a procesů a nutné pro závěrečnou zprávu k incidentu.

8 PŘÍKLAD

Během pozemního odbavení letounu došlo ke kontaktu pásového dopravníku a vstupního hrdla motoru. Řidič pásového dopravníku nejprve posunul kužely pro označení minimální vzdálenosti od letadla až pod okraj vstupního hrdla motoru. Po skončení nakládky zavazadel začal vyjíždět směrem od letadla. Signalista byl na svém místě a pomáhal řidiči s orientací v prostoru, zejména s přehledem o tom, jaká vzdálenost je mezi letadlem a vozidlem. Řidič v domnění, že ke zvrácení kontaktu pásového dopravníku s motorem je nutný manévr, zatočil volantem prudce doprava, patrně nedbaje signálů svého kolegy. Přední část pásového dopravníku pak narazila do motoru. Řídicí smyčka incidentu je na Obr. 11. Tam je také znázorněno, že vazba mezi signalistou a řidičem vozidla podléhá významnému zpoždění, které možná hrálo roli i v tomto incidentu. Samotná nebezpečná řídicí akce neboli UCA (Unsafe Control Action) je zvýrazněna červenou barvou.



Obr. 11: Řídicí smyčka incidentu [vlastní tvorba podle závěrečné zprávy]

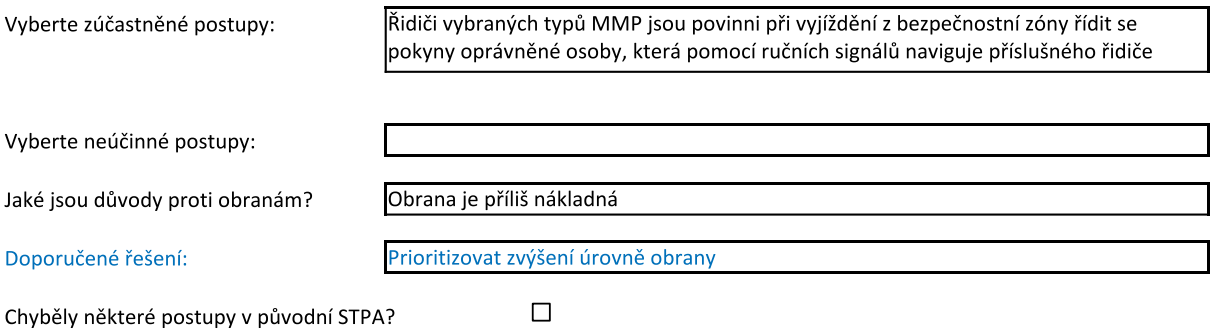
Data, která architektura softwaru používá a která jsou nezbytná pro jeho správnou funkčnost, byla importována z bakalářské práce Ondřeje Vašaty (viz zdroj [24]), která se zabývala mj. původní analýzou STPA pro procesy pozemního odbavení na ruzyňském letišti. Pro plnou funkci architektury však některé prvky chyběly, a byly tedy doplněny ručně. Tato skutečnost je uvedena v jednotlivých krocích. Pro pohodlnější práci s budoucím softwarem je doporučeno tyto chybějící knihovny údajů zavést. Pro ukázku práce softwaru, který by mohl být v budoucnosti navržen, byl použit databázový nástroj Microsoft Access.

Informace o incidentu byla poskytnuta oddělením řízení kvality, safety a procesů společnosti Letiště Praha, a. s. Ze závěrečné zprávy k incidentu byly čerpány jak samotné informace o události, tak některá data, ze kterých vybírá uživatel v rámci cesty systémem a která chyběla ve výše zmíněné bakalářské práci. Z důvodu anonymizace se nevyskytuje v seznamu zdrojů.

Na začátku uživatel podle zásad uvedených v části návrhu architektury softwaru (kapitola 7) vybere postupy, které se účastnily incidentu, respektive ty, které mu měly zabránit. Zde se jedná o součinnost řidiče a signalisty, která zaručuje bezpečnou vzdálenost vozidla od letounu. Jelikož množina postupů nebyla součástí původní analýzy STPA z bakalářské práce, byl tento konkrétní postup doplněn podle závěrečné zprávy k incidentu od oddělení řízení kvality, safety a procesů. Pro činnost budoucího softwarového nástroje se počítá se seznamem postupů. V kolonce neúčinné postupy se nic nenachází, neboť incident byl způsoben jeho nedodržením, nikoliv však jeho selháním. Zúčastněných a neúčinných postupů může být v samozřejmě více. Zde byl však pro zjednodušení vybrán jeden. Toto zjednodušení nemá vliv na práci systému v celkové rovině. Jako obranu, jež se řeší v další části, bychom mohli brát instalaci dostatečného počtu senzorů na všechna vozidla, která se pohybují v blízkosti letadel. Tento krok by však byl značně finančně náročný a v důsledku by nemusel přinést až takové zvýšení bezpečnosti, jaké by se od něj očekávalo. Z možností

1) obrana je příliš nákladná,
2) nebyl čas na implementaci všech obran,
3) doporučená obrana není proveditelná,
4) obrana koliduje s existujícím postupem,
5) výsledky analýzy nebyly komunikovány správným subjektům

byla tedy vybrána nákladnost obranných opatření. Vidíme, že nástroj radí prioritizovat řízení provozní bezpečnosti. Mohlo by se například jednat o jeden z podkladů pro zvýšení rozpočtu oddělení provozní bezpečnosti na letištích. Posledním aktivním prvkem je zde zaškrtávací políčko ohledně chybějících postupů. Pokud by některé postupy chyběly, lze je jeho označením doplnit v kolonce, která by se poté objevila. V softwarovém nástroji by taktéž byla možnost případné postupy vyjmout. Vizuální návrh je vyobrazen na Obr. 12.

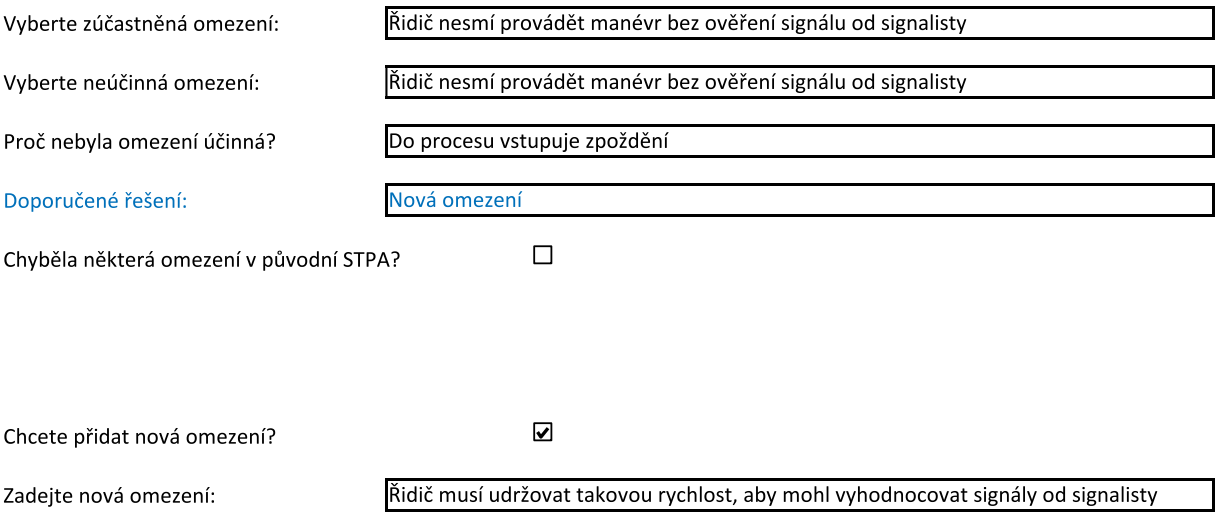


Obr. 12: Ukázka vizuální stránky softwaru – krok 1.1 [vlastní tvorba]

Dále je uživatel postaven před úkol vybrat zúčastněná omezení řídicích prvků. Zde opět nebyla k dispozici knihovna, která by tato data obsahovala, proto bylo toto omezení přidáno ručně. Pro software se však počítá s jejím zavedením a následným výběrem uživatelem. Opět jako u prvního kroku bude v reálném softwaru možnost vybrat více omezení. Zúčastněné omezení je takové, že řidič vozidla nesmí provádět manévr bez ověření signálu od signalisty. Zde nelze jednoznačně určit, zda bylo omezení neúčinné. V případě, že řidič pouze nedbal signálu od kolegy, omezení mělo incidentu zabránit. Na druhou stranu však není možné přesně určit, do jaké míry mělo na incident vliv zpoždění mezi reakcí signalisty, jeho signálem a reakcí řidiče. Proto je zde uvedena ta horší varianta, tedy že by dané omezení bylo neúčinné. V tomto případě uživatel vybírá i důvod neúčinného omezení, a to z následujících možností:

1) systém je zatížen provozní odchylkou,
2) model řídicího procesu již není platný,
3) do procesu vstupuje zpoždění,
4) předpoklady systému již nejsou platné.

Zde je důvodem, jak již bylo uvedeno výše, zpoždění, které vstupuje do systému. Nástroj v další kolonce navrhuje přidat omezení, která by již mohla incidentu zabránit. Například by se mohlo jednat o omezení rychlosti manévru vozidla, kteréžto omezení je také přidáno, jak je vidět na Obr. 13. Na začátku bylo zmíněno, že pro tato data neexistuje knihovna, z níž by uživatel mohl vybírat, nicméně se předpokládá, že zúčastněné a zároveň i neúčinné omezení je zjevné a bylo by v ní zapracované. Proto nebylo nutné zatrhávat políčko pro přidání chybějících omezení a tato omezení (řídicích prvků) přidávat, resp. měnit.

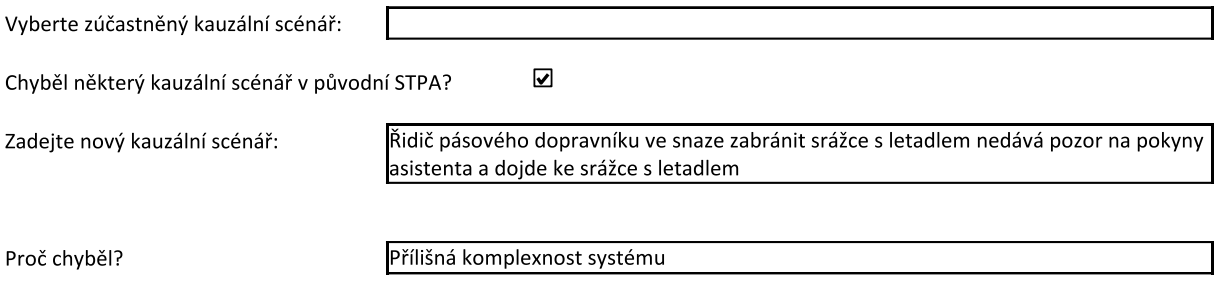


Obr. 13: Ukázka vizuální stránky softwaru – krok 1.2 [vlastní tvorba]

Práce nástroje přechází ke kauzálním scénářům (viz Obr. 14). Zde uživatel vybere kauzální scénář, který se účastnil incidentu. Jelikož takový kauzální scénář (řidič ve snaze zabránit srážce nedával pozor na pokyny signalisty a srazil se s letadlem) v knihovně nebyl uveden (součástí bakalářské práce byl pouze obdobný scénář pro zajetí k letadlu), bylo nutné jeho absenci označit a přidat jej. Také byl vybrán důvod pro jeho neuvedení v původní analýze STPA, tedy přílišná složitost systému. Na výběr bylo z těchto možností:

1) nedostatek času na provedení STPA,
2) omezené informace o systému,
3) nedostatečné zkušenosti bezpečnostního analytika,
4) účelové vytvoření analýzy pouze pro splnění požadavků,
5) přílišná komplexnost systému,
6) nedostatečné zohlednění vazeb s okolím.

Důvodů by mohlo být více, jmenovitě nedostatek času na provedení analýzy, nedostatek zkušeností, možná i účelové vytvoření analýzy. Zde, jako i do budoucna, se však počítá s výběrem jen jednoho důvodu, a sice toho, který nejvíce odpovídá skutečnosti a nejvíce přispěl k absenci kauzálního scénáře. Podobně i kauzální scénář bude možno vybrat pouze jeden. Ačkoliv není vyloženě vyloučené, že by se incidentu mohlo účastnit více nebezpečných řídicích akcí, a tedy i více scénářů, je lepší pro každý kauzální scénář vyhotovit novou analýzu Active STPA a tyto případy pak řešit odděleně, i když budou mít některé zadávané informace společné.

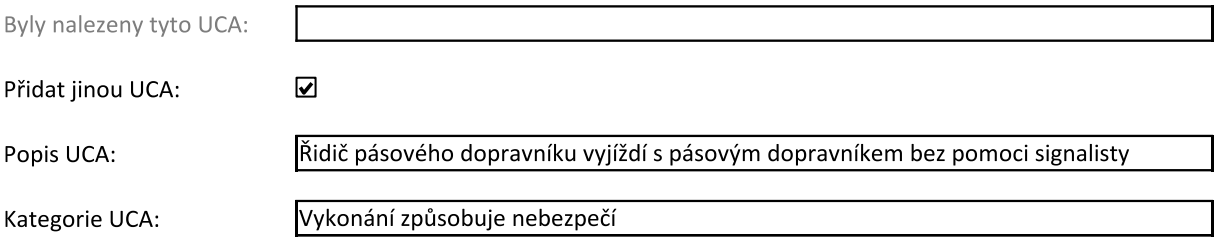


Obr. 14: Ukázka vizuální stránky softwaru – krok 1.3 [vlastní tvorba]

Pokud by daný kauzální scénář z předchozího kroku byl uveden v knihovně STPA, nyní by se zde (Obr. 15) automaticky objevila nebezpečná řídicí akce, která mu byla původně přiřazena. Jelikož byl však scénář přidán až v rámci Active STPA, je nutné přidat i nebezpečnou řídicí akci. V plné funkčnosti budoucího softwaru se tyto dvě entity spárují a přidají do knihovny. Posledním úkolem uživatele v kroku 1.4 je vybrat kategorii UCA podle příručky STPA, tedy:

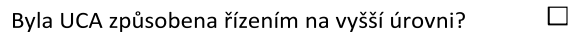
1) nevykonání řídicí akce způsobuje nebezpečí,
2) vykonání řídicí akce způsobuje nebezpečí,
3) řídicí akce byla vykonána brzy, pozdě nebo ve špatném pořadí,
4) kontinuální akce trvala příliš krátce nebo příliš dlouze.

Zde se jedná o nebezpečné vyjíždění od letadla, kategorií je tedy druhá možnost: vykonání nebezpečné řídicí akce způsobuje nebezpečí.



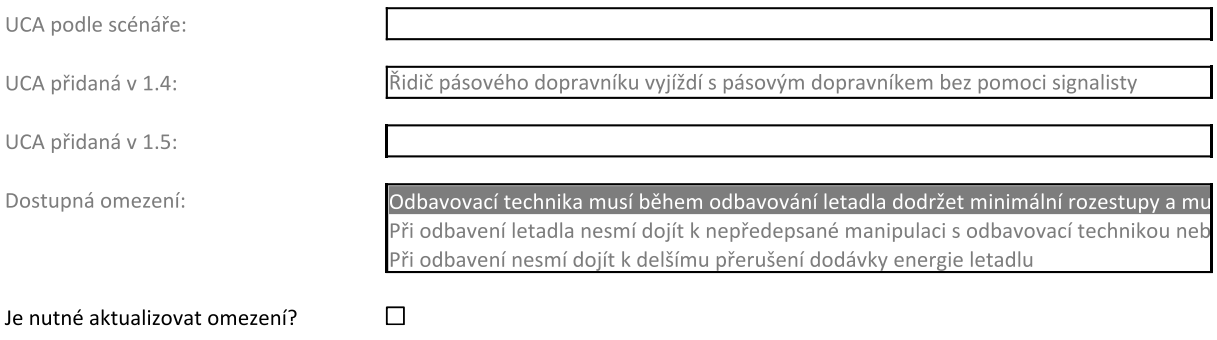
Obr. 15: Ukázka vizuální stránky softwaru – krok 1.4 [vlastní tvorba]

V další fázi je zkoumán vliv vyšších hierarchických prvků na nebezpečnou řídicí akci. V tomto incidentu však žádný prvek vyššího řízení neměl vliv na rozhodnutí řidiče pásového dopravníku. Proto ani zde (Obr. 16) není označeno zaškrtávací políčko.



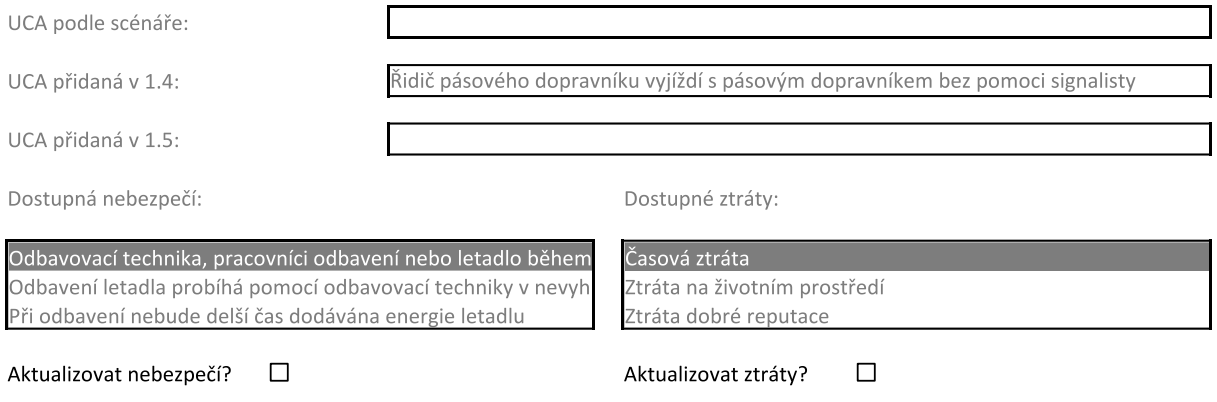
Obr. 16: Ukázka vizuální stránky softwaru – krok 1.5 [vlastní tvorba]

Fáze 1.6 hodnotí omezení na systémové úrovni, která jsou přímo odvozená z nebezpečí a nebezpečných řídicích akcí. Uživateli zde pomáhají UCA, které buď přímo, anebo nepřímo zvolil v předchozích krocích a které se automaticky přepisují do této fáze (viz Obr. 17). Jelikož byla v kroku 1.4 přidána uživatelem UCA, objevila se i zde a pomáhá s rozhodováním, zda aktualizovat nebezpečí. Dalším neaktivním prvkem je rozvinovací seznam, v němž uživatel může hledat zaznamenaná omezení na systémové úrovni. Zde se jedná o omezení „odbavovací technika musí během odbavování letadla dodržet minimální rozestupy a musí zabránit kontaktu s jinou odbavovací technikou/letadlem“. Na výběr však byla například i nutnost odbavení na čisté stojánce, dodržení časových harmonogramů nebo zajištění podélné stability letounu. Pokud by v tomto seznamu nenašel odpovídající omezení, je nutné jej přidat pomocí zaškrtávacího políčka a vyplnění pole, jež se vzápětí objeví. Součástí budoucího softwarového nástroje by pak byla i možnost systémová omezení vyjmout.



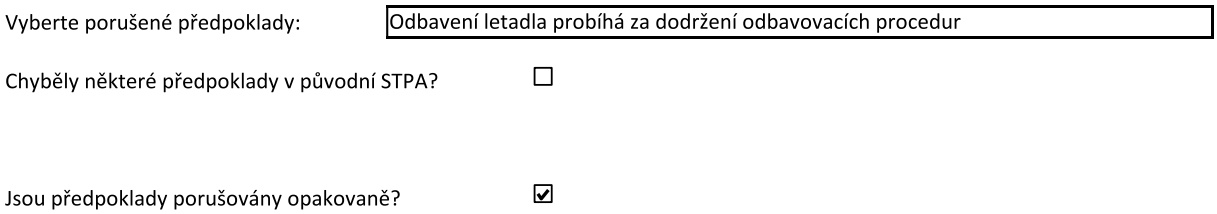
Obr. 17: Ukázka vizuální stránky softwaru – krok 1.6 [vlastní tvorba]

Na konci první části architektury softwaru založené na analýze Active STPA jsou revidovány nebezpečí a ztráty. V tom uživateli opět pomáhá výčet přímo či nepřímo vybraných nebezpečných řídicích akcí z předchozích fází (Obr. 18). Je zde také možné prohlédnout si seznam nebezpečí a ztrát, které jsou již zavedené v knihovně STPA. Tento seznam nefiguruje v softwaru jako aktivní prvek, má pouze informační funkci. Podle něj se uživatel rozhoduje, zda je nutné aktualizovat nebezpečí nebo ztráty. V tomto konkrétním případě jsou označeny ty položky seznamu, které souvisejí s incidentem a UCA. Pro úplnost je zde nebezpečím „Odbavovací technika, pracovníci odbavení nebo letadlo během odbavení překročí minimální bezpečné rozestupy vzhledem k jiné odbavovací technice/letadlu“. Jelikož v seznamech figurují nebezpečí i ztráty související s incidentem, není nutné žádné další položky těchto seznamů přidávat.



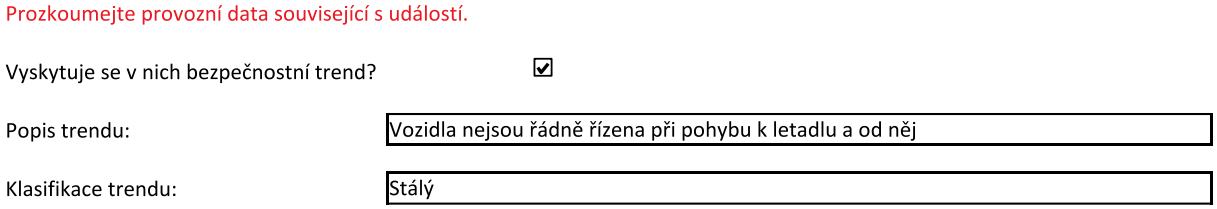
Obr. 18: Ukázka vizuální stránky softwaru – krok 1.7 [vlastní tvorba]

Druhá část systému začíná výběrem porušených předpokladů (Obr. 19), a to i více než jednoho. Ty jsou taktéž importovány z bakalářské práce uvedené výše. Zde se jedná o předpoklad dodržení procedur při odbavení, který byl očividně porušen. Pokud by některé předpoklady v knihovně STPA chyběly, je možné je pomocí zaškrtávacího políčka přidat. Na této stránce uživatel ještě označí, zda jsou předpoklady porušovány opakovaně. V tomto případě pro přehled posloužila data z inspekcí za rok 2019, kdy bylo zjištěno, že se nejedná o ojedinělou událost. Toto zjištění bude použito v dalších krocích.



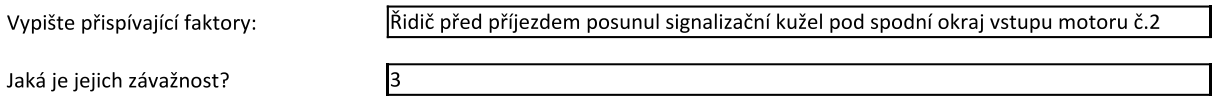
Obr. 19: Ukázka vizuální stránky softwaru – krok 2.1 [vlastní tvorba]

Nyní přichází na řadu další krok, v němž je patrná integrace klasických metod s provozními daty. Uživatel totiž dle instrukce na obrazovce (Obr. 20) bude muset prozkoumat data týkající se události. V tomto případě se jedná o závěry inspekcí v oblasti pozemního odbavení. Během řady inspekcí za rok 2019 totiž bylo zjištěno, že vozidla nejsou správně (tj. v souladu s pravidly a postupy) vedena k letadlu nebo od něj. V praxi to znamená, že signalista není na místě, ať už jde o nájezd nebo odjezd pásového dopravníku. Proto je na obrázku zatržena možnost výskytu trendu v provozních datech. O úroveň níže je také jev v krátkosti popsán a nakonec je vybrána jeho klasifikace – klesající, rostoucí či stálý. Jelikož z dat není patrný ani výrazný nárůst, ani pokles počtu inspekcí, při kterých bylo zjištěno pochybení, byla vybrána možnost „stálý“. To samo o sobě nepodává zprávu o vážnosti trendu, jen informuje, že nedochází ke zhoršování. Zde je uveden pouze jeden trend, avšak je možné, že jich s událostí bude souviset více, a proto je bude možné přidat také.



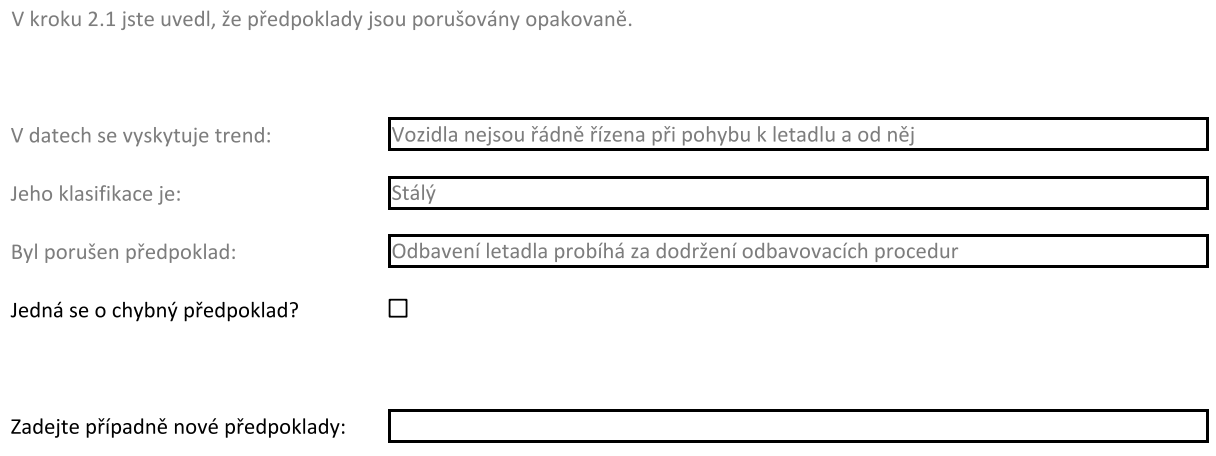
Obr. 20: Ukázka vizuální stránky softwaru – krok 2.2 [vlastní tvorba]

Dalším pilířem budoucího rozhodování o porušených předpokladech je existence přispívajících faktorů (zobrazeno na Obr. 21). Tyto přispívající faktory si můžeme představit pohledem Reasonova modelu, kdy každý svým dílem přispěl k události. Opět je myšlenkově i softwarově možné přidat více přispívajících faktorů, avšak pro jednoduchou názornost je zde uveden pouze jeden, a to přisunutí kuželů směrem pod motory. Ideálně by se kužely měly nacházet přibližně 0,5–1 m od vstupního hrdla motorů. Dalším přispívajícím faktorem by mohla být relativně malá vzdálenost mezi motory a dveřmi nákladového prostoru. Ke každému přispívajícímu faktoru uživatel přidá i jeho závažnost. Jedná se o hodnocení rizik, která by mohla vzniknout přispěním toho konkrétního faktoru. V případě posunutí kuželu pod vstup do motoru je hodnocení závažnosti na čísle tři, což na škále 1–5 značí střední závažnost. Následkem by totiž mohlo být poničení techniky nebo i zranění osob.



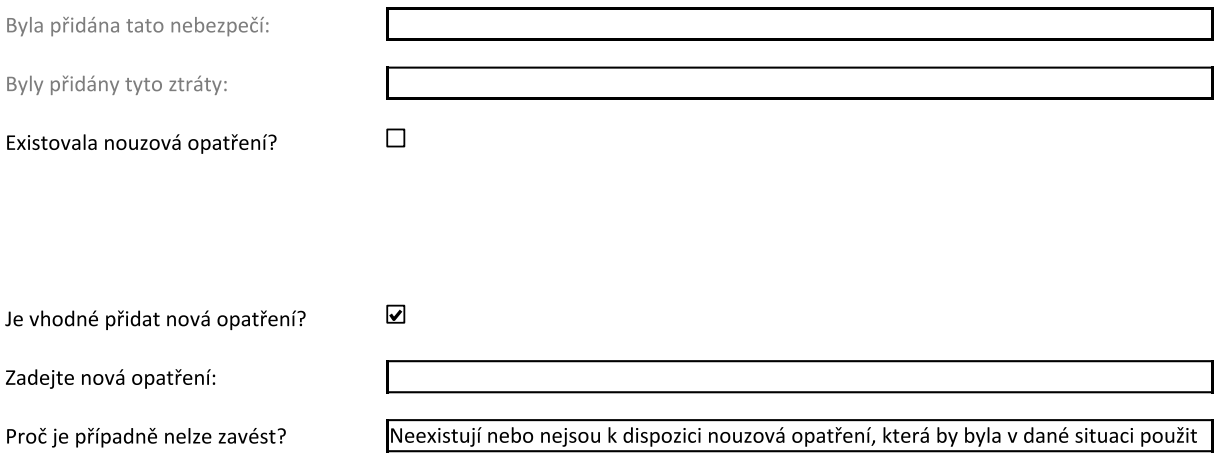
Obr. 21: Ukázka vizuální stránky softwaru – krok 2.3 [vlastní tvorba]

Nyní se plně zhodnotí poznatky z předchozích fází, kdy uživatel studoval trendy v oblasti provozních dat. Nástroj intuitivně uživateli nabízí informace (Obr. 22), které mu nyní pomohou s rozhodováním o chybných předpokladech. Hlavně se jedná o údaje z kroku 2.1 o opakovaném porušování předpokladů a údaje z předchozího kroku o trendech v bezpečnostních datech. Také se uživateli zobrazuje předpoklad, který označil za porušený. Nyní musí rozhodnout, zda se jedná o chybný předpoklad, jenž by měl být z knihovny odstraněn. To by bylo celkem závažné zjištění pro celý systém, při němž by také musel zadat, proč byl tento předpoklad chybný. V tomto případě však vidíme, že předpoklady jsou sice porušovány opakovaně, nicméně podle trendu v provozních datech je zřejmé, že letiště danou oblast sleduje a řídí ji. Nejedná se tedy o známku změny systému nebo zcela chybné předpoklady, nýbrž o setrvalý trend, který v systému způsobuje lidský faktor.



Obr. 22: Ukázka vizuální stránky softwaru – krok 2.4 [vlastní tvorba]

Z druhé části analýzy Active STPA zbyl už jen poslední krok, týkající se nouzových opatření. Nouzová opatření reagují na vzniklou událost a zabraňují jejím následkům nebo se je alespoň pokoušejí zmírnit. Jedná se například o prvky pasivní bezpečnosti v automobilech, jako jsou bezpečnostní pásy, airbagy nebo deformační zóny vozidla. Jmenovitě bezpečnostní pásy by shodou okolností v tomto případě mohly být právě nouzovými opatřeními, která by chránila zdraví a život řidiče vozidla. Toto opatření by možná nebylo až tak účinné v rámci pozemního odbavení vzhledem k nízké rychlosti pásového dopravníku, ale jelikož je cíleno na systematičnost řešení, je vhodné zvážit také možné důsledky tohoto pochybení v jiných, závažnějších souvislostech. Bylo by tedy možné jej zavést do budoucna nebo o něm alespoň v jistých oblastech začít uvažovat. Na druhé straně by bylo možné přidávat i nouzová opatření na letadle, což by například mohlo zabránit závažnějšímu poškození motorů nebo draku letounu. V současné době však „neexistují nebo nejsou k dispozici nouzová opatření, která by byla v dané situaci použitelná“ (viz Obr. 23). Dále bylo možné vybrat, že jsou nouzová opatření příliš nákladná nebo jsou v konfliktu s jinými prvky systému. Pokud by uživatel přidával nouzová opatření, bude upozorněn na nutnost zajištění jejich bezkonfliktnosti s ostatními prvky systému. Také bude nutné průběžně sledovat jejich dopad a funkčnost.



Obr. 23: Ukázka vizuální stránky softwaru – krok 2.5 [vlastní tvorba]

Na tomto místě, kdy uživatel již prošel téměř celým systémem a odhalil nedostatky v něm, je postaven před úkol přidat takové obranné mechanismy, které by prosazovaly vybraná či přidaná omezení. Na Obr. 24 jsou vidět všechny informace, jež uživateli pomáhají s vymýšlením obran. Jedná se o přidané nebezpečí a ztráty (zde konkrétně nic přidáno nebylo), doporučení ohledně prioritizace provozní bezpečnosti a zejména omezení na hladině řídicích prvků. Cílem této fáze a vůbec poslední části Active STPA je totiž pomocí obran dosáhnout splnění a dodržování uvedených omezení, zde požadavek na interakci řidiče a signalisty. Do tabulky možných obran pak byly vepsány tyto možnosti:

1) Nákup senzorů do vozidel: Letištní vozidla by mohla mít, podobně jako osobní automobily, nainstalované senzory, které upozorní na blízkost jiného objektu. Mohlo by se jednat pouze o indikaci vzdálenosti pomocí různých (jinak častých) zvukových signálů či systém kamer s obrazovým výstupem přímo u řidiče. Jelikož by společnost vlastnící tato vozidla musela do všech zařízení nainstalovat tyto senzory, je náročnost ohodnocena číslem 3 – střední.
2) Vylepení výstražných cedulí ve vozidlech: Ve vozidlech pozemního odbavení pohybujících se v blízkosti letadla by byla umístěna informace o nebezpečí prudkých a rychlých pohybů v okolí letounu. Řidiči by tímto byli více upozorněni na nutnost dodržovat příslušná opatření a jednat co možná nejostražitěji. Toto opatření je ze všech zmíněných nejjednodušší, na druhou stranu je však velmi „měkké“, a tak se očekává, že bude mít nejmenší vliv na provozní bezpečnost.
3) Bezpečnostní školení: Zaměstnanci pozemního odbavení by byli znovu seznámeni s nutností opatrného zacházení s technikou a přísného dodržování předpisů. Kromě pouhých přednášek by se mohlo jednat i o praktická školení, kde by zaměstnanci přímo v okolí letadla byli znovu upozorněni na nutnost pracovat podle postupů společnosti. Předpokládá se, že praktická ukázka by zafungovala lépe než jen ústní sdělení.
4) Systém detekce signalisty: V diplomové práci Jindřicha Dudy je uveden návrh na snížení počtu takových odbavení, při nichž není přítomen signalista. *„Takovým prvkem by mohl být spínač (tlačítko) umístěný na straně řidiče u konce ramene pásového dopravníku tak, aby ho nemohl zmáčknout sám řidič. Během přiblížení pásového dopravníku k letadlu by muselo dojít k interakci mezi signalistou a řidičem. Řidič by musel mít svoji levou nohu na ‚bezpečnostním' pedálu a signalista by zmáčkl spínač, tím by došlo k ověření stavu, že signalista je na místě."* [25] Složitostí zavedení se toto opatření může rovnat nákupu senzorů. Na druhou stranu se jedná o novinku, jež ještě není vyzkoušená, a předpokládá se tedy, že by její zavedení přineslo do systému i možné problémy se spolehlivostí.

Byla přidána tato nebezpečí:

Byly přidány tyto ztráty:

Doporučení z kroku 1.1: Prioritizovat zvýšení úrovně obrany

Omezení řídicích prvků: Řidič nesmí provádět manévr bez ověření signálu od signalisty

Vypište seznam možných obran a ohodnoťte je podle náročnosti jejich zavedení (1 – nejjednodušší, 5 – nejsložitější):

ID	Popis	Náročnost zavedení
1	Nákup senzorů do vozidel	3
2	Vylepení výstražných cedulí ve vozidlech	1
3	Bezpečnostní školení	2
4	Systém detekce signalisty	4

Obr. 24: Ukázka vizuální stránky softwaru – krok 3.1 [vlastní tvorba]

V předešlé fázi byly vymyšleny obrany i s přiřazeným ohodnocením náročnosti jejich zavedení. Nyní je načase je hlouběji zanalyzovat, připsat k nim jejich klady a zápory a také se zamyslet nad opatřeními, která by bylo nutné zavést při jejich implementaci. Všechny informace, které zde budou podrobně rozebrány, jsou zkratkovitě vypsány na Obr. 25. Nyní k jednotlivým obranám:

1) Nákup senzorů do vozidel: Jedná se o poměrně jednoduchý a spolehlivý nástroj, který je již vyzkoušen z oblasti automobilového průmyslu. Jelikož se spoléhá na technologie v podobě emise, odrazu a příjmu záření, daří se díky němu eliminovat chyby lidského faktoru. V konečném důsledku by mohlo dojít až k úplné ztrátě nutnosti stání signalisty na určeném místě. Na druhou stranu by se všechna vozidla musela vybavit těmito senzory, což by bylo značně finančně náročné. Při postupné implementaci pak vznikají zase další rizika spojená s různými předpisy pro různá vozidla. Z hlediska provozu těchto modernějších vozidel by pak bylo nutné zajistit certifikaci a potřebnou údržbu instalovaných prvků. Co se týče opatření, bylo by nutné s novými senzory seznámit zejména řidiče vozidel pozemního odbavení, ale také pracovníky technického oddělení. Bylo by nutné vytvořit nové postupy pro pohyb vozidel kolem letounu s důrazem na použití zavedených senzorů. Při absenci signalisty by se také musela zrevidovat omezení a další prvky knihovny STPA. Například omezení „Řidič nesmí provádět manévr bez ověření signálu od signalisty“ by se v tomto případě stalo lichým.
2) Vylepení výstražných cedulí ve vozidlech: Jak již bylo uvedeno výše, toto opatření lze zavést prakticky hned, má jen velmi malé finanční dopady na společnost a je celkově velmi jednoduché. Na druhou stranu cedulku řidiči mohou přehlédnout, při delší době od její instalace si jí mohou přestat všímat úplně. Pro dlouhodobější použití je také nutné tyto štítky obnovovat a celkově se jedná o nepříliš systémové řešení provozní bezpečnosti. Poměrně značnou výhodou je absence jakýchkoliv návazných opatření.
3) Bezpečnostní školení: Jedná se o relativně běžný prvek řízení provozní bezpečnosti. Personál je upozorněn na problémy při pozemním odbavení, je opět informován o nutnosti dodržovat opatření a seznámen s případnými důsledky nesprávného jednání. Účinnější by pak bylo školení přímo na pracovní ploše s názornou zkouškou odbavení jednotlivými pracovníky. Při opakování by pak pro řidiče bylo snazší vybudovat si správné pracovní návyky. Výhodou je, jak již bylo zmíněno výše, zkušenost bezpečnostního oddělení s podobnou formou řešení. Finanční nákladnost je také relativně příznivá. Proti této obraně však mluví nízká účinnost, pokud by mělo školení proběhnout jednorázově. Pro vyšší účinnost je nutná systematičnost školení a neustálé opakování procedur různými směry. Jistým omezením je také fakt, že tímto krokem se přesouvá zodpovědnost z vyšších hierarchických prvků (vedení letiště,

oddělení provozní bezpečnosti atd.) na nižší hierarchické prvky (tj. zaměstnance). Výsledkem by tak opět mohla být jejich penalizace namísto systémového řešení. Jako u předchozí obrany je i zde výhodou praktická absence souvisejících opatření.

4) Systém detekce signalisty: Poslední navrženou obranou je systém detekce signalisty zmíněný v diplomové práci Jindřicha Dudy. Výhodou tohoto řešení je jeho jednoduchost. Stačí totiž v jeden čas stisknout dvě tlačítka a vozidlo může odjet od letadla. To také podporuje myšlenku dodržení předpisů, a tedy i omezení. Na druhou stranu se jedná o stále nevyzkoušené řešení, které s sebou může do provozu přinést problémy se spolehlivostí. Ty by se projevily zvýšením času potřebného pro provedení pozemního odbavení letadel. Podobně jako u první navržené obrany je také finančně nákladnější a souvisejí s ním nutná opatření v podobě školení personálu pozemního odbavení, školení mechaniků a vydání nových postupů pro pozemní odbavení.

K navrženým obranám připište klady, zápory a nutné změny v systému:

Popis	Klady	Zápory	Opatření
Nákup senzorů do vozidel	Spolehlivost, omezení lidského faktoru	Vysoké náklady, nutnost údržby	Školení řidičů a mechaniků, nové postupy, nová omezení
Vylepení výstražných cedulí ve vozidlech	Nízké náklady, jednoduchost	Nízká účinnost, nesystémovost	×××
Bezpečnostní školení	Nízké náklady, zkušenosti	Nízká účinnost, přesun zodpovědnosti	×××
Systém detekce signalisty	Jednoduchost, dodržení předpisů	Vyšší náklady, spolehlivost, zdržení	Školení řidičů, signalistů a mechaniků, nové postupy

Obr. 25: Ukázka vizuální stránky softwaru – krok 3.2 [vlastní tvorba]

Po zvážení všech pozitiv a negativ navržených obran je na pověřené osobě, aby rozhodla o jejich zavedení či nezavedení. Je doporučeno, aby při tomto rozhodování letiště používalo metody, které má k dispozici a s nimiž má zkušenosti. Bezpečnostní analytik by měl vzít v potaz jak náročnost zavedení, tak i klady, zápory a opatření, která je nutné zavést v návaznosti na přijatou obranu. V softwarovém nástroji bude poté možné vybrat více obran, zde však je pro názornost zvolena pouze jedna, a sice systém pro detekci signalisty z výše zmíněné diplomové práce (viz Obr. 26). V praxi by nejspíše byla vybrána druhá nebo třetí obrana, a to vzhledem k nízké náročnosti zavedení a lepší vymahatelnosti. Zejména po pandemii v roce 2020 totiž společnosti operující v leteckém provozu nedisponují takovými finančními prostředky, aby mohly provádět větší investice. Jelikož však druhá a třetí obrana s sebou nenesou žádná související opatření, pro větší názornost tohoto i dalšího kroku byla vybrána čtvrtá možnost. Ta také splňuje poučku, která říká, že obrany mají zajišťovat dodržování omezení, což by zde po zavedení systému detekce signalisty mělo být splněno. Zde je také nutné podotknout, že letiště může nad rámec svých možností tuto úpravu společnosti pouze doporučit. Na Obr. 26 jsou uživateli též znovu předkládána nutná související opatření, aby se zabránilo případným opomenutím způsobeným lidským faktorem.

Seznam navržených obran:

Popis	Náročnost	Klady	Zápory	Opatření
Nákup senzorů do vozidel	3	Spolehlivost, omezení lidského faktoru	Vysoké náklady, nutnost údržby	Školení řidičů a mechaniků, nové postupy, nová omezení
Vylepení výstražných cedulí ve vozidlech	1	Nízké náklady, jednoduchost	Nízká účinnost, nesystémovost	×××
Bezpečnostní školení	2	Nízké náklady, zkušenosti	Nízká účinnost, přesun zodpovědnosti	×××
Systém detekce signalisty	4	Jednoduchost, dodržení předpisů	Vyšší náklady, spolehlivost, zdržení	Školení řidičů, signalistů a mechaniků, nové postupy

Vyberte alespoň jednu obranu: Systém detekce signalisty

Nutná opatření: Školení řidičů, signalistů a mechaniků, nové postupy

Obr. 26: Ukázka vizuální stránky softwaru – krok 3.3 [vlastní tvorba]

Nyní přichází důležité místo, kde uživatel zavede jednotlivé obrany, které přidal v předchozím kroku. Nástroj radí (Obr. 27) nejdříve zavést opatření na malém vzorku a přesvědčit se, že jsou aplikovatelná i v reálném provozu, že negenerují další nebezpečí a nejsou v konfliktu s jinými postupy, opatřeními nebo prvky systému. Opět je zde uživateli připomínáno, že obranná opatření vyžadují ještě další související změny v systému, na něž se nesmí zapomenout. Pokud uživatel během zkušební doby nezaznamená žádné problémy s implementací, zaškrtne možnost zavedení obran do provozu. V další části se mu rozevře seznam zaměstnanců, z něhož vybere osobu zodpovědnou za implementaci obrany do prostředí letiště. Také zadá termín, před kterým mají být dané změny zavedeny. Ještě jednou jsou zde pro připomínku uvedena návazná opatření. Poslední zprávou této strany je informace o nutnosti aktualizace dokumentace, prosazení změn a sledování a průběžném vyhodnocování opatření. Provoz na letišti, stejně jako analýza STPA a Active STPA, by totiž měl být stále se zdokonalující proces. V provozu se pak i přes veškerou snahu o bezkonfliktnost v testovacích a zaváděcích fázích mohou vyskytnout situace, které je nutno vyřešit.

Pokud je to možné, zaveďte na malém vzorku obranná opatření.

Nezapomeňte na související opatření: Školení řidičů, signalistů a mechaniků, nové postupy

Mohou být obrany zavedeny do provozu? ☑

Zadejte zodpovědnou osobu: Ing. Karel Novák

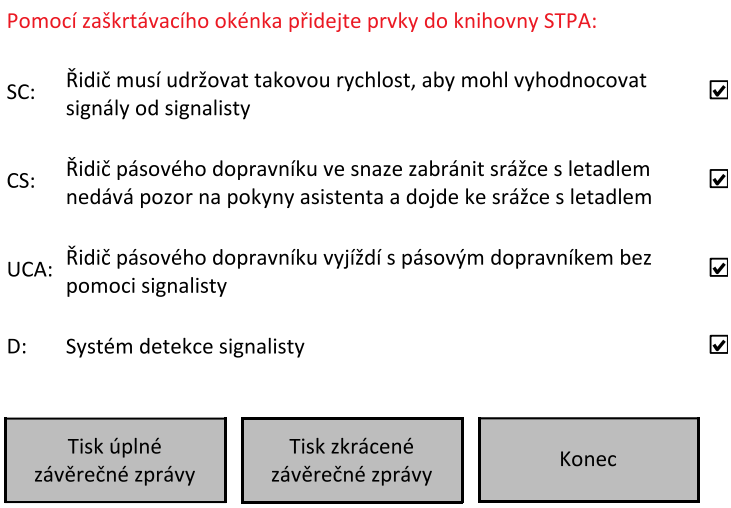
Zadejte datum implementace: 30. 6. 2023

Nutná opatření: Školení řidičů, signalistů a mechaniků, nové postupy

Aktualizujte dokumentaci, prosaďte změny a stále sledujte jejich dopad.

Obr. 27: Ukázka vizuální stránky softwaru – krok 3.4 [vlastní tvorba]

Jak již bylo několikrát zmíněno v průběhu návrhu architektury, na konci samotného nástroje přichází aktualizační fáze, kdy jsou změny provedené uživatelem zahrnuty do knihovny STPA. Smyslem tohoto kroku je uživatele znovu upozornit na prvky, které přidává. V levé části seznamu se objevuje ve zkratce popis přidávaného prvku podle zásad STPA. V pomyslném prostředním sloupci je umístěn popis, zde (Obr. 28) např. přidaná obrana „systém detekce signalisty“. Napravo se pak nacházejí zatrhávací okénka pro konečné přidání prvku do knihovny STPA. Tím je samotná práce se systémem ukončena. V rámci zjednodušení práce je uživateli ještě nabízeno vytisknout úplnou nebo zkrácenou závěrečnou zprávu. Tématem závěrečných zpráv softwaru se zabývá další část bakalářské práce.



Obr. 28: Ukázka vizuální stránky softwaru – krok 3.5 [vlastní tvorba]
(SC – omezení, CS – kauzální scénáře,
UCA – nebezpečné řídicí akce, D – obrany)

8.1 Závěrečná zpráva

Na konci řešení případu pomocí Active STPA je nasnadě využít softwarové možnosti a nechat si vyhotovit závěrečnou zprávu, která by shrnula práci uživatele se softwarem. Tato zpráva by měla být vyhotovována automaticky a níže je uvedena ve dvou vzorech: úplném a kratším. Úplná závěrečná zpráva obsahuje všechny informace, které uživatel zadal do softwaru při řešení události a je určena k zevrubnému shrnutí problematiky. Naproti tomu zkrácená závěrečná zpráva je uplatnitelná v SMS, protože ze všech informací, které se v systému vyskytují, jsou vytaženy pouze takové, které se objevují v závěrečných zprávách k incidentům.

8.1.1 Úplná závěrečná zpráva

Následuje příklad úplné závěrečné zprávy z předchozího příkladu. Pro lepší orientaci uživatele je u každého bodu barevně odlišená odrážka. Černá barva (■) signalizuje obecnou informaci, zelená (■) ideální stav nebo nízkou závažnost sdělení, žlutá (■) střední závažnost sdělení a červená (■) vysokou závažnost, například porušení předpokladů nebo absenci v knihovně.

Závěrečná zpráva Active STPA 07/2022

Postupy:

■ Zúčastněný postup 1: Řidiči vybraných typů MMP jsou povinni při vyjíždění z bezpečnostní zóny řídit se pokyny oprávněné osoby, která pomocí ručních signálů naviguje příslušného řidiče.

■ Nebyly vybrány neúčinné postupy.

■ Důvody proti obranám: Obrana je příliš nákladná (prioritizovat zvýšení úrovně obrany).

■ Postupy v knihovně STPA byly kompletní.

Omezení řídicích prvků:

■ Zúčastněné omezení 1: Řidič nesmí provádět manévr bez ověření signálu od signalisty.

■ Neúčinné omezení 1: Řidič nesmí provádět manévr bez ověření signálu od signalisty.

■ Důvod neúčinného omezení 1: Do procesu vstupuje zpoždění.

■ Omezení řídicích prvků v knihovně STPA byla kompletní.

■ Bylo přidáno omezení: Řidič musí udržovat takovou rychlost, aby mohl vyhodnocovat signály od signalisty.

■ SMS: Řidič musí udržovat takovou rychlost, aby mohl vyhodnocovat signály od signalisty.

Kauzální scénáře:

■ Nebyl vybrán kauzální scénář z knihovny STPA.

■ Kauzální scénáře v knihovně STPA nebyly kompletní.

■ Byl přidán kauzální scénář: Řidič pásového dopravníku ve snaze zabránit srážce s letadlem nedává pozor na pokyny asistenta a dojde ke srážce s letadlem.

■ Důvod absence kauzálního scénáře: Přílišná komplexnost systému.

Nebezpečné řídicí akce:

■ Nebyly nalezeny žádné nebezpečné řídicí akce z knihovny STPA.

■ Nebezpečné řídicí akce v knihovně STPA nebyly kompletní.

■ Byla přidána nebezpečná řídicí akce: Řidič pásového dopravníku vyjíždí s pásovým dopravníkem bez pomoci signalisty.

■ Kategorie nebezpečné řídicí akce: Vykonání způsobuje nebezpečí.

Nebezpečné řídicí akce na vyšších hierarchických úrovních:

■ Nebezpečné řídicí akce na vyšších hierarchických úrovních nebyly nalezeny.

Omezení na systémové úrovni:

■ Omezení na systémové úrovni v knihovně STPA byla kompletní.

Nebezpečí:

■ Nebezpečí v knihovně STPA byla kompletní.

Ztráty:

■ Ztráty v knihovně STPA byly kompletní.

Porušené předpoklady:

■ Porušený předpoklad 1: Odbavení letadla probíhá za dodržení odbavovacích procedur.

■ Předpoklady v knihovně STPA byly kompletní.

■ Předpoklady jsou porušovány opakovaně.

Analýza trendů:

■ Trend 1: Vozidla nejsou řádně řízena při pohybu k letadlu a od něj.

■ Klasifikace trendu 1: Stálý.

Přispívající faktory:

■ Přispívající faktor 1: Řidič před příjezdem posunul signalizační kužel pod spodní okraj vstupu motoru č. 2.

■ Závažnost přispívajícího faktoru 1: 3.

Chybné předpoklady:

■ Předpoklady nebyly chybné.

■ Předpoklady v knihovně STPA byly kompletní.

Nouzová opatření:

■ Nouzová opatření neexistovala.

■ Opatření nelze zavést, protože neexistují nebo nejsou k dispozici nouzová opatření, která by byla v dané situaci použitelná.

Navržené obrany:

■ Byly navrženy tyto obrany (Tab. 4):

Tab. 4: Seznam navržených obran [vlastní tvorba]

ID	Popis	Náročnost	Klady	Zápory	Související opatření
1	Nákup senzorů do vozidel	3	Spolehlivost, omezení lidského faktoru	Vysoké náklady, nutnost údržby	Školení řidičů a mechaniků, nové postupy, nová omezení
2	Vylepení výstražných cedulí ve vozidlech	1	Nízké náklady, jednoduchost	Nízká účinnost, nesystémovost	×××
3	Bezpečnostní školení	2	Nízké náklady, zkušenosti	Nízká účinnost, přesun zodpovědnosti	×××
4	Systém detekce signalisty	4	Jednoduchost, dodržení předpisů	Vyšší náklady, spolehlivost, zdržení	Školení řidičů, signalistů a mechaniků, nové postupy

■ Byla vybrána obrana č. 4: Systém detekce signalisty.

Zavedení obran:

■ Obrany mohou být zavedeny do provozu.

■ Zodpovědná osoba: Ing. Karel Novák.

■ Datum implementace: 30. 6. 2023.

■ SMS: Školení řidičů, signalistů a mechaniků, nové postupy.

Aktualizace STPA:

■ Omezení řídicích prvků: Řidič musí udržovat takovou rychlost, aby mohl vyhodnocovat signály od signalisty.

■ Kauzální scénář: Řidič pásového dopravníku ve snaze zabránit srážce s letadlem nedává pozor na pokyny asistenta a dojde ke srážce s letadlem.

■ Nebezpečná řídicí akce: Řidič pásového dopravníku vyjíždí s pásovým dopravníkem bez pomoci signalisty.

■ Obrana: Systém detekce signalisty.

■ Analýza Active STPA byla úspěšně dokončena.

8.1.2 Zkrácená závěrečná zpráva

Zkrácená závěrečná zpráva oproti úplné neobsahuje všechny informace, nýbrž se zaměřuje pouze na ty podstatné pro řešení incidentu oddělením řízení kvality, safety a procesů. Data ze softwaru by totiž mohla být jednoduše použita v závěrečné zprávě k incidentu, kterou vyhotovuje právě oddělení provozní bezpečnosti. Jelikož se v softwaru neřeší všechny otázky uvedené v závěrečné zprávě k incidentu, musel by odpovědný pracovník patrně vždy některé části doplnit. Jedná se například o důkazní materiály, s nimiž analýza Active STPA nepracuje. Spolupráce s tímto softwarem by zaměstnancům nicméně výrazně usnadnila práci.

Závěrečná zpráva Active STPA 07/2022

Kauzální scénář: Řidič pásového dopravníku ve snaze zabránit srážce s letadlem nedává pozor na pokyny asistenta a dojde ke srážce s letadlem.

Nebezpečná řídicí akce: Řidič pásového dopravníku vyjíždí s pásovým dopravníkem bez pomoci signalisty.

Postupy: Řidiči vybraných typů MMP jsou povinni při vyjíždění z bezpečnostní zóny řídit se pokyny oprávněné osoby, která pomocí ručních signálů naviguje příslušného řidiče.

Přijatá opatření:

Opatření 1: Řidič musí udržovat takovou rychlost, aby mohl vyhodnocovat signály od signalisty.

Opatření 2: Systém detekce signalisty (zodpovědná osoba: Ing. Karel Novák, datum implementace: 30. 6. 2023, návazná opatření: školení řidičů, signalistů a mechaniků, nové postupy).

9 ZAVEDENÍ DO SMS

Systém řízení bezpečnosti (tj. SMS) je z definice leteckého předpisu L 19 *„systematický přístup k řízení bezpečnosti zahrnující nezbytné organizační struktury, odpovědnosti, zásady a postupy“* [1]. Jeho cílem je komplexní řízení provozní bezpečnosti s použitím reaktivních, ale hlavně proaktivních a prediktivních metod. Pokud již dojde k události, letiště využívá reaktivního způsobu k navržení takových nápravných opatření, aby se podobná událost již neopakovala. Ačkoliv se Active STPA zaměřuje zejména na integraci proaktivní a prediktivní metody, lze ji použít i v tomto případě (a shodou okolností použita byla). Výhodou oproti klasickému řešení oddělením řízení kvality, safety a procesů by pak byla výrazná automatizace procesů v čele s vydáním závěrečné zprávy.

Proaktivní přístup k bezpečnosti evokuje, že v systému se budou proaktivně vyhledávat chyby, slabá místa atd. Pomocí tohoto procesu dojde ke zvýšení úrovně provozní bezpečnosti. Vstupní entitou může být například dobrovolné hlášení nebo výstup z inspekcí. Na oba zmíněné vstupy přitom návrh architektury softwarového nástroje může navázat a v obou případech může navrhnout potřebné obrany.

Poslední možností je přístup prediktivní. Ten se pohledem na aktuální nebo historická data snaží předpovědět bezpečnostní situaci v budoucnosti. Širší zavedení prediktivních metod by usnadnilo rozšíření automaticky sbíraných dat na letišti. Předpokládá se, že tato data by také byla dostupná v reálném čase, což s sebou přináší další benefity. S těmito daty by pak software mohl lépe pracovat. Data jsou kromě práce v samotné architektuře softwaru potřebná i při jeho spuštění. Ačkoliv je v práci navržena metoda sledování dat, je na druhou stranu doporučeno, v souvislosti s uživatelskou přívětivostí, aby letiště jako doposud využívalo bezpečnostních indikátorů, s nimiž má již zkušenosti. U nich je nastavena cílová hodnota a hodnota, při jejímž překročení dojde k určité akci. Zde by se jednalo právě o spuštění softwaru.

Představený nástroj staví na poznatcích z analýzy Active STPA. Ta se sama mimo jiné v jedné kapitole zabývá integrací do SMS. To je také jeden z důvodů, proč je možné podotknout, že architektura softwarového nástroje je v souladu s pravidly SMS a z normativního hlediska by neměly vznikat problémy při jejím zavedení. Implementace by také přinesla uživateli řadu výhod, o čemž hovoří další část této kapitoly. Na druhou stranu není možné zatajit ani úskalí, která stojí na cestě jeho zavedení do SMS. O tom všem se ještě zmiňuje aktuální kapitola tohoto dokumentu.

Nejdříve představme hlavní body, které hovoří pro zavedení architektury či budoucího nástroje do systému řízení provozní bezpečnosti:

1) Jedná se o intuitivnější a uživatelsky přívětivé prostředí, které uživatele přirozeně vede cestou analýzy Active STPA.
2) Uživateli jsou kladeny jasné otázky a dávány přesné instrukce, což podporuje jednodušší pochopení analýzy i za neúplné znalosti slovníku STAMP.
3) Do budoucího softwarového nástroje se doporučuje přidat ke každému kroku okno s legendou nebo nápovědou, kde by byly vysvětleny aktuálně používané pojmy. Toto opatření opět usnadňuje práci uživatele se softwarem, i když by nebyl zcela seznámen s problematikou modelu STAMP.
4) Kde je to možné, využívá se v návrhu rozbalovacích seznamů nebo zaškrtávacích políček. Tím se podstatně zjednoduší práce se softwarem a sníží se riziko možných překlepů ze strany uživatele.
5) Architektura softwaru využívá slovník modelu STAMP. Výhodou je konkrétní a přesné pojmenování problémů a vzájemné porozumění mezi různými uživateli této architektury či budoucího softwarového nástroje.
6) Jednotlivé části (fáze) analýzy spolu prostřednictvím vazeb v návrhu architektury softwaru komunikují. V aktuálním kroku se proto zobrazují takové informace z předchozích částí, které uživateli pomáhají s rozhodováním o aktuálně řešeném problému analýzy Active STPA. Nejčastěji používané informace tak uživatel nemusí dohledávat v přechozích fázích, nýbrž je má přehledně na očích.
7) Uživatel má na konci procesu možnost vytisknout dvě automatické závěrečné zprávy, a to úplnou a zkrácenou. V úplné zprávě se vyskytují všechny informace získané od uživatele v průběhu procesu, zkrácená zpráva pak má potenciál využití pro oddělení řízení kvality, safety a procesů v systému SMS.
8) Další možností budoucího softwarového řešení je automatická aktualizace knihovny STPA, která opět zjednodušuje uživateli práci a snižuje čas potřebný na úplné vyřešení události.
9) Pro jednodušší implementaci do SMS ruzyňského letiště také mluví návaznost této práce na bakalářskou práci zabývající se analýzou STPA pro procesy pozemního odbavení. Tímto je zaručen „bezešvý“ spoj mezi dvěma systémy zabývajícími se dotčenými analýzami a jejich bezproblémové použití v budoucnu.

Ačkoliv nyní byly vyjmenovány všechny benefity, které tato bakalářská práce a její návrh architektury softwaru skýtá, je nutné podotknout, že do cesty úplné integrace nástroje do systému SMS mezinárodního civilního letiště by se však ještě mohlo stavět několik překážek:

1) Nedostatek zkušeností: Vzhledem k tomu, že architektura je postavena na logice modelu STAMP a na analýzách STPA a Active STPA, představuje v prostředí letiště novum. Ačkoliv se tato bakalářská práce snaží práci se systémem co nejvíce usnadnit a přiblížit koncovému uživateli skrze intuitivní prostředí a nápovědy vysvětlující termíny, bude nutné personál vyškolit, a to zejména v oblasti používání logiky modelu STAMP. Pro plnou funkčnost softwaru budou muset uživatelé pochopit pojmy, jako např. indukční smyčka, omezení systému nebo předpoklady na systém.
2) Absence analýzy STPA: Letiště zatím nemá k dispozici kompletní analýzu STPA, která například zahrnuje celkový model letiště. Protože však analýza Active STPA vyžaduje již proběhlou analýzu STPA, nelze v současné době ani tento návrh plně použít. Na druhou stranu tento nástroj navazuje i na poznatky bakalářské práce Ondřeje Vašaty, který některé části pro procesy pozemního odbavení navrhl. Při zavedení analýzy STPA na letišti tak lze očekávat funkčnost i tohoto systému. Fakulta dopravní ČVUT navíc spolupracuje s letištěm na kompletní analýze STPA i s celkovým modelem letiště. Až bude tento koncept představen, bude možné na něj navázat analýzou navrženou v této bakalářské práci.
3) Absence softwarového řešení: Tato bakalářská práce se snaží práci s analýzou co nejvíce usnadnit. Přestože se jedná pouze o návrh architektury softwaru, zvyšuje se jím použitelnost analýzy Active STPA v praxi. Je však nutné mít na paměti, že se stále jedná pouze o návrh architektury softwaru. Ačkoliv všechny důležité prvky pro návrh budoucího softwarového nástroje jsou načrtnuty v této práci, bude nutné na ni navázat naprogramováním takového nástroje, který by všechny tyto poznatky převedl do praxe. Na druhou stranu je tímto dokázáno, že na tuto bakalářskou práci je možné a vhodné navazovat dalším výzkumem.

V současné době je tedy využití této práce stále ještě omezeno tímto výčtem překážek. Asi největší z nich je absence analýzy STPA a vůbec modelu STAMP pro letiště. Toto je omezení, které značně limituje systémové použití nástroje popsaného v této práci. Pro každý záznam by totiž musela být vymodelována nová řídicí smyčka a pole, kde má uživatel vybírat možnosti z knihovny STPA, by musela být vyplňována ručně. Značně by se tak stíraly výhody řešení touto metodou. Proto by nyní tento nástroj mohl být využíván jen jako doplněk metod praktikovaných letištěm. Pokud by však byly vyřešeny výše zmíněné nedostatky, může se z tohoto nástroje stát plnohodnotná součást systému řízení provozní bezpečnosti.

10 ZÁVĚR

Úroveň provozní bezpečnosti mezinárodního civilního letectví rok od roku roste a od prvopočátků aviatiky došlo k její razantní změně. Místo reakcí na události a poučení se z nich se snažíme těmto událostem předcházet, cíleně hledat v systému chyby a reagovat na ně. Základem dnešního řízení provozní bezpečnosti je použití proaktivních a prediktivních metod, díky nimž je některým událostem v provozu zabráněno ještě dříve, než by se mohly stát. Jelikož je však rozvoj provozní bezpečnosti kontinuální a nikdy nekončící proces, zkoumá se v současné době i možnost integrace těchto metod. Ta poskytuje více benefitů než používání proaktivního a prediktivního pohledu na bezpečnost odděleně. Jednou z odborných prací zaměřených na tuto problematiku je disertační práce zabývající se analýzou Active STPA. Překážkou na cestě jejího plnohodnotného uplatnění v SMS je však absence softwarového řešení, na což reaguje tato bakalářská práce.

Hlavním cílem výzkumu v rámci bakalářské práce byl návrh architektury softwaru, který by teoretičnost analýzy Active STPA přiblížil praxi a zvýšil by možnosti jejího využití v prostředí mezinárodního civilního letiště. Dalším, neméně důležitým bodem bylo představit funkčnost architektury softwaru na sadě dat, kterou poskytla společnost Letiště Praha, a. s. Jednalo se o závěry inspekcí pozemního odbavení a incident, který s těmito daty souvisel. Nakonec byly zhodnoceny benefity uplatnění nástroje v praxi a možné překážky na cestě uplatnění tohoto i budoucího softwaru v praxi.

Architektura softwaru staví na základech Active STPA, ale snaží se problematiku co nejvíce přiblížit uživateli, a stát se tak uživatelsky přívětivou. Toho se dosahuje několika kroky. Již v rámci návrhu architektury softwaru byly navrženy vazby mezi jednotlivými prvky, díky čemuž mezi sebou jednotlivé části komunikují a poskytují si (a uživateli) informace, jež jsou zrovna pro řešení incidentu v dané části potřebné. Systém také intuitivně uživatele vede cestou Active STPA. Další výhodou je zavedení rozbalovacích seznamů a zaškrtávacích oken, která zjednodušují uživateli práci a snižují riziko překlepů. Možnosti, které rozbalovací seznamy používají, byly importovány z bakalářské práce Ondřeje Vašaty, který se mj. zabýval analýzou STPA pro procesy pozemního odbavení, a disertační práce Active STPA od Dioga Silvy Castilha. Díky použití bakalářské práce, která se zabývala analýzou STPA pro procesy pozemního odbavení na ruzyňském letišti, je také zaručena kompatibilita nástroje představeného v této práci. V procesu zjišťování informací od uživatele se návrh architektury softwaru snaží o co nejjednodušší otázky a nejpřímější instrukce, avšak s přihlédnutím k odbornému slovníku modelu STAMP. Výhodou budoucího softwarového řešení taktéž bude automatická aktualizace STPA knihoven a možnost vytisknutí nebo exportu závěrečných zpráv.

V oblasti praktického řešení návrhu architektury softwarového nástroje byla analyzována data z inspekcí pohybu pásových dopravníků a zhodnoceny možnosti stanovování hranice pro spuštění analýzy. V samotné části řešení incidentu byla i s návrhem vizuální stránky představena faktická funkčnost popsaného řešení. Původní knihovna STPA byla obohacena o jeden kauzální scénář a jednu nebezpečnou řídicí akci. V rámci návrhu nápravných opatření bylo doporučeno vydat jedno omezení a jedno obranné opatření, kterážto doporučení se do reálného provozu promítnou zejména ve formě nových postupů. Ty mají za úkol zajistit, aby se zamezilo pochybením nalezeným v rámci řešení této bakalářské práce a aby se prosazovaly postupy uvedené v dokumentaci letiště.

Tato bakalářská práce navrhla architekturu softwaru, který má zvýšit použitelnost analýzy Active STPA v praxi. Ačkoliv i samotná architektura zjednodušuje práci s analýzou a přináší uživateli vyšší komfort při jejím řešení, software zatím navržen nebyl. Proto je zřejmé, že toto téma má potenciál pro další výzkum, který by například sestrojil softwarový nástroj podle zde uvedených zásad. Ačkoliv již samotný návrh architektury softwaru zvyšuje použitelnost integrační metody, se softwarovým řešením by se tato použitelnost posunula ještě dále a mohla by se stát nedílnou součástí řízení provozní bezpečnosti v prostředí mezinárodního civilního letiště.

11 POUŽITÉ ZDROJE

1. **Ministerstvo dopravy České republiky.** L 19 Řízení bezpečnosti. *Řízení letového provozu ČR.* [Online] 2013. [Citace: 29. prosinec 2021.] Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm. 166/2013-220-LPR/1.

2. **International Civil Aviation Organization.** *Annex 19 to the Convention on International Civil Aviation.* Montréal: International Civil Aviation Organization, 2016. ISBN 978-92-9249-965-5.

3. **Úřad pro civilní letectví.** Letecké předpisy. *Úřad pro civilní letectví.* [Online] [Citace: 30. listopad 2021.] Dostupné z: https://www.caa.cz/dokumenty/predpisy/letecke-predpisy/.

4. **International Civil Aviation Organization.** *Doc 9859.* Montréal: International Civil Aviation Organization, 2018. ISBN 978-92-9258-552-5.

5. **Letiště Praha, a. s.** *Manuál SMS Letiště Praha.* [Manuál] Praha: Letiště Praha, a. s., 2020. LP-RD-002F/2011.

6. **Evropská komise.** EUR-Lex - 02014R0139-20220127 - EN. *EU law - EUR-Lex.* [Online] 27. leden 2022. [Citace: 10. únor 2022.] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0139.

7. **Řízení letového provozu ČR.** AIP - Aeronautical Information Publication. *Řízení letového provozu ČR.* [Online] 4. listopad 2021. [Citace: 16. únor 2022.] Dostupné z: https://aim.rlp.cz/ais_data/www_main_control/frm_cz_aip.htm.

8. **ŠEDIVÁ KAFKOVÁ, Markéta.** *Systemic Integration of Safety Studies with Operational Safety Data in the Aviation.* [Ústní sdělení] 25. října 2021.

9. **CASTILHO, Diogo Silva.** *Active STPA: Integration of Hazard Analysis into a Safety Management System Framework.* [Disertační práce] Massachusetts: Massachusetts Institute of Technology, 2019.

10. **LEVESON, Nancy.** STAMP – Holistic system safety approach or just another risk model? *ScienceDirect.* [Online] 2004. [Citace: 15. červen 2021.] Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0950423014001193.

11. **LEVESON, Nancy G. a THOMAS, John P.** *STPA Handbook.* 2018.

12. **Ústav pro jazyk český Akademie věd České republiky.** Ontologie. *Internetová jazyková příručka.* [Online] [Citace: 3. květen 2022.] Dostupné z: https://prirucka.ujc.cas.cz/?slovo=ontologie.

13. **REJZEK, Jiří.** *Český etymologický slovník.* Třetí vydání (druhé přepracované a rozšířené vydání). Praha: LEDA, 2015. ISBN 978-80-7335-393-3.

14. **GUIZZARDI, Giancarlo.** *Ontological Foundations for Structural Conceptual Models.* [Disertační práce] Enschede: Telematics Instituut Fundamental Research Series, 2005. ISBN 90-75176-81-3.

15. **GUSKOVA, Natalia.** *Konceptualizace vybraných částí modelu bezpečnosti STAMP.* [Bakalářská práce] Praha, 2018.

16. **University of Cambridge.** Assumption. *Cambridge Dictionary.* [Online] Cambridge University Press. [Citace: 27. květen 2022.] Dostupné z: https://dictionary.cambridge.org/dictionary/english/assumption.

17. **MARTIN, Robert Cecil.** *Clean Architecture: A Craftsman's Guide to Software Structure and Design.* Londýn: Prentice Hall, 2018. ISBN 978-0-13-449416-6.

18. **DEWAYNE, E. Perry a WOLF, Alexander L.** Foundations for the Study of Software Architecture. *Software Architecture.* [Online] říjen 1992. [Citace: 18. březen 2022.] Dostupné z: http://users.ece.utexas.edu/~perry/work/papers/swa-sen.pdf.

19. **CLEMENTS, Paul et al.** *Documenting Software Architectures: Views and Beyond. Second Edition.* Boston: Pearson Education, Inc., 2011. ISBN 978-0-321-55268-6.

20. **GARLAN, David a PERRY, Dewayne.** Introduction to the Special Issue on Software Architecture. *IEEE Transactions on Software Engineering.* 1995, Sv. 21, 4.

21. **BOOCH, Grady, RUMBAUGH, James a JACOBSON, Ivar.** *Unified Modeling Language User Guide.* Massachusetts: Addison Wesley, 1998. ISBN 0-201-57168-4.

22. **Software Engineering Standards Committee of the IEEE Computer Society.** *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems.* New York: The Institute of Electrical and Electronics Engineers, Inc., 2000. ISBN 0-7381-2518-9.

23. **Letiště Praha, a. s.** Letiště Václava Havla Praha odbavilo za rok 2019 rekordních 17,8 milionů cestujících. *Letiště Václava Havla Praha, Ruzyně.* [Online] Letiště Praha, a. s., 16. leden 2020. [Citace: 8. srpen 2022.] https://www.prg.aero/letiste-vaclava-havla-praha-odbavilo-za-rok-2019-rekordnich-178-milionu-cestujicich.

24. **VAŠATA, Ondřej.** *Návrh proaktivních indikátorů bezpečnosti pro letiště s využitím modelu STAMP.* [Bakalářská práce] Praha, 2021.

25. **DUDA, Jindřich.** *Modelování koordinačních procesů letiště a nastavení safety mechanismů.* [Diplomová práce] Praha, 2019.

12 SEZNAM OBRÁZKŮ

13 SEZNAM TABULEK

14 SEZNAM PŘÍLOH