ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Porovnání metod při hodnocení provozní bezpečnosti specifického provozu UAS

Comparison of Methods for the Safety Evaluation of a Specific UAS Operation

Diplomová práce

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

Vedoucí práce: doc. Ing. Jakub Kraus, Ph.D.
Ing. Šárka Hulínská

Bc. Jan Stádník

Praha 2022

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

K621.....Ústav letecké dopravy

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Jan Stádník

Studijní program (obor/specializace) studenta:

navazující magisterské –PL– Provoz a řízení letecké dopravy

Název tématu (česky): **Porovnání metod při hodnocení provozní bezpečnosti specifického provozu UAS**

Název tématu (anglicky): **Comparison of Methods for the Safety Evaluation of a Specific UAS Operation**

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je porovnat vhodnost aplikace metod pro hodnocení provozní bezpečnosti aktuálně používaných v letectví na jeden vybraný specifický provoz UAS.
- Provozní bezpečnost v letectví a používané metody
- Výběr specifického provozu UAS pro hodnocení a tvorba konceptu provozu
- Aplikace metod na specifický provoz UAS
- Porovnání výsledků metod
- Zhodnocení výsledků a doporučení používání metod

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury:
Leveson, N. G., Thomas, J.P.: STPA Handbook, March 2018
Hollnagel, E.: FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. 2012
EASA: Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU)

Vedoucí diplomové práce: **doc. Ing. Jakub Kraus, Ph.D.**
Ing. Šárka Hulínská

Datum zadání diplomové práce: **16. července 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 diplomové práce: **16. května 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 diplomové práce.

Bc. Jan Stádník
jméno a podpis studenta

V Praze dne ..... 16. července 2021

Abstrakt

Cílem této diplomové práce je zhodnotit metody pro hodnocení provozní bezpečnosti aktuálně používaných v letectví na jeden vybraný provoz UAS specifické kategorie. Základem zhodnocení je metoda Posouzení rizik specifické kategorie provozu (SORA). Dále byly vytvořeny analýzy podle aktuálně používaných systémových metod pro hodnocení provozní bezpečnosti v letectví. Jedná se o metody STPA a FRAM. Výsledky analýzy založené na systémové metodě STPA byly ve formě omezení a požadavků na systém porovnány s cíli provozní bezpečnosti stanovené metodou SORA. Metoda FRAM je vypracována pomocí kvantitativního přístupu k hodnocení variability. Konkrétně se jedná o simulaci Monte Carlo. Variabilita výstupu je hodnocena z pohledu načasování a přesnosti. Jsou uváženy i externí faktory ovlivňující systém. Výsledek analýzy je ve formě odhalených kritických funkcí systému porovnán s aktuálními požadavky na provoz. Porovnání odhalilo rozpory v poskytování a vyhodnocení U-space služeb a nesrovnalosti v teoretickém a praktickém výcviku dálkově řídící posádky.

Klíčová slova

FRAM, Provozní bezpečnost, SORA, STPA, UAS

Abstract

The aim of this diploma thesis is to evaluate the methods for evaluating operational safety currently used in aviation for one selected UAS operation of a specific category. The evaluation is based on the Specific operation risk assessment (SORA). Furthermore, analyzes were created according to currently used system methods for assessing operational safety in aviation. These are the STPA and FRAM methods. The results of the analysis based on the STPA system method were compared in the form of limitations and system requirements with the operational safety objectives set by the SORA method. The FRAM method is developed using a quantitative approach to assessing variability. Specifically, it is a Monte Carlo simulation. Output variability is evaluated in terms of timing and accuracy. External factors influencing the system are also considered. The result of the analysis is compared with the current operational requirements in the form of revealed critical functions of the system. The comparison revealed discrepancies in the provision and evaluation of U-space services and inconsistencies in the theoretical and practical training of the remote control crew.

Keywords

FRAM, Safety, SORA, STPA, UAS

Poděkování

Na tomto místě bych rád poděkoval všem, kteří mi poskytli podklady pro vypracování této diplomové práce. Zvláště pak děkuji panu doc. Ing. Jakubu Krausovi, Ph.D. za odborné vedení, poskytnuté cenné rady a konzultování této diplomové práce. Dále je mou milou povinností poděkovat rodině a blízkým za morální a materiální podporu, které se mi dostávalo po celou dobu studia.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Porovnání metod při hodnocení provozní bezpečnosti specifického provozu UAS vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

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

V Praze dne 11. května 2022

.....

Podpis

Obsah

Přílohy

Příloha 1: STPA

Příloha 2: Řídící struktura STPA

Příloha 3: Porovnání metod STPA a SORA

Příloha 4: FRAM podle Monte Carlo simulace

Příloha 5: FRAM model

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AGL	Above Ground Level	Nad úrovní země
AH	Abstraction Hierarchy	Abstrakční hierarchie
AMC	Acceptable Means of Compliance	Přijatelné způsoby průkazu
ANSP	Air Navigation Service Provider	Poskytovatel letových navigačních služeb
ARC	Air Risk Class	Třída rizika ve vzduchu
ATSP	Air Traffic Services	Poskytovatel služeb letového provozu
ATZ	Aerodrome Traffic Zone	Letištní provozní zóna
BVLOS	Beyond Visual Line of Sight	Mimo vizuální dohled
CAST	Causal Analysis based on Systems Theory	Kauzální analýza založená na systémové teorii
CIS	Common Information Service	Společná informační služba
ConOps	Concept of Operations	Koncept provozu
CTR	Control Zone	Řízený okrsek
ČR	Czech Republic	Česká republika
EASA	European Aviation Safety Agency	Evropská agentura pro bezpečnost letectví
ECCAIRS	European Coordination centre for Accident and Incident Reporting Systems	Evropské koordinační centrum pro systémy hlášení nehod a incidentů
ERP	Emergency Response Plan	Pohotovostní plán
EU	European Union	Evropská unie
EVLOS	Extended Visual Line of Sight	Rozšířený vizuální dohled
FHA	Functional Hazard Assessment	Analýza funkčních rizik
FMEA	Failure Mode and Effects Analysis	Analýza příčin a důsledků poruch
FRAM	Functional Resonance Analysis Method	Metoda funkční rezonanční analýzy
FTA	Fault Tree Analysis	Analýza stromu poruch
GM	Guidance Material	Poradenský materiál
GNSS	Global Navigation Satellite System	Globální navigační satelitní systém

GRC	Ground Risk Class	Třída rizika na zemi
HAZOP	Hazard and Operability Study	Analýza nebezpečnosti a provozovatelnosti
HMI	Human Machine Interface	Rozhraní člověka a stroje
JARUS	Joint Authorities for Rulemaking on Unmanned Systems	Sdružení úřadů pro předpisovou činnost v oblasti bezpilotních systémů
MD	Ministry of Transport	Ministerstvo dopravy
MIT	Massachusetts Institute of Technology	Massachusettský technologický institut
OkP	Authorization to Operate	Oprávnění k provozu
OSO	Operational Safety Objectives	Cíle provozní bezpečnosti
SAIL	Specific Assurance and Integrity Level	Konkrétní úroveň jistoty a integrity
SMS	Safety Management System	Systém řízení bezpečnosti
SORA	Specific Operations Risk Assessment	Posouzení rizika specifické kategorie provozu
SPC	Scenario Performance Condition	Výkonnostní podmínka scénáře
STAMP	System-Theoretic Accident Model and Process	Model a proces nehody systémové teorie
STPA	System-Theoretic Process Analysis	Procesní analýza systémové teorie
TMPR	Tactical Mitigation Performance Requirement	Požadavky na výkonnost taktických zmírnění
TMZ	Transponder Mandatory Zone	Oblast s povinným odpovídačem
UA	Unmanned Aircraft	Bezpilotní letadlo
UAS	Unmanned Aircraft System	Bezpilotní systém
UCA	Unsafe Control Action	Nebezpečná řídící akce
ÚCL	Civil Aviation Authority	Úřad pro civilní letectví
USSP	U-space Service Provider	Poskytovatel U-space služeb
VLOS	Visual Line of Sight	Ve vizuálním dohledu

Úvod

Provoz bezpilotních systémů zažívá v posledních letech velký rozmach, se kterým je spojena snaha regulátorů o tvorbu legislativních rámců, jenž by s rostoucí poptávkou po provozu držela krok. Členské státy Evropské unie si dříve stanovovaly pravidla pro provoz bezpilotních systému samostatně. V posledních letech je však situace odlišná a pravidla se mezi státy harmonizují. Evropská komise publikovala Prováděcí nařízení Komise (EU) 2019/947, ve kterém je představeno rozdělení provozu bezpilotních systémů do 3 kategorií: „otevřené“, „specifické“ a „certifikované“ [1]. Podmínky pro určení kategorie provozu zohledňují rizika, která daný provoz představuje. Provoz v „otevřené“ kategorii provozu představuje nejnižší míru rizika ve vzduchu i na zemi. Opakem je provoz v kategorii „certifikované“, ve které se předpokládá s nejvyšší mírou rizika. Pravidla provozu v „certifikované“ kategorii provozu nebyla v době publikace této diplomové práce pevně stanovena a je počítáno s provozem bezpilotních systémů, který bude z většiny spadat do „otevřené“ nebo „specifické“ kategorie provozu.

Pro provoz ve „specifické“ kategorii je podle [1] popsána metoda, jakožto přijatelný způsob průkazu Článku 11. Jedná se o metodu SORA, která je určena pro provozovatele UAS pro určení podmínek, podle nichž je možné provést zamýšlený provoz. Ruku v ruce s rostoucí poptávkou po provozu a postupnou implementací pravidel a služeb U-space je počítáno s postupnými revizemi metody SORA, které pomohou odhalit a doplnit případné nedostatky metody. V letectví jsou pro analýzu provozní bezpečnosti aktuálně používané systémové metody vycházející z předpokladů Safety-II. Jedná se o metody STPA a FRAM.

Cílem této diplomové práce je porovnání výsledků zvolených metod pro hodnocení provozní bezpečnosti pro jeden vybraný provoz UAS „specifické“ kategorie.

1 Provozní bezpečnost v letectví a používané metody

Bezpečnost je značně široký pojem, který nás provází již od nepaměti a který je nutně s vývojem a pokrokem společnosti skloňován ve stále více oblastech lidského života a lidské činnosti. Pro letectví představuje bezpečnost fundamentální faktor, jedná se o základní kámen celého odvětví. Před dalším použitím pojmu provozní bezpečnost je nutné jej ukotvit definicí. Definic existuje velké množství, Mezinárodní organizace pro civilní letectví jej ve své publikaci [8] definuje takto: *„Stav, ve kterém jsou rizika spojená s letectvím, činnosti související s provozem letadel nebo s přímou podporou provozu letadel omezeny a kontrolovány na přijatelnou úroveň“* [8]. Bezpečnost je vždy spojená s nějakou ztrátovou událostí, která může být ve formě života, zdraví, finančních prostředků atd. Motivace řešit bezpečnost pak vychází z této ztráty.

Provozní bezpečnost prošla určitou transformací, tak aby používané přístupy, co nejlépe odpovídaly potřebám aktuálních systémů. Publikace [9] popisuje historické milníky z pohledu bezpečnosti. První zmínky o bezpečnosti na pracovišti sahají k počátku průmyslové revoluce v roce 1769, kdy bylo nutné nalézt prostředky k zabezpečení strojního zařízení, k zabránění zhroucení konstrukcí či zastavení výbuchů. Prvním dokumentem, který se zabýval bezpečností na pracovišti byl Zákon o zařízeních pro bezpečnost na železnici z roku 1893. Postupným technologickým vývojem, potřebou nových přístupů pro řešení problémů, které s sebou pokrok přinesl bylo potřeba představit nové pohledy a metody pro vysvětlení vzniku nehod. Příkladem je analýza Fault Tree (FTA) vytvořena v roce 1961 pro armádní účely. Metoda FTA popisuje souhrn událostí, které ve vzájemné kombinaci mohou vést k nehodě. Další technické bezpečnostní metody, jako jsou FMEA, HAZOP a Event Tree, byly vytvořeny nejen za účelem identifikování nebezpečí a příčin nehod, ale také k identifikaci rizik a nebezpečí před uvedením systému do provozu. Zmíněné metody vychází z modelu řetězce událostí.

Z [3] vyplývá, že pro analýzy systémů, ve kterých zastával člověk určitou funkci, musel být vytvořen přístup, jak tuto skutečnost ohodnotit. Začala se hodnotit lidská spolehlivost. První generace metod pro hodnocení lidské spolehlivosti pracovala s myšlenkou, při které se určovala pravděpodobnost lidského selhání. Tuto pravděpodobnost ovlivňovaly externí faktory s výkonnostním vlivem, avšak hlavní pozornost byla věnována pravděpodobnosti lidského selhání. V druhé generaci těchto metod začal být přisuzován větší vliv faktorům ovlivňující výkonnost a pravděpodobnost lidského selhání se považovala za minoritní část.

Dle publikace [2] je tradiční přístup zkoumání systémů je založen na dekompozici. Systém je rozložen na části, které jsou poté analyzovány samostatně. Výsledky jednotlivých analýz poté tvoří celkový výsledek. Systém je možné tímto způsobem rozložit na funkční a fyzické části. Chování systému je tradičním přístupem zobrazováno jako samostatné události, které se dějí v čase. Každá z těchto událostí je přímým důsledkem předcházející události. Události je možné popsat jako řetězce, jež mohou vznikat kombinacemi jednotlivých událostí za použití logických hradel. Přístup dekompozice je proveditelný pouze za předpokladu, že je možné systém rozložit na komponenty, kdy každá z těchto komponent pracuje nezávisle na ostatních. Další podmínky dekompozice jsou: komponenty musí fungovat stejně samostatně i jako součást systému, komponenty a události nesmí podléhat smyčkám zpětné vazby a v neposlední řadě interakce mohou být zkoumány mezi 2 komponentami a složeny do výsledného obrazce systému.

Potřeba vytvoření nového přístupu k řešení bezpečnosti vzešla z přirozeného vývoje systémů, u kterých bylo nutné bezpečnost řešit. Při zkoumání předpokladů, podle nichž byly vytvořeny první metody hodnocení bezpečnosti pro technické systémy, bylo zjištěno, že tento přístup nelze uplatnit pro všechny typy systémů. Popisované předpoklady vychází z přístupu Safety-I. Hlavní předpoklady pro tyto metody dle [3] jsou:

- Zkoumaný systém i událost je rozložitelná do jednotlivých části, komponent nebo kroků.
- U částí a komponent může být binárně určeno, zda fungují nebo ne. Pro každou část nebo komponentu může být určena pravděpodobnost selhání.
- Pořadí událostí je předem určeno prezentací zvolené metody. Změna pořadí je možná pouze vytvořením nové prezentace metody.
- Události jsou uspořádané, lineární, mohou být popsány logickými členy a výstupy jsou úměrné vstupům událostí.

K analýze technických systémů je potřebná jejich kompletní znalost, jelikož pouze tak je možné určit vztahy a chování mezi částmi systému. Problém nastává při uvážení softwaru, jelikož jeho pochopení a vliv na ostatní části může být z pohledu provozní bezpečnosti komplexní. Dle [9] je u socio-technických systémů důležitá znalost jejich vstupů, funkcí a specifikací, avšak z důvodu proměnlivosti v čase není možné systém popsat jako čistě technický. Bezpečnostní analýzy jsou pak tvořeny s částečnou neznalostí kompletního systému, což je v rozporu s výše uvedenými předpoklady z přístupu Safety-I metod.

Dalším vývojovým krokem při pochopení katastrof či havárií v minulém století byla snaha o určení pravděpodobnosti organizační chyby nebo úrovně, při které dochází k organizačnímu

selhání [3]. Později se však ukázalo, že tento pohled není správný. Odhalení selhání u komplexnějších systémů jakým může být právě organizace je obtížnější.

Podle [3] je právě komplexita jedním z důvodu pro vytvoření nových přístupů k řešení provozní bezpečnosti dnešních systémů. Na komplexitu je možné nahlížet několika způsoby, pro účely bezpečnostních analýz představuje množství času, které je potřebné pro pochopení systému. Komplexita nepředstavuje složitost systému. Pro účely analýz dnešních systémů je často množství potřebného času nereálné, jelikož není možné v rozumném časovém horizontu pochopit chování softwaru systému v dynamickém prostředí.

1.1 Aktuálně používané systémové metody v letectví

Aktuálně používané systémové metody pro hodnocení provozní bezpečnosti komplexních systémů vychází z úsudků, které je možné označit pojmem Safety-II. Z [8] vyplývá, že pozornost je přesunuta od událostí, které se nepovedly a skončily nehodou nebo téměř nehodou na události, které se běžně daří. Výsledkem je více dat, která mohou sloužit jako podklad pro vylepšení systémů. Za příčiny nehod byly považovány selhání a poruchy, v novém přístupu je uvažováno, že úspěchy i nehody mají stejný původ. Změnil se pohled na lidi jako součásti systému, kdy dříve byli považováni za zdroje selhání, v novém pohledu představují nezbytný zdroj pro flexibilitu a odolnost systému.

Metody, které jsou aktuálně v letectví používány pro hodnocení provozní bezpečnosti komplexních systémů jsou: Metoda funkční rezonanční analýzy (FRAM, Functional Resonance Analysis Method) a metody vycházející z Modelu a procesu nehody systémové teorie (STAMP, System-Theoretic Accident Model and Process) a to Procesní analýza systémové teorie (STPA, System-Theoretic Process Analysis) a Kauzální analýza založená na systémové teorii (CAST, Causal Analysis based on Systems Theory). Model STAMP přináší nový pohled na řešení bezpečnosti, jelikož model řetězce událostí není vhodný pro analýzy komplexních systémů [6]. Model je založen na systémové teorii, pohled na bezpečnost se přesunul z pohledu spolehlivosti částí systému na jeho řízení.

Bezpečnost provozu bezpilotních systémů podléhá nařízením Evropské komise. Pro daný provoz musí být podle Článku 11 Prováděcího nařízení Komise (EU) 2019/947 posouzeno, zdali může být provoz proveden a za jakých podmínek. Pro tyto účely byla navržena metoda Posouzení rizika specifické kategorie provozu (SORA, Specific Operations Risk Assessment), jakožto přijatelný způsob průkazu. Je však zřejmé, že pro plánovaný provoz bezpilotních systémů v rámci ekosystému U-space, bude muset metoda projít revizemi.

Podle [10] U-space představuje soubor kroků a pravidel, jejichž cílem je vytvoření společného efektivního a bezpečného vzdušného prostoru pro všechny uživatele, který bude vyhovovat všem jejich potřebám. Základním kamenem je vysoká úroveň digitalizace a automatizace poskytovaných služeb, které umožní provoz velkého množství bezpilotních systémů v momentálně zřídka využitých vzdušných prostorech.

Legislativa již požadavky vycházející z postupné implementace U-space kroků zohledňuje. Metoda SORA stanovuje požadavky na provozovatele ve formě externích služeb nezbytných pro provoz bezpilotního systému, kdy se za tyto služby považuje např. GNSS nebo poskytované U-space služby.

1.2 Provozní bezpečnost UAS v odborných publikacích

Navzdory tomu, že se jedná o aktuální téma, které se teprve formuje do své finální podoby, byly již napsány odborné publikace, které se zabývají provozní bezpečností bezpilotních systémů.

Publikace [11] se zabývá posouzením aktuálních a plánovaných legislativních rámců řešící bezpečnost provozu bezpilotních systémů. V práci jsou popsány nedostatky, které znemožňují ve velké míře provoz bezpilotních letadel mimo vizuální dohled dálkově řídících pilotů (BVLOS, Beyond Visual Line of Sight Operation). Aktuálně je tento typ provozu omezen, v publikaci je vyzdvihnuto úsilí o dokončení Standardů a doporučených postupů pro BVLOS provoz, jenž začal v roce 2018 a měl být vydán v roce 2020, nový termín vydání je stanoven na rok 2023.

Problém, který provoz bezpilotních systémů z pohledu bezpečnosti představuje je jeho pozice a trajektorie letu. Jsou zřejmé faktory jako nepřesnost predikce trajektorie letu, povětrnostní podmínky, navigační chyby či chyby řízení, které více nebo méně ovlivňují výslednou pozici letadla. Cílem publikace [12] je zvýšení bezpečnosti a efektivity ve vzdušném prostoru zamýšleného pro provoz UAS a určení kritéria separace bezpilotních letadel. Publikace je rozdělena do 4 fází, které mají být dokončeny v srpnu 2022.

V publikaci [12] byly pomocí simulace Monte Carlo stanoveny bezpečnostní hranice systému založené na pravděpodobnosti rizika, uváženy byly faktory ovlivňující pozici a trajektorii bezpilotního letadla. Vstupními daty pro simulaci byly měření výkonnosti, polohy, vlastnosti řízení a palubní systém sledování letu. V simulaci byly uváženy i další vlivy jako chyba polohové systému, síla a náhodnost větru. Po vytvoření bezpečnostních hranic systému byly

stanoveny další kroky práce, určení pravděpodobnosti konfliktu, využití zpětnovazebního učení pro předcházení kolizím mezi bezpilotními letadly a závěrem vývoj rámce pro provoz s využitím generativního adversariálního strojového učení k zajištění bezpečnosti.

Publikace [13] se zabývá provozem bezpilotních systémů z pohledu hlášení incidentů a nehod. Pro společnosti v leteckém odvětví je zavedení systému řízení bezpečnosti (SMS, Safety Management System) povinné. Jedním z pilířů SMS je systém hlášení událostí. Hlášení může být na dobrovolné nebo povinné bázi a nereportují se pouze incidenty nebo nehody, ale všechny skutečnosti, které by mohly ovlivnit bezpečnost letectví. Ve společnostech spjatých s letadly s posádkou na palubě jsou data a podněty z reportingu důležitým vstupem pro proaktivní přístup k řešení provozní bezpečnosti. Dále publikace poukazuje na fakt, že stejně by tomu mělo být v provozu bezpilotních systémů. Prováděcí nařízení Komise (EU) 2019/947 stanovuje podmínky pro získání osvědčení provozovatele lehkých bezpilotních systémů (LUC, Light UAS Operator Certificate), které držiteli umožňuje schválení vlastního provozu ve specifické kategorii. Jednou z podmínek, které je nutné pro získání osvědčení splnit je implementace a spravování systému řízení bezpečnosti a jelikož rámec nedefinuje požadavky na tento systém, pak se systém musí řídit Nařízením (EU) 376/2014.

Publikace [13] popisuje skokový nárůst hlášených událostí v databázi ECCAIRS mezi lety 2015 až 2017. Hlášení jsou vkládána na úrovni členských států Evropské unie. Autoři popisují problém, který tkví v nesrovnalostech mezi hlášenými událostmi v databázi ECCAIRS a jiných statistikách. Pro příklad je uveden dokument Drone Collision Task Force Report (2016) publikovaný Evropskou agenturou pro bezpečnost letectví (EASA, European Aviation Safety Agency). V závěru dokument upozorňuje na přibližně 25 % rozdíl v hlášených událostech oproti evropské databázi. Na základě předpokladu z následujících let, autoři tvrdí, že počet hlášených událostí v databázi ECCAIRS by měl být o 30 % větší, tak aby více odpovídal skutečnému počtu hlášení.

Systémová metoda STPA byla aplikována na vzlet bezpilotního letadla s pevným křídlem v rámci Univerzity Beihang v Pekingu. Výsledkem publikace [14] byly konkrétní omezení pro specifikovaný provoz, které mají zabránit objeveným nebezpečným řídícím akcím a ztrátovým scénářům.

Publikace [15] popisuje aplikaci metody STPA pro provoz malých bezpilotních systémů. V práci jsou také zmíněna hodnocení spolehlivosti určitých modelů UAS provozu za využití metod FMEA a FTA, avšak právě nedostatek relevantních statistických dat z provozu se pro tyto metody jeví jako problém. Dále byl popsán rámec řízení rizik založený na úsudku, že nebezpečí a kauzální faktory lze odvodit z analýzy funkčních rizik (FHA, Functional Hazard Assessment), HAZOP a FMEA. Práce byla publikována v roce 2015, tudíž nezohledňuje

pravidla, která byla představena v legislativních rámcích v následujících letech, ale i tak nabízí systémový pohled na provoz bezpilotních systému. Výsledkem je identifikování 67 systémových požadavků, které autoři rozdělili mezi hlavní části systému a to: autoritu, výrobce UAS, provozovatele a řídící systém UAS.

V době tvorby této diplomové práce nebyla autorovi známa žádná publikace, která by se zabývala srovnáním cílů provozní bezpečnosti stanovené metodou SORA s požadavky stanovené metodou STPA pro předejití ztrátovým scénářům a nebezpečným řídícím akcím, ani výsledky systémové metody FRAM, ani žádného jiného využití těchto metod. Pomocí metody FRAM je možné identifikovat kritické funkce systému a zabránit jejich variabilitě. Jelikož kombinace variability ostatních funkcí by mohla vést k nežádoucímu výsledku – funkční rezonanci.

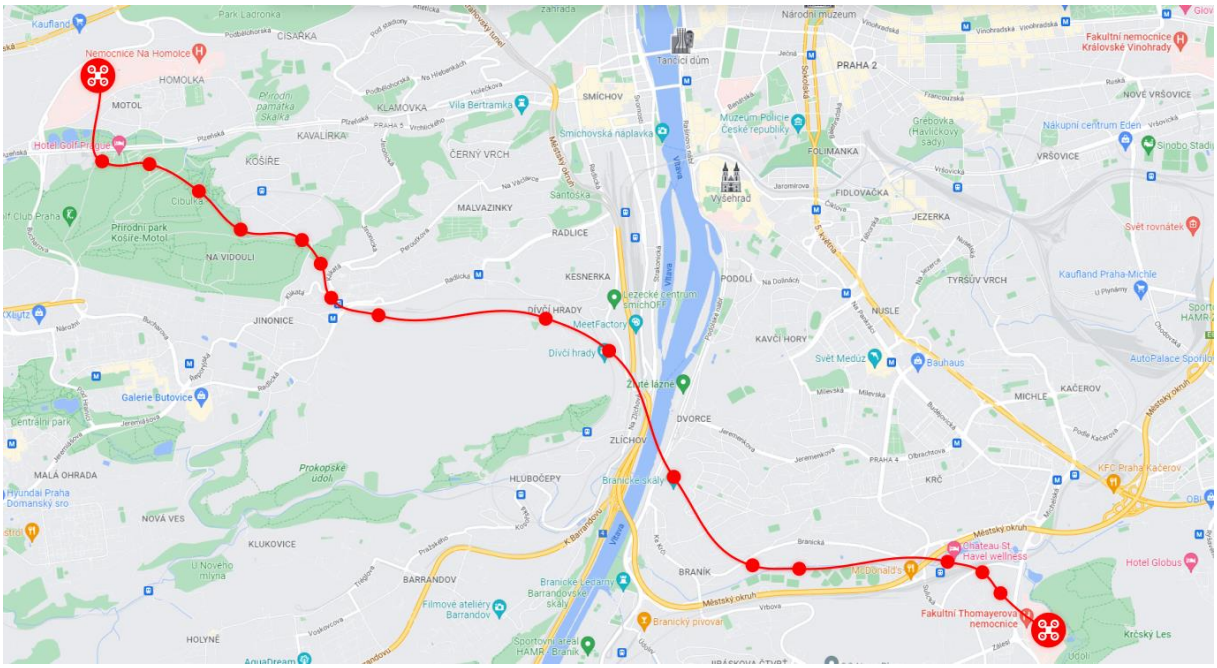
2 Výběr specifického provozu UAS pro hodnocení a tvorba konceptu provozu

Při výběru provozu bylo zvažováno několik atributů. Pro účely této práce byl vybrán komplikovaný provoz na území hlavního města Prahy. Jedná se o přepravu lékařského materiálu z areálu Thomayerovy nemocnice do Fakultní nemocnice v Motole.

Zamýšlený provoz spadá do specifické kategorie provozu. Pro schválení provozu v této kategorii je provozovatel povinen získat Oprávnění k provozu (OkP) vydané Úřadem pro civilní letectví České republiky. Součástí žádosti o OkP je zhodnocení rizik, která daný provoz představuje a návrh zmírňujících opatření pro snížení rizik na přijatelnou úroveň. K tomuto procesu je v legislativním rámci určena metoda SORA. SORA je založena na dokumentu vytvořeném uskupením JARUS [1]. Jedná se o metodu, která vede provozovatele UAS a příslušný úřad k posouzení, za jakých podmínek je provoz bezpečný a určuje potřebná zmírňující opatření za účelem snížení rizika. Je počítáno s postupnou revizí metodiky do finální podoby podle zpětné vazby získané z reálného provozu UAS.

Prvním krokem metodiky SORA je vytvoření konceptu provozu – (ConOps, Concept of Operations). Jedná se o dokument s velmi detailním popisem zamýšleného provozu. Obsahem konceptu provozu jsou veškeré informace o provozu po technické, provozní a systémové stránce.

Let je prováděn za účelem přepravy lékařského materiálu mezi nemocničními areály Thomayerovy a Fakultní nemocnice v Motole v Praze. Celý let je plánován v hlavním městě Praha, což z pohledu předpisů představuje hustě osídlený prostor. Délka zamýšlené trasy je 10890 m, oproti přímé vzdálenosti mezi nemocničními areály se jedná o navýšení o 1390 m. Letová trasa je naplánována od areálu Thomayerovy nemocnice přes Jižní spojku, trasa pokračuje nad Kunratickým potokem přes Branické skály a řeku Vltavu. Trasa dále vede nad ulicí Strakonickou, kopcem Dívčí hrady a přes čtvrť Jinonice kolem areálu Waltrovka. Závěrečná část letové trasy je vedena nad přírodním parkem Košíře – Motol, přes ulici Plzeňskou a končí nad areálem Fakultní nemocnice v Motole. Celá trasa je vyobrazena na Obrázku č. 1.



Obrázek 1: Letová trasa zamýšleného provozu

Kompletní letová trasa je umístěna v řízeném okrsku CTR Ruzyně a LKR9 Praha. Areál Thomayerovy nemocnice se částečně nachází ve vzdušném prostoru letištní provozní zóny (ATZ, Aerodrome Traffic Zone) LKTC. Provoz bezpilotních systémů v prostoru ATZ LKTC je povolen pouze se souhlasem provozovatele letiště a s koordinací s letištní službou AFIS nebo RADIO. V neposlední řadě let bezpilotního letadla zasahuje do ochranných pásem nadzemních dopravních staveb, inženýrských a telekomunikačních sítí. Provoz je uvažován v prostředí U-space a počítá se službou poskytování informací o okolním provozu (Traffic Information Service).

Zamýšlený provoz je prováděn mimo vizuální dohled dálkově řídícího pilota, jedná se tedy o provoz BVLOS a pravidla provozu jsou VFR. Let začíná z vybudované startovací plošiny v areálu Fakultní Thomayerovi nemocnice, souřadnice zamýšleného místa jsou 50°01'49.0"N 14°27'27.3"E. Uskutečnění letu je provedeno automaticky, avšak pod nepřetržitým dohledem dálkově řídícího pilota. Výška letu je stanovena na 330 ft nad úrovní země (AGL, Above Ground Level). Rychlost letu je stanovena na 20 $m \cdot s^{-1}$.

Dálkově řídící posádka je tvořena 2 pozicemi: dálkově řídícím pilotem a členem personálu. Úkolem dálkově řídícího pilota je zahájení automatického letu a poté jeho kontrola. Pilot kontroluje dodržování předdefinované letové trati, výšky a rychlosti letu. Vyhodnocuje letová data a informace z provozu, přijímá také U-space službu, jenž informuje o okolním provozu. Činnosti člena personálu jsou provedení předletové a poletové kontroly, provedení činnost

údržby a zajištění přepravovaného materiálu, čímž se rozumí fyzické upevnění k bezpilotnímu letadlu. Hmotnost přepravovaného materiálu je 1500 g. Veškerým úkonům dálkově řídící posádky předchází výcvik.

Doložený výcvik personálu je podstatnou informací, podle které příslušný úřad posuzuje žádost o OkP, avšak je také velmi důležitý pro bezpečné a zdárné provedení letu. Pro zamýšlený provoz je požadováno, aby každý člen dálkově řídící posádky absolvoval teoretický a praktický výcvik. Následně je nezbytné absolvovat pravidelná přezkoušení. Teoretický výcvik je založen na tématech uvedených v Prováděcím nařízení Komise (EU) 2019/947 [1]: bezpečnost létání, letecké předpisy, navigace, omezení lidské výkonnosti, provozní postupy, všeobecné znalosti UAS, meteorologie a postupy při pohotovostním plánu.

Praktický výcvik je prováděn za využití simulátoru. Výcvik je zaměřen na normální postupy, postupy zhodnocení podmínek prostředí před a v průběhu mise, postupy zvládání neočekávaných provozních podmínek, postupy pro nenadálé situace a nouzové postupy jako je vysazení pohonné jednotky, částečné uvolnění užitečného zatížení, selhání řídícího a kontrolního datového spoje a v neposlední řadě také postupy při nenadálých omezeních dálkově řídícího pilota jako jsou zdravotní komplikace nebo rušení nezapojenou osobou.

Člen personálu je odpovědný za provádění činností spojených s údržbou bezpilotního systému a těmto činnostem předchází teoretický a praktický výcvik. Výsledkem absolvování výcviku je oprávnění k provádění údržby UAS. Postupy údržby vychází z instrukcí a požadavků výrobce UAS a provedené úkony jsou součástí dokumentace vedené provozovatelem bezpilotního systému.

Pro provedení zamýšleného provozu byl vybrán bezpilotní systém DJI Matrice 300 RTK. Jedná se o kvadrokoptéru o délce 810 mm, šířce 670 mm a výšce 429 mm. Bezpilotní systém má elektrický pohon, jenž je napájen lithium-polymerovými (LiPol) akumulátory. Baterie má 12 článku, její napětí je 52,8 V a kapacita 5 935 mAh. Přibližná hmotnost s dvěma bateriemi TB60 je 6,3 kg a maximální vzletová hmotnost je 9 kg [16].

3 Aplikace metod pro specifický provoz UAS

Pro zamýšlený provoz, který byl detailně popsán v předchozí kapitole, musí být dle přijatelného způsobu průkazu Článku 11 Prováděcího nařízení Komise (EU) 2019/947 posouzeno, zdali může být proveden a za jakých podmínek. Pro tyto účely byla navržena metoda SORA, jakožto přijatelný způsob průkazu. Očekává se, že metoda bude v průběhu nárůstu objemu provozu specifické kategorie procházet revizemi.

Na představený provoz specifické kategorie provozu byla aplikována metoda SORA a aktuálně používané systémové metody v letectví STPA a FRAM. Výsledkem metody SORA jsou cíle provozní bezpečnosti, jenž musí žadatel zajistit ke schválení daného provozu. Metoda STPA představuje přístup k provozní bezpečnosti z pohledu řízení. Výsledkem je stanovení systémových požadavků, které mají za cíl zabránit nebezpečným řídícím akcím a scénářům, jež vedou k ztrátové události. Metoda FRAM představuje pohled na systém z pohledu jeho funkcí, díky aplikaci metody jsou identifikovány kritické funkce systému.

Poslední část této kapitoly je věnována způsobu porovnání výsledků jednotlivých metod. Výsledky obou systémových metod jsou porovnány samostatně s cíli provozní bezpečnosti, jež jsou stanoveny jako výsledek metody SORA, a ostatními požadavky, které jsou stanoveny legislativním rámcem.

3.1 Metoda SORA

Metoda SORA se skládá z 10 stanovených kroků, které jsou popsány v přijatelném způsobu průkazu (AMC) a poradenském materiálu (GM) k Článku 11 [1]. Aby bylo možné zamýšlený provoz bezpečně provést, byla definována třídy rizika ve vzduchu i na zemi a zároveň byla navržena zmírňující opatření těchto rizik. Kombinace výsledných hodnot rizik ve vzduchu a na zemi slouží jako podklad pro určení robustnosti cílů provozní bezpečnosti. Princip vyhodnocení metody vychází z bezpečnostního rizika celkového systému.

Definic rizika existuje mnoho, avšak pro účely posouzení provozní bezpečnosti bezpilotních systémů je nejvhodnější následující definice, dle které je riziko: *„riziko je kombinace frekvence (pravděpodobnosti) výskytu a související úrovně závažnosti“* [1].

Pro správné použití a pochopení metody je potřeba představit termín robustnost, kterým jsou v procesu označovány zmírňující opatření nebo cíle provozní bezpečnosti – OSO,

z anglického *Operational Safety Objectives*. Dle [1] je robustnost určena podle úrovně integrity a úrovně jistoty. Integrita představuje přírůstek bezpečnosti, která je zajištěna zmírňujícím opatřením. Jistota určuje důkaz, že bylo přírůstku bezpečnosti dosaženo. Integrita i jistota se dělí na 3 úrovně: nízkou, střední a vysokou. Obecně je možné úrovně jistoty definovat následovně: nízká úroveň jistoty je dosažena na základě prohlášení žadatele, střední úrovně jistoty je dosaženo na základě předložení podpůrného důkazu, kterým může být zkouška nebo výcvik posádky. Vysoká úroveň jistoty je dosažena pouze v případě rozhodnutí způsobilé třetí strany. Úroveň robustnosti se určuje na základě kombinace úrovní integrity a jistoty, jak je zobrazeno v Tabulce č. 1.

Tabulka 1: Určení úrovně robustnosti [1]

	Nízká jistota	**Střední jistota**	**Vysoká jistota**
Nízká integrita	Nízká robustnost	Nízká robustnost	Nízká robustnost
Střední integrita	Nízká robustnost	Střední robustnost	Střední robustnost
Vysoká integrita	Nízká robustnost	Střední robustnost	Vysoká robustnost

Krok #1 – Popis ConOps

Prvním krokem metody je vypracování konceptu provozu. Je vyžadováno, aby žadatel vytvořil dokument konceptu provozu, ve kterém uvede všechny relevantní technické, provozní a systémové informace o zamýšleném provozu. Jedná se o důležitý dokument, který slouží jako podklad pro schválení daného provozu příslušným úřadem.

Krok #2 – Určení vlastní třídy rizika na zemi GRC

V druhém kroku je nutné určit vlastní třídu rizika na zemi, neboli GRC z anglického *Ground Risk Class*. Riziko na zemi představuje situaci, při které by mohlo dojít ke srážce bezpilotního letadla s nezapojenou osobou. Postup určení GRC vychází z charakteristického rozměru bezpilotního letadla, případně očekávané typické kinetické energie a provozního scénáře. Provozní scénář je definován podle typu provozu, pod kterým se rozumí let bezpilotního letadla v nebo mimo vizuální dohled dálkově řídícího pilota (VLOS / BVLOS) a zeměpisný prostor, který představuje prostor z pohledu počtu nezapojených osob.

Tabulka 2: Určení vlastní třídy rizika na zemi [1]

Vlastní třída rizika na zemi UAS				
Max. charakteristický rozměr UAS	1 m	3 m	8 m	> 8 m
Očekávaná kinetická energie	< 700 J	< 34 kJ	< 1 084 kJ	> 1 084 kJ
Provozní scénáře				
VLOS/BVLOS nad kontrolovanou pozemní oblastí	1	2	3	4
VLOS nad řídce zalidněnou oblastí	2	3	4	5
BVLOS nad řídce zalidněnou oblastí	3	4	5	6
VLOS nad zalidněnou oblastí	4	5	6	8
BVLOS nad zalidněnou oblastí	5	6	8	10
VLOS nad shromážděním lidí	7			
BVLOS nad shromážděním lidí	8			

Při uvážení charakteristických rozměrů, očekávané typické kinetické energie a provozního scénáře vychází hodnota GRC 6.

Krok #3 – Určení konečné třídy rizika na zemi GRC

Hodnota stanovená v předchozím kroku představuje riziko pádu bezpilotního letadla a zasažení nezapojené osoby. V třetím kroku metody SORA jsou představena zmírňující opatření, která mají za cíl snížit riziko na přijatelnou úroveň. Zmírňující opatření jsou rozdělena do 3 kategorií. První kategorie M1 se zabývá snížením rizika z pohledu prostoru, ve kterém bude let prováděn. Uvažováno je s hustotou obyvatel v oblasti, horizontální vzdáleností od nezapojené osoby, ale i s ostatními faktory, jež mohou přispět nebo být příčinou havárie a to: meteorologické podmínky, reakční doba nebo výkonnost bezpilotního letadla. Kategorie M2 se zabývá opatřeními, které mají za cíl snížit následky pádu bezpilotního letadla. Poslední kategorií je M3 a je věnována pohotovostnímu plánu. Jedná se o dokument, ve kterém jsou popsány nouzové postupy v případě ztráty řízení.

Tabulka 3: Zmírňující opatření pro určení konečné třídy rizika na zemi [1]

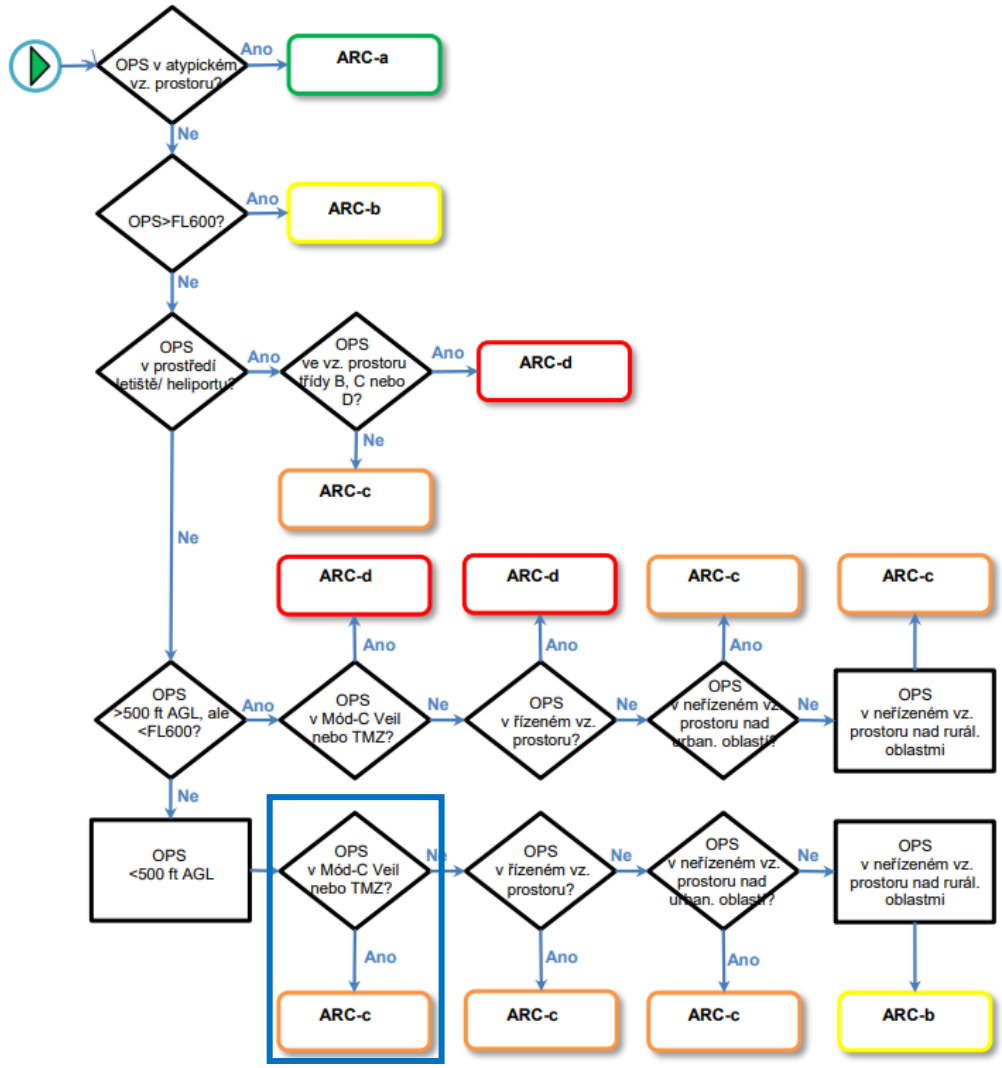
		Robustnost		
Pořadí	**Zmírňující opatření**	**Žádná/ Nízká**	**Střední**	**Vysoká**
1	M1 – Strategická zmírnění rizika na zemi	-1: Nízká	-2	-4
2	M2 – Snížení následků nárazu	0	-1	-2
3	M3 – Je zaveden pohotovostní plán (ERP), provozovatel UAS je ověřený a účinný	1	0	-1

Pro M1 byla stanovena úroveň nízké robustnosti, což má za následek snížení hodnoty GRC o 1. Letová trasa je navržena s důrazem na dodržení maximální možné vzdálenosti od nezapojených osob. Zmírňující opatření M2 jsou zřízena za účelem zmírnění následků pádu bezpilotního letadla po ztrátě řízení. Zřízeným zmírňujícím opatřením pro daný provoz je instalace padákového zařízení, které se automaticky aktivuje v případě ztráty řízení bezpilotního systému. Úroveň robustnosti pro zmírňující opatření M2 byla zvolena střední a hodnotu GRC sníží o 1. Úroveň robustnosti zmírňujících opatření M3 je určena podle zavedení pohotovostního plánu (ERP, Emergency Response Plan). Je předpokládáno, že provozovatel pro zamýšlený provoz bude disponovat ERP validovaným způsobilou třetí stranou. Pohotovostní plán by měl obsahovat postupy pro případ, kdy dojde ke ztrátě řízení bezpilotního letadla a nebude možné ovlivnit jeho trajektorii nebo místo dopadu. Je očekáváno, že ERP bude obsahovat postupy pro omezení stupňujících se následků havárie a stanovené podmínky, při kterých bude upozorněno stanoviště řízení letového provozu. Pro zamýšlený provoz je uvažováno s vysokou úrovní robustnosti a snížením GRC o 1.

Konečná hodnota GRC je po uvážení zmírňujících opatření rovna 3.

Krok #4 – Určení počáteční třídy rizika ve vzduchu ARC

V následujících dvou krocích je určena třída rizika ve vzduchu. Proces určení počáteční třídy rizika ve vzduchu ARC vychází z diagramu, který je zobrazen na Obrázku č. 2. Pomocí parametrů zamýšleného provozu byla zvolena třída rizika *ARC-c*. Obecně je tato třída definována jako vzdušný prostor, ve kterém je rostoucí riziko srážky bezpilotního letadla s letadlem s posádkou na palubě. Navržený provoz je po celou dobu letu prováděn v řízeném okrsku – CTR Ruzyně, ve kterém je vyžadováno být vybaven odpovídačem sekundárního radaru. Jedná se totiž o prostor TMZ (Transponder Mandatory Zone), kde je nutné disponovat transpondérem.



Obrázek 2: Diagram určení počáteční třídy rizika ve vzduchu [1]

Krok #5 – Použití strategických zmírňujících opatření za účelem určení zbytkové ARC

Podobně jako u třídy rizika na zemi je možné snížit i počáteční třídu rizika ve vzduchu ARC. Třída rizika ARC kvalitativně určuje pravděpodobnost setkání bezpilotního letadla s letadlem s posádkou na palubě a to od omezení letového provozu až po případnou srážku obou letadel. Pokud žadatel věří, že stanovená třída rizika se liší od reálné situace v provozním prostoru, je možné zažádat o snížení třídy rizika ARC.

Zamýšlený provoz je po celou dobu letu prováděn v řízeném okrsku CTR Ruzyně. Jedná se o vzdušný prostor, ve kterém musí být uživatelé vybaveni odpovídačem sekundárního radaru. V zamýšlené výšce letu není možné přijít do kontaktu s jiným letovým provozem vyjma zákroku letecké záchranné služby. Z tohoto důvodu je žádáno o snížení třídy rizika ve vzduchu

na *ARC-b*. V případě zásahu nebo přeletu letecké záchranné služby by byl dálkově řídící pilot informován poskytovatelem U-space služby (služba Traffic Information). Na základě této informace by přistál na nejbližším z míst určených v provozních postupech.

Krok #6 – TMPR a úrovně robustnosti

V tomto kroku jsou představena taktická zmírňující opatření - TMPR, jenž jsou zřizována za účelem zmírnění zbytkového rizika srážky bezpilotního letadla s letadlem s posádkou na palubě. Je zohledněno, zdali se jedná o provoz VLOS/EVLOS nebo BVLOS. Pro případy, kdy dálkově řídící pilot nebo pozorovatel nebude udržovat vizuální kontakt s bezpilotním letadlem je potřebné určit úroveň robustnosti podle zbytkové třídy rizika ve vzduchu.

Pro účely této práce je zbytková třída rizika na úrovni *ARC-b*, proto taktická zmírňující opatření musí být na nízké úrovni. Tato úroveň je vyžadována pro provoz ve vzdušném prostoru, ve kterém je pravděpodobnost kontaktu s jiným leteckým provozem nízká, avšak nikoli zanedbatelná. Pro zamýšlený provoz je počítáno s informováním o okolním provozu pomocí přijímané U-space služby. Vyhýbací manévry jsou založeny na rapidním sestupu do nižší výšky, kde nehrozí srážka s jiným letadlem.

Krok #7 – Určení SAIL

Akronym SAIL znamená *Specific Assurance and Integrity Level* neboli konkrétní úroveň jistoty a integrity. Na základě určení konečného GRC a zbytkového ARC, tak jak bylo provedeno v krocích 3 a 5, je možné určit hodnotu SAIL. Parametr SAIL spojuje třídy rizika na zemi a ve vzduchu podle Tabulky č. 4 a představuje úroveň důvěry, se kterou provoz bezpilotního systému zůstane pod kontrolou. Hodnota SAIL není kvantitativní vyjádření, ale odpovídá cílům provozní bezpečnosti, které jsou díky ní identifikovány v následujícím kroku.

V případě uvažovaného provozu vychází konečná GRC hodnota 3 a zbytková třída rizika ve vzduchu ARC-b. Kombinací těchto dvou hodnot se získá výsledná hodnota SAIL II.

Tabulka 4: Určení hodnoty SAIL [1]

SAIL				
	Zbytková ARC			
Konečná GRC	a	b	c	d
≤2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Certifikovaná kategorie			

Krok #8 – Identifikace cílů provozní bezpečnosti OSO

Jak bylo zmíněno v předchozím kroku, na základě určené úrovně SAIL se vyhodnotí cíle provozní bezpečnosti OSO. Vyhodnocení je provedeno podle související úrovně robustnosti. Každá úroveň SAIL představuje určité úrovně robustnosti, kterých musí být pro jednotlivé cíle provozní bezpečnosti dosaženo. [1]

„O“ značí, že splnění cíle je volitelné, „L“ značí nízkou úroveň robustnosti, „M“ značí střední úroveň robustnosti, „H“ značí vysokou úroveň robustnosti, ale ta pro žádné OSO na úrovni SAIL II není vyžadována.

Tabulka 5: Cíle provozní bezpečnosti [1]

OSO		**SAIL**
	Technické záležitosti UAS	**II**
OSO#01	Provozovatel UAS je odborně způsobilý a/nebo prověřený	L
OSO#02	UAS je vyroben odborně způsobilým a/nebo prověřeným subjektem	O
OSO#03	UAS je udržován odborně způsobilým a/nebo prověřeným subjektem	L
OSO#04	UAS je vytvořen podle úřadem uznávaných konstrukčních standardů	O
OSO#05	UAS je navržen s ohledem na bezpečnost a spolehlivost	O
OSO#06	Výkonnost C3 spojení je přiměřená danému provozu	L
OSO#07	Inspekce UAS (inspekce produktu) k zajištění souladu s ConOps	L
OSO#08	Provozní postupy jsou definovány, ověřeny a dodržovány	M
OSO#09	Dálkově řídící posádka vyškolena, výcvik je aktuální a je schopna vyřešit mimořádné situace	L
OSO#10	Bezpečné zotavení z technického problému	L
	Degradace externích systémů podporujících provoz UAS	

OSO#11	Jsou zavedeny postupy pro řešení zhoršení externích podpůrných systémů provozu UAS	M
OSO#12	UAS je navržen tak, aby se vyrovnal s degradací externích systémů podporujících provoz UAS	L
OSO#13	Externí služby podporující provoz UAS odpovídají provozu	L
	Lidská chyba	
OSO#14	Provozní postupy jsou definovány, ověřeny a dodržovány	M
OSO#15	Dálkově řídící posádka vyškolena a je schopna kontrolovat mimořádné situace, výcvik je aktuální	L
OSO#16	Spolupráce ve vícečlenné posádce	L
OSO#17	Dálkově řídící posádka je pro provoz zdravotně způsobilá	L
OSO#18	Automatická ochrana letové obálky před lidskou chybou	O
OSO#19	Bezpečné vybrání z následků lidské chyby	O
OSO#20	Bylo provedeno hodnocení lidského činitele a nalezeno vhodné rozhraní člověka a stroje (HMI) pro daný úkol	L
	Nepříznivé provozní podmínky	
OSO#21	Provozní postupy jsou definovány, ověřeny a dodržovány	M
OSO#22	Dálkově řídící posádka je vyškolena, aby identifikovala kritické podmínky prostředí a vyhnula se jim	L
OSO#23	Podmínky prostředí pro bezpečný provoz jsou definovány, změřitelné a dodržovány	L
OSO#24	UAS je navrženo a způsobilé pro nepříznivé podmínky prostředí	O

Krok #9 – Zohlednění přilehlé oblasti/vzdušného prostoru

Obsahem devátého kroku je uvážení rizik, které představuje ztráta řízení pro přilehlé oblasti a přilehlý vzdušný prostor. V případě, že bylo aplikováno zmírňující opatření M1, které snižuje riziko třídy na zemi, dle [1] je žadatel povinen splnit následující podmínky:

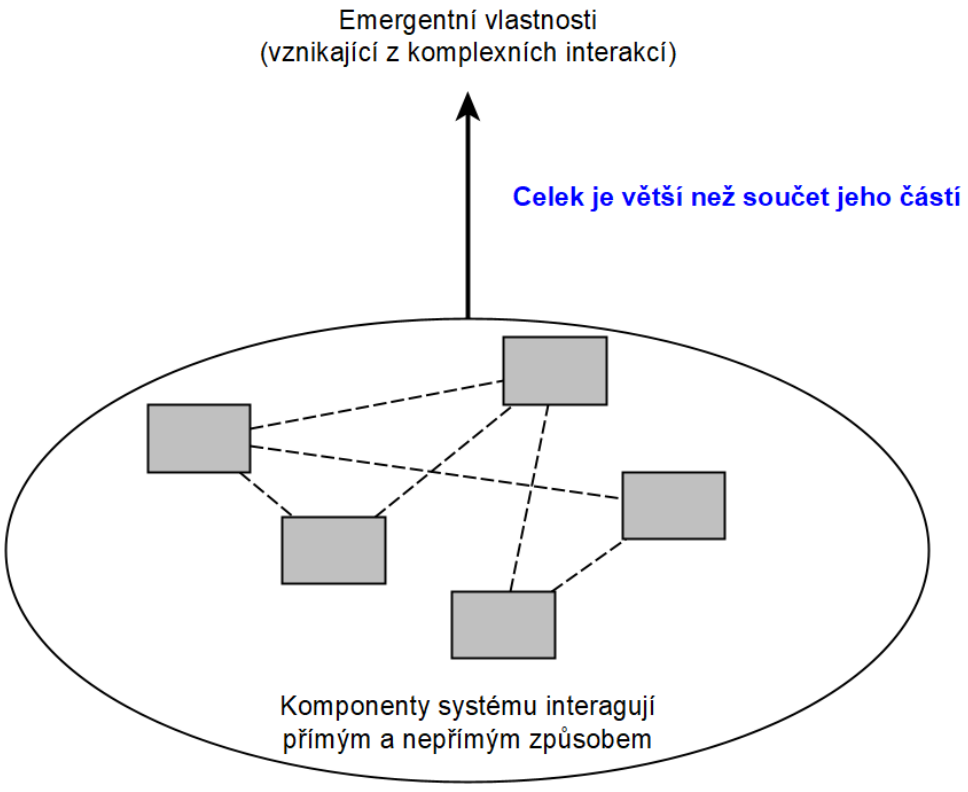
- UAS je navrženo dle standardů, které příslušný úřad považuje za vhodné;
- pravděpodobnost, při které bezpilotní letadlo opustí zamýšlený provozní prostor je menší než 10^{-4} za letovou hodinu;
- žádná závada bezpilotního systému nebo externího služby nesmí vést k provozu mimo zamýšlený provozní prostor.

Pokud je součástí systému software nebo hardware, jehož porucha by mohla způsobit porušení výše stanovených podmínek, pak musí být tato část schválena příslušným orgánem.

3.2 Metoda STPA

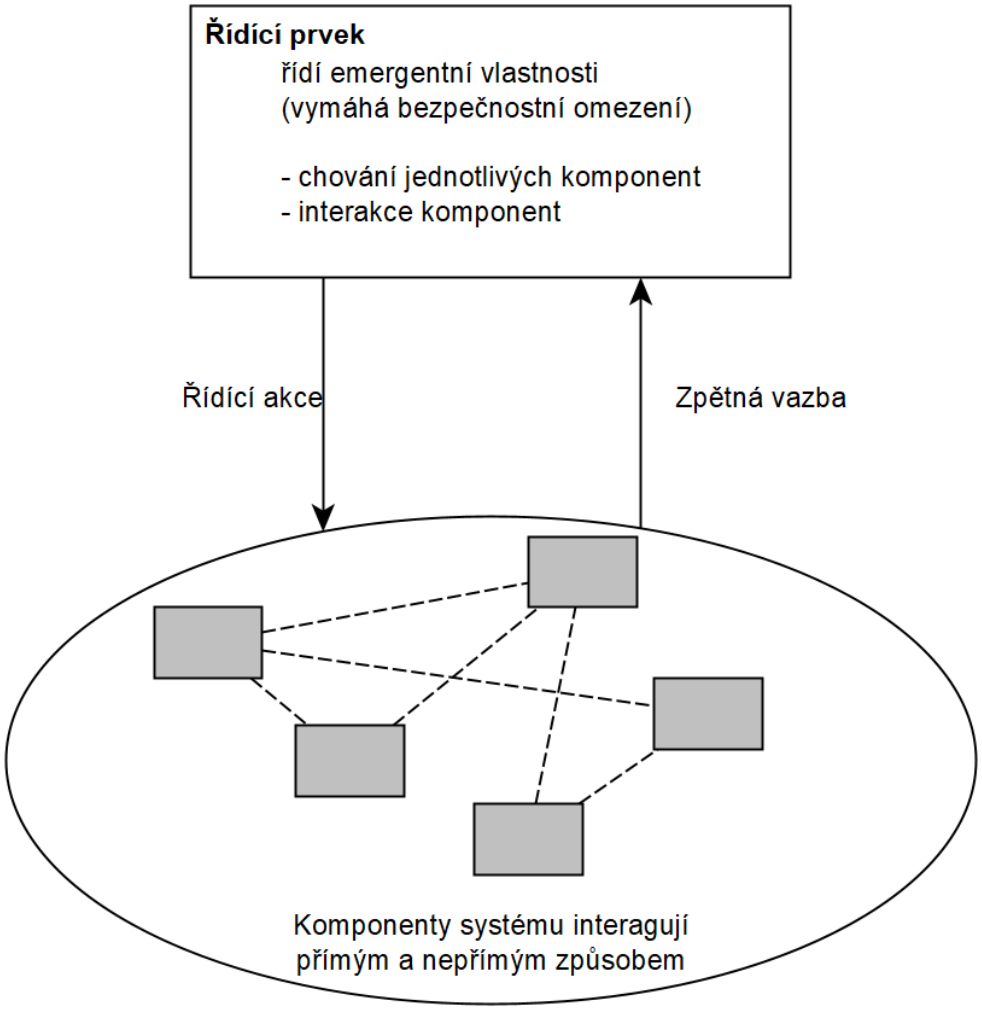
Teoretická základna metody STPA vychází z modelu STAMP. Dle [6] je STAMP označení pro rozšířený model kauzality nehod, který je použitelný pro jakýkoliv komplexní systém, jelikož jeho postup je koncipován z širšího pohledu a postupně se analyzují konkrétnější části systému. Model zohledňuje všechny části systému a to i software nebo kulturu bezpečnosti. Model STAMP byl představen profesorkou Nancy Leveson z americké univerzity MIT v roce 2012.

Model STAMP je založen na systémové teorii. Z [2] vyplývá, že systémová teorie byla vyvinuta v druhé polovině minulého století z důvodu rostoucí komplexity systémů. Tradiční přístup již nebyl dostatečný, protože nové systémy nebylo možné zkoumat pomocí dekompozice. Ze systémové teorie vychází poznatky jako je například zacházení se systémem jako s celkem. Další důležitým zjištěním je, že interakce komponent vykazuje emergentní vlastnosti. Emergence vzniká díky vzájemnému působení mezi částmi systému a nabízí nový pohled na vznik výstupu, který nemusí být vysvětlitelný jako výsledek fungování části nebo systému. Emergentní výstup vzniká na systémové úrovni a nelze jej vysvětlit jako výsledný výstup.



Obrázek 3: Emergentní vlastnosti systému [2], vlastní úprava

V publikaci [2] byla představena myšlenka přidání řídícího prvku do systému, který řídí emergentní vlastnosti systému řídícími akcemi a zároveň získává zpětnou vazbu z interakce komponent. Úkolem řídícího prvku je pak nastavení pravidel systému, která musí být dodržena za účelem zachování bezpečnosti.



Obrázek 4: Řídící prvek v systému [2], vlastní úprava

Z modelu vychází 2 nejpoužívanější nástroje a to STPA a CAST. Rozdíl mezi těmito analytickými metodami spočívá v tom, že CAST analyzuje události retrospektivně, zatímco STPA analyzuje potenciální příčiny nehod [2]. STPA je technika analýzy rizik založená na rozšířeném modelu kauzality nehod. Nehody mohou nastat selháním komponent, ale také nebezpečnou interakcí mezi částmi systému, bez toho aniž by některá část předtím selhala.

3.2.1 Definování účelu analýzy

Při tvorbě analýzy STPA je potřeba se v první řadě zamyslet, čeho by měla analýza dosáhnout, co je její účel a čemu je potřeba předejít. Z tohoto důvodu je prvním krokem určení ztrát nebo ztrátových scénářů. Ztráta podle [2] může představovat cokoliv nepřijatelného pro jakoukoliv zapojenou stranu systému. Ztráta může být materiální, finanční, ztráta reputace, zdraví nebo např. informace. Označení ztráty je ponecháno z anglického slova „*loss*".

Cílem analýzy je určit podmínky pro bezpečné provedení zamýšleného provozu. V Tabulce č. 6 jsou uvedeny všechny ztráty, kterým je nutné zabránit.

Tabulka 6: Určení ztrát

L-1:	Ztráta UAS	L-5:	Ztráta nebo poškození majetku
L-2:	Ztráta převáženého materiálu	L-6:	Ztráta akceptace veřejností
L-3:	Zranění osoby	L-7:	Ztráta mise
L-4:	Ztráta Oprávnění k provozu		

Po uvážení všech ztrát je nutné stanovit hranice systému, které určují v jakém rozsahu bude analýza provedena a co všechno bude považováno za součást systému. Další krok metody je zaměřen na určení nebezpečí na úrovni systému. Nebezpečí vychází z anglického výrazu „*hazard*". Dle [2] je definice nebezpečí následující: *Nebezpečí je stav systému nebo soubor podmínek, které spolu v kombinaci s nejhorší kombinací podmínek prostředí vedou ke ztrátě.*

Před tvorbou dalších kroků metody je vhodné uvést také definici systému dle [2]: *Systém je soubor komponent, které jednají společně jako celek, aby dosáhly společného cíle. Systém může obsahovat subsystémy a může být také součástí většího systému.*

Pro účely analýzy je příhodné u každého nebezpečí uvést k jakým ztrátám může v nejhorším případě dojít. Při analýze systému je vhodné se zaměřit na nebezpečí, která lze ovlivnit. Právě rozlišení mezi aspekty, které je možné z pohledu systému ovlivnit a těmi, které ovlivnit nelze, je hlavní pomůckou při určení ztrát a nebezpečí. Ztráta může být i z prostředí za hranicemi systému, proti tomu nebezpečí je definované pouze uvnitř systému. Zvolená nebezpečí jsou obsahem Tabulky č. 7.

Tabulka 7: Určení nebezpečí

	Nebezpečí	**Reference k ztrátám**
H-1:	Ztráta kontroly nad UAS	1,2,3,4,5,6,7
H-2:	UAS není způsobilý pro provoz	1,2,3,4,5,6,7
H-3:	Nedodržení stanovené výšky letu	1,2,3,4,5,6,7
H-4:	Nedodržení letové trajektorie	4,7
H-5:	Narušení minimální separace mezi UAS a jiným letadlem	1,2,3,4,5,6,7
H-6:	Personál není způsobilý pro provoz	1,2,3,4,5,6,7

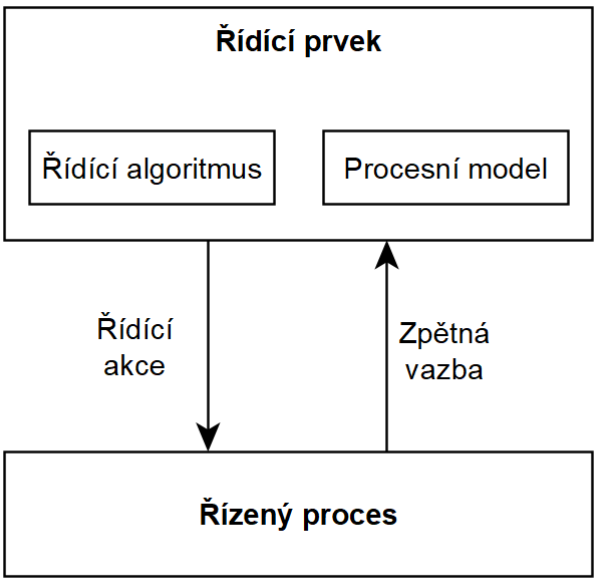
Následuje stanovení omezení na úrovni systému. Pro účely této práce se omezením rozumí: *Omezení na úrovni systému specifikuje systémové podmínky nebo chování, které je třeba splnit, aby se předešlo nebezpečí* [2]. Omezení na úrovni systému jsou určena pomocí převrácení podmínky z nebezpečí na úrovni systému. Výstupem dalších kroků analýzy je odhalení scénářů, které vedou k porušení stanovených omezení a tudíž i k nebezpečí a ztrátám.

Tabulka 8: Určení omezení na úrovni systému

	Omezení na úrovni systému	**Reference**
SC-1:	Nesmí dojít ke ztrátě kontroly nad UAS	H-1
SC-2:	UAS musí být způsobilý pro provoz	H-2
SC-3:	Musí být dodržena stanovená výška letu	H-3
SC-4:	Musí být dodržena letová trajektorie	H-4
SC-5:	Musí být dodržena minimální separace mezi UAS a jiným letadlem	H-5
SC-6:	Personál musí být způsobilý pro provoz	H-6

3.2.2 Modelování řídící struktury

Druhým krokem tvorby metody STPA je modelování řídící struktury. Jedná se o hierarchickou strukturu systému, která je tvořena řídícími a zpětnými vazbami. Tato vazba mezi dvěma částmi systému se nazývá řídící smyčka a je znázorněna na následujícím Obrázku č. 5. [2]



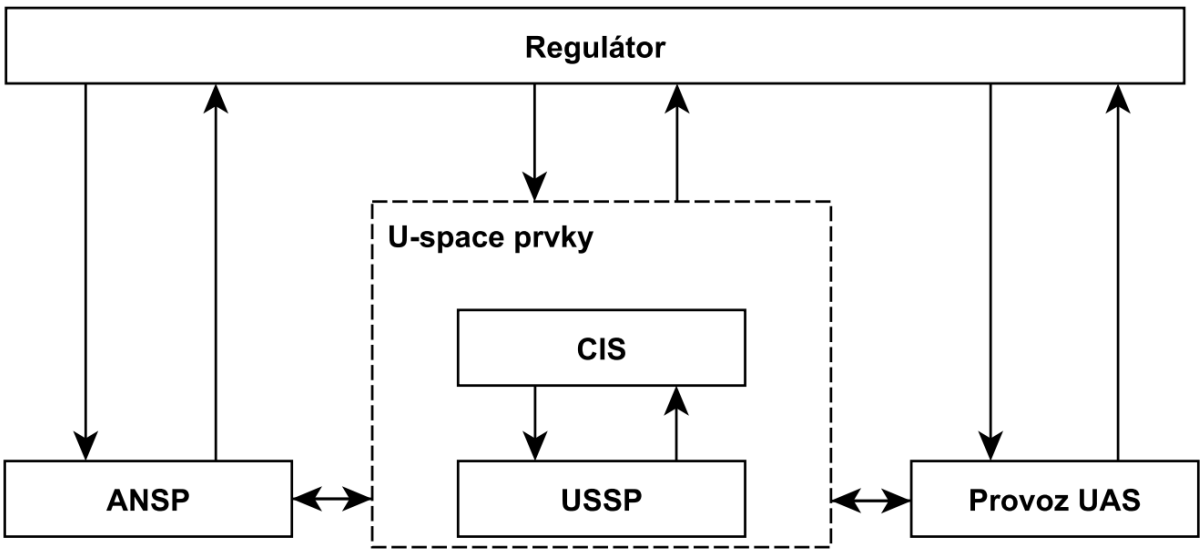
Obrázek 5: Řídící smyčka [2], vlastní úprava

Dle [2] jsou dalšími částmi řídící smyčky řídící algoritmus a procesní model. Na základě řídícího algoritmu rozhoduje řídící prvek, jakým způsobem poskytne řídící akci. Jedná se o znázornění procesu, jehož výstupem je specifická řídící akce. Procesní model představuje vnitřní přesvědčení řídícího prvku, ze kterého vychází jeho rozhodování. Zmíněné přesvědčení může být ovlivněno zpětnou vazbou, kterou řídící prvek získává, avšak existuje i možnost, že zpětná vazba bude poskytnuta v rozporu s realitou, pozdě či vůbec. V takovém případě bude rozhodování řídícího prvku negativně ovlivněno a řídící akce bude poskytnuta na základě špatného úsudku a tedy pravděpodobně špatně.

Jak bylo zmíněno výše, jedná se o hierarchickou strukturu systému. Použitý model je funkčního charakteru, nejedná se o model fyzických částí systému. Vertikální rozdělení systému znázorňuje řízení a autoritu. Prvky s nejvyšší úrovní řízení a autoritou jsou umístěny v horní části modelu a prvky s nižší úrovní jsou umístěny níže [2]. Řídící akce je znázorněna šipkou směřující dolů, zpětná vazba je znázorněna šipkou směřující nahoru.

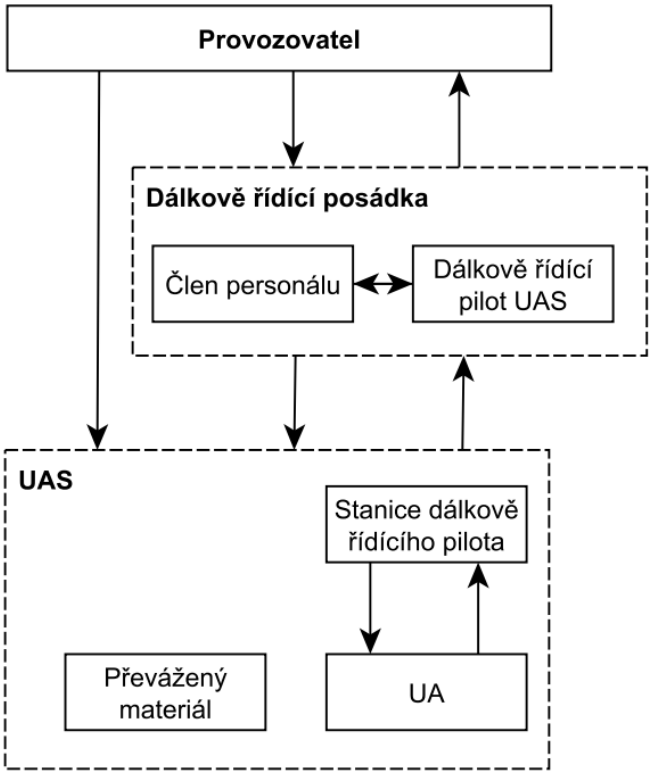
Pro modelování systému byl použit software yEd Graph Editor. Kompletní model není možné zobrazit z důvodu velikosti, tudíž je znázorněna pouze jeho kostra. Model je ve své finální podobě přiložen formou Přílohy č. 2 této diplomové práce. Kostra zamýšleného provozu je uvažována následovně. Regulátor představuje řídící autoritu. Prvkem s nejvyšší úrovní autority v zamýšleném provozu je Evropská agentura pro bezpečnost letectví EASA, která z pohledu provozu UAS tvoří harmonizovaná pravidla a certifikuje poskytovatele U-space služeb. Dalším prvkem v hierarchické struktuře jsou zástupci státu. Z pohledu regulátora

se jedná o Ministerstvo dopravy a o úroveň níže Úřad pro civilní letectví. Kostra je znázorněna na Obrázku č. 6.



Obrázek 6: Kostra zamýšleného systému

ANSP představuje Řízení letového provozu ČR, jenž v České republice poskytuje letové navigační služby letadlům s posádkou na palubě. Provoz v prostředí U-space je v systému reprezentován 2 hlavními prvky. Společná informační služba (CIS, Common Information Service) zastává funkci prvku, který je zodpovědný za výměnu dat mezi poskytovateli letových navigačních služeb a U-space služeb. Poskytovatel U-space služeb (USSP, U-space Service Provider) na základě dostupných dat poskytuje službu dle stanovených pravidel. Provoz UAS je možné blíže specifikovat dle následující struktury, jak je zobrazeno na Obrázku č. 7.



Obrázek 7: Struktura provozu UAS

3.2.3 Identifikace nebezpečných řídících akcí

Třetím krokem metody STPA je identifikace nebezpečných řídících akcí. Řídící akce vychází z řídící struktury, která byla vytvořena v předchozím kroku. V první řadě je vhodné uvést definici nebezpečné řídící akce dle [2]: *Nebezpečná řídící akce (UCA, Unsafe Control Action) je taková řídící akce, která v konkrétním kontextu a prostředí nejhoršího scénáře, povede k nebezpečí.*

Dle [2] existují 4 způsoby vzniku nebezpečné řídící akce:

- neposkytnutí řídící akce,
- poskytnutí řídící akce,
- poskytnutí řídící akce příliš brzy, příliš pozdě nebo ve špatném pořadí,
- řídící akce trvala příliš dlouho nebo byla přerušena příliš brzy.

Podstatné je uvědomění si, že řídící akce nejsou vždy nebezpečné. Pokud by byly, pravděpodobně by neměly být součástí systému. Je tedy důležité, pokud je to možné, specifikovat kontext, ve kterém může být řídící akce nebezpečná. Při procesu určování je nápomocné používat slova jako „když“, „zatímco“ nebo „během“ [2].

Nebezpečných řídících akcí bylo v analýze identifikováno celkem 131. Kompletní analýza je z důvodu obsáhlosti přiložena k diplomové práci formou Přílohy č. 1. Pro ilustraci je uvedena řídící akce *zajištění teoretického a praktického výcviku pro danou pozici* mezi provozovatelem a členem posádky.

Tabulka 9: Nebezpečné řídící akce

Řídící akce	**Neposkytnutí řídící akce**	**Poskytnutí řídící akce**	**Příliš brzy, pozdě nebo ve špatném pořadí**	**Příliš dlouho nebo přerušena příliš brzy**
Zajištění teoretického a praktického výcviku pro danou pozici	UCA-6.4.1: Teoretický nebo praktický výcvik není zajištěn před zahájením provozu [H-1, H-3, H-4, H-5, H-6]	UCA-6.4.2: Teoretický nebo praktický výcvik je při zahájení provozu nedostatečný [H-1, H-3, H-4, H-5, H-6]	UCA-6.4.3: Teoretický nebo praktický výcvik je zajištěn po zahájení provozu [H-1, H-3, H-4, H-5, H-6]	UCA-6.4.4: Teoretický nebo praktický výcvik skončí před jeho dokončením [H-1, H-3, H-4, H-5, H-6]

Nebezpečná řídící akce se dle [2] skládá až z 5 částí:

UCA-6.4.1: Provozovatel nezajistí teoretický a praktický výcvik před zahájením provozu [H-1, H-3, H-4, H-5, H-6]

ve formátu <zdroj akce> <druh akce> <řídící akce> <kontext> <odkaz na nebezpečí>

Zdroj akce představuje řídící prvek, který poskytuje řídící akci. Druh akce popisuje činnost jako poskytnutí, neposkytnutí včas, pozdě atd. Řídící akce byla určena při tvorbě řídící struktury. Kontext blíže specifikuje podmínky či prostředí, při kterých může k nebezpečné řídící akci dojít. Podmínky by měly odpovídat skutečnému stavu.

Dalším krokem je stanovení omezení řídícího prvku (C, *Controller Constraint*), které musí být dodrženo proto, aby se předešlo nebezpečné řídící akci. Definice tohoto omezení je dle [2]: *Omezení řídícího prvku upřesňuje chování, které je potřeba uspokojit pro zabránění nebezpečným řídícím akcím.*

Omezení je možné vytvořit převrácením každé nebezpečné řídící akce. Pro příklad jsou uvedeny UCA-6.4.

Tabulka 10: Nebezpečné řídící akce a omezení řídícího prvku

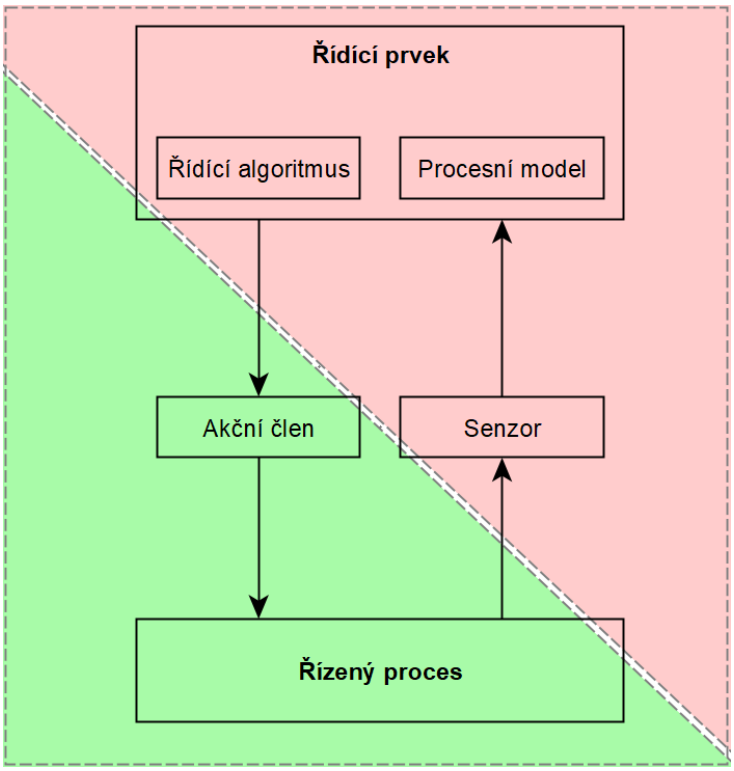
UCA	**Omezení řídícího prvku C**
UCA-6.4.1: Teoretický nebo praktický výcvik není zajištěn před zahájením provozu	C-6.4.1: Teoretický a praktický výcvik musí být zajištěn před zahájením provozu
UCA-6.4.2: Teoretický nebo praktický výcvik je při zahájení provozu nedostatečný	C-6.4.2: Teoretický a praktický výcvik musí být při zahájení provozu dostatečný
UCA-6.4.3: Teoretický nebo praktický výcvik je zajištěn po zahájení provozu	C-6.4.3: Teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu
UCA-6.4.4: Teoretický nebo praktický výcvik skončí před jeho dokončením	C-6.4.4: Teoretický a praktický výcvik nesmí skončit před jeho dokončením

3.2.4 Identifikace ztrátových scénářů

Závěrečným krokem metody STPA je identifikace ztrátových scénářů. Definice dle [2] je: *Ztrátový scénář popisuje kauzální faktory, které vedou k nebezpečné řídící akci a nebezpečí.* Profesorka Leveson ve své publikaci [2] dále představila 2 způsoby vzniku ztrátového scénáře. Určení způsobu vzniku ztrátového scénáře se zakládá na následujících otázkách:

- Proč by nebezpečná řídící akce nastala?
- Proč by byla řídící akce vykonána špatně nebo nebyla vykonána vůbec?

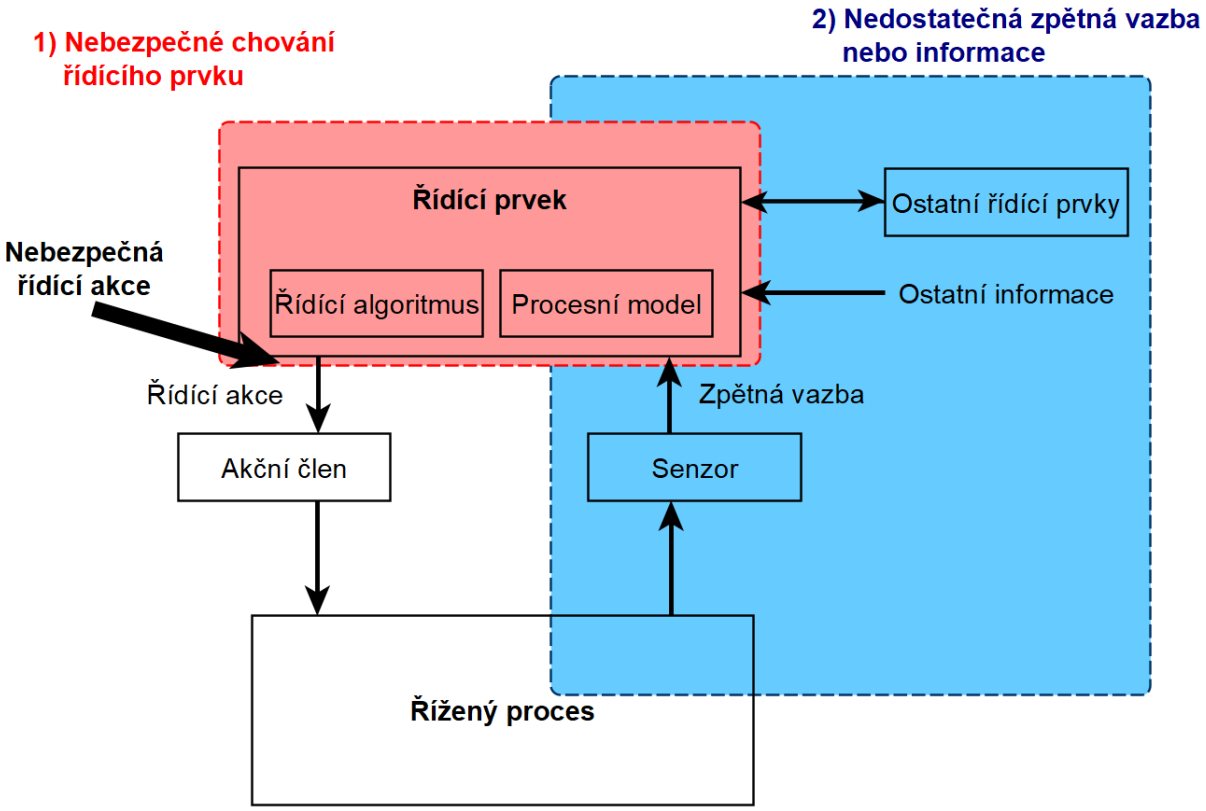
K tomu, aby mohly být otázky zodpovězeny a nalezeny tak ztrátové scénáře, je schéma modelování řídící struktury, jenž je v této diplomové práci zobrazeno na Obrázku č. 5, rozšířeno o akční člen a senzor. Akční člen je zaveden pro účely předání řídící akce od řídícího prvku k řízenému procesu. Účel senzoru je předání zpětné vazby od řízeného procesu k řídícímu prvku. Důvodem přidání těchto členů je uvážení scénářů, při kterých může ztrátový scénář nastat z důvodu jejich poruchy. Následující Obrázek č. 8 znázorňuje rozšířené schéma modelování řídící struktury, kdy růžová část struktury znázorňuje scénáře, které vychází z otázky proč by nebezpečná řídící akce nastala a zelená část struktury zobrazuje případy, které vychází z otázky proč by byla řídící akce vykonána špatně nebo nebyla vykonána vůbec.



Obrázek 8: Rozšířené schéma řídící struktury [2], vlastní úprava

Identifikace scénářů, které vedou k nebezpečné řídící akci

Prvním způsobem identifikace scénářů, které vedou k UCA je série otázek, proč by k dané nebezpečné řídící akci mohlo dojít. Při takovém postupu je nutné brát v potaz všechny faktory znázorněné na Obrázku č. 9.



Obrázek 9: Identifikace scénářů [2], vlastní úprava

Jak je znázorněno na výše uvedeném Obrázku č. 9, Dr. Leveson v publikaci [2] rozděluje tvorbu ztrátových scénářů podle nebezpečného chování řídícího prvku (1) a nedostatečné zpětné vazby nebo informace (2).

Autorka ve své publikaci [2] uvádí 4 hlavní důvody, které vysvětlují nebezpečné chování řídícího prvku a které mají za následek nebezpečnou řídící akci:

- porucha řídícího prvku,
- nesprávný řídící algoritmus,
- nebezpečný řídící vstup,
- nesprávný procesní model.

Z [2] vyplývá, že porucha řídícího prvku může nastat, pokud se jedná o fyzický prvek. Může dojít k fyzické poruše či poruše napájení apod. Nesprávný řídící algoritmus může představovat jeho chybnou implementaci nebo chybu v samotném algoritmu. Nebezpečný řídící vstup zahrnuje scénáře, ve kterých řídící prvek obdrží formou vstupu nebezpečnou řídící akci od jiného prvku. Nesprávný procesní model zahrnuje případy, ve kterých řídící prvek obdrží nesprávnou zpětnou vazbu nebo informaci, nebo obdrží správnou zpětnou vazbu či informaci

a vyhodnotí jí nesprávně případně zpětnou vazbu či informaci neobdrží nebo obdrží příliš pozdě.

Nedostačující zpětná vazba a informace může také způsobit nebezpečnou řídící akci a proto je nutné analyzovat, proč by k takové situaci mohlo dojít. Dle [2] přichází zpětná vazba k řídícímu prvku od řízeného procesu skrz senzor. Informace jsou vyměňovány mezi ostatními částmi systému, příkladem je komunikační vazba mezi řídícími prvky na stejné úrovni hierarchické struktury. Mezi nejběžnější scénáře týkající se nedostatečné zpětné vazby a informace jsou neobdržení zpětné vazby či informace a obdržení nesprávné zpětné vazby. První ze zmíněných kategorií obsahuje: odeslání zpětné vazby senzorem, avšak řídící prvek zpětnou vazbu neobdrží; zpětná vazba není odeslána senzorem nebo zpětná vazba není přijata senzorem. Případy, ve kterých je zpětná vazba či informace obdržena, avšak není správná jsou např.: senzor odešle zpětnou vazbu správně, avšak řídící prvek ji obdrží špatně nebo senzor nevhodně zareaguje na přijatou zpětnou vazbu.

Postup identifikování scénářů je znázorněn na příkladu z Přílohy č. 1. Příklad navazuje na Tabulku č. 11, ve které byly identifikovány nebezpečné řídící akce.

Tabulka 11: Ztrátové scénáře a systémové požadavky

UCA	**Scénář**	**Požadavek**
UCA-6.4: Provozovatel UAS nezajistí teoretický a praktický výcvik před zahájením provozu, nebo je teoretický a praktický výcvik při zahájení provozu nedostatečný, nebo je teoretický a praktický výcvik zajištěn po zahájení provozu, nebo teoretický a praktický výcvik skončí před jeho dokončením, protože	-Nepovažuje výcvik za důležitý -Nemá znalosti nebo prostředky k zajištění výcviku pro danou misi -Poskytnutý výcvik není pro danou misi dostatečný	-Provozovatel musí považovat výcvik za důležitý -Provozovatel UAS musí mít znalosti i prostředky k zajištění výcviku pro danou misi -Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi

Celkem bylo identifikováno 131 omezení řídících prvků a 100 systémových požadavků. Pro ilustraci jsou některé z nich zobrazeny v Tabulce č. 12. Všechny požadavky a omezení jsou s ostatními kroky metody STPA přiloženy formou Přílohy č. 1.

Tabulka 12: Ukázka omezení řídících prvků a systémových požadavků

Omezení řídicích prvků	Systémové požadavky
- Teoretický nebo praktický výcvik musí být zajištěn před zahájením provozu - Teoretický a praktický výcvik musí být dostatečný při zahájení provozu - Teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu - Teoretický a praktický výcvik nesmí skončit před jeho dokončením	- Provozovatel UAS musí považovat praktický a teoretický výcvik za důležitý - Provozovatel UAS musí mít znalosti i prostředky k zajištění praktického a teoretického výcviku pro danou misi - Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi
- Požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány - Požadované znalosti a výcvik musí být průběhu provozu úplně periodicky kontrolovány	- Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - Provozovatel UAS si musí uvědomovat vážnost mise a zodpovědnost za ní - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky
- Postupy koordinace vícečlenné posádky musí být stanoveny před zahájením provozu - Postupy koordinace vícečlenné posádky musí být stanoveny úplně před zahájením provozu - Postupy koordinace vícečlenné posádky nesmí být stanoveny po zahájení provozu	- Provozovatel UAS musí znát své povinnosti - Provozovatel UAS musí být obeznámen s problematikou bezpilotního létání - Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou
- Data v UA musí být před zahájením provozu aktualizována - Data v UA musí být před zahájením provozu kompletně aktualizována - Data v UA nesmí být aktualizována po zahájení provozu	- Provozovatel UAS musí vědět, jak správně aktualizovat data v UA - Provozovatel UAS musí si uvědomovat vážnost aktualizace dat v UA - Provozovatel UAS musí být obeznámen se zodpovědností za provoz
- Provozní postupy musí být stanoveny před zahájením provozu - Provozní postupy musí být stanoveny úplně před zahájením provozu - Provozní postupy nesmí být stanoveny po zahájení provozu	- Provoz musí být kompletně definován - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů
- U-space služby musí být v průběhu provozu poskytovány - U-space služby musí být v průběhu provozu poskytovány úplně - U-space služby nesmí být poskytovány pozdě - Poskytování U-space služeb nesmí v průběhu provozu přestat	- Musí být definován rámec, který vymezuje rozsah poskytování U-space služeb - Poskytování U-space služeb musí být kontrolováno - Musí být definován rámec, podle kterého je kontrolováno plnění závazků USSP
- Předletová a poletová kontrola musí být provedena - Předletová a poletová kontrola musí být provedena úplně - Předletová a poletová kontrola nesmí být provedeny pozdě	- Provedení předletové kontroly musí být obsahem práce personálu - Práce personálu musí obsahovat kompletní předletovou kontrolu - Musí být schopen provést předletovou kontrolu správně a kompletně
- Řídící pokyny pro pohyb UA musí být v průběhu provozu provedeny - Řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny špatně - Řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny pozdě - Provádění řídících pokynů pro pohyb UA nesmí v průběhu provozu přestat	- Pilotní výcvik musí být dostatečný pro daný provoz - Nesmí dojít ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - V průběhu mise dálkově řídící pilot musí být neustále schopen provádět řídící pokyny
- Nastavení UAS a kontrola funkčnosti musí být provedena před zahájením provozu - Nastavení UAS a kontrola funkčnosti nesmí být provedena špatně před zahájením provozu - Nastavení UAS a kontrola funkčnosti nesmí být provedeno po zahájení provozu	- Dálkově řídící pilot musí disponovat výcvikem a znalostmi k nastavení UAS a kontrole funkčnosti - Provedení nastavení UAS a kontrola funkčnosti musí být obsahem práce pilota
- Informace z poskytované U-space služby musí být v průběhu provozu vyhodnocena - Informace z poskytované U-space služby nesmí být v průběhu provozu vyhodnocena špatně - Informace z poskytované U-space služby nesmí být vyhodnocena pozdě	- Dálkově řídící pilot musí mít výcvik k vyhodnocení informace z poskytované U-space služby - U-space služba musí být poskytována správně a včas
- Činnost podle řídících signálů musí být v průběhu provozu provedena - Činnost podle řídících signálů nesmí být v průběhu provozu provedena špatně - Činnost podle řídících signálů nesmí být provedena pozdě - Provádění činnosti podle řídících signálu nesmí v průběhu provozu přestat	- Nesmí dojít ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - Pohyby UA musí odpovídat řídícím signálům stanice dálkově řídícího pilota - Stanice dálkově řídícího pilota nesmí přestat vysílat řídící signály v průběhu provozu
- U-space služby musí být v průběhu provozu přijímány nebo zobrazovány - U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány neúplně - U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány pozdě - Přijímání nebo zobrazování U-space služeb nesmí v průběhu provozu přestat	- Stanice dálkově řídícího pilota musí být schopna přijímat a zobrazovat U-space služby v průběhu provozu

3.3 Metoda FRAM

Tradiční přístup popisu systému je založen na jeho dekompozici. Pokud je to možné, systém je rozložen na části či komponenty a ty jsou následně zkoumány a popisovány. Zohledněno by mělo být, jakým způsobem jsou části systému propojeny a jak interagují. Nevýhoda tohoto přístupu je, že analýza samostatných komponent nezohledňuje vlastnosti, které se dají popsat zkoumáním širších souvislostí částí systému. [9]

Profesor Hollnagel ve své publikaci [3] představil jiný způsob popisu systému. Tento přístup je založen na popisu funkcí, pozornost je věnována fungování systému. Jedná se o pohled, při kterém nezáleží na tom, o jakou část se jedná, ale spíše o její funkci. Může se jednat o funkci stroje, člověka nebo organizace. Systém je pak souhrn vzájemně propojených nebo závislých funkcí.

Jeví se, že pohled na systém z hlediska jeho funkcí namísto jeho částí je validní. Pokud bychom chtěli systém analyzovat tímto způsobem, namísto popisu jednotlivých částí systému, budou popsány všechny jeho funkce. Na funkci systému je poté možné nahlížet z pohledu jejího výstupu. Výstup funkce je proměnný v závislosti na podmínkách a to jak interního, tak externího charakteru. Tuto vlastnost je možné pozorovat u všech funkcí a nazývá se variabilita. [3] Záměrem metody FRAM je zjistit, jak velká musí být variabilita funkce, aby již tato funkce nebyla schopna poskytovat požadovaný výstup.

FRAM byl vyvinut za účelem poskytnutí metody, která bude zkoumat systémy při jejich každodenních aktivitách. Nejedná se tedy o metodu, která by byla zaměřena na neúspěchy, ale spíše na každodenní úspěchy. Metodu je možné aplikovat na události retrospektivně i prospektivně. FRAM vychází ze 4 pilířů [3]:

- Selhání a úspěchy mají stejný způsob vzniku.
- Každodenní výkonnost lidí i socio-technických systémů jako celků se vždy přizpůsobí podmínkám.
- Na výstupy musí být nahlíženo spíše jako na emergentní než na výsledné.
- Vztahy a závislosti mezi funkcemi systému se vyvíjí v závislosti na dané situaci a tak k nim musí být přistupováno, nejedná se o předem určená spojení.

Každý ze zmíněných pilířů metody FRAM bude blíže specifikován v následující části diplomové práce.

Ekvivalence selhání a úspěchů

Dle [3] první pilíř metody FRAM popisuje ekvivalenci selhání a úspěchu, přičemž tato ekvivalence vychází ze stejného původu. Jinými slovy, na selhání a úspěch je potřeba se dívat jako na stejnou věc z pohledu jejich původu. Na počátku každého záměru je záminka provést určitou činnost správně a to platí i pro případy neblahých činností, jelikož i ty se člověk snaží provést správně. Určení, zdali činnost skončila úspěchem nebo selháním je možné provést až po tom, co je znám výsledek této činnosti. Rozdíl oproti tradičním přístupům k řešení provozní bezpečnosti je ten, že veškerá energie byla soustředěna na pochopení skutečnosti, proč se daná věc nebo aktivita nepovedla. Žádná energie nebyla věnována každodenním věcem, které se daří. Profesor Hollnagel ve své publikaci [3] zmiňuje myšlenku fyzika Ernsta Macha, která pilíř ekvivalence podporuje: „*znalosti a omyly plynou ze stejných duševních zdrojů, pouze úspěch může rozlišit jedno od druhého*“.

Přizpůsobení se podmínkám

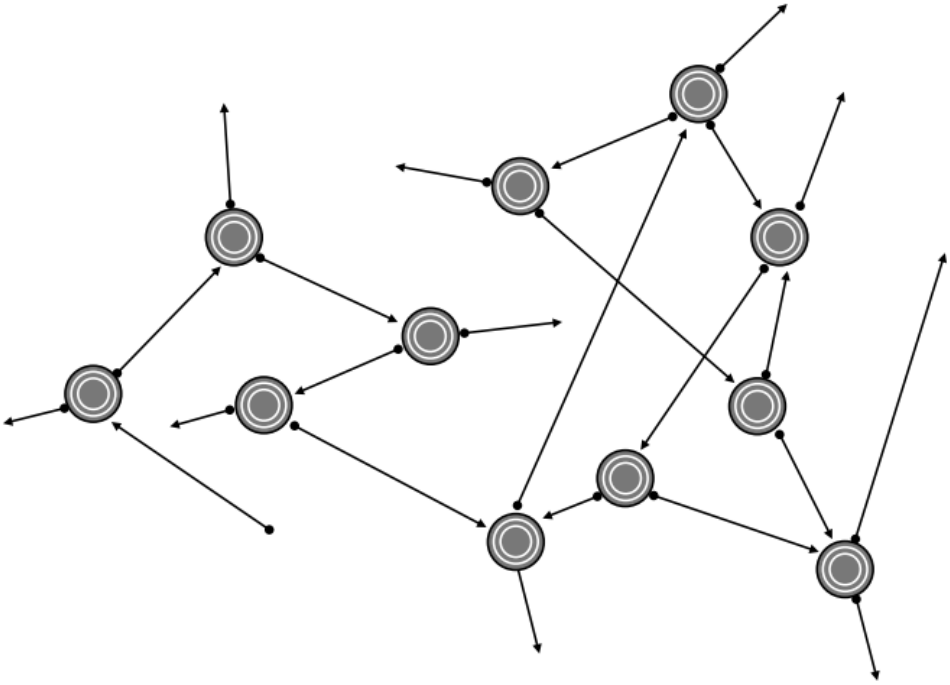
Druhý pilíř popisuje adaptabilitu výkonnosti podmínkám prostředí. Primárně se jedná o výkonnost lidskou, avšak i organizační výkonnost je proměnlivá hned z několika důvodu. Při bližším pohledu na lidskou výkonnost je možné určit několik faktorů, které na ni mají přímý vliv. Tyto faktory se dají dále kategorizovat. Profesor Hollnagel na ně v [3] pohlíží jako na interní a externí. Interní faktory představují fyziologické a psychologické vlastnosti jedince, jelikož mají přímý vliv na lidskou výkonnost. Příklady těchto faktorů je únava ve smyslu reakce organismu na nedostatek spánku nebo cirkadiánní rytmus. Pokud to pracovní podmínky dovolí, měla by být těmto faktorům věnována pozornost. Další kategorií interních faktorů jsou psychologické jevy, jako je vynalézavost, kreativita či schopnost se přizpůsobit. Za pomoci těchto vlastností může jedinec vyřešit určitý problém. V neposlední řadě by měly být uváženo očekávání, které mají lidé vůči sami sobě i ostatním. Mezi externí vlivy se řadí podmínky na pracovišti, jelikož lidé jsou citliví na celou řadu faktorů, příkladem mohou být výkyvy teplot nebo zvýšená hladinu hluku. Faktorem může být také změna pracoviště či pracovních kolegů.

Výkonnost organizace je také proměnlivá, jelikož jsou její součástí lidé. Mezi další faktory mohou patřit interní procesy, organizační kultura nebo nedostatek důvěry mezi spolupracovníky [3].

Přizpůsobování se podmínkám je přirozenou lidskou vlastností a často se jedná o důvod, proč se určité věci v systémech dějí, tak jak mají.

Emergence

Třetím pilířem, na kterém je postavena metoda FRAM se zabývá emergencí. Emergence je vlastnost výstupu funkce. Výstup je označován za výsledný z anglického *resultant*, pokud lze dohledat a určit, co jej zapříčinilo, či jaké kroky k němu vedly. Emergentní výstup tímto způsobem není možné objasnit. Neznamená to, že výstup funkce by nebyl plnohodnotný nebo trvalý, ale jde o způsob jeho vzniku. Emergentní výstup může vzniknout za určitých kombinací podmínek v systému, tyto kombinace představují vzorce specifických podmínek, které mohly existovat pouze v jednom okamžiku. Z tohoto důvodu není možné dohledat příčiny vzniku emergentního výstupu. S touto vlastností výstupu se setkáváme stále častěji u moderních systémů. [9] Na obrázku je zobrazen vzorec podmínek pro vznik emergentního výstupu.



Obrázek 10: Znázornění emergence [9]

Rezonance

Poslední pilíř metody FRAM se zabývá funkční rezonancí. Jak bylo zmíněno výše, přizpůsobení se okolním podmínkám je přirozená vlastnost socio-technických systémů a přispívá k tomu, že se skutečnosti dějí, tak jak mají. Tato vlastnost se nazývá variabilita výkonnosti. Nemusí se nijak projevovat a může být i nedetekovatelná. Stochastická rezonance ji popisuje jako náhodný šum. Profesor Hollnagel však ve své publikaci [3] představil pojem

funkční rezonance, jelikož tvrdí, že variabilita výkonnosti v socio-technických systémech není náhodná.

Čtvrtý pilíř souvisí také s výskytem emergentních výstupů, které není možné vysvětlit pomocí tradičního přístupu. Funkční rezonance nabízí nástroj, který dokáže vznik emergentních výstupů komplexních socio-technických systémů vysvětlit.

3.3.1 Kombinace Abstraktní hierarchie a metody FRAM

Výzkumný tým pod vedením doktora Riccarda Patriarca z Univerzity La Sapienza v Římě a švédské Lundské univerzity vytvořil publikaci, již zkoumá přínosy plynoucí z kombinace přístupu Abstraktní hierarchie představené profesorem Jensem Rasmussenem a systémového přístupu metody FRAM.

Abstraktní hierarchie je přístup, který v roce 1986 představil profesor Rasmussen. Dle [7] bylo využití tohoto přístupu zamýšleno pro socio-technické systémy a hlavní využití našel v jaderné energetice. Využívali je systémoví inženýři pro systémy kontroly chodu elektráren kvůli snaze zlepšit spolehlivost interakce člověka a stroje po havárii elektrárny Three Mile Island. Přístup je založen na strukturování zkoumaného systému. Vypořádání se s komplexitou vyžaduje strukturování situací. Z tohoto důvodu je výhodnější analyzovat různé úrovně systému, což umožňuje různé reprezentace znalostí.

Profesor Rasmussen ve své publikaci [7] definoval dvourozměrnou strukturu, kdy první část představuje dekompozici systému na:

- celý systém;
- subsystémy;
- funkční části;
- sestavy;
- komponenty.

Druhý rozměr představuje úrovně abstrakce. Tyto úrovně byly definovány:

- funkční účel: zamýšlený funkční účinek systému;
- abstraktní funkce: celková funkce systému reprezentovaného kauzální sítí;
- zobecněná funkce: zobecněné procesy systému, které zohledňují funkční strukturu;
- fyzická funkce: konkrétní interakce částí systémů a jejich komponent;
- fyzická forma: fyzický popis konkrétních objektů v systému.

Rozdělení systému do těchto úrovní pomáhá k pochopení chování a vztahů mezi jeho částmi v různých úrovních abstrakce. Počet úrovní není pevně stanoven a liší se podle typu systému a cíle analýzy.

V minulosti bylo publikováno několik prací, které vyzdvihovaly hierarchické funkční modelování systémů za účelem proaktivního řízení rizik a provozní bezpečnosti. Abstraktní hierarchie byla použita v několika v analýzách provozní bezpečnosti a to v kombinaci s Bayesovskou sítí nebo s Barevnou Petriho sítí [4]. Důležitým poznatkem však je, že práce vycházely z předpokladu dekompozice, jenž je založena na lineárních vztazích mezi funkcemi systému. V těchto přístupech nelze efektivně popsat úzké propojení částí systémů. Po teoretické stránce Abstraktní hierarchie považuje funkce za složité a úzce propojené, což je v rozporu s přístupem lineárních vztahů.

Vyjma publikace [4], jejímž autorem je doktor Patriarca a jeho tým, není vytvořena systémová metoda, která by vycházela z předpokladů Safety-II a kombinovala by prvky Abstraktní hierarchie. Metoda FRAM ve svém tradičním přístupu nerozděluje systém do jednotlivých úrovní či vrstev.

V publikaci doktora Patriarca jsou z Abstraktní hierarchie převzaty definované úrovně abstrakce. Úrovně dekompozice nejsou použity z důvodu charakteru zkoumaných socio-technických systémů. Místo přístupu dekompozice je systém znázorněn z pohledu zapojených subjektů, které společně tvoří kompletní systém. V publikaci [4] se tyto subjekty označují jako *agenti* a pro účely této diplomové práce je toto označení zachováno. Každý z agentů má své vlastní cíle a funkční účel, kterého chce dosáhnout. Pod pojmem agent je možné si z pohledu systému představit kohokoliv od zapojených organizací až po operátora vykonávající specifickou činnost. Propojení mezi těmito agenty je komplexnější než fyzická dekompozice a nemůže být popsáno pouze pomocí úrovní abstrakce. Přístup, který doktor Patriarca představil je dvojrozměrný systémový model, jenž propojuje úrovně abstrakce a jednotlivé agenty. Počet úrovní abstrakce není pevně stanovený a záleží na účelu tvořené analýzy.

Cílem metody FRAM je vytvořit reprezentaci systému, která zobrazuje, jak se události skutečně dějí na denní bázi. Metoda nepracuje s žádnými předpoklady o struktuře zkoumaného systému, ani o možných vztazích příčiny a následku. Bez toho, aby byl tento přístup narušen, je možné dle [4] definovat 4 úrovně abstrakce, které jsou kompatibilní s Abstraktní hierarchií profesora Rasmussena. Tyto úrovně abstrakce jsou: funkční účel, zobecněné funkce, fyzické funkce a fyzická a technologická forma.

Podle publikace [4] je první úrovní abstrakce funkční účel. Jedná se o výslednou funkci, které chce agent docílit. Druhá úroveň abstrakce nabízí detailnější pohled na agentovy funkce,

jejichž cíl je eventuálně dosáhnout výsledné funkce. Úroveň fyzických funkcí vychází z technologických komponent systému, které jsou nezbytné k implementaci funkcí na vyšší úrovni abstrakce. Poslední zvolená úroveň představuje fyzickou a technologickou formu, která představuje funkce popisující komponenty a zařízení systému z pohledu jejich fungování a uspořádání.

Pro zvolený systém byli zvoleni následující agenti: EASA, ÚCL, Provozovatel, USSP, Pilot, CIS, ATSP a ANSP. Pro analýzu systému byly použity 3 úrovně abstrakce: funkční účel, zobecněné a fyzické funkce. Úroveň fyzické a technologické formy nebyla pro účely této diplomové práce využita. Následující Tabulka č. 13 zobrazuje, jaké úrovně abstrakce byly u jednotlivých agentů popsány.

Tabulka 13: Popsané úrovně abstrakce

Agent / Abstrakce	EASA	ÚCL	Provozovatel	USSP	Pilot	CIS	ATSP	ANSP
Funkční účel								
Zobecněné funkce								
Fyzické funkce								

Dvojrozměrný rámec napomáhá k získání kompletní představy o tom, jaké činnosti vykonávají různí agenti na různých úrovních abstrakce. Systémové struktuře nejsou přidány žádné předpoklady nebo domněnky o agendách jednotlivých agentů. Každá úroveň abstrakce by měla popisovat stejnou činnost agenta jako úroveň vyšší, avšak v detailnějším pohledu. Použití popisované kombinace lze bez výhrad použít pro další kroky tvoření FRAM metody.

Pro další kroky vypracování metody FRAM byla zvolena jedna úroveň abstrakce pro funkční reprezentaci analyzovaného systému a to úroveň fyzických funkcí. V první řadě je však potřeba analyzovat zvolený specifický provoz UAS. Pro jednotlivé úrovně abstrakce byly zvoleny funkce potřebné k provedení zamýšleného letu. Jednotlivé funkce jsou zobrazeny v následující tabulce. Z důvodu rozměrů Tabulky č. 15 nejsou uvedeni všichni agenti a jejich funkční účel, konkrétně se jedná o:

Tabulka 14: Agenti a jejich funkční účel

Agent	Funkční účel
CIS	Zajistit výměnu a sdílení dat
ATSP	Poskytovat data o provozu letadel s posádkou na palubě
ANSP	Bezpečně a efektivně řídit letový provoz

Tabulka 15: Funkce jednotlivých agentů podle úrovně abstrakce

Agent/ Abstrakce	**EASA**	**ÚCL**	**Provozovatel**	**USSP**	**Pilot**
Funkční účel	-Vytvořit prostředí pro bezpečný a efektivní provoz UAS	-Zajistit bezpečný a efektivní provoz UAS v České republice	-Zajistit bezpečné dosažení cíle mise v souladu s nastavenými pravidly	-Poskytovat U-space službu dle svých závazků	-Zajistit bezpečný průběh letu
Zobecněné funkce	-Vytvořit harmonizovaná pravidla pro provoz UAS v členských státech	-Stanovit pravidla provozu UAS v České republice	-Splnit povinnosti provozovatele	-Splnit certifikaci poskytovatele U-space služeb -Plnit své závazky vůči zákazníkům podle stanovených pravidel	-Splnit certifikaci dálkově řídícího pilota dle ÚCL -Provádět své činnosti v souladu s provozními postupy a stanovenými pravidly
Fyzické funkce	-Publikovat jednotná pravidla pro provoz UAS a jejich výklad	-Dohlížet na dodržování pravidel -Certifikovat zapojený subjekt -Registrovat provozovatele -Posuzovat žádosti o Oprávnění k provozu -Publikovat pravidla pro poskytování U-space služeb	-Zajistit teoretický a praktický výcvik posádky -Stanovit postupy koordinace vícečlenné posádky -Stanovit provozní postupy -Získat Oprávnění k provozu	-Vyhodnotit přijímaná data -Poskytovat specifickou U-space službu dle stanovených pravidel	-Zahájit let -Převzít kontrolu nad automatickým letem -Komunikovat s ostatními členy personálu -Vyhodnocovat informace ze služeb U-space -Vyhodnocovat informace z provozu UA -Zajistit provozuschopný stav UA

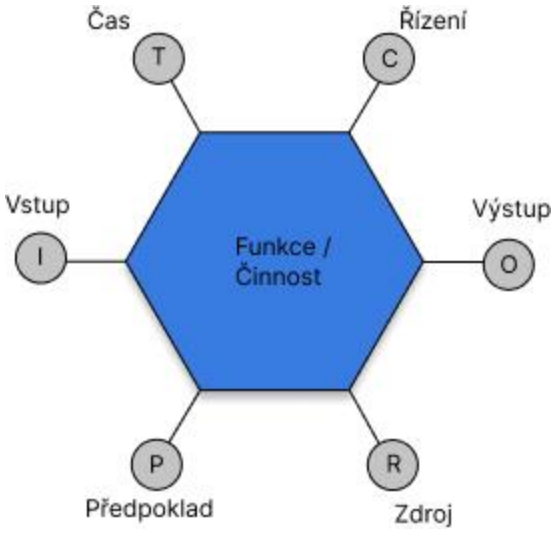
3.3.2 Identifikace a popis funkcí systému

Metoda FRAM je rozdělena do 4 kroků. Prvním krokem je identifikace a popis funkcí systému, které jsou potřeba pro splnění každodenní práce. Cílem tohoto kroku je detailní popis, jak probíhá každodenní aktivita. Podstatná část tohoto kroku byla provedena v předchozí části a pro další kroky tvoření metody FRAM je pracováno s abstrakcí na úrovni fyzických funkcí. Tato úroveň popisuje systém v nejvhodnějším detailu pro účely této diplomové práce. Po identifikování a popisu všech funkcí je vytvořen model systému. Pro tyto účely je k dispozici software FRAM Model Visualizer (FMV). Pomocí tohoto softwaru byl vytvořen model zkoumané úrovně abstrakce systému.

Před zahájením modelování systému je důležité se seznámit s grafickým zobrazením funkce. Funkce je zobrazena hexagonem, kde každý roh představuje 1 z 6 aspektů funkce. Pro účely modelování a dalších kroků tvoření by funkce měla být sloveso a aspekt podstatné jméno. Není stanoveno, kolik a jaké aspekty by měla jednotlivá funkce mít definovaných, avšak je důležité si uvědomit, že jakýkoliv aspekt kromě výstupu je výstup jiné funkce. Pokud má funkce definovaný pouze výstup, jedná se o tzv. *background* funkci a představuje určitou hranici systému, všechny ostatní funkce jsou pak označovány jako *foreground* funkce [3].

Ve vytvořeném modelu této diplomové práci jsou *background* funkce: *Publikovat jednotná pravidla a jejich výklad* a *Publikovat pravidla pro poskytování jakýchkoliv služeb*. Pro zamýšlený provoz tyto funkce představují hranice systému.

Obrázek č. 11 zobrazuje funkci v podobě hexagonu, celkem je definováno 6 různých aspektů funkce:



Obrázek 11: Funkce a její aspekty [5], vlastní úprava

Následující část textu popisuje dle [3] jednotlivé aspekty funkce, jakým způsobem jsou funkce propojeny a uspořádány.

Vstup (I, Input)

Vstup funkce je obecně definován jako něco, co je použito nebo transformováno funkcí pro získání výstupu. Vstupem funkce může být energie, informace nebo hmotná věc [3]. Z pohledu metody FRAM představuje vstup to, co aktivuje nebo spustí danou funkci. V tomto případě může vstup představovat povolení, odbavení, pokyn nebo příkaz k provedení určité akce. Obecně lze tedy říct, že vstup je změna stavu, který je funkcí rozpoznán jako podnět k zahájení funkce.

Předpoklad (P, Precondition)

Předpoklad je podmínka, která musí být naplněna před zahájením funkce. Někdy může být nejasné, zdali se jedná o vstup nebo předpoklad funkce, avšak podstatný rozdíl je, že předpoklad neposkytuje signál pro zahájení funkce, určuje pouze podmínku, jenž musí být před zahájením splněna [3]. Příkladem ze zamýšleného provozu je certifikace poskytovatele před zahájením poskytování U-space služeb.

Zdroj (R, Resource)

Zdroj je pro funkci potřeba při jejím vykonávání a je při ní spotřebováván. Může jím být energie, informace či pracovní síla. Příkladem zdroje ze zamýšleného provozu je U-space služba, která má za úkol pro funkci vyhodnocovat informace ze služeb U-space.

Čas (T, Time)

Tento aspekt představuje několik způsobů, jakými může čas ovlivnit provedení funkce. Čas je možné vnímat jako formu řízení či pořadí dvou a více akcí, je možné jej vnímat z pohledu zdroje, kdy akce musí být dokončena v určitém okamžiku nebo časovém intervalu [3]. V neposlední řadě může být čas vnímám jako předpoklad, který určuje, že funkce nesmí být vykonána před dokončením jiné funkce.

Řízení (C, Control)

Aspekt řízení dohlíží na správné provedení funkce. Dle [3] se jedná o nastavená pravidla, plán, harmonogram či instrukce. Méně formální formou řízení je také očekávání, jak by daná funkce měla být provedena. Může mít podobu interního i externího charakteru. Interní očekávání nastává při procesu plánování práce, jakým způsobem ji vykonat. Externí pak značí očekávání od spolupracovníků, okolí a společnosti. Příkladem ze zamýšleného provozu může být funkce převzít kontrolu nad automatickým letem, která je řízena aspektem provozní postupy.

Výstup (O, Output)

Výstup označuje výsledek po provedení funkce. Jedná se o výsledek po zpracování vstupu. Výstupem může být hmotná věc, energie nebo informace [3]. Představuje změnu stavu systému nebo parametru výstupu. Pro příklad je uvedena funkce a její výstup ze zamýšleného provozu, výstupem funkce stanovit provozní postupy jsou stanovené provozní postupy.

Spojení funkcí (Couplings)

Po definování všech aspektů je důležité definovat, jakým způsobem dochází k propojení mezi funkcemi. Pokud je výstup pojmenován stejně jako jakýkoliv jiný aspekt jiné funkce, pak dochází mezi těmito dvěma funkcemi ke spojení. Spojení jsou *n* ku *n* charakteru, což znamená, že výstup jedné funkce může být aspektem *n* jiných funkcí a jedna funkce může mít *n* různých aspektů od *n* různých funkcí [3].

Upstream a Downstream funkce

Při modelování systému není nijak stanoveno, jakým způsobem mají být funkce vůči sobě uspořádané. Po definování všech aspektů a jejich vzájemných spojení se však nabízí zohlednit, které funkce ovlivňují jiné a naopak. Pokud funkce mezi sebou mají spojení – *coupling*, pak funkce, pro kterou je toto spojení výstupem je pro druhou *upstream* funkcí, děje se před ní a její výstup jí ovlivňuje. Z pohledu druhé funkce se jedná o *downstream* funkci, jelikož se děje po ní [3]. Tento poznatek je podstatný pro další kroky metody a uvažování variabilit funkcí.

Z důvodu obsáhlosti je model systému připojen jako Příloha č. 5 této diplomové práce a pro konkrétní případy budou dále v práci zobrazeny pouze části modelu.

3.3.3 Metoda Monte Carlo – Kvantifikace variability funkcí

V návaznosti na publikaci, která kombinuje Abstraktní hierarchii a FRAM byly další kroky metody provedeny podle publikace [5] od stejného autora doktora Riccarda Patriarca. Při tvorbě metody FRAM podle [3] je variabilita funkcí určována kvalitativně. Publikace doktora Patriarca představuje semikvantitativní přístup k určování variabilit funkcí. Konkrétně se jedná o simulaci Monte Carlo uzpůsobenou pro kroky metody FRAM.

Určení variability výstupu funkce

V následujícím kroku metody je dle [5] každý výstup funkce ohodnocen z pohledu načasování a přesnosti. Výstup může nastat *příliš brzy, včas, příliš pozdě* nebo *nenastat vůbec*. S krajní možností, při které výstup nenastane vůbec není v diplomové práci dále pracováno. Z pohledu přesnosti je rozlišován výstup *přesný, přijatelný* a *nepřesný*. Oproti tomu je možné výstupu přiřadit numerickou hodnotu, čím vyšší hodnota bude, tím více je výstup variabilní.

Tabulka 16: Číselné ohodnocení výstupu z pohledu načasování a přesnosti

Načasování	**Hodnota**	**Přesnost**	**Hodnota**
Příliš brzy	2	Přesné	1
Včas	1	Přijatelné	2
Příliš pozdě	3	Nepřesné	4

Pro každou kombinaci výstupu z pohledu načasování a přesnosti je možné určit variabilitu OV_j výstupu funkce *j*:

$$OV_j = V_j^T \times V_j^P$$

V_j^T *představuje hodnotu výstupu funkce j z pohledu načasování*

V_j^P *představuje hodnotu výstupu funkce j z pohledu přesnosti*

Tlumící a zesilující efekt variability

V dalším kroku je pro každý výstup funkce *j* určeno, zdali má tlumící nebo zesilující efekt na variabilitu downstream funkce *i.* Tento efekt je vyjádřen proměnou *a* [5].

$$a_{ij}^T\ (a_{ij}^P) \begin{cases} = 0{,}5 \quad v\ případě, že\ výstup\ funkce\ j\ má\ tlumící\ efekt\ na\ funkci\ i \\ = 1 \quad v\ případě, že\ výstup\ funkce\ j\ nemá\ žádný\ efekt\ na\ funkci\ i \\ = 2 \quad v\ případě, že\ výstup\ funkce\ j\ má\ zesilující\ efekt\ na\ funkci\ i \end{cases}$$

Tlumící nebo zesilující efekt výstupu na downstream funkci záleží na charakteru obou konkrétních funkcí, příkladem tlumícího efektu může být přesnost výstupu teoretického a praktického výcvik posádky. V případě, že výstup bude přesný, posádka bude dobře připravena i na neobvyklé scénáře a dokáže svým správným jednáním snížit variabilitu funkce *i.* Po uvážení efektu na funkci *i* je dle [5] možné určit variabilitu funkční tokové vazby CV_{ij} mezi výstupem funkce *j* a funkcí *i*:

$$CV_{ij} = OV_j \times a_{ij}^{T} \times a_{ij}^{P}$$

V následující Tabulce č. 17 byl určen efekt *a.* Největší hodnota funkční tokové vazby nastává v případech, kdy je výstup funkce *j* poskytnut příliš pozdě a je nepřesný. Druhá nejvyšší hodnota nastává pro určité funkce při poskytnutí výstupu příliš brzy a nepřesně.

Tabulka 17: Tlumící nebo zesilující efekt variability

Output funkce *j*	Funkce *i*	Načasování			Přesnost		
		Příliš brzy	Včas	Příliš pozdě	Přesné	Přijatelné	Nepřesné
Jednotná pravidla a jejich výklad	Certifikovat zapojený subjekt	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Dohlížet na dodržování pravidel	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Zajistit teoretický a praktický výcvik posádky	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Stanovit provozní postupy	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Posuzovat žádosti o oprávnění k provozu	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Registrovat provozovatele	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Získat oprávnění k provozu	2	1	6	1	2	8
Jednotná pravidla a jejich výklad	Publikovat pravidla pro poskytování U-space služeb	2	1	6	1	2	8
Certifikace zapojeného subjektu	Poskytovat specifickou U-space službu dle stanovených pravidel	2	1	6	1	2	8
Dohlížení na dodržování pravidel	Zajistit teoretický a praktický výcvik posádky	4	1	6	0,5	2	8
Dohlížení na dodržování pravidel	Poskytovat specifickou U-space službu dle stanovených pravidel	4	1	6	0,5	2	8
Dohlížení na dodržování pravidel	Stanovit postupy koordinace vícečlenné posádky	4	1	6	0,5	2	8
Dohlížení na dodržování pravidel	Stanovit provozní postupy	4	1	6	0,5	2	8
Registrace provozovatele	Získat oprávnění k provozu	2	1	6	1	2	8
Schválení žádosti o oprávnění k provozu	Získat oprávnění k provozu	4	1	6	1	2	8
Pravidla pro poskytování U-space služeb	Vyhodnotit přijímaná data	2	1	6	1	2	8
Pravidla pro poskytování U-space služeb	Poskytovat specifickou U-space službu dle stanovených pravidel	2	1	6	1	2	8
Teoretický a praktický výcvik posádky	Zahájit let	2	1	6	0,5	2	8
Teoretický a praktický výcvik posádky	Převzít kontrolu nad automatickým letem	2	1	6	0,5	2	8
Teoretický a praktický výcvik posádky	Vyhodnocovat informace z provozu UA	2	1	6	0,5	2	8
Teoretický a praktický výcvik posádky	Vyhodnocovat informace ze služeb U-space	2	1	6	0,5	2	8
Teoretický a praktický výcvik posádky	Zajistit provozuschopný stav UA	2	1	6	0,5	2	8
Postupy koordinace vícečlenné posádky	Komunikovat s ostatními členy personálu	2	1	6	0,5	2	8
Provozní postupy	Komunikovat s ostatními členy personálu	2	1	6	0,5	2	8
Provozní postupy	Zahájit let	2	1	6	0,5	2	8
Provozní postupy	Převzít kontrolu nad automatickým letem	2	1	6	0,5	2	8
Provozní postupy	Vyhodnocovat informace z provozu UA	2	1	6	0,5	2	8
Provozní postupy	Zajistit provozuschopný stav UA	2	1	6	0,5	2	8
Provozní postupy	Vyhodnocovat informace ze služeb U-space	2	1	6	0,5	2	8
Oprávnění k provozu	Zahájit let	4	1	6	1	2	8
U-space služba	Vyhodnocovat informace ze služeb U-space	4	1	6	0,5	2	8
Vyhodnocená data	Poskytovat specifickou U-space službu dle stanovených pravidel	4	1	6	1	2	8
Komunikace členů personálu	Zahájit let	4	1	6	0,5	2	8
Let zahájen	Převzít kontrolu nad automatickým letem	4	1	6	1	2	8
Vyhodnocení informace z provozu UA	Převzít kontrolu nad automatickým letem	4	1	6	0,5	2	8
Vyhodnocení informace ze služeb U-space	Převzít kontrolu nad automatickým letem	4	1	6	0,5	2	8
Zajištění provozuschopného stavu UA	Zahájit let	2	1	6	0,5	2	8

Určení výkonnostních podmínek SPC

Další krok metody Monte Carlo dle publikace doktora Patriarca [5] je věnován scénářům, které mohou při běžném provozu nastat a ovlivnit běžné fungování zvoleného systému. Tyto scénáře se nazývají výkonností podmínky a označují se *SPC*^{k} - *Scenario Performance Conditions*. Byly určeny 3 výkonnostní podmínky, které se pro zamýšlený provoz jeví jako nejpravděpodobnější a zároveň mají vliv na bezpečné provedení letu. Podmínky jsou uvedeny v Tabulce č. 18.

Tabulka 18: Výkonnostní podmínky SPC

SPC^1	Lidský faktor negativně ovlivní úkony personálu
SPC^2	Provoz bude narušen zásahem letecké záchranné služby
SPC^3	Dojde k překročení limitních meteorologických podmínek

Pro každou funkci *j* je možné určit, jaký vliv b^k na ní bude mít každá z výkonnostních podmínek.

$$b_j^k \begin{cases} = 0 \quad výkonností\ podmínka\ nemá\ žádný\ vliv\ na\ funkci\ j \\ = 0{,}5 \quad výkonností\ podmínka\ má\ mírný\ vliv\ na\ funkci\ j \\ = 1 \quad výkonností\ podmínka\ má\ velký\ vliv\ na\ funkci\ j \end{cases}$$

V Tabulce č. 19 je určen vliv výkonnostních podmínek pro každou funkci.

Tabulka 19: Vliv výkonnostních podmínek SPC na jednotlivé funkce

#	**Funkce *j***	**SPC^1**	**SPC^2**	**SPC^3**
1	Publikovat jednotná pravidla a jejich výklad	0	0	0
2	Certifikovat zapojený subjekt	0	0	0
3	Dohlížet na dodržování pravidel	0	0	0
4	Registrovat provozovatele	0	0	0
5	Posuzovat žádosti o oprávnění k provozu	0	0	0
6	Publikovat pravidla pro poskytování U-space služeb	0	0	0
7	Zajistit teoretický a praktický výcvik posádky	0	0	0
8	Stanovit postupy koordinace vícečlenné posádky	0	0	0
9	Stanovit provozní postupy	0	0	0
10	Získat oprávnění k provozu	0	0	0
11	Poskytovat specifickou U-space službu dle stanovených pravidel	0	1	0
12	Vyhodnotit přijímaná data	0	0	0
13	Komunikovat s ostatními členy personálu	1	0.5	0
14	Zahájit let	1	0.5	1
15	Vyhodnocovat informace z provozu UA	1	1	1
16	Vyhodnocovat informace ze služeb U-space	1	1	0
17	Zajistit provozuschopný stav UA	1	0	0

Provozní scénáře a jejich vliv na variabilitu

Provozní scénáře jsou tvořeny kombinací vlivu výkonnostních podmínek SPC^k. Jsou rozlišovány 3 varianty podle toho, jaký vliv má daná výkonností podmínka na variabilitu [5].

$$SPC_z^k \begin{cases} = 1 & \check{z}\acute{a}dn\acute{y}\ vliv\ na\ variabilitu \\ = 2 & mal\acute{y}\ vliv\ na\ variabilitu \\ = 4 & velk\acute{y}\ vliv\ na\ variabilitu \end{cases}$$

K je index výkonnostní podmínky a *z* je index scénáře. V dalším kroku je možné vytvořit matici S, která bude tvořena výkonnostními podmínkami a jejich vlivem na variabilitu. Jelikož byly definovány 3 výkonnostní podmínky a každá z nich může nabývat 3 hodnot vlivu na variabilitu, existuje proto 27 rozdílných scénářů. Pro další výpočty byly uvažovány pouze scénáře, které se co nejvíce přibližují reálné situaci v zamýšleném provozu. Pro první výkonnostní podmínku je uvažováno, pokud lidský faktor negativně ovlivní úkony personálu, pak tato skutečnost bude mít vždy velký vliv na variabilitu a proto není vhodné uvažovat jiný scénář. Pro ostatní dvě výkonnostní podmínky je uvažováno s malým a velkým vlivem na variabilitu u obou podmínek. Není uvažován scénář, ve kterém by alespoň jedna z těchto podmínek neměla žádný vliv na variabilitu. Z tohoto důvodu byly z matice S dále uvažovány pouze scénáře 23, 24, 26 a 27.

Tabulka 20: Vybrané scénáře

Scénář	SPC^1	SPC^2	SPC^3
23	4	2	2
24	4	2	4
26	4	4	2
27	4	4	4

Podmíněná variabilita

V tomto stádiu metody je dle [5] možné určit podmíněnou variabilitu e^z každého výstupu funkce *j* a každého scénáře *z* podle uvedeného vzorce. Proměnná *m* označuje počet výkonnostních podmínek SPC. Pokud by funkce *j* nebyla ovlivněna žádným SPC, tj. $b_j^k = 0$ pro všechny *k,* pak by se podmíněná variabilita rovnala 0. Tento případ je ošetřen úpravou, kdy se podmíněná variabilita rovná vyšší hodnotě z daného výpočtu nebo 1. Tato úprava ošetřuje případy, kdy scénář nezvyšuje podmíněnou variabilitu.

$$e_j^z = max\left\{1; \frac{\sum_{k=1}^{m} SPC_z^k \cdot b_j^k}{m}\right\}$$

Rovnice 1 [5]

Celková variabilita funkční tokové vazby

Při přiřazování hodnot v průběhu tvorby metody by mělo být uvažováno s faktem, že systém se v reálném prostředí nejeví jako statický. U organizačních a lidských funkcí nemusí hodnota odpovídat reálné situaci, protože nelze říct, že výstup je obecně správně načasován nebo neobsahuje nepředvídatelné chyby. Z tohoto důvodu je možné pro výstupy funkcí zavést rozdělení pravděpodobnosti diskrétní náhodné veličiny. Zamýšlený provoz je uvažován jako modelová situace s budoucím využitím prvků U-space prostoru a k zavedení rozdělení pravděpodobnosti je třeba vycházet z dat z reálného provozu nebo vycházet z předpovědi těchto hodnot. Pro zamýšlený provoz však tuto pravděpodobnost určit nelze. Simulace je tedy dokončena bez ní a výsledek byl vyhodnocen expertním názorem dle již známých informací o provozu v prostředí U-space.

V posledním kroku simulace je možné za pomoci všech předchozích kroků určit celkovou variabilitu funkční tokové vazby mezi funkcemi *j* a *i* za scénáře *z* podle následujícího vzorce [5]:

$$VPN_{ij}^z = V_j^T \cdot V_j^P \cdot a_{ij}^T \cdot a_{ij}^P \cdot e_j^z$$

Rovnice 2 [5]

3.3.4 Vyhodnocení

Při vyhodnocení metody muselo být určeno, jaká hodnota celkové variability funkční tokové vazby bude z pohledu variability systému zajímavá a bude dále zkoumána. Prahová hodnota byla stanovena na 50 a všechny funkční tokové vazby s hodnotou vyšší byly zkoumány. Konkrétně se jednalo o 6 funkčních tokových vazeb.

První z vazeb je mezi funkcí *j Poskytovat specifickou U-space službu dle stanovených pravidel* a funkcí *i Vyhodnocovat informace ze služeb U-space*. Výstup funkce *j* je *U-space služba*. Hodnota VPN_{ij}^z je při scénářích 26, 27 a při kombinaci výstupu funkce *j* příliš pozdě a nepřesně rovna 64. Je tedy nutné zamezit tomu, aby byl výstup v první řadě nepřesný a dále, aby byl

poskytnut příliš pozdě. Je také potřeba zvážit, jaké funkce jsou pro funkci *i* downstream funkcemi, jelikož variabilita funkční tokové vazby na ně má přímý vliv. Taková funkce je v systému pouze jedna a to *Převzít kontrolu nad automatickým letem*. Pokud bude *U-space služba* poskytnuta nepřesně a příliš pozdě, pak bude negativně ovlivněna právě i tato funkce.

Další odhalená vazba je mezi funkcemi *Komunikovat s ostatními členy personálu* a *Zahájit let*. Výstup funkce *j* je *Komunikace členů personálu*. Hodnoty VPN_{ij}^{z} jsou při kombinaci výstupů příliš brzy a nepřesně 53 pro scénáře 23, 24 a 64 pro scénáře 26, 27. Kombinace výstupů příliš pozdě a nepřesně je 80 pro scénáře 23, 24 a 96 pro scénáře 26, 27. Nepřesné komunikaci mezi členy posádky je možné zabránit stanovenými provozními postupy a postupy koordinace vícečlenné posádky. Funkce, která by mohla být ovlivněna, jelikož se jedná o downstream funkci je *Převzít kontrolu nad automatickým letem.*

Třetí z odhalených vazeb je mezi funkcí *j Zahájit let* a funkcí *i Převzít kontrolu nad automatickým letem.* Výstup funkce *j* je *Let zahájen*. Hodnoty VPN_{ij}^{z} jsou při kombinaci výstupů příliš brzy a nepřesně 75, 96, 85 a 107 pro scénáře 23, 24, 26 a 27 v tomto pořadí. Pro kombinace výstupů příliš pozdě a nepřesně jsou poté hodnoty 112, 144, 128 a 160 pro scénáře 23, 24, 26 a 27 v tomto pořadí. Z výsledků vyplývá, že zahájení letu je klíčovou funkcí pro zamýšlený provoz. Před zahájením letu musí být řádně provedena předletová příprava, musí být řádně upevněn převážený materiál, musí být správně nastaveny provozní postupy a komunikace členů posádky. *Let zahájen* je předpoklad pro provedení funkce *i*, z pohledu provozní bezpečnosti systému je důležité zajistit, že variabilita funkční tokové vazby nenabyde vysokých hodnot. Důležité je se také zaměřit na funkce, které se dějí před funkcí *Zahájit let,* konkrétně velmi podstatné se jeví funkce *Zajistit teoretický a praktický výcvik posádky*, ze které provádění činnosti a rozhodování vychází a funkce *Stanovit provozní postupy*, která stanovuje, jak bude posádka postupovat.

Další odhalená funkční tokova vazba je mezi funkcemi *Vyhodnocovat informace z provozu UA* a *Převzít kontrolu nad automatickým letem.* Výstup první z dvojice funkcí je *Vyhodnocení informace z provozu UA.* Pro druhou funkci se jedná o aspekt vstup. Vyhodnocovat informace z provozu UA je podstatnou náplní práce dálkově řídícího pilota, předchází jí teoretický a praktický výcvik a řídí se provozními postupy provozovatele. U funkční tokové vazby byly zjištěny nejvyšší hodnoty ze všech odhalených vazeb. Pro kombinace výstupů příliš brzy a nepřesně jsou hodnoty 85, 107, 107 a 128 pro scénáře 23, 24, 26 a 27 v tomto pořadí. Pro kombinace výstupu příliš pozdě a nepřesně jsou hodnoty 128, 160, 160 a 192 pro scénáře 23,24, 26 a 27 v tomto pořadí.

Předposlední zkoumanou funkční tokovou vazbou je vazba mezi funkcemi *Vyhodnocovat informace ze služeb U-space*, s výstupem *Vyhodnocení informace ze služeb U-space,* a *Převzít kontrolu nad automatickým letem*. Hodnoty VPN_{ij}^{z} jsou při kombinaci výstupů příliš brzy a nepřesně 64, 64, 85 a 85 pro scénáře 23, 24, 26 a 27 v tomto pořadí. Pro kombinace výstupů příliš pozdě a nepřesně se poté jedná o hodnoty 96, 96, 128 a 128 pro scénáře 23, 24, 26 a 27 v tomto pořadí. Obdobně jako u předchozí funkce *j* je možné u vazby snížit variabilitu správně nastavenými provozními postupy, které jsou pro funkci *Vyhodnocovat informace ze služeb U-space* aspektem řízení. Další upstream funkcí je teoretický a praktický výcvik posádky. Třetím vstupem je pak *U-space služba*, u které musí být zajištěna přesnost a načasování.

Šestou a poslední ze zkoumaných vazbou je mezi funkcí *j Zajistit provozuschopný stav UA* a funkcí *i Zahájit let*. Výstup funkce *j* je *Zajištění provozuschopného stavu UA*. Kombinace výstupů příliš pozdě a nepřesně je 64 pro všechny uvažované scénáře. Upstream funkce jsou, jako u předchozích funkcí, *Zajistit teoretický a praktický výcvik posádky* a *Stanovit provozní postupy*.

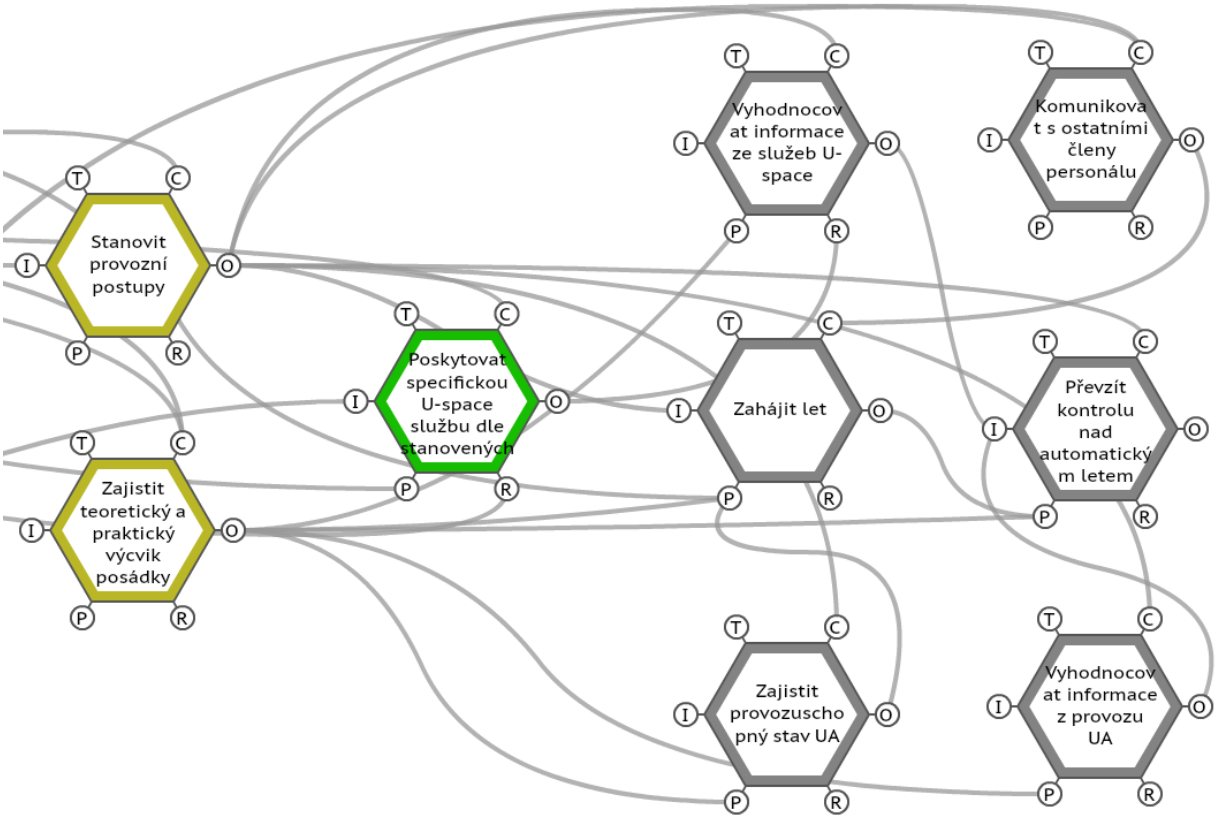
Po analýze výše určených funkčních tokových vazeb bylo odhaleno 7 funkcí, u kterých může zvýšená variabilita vést ke vzniku funkční rezonance. Mimo těchto 7 kritických funkcí byly identifikovány další 2 funkce, jenž v mnoha případech představují *upstream* funkce pro odhalené funkce.

Všechny odhalené funkce jsou vypsány v Tabulce č. 21. Porovnání s výsledky metody SORA je součástí dalších kapitoly.

Tabulka 21: Odhalené funkce

Odhalené funkce
Poskytovat specifickou U-space službu dle stanovených pravidel
Vyhodnocovat informace ze služeb U-space
Komunikovat s ostatními členy personálu
Zahájit let
Převzít kontrolu nad automatickým letem
Vyhodnocovat informace z provozu UA
Zajistit provozuschopný stav UA
Odhalené upstream funkce
Zajistit teoretický a praktický výcvik posádky
Stanovit provozní postupy

Kompletní model je vytvořen za pomocí softwaru FRAM Model Visualiser a je součástí diplomové práce ve formě Přílohy č. 5. Pro ilustraci je přiložen Obrázek č. 12 jako výstřižek odhalených kritických funkcí systému. Žlutou barvou jsou zobrazeny funkce provozovatele UAS, zelená barva zobrazuje funkci USSP a šedou barvou jsou znázorněny funkce dálkově řídícího pilota. Funkce jsou propojeny formou 6 aspektů, tak jak bylo popsáno v kapitole 3.3.2. Kompletní model obsahuje i popis spojení funkcí (*couplings)*, avšak z důvodu jejich množství nejsou součástí zobrazené části modelu.



Obrázek 12: Výstřižek odhalených funkcí v modelu FRAM

3.4 Způsob porovnání metod

Po vytvoření bezpečnostních analýz dle metod, jejichž postupy a vyhodnocení byly popsány v předchozích kapitolách je dalším krokem jejich porovnání. Porovnání výsledků metod je věnována samostatná kapitola. Před porovnáním je však potřeba popsat, jakým způsobem budou výsledky porovnávány.

Výsledky systémových metod STPA a FRAM budou porovnány s požadavky na specifický provoz stanovené cíli provozní bezpečnosti OSO, které byly určeny vypracováním metody SORA. Pro provoz ve specifické kategorii provozu musí být splněny mimo OSO také požadavky vycházející z Prováděcích nařízení Evropské komise, proto jsou výsledky metod porovnány i s těmito požadavky v závislosti na charakteru požadavku.

Výsledky metody STPA jsou pro účely porovnávání specifických požadavků vhodnější, jelikož se jedná o specifická omezení nebo systémové požadavky. Výsledkem metody FRAM byla identifikace funkcí, které jsou pro systém kritické a jejich velká variabilita by mohla vést k funkční rezonanci.

Požadavky vycházející z OSO byly rozřazeny do 6 kategorií a vloženy do Tabulky č. 22.

Tabulka 22: Požadavky stanovené metodou SORA

Provozní postupy
- Provozní postupy musí zahrnovat kontrolní seznamy, údržbu, výcvik, odpovědnosti a související povinnosti. (OSO#1, I) - ConOps musí obsahovat provozní postupy. (OSO#1, J) - Musí být definovány provozní postupy vhodné pro navrhovaný provoz a musí pokrývat (OSO#8, I): - Plánování letu; - Kontroly před a po letu; - Postupy zhodnocení podmínek prostředí před a v průběhu mise (tj. hodnocení v reálném čase); - Postupy zvládání neočekávaných nepříznivých provozních podmínek; - Normální postupy; - Postupy pro nenadálé situace; - Nouzové postupy; - V provozní příručce musí být uvedeno omezení externích systémů podporujících provoz UAS - Provozní postupy musí brát v úvahu lidskou chybu. (OSO#8, I) - Při nenadálých situacích/nouzových postupech musí být UAS řízeno manuálně dálkově řídícím pilotem, i když je běžně řízeno automaticky. (OSO#8, I) - Provozní postupy musí být validovány oproti standardům považovaným příslušným úřadem za dostatečné a/nebo musí být v souladu se způsobem průkazu přijatelným pro tento úřad. (OSO#8, J)
Teoretický a praktický výcvik
- Teoretický a praktický výcvik je založen na kompetencích, je přiměřený uvažovanému provozu a obsahuje (OSO#9, I): - Nařízení o provozu UAS; - Provozní principy vzdušného provozu UAS; - Pilotování a bezpečnost letectví; - Omezení lidské výkonnosti; - Meteorologie; - Navigace/mapy; - Znalost UAS; a - Provozní postupy. - Výcvik je absolvován na základě vlastního prohlášení. (OSO#9, J) - Dálkově řídící posádka musí být vyškolena k provádění inspekce UAS. Školení je samo deklarováno. (OSO#7, J) - Výcvik dálkově řídící posádky musí zahrnovat spolupráci ve vícečlenné posádce. (OSO#16, I) - Výcvik koordinace vícečlenné posádky je na základě vlastního prohlášení. (OSO#16, J) - Výcvik musí zahrnovat posouzení meteorologických podmínek. (OSO#23, I) - Výcvik posouzení podmínek prostředí je na základě vlastního prohlášení. (OSO#23, J)
Údržba
- Musí být stanoveny instrukce pro údržbu UAS, pokud je to možné, zahrnují instrukce a požadavky výrobce UAS. (OSO#3, I) - Personál údržby musí být odborně způsobilý a mít oprávnění k provádění údržby UAS. (OSO#3, I) - Personál údržby musí provádět údržbu UAS podle instrukcí pro údržbu. (OSO#3, I) - Instrukce pro údržbu musí být zdokumentované. (OSO#3, J) - Úkony údržby musí být zaznamenány v deníku údržby. (OSO#3, J) - Musí být stanoven a aktualizován seznam personálu oprávněného k provádění údržby. (OSO#3, J) - Musí být veden a aktualizován záznam všech kvalifikací, praxe a/nebo výcviku absolvovaný personálem údržby. (OSO#3, J)
Ostatní povinnosti*

- Žadatel musí stanovit, jak dálkově řídící posádka sama deklaruje svou zdravotní způsobilost k provozu před provedením jakéhokoli letu. (OSO#17, I)
- Způsob deklarace zdravotní způsobilosti musí být zdokumentován. (OSO#17, J)
- Musí být definovány podmínky prostředí pro bezpečný provoz a musí být zohledněny v letové příručce nebo rovnocenném dokumentu. (OSO#23, I)
- Musí být stanoveny postupy pro vyhodnocení podmínek prostředí před a během letu. Postupy musí zahrnovat posouzení meteorologických podmínek pomocí jednoduchého záznamového systému. (OSO#23, I)
- Musí být deklarována přiměřenost postupů a kontrolních seznamů. (OSO#23, J)
- Žadatel musí stanovit, že výkonnost, radiové spektrum a podmínky prostředí pro spoje C3 jsou dostatečné pro bezpečné provedení zamýšleného provozu. (OSO#6, I)
- Dálkově řídící pilot musí mít způsob, jak nepřetržitě monitorovat výkonnost C3, a musí zajišťovat, že jsou trvale splněny provozní požadavky. (OSO#6, I)
- Dálkově řídící posádka musí zajistit, že UAS je ve stavu pro bezpečný provoz a odpovídá schválenému ConOps. (OSO#7, I)
- Inspekce UAS musí být zdokumentována a zohledňovat doporučení výrobce. (OSO#7, J)
- Informační a řídící rozhraní UAS musí jasné a zřetelné. Nesmí být zmatečné, způsobovat neopodstatněnou únavu a přispívat k chybám dálkově řídící posádky. (OSO#20, I)
- Žadatel musí posoudit, zdali je HMI vhodné pro daný provoz. Posouzení je založeno na kontrole nebo analýze. Příslušný úřad může požádat EASA, aby byla svědkem hodnocení HMI. (OSO#20, J)
- Při provozu nad obydlenými oblastmi nebo shromážděními lidí musí být důvodně očekáváno, že nedojde k smrtelnému úrazu v důsledku jakéhokoliv pravděpodobného selhání UAS nebo jakéhokoliv externího systému podporující provoz. (OSO#10, I)
- Musí být k dispozici posouzení návrhu a „instalace“ a musí obsahovat (OSO#10, J):
    - Vlastnosti návrhu a instalace (nezávislost, oddělení a redundance)
    - Konkrétní rizika související s ConOps neporušují případné nároky na nezávislost

Koordinace vícečlenné posádky

- Musí být stanoveny postupy k zajištění koordinace mezi členy posádky, které obsahují minimálně (OSO#16, I):
    - Přidělení úkolů posádce; a
    - Navázání spojení krok po kroku.
- Musí být zajištěny spolehlivé a účinné komunikační kanály. (OSO#16, I)
- Musí být deklarována přiměřenost postupů a kontrolních seznamů. (OSO#16, J)

Externí služby

- Žadatel musí zajistit, že úroveň výkonnosti jakékoli externě poskytované služby nezbytné pro bezpečnost zamýšleného provozu je dostačující. (OSO#13, I)
- Pokud externě poskytovaná služba vyžaduje komunikaci mezi provozovatelem UAS a poskytovatelem služby, pak žadatel musí zajistit efektivní komunikaci. (OSO#13, I)
- Musí být definovány role a odpovědnost mezi žadatelem a externím poskytovatelem služby. (OSO#13, I)
- Žadatel musí prohlásit, že je dosaženo požadované úrovně výkonnosti pro jakoukoli externě poskytovanou službu nezbytnou pro bezpečnost zamýšleného provozu. (OSO#13, J)

4 Porovnání výsledků metod

Porovnání výsledků je rozděleno do 2 částí, pro obě systémové metody samostatně. První z porovnávaných metod je STPA. Výsledek metody STPA je ve formě omezení, jež jsou vyvozena z nebezpečných řídících akcí a systémových požadavků sloužící k zabránění ztrátových scénářů. Vytvořená metoda STPA zahrnuje pro zamýšlený provoz důležité regulátory a jiné řídící prvky, které nejsou součástí porovnání. Konkrétně se jedná o agenturu EASA, MD, ÚCL, výrobce UAS a ANSP ČR. Omezení a systémové požadavky pro tyto zmíněné prvky není možné porovnávat s výsledky metody SORA. Kompletní tabulky vyhodnocení pro obě vytvořené metody jsou přiloženy formou Přílohy č.3 a Tabulky č. 29.

Výsledkem metody FRAM je identifikování kritických funkcí sytému. K identifikaci byla použita metoda vycházející ze simulace Monte Carlo podle publikace doktora Patriarca, jak bylo popsáno v kapitole 3.3.3. Celkem bylo odhaleno 9 kritických funkcí systému. Na základě překročené prahové hodnoty celkové variability funkční tokové vazby bylo odhaleno 7 funkcí a po jejich následné analýze byly určeny další 2 *upstream* kritické funkce.

4.1 Porovnání výsledků STPA

V této části diplomové práce jsou uvedena všechna omezení a požadavky, u kterých byl nalezen rozpor s výsledky metody SORA a některá další pro lepší ilustraci výsledků. Index UCA je uveden pro lepší orientaci, ze které částí metody požadavky vychází. Omezení řídícího prvku jsou stanovena za účelem zabránění uvedených UCA. Systémové požadavky zabraňují ztrátovým scénářům určeným ve 4. kroku metody STPA. Každé stanovené omezení a požadavek je porovnán s požadavky určenými metodou SORA nebo legislativou, např. formou odpovědností provozovatele.

V Tabulce č. 23 jsou popsány omezení a požadavky, které vychází z řídící akce poskytnutí provozní příručky mezi provozovatel a členem personálu. Všechny požadavky jsou uvedeny v [1], konkrétně v části UAS.SPEC.050 (1)(e)(ii).

Tabulka 23: Omezení řídícího prvku a systémové požadavky pro UCA-6.1

	Omezení řídícího prvku	**Systémové požadavky**
UCA-6.1:	- Provozní příručka musí být poskytnuta před zahájením provozu - Provozní příručka musí být poskytnuta kompletní před zahájením provozu - Provozní příručka nesmí být poskytnuta po zahájení provozu	- Provozovatel UAS musí vytvořit provozní příručku a poskytnout jí členům personálu - Provozovatel UAS musí vědět, že má povinnost poskytnout provozní příručku

Požadavky v Tabulce č. 24 vychází z řídící akce stanovení provozních postupů. Omezení řídícího prvku jsou uvedena v [1] části UAS.SPEC.050 (1)(a). Jedná o podmínky, které musí provozovatel splnit k získání OkP. První uvedený systémový požadavek, jenž provozovatele zavazuje k definování zamýšleného provozu je také podmínkou pro získání OkP. Zbylé 2 systémové požadavky nejsou ukotveny v legislativě, avšak počítá se, že jsou dodrženy. Ve vyhodnocení jsou tyto požadavky označeny oranžovou barvou a jsou součástí diskuse v závěru této diplomové práce.

Tabulka 24: Omezení řídícího prvku a systémové požadavky pro UCA-6.3

	Omezení řídícího prvku	**Systémové požadavky**
UCA-6.3:	- Provozní postupy musí být stanoveny před zahájením provozu - Provozní postupy musí být stanoveny úplně před zahájením provozu - Provozní postupy nesmí být stanoveny po zahájení provozu	- Provozovatel UAS musí kompletně definovat provoz - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů - Provozovatel UAS musí dostatečně znát problematiku bezpilotního letectví

Nebezpečná řídící akce uvedená v Tabulce č. 25 je vztažena k periodické kontrole požadovaných znalostí a výcviku pro danou pozici. Tento požadavek není v metodě SORA nebo legislativě obsažen, jedinou podmínkou uvedenou v [1] je platnost osvědčení dálkově řídícího pilota, která je 5 let. Rozpor je také v 3. systémovém požadavku uvedeném v tabulce, který stanovuje povinnost provozovatele zhodnotit potřebné znalosti a výcvik personálu. Výsledkem metody SORA je absolvování výcviku na základě vlastního prohlášení.

Tabulka 25: Omezení řídícího prvku a systémové požadavky pro UCA-6.5

	Omezení řídícího prvku	**Systémové požadavky**
UCA-6.5:	- Požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány - Požadované znalosti a výcvik musí být v průběhu provozu úplně periodicky kontrolovány	- Provozovatel UAS musí považovat požadované znalosti a výcvik pro misi za důležité - Provozovatel UAS si musí uvědomovat vážnost mise a nést za ní odpovědnost - Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky

Požadavky uvedené v Tabulce č. 26 byly určeny z řídící akce poskytování U-space služeb. První z uvedených omezení řídícího prvku: U-space služby musí být v průběhu provozu poskytovány je v souladu s podmínkou stanovenou OSO#13. Konkrétně se jedná o podmínku nízké úrovně jistoty. K rozporu však dochází u zbylých 3 omezení řídícího prvku, jelikož ty jsou v metodě SORA vyžadovány až od střední a vysoké úrovně jistoty výše zmíněného cíle provozní bezpečnosti. Systémové požadavky jsou obsahem dokumentu [17], který je AMC a GM k Prováděcím nařízení komise (EU) 2021/664, 2021/665 a 2021/666.

Tabulka 26: Omezení řídícího prvku a systémové požadavky pro UCA-7.1

	Omezení řídícího prvku	**Systémové požadavky**
UCA-7.1:	- U-space služby musí být v průběhu provozu poskytovány - U-space služby musí být v průběhu provozu poskytovány kompletně - U-space služby nesmí být poskytovány pozdě - Poskytování U-space služeb nesmí v průběhu provozu přerušeno	- Musí být definován rámec, který vymezuje rozsah poskytování U-space služeb - Poskytování U-space služeb musí být kontrolováno - Musí být definován rámec, podle kterého je kontrolováno plnění závazků USSP

Požadavky v Tabulce č. 27 se týkají řídící akce řídící pokyny pro pohyb UA. Na zajištění omezení, která jsou stanovena je možné pohlížet dvěma způsoby. Řídící pokyny pro pohyb UA jsou podmíněny správným výcvikem dálkově řídícího pilota, tato podmínka je stanovena v OSO#9. Další podmínka tkví ve zdravotní způsobilosti členů dálkově řídící posádky. Tato podmínka je stanovena OSO#17. Obě podmínky ze zmíněných OSO jsou podle metody SORA prokázány na základě vlastní deklarace členů posádky.

Tabulka 27: Omezení řídícího prvku a systémové požadavky pro UCA-9.1

	Omezení řídícího prvku	**Systémové požadavky**
UCA-9.1:	- Řídící pokyny pro pohyb UA musí být v průběhu provozu provedeny - Řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny špatně - Řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny pozdě - Provádění řídících pokynů pro pohyb UA nesmí být v průběhu provozu přerušeno	- Pilotní výcvik musí být dostatečný pro daný provoz - V průběhu mise musí být dálkově řídící pilot schopen neustále provádět řídící pokyny

Tabulka č. 28 obsahuje požadavky vycházející z řídící akce vyhodnocení informace z poskytované U-space služby. Žádné ze stanovených omezení řídícího prvku není obsahem cílů provozní bezpečnosti, které by stanovily pravidla nebo postup pro vyhodnocení U-space služeb. Systémový požadavek stanovil povinnost implementování vyhodnocení informace z U-space služby do výcviku dálkově řídícího pilota. Metoda SORA tento požadavek nezohledňuje. Druhý systémový požadavek je cílen na USSP a je obsahem [17].

Tabulka 28: Omezení řídícího prvku a systémové požadavky pro UCA-9.3

	Omezení řídícího prvku	**Systémové požadavky**
UCA-9.3:	- Informace z poskytované U-space služby musí být v průběhu provozu vyhodnocena - Informace z poskytované U-space služby nesmí být v průběhu provozu vyhodnocena špatně - Informace z poskytované U-space služby nesmí být vyhodnocena pozdě	- Dálkově řídící pilot musí mít výcvik k vyhodnocení informace z poskytované U-space služby - U-space služba musí být poskytována správně a včas

4.2 Porovnání výsledků FRAM

Každá odhalená kritická funkce systému byla porovnána s požadavky stanovenými výslednými OSO nebo požadavky vycházejícími z legislativních předpisů. Porovnání je obsahem Tabulky č. 29. Jednou z odhalených kritických funkcí metody FRAM je zajištění teoretického a praktického výcviku posádky. Metoda SORA tento požadavek také stanovuje, avšak jeho splnění je na základě vlastního prohlášení. Nejedná se o přímý rozpor výsledků metod, avšak o jistou nesrovnalost, jež je více popsána v diskusi práce.

Tabulka 29: Odhalené funkce a porovnané požadavky

	Odhalené funkce	**Požadavky**
#1	Poskytovat specifickou U-space službu dle stanovených pravidel	- Je obsahem AMC a GM k Prováděcím nařízení komise (EU) 2021/664, 2021/665 a 2021/666 - Není obsahem metody SORA, ani Prováděcího nařízení komise (EU) 2021/947
#2	Vyhodnocovat informace ze služeb U-space	- Není stanoveno
#3	Komunikovat s ostatními členy personálu	- OSO#13
#4	Zahájit let	- OSO#8 (Normální postupy), OSO#9
#5	Převzít kontrolu nad automatickým letem	- OSO#8 (Postupy pro nenadále situace, Nouzové postupy), OSO#9
#6	Vyhodnocovat informace z provozu UA	- OSO#9
#7	Zajistit provozuschopný stav UA	- Je obsahem části UAS.SPEC.060 Prováděcího nařízení Komise (EU) 2019/947, OSO#3
	Odhalené upstream funkce	
#8	Zajistit teoretický a praktický výcvik posádky	- OSO#7, OSO#9, OSO#16, OSO#23
#9	Stanovit provozní postupy	- OSO#1, OSO#8

5 Diskuse výsledků

Metoda SORA slouží jako nástroj pro provozovatele a příslušný úřad k posouzení proveditelnosti zamýšleného provozu specifické kategorie. Navzdory tomu, že žadatel při tvorbě metody postupuje podle předem stanovených kroků, mohou být kroky a jejich výsledky interpretovány různě. Žadatel pro provoz navrhne zmírňující opatření za účelem snížení provozního rizika na zemi a ve vzduchu, příslušný úřad zmírňující opatření posoudí a může žadateli úroveň zmírňujících opatření snížit.

Výsledky metody SORA pro zamýšlený provoz jsou: konečná třída rizika na zemi GRC na úrovni 3 a zbytková třída rizika ve vzduchu na úrovni *arc-b*. Kombinací těchto tříd je určena hodnota SAIL 2. Výsledek nelze považovat za absolutní. Je možné, že vyhodnocení by podle Úřadu pro civilní letectví České republiky bylo odlišné a tudíž by se lišily i stanovené cíle provozní bezpečnosti.

Metoda SORA zohledňuje U-space prvky jako externí služby a stanovuje na ně požadavky pod označením OSO#13. Pro zamýšlený provoz je vyžadováno, aby poskytovaná služba dosahovala požadované úrovně výkonnosti, tak aby nebyla ohrožena bezpečnost provozu. Podstatné také je, že dálkově řídící posádka prokazuje absolvování teoretického a praktického výcviku formou vlastního prohlášení. Stejně je tomu i u deklarace zdravotní způsobilosti před zahájením provozu a doložení výcviku koordinace vícečlenné posádky.

Jedním z poznatků je, že při tvorbě metody STPA byly stanoveny systémové požadavky, které se považují za integrální součást systému a berou se tak za samozřejmost. Ve vyhodnocení STPA analýzy, které je přiloženo ve formě Přílohy č. 3 jsou znázorněny oranžovou barvou. Požadavky tohoto typu jsou obtížně prokazatelné, většina z nich je vztažena k provozovateli UAS, pro příklad je uveden požadavek: Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou. Takovýto požadavek není explicitně, ve formě podmínky, zmíněn v metodě SORA, ani v Prováděcím nařízení Komise (EU) 2019/947.

Rozpor byl nalezen u požadavků, které vychází z řídící akce: Periodická kontrola požadovaných znalostí a výcviku pro danou pozici. Konkrétně se jedná o rozpor u dvou požadavků určených z nebezpečných řídících akcí a dvou systémových požadavků. Pro zamýšlený provoz není výcvik kontrolován provozovatelem ani třetí stranou. Aktuálně je certifikace dálkově řídícího pilota platná po dobu pěti let, což se v prostředí provozu bezpilotních systémů jeví jako neoptimální, jelikož se prostředí formuje do své finální podoby a dochází k postupnému dotváření pravidel.

Nesoulad byl také nalezen v oblasti poskytování U-space služeb. Jeden z požadavků vycházející z UCA-7.1 je splněn, jelikož je obsahem OSO#13 na úrovni nízké jistoty. Pro následující 3 požadavky, však došlo k rozporu.

- U-space služby musí být v průběhu provozu poskytovány kompletně.
- U-space služby nesmí být poskytovány pozdě.
- Poskytování U-space služeb nesmí být v průběhu provozu přerušeno.

Požadavky sice jsou obsahem OSO#13, ale na střední a vysoké úrovni jistoty, tudíž pro zamýšlený provoz nejsou dle metody SORA vyžadovány.

Další nalezený rozpor se týká vyhodnocování informací z poskytovaných U-space služeb. Výsledkem STPA metody jsou požadavky:

- informace z poskytované U-space služby musí být v průběhu provozu vyhodnocena;
- informace z poskytované U-space služby nesmí být v průběhu provozu vyhodnocena špatně;
- informace z poskytované U-space služby nesmí být vyhodnocena pozdě.

Aktuální podoba metody SORA nestanovuje žádné požadavky na dálkově řídícího pilota nebo jiného člena posádky, které se týkají vyhodnocování U-space služeb. Systémový požadavek: Dálkově řídící pilot musí mít výcvik k vyhodnocení informace z poskytované U-space služby také není z pohledu metody SORA řešen.

Rozpory jsou v Příloze č. 3 vyznačeny červenou barvou.

Vyhodnocení metody FRAM poukázalo na rozpor u funkce Vyhodnocovat informace ze služeb U-space. Funkce byla pro systém označena za kritickou a stejně jako bylo argumentováno u rozporu při vyhodnocení metody STPA, tento požadavek aktuální metoda SORA a legislativa nestanovuje.

Z pohledu metody FRAM byla odhalena nesrovnalost u funkce Zajistit teoretický a praktický výcvik. Jedná se o funkci, která je předpokladem pro vyhodnocení informace ze služeb U-space, ale také pro mnoho jiných funkcí. Jedná se o klíčovou funkci pro systém. Nedostatek byl odhalen v obsahu výcviku, ale také při jeho prokázání, kdy se absolvování na základě vlastního prohlášení jeví jako nedostatečné. Posouzení znalostí a dovedností způsobilou třetí stranou se pro takto kritickou funkci jeví jako nutnost.

6 Závěr

V této diplomové práci bylo dosaženo stanoveného cíle, kterým bylo porovnání vhodnosti aplikace metod pro hodnocení provozní bezpečnosti aktuálně používaných v letectví na jeden vybraný specifický provoz UAS. Na vybraný provoz specifické kategorie, kterým je převoz lékařského materiálu mezi nemocničními areály v Praze, byla aplikována metoda SORA, tak jak Úřad pro civilní letectví České republiky po žadatelích o schválení Oprávnění k provozu vyžaduje. Metoda SORA nabízí holistický přístup a slouží jako nástroj pro žadatele i příslušný úřad k hodnocení provozních rizik, která daný provoz představuje. Je počítáno s postupnými revizemi metody, což porovnání s výsledky systémových metod potvrdilo.

Pro dosažení cíle této diplomové práce byly vybrány systémové metody hodnocení provozní bezpečnosti STPA a FRAM. Na zamýšlený provoz je pohlíženo jako na socio-technický systém, jehož součástí jsou prvky vzdušného prostoru U-space. Vypracování metody STPA bylo provedeno podle autory definovaných kroků. Výsledky metody ve formě omezení a systémových požadavků byly porovnány s cíli provozní bezpečnosti stanovené metodou SORA. Metoda FRAM byla vypracována podle práce týmu doktora Patriarca. Konkrétně se jedná o dekompozici systému z pohledu jeho funkcí do jednotlivých úrovní abstrakce, tak aby bylo dosaženo optimální úrovně detailu, se kterou byly provede další kroky analýzy. Pro další postup byla zvolena úroveň abstrakce fyzických funkcí. Vypracování analýzy bylo dále provedeno za pomocí kvantitativního přístupu simulace Monte Carlo vytvořenou pro metodu FRAM. Posledním krokem bylo porovnání výsledků s požadavky stanovené aktuálně používanou metodou SORA a platnou legislativou.

Limitací této práce je skutečnost, že vypracována metoda STPA zahrnuje pro zamýšlený provoz všechny důležité prvky, avšak kostru zamýšleného provozu je možné analyzovat podrobněji. Velmi detailní analýza by mohla blíže zkoumat fungování dálkově řídící stanice pilota nebo způsob, jakým jsou přijímány externí služby, jako jsou pro příklad U-space služby. Obsahem analýzy by mohl být také systém, který je zodpovědný za provedení automatického letu a systém pro převzetí manuálního řízení bezpilotního letadla.

Druhou limitací je vyhodnocení simulace, která je v této práci součástí metody FRAM. Simulace Monte Carlo je vyhodnocena za pomoci expertního názoru namísto rozdělení pravděpodobnosti jednotlivých výstupů funkcí. Výsledky analýzy, která by byla vytvořena s ohledem na reálná data z provozu, by se mohly lišit od výsledků prezentovaných v této diplomové práci. Překážkou však zůstává tato data získat nebo predikovat, jelikož se jedná o provoz v prostředí U-space.

I přes výše zmíněné limitace tato práce přináší kompletní bezpečnostní analýzu založenou na metodě STPA, která může sloužit jako podklad pro další zkoumání provozu bezpilotních systémů. V neposlední řadě je také vytvořena komparace omezení a požadavků na systém s požadavky aktuální verze metody SORA. Je vytvořena také kompletní bezpečnostní analýza podle metody FRAM, která kombinuje prvky Abstraktní hierarchie. Použitá simulace Monte Carlo nabízí kvantitativní přístup k hodnocení variability a tato práce může sloužit jako podklad pro její další využití. V neposlední řadě tato práce odhalila požadavky, které by při nedodržení mohly představovat rizika pro provoz bezpilotních systému.

Výsledek této diplomové práce může sloužit jako podnět pro rozšíření a zpřesnění stávajících legislativních požadavků. Dále může výsledek sloužit pro modifikaci metody SORA, tak aby odpovídala požadavkům aktuálního a plánovaného provozu bezpilotních systémů. Navzdory tomu, že SORA zohledňuje výkonnost U-space služeb a ostatních externích služeb nezbytných k bezpečnému provedení zamýšleného provozu, nestanovuje žádné požadavky k jejich vyhodnocení.

Zdroje

[1] *Easy Access Rules for Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945)* [online]. 30.8.2021 [cit. 2022-04-21]. Dostupné z: https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu

[2] LEVESON, Nancy G. a John P. THOMAS. *STPA Handbook* [online]. 2018 [cit. 2022-04-25]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[3] HOLLNAGEL, Erik. (2012). *FRAM: The functional resonance analysis method: Modelling complex Socio-technical systems*. Ashgate Publishing.

[4] PATRIARCA, Riccardo, Johan BERGSTRÖM a Giulio Di GRAVIO. *Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM* [online]. 2017, 34-46 [cit. 2022-04-24]. Dostupné z: https://doi.org/10.1016/j.ress.2017.03.032

[5] PATRIARCA, Riccardo, Giulio DI GRAVIO a Francesco COSTANTINO. *A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems*. Safety Science [online]. 2017, 91, 49-60 [cit. 2022-04-24]. ISSN 09257535. Dostupné z: https://doi.org/10.1016/j.ssci.2016.07.016

[6] LEVESON, Nancy G. (2012). *Engineering a Safer World*, MIT Press.

[7] LIND, Morten. *Making Sense of the Abstraction Hierarchy* [online]. 1999 [cit. 2022-05-04]. Dostupné z: https://www.researchgate.net/publication/2390022_Making_Sense_of_the_Abstraction_Hierarchy

[8] *Safety Management Manual: Doc 9859* [online]. Fourth Edition. 2018 [cit. 2022-05-02]. ISBN 978-92-9258-552-5. Dostupné z: https://skybrary.aero/sites/default/files/bookshelf/5863.pdf

[9] HOLLNAGEL, Erik. *Safety-I and Safety-II: The Past and Future of Safety Management*. ASHGATE, 2014. ISBN 978 1 4724 2306 1.

[10] *SESAR Joint Undertaking: Smart ATM U-space* [online]. [cit. 2022-05-02]. Dostupné z: https://www.sesarju.eu/U-space

[11] ALAMOURI, Ahmed, Astrid LAMPERT a Markus GERKE. *New UAS regulations in the EU and their impact on effective usage of UAS* [online]. [cit. 2022-05-02]. Dostupné z: https://www.researchgate.net/publication/359587574_New_UAS_regulations_in_the_EU_and_their_impact_on_effective_usage_of_UAS

[12] HU, Jueming. *Probabilistic Risk Assessment and Mitigation for UAS Safety and Traffic Management* [online]. [cit. 2022-05-02]. Dostupné z: https://www.researchgate.net/publication/349499971_Probabilistic_Risk_Assessment_and_Mitigation_for_UAS_Safety_and_Traffic_Management?fbclid=IwAR32e7pDWfUEQbHhJPkdfulxApmWGGG6tslFnJnWs1OQbxIYO9AALIrl03g

[13] KONERT, Anna a Piotr KASPRZYK. *UAS Safety Operation – Legal Issues on Reporting UAS Incidents* [online]. [cit. 2022-05-03]. Dostupné z: https://www.researchgate.net/publication/355689027_UAS_Safety_Operation_-_Legal_Issues_on_Reporting_UAS_Incidents?fbclid=IwAR0CSbf4xvda5xYfIJbfFsmHy5j5X6Oxmk2xVKlMJRk5PwoLh7M7XXCliCY

[14] CHEN, Jieyu, Shuguang ZHANG, Yi LU a Peng TANG. *STPA-based Hazard Analysis of a Complex UAV System in Take-off* [online]. 2015 [cit. 2022-05-03]. Dostupné z: https://www.researchgate.net/publication/304465020_STPA-based_hazard_analysis_of_a_complex_UAV_system_in_take-off

[15] CHATZIMICHAILIDOU, Maria Mikela, Nektarios KARANIKAS a Anastasios PLIOUTSIAS. *Application of STPA on Small Drone Operations: A Benchmarking Approach* [online]. 2017 [cit. 2022-05-03]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877705817312079

[16] MATRICE 300 RTK - Specification. Dji.com [online]. [cit. 2022-05-05]. Dostupné z: https://www.dji.com/cz/matrice-300/specs

[17] Notice of Proposed Amendment 2021-14: Development of acceptable means of compliance and guidance material to support the U-space regulation [online]. 2021, 117 [cit. 2022-05-07]. Dostupné z: https://www.easa.europa.eu/downloads/134303/en?fbclid=IwAR0EKrly5NTtzBNFAbGoySut1Z57M1W1ypN-NQL2ifFamqjkEn5WUpHnuak

Příloha 1: STPA

ID	***Loss***	
L-1:	Ztráta UAS	
L-2:	Ztráta převáženého materiálu	
L-3:	Zranění osoby	
L-4:	Ztráta Oprávnění k provozu	
L-5:	Ztráta nebo poškození majetku	
L-6:	Ztráta akceptace veřejností	
L-7:	Ztráta mise	
ID	***Hazard***	***Reference***
H-1:	Ztráta kontroly nad UAS	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]
H-2:	UAS není způsobilý pro provoz	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]
H-3:	Nedodržení stanovené výšky letu	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]
H-4:	Nedodržení letové trajektorie	[L-4, L-7]
H-5:	Narušení minimální separace mezi UAS a jiným letad	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]
H-6:	Personál není způsobilý pro provoz	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]
ID	***System-level Constraints***	***ID***
SC-1:	Nesmí dojít ke ztrátě kontroly nad UAS	[H-1]
SC-2:	UAS musí být způsobilý pro provoz	[H-2]
SC-3:	Musí být dodržena stanovená výška letu	[H-3]
SC-4:	Musí být dodržena letová trajektorie	[H-4]
SC-5:	Musí být dodržena minimální separace mezi UAS a ji	[H-5]
SC-6:	Personál musí být způsobilý pro provoz	[H-6]

Role	Responsibility	Control Actions
1. úroveň		
EASA	- harmonizovaná pravidla provozu UAS - pravidla a postupy registru - požadavky na konstrukci UAS	MD: - stanovení jednotných pravidel a jejich výkladu ÚCL: - stanovení pokynů k zajištění dozoru nad implementací pravidel - auditování nastavených pravidel ÚZPLN: - stanovení postupů vyšetřování leteckých nehod Výrobce UAS: - stanovení harmonizovaných pravidel konstrukce
2. úroveň		
MD	- tvorba legislativy - odvolávací orgán	ÚCL: - tvorba legislativy LAA ČR: - projednání prostorů
3. úroveň		
ÚCL	- pravidla pro standardní scénáře - pravidla létání obecně - požadavky na personál bezpilotního systému - cerfifikace pilota - požadavky na provozovatele - registrace provozovatele - požadavky na UA - schvalování provozu specifické kategorie - stanovení prostorů - geofencing - certifikace poskytovatele U-space služeb - poskytnutí dat od státu do CIS - certifikace CIS poskytovatele	Provozovatel UAS: - stanovení pravidel pro registraci provozovatele - schválení daného provozu specifické kategorie - auditování schváleného provozu - stanovení požadavků na provozovatele UAS Dálkově řídící pilot: - stanovení pravidel pro certifikaci pilota - stanovení požadavků na dálkově řídícího pilota Člen personálu: - stanovení požadavků údržby UAS FIS (AFIS): - osvědčení ATSP a pravidla poskytování ANSP ČR: - certifikace ANSP a pravidla poskytování CIS: - certifikace a poskytování dat USSP: - stanovení pravidel pro poskytování U-space služeb - certifikace USSP a pravidla poskytování - kontrola plnění závazků
4. úroveň		
ÚZPLN	- odborné šetření příčin leteckých nehod - publikace závěrů šetření za účelem zvýšení bezpečnosti	
Výrobce UAS	- výroba UAS v souladu s harmonizovanými pravidly	Provozovatel UAS: - poskytnutí provozního manuálu UAS
5. úroveň		
CIS	- poskytování informací potřebných pro zajištění služeb U-space - výměna dat mezi USSP a ANSP - výměna dat s CIS jiných států - data pro mapu provozu (informace o provozu a prostorech) - poskytuje informace o provozu PČR a AČR	
FIS (AFIS)		
ANSP ČR	- řízení letů řízeného "manned" provozu - poskytování dat o prostorech, řízeném provozu	Řízený "manned" provoz - řízení, poskytování letových navigačních služeb
Provozovatel UAS	- nese odpovědnost za misi - definování mise - stanovení provozních postupů - poskytnutí provozní příručky - aktualizace dat v UA - zajištění provozuschopného stavu UA - požadavky na doplňkové služby - požadavky na služby U-space - zajištění teoretického a praktického výcviku posádce - splnění registrace provozovatele - získání Oprávnění k provozu pro zamýšlený provoz - hlášení událostí ÚZPLN - stanovení postupů koordinace vícečlenné posádky - zapisování činností o letu a vedení záznamů - zajištění pojistného krytí - vedení záznamů o výcviku posádky	Člen personálu - poskytnutí provozní příručky - definování zamýšleného provozu - stanovení provozních postupů - zajištění teoretického a praktického výcviku pro danou pozici - periodická kontrola požadovaných znalostí a výcviku pro danou pozici - stanovení postupů koordinace vícečlenné posádky Dálkově řídící pilot - poskytnutí provozní příručky - definování zamýšleného provozu - stanovení provozních postupů - zajištění teoretického a praktického výcviku pro danou pozici - periodická kontrola požadovaných znalostí a výcviku pro danou pozici - stanovení postupů koordinace vícečlenné posádky UA - aktualizace dat v UA - zajištění provozuschopného stavu UA
USSP	- poskytování U-space služeb podle předem definovaných pravidel - plnění certifikace - hlášení událostí ÚZPLN	Dálkově řídící pilot - poskytování U-space služeb
6. úroveň		
Řízený "manned" provoz		
Člen personálu	- odpovědnost za zajištění vzletového a přistávácího místa - provedení předletové kontroly bezpilotního letadla - odpovědnost za zajištění přepravovaného materiálu - absolvování teoretického a praktického výcviku - provádění činností údržby	UA - provedení předletové a poletové kontroly - provádění činnosti údržby Přepravovaný materiál - zajištění přepravovaného materiálu
Dálkově řídící pilot	- odpovědnost za bezpečné provedení letu UA - v případě potřeby převezme řízení nad UA - absolvování vstupního výcviku, pravidelných školení a přezkoušení - splnění požadavků a certifikace pilota dle ÚCL - vyhodnocení informace z poskytované U-space služby	Stanice dálkově řídícího pilota - řídící pokyny pro pohyb UA - nastavení UAS a ověření funkčnosti - vyhodnocení informace z poskytované U-space služby
7. úroveň		
Stanice dálkově řídícího pilota	- zajištění řídících pokynů UA od dálkově řídícího pilota - přijímat a zobrazovat informace U-space služeb	UA - činnost podle řídících signálů - přijímání a zobrazování U-space služeb
8. úroveň		
Převážený materiál	- musí být správně zajištěn k UA	
UA	- chování dle řídících signálů a přednastavených pravidel	

UCA ID	from	to	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long	Controller Constraint 1	Controller Constraint 2	Controller Constraint 3	Controller Constraint 4
UCA-1.1:	EASA	MD	stanovení jednotných pravidel a jejich výkladu	jednotná pravidla a jejich výklad nejsou stanovena před zahájením provozu	jednotná pravidla a jejich výklad jsou stanovena neúplně před zahájení provozu	jednotná pravidla a jejich výklad jsou stanovena po zahájení provozu	-	jednotná pravidla a jejich výklad musí být stanovena před zahájením provozu	jednotná pravidla a jejich výklad musí být stanovena úplně před zahájením provozu	jednotná pravidla a jejich výklad nesmí být stanovena po zahájení provozu	
UCA-1.2:		ÚCL	stanovení pokynů k zajištění dozoru nad implementací pravidel	pokyny k zajištění dozoru nad implementací pravidel nejsou stanoveny před zahájením provozu	pokyny k zajištění dozoru nad implementací pravidel jsou stanoveny před zahájení provozu neúplně	pokyny k zajištění dozoru nad implementací pravidel jsou stanoveny po zahájení provozu	-	pokyny k zajištění dozoru nad implementací pravidel musí být stanoveny před zahájením provozu	pokyny k zajištění dozoru nad implementací pravidel musí být stanoveny úplně před zahájením provozu	pokyny k zajištění dozoru nad implementací pravidel nesmí být stanoveny po zahájení provozu	
UCA-1.3:			auditování nastavených pravidel	nastavená pravidla se po zahájení provozu neauditují	nastavená pravidla se auditují neúplně po zahájení provozu	-	-	nastavená pravidla se po zahájení provozu musí auditovat	nastavená pravidla se po zahájení provozu musí auditovat úplně		
UCA-1.4:		ÚZPLN	stanovení postupů vyšetřování leteckých nehod	postupy vyšetřování leteckých nehod nejsou stanoveny	postupy vyšetřování leteckých nehod jsou stanoveny neúplně	postupy vyšetřování leteckých nehod jsou stanoveny pozdě	-	postupy vyšetřování leteckých nehod musí být stanoveny	postupy vyšetřování leteckých nehod musí být stanoveny úplně	postupy vyšetřování leteckých nehod nesmí být stanoveny pozdě	
UCA-1.5:		Výrobce UAS	stanovení harmonizovaných pravidel konstrukce	harmonizovaná pravidla konstrukce nejsou stanovena před zahájením provozu	harmonizovaná pravidla konstrukce jsou stanovena neúplně před zahájením provozu	harmonizovaná pravidla konstrukce jsou stanovena po zahájení provozu	-	harmonizovaná pravidla konstrukce musí být stanovena před zahájením provozu	harmonizovaná pravidla konstrukce musí být stanovena úplně před zahájením provozu	harmonizovaná pravidla konstrukce nesmí být stanovena po zahájení provozu	
UCA-2.1:	MD	ÚCL	tvorba legislativy	legislativa není před zahájením provozu vytvořena	legislativa je před zahájením vytvořena neúplně	legislativa je vytvořena po zahájení provozu	-	legislativa musí být vytvořena před zahájením provozu	legislativa musí být vytvořena úplně před zahájením provozu	legislativa nesmí být vytvořena po zahájení provozu	
UCA-2.2:		LAA ČR	projednání prostorů	prostory nejsou před tvorbou pravidel projednány	-	-	-	prostory musí být před tvorbou pravidel projednány			
UCA-3.1:	ÚCL	Provozovatel UAS	stanovení pravidel pro registraci provozovatele	pravidla pro registraci provozovatele nejsou před zahájením provozu stanovena	pravidla pro registraci provozovatele jsou před zahájením provozu stanovena neúplně	pravidla pro registraci provozovatele jsou stanovena po zahájení provozu	-	pravidla pro registraci provozovatele musí být stanovena před zahájením provozu	pravidla pro registraci provozovatele musí být stanovena úplně před zahájením provozu	pravidla pro registraci provozovatele nesmí být stanovena po zahájení provozu	
UCA-3.2:			schválení daného provozu specifické kategorie	daný provoz není schválen před zahájením provozu	daný provoz je před zahájením provozu schválen, avšak neměl by být	daný provoz je schválen po zahájení provozu	-	daný provoz musí být schválen před zahájením provozu	daný provoz nesmí být před zahájením provozu schválen, pokud nejsou splněny všechny požadavky	daný provoz nesmí být schválen po zahájení provozu	
UCA-3.3:			auditování schváleného provozu	schválený provoz se po zahájení provozu neaudituje	schválený provoz se po zahájení provozu audituje neúplně	-	-	schválený provoz se po zahájení provozu musí auditovat	schválený provoz se po zahájení musí auditovat úplně		
UCA-3.4:			stanovení požadavků na provozovatele UAS	požadavky na provozovatele UAS nejsou před zahájením provozu stanoveny	požadavky na provozovatele UAS jsou před zahájením provozu stanoveny neúplně	požadavky na provozovatele UAS jsou stanoveny po zahájení provozu	-	požadavky na provozovatele UAS musí být stanoveny před zahájením provozu	požadavky na provozovatele UAS musí být stanoveny úplně před zahájením provozu	požadavky na provozovatele UAS nesmí být stanoveny po zahájení provozu	
UCA-3.5:		Dálkově řídící pilot UAS	stanovení pravidel pro certifikaci pilota	pravidla pro certifikaci pilota nejsou před zahájením provozu stanovena	pravidla pro certifikaci pilota jsou před zahájením provozu stanovena neúplně	pravidla pro certifikaci pilota jsou stanovena po zahájení provozu	-	pravidla pro certifikaci pilota musí být stanovena před zahájením provozu	pravidla pro certifikaci pilota musí být stanovena úplně před zahájením provozu	pravidla pro certifikaci pilota nesmí být stanovena po zahájení provozu	
UCA-3.6:			stanovení požadavků na dálkově řídícího pilota	požadavky na dálkově řídícího pilota nejsou před zahájením provozu stanoveny	požadavky na dálkově řídícího pilota jsou před zahájením provozu stanoveny neúplně	požadavky na dálkově řídícího pilota jsou stanoveny po zahájení provozu	-	požadavky na dálkově řídícího pilota musí být stanoveny před zahájením provozu	požadavky na dálkově řídícího pilota musí být stanoveny úplně před zahájením provozu	požadavky na dálkově řídícího pilota nesmí být stanoveny po zahájení provozu	
UCA-3.7:		Člen personálu	stanovení požadavků údržby UAS	požadavky údržby UAS nejsou před zahájením provozu stanoveny	požadavky údržby UAS jsou před zahájením provozu stanoveny neúplně	požadavky údržby UAS jsou stanoveny po zahájení provozu		požadavky údržby UAS musí být stanoveny před zahájením provozu	požadavky údržby UAS musí být stanoveny úplně před zahájením provozu	požadavky údržby UAS nesmí být stanoveny po zahájení provozu	
UCA-3.8:		FIS (AFIS)	osvědčení ATSP a pravidla poskytování	osvědčení ATSP a pravidla poskytování nejsou stanovena	osvědčení ATSP a pravidla poskytování jsou stanovena neúplně	osvědčení ATSP a pravidla poskytování jsou stanovena pozdě	-	osvědčení ATSP a pravidla poskytování musí být stanovena	osvědčení ATSP a pravidla poskytování musí být stanovena úplně	osvědčení ATSP a pravidla poskytování nesmí být stanovena pozdě	
UCA-3.9:		ANSP ČR	certifikace ANSP a pravidla poskytování	certifikace ANSP a pravidla poskytování nejsou stanovena	certifikace ANSP a pravidla poskytování jsou stanovena neúplně	certifikace ANSP a pravidla poskytování jsou stanovena pozdě	-	certifikace ANSP a pravidla poskytování musí být stanovena	certifikace ANSP a pravidla poskytování musí být stanovena úplně	certifikace ANSP a pravidla poskytování nesmí být stanovena pozdě	
UCA-3.10:		CIS	certifikace CIS a poskytování dat	certifikace CIS a poskytování dat není stanoveno	certifikace CIS a poskytování dat je stanoveno neúplně	certifikace CIS a poskytování dat je stanoveno pozdě	-	certifikace CIS a poskytování dat musí být stanoveno	certifikace CIS a poskytování dat musí být stanovena úplně	certifikace CIS a poskytování dat nesmí být stanovena pozdě	
UCA-3.11:		USSP	stanovení pravidel pro poskytování U-space služeb	pravidla pro poskytování U-space služeb nejsou před zahájením provozu stanovena	pravidla pro poskytování U-space služeb jsou před zahájením provozu stanovena neúplně	pravidla pro poskytování U-space služeb jsou stanovena po zahájení provozu	-	pravidla pro poskytování U-space služeb musí být stanovena před zahájením provozu	pravidla pro poskytování U-space služeb musí být stanovena před zahájením provozu úplně	pravidla pro poskytování U-space služeb nesmí být stanovena po zahájení provozu	
UCA-3.12:			certifikace USSP a pravidla poskytování	certifikace USSP a pravidla poskytování nejsou stanovena	certifikace USSP a pravidla poskytování jsou stanovena neúplně	certifikace USSP a pravidla poskytování jsou stanovena pozdě	-	certifikace USSP a pravidla poskytování musí být stanovena	certifikace USSP a pravidla poskytování musí být stanovena úplně	certifikace USSP a pravidla poskytování nesmí být stanovena pozdě	
UCA-3.13:			kontrola plnění závazků	plnění závazků není v průběhu provozu kontrolováno	plnění závazků je v průběhu provozu kontrolováno neúplně	-	-	plnění závazků musí být kontrolováno v průběhu provozu	plnění závazků musí být kontrolováno úplně v průběhu provozu		

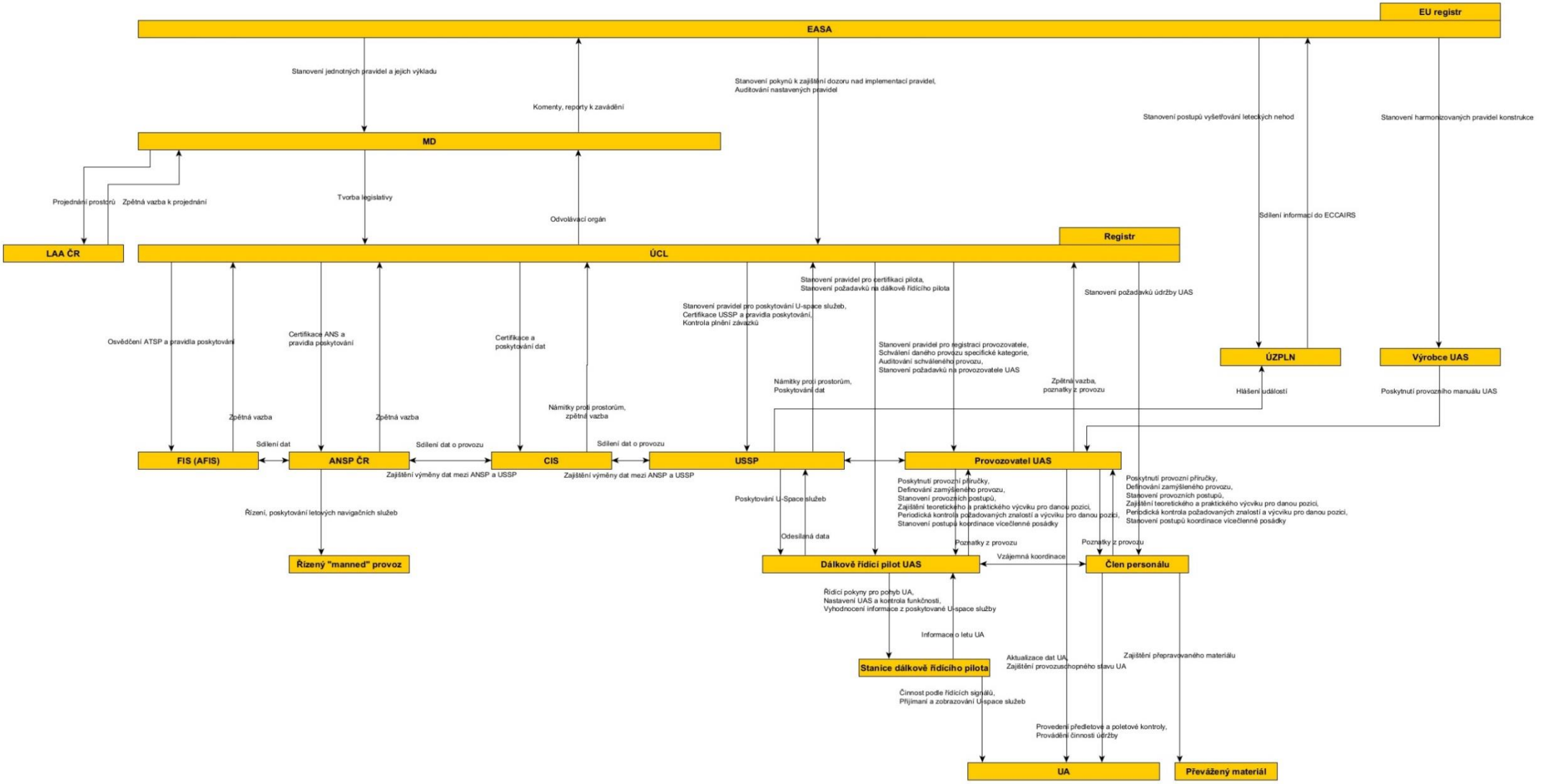
UCA-4.1:	Výrobce UAS	Provozovatel UAS	poskytnutí provozního manuálu UAS	provozní manuál UAS není poskytnut	provozní manuál UAS je poskytnut nekompletní	provozní manuál UAS je poskytnut pozdě	-	provozní manuál UAS musí být poskytnut	provozní manuál UAS musí být poskytnut kompletní	provozní manuál UAS nesmí být poskytnut pozdě	
UCA-5.1:	ANSP ČR	Řízený "manned" provoz	řízení, poskytování letových navigačních služeb	řízení, letové navigační služby nejsou poskytnuty	řízení, letové navigační služby jsou poskytnuty neúplně	řízení, letové navigační služby jsou poskytnuty pozdě	řízení, letové navigační služby přestanou být poskytovány	řízení, letové navigační služby musí být poskytnuty	řízení, letové navigační služby musí být poskytnuty úplně	řízení, letové navigační služby nesmí být poskytnuty pozdě	řízení, letové navigační služby nesmí přestat být poskytováno
UCA-6.1:	Provozovatel UAS	Člen personálu	poskytnutí provozní příručky	provozní příručka není poskytnuta před zahájením provozu	provozní příručka je poskytnuta před zahájením provozu nekompletní	provozní příručka je poskytnuta po zahájení provozu	-	provozní příručka musí být poskytnuta před zahájením provozu	provozní příručka musí být poskytnuta kompletní před zahájením provozu	provozní příručka nesmí být poskytnuta po zahájení provozu	
UCA-6.2:			definování zamýšleného provozu	zamýšlený provoz není před zahájením provozu definován	zamýšlený provoz je před zahájením provozu definován neúplně	zamýšlený provoz je definován po zahájení provozu	-	zamýšlený provoz musí být definován před jeho zahájením	zamýšlený provoz musí být kompletně definován před jeho zahájením	zamýšlený provoz nesmí být definován po jeho zahájením	
UCA-6.3:			stanovení provozních postupů	provozní postupy nejsou před zahájením provozu stanoveny	provozní postupy jsou před zahájením provozu stanoveny neúplně	provozní postupy jsou stanoveny po zahájení provozu	-	provozní postupy musí být stanoveny před zahájením provozu	provozní postupy musí být kompletně stanoveny před zahájením provozu	provozní postupy nesmí být stanoveny po zahájení provozu	
UCA-6.4:			zajištění teoretického a praktického výcviku pro danou pozici	teoretický nebo praktický výcvik není zajištěn před zahájením provozu	teoretický nebo praktický výcvik je při zahájení provozu nedostatečný	teoretický nebo praktický výcvik je zajištěn po zahájení provozu	teoretický nebo praktický výcvik skončí před jeho dokončením	teoretický nebo praktický výcvik musí být zajištěn před zahájením provozu	teoretický a praktický výcvik musí být dostatečný při zahájení provozu	teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu	teoretický a praktický výcvik nesmí skončit před jeho dokončením
UCA-6.5:			periodická kontrola požadovaných znalostí a výcviku pro danou pozici	požadované znalosti a výcvik nejsou v průběhu provozu periodicky kontrolovány	požadované znalosti a výcvik nejsou v průběhu provozu kontrolovány kompletně a periodicky	-	-	požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány	požadované znalosti a výcvik musí být průběhu provozu kontrolovány kompletně a periodicky		
UCA-6.6:			stanovení postupů koordinace vícečlenné posádky	postupy koordinace vícečlenné posádky nejsou před zahájením provozu stanoveny	postupy koordinace vícečlenné posádky jsou před zahájením provozu stanoveny nekompletně	postupy koordinace vícečlenné posádky jsou stanoveny po zahájení provozu	-	postupy koordinace vícečlenné posádky musí být stanoveny před zahájením provozu	postupy koordinace vícečlenné posádky musí být stanoveny kompletně před zahájením provozu	postupy koordinace vícečlenné posádky nesmí být stanoveny po zahájení provozu	
UCA-6.7:		Dálkově řídící pilot UAS	poskytnutí provozní příručky	provozní příručka není poskytnuta před zahájením provozu	provozní příručka je poskytnuta před zahájením provozu nekompletní	provozní příručka je poskytnuta po zahájení provozu	-	provozní příručka musí být poskytnuta před zahájením provozu	provozní příručka musí být poskytnuta kompletní před zahájením provozu	provozní příručka nesmí být poskytnuta po zahájení provozu	
UCA-6.8:			definování zamýšleného provozu	zamýšlený provoz není před zahájením provozu definován	zamýšlený provoz je před zahájením provozu definován neúplně	zamýšlený provoz je definován po zahájení provozu	-	zamýšlený provoz musí být definován před jeho zahájením	zamýšlený provoz musí být kompletně definován před jeho zahájením	zamýšlený provoz nesmí být definován po jeho zahájením	
UCA-6.9:			stanovení provozních postupů	provozní postupy nejsou před zahájením provozu stanoveny	provozní postupy jsou před zahájením provozu stanoveny neúplně	provozní postupy jsou stanoveny po zahájení provozu	-	provozní postupy musí být stanoveny před zahájením provozu	provozní postupy musí být kompletně stanoveny před zahájením provozu	provozní postupy nesmí být stanoveny po zahájení provozu	
UCA-6.10:			zajištění teoretického a praktického výcviku pro danou pozici	teoretický nebo praktický výcvik není zajištěn před zahájením provozu	teoretický nebo praktický výcvik je při zahájení provozu nedostatečný	teoretický nebo praktický výcvik je zajištěn po zahájení provozu	teoretický nebo praktický výcvik skončí před jeho dokončením	teoretický nebo praktický výcvik musí být zajištěn před zahájením provozu	teoretický a praktický výcvik musí být dostatečný při zahájení provozu	teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu	teoretický a praktický výcvik nesmí skončit před jeho dokončením
UCA-6.11:			periodická kontrola požadovaných znalostí a výcviku pro danou pozici	požadované znalosti a výcvik nejsou v průběhu provozu periodicky kontrolovány	požadované znalosti a výcvik nejsou v průběhu provozu kontrolovány kompletně a periodicky	-	-	požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány	požadované znalosti a výcvik musí být průběhu provozu kontrolovány kompletně a periodicky		
UCA-6.12:			stanovení postupů koordinace vícečlenné posádky	postupy koordinace vícečlenné posádky nejsou před zahájením provozu stanoveny	postupy koordinace vícečlenné posádky jsou před zahájením provozu stanoveny nekompletně	postupy koordinace vícečlenné posádky jsou stanoveny po zahájení provozu	-	postupy koordinace vícečlenné posádky musí být stanoveny před zahájením provozu	postupy koordinace vícečlenné posádky musí být stanoveny kompletně před zahájením provozu	postupy koordinace vícečlenné posádky nesmí být stanoveny po zahájení provozu	
UCA-6.13:		UA	aktualizace dat v UA	data v UA nejsou před zahájením provozu aktualizována	data v UA jsou před zahájením provozu aktualizována nekompletně	data v UA jsou aktualizována po zahájení provozu	-	data v UA musí být před zahájením provozu aktualizována	data v UA musí být před zahájením provozu kompletně aktualizována	data v UA nesmí být aktualizována po zahájení provozu	
UCA-6.14:			zajištění provozuschopného stavu UA	UA není v provozuschopném stavu před zahájením provozu	-	-	-	UA musí být v provozuschopném stavu před zahájením provozu			
UCA-7.1:	USSP	Dálkově řídící pilot UAS	poskytování U-space služeb	U-space služby nejsou v průběhu provozu poskytovány	U-space služby jsou v průběhu provozu poskytovány nekompletně	U-space služby jsou poskytovány pozdě	U-space služby přestanou být v průběhu provozu poskytovány	U-space služby musí být v průběhu provozu poskytovány	U-space služby musí být v průběhu provozu poskytovány kompletně	U-space služby nesmí být poskytovány pozdě	Poskytování U-space služeb nesmí být v průběhu provozu přerušeno
UCA-8.1:	Člen personálu	UA	provedení předletové a poletové kontroly	předletová nebo poletová kontrola nebyla provedena	předletová nebo poletová kontrola byla provedena neúplně	předletová nebo poletová kontrola byla provedena pozdě	-	předletová a poletová kontrola musí být provedena	předletová a poletová kontrola musí být provedena kompletně	předletová a poletová kontrola nesmí být provedeny pozdě	
UCA-8.2:			provádění činnosti údržby	činnosti údržby nebyly před zahájením provozu provedeny	činnosti údržby byly před zahájením provozu provedeny v rozporu s manuálem výrobce	-	-	činnosti údržby musí být provedeny před zahájením provozu	činnosti údržby nesmí být před zahájením provozu provedeny v rozporu s manuálem výrobce		
UCA-8.3:		Přepravovaný materiál	zajištění přepravovaného materiálu	přepravovaný materiál nebyl před zahájením provozu zajištěn	přepravovaný materiál byl před zahájením provozu zajištěn špatně	-	-	přepravovaný materiál musí být před zahájením provozu zajištěn	přepravovaný materiál nesmí být před zahájením provozu zajištěn špatně		
UCA-9.1:	Dálkově řídící pilot	Stanice dálkově řídícího pilota	řídící pokyny pro pohyb UA	řídící pokyny pro pohyb UA v průběhu provozu nejsou provedeny	řídící pokyny pro pohyb UA jsou v průběhu provozu provedeny špatně	řídící pokyny pro pohyb UA jsou v průběhu provozu provedeny pozdě	řídící pokyny pro pohyb UA přestanou být v průběhu provozu prováděny	řídící pokyny pro pohyb UA musí být v průběhu provozu provedeny	řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny špatně	řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny pozdě	provádění řídících pokynů pro pohyb UA nesmí v průběhu provozu přestat
UCA-9.2:			nastavení UAS a kontrola funkčnosti	nastavení UAS a kontrola funkčnosti není před zahájením provozu provedena	nastavení UAS a kontrola funkčnosti je před zahájením provozu provedena špatně	nastavení UAS a kontrola funkčnosti je provedena po zahájení provozu	-	nastavení UAS a kontrola funkčnosti musí být provedena před zahájením provozu	nastavení UAS a kontrola funkčnosti nesmí být provedena špatně před zahájením provozu	nastavení UAS a kontrola funkčnosti nesmí být provedeno po zahájení provozu	
UCA-9.3:			vyhodnocení informace z poskytované U-space služby	informace z poskytované U-space služby není v průběhu provozu vyhodnocena	informace z poskytované U-space služby je v průběhu provozu vyhodnocena špatně	informace z poskytované U-space služby je vyhodnocena pozdě	-	informace z poskytované U-space služby musí být v průběhu provozu vyhodnocena	informace z poskytované U-space služby nesmí být v průběhu provozu vyhodnocena špatně	informace z poskytované U-space služby nesmí být vyhodnocena pozdě	
UCA-10.1:	Stanice dálkově řídícího pilota	UA	činnost podle řídících signálů	činnost podle řídících signálů není v průběhu provozu provedena	činnost podle řídících signálů je v průběhu provozu provedena špatně	činnost podle řídících signálů je provedena pozdě	činnost podle řídících signálů přestane být v průběhu provozu prováděna	činnost podle řídících signálů musí být v průběhu provozu provedena	činnost podle řídících signálů nesmí být v průběhu provozu provedena špatně	činnost podle řídících signálů nesmí být provedena pozdě	provádění činnosti podle řídících signálu nesmí v průběhu provozu přestat
UCA-10.2:			přijímaní a zobrazování U-space služeb	U-space služby nejsou v průběhu provozu přijímány nebo zobrazovány	U-space služby jsou v průběhu provozu přijímány nebo zobrazovány neúplně	U-space služby jsou v průběhu provozu přijímány nebo zobrazovány pozdě	U-space služby přestanou být v průběhu provozu přijímány nebo zobrazovány	U-space služby musí být v průběhu provozu přijímány nebo zobrazovány	U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány neúplně	U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány pozdě	přijímání nebo zobrazování U-space služeb nesmí v průběhu provozu přestat

ID	UCA ID	UCA	Hazard ref.	Loss ref.	Scenario: current level	Systemic requirements
Scenario 1	UCA-1.1:	EASA nestanoví jednotná pravidla a jejich výklad před zahájením provozu, nebo stanoví jednotná pravidla a jejich výklad před zahájením provozu neúplně, nebo stanoví jednotná pravidla a jejich výklad po zahájení provozu, protože…	[H-1, H-2, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nezná reálnou problematiku bezpilotního létání - nepovažuje jednotná pravidla a jejich výklad za podstatná - není schopna jednotná pravidla a jejich výklad vytvořit	- EASA musí znát problematiku bezpilotního létání - EASA musí považovat jednotná pravidla a jejich výklad za podstatná - EASA musí být schopna jednotná pravidla a jejich výklad vytvořit
Scenario 2	UCA-1.2:	EASA nestanoví pokyny k zajištění dozoru nad implementací pravidel před zahájením provozu, nebo stanoví pokyny k zajištění dozoru nad implementací pravidel před zahájením provozu neúplně, nebo stanoví pokyny k zajištění dozoru nad implementací pravidel po zahájení provozu, protože…	[H-2, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není schopna pokyny k zajištění dozoru nad implementací pravidel vytvořit	- EASA musí být schopna pokyny k zajištění dozoru nad implementací pravidel vytvořit
Scenario 3	UCA-1.3:	EASA neaudituje nastavená pravidla po zahájení provozu, nebo audituje nastavená pravidla po zahájení provozu neúplně, protože…	[H-2, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- auditování stanovenách pravidel není stanoveno	- EASA musí stanovit auditování stanovených pravidel
Scenario 4	UCA-1.4:	EASA nestanoví postupy vyšetřování leteckých nehod, nebo stanoví postupy vyšetřování leteckých nehod neúplně, nebo stanoví postupy vyšetřování leteckých nehod pozdě, protože…	[H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nezná problematiku vyšetřování leteckých nehod - postupy nezahrnují všechny možné scénáře leteckých nehod	- EASA musí znát problematiku vyšetřování leteckých nehod - EASA musí do postupů vyšetřování leteckých nehod zahrnout všechny možné scénáře leteckých nehod
Scenario 5	UCA-1.5:	EASA nestanoví harmonizovaná pravidla konstrukce UAS před zahájením provozu, nebo stanoví harmonizovaná pravidla konstrukce před zahájením provozu neúplně, nebo stanoví harmonizovaná pravidla konstrukce po zahájení provozu, protože…	[H-2, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- harmonizovaná pravidla konstrukce nejsou vytvořena - harmonizovaná pravidla konstrukce nejsou konzultována s výrobci UAS - nerozumí problematice konstrukce UAS	- EASA musí vytvořit harmonizovaná pravidla konstrukce - EASA musí konzultovat harmonizovaná pravidla konstrukce s výrobci UAS - EASA musí rozumět problematice konstrukce UAS
Scenario 6	UCA-2.1:	MD nevytvoří legislativu a pravidla před zahájením provozu, nebo vytvoří legislativu a pravidla před zahájením provozu neúplně, nebo vytvoří legislativu a pravidla po zahájení provozu, protože…	[H-1, H-2, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- legislativa a pravidla nejsou vytvořena - legislativa a pravidla jsou vytvořena neúplně nebo pozdě - legislativa a pravidla neodpovídají aktuální problematice	- MD musí vytvořit legislativu a pravidla - MD musí vytvořit legislativu úplně a včas - MD musí vytvořit legislativu a pravidla odpovídající aktuální problematice
Scenario 7	UCA-2.2:	MD neprojedná prostory před tvorbou pravidel, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neví, že prostory mají být projednány - projednání prostorů nepovažuje za důležité	- MD musí projednat prostory - MD musí projednání prostorů považovat za důležité
Scenario 8	UCA-3.1:	ÚCL nestanoví pravidla pro registraci provozovatele před zahájením provozu, nebo stanoví pravidla pro registraci provozovatele před zahájením provozu neúplně, nebo stanoví pravidla pro registraci provozovatele po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- pravidla pro registraci provozovatele nejsou stanovena	- ÚCL musí stanovit pravidla pro registraci provozovatele
Scenario 9	UCA-3.2:	ÚCL neschválí daný provoz před jeho zahájením, nebo schválí provoz před jeho zahájením, který by neměl být schválen, nebo schválí provoz po zahájení provozu, protože…	[H-1, H-2, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- se neřídí jednotnými pravidly - nemá dostatečnou kapacitu pro vyřizování žádostí o Oprávnění k provozu - nemá zkušenosti s vyřizováním žádostí o Oprávnění k provozu	- ÚCL se musí řídit jednotnými pravidly - ÚCL musí mít dostatečnou kapacitu pro vyřizování žádostí o Oprávnění k provozu - ÚCL musí mít zkušenosti s vyřizováním žádostí o Oprávnění k provozu
Scenario 10	UCA-3.3:	ÚCL neaudituje schválený provoz po jeho zahájení, nebo audituje schválený provoz po jeho zahájení neúplně, protože…	[H-1, H-2, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nejsou stanovena pravidla pro auditování provozu - nemá dostatečnou kapacitu pro auditování provozu - nemá dostatečné znalosti nebo zkušenosti pro auditování provozu	- ÚCL musí mít stanovené pravidla pro auditování provozu - ÚCL musí mít dostatečnou kapacitu pro auditování provozu - ÚCL musí mít dostatečné znalosti a zkušenosti pro auditování provozu
Scenario 11	UCA-3.4:	ÚCL nestanoví požadavky na provozovatele UAS před zahájením provozu, nebo stanoví požadavky na provozovatele UAS před zahájením provozu neúplně, nebo stanoví požadavky na provozovatele UAS po zahájení provozu, protože…	[H-1, H-2, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není stanoven rámec, ze kterého by ÚCL požadavky mohla stanovit	- ÚCL musí zajistit existenci rámce, podle kterého jsou stanoveny požadavky na provozovatele UAS
Scenario 12	UCA-3.5:	ÚCL nestanoví pravidla pro certifikaci pilota před zahájením provozu, nebo stanoví pravidla pro certifikaci pilota před zahájením provozu neúplně, nebo stanoví pravidla pro certifikaci pilota po zahájení provozu, protože…	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- pravidla pro certifikaci pilota nejsou vytvořena - pravidla pro certifikaci pilota nevychází z jednotných pravidel EU	- ÚCL musí vytvořit pravidla pro certifikaci pilota - ÚCL musí zajistit, že pravidla vychází z jednotných pravidel EU
Scenario 13	UCA-3.6:	ÚCL nestanoví požadavky na dálkově řídícího pilota UAS před zahájením provozu, nebo stanoví požadavky na dálkově řídícího pilota před zahájením provozuneúplně, nebo stanoví požadavky na dálkově řídícího pilota po zahájení provozu, protože…	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není stanoven rámec, ze kterého by ÚCL požadavky mohla stanovit	- ÚCL musí zajistit existenci rámce, podle kterého jsou stanoveny požadavky na dálkově řídícího pilota
Scenario 14	UCA-3.7:	ÚCL nestanoví požadavky údržby UAS před zahájením provozu, nebo stanoví požadavky údržby UAS před zahájením provozu neúplně, nebo stanoví požadavky údržby UAS po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není stanoven rámec, ze kterého by ÚCL požadavky mohla stanovit	- ÚCL musí zajistit existenci rámce, podle kterého jsou stanoveny požadavky údržby UAS
Scenario 15	UCA-3.8:	ÚCL nestanoví osvědčení ATPS a pravidla poskytování, nebo stanoví osvědčení ATPS a pravidla poskytování neúplně, nebo stanoví osvědčení ATPS a pravidla poskytování pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- osvědčení ATPS a pravidla poskytování nejsou stanovena	- ÚCL musí stanovit osvědčení ATPS a pravidla poskytování

Scenario 16	UCA-3.9:	ÚCL nestanoví certifikaci ANSP a pravidla poskytování, nebo stanoví certifikaci ANSP a pravidla poskytování neúplně, nebo stanoví certifikaci ANSP a pravidla poskytování pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- certifikace ANSP a pravidla poskytování nejsou stanovena	- ÚCL musí stanovit certifikaci ANSP a pravidla poskytování
Scenario 17	UCA-3.10:	ÚCL nestanoví certifikaci a poskytování dat, nebo stanoví certifikaci a poskytování dat neúplně, nebo stanoví certifikaci a poskytování dat pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- certifikace CIS a poskytování dat není stanoveno	- ÚCL musí stanovit certifikaci CIS a poskytování dat
Scenario 18	UCA-3.11:	ÚCL nestanoví pravidla pro poskytování U-space služeb před zahájením provozu, nebo stanoví pravidla pro poskytování U-space služeb před zahájením neúplně, nebo stanoví pravidla pro poskytování U-space služeb po zahájení provozu, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- pravidla pro poskytování U-space služeb nejsou stanovena	- ÚCL musí stanovit pravidla pro poskytování U-space služeb
Scenario 19	UCA-3.12:	ÚCL nestanoví pravidla pro certifikaci USSP, nebo stanoví pravidla pro certifikaci USSP neúplně, nebo stanoví pravidla pro certifikaci USSP pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- pravidla pro certifikaci USSP nejsou stanovena	- ÚCL musí stanovit pravidla pro certifikaci USSP
Scenario 20	UCA-3.13:	ÚCL v průběhu provozu nekontroluje plnění závazků, nebo v průběhu provozu kontroluje plnění závazků neúplně, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nejsou stanovena pravidla pro kontrolu plnění závazků - neví, jak kontrolovat plnění závazků - nemá kapacitu pro kontrolu plnění závazků	- Pravidla pro kontrolu plnění závazků musí být stanovena - ÚCL musí být schopno kontrolovat plnění závazků
Scenario 21	UCA-4.1:	Výrobce UAS neposkytne provozní manuál UAS, nebo poskytne provozní manuál UAS nekompletní, nebo poskytne provozní manuál UAS pozdě, protože…	[H-1, H-2, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provozní manuál UAS není vytvořen - není stanoven rámec, který by poskytnutí provozního manuálu UAS nařizoval	- Výrobce UAS musí vytvořit provozní manuál UAS - Musí být stanoven rámec, který výrobci nařizuje poskytnutí provozního manuálu UAS
Scenario 22	UCA-5.1:	ANSP ČR neposkytne řízení, letové navigační služby, nebo poskytne řízení, letové navigační služby neúplně, nebo poskytne řízení, letové navigační služby pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neexistuje rámec, který by poskytování služeb definoval - nemá dostatečné zdroje k poskytování služeb	- Musí existovat rámec, podle kterého se poskytují letové navigační služby - ANSP ČR musí mít dostatečné zdroje k poskytování služeb
Scenario 23	UCA-6.1:	Provozovatel UAS neposkytne provozní příručku před zahájením provozu, nebo poskytne provozní příručku před zahájením provozu nekompletní, nebo poskytne provozní příručku po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provozní příručka neexistuje - neví, že má povinnost provozní příručku poskytnout	- Provozovatel musí vytvořit provozní příručku a poskytnout ji členům personálu - Provozovatel UAS musí vědět, že má povinnost poskytnout provozní příručku
Scenario 24	UCA-6.2:	Provozovatel UAS nedefinuje zamýšlený provoz před jeho zahájením, nebo definuje zamýšlený provoz před jeho zahájením neúplně, nebo definuje zamýšlený provoz po jeho zahájení, protože…	[H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neví, že by provoz měl být včas kompletně definován	- Provozovatel UAS musí včas a kompletně definovat provoz
Scenario 25	UCA-6.3:	Provozovatel UAS nestanoví provozní postupy před zahájením provozu, nebo stanoví provozní postupy před zahájením provozu neúplně, nebo stanoví provozní postupy po zahájení provozu, protože…	[H-1, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provoz není kompletně definován - provozovatel UAS nemá dostatečné znalosti nebo prostředky k definování provozních postupů - provozovatel UAS nezná dostatečně problematiku bezpilotního létání	- Provozovatel UAS musí kompletně definovat provoz - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů - Provozovatel UAS musí dostatečně znát problematiku bezpilotního létání
Scenario 26	UCA-6.4:	Provozovatel UAS nezajistí teoretický a praktický výcvik před zahájením provozu, nebo je teoretický a praktický výcvik při zahájení provozu nedostatečný, nebo je teoretický a praktický výcvik zajištěn po zahájení provozu, nebo teoretický a praktický výcvik skončí před jeho dokončením , protože	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nepovažuje praktický nebo teoretický výcvik za důležitý - nemá znalosti nebo prostředky k zajištění praktického a teoretického výcviku pro danou misi - poskytnutý praktický a teoretický výcvik není dostatečný pro danou misi	- Provozovatel UAS musí považovat praktický a teoretický výcvik za důležitý - Provozovatel UAS musí mít znalosti i prostředky k zajištění praktického a teoretického výcviku pro danou misi - Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi
Scenario 27	UCA-6.5:	Provozovatel UAS v průběhu provozu periodicky nekontroluje požadované znalosti a výcvik, nebo periodicky kontroluje v průběhu provozu požadované znalosti a výcvik neúplně, protože…	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nepovažuje znalosti a výcvik důležité pro misi - nedokáže objektivně potřebné znalosti a výcvik zhodnotit - neuvědomuje si vážnost mise a zodpovědnost za ní - nekontroluje znalosti a výcvik periodicky	- Provozovatel UAS musí považovat požadované znalosti a výcvik pro misi za důležité - Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - Provozovatel UAS si musí uvědomovat vážnost mise a zodpovědnost za ní - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky
Scenario 28	UCA-6.6:	Provozovatel UAS nestanovil postupy koordinace vícečlenné posádky před zahájením provozu, nebo stanovil postupy koordinace vícečlenné posádky před zahájením provozu neúplně, nebo stanovil postupy koordinace vícečlenné posádky po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nezná povinnosti provozovatele UAS - není obeznámen s problematikou bezpilotního létání - nepovažuje koordinaci vícečlenné posádky za důležitou	- Provozovatel UAS musí znát své povinnosti - Provozovatel UAS musí být obeznámen s problematikou bezpilotního létání - Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou
Scenario 29	UCA-6.7:	Provozovatel UAS neposkytne provozní příručku před zahájením provozu, nebo poskytne provozní příručku před zahájením provozu nekompletní, nebo poskytne provozní příručku po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provozní příručka neexistuje - neví, že má povinnost provozní příručku poskytnout	- Provozní příručka musí být vytvořena a poskytnuta členům personálu - Provozovatel UAS musí vědět, že má povinnost poskytnout provozní příručku
Scenario 30	UCA-6.8:	Provozovatel UAS nedefinuje zamýšlený provoz před jeho zahájením, nebo definuje zamýšlený provoz před jeho zahájením neúplně, nebo definuje zamýšlený provoz po jeho zahájení, protože…	[H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neví, že by provoz měl být včas kompletně definován	- Provozovatel UAS musí včas a kompletně definovat provoz

Scenario 31	UCA-6.9:	Provozovatel UAS nestanoví provozní postupy před zahájením provozu, nebo stanoví provozní postupy před zahájením provozu neúplně, nebo stanoví provozní postupy po zahájení provozu, protože…	[H-1, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provoz není kompletně definován - provozovatel UAS nemá dostatečné znalosti nebo prostředky k definování provozních postupů - provozovatel UAS nezná dostatečně problematiku bezpilotního létání	- Provozovatel UAS musí kompletně definovat provoz - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů - Provozovatel UAS musí dostatečně znát problematiku bezpilotního létání
Scenario 32	UCA-6.10:	Provozovatel UAS nezajistí teoretický a praktický výcvik před zahájením provozu, nebo je teoretický a praktický výcvik při zahájení provozu nedostatečný, nebo je teoretický a praktický výcvik zajištěn po zahájení provozu, nebo teoretický a praktický výcvik skončí před jeho dokončením , protože	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nepovažuje praktický nebo teoretický výcvik za důležitý - nemá znalosti nebo prostředky k zajištění praktického a teoretického výcviku pro danou misi - poskytnutý praktický a teoretický výcvik není dostatečný pro danou misi	- Provozovatel UAS musí považovat praktický a teoretický výcvik za důležitý - Provozovatel UAS musí mít znalosti i prostředky k zajištění praktického a teoretického výcviku pro danou misi - Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi
Scenario 33	UCA-6.11:	Provozovatel UAS v průběhu provozu periodicky nekontroluje požadované znalosti a výcvik, nebo periodicky kontroluje v průběhu provozu požadované znalosti a výcvik neúplně, protože…	[H-1, H-3, H-4, H-5, H-6]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nepovažuje znalosti a výcvik důležité pro misi - nedokáže objektivně potřebné znalosti a výcvik zhodnotit - neuvědomuje si vážnost mise a zodpovědnost za ní - nekontroluje znalosti a výcvik periodicky	- Provozovatel UAS musí považovat požadované znalosti a výcvik pro misi za důležité - Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - Pprovozovatel UAS si musí uvědomovat vážnost mise a zodpovědnost za ní - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky
Scenario 34	UCA-6.12:	Provozovatel UAS nestanovil postupy koordinace vícečlenné posádky před zahájením provozu, nebo stanovil postupy koordinace vícečlenné posádky před zahájením provozu neúplně, nebo stanovil postupy koordinace vícečlenné posádky po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nezná povinnosti provozovatele UAS - není obeznámen s problematikou bezpilotního létání - nepovažuje koordinaci vícečlenné posádky za důležitou	- Provozovatel UAS musí znát své povinnosti - Provozovatel UAS musí být obeznámen s problematikou bezpilotního létání - Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou
Scenario 35	UCA-6.13:	Provozovatel UAS neaktualizuje data v UA před zahájením provozu, nebo aktualizuje data před zahájením provozu neúplně, nebo aktualizuje data po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neví, jak správně data aktualizovat - neuvědomuje si vážnost aktualizace dat v UA - není obeznámen se zodpovědností za provoz	- Provozovatel UAS musí vědět, jak správně aktualizovat data v UA - Provozovatel UAS musí si uvědomovat vážnost aktualizace dat v UA - Provozovatel UAS musí být obeznámen se zodpovědností za provoz
Scenario 36	UCA-6.14:	Provozovatel UAS nezajistí před zahájením provozu provozuschopný stav UA, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- neví, jak posoudit provozuschopnost stavu UA a jak ho dosáhnout	- Provozovatel UAS musí umět posoudit provozuschopnost stavu UA - Provozovatel UAS musí vědět, jak dosáhnout provozuschopného stavu UA
Scenario 37	UCA-7.1:	USSP neposkytuje U-space služby v průběhu provozu, nebo poskytuje U-space služby v průběhu provozu neúplně, nebo poskytuje U-space služby pozdě, nebo U-space služby přestanou být v průběhu provozu poskytovány, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není definován rámec, který by vymezoval rozsah poskytování U-space služeb - poskytování U-space služeb není kontrolováno - neexistuje rámec, podle kterého by byly kontrolovány plnění závazků USSP	- Musí být definován rámec, který vymezuje rozsah poskytování U-space služeb - Poskytování U-space služeb musí být kontrolováno - Musí být definován rámec, podle kterého je kontrolováno plnění závazků USSP
Scenario 38	UCA-8.1:	Člen personálu neprovede předletovou nebo poletovou kontrolu, nebo provede předletovou nebo poletovou kontrolu neúplně, nebo provede předletovou nebo poletovou kontrolu pozdě, protože…	[H-1, H-2, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- provedení předletové kontroly není obsahem práce personálu - práce personálu neobsahuje kompletní předletovou kontrolu - není schopen předletovou kontrolu provést správně a kompletně - si není vědom vážnosti mise a nesení odpovědnosti za ní	- Provedení předletové kontroly musí být obsahem práce personálu - Práce personálu musí obsahovat kompletní předletovou kontrolu - Musí být schopen provést předletovou kontrolu správně a kompletně - Musí si být vědom vážnosti mise a nesení odpovědnosti za ní
Scenario 39	UCA-8.2:	Člen personálu neprovede činnosti údržby před zahájením provozu, nebo provede činnosti údržby před zahájením provozu v rozporu s manuálem výrobce, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- není způsobilý pro činnosti údržby - nepovažuje činnosti údržby za důležité - nepřikládá činnostem údržby jejich závažnost	- Člen personálu musí být způsobilý pro činnosti údržby - Člen personálu musí považovat činnosti údržby za důležité - Člen personálu musí činnostem údržby přikládat jejich závažnost
Scenario 40	UCA-8.3:	Člen personálu nezajistí přepravovaný materiál před zahájením provozu, nebo zajistí přepravovaný materiál před zahájením provozu nedostatečně, protože…	[H-1]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- zajištění přepravovaného materiálu není obsahem práce personálu - neví, jak správně zajistit přepravovaný materiál - si není vědom vážnosti mise	- Zajištění přepravovaného materiálu musí být obsahem práce člena personálu - Člen personálu musí vědět, jak správně zajistit přepravovaný materiál - Člen personálu si musí být vědom vážnosti mise
Scenario 41	UCA-9.1:	Dálkově řídící pilot neprovede v průběhu provozu řídící pokyny pro pohyb UA, nebo provede v průběhu provozu řídící pokyny pro pohyb UA špatně, nebo provede v průběhu provozu řídící pokyny pro pohyb UA pozdě, nebo přestane v průběhu provozu provádět řídící pokyny pro pohyb UA, protože…	[H-1, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- pilotní výcvik není dostatečný - dojde ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - v průběhu mise přestane být schopen provádět řídící pokyny	- Pilotní výcvik musí být dostatečný pro daný provoz - Nesmí dojít ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - V průběhu mise dálkově řídící pilot musí být neustále schopen provádět řídící pokyny
Scenario 42	UCA-9.2:	Dálkově řídící pilot neprovede nastavení UAS a kontrolu funkčnosti před zahájením provozu, nebo provede nastavení UAS a kontrolu funkčnosti před zahájením provozu špatně, nebo provede nastavení UAS a kontrolu funkčnosti po zahájení provozu, protože…	[H-2]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nemá k nastavení UAS a kontrole funkčnosti dostatečné znalosti a dovednosti - provedení nastavení UAS a kontrola funkčnosti není obsahem práce pilota - si neuvědomuje vážnost nastavení UAS a kontrolu funkčnosti	- Dálkově řídící pilot musí disponovat výcvikem a znalostmi k nastavení UAS a kontrole funkčnosti - Provedení nastavení UAS a kontrola funkčnosti musí být obsahem práce pilota - Dálkově řídící pilot si musí uvědomovat vážnost nastavení UAS a kontrolu funkčnosti
Scenario 43	UCA-9.3:	Dálkově řídící pilot nevyhodnotí v průběhu provozu informace z poskytované U-space služby, nebo vyhodnotí v průběhu provozu informace z poskytované U-space služby špatně, nebo vyhodnotí informace z poskytované U-space služby pozdě, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- nemá výcvik k vyhodnocení informace z poskytované U-space služby - U-space služba je poskytována pozdě - U-space služba je poskytována špatně	- Dálkově řídící pilot musí mít výcvik k vyhodnocení informace z poskytované U-space služby - U-space služba musí být poskytována správně a včas
Scenario 44	UCA-10.1:	Stanice dálkově řídícího pilota v průběhu provozu neprovede činnost podle řídících signálů, nebo v průběhu provozu provede činnost podle řídících signálu špatně, nebo provede činnost podle řídících signálu pozdě, nebo přestane v průběhu provozu provádět činnost podle řídících signálu, protože…	[H-1, H-3, H-4, H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- dojde ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - řídící signály stanice dálkově řídícího pilota neodpovídají pohybu UA - stanice dálkově řídícího pilota přestane vysílat řídící signály v průběhu provozu	- Nesmí dojít ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - Pohyby UA musí odpovídat řídícím signálům stanice dálkově řídícího pilota - Stanice dálkově řídícího pilota nesmí přestat vysílat řídící signály v průběhu provozu
Scenario 45	UCA-10.2:	Stanice dálkově řídícího pilota v průběhu provozu nepřijme nebo nezobrazí U-space služby, nebo v průběhu provozu přijme nebo zobrazí U-space služby neúplně, nebo v průběhu provozu přijme nebo zobrazí U-space služby pozdě, nebo v průběhu provozu přestane přijímat nebo zobrazovat U-space služby, protože…	[H-5]	[L-1, L-2, L-3, L-4, L-5, L-6, L-7]	- přestane být schopna přijímat nebo zobrazovat U-space služby	- Stanice dálkově řídícího pilota musí být schopna přijímat a zobrazovat U-space služby v průběhu provozu

Příloha 2: Řídící struktura STPA



Příloha 3: Porovnání metod STPA a SORA

	Controller Constraints				Systemic requirements
UCA-6.1:	provozní příručka musí být poskytnuta před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní příručka musí být poskytnuta kompletní před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní příručka nesmí být poskytnuta po zahájení provozu - **2019/947 UAS.SPEC.050**		- Provozovatel musí vytvořit provozní příručku a poskytnout ji členům personálu - **2019/947 UAS.SPEC.050** - Provozovatel UAS musí vědět, že má povinnost poskytnout provozní příručku - **2019/947 UAS.SPEC.050**
UCA-6.2:	zamýšlený provoz musí být definován před jeho zahájením - **ano, jedná se o podmínku pro získání OkP**	zamýšlený provoz musí být kompletně definován před jeho zahájením - **ano, jedná se o podmínku pro získání OkP**	zamýšlený provoz nesmí být definován po jeho zahájením - **ano, jedná se o podmínku pro získání OkP**		- Provozovatel UAS musí včas a kompletně definovat provoz - **ano, jedná se o podmínku pro získání OkP**
UCA-6.3:	provozní postupy musí být stanoveny před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní postupy musí být kompletně stanoveny před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní postupy nesmí být stanoveny po zahájení provozu - **2019/947 UAS.SPEC.050**		- Provozovatel UAS musí kompletně definovat provoz - **ano, jedná se o podmínku pro získání OkP** - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů - Provozovatel UAS musí dostatečně znát problematiku bezpilotního létání
UCA-6.4:	teoretický nebo praktický výcvik musí být zajištěn před zahájením provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik musí být dostatečný při zahájení provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik nesmí skončit před jeho dokončením - **2019/947 UAS.SPEC.050**	- Provozovatel UAS musí považovat praktický a teoretický výcvik za důležitý - Provozovatel UAS musí mít znalosti i prostředky k zajištění praktického a teoretického výcviku pro danou misi - Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi - **(OSO#9, I)**
UCA-6.5:	požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány - **není stanoveno**	požadované znalosti a výcvik musí být průběhu provozu kontrolovány kompletně a periodicky - **není stanoveno**			- Provozovatel UAS musí považovat požadované znalosti a výcvik pro misi za důležité - Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - **není stanoveno (je stanoveno na základě vlastního prohlášení)** - Provozovatel UAS si musí uvědomovat vážnost mise a zodpovědnost za ní - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky - **není stanoveno**
UCA-6.6:	postupy koordinace vícečlenné posádky musí být stanoveny před zahájením provozu - **(OSO#16, I)**	postupy koordinace vícečlenné posádky musí být stanoveny kompletně před zahájením provozu - **(OSO#16, I)**	postupy koordinace vícečlenné posádky nesmí být stanoveny po zahájení provozu - **(OSO#16, I)**		- Provozovatel UAS musí znát své povinnosti - Provozovatel UAS musí být obeznámen s problematikou bezpilotního létání - Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou
UCA-6.7:	provozní příručka musí být poskytnuta před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní příručka musí být poskytnuta kompletní před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní příručka nesmí být poskytnuta po zahájení provozu - **2019/947 UAS.SPEC.050**		- Provozovatel musí vytvořit provozní příručku a poskytnout ji členům personálu - **2019/947 UAS.SPEC.050** - Provozovatel UAS musí vědět, že má povinnost poskytnout provozní příručku - **2019/947 UAS.SPEC.050**
UCA-6.8:	zamýšlený provoz musí být definován před jeho zahájením - **ano, jedná se o podmínku pro získání OkP**	zamýšlený provoz musí být kompletně definován před jeho zahájením - **ano, jedná se o podmínku pro získání OkP**	zamýšlený provoz nesmí být definován po jeho zahájením - **ano, jedná se o podmínku pro získání OkP**		- Provozovatel UAS musí včas a kompletně definovat provoz - **ano, jedná se o podmínku pro získání OkP**
UCA-6.9:	provozní postupy musí být stanoveny před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní postupy musí být kompletně stanoveny před zahájením provozu - **2019/947 UAS.SPEC.050**	provozní postupy nesmí být stanoveny po zahájení provozu - **2019/947 UAS.SPEC.050**		- Provozovatel UAS musí kompletně definovat provoz - **ano, jedná se o podmínku pro získání OkP** - Provozovatel UAS musí mít dostatečné znalosti a prostředky k definování provozních postupů - Provozovatel UAS musí dostatečně znát problematiku bezpilotního létání
UCA-6.10:	teoretický nebo praktický výcvik musí být zajištěn před zahájením provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik musí být dostatečný při zahájení provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik nesmí být zajištěn po zahájení provozu - **2019/947 UAS.SPEC.050**	teoretický a praktický výcvik nesmí skončit před jeho dokončením - **2019/947 UAS.SPEC.050**	- Provozovatel UAS musí považovat praktický a teoretický výcvik za důležitý - Provozovatel UAS musí mít znalosti i prostředky k zajištění praktického a teoretického výcviku pro danou misi - Poskytnutý praktický a teoretický výcvik musí být dostatečný pro danou misi - **(OSO#9, I)**
UCA-6.11:	požadované znalosti a výcvik musí být v průběhu provozu periodicky kontrolovány - **není stanoveno**	požadované znalosti a výcvik musí být průběhu provozu kontrolovány kompletně a periodicky - **není stanoveno**			- Provozovatel UAS musí považovat požadované znalosti a výcvik pro misi za důležité - Provozovatel UAS musí být schopný objektivně zhodnotit potřebné znalosti a výcvik personálu - **není stanoveno (je stanoveno na základě vlastního prohlášení)** - Provozovatel UAS si musí uvědomovat vážnost mise a zodpovědnost za ní - Provozovatel UAS musí kontrolovat znalosti a výcvik personálu periodicky - **není stanoveno**

UCA-6.12:	postupy koordinace vícečlenné posádky musí být stanoveny před zahájením provozu - **(OSO#16, I)**	postupy koordinace vícečlenné posádky musí být stanoveny kompletně před zahájením provozu - **(OSO#16, I)**	postupy koordinace vícečlenné posádky nesmí být stanoveny po zahájení provozu - **(OSO#16, I)**		- Provozovatel UAS musí znát své povinnosti - Provozovatel UAS musí být obeznámen s problematikou bezpilotního létání - Provozovatel UAS musí považovat koordinaci vícečlenné posádky za důležitou
UCA-6.13:	data v UA musí být před zahájením provozu aktualizována - **2019/947 UAS.SPEC.050, pouze implicitně - "have been informed about the UAS operator's operations manual"**	data v UA musí být před zahájením provozu kompletně aktualizována - **2019/947 UAS.SPEC.050, pouze implicitně - "have been informed about the UAS operator's operations manual"**	data v UA nesmí být aktualizována po zahájení provozu - **2019/947 UAS.SPEC.050, pouze implicitně - "have been informed about the UAS operator's operations manual"**		- Provozovatel UAS musí vědět, jak správně aktualizovat data v UA - **2019/947 UAS.SPEC.050** - Provozovatel UAS musí si uvědomovat vážnost aktualizace dat v UA - Provozovatel UAS musí být obeznámen se zodpovědností za provoz
UCA-6.14:	UA musí být v provozuschopném stavu před zahájením provozu - **UAS.SPEC.060**				- Provozovatel UAS musí umět posoudit provozuschopnost stavu UA - Provozovatel UAS musí vědět, jak dosáhnout provozuschopného stavu UA
UCA-7.1:	U-space služby musí být v průběhu provozu poskytovány - **(OSO#13, J)**	U-space služby musí být v průběhu provozu poskytovány kompletně - **není stanoveno, určuje až střední úroveň jistoty OSO#13**	U-space služby nesmí být poskytovány pozdě - **není stanoveno, určuje až střední úroveň jistoty OSO#13**	Poskytování U-space služeb nesmí být v průběhu provozu přerušeno - **není stanoveno, určuje až střední úroveň jistoty OSO#13**	- Musí být definován rámec, který vymezuje rozsah poskytování U-space služeb - **NPA 2021-14** - Poskytování U-space služeb musí být kontrolováno - **NPA 2021-14** - Musí být definován rámec, podle kterého je kontrolováno plnění závazků USSP - **NPA 2021-14**
UCA-8.1:	předletová a poletová kontrola musí být provedena - **(OSO#8, I)**	předletová a poletová kontrola musí být provedena kompletně - **(OSO#8, I)**	předletová a poletová kontrola nesmí být provedeny pozdě - **(OSO#8, I)**		- Provedení předletové kontroly musí být obsahem práce personálu - **(OSO#8, I)** - Práce personálu musí obsahovat kompletní předletovou kontrolu - **(OSO#8, I)** - Člen personálu musí být schopen provést předletovou kontrolu správně a kompletně - **(OSO#9, I)** - Člen personálu si musí být vědom vážnosti mise a nesení odpovědnosti za ní
UCA-8.2:	činnosti údržby musí být provedeny před zahájením provozu - **AMC1 UAS.SPEC.060(2)(c); UAS.SPEC.050**	činnosti údržby nesmí být před zahájením provozu provedeny v rozporu s manuálem výrobce - **AMC1 UAS.SPEC.060(2)(c); UAS.SPEC.050**			- Člen personálu musí být způsobilý pro činnosti údržby - **(OSO#3, I)** - Člen personálu musí považovat činnosti údržby za důležité - Člen personálu musí činnostem údržby přikládat jejich závažnost
UCA-8.3:	přepravovaný materiál musí být před zahájením provozu zajištěn - **AMC1 UAS.SPEC.060(2)(c)**	přepravovaný materiál nesmí být před zahájením provozu zajištěn špatně - **AMC1 UAS.SPEC.060(2)(c)**			- Zajištění přepravovaného materiálu musí být obsahem práce člena personálu - **(OSO#1, I); AMC1 UAS.SPEC.060(2)(c)** - Člen personálu musí vědět, jak správně zajistit přepravovaný materiál - **UAS.SPEC.050 (1)(e)** - Člen personálu si musí být vědom vážnosti mise
UCA-9.1:	řídící pokyny pro pohyb UA musí být v průběhu provozu provedeny - **(OSO#9, I), (OSO#17)**	řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny špatně - **(OSO#9, I), (OSO#17)**	řídící pokyny pro pohyb UA nesmí být v průběhu provozu provedeny pozdě - **(OSO#9, I), (OSO#17)**	provádění řídících pokynů pro pohyb UA nesmí v průběhu provozu přerušeno - **(OSO#9, I), (OSO#17)**	- Pilotní výcvik musí být dostatečný pro daný provoz - **(OSO#9, I)** - V průběhu mise dálkově řídící pilot musí být neustále schopen provádět řídící pokyny - **(OSO#17, I) (stanoveno na základě vlastního prohlášení)**
UCA-9.2:	nastavení UAS a kontrola funkčnosti musí být provedena před zahájením provozu - **UAS.SPEC.060**	nastavení UAS a kontrola funkčnosti nesmí být provedena špatně před zahájením provozu - **UAS.SPEC.060**	nastavení UAS a kontrola funkčnosti nesmí být provedeno po zahájení provozu - **UAS.SPEC.060**		- Dálkově řídící pilot musí disponovat výcvikem a znalostmi k nastavení UAS a kontrole funkčnosti - **(OSO#9, I) (stanoveno na základě vlastního prohlášení)** - Provedení nastavení UAS a kontrola funkčnosti musí být obsahem práce pilota - **UAS.SPEC.060** - Dálkově řídící pilot si musí uvědomovat vážnost nastavení UAS a kontrolu funkčnosti
UCA-9.3:	informace z poskytované U-space služby musí být v průběhu provozu vyhodnocena - **není stanoveno**	informace z poskytované U-space služby nesmí být v průběhu provozu vyhodnocena špatně - **není stanoveno**	informace z poskytované U-space služby nesmí být vyhodnocena pozdě - **není stanoveno**		- Dálkově řídící pilot musí mít výcvik k vyhodnocení informace z poskytované U-space služby - **není stanoveno** - U-space služba musí být poskytována správně a včas - **NPA 2021-14**
UCA-10.1:	činnost podle řídících signálů musí být v průběhu provozu provedena - **(OSO#6, I); (OSO#7, I)**	činnost podle řídících signálů nesmí být v průběhu provozu provedena špatně - **(OSO#6, I); (OSO#7, I)**	činnost podle řídících signálů nesmí být provedena pozdě - **(OSO#6, I); (OSO#7, I)**	provádění činnosti podle řídících signálu nesmí v průběhu provozu přestat - **(OSO#6, I); (OSO#7, I)**	- Nesmí dojít ke ztrátě spojení mezi stanicí dálkově řídícího pilota a UA - **(OSO#6, I)** - Pohyby UA musí odpovídat řídícím signálům stanice dálkově řídícího pilota - Stanice dálkově řídícího pilota nesmí přestat vysílat řídící signály v průběhu provozu - **(OSO#6, I)**
UCA-10.2:	U-space služby musí být v průběhu provozu přijímány nebo zobrazovány - **(OSO#13, I);(OSO#13, I) ; NPA 2021-14**	U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány neúplně - **(OSO#13, I);(OSO#13, I) ; NPA 2021-14**	U-space služby nesmí být v průběhu provozu přijímány nebo zobrazovány pozdě - **(OSO#13, I);(OSO#13, I) ; NPA 2021-14**	přijímání nebo zobrazování U-space služeb nesmí v průběhu provozu přestat - **(OSO#13, I);(OSO#13, I) ; NPA 2021-14**	- Stanice dálkově řídícího pilota musí být schopna přijímat a zobrazovat U-space služby v průběhu provozu - **NPA 2021-14**

Příloha 4: FRAM podle Monte Carlo simulace

Funkce *j*	Output funkce *j*	Funkce *i*	Načasování			Přesnost		
			Příliš brzy	Včas	Příliš pozdě	Přesné	Přijatelné	Nepřesné
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Certifikovat zapojený subjekt	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Dohlížet na dodržování pravidel	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Zajistit teoretický a praktický výcvik posádky	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Stanovit provozní postupy	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Posuzovat žádosti o oprávnění k provozu	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Registrovat provozovatele	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Získat oprávnění k provozu	2	1	6	1	2	8
Publikovat jednotná pravidla a jejich výklad	Jednotná pravidla a jejich výklad	Publikovat pravidla pro poskytování U-space služeb	2	1	6	1	2	8
Certifikovat zapojený subjekt	Certifikace zapojeného subjektu	Poskytovat specifickou U-space službu dle stanovených pravi	2	1	6	1	2	8
Dohlížet na dodržování pravidel	Dohlížení na dodržování pravidel	Zajistit teoretický a praktický výcvik posádky	4	1	6	0.5	2	8
Dohlížet na dodržování pravidel	Dohlížení na dodržování pravidel	Poskytovat specifickou U-space službu dle stanovených pravi	4	1	6	0.5	2	8
Dohlížet na dodržování pravidel	Dohlížení na dodržování pravidel	Stanovit postupy koordinace vícečlenné posádky	4	1	6	0.5	2	8
Dohlížet na dodržování pravidel	Dohlížení na dodržování pravidel	Stanovit provozní postupy	4	1	6	0.5	2	8
Registrovat provozovatele	Registrace provozovatele	Získat oprávnění k provozu	2	1	6	1	2	8
Posuzovat žádosti o oprávnění k provozu	Schválení žádosti o oprávnění k provozu	Získat oprávnění k provozu	4	1	6	1	2	8
Publikovat pravidla pro poskytování U-space služeb	Pravidla pro poskytování U-space služeb	Vyhodnotit přijímaná data	2	1	6	1	2	8
Publikovat pravidla pro poskytování U-space služeb	Pravidla pro poskytování U-space služeb	Poskytovat specifickou U-space službu dle stanovených pravi	2	1	6	1	2	8
Zajistit teoretický a praktický výcvik posádky	Teoretický a praktický výcvik posádky	Zahájit let	2	1	6	0.5	2	8
Zajistit teoretický a praktický výcvik posádky	Teoretický a praktický výcvik posádky	Převzít kontrolu nad automatickým letem	2	1	6	0.5	2	8
Zajistit teoretický a praktický výcvik posádky	Teoretický a praktický výcvik posádky	Vyhodnocovat informace z provozu UA	2	1	6	0.5	2	8
Zajistit teoretický a praktický výcvik posádky	Teoretický a praktický výcvik posádky	Vyhodnocovat informace ze služeb U-space	2	1	6	0.5	2	8
Zajistit teoretický a praktický výcvik posádky	Teoretický a praktický výcvik posádky	Zajistit provozuschopný stav UA	2	1	6	0.5	2	8
Stanovit postupy koordinace vícečlenné posádky	Postupy koordinace vícečlenné posádky	Komunikovat s ostatními členy personálu	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Komunikovat s ostatními členy personálu	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Zahájit let	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Převzít kontrolu nad automatickým letem	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Vyhodnocovat informace z provozu UA	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Zajistit provozuschopný stav UA	2	1	6	0.5	2	8
Stanovit provozní postupy	Provozní postupy	Vyhodnocovat informace ze služeb U-space	2	1	6	0.5	2	8
Získat oprávnění k provozu	Oprávnění k provozu	Zahájit let	4	1	6	1	2	8
Poskytovat specifickou U-space službu dle stanovených pravi	U-space služba	Vyhodnocovat informace ze služeb U-space	4	1	6	0.5	2	8
Vyhodnotit přijímaná data	Vyhodnocená data	Poskytovat specifickou U-space službu dle stanovených pravi	4	1	6	1	2	8
Komunikovat s ostatními členy personálu	Komunikace členů personálu	Zahájit let	4	1	6	0.5	2	8
Zahájit let	Let zahájen	Převzít kontrolu nad automatickým letem	4	1	6	1	2	8
Vyhodnocovat informace z provozu UA	Vyhodnocení informace z provozu UA	Převzít kontrolu nad automatickým letem	4	1	6	0.5	2	8
Vyhodnocovat informace ze služeb U-space	Vyhodnocení informace ze služeb U-spa	Převzít kontrolu nad automatickým letem	4	1	6	0.5	2	8
Zajistit provozuschopný stav UA	Zajištění provozuschopného stavu UA	Zahájit let	2	1	6	0.5	2	8

#	**Funkce *j***	**SPC 1**	**SPC 2**	**SPC 3**
1	Publikovat jednotná pravidla a jejich výklad	0	0	0
2	Certifikovat zapojený subjekt	0	0	0
3	Dohlížet na dodržování pravidel	0	0	0
4	Registrovat provozovatele	0	0	0
5	Posuzovat žádosti o oprávnění k provozu	0	0	0
6	Publikovat pravidla pro poskytování U-space služeb	0	0	0
7	Zajistit teoretický a praktický výcvik posádky	0	0	0
8	Stanovit postupy koordinace vícečlenné posádky	0	0	0
9	Stanovit provozní postupy	0	0	0
10	Získat oprávnění k provozu	0	0	0
11	Poskytovat specifickou U-space službu dle stanovených pravide	0	1	0
12	Vyhodnotit přijímaná data	0	0	0
13	Komunikovat s ostatními členy personálu	1	0.5	0
14	Zahájit let	1	0.5	1
15	Vyhodnocovat informace z provozu UA	1	1	1
16	Vyhodnocovat informace ze služeb U-space	1	1	0
17	Zajistit provozuschopný stav UA	1	0	0

e_j^z	Funkce 1	Funkce 2	Funkce 3	Funkce 4	Funkce 5	Funkce 6	Funkce 7	Funkce 8	Funkce 9	Funkce 10	Funkce 11	Funkce 12	Funkce 13	Funkce 14	Funkce 15	Funkce 16	Funkce 17
Scénář 23	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.67	2.33	2.67	2.00	1.33
Scénář 24	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.67	3.00	3.33	2.00	1.33
Scénář 25	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Scénář 26	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.33	1.00	2.00	2.67	3.33	2.67	1.33
Scénář 27	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.33	1.00	2.00	3.33	4.00	2.67	1.33

	Kombinace výstupů								
Funkce	**early+prec**	**early+accept**	**early+impr**	**ontme+prec**	**ontme+accept**	**ontme+impr**	**toola+prec**	**toola+accept**	**toola+imp**
1	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
2	2	4	16	1	2	8	6	12	48
3	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
4	2	4	16	1	2	8	6	12	48
5	4	8	32	1	2	8	6	12	48
6	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
7	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
8	1	4	16	0.5	2	8	3	12	48
9	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
10	4	8	32	1	2	8	6	12	48
11	2	8	32	0.5	2	8	3	12	48
12	4	8	32	1	2	8	6	12	48
13	2	8	32	0.5	2	8	3	12	48
14	4	8	32	1	2	8	6	12	48
15	2	8	32	0.5	2	8	3	12	48
16	2	8	32	0.5	2	8	3	12	48
17	1	4	16	0.5	2	8	3	12	48

	Scénář 23								
Funkce	**early+prec**	**early+accep**	**early+impr**	**ontme+pre**	**ontme+acce**	**ontme+impr**	**toola+prec**	**toola+accept**	**toola+imp**
1	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
2	2	4	16	1	2	8	6	12	48
3	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
4	2	4	16	1	2	8	6	12	48
5	4	8	32	1	2	8	6	12	48
6	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
7	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
8	1	4	16	1	2	8	3	12	48
9	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
10	4	8	32	1	2	8	6	12	48
11	2	8	32	1	2	8	3	12	48
12	4	8	32	1	2	8	6	12	48
13	3	13	53	1	3	13	5	20	80
14	9	19	75	2	5	19	14	28	112
15	5	21	85	1	5	21	8	32	128
16	4	16	64	1	4	16	6	24	96
17	1	5	21	1	3	11	4	16	64

	Scénář 24								
Funkce	**early+prec**	**early+accept**	**early+impr**	**ontme+pr**	**ontme+acce**	**ontme+impr**	**toola+prec**	**toola+accept**	**toola+imp**
1	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
2	2	4	16	1	2	8	6	12	48
3	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
4	2	4	16	1	2	8	6	12	48
5	4	8	32	1	2	8	6	12	48
6	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
7	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
8	1	4	16	1	2	8	3	12	48
9	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
10	4	8	32	1	2	8	6	12	48
11	2	8	32	1	2	8	3	12	48
12	4	8	32	1	2	8	6	12	48
13	3	13	53	1	3	13	5	20	80
14	12	24	96	3	6	24	18	36	144
15	7	27	107	2	7	27	10	40	160
16	4	16	64	1	4	16	6	24	96
17	1	5	21	1	3	11	4	16	64

	Scénář 26								
Funkce	**early+prec**	**early+accept**	**early+impr**	**ontme+pr**	**ontme+acc**	**ontme+impr**	**toola+prec**	**toola+accept**	**toola+imp**
1	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
2	2	4	16	1	2	8	6	12	48
3	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
4	2	4	16	1	2	8	6	12	48
5	4	8	32	1	2	8	6	12	48
6	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
7	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
8	1	4	16	1	2	8	3	12	48
9	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
10	4	8	32	1	2	8	6	12	48
11	3	11	43	1	3	11	4	16	64
12	4	8	32	1	2	8	6	12	48
13	4	16	64	1	4	16	6	24	96
14	11	21	85	3	5	21	16	32	128
15	7	27	107	2	7	27	10	40	160
16	5	21	85	1	5	21	8	32	128
17	1	5	21	1	3	11	4	16	64

	Scénář 27								
Funkce	**early+prec**	**early+accept**	**early+impr**	**ontme+pre**	**ontme+acce**	**ontme+imp**	**toola+pre**	**toola+acc**	**toola+imp**
1	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
2	2	4	16	1	2	8	6	12	48
3	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
	2	8	32	0.5	2	8	3	12	48
4	2	4	16	1	2	8	6	12	48
5	4	8	32	1	2	8	6	12	48
6	2	4	16	1	2	8	6	12	48
	2	4	16	1	2	8	6	12	48
7	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
	1	4	16	0.5	2	8	3	12	48
8	1	4	16	1	2	8	3	12	48
9	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
	1	4	16	1	2	8	3	12	48
10	4	8	32	1	2	8	6	12	48
11	3	11	43	1	3	11	4	16	64
12	4	8	32	1	2	8	6	12	48
13	4	16	64	1	4	16	6	24	96
14	13	27	107	3	7	27	20	40	160
15	8	32	128	2	8	32	12	48	192
16	5	21	85	1	5	21	8	32	128
17	1	5	21	1	3	11	4	16	64

Příloha 5: FRAM model