ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Eva Milerová

SYSTÉMOVÝ PŘÍSTUP K NASTAVENÍ PROVOZNÍ BEZPEČNOSTI BEZPILOTNÍHO LETECTVÍ V ČR

Diplomová práce

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. Eva Milerová

Studijní program (obor/specializace) studenta:

navazující magisterské – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Systémový přístup k nastavení provozní bezpečnosti bezpilotního letectví v ČR**

Název tématu (anglicky): **System Approach to Unmanned Aircraft Systems Safety in the Czech Republic**

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je zhodnotit bezpečnost (safety) provozního prostředí České republiky pro provoz bezpilotních systémů pomocí využití vybrané systémové metody a navrhnout kroky pro zlepšení tohoto stavu.
- Provozní prostředí bezpilotních systémů v ČR
- Zvolení systémové metody pro hodnocení
- Aplikace metody na provozní prostředí
- Interpretace výsledků
- Stanovení doporučení pro ČR

Rozsah grafických prací: Podle 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
EASA: Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945)
Návrh změny zákona o civilním letectví

Vedoucí diplomové práce: **doc. Ing. Jakub Kraus, Ph.D.**
Ing. Adam Kleczatský

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

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

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

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

Potvrzuji převzetí zadání diplomové práce.

Bc. Eva Milerová
jméno a podpis studenta

V Praze, dne ..... **16. července 2021**

Poděkování

Ráda bych poděkovala panu doc. Ing. Jakubu Krausovi, Ph.D. a Ing. Adamu Kleczatskému za vedení mé diplomové práce, poskytnutí odborných konzultací a za cenné rady. Dále bych chtěla z celého srdce poděkovat mým rodičům, rodině a přátelům za jejich trpělivost a za absolutní podporu po celou dobu studia.

Čestné prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání 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. 5. 2022 ……...

Podpis

Jméno: Bc. Eva Milerová

Název diplomové práce: Systémový přístup k nastavení provozní bezpečnosti bezpilotního letectví v ČR

Univerzita: České vysoké učení technické v Praze, Fakulta dopravní

Rok vydání: 2022

Abstrakt

Tato práce seznamuje čtenáře s problematikou bezpilotního letectví v České republice. Popisuje aktuálně platná pravidla pro provoz bezpilotních systémů a také naznačuje, jaká pravidla budou platit v nadcházejících letech. Práce se soustředí na bezpečnost provozu bezpilotních letadel a letadel s pilotem na palubě ve společném vzdušném prostoru U-space. Bezpečnost U-space je analyzována pomocí systémových metod STPA a FRAM a na základě výsledků těchto metod jsou navržena doporučení pro zlepšení bezpečnosti provozu bezpilotních systémů v České republice.

Klíčová slova

Bezpilotní systémy, UAS, U-space, Safety-I, Safety-II, systémové metody, STPA, FRAM.

Abstract

The thesis introduces the issue of unmanned aviation in the Czech Republic. Describes the current rules for UAS operations and also introduce what rules will apply in the coming years. The aim of the thesis is safety of unmanned aircrafts and manned aircrafts in the common U-space airspace. The safety of U-space airspace is analyzed using the STPA and FRAM systemic methods. Using the results of these methods, recommendations are proposed to improve the safety of operations of UAS in the Czech Republic.

Key words

Unmanned aircraft systems, UAS, U-space, Safety-I, Safety-II, systemic safety methods, STPA, FRAM.

Obsah

Seznam zkratek

AFIS	Letištní letová informační služba	Aerodrome Flight Information Service
AGL	Nad úrovní země	Above Ground Level
ARC	Třída rizika ve vzduchu	Air Risk Class
ATZ	Letištní provozní zóna	Air Traffic Zone
BVLOS	(Provoz) mimo vizuální dohled	Beyond Visual Line Of Sight
CTR	Řízený okrsek letiště	Controlled Traffic Region
EASA	Agentura Evropské komise pro bezpečnost letectví	European Union Aviation Safety Agency
FIS	Letová informační služba	Flight Information Service
FRAM	Metoda funkční rezonanční analýzy	Functional Resonance Analysis Method
FTA	Analýza stromu poruchových stavů	Fault Tree Analysis
GRC	Třída rizika na zemi	Ground Risk Class
LUC	Osvědčení provozovatele lehkého bezpilotního systému	Light UAS Operator Certificate
MORT	Řízení dozoru a strom rizik	Management Oversight and Risk Tree
MTOW	Maximální vzletová hmotnost	Maximum Take Off Weight
OOP	Opatření obecné povahy	-
OSO	Cíl provozní bezpečnosti	Operational Safety Objective
RAG	Schéma k posouzení odolnosti	Resilience Assessment Grid
ŘLP	Řízení letového provozu	-
SAIL	Specifická úroveň zabezpečení a integrity	Specific Assurance and Integrity Level
SHELL	-	Software, Hardware, Environment, Lifeware
SORA	Posouzení rizika specifické kategorie provozu	Specific Operations Risk Assessment
STAMP	Model nehod a procesů založený na systémové teorii	System-Theory Based Accident Model and Processes
STPA	Systémově-teoretická analýza procesů	Systems Theoretic Process Analysis
STS	Standartní scénář	Standart Scenario
UAS	Bezpilotní systém	Unmanned Aerial System
ÚCL	Úřad pro civilní letectví	Civil aviation authority
USSP	Poskytovatel služby U-space	U-space Service Provider
VLOS	(Provoz) ve vizuálním dohledu	Visual Line Of Sight

Úvod

Bezpilotní systémy jsou velmi rychle rozvíjející se technologií po celém světě. V České republice tomu není jinak. Vzhledem k rostoucímu provozu bezpilotních systémů a také vzhledem k růstu provozu letecké dopravy celkově bylo nutné stanovit způsob, jak začlenit bezpilotní systémy a letectví s pilotem na palubě do jednoho vzdušného prostoru. Tento problém řeší vytvoření vzdušného prostoru U-space. Prostor, který umožní společný provoz bezpilotních systémů (UAS) a letadel s pilotem na palubě ve stejném vzdušném prostoru nad městy i v nízkých výškách. Právě díky tomuto vzdušnému prostoru nám budou nad hlavami létat bezpilotní letadla bez pilota na palubě, která budou převážet osoby v rámci městské hromadné dopravy.

Provoz U-space bude zajištěn na základě sdílení provozních informací bezpilotních systémů a letadel s pilotem na palubě, pomocí společných informačních služeb. Bezpilotní letadla budou mít informace o letadlech s pilotem na palubě a naopak. Bude k dispozici několik služeb, které budou zajišťovat rozestupy a bezpečnost vzdušného prostoru U-space. Právě teď se nacházíme na samém začátku vývoje tohoto vzdušného prostoru. Bylo již vydáno několik legislativních dokumentů, které definují, jak bude provoz v U-space vypadat. Proto nastal pravý čas posoudit jeho bezpečnost.

Potřeba udržení bezpečnosti v letectví je velice vysoká. Proaktivní způsob zjišťování hrozících nebezpečí ještě před uvedením výrobku, systému, postupu koncovým uživatelům je nutnou součástí jejich výrobního procesu. Právě z tohoto důvodu bylo vytvořeno odvětví provozní bezpečnosti (safety). Safety inženýři pomocí různorodých nástrojů a metod analyzují provozní bezpečnost letectví a zavádějí pravidla, která udržují leteckou dopravu bezpečnou.

Cílem této práce je pomocí vybraných systémových metod zhodnotit provozní bezpečnost provozního prostředí vzdušného prostoru U-space v České republice. Výsledky těchto metod budou porovnány s aktuálně platnou legislativou a na základě porovnání budou navrhnuta doporučení, jakým způsobem by bezpečnost provozu UAS v U-space mohla být zvýšena. Jako vhodné systémové metody pro posouzení bezpečnosti byly vybrány STPA a FRAM. Společným prvkem obou metod je systémový přístup. Metodika obou metod je v práci důkladně popsána a následně aplikována na provozní prostředí U-space.

1 Provozní prostředí bezpilotních systémů v ČR

V této kapitole je popsána problematika provozu bezpilotních systémů v České republice. Jsou zde podrobně rozebrána pravidla provozu, rozdělení provozu do kategorií a jakým směrem se bezpilotní letectví ubírá, aby byly definovány základní informace, které budou sloužit jako vstup pro hodnocení provozní bezpečnosti.

1.1 Jak létáme nyní a co nás čeká

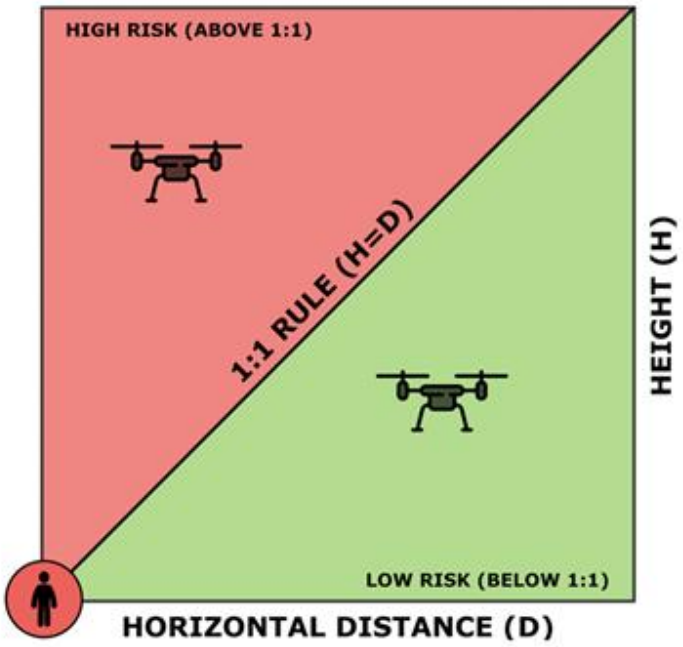
Od 31.12.2020 dle Prováděcího nařízení Komise (EU) 2019/947 ze dne 24. května 2019 o pravidlech a postupech pro provoz bezpilotních letadel [1] a Nařízení Komise v přenesené pravomoci (EU) 2019/945 ze dne 12. března 2019 o bezpilotních systémech a o provozovatelích bezpilotních systémů ze třetích zemí [2] v ČR a ve všech členských státech Evropské unie platí harmonizovaná pravidla pro provoz bezpilotních systémů. To znamená, že již nezáleží na tom, jestli je provoz UAS volnočasová aktivita, nebo výdělečná činnost. Již záleží na tom, jakou míru rizika provoz vytváří. V návaznosti na tuto změnu ÚCL vydalo Opatření obecné povahy (OOP), které upravuje provoz bezpilotních systémů na území ČR. Vychází z předchozího leteckého předpisu L2 – Doplněk X. Dále je důležité pamatovat, že stále platí zákon č. 49/1997 Sb. o civilním letectví. Každý členský stát si může definovat dodatečné podmínky platící pro danou zemi, zejména například vzdušné prostory, kde se létat nesmí, kde se může létat pouze s oprávněním apod.

Aktuálně je období, kdy platí všechna výše zmíněná legislativní nařízení zároveň. Evropská legislativa toto období definovala jako přechodné období, které má zatím trvat do 1. 1. 2024. Datum již bylo několikrát změněno a stále existuje šance, že ještě změněno bude. Jak dlouho bude trvat přechodné období záleží na schopnosti autorit v ČR implementovat evropská pravidla a na rychlosti zavádění nových technologií.

OOP definuje nový omezený vzdušný prostor LKR10 – UAS, který je vymezen státní hranicí ČR a pro bezpilotní systémy vyhrazuje vzdušný prostor do maximální výšky do 120 m nad zemí. Tento prostor umožňuje celkem snadno provozovat bezpilotní systémy při splnění podmínek užívání prostoru. Dále definuje, za jakých podmínek je možné létat v okolí letišť, tedy v prostorech CTR, ATZ atd. Pro let v blízkosti zástavby neboli hustě osídleného prostoru je potřeba dodržovat určitá pravidla, jako například pravidlo 1:1 ve smyslu horizontální vzdálenosti a výšky nad zemí, které je znázorněno na obrázku 1. Také definuje ochranná pásma liniových staveb, jako například nadzemních dopravních staveb nebo inženýrských sítí, ale také ochranná písma vodních zdrojů, zvláštně chráněných území atd. OOP je předmětem

dalšího vývoje, rozsáhlejší změny je možné očekávat po přijetí novely zákona o civilním letectví (č. 49/1997 Sb.) [3] v následujících letech.

Jak již bylo zmíněno výše, pravidla nové legislativy jsou založena na míře rizika, jaký provoz vytváří. Záleží tedy na tom, kde je provoz zamýšlen, s jakým UAS, v jaké výšce a na mnoha dalších faktorech. Vznikly proto tři nové kategorie provozu: OPEN, SPECIFIC a CERTIFIED (česky otevřená, specifická a certifikovaná).



Obrázek 1Pravidlo 1:1 [4]

1.1.1 Kategorie OPEN

Kategorie OPEN je kategorie, která má z těchto tří kategorií nejmírnější požadavky na provozovatele a piloty a zatím jako jediná má přesně definovaná pravidla provozu. Dále se dělí do třech podkategorií, A1, A2 a A3, které mají odlišné požadavky na minimální vzdálenost od lidí, maximální hmotnost UAS, úrovně proškolení pilota apod. Dle pravidel kategorie OPEN je možné létat bez předchozího oprávnění Úřadu pro civilní letectví.

V každé z nových podkategorií provozu kategorie OPEN je povoleno provozovat určitý typ UAS. Evropská legislativa počítá s tím, že v následujících letech budou UAS dostupné na trhu spadat do konkrétních tříd. Každá třída se vyznačuje rozdílnými specifikacemi. Třídy budou mít označení C0 až C6 a bezpilotní systémy budou na sobě muset mít štítek, na kterém bude

třída uvedena. V kategorii OPEN bude možné létat s UAS tříd C0 až C4. Specifikace tříd C0 až C4 jsou popsány v tabulce 1. Zatím ale žádné bezpilotní systémy s označením třídy nejsou dostupné. Proto se zatím UAS rozlišují dle maximální vzletové hmotnosti letounu.

Tabulka 1 Třídy UAS pro OPEN kategorii [5]

Parametry	***C0***	***C1***	***C2***	***C3***	***C4 (modely)***
Maximální vzletová hmotnost	<250 g	< 900 g nebo < 80 J (dopadová energie)	< 4 kg	< 25 kg a 3 m	< 25 kg
Maximální provozní rychlost	< 19 m/s	< 19 m/s	nastavitelné < 3 m/s (kr. letounů)	ne	ne
Maximální výška letu nad zemí	< 120 m AGL	< 120 m AGL	< 120 m AGL	< 120 m AGL	ne
Pohon - omezení	elektro < 24 V	elektro < 24 V	elektro < 48 V	elektro < 48 V	ne
Follow-me režim	< 50 m	< 50 m	ne	ne	ne
Failsafe systém	ne	ano	ano (kr. upoutaných)	ano (kr. upoutaných)	jen přednastavená poloha, zákaz automatického letu
Upoutaný provoz	ne	ne	lanko < 50 m	lanko < 50 m	ne
Zabezpečený řídící a kontrolní spoj	ne	ne	ano (kr. upoutaných)	ano (kr. upoutaných)	ne
Limitovaná hlučnost	ne	<85 dB (kr. letounů)	< 97 dB dle MTOM (kr. letounů)	ne, jen povinný štítek (kr. letounů)	ne
Sériové číslo	ne	ano	ano	ano	ne
Identifikace za letu	ne	ano (sér. č., reg. č. provozovatele, poloha, výška, traťový úhel a rychlost a poloha pilota nebo místa vzletu)	ano (kr. upoutaných) (sér. č., reg. č. provozovatele, poloha, výška, traťový úhel a rychlost a poloha pilota nebo místa vzletu)	ne	identifikace za letu
Geo-awareness	ne	ano (upozornění pilota na omezené prostory)	ne	geo-awareness	ne
Indikace nízkého stavu baterie	ne	ano	ano	ano	ne
Světla pro řiditelnost a odlišení	ne	ano	ano	ano	ne
Uživatelská příručka	ano	ano	ano	ano	ano
Informační leták EASA	ano	ano	ano	ano	ano

Podkategorie A1 umožňuje pilotům létat v blízkosti lidí, protože zde nejsou definovány žádné vzdálenosti od nezapojených osob, ani od budov. To znamená, že v této podkategorii je možné přelétávat nezapojené osoby, ale pilot by se tomu měl, pokud možno, vyhnout a zbytečně se nad nezapojenými osobami nezdržovat. Toto je ale umožněno pouze těm, kteří vlastní bezpilotní systém, jehož MTOW nepřekračuje 250 g. Hmotnostní limity pro UAS v této

podkategorii jsou aktuálně nastaveny na 500 g. V budoucnu zde budou spadat bezpilotní systémy se štítky C0 a C1.

S o něco těžším UAS se je možné létat v zastavěné oblasti, tedy v hustě osídleném prostoru (HOP) v rámci podkategorie A2. Let je v rámci této podkategorie povolen s UAS od 500 g do 2 kg a v budoucnu s bezpilotními systémy s označením třídy C2. Minimální horizontální vzdálenost od nezapojených osob je 50 m, ale při využití nízkorychlostního režimu (udržování konstantní rychlosti $3\ \frac{m}{s}$) je možné se k nezapojeným osobám přiblížit až na 5 m. Jinak je vzdálenost od nezapojených osob definována pravidlem 1:1. Nezapojené osoby jsou osoby nezapojené do provozu, které neudělily souhlas s účastí na provozu.

V podkategorii A3 je nutné dodržovat minimální vzdálenost od obytných, obchodních, průmyslových a rekreačních oblastí alespoň 150 m. Zjednodušeně řečeno to znamená, že můžeme létat na loukách a polích. Při setkání s nezapojenou osobou je nutné udržovat od ní vzdálenost alespoň 30 m a dále se řídit pravidlem 1:1. Bezpilotní systémy do 25 kg mohou létat v rámci této kategorie, a jakmile se budou vyrábět UAS se štítkem, budou sem spadat třídy C2, C3 a C4. Ve všech podkategoriích kategorie OPEN jsou lety nad shromážděním osob a zásahy IZS zakázány.

Nová evropská legislativa definuje povinnost registrace provozovatelů UAS. Registrace se provádí pouze jednou, nezávisle na počtu UAS, které provozovatel vlastní. Po registraci je provozovateli přiděleno registrační číslo provozovatele, kterým musí označit všechny své bezpilotní systémy, se kterými chce do vzduchu. Ten, kdo chce navíc s UAS vzlétnout, tedy piloti, musí projít zkouškou znalostí a po jejím úspěšném splnění získá oprávnění létat v podkategorii A1/A3 v rámci kategorie OPEN. Pokud pilotovi pro zamýšlený provoz nestačí pilotní průkaz A1/A3, má možnost si rozšířit svou pilotní licenci o způsobilost pilota v podkategorii provozu A2. Výhodou je, že jak registrace provozovatele, tak pilotní licence jsou platné ve všech státech EU. Nicméně každý stát si může podmínky provozu upravit, respektive zpřísnit, proto je před letem potřeba zjistit si pravidla platná pro daný členský stát.

Výjimku z povinnosti registrace pilota mají ti, kteří chtějí létat s UAS do 250 g bez kamery a jiného senzoru, který je schopen zaznamenat osobní údaje, nebo s UAS se štítkem C0. Výjimku mají i piloti modelů letadel v rámci existujících klubů a sdružení leteckých modelářů. Protože provoz modelů letadel probíhal a stále probíhá na speciálních letištích k tomu vyhrazených a jejich provoz probíhá bezpečně dle předchozí legislativy, zatím se na ně povinnost registrace vyplývající z nové evropské legislativy nevztahuje.

1.1.2 Kategorie SPECIFIC

Kategorie SPECIFIC je kategorie se střední mírou rizika a je určena pro ty, kterým nestačí limity kategorie OPEN a potřebují je v rámci svého provozu přesáhnout. Protože při provozu v této kategorii vzniká větší provozní riziko, je třeba získat oprávnění od ÚCL. Oprávnění je vydáváno na základě provedení analýzy provozního rizika SORA („Specific Operations Risk Assessment“). Analýzu musí provést provozovatel při podávání žádosti a následně je znova posouzeno riziko přímo Úřadem.

V kategorii SPECIFIC existují tři možnosti, jak zde létat:

a) Oprávnění k provozu vydané Úřadem;
b) Standartní scénář („Standart Scenario“ neboli STS);
c) Oprávnění provozovatele lehkého bezpilotního systému („Light UAS operator Certificate“ neboli LUC).

1.1.2.1 Oprávnění k provozu

Oprávnění k provozu (OkP) je v současné době nejběžnější způsob, jak si provozovatelé a piloti zalétají v kategorii SPECIFIC. Jedná se o soubor dokumentů, které je potřeba vyplnit a odeslat na ÚCL. Ve všech dokumentech je potřeba vyplnit registrační číslo provozovatele a jméno provozovatele. V prvním dokumentu je například třeba vyplnit, s jakým UAS bude let proveden, zdali bude mít zajištěno pojistné krytí a jaké zmírňující opatření a cíle provozní bezpečnosti (OSO) je provozovatel schopen splnit. Příkladem OSO je OSO#01, které říká, že je nutné zajistit, že provozovatel UAS je odborně způsobilý a/nebo prověřený [6].

Druhý dokument se provozovatele ptá na konkrétnější informace o zamýšleném provozu. Definuje zde, kde chce létat, v jaké výšce, za jakých podmínek (VLOS, BVLOS) a na kdy je provoz naplánován. Součástí tohoto dokumentu je také seznam pilotů, kteří budou do provozu zapojení a analýza SORA. Analýza se ptá, jakou míru rizika na zemi (GRC) provoz vytváří. Riziko na zemi je definováno třemi parametry; maximálním charakteristickým rozměrem UAS, očekávanou specifickou kinetickou energií a provozním scénářem. Dále zjišťuje třídu rizika ve vzduchu (ARC). Ta se určuje na základě toho, v jakém vzdušném prostoru bude let proveden. Jestli to bude v okolí letiště, řízeném prostoru, neřízeném prostoru atd. Kombinace GRC a ARC dávají dohromady hodnotu SAIL, což je specifická úroveň zabezpečení a integrity. Podle toho, jaké SAIL vyjde, takové OSO je potřeba splnit. Nakonec v tomto dokumentu provozovatel definuje, v jaké zeměpisné zóně se provoz nachází (CHKO, hustě osídlený prostor, ochranné pásmo liniových staveb apod.).

Třetí dokument se provozovatele ptá, jakým způsobem je schopen zajistit ochranu osobních údajů. Poslední dokumentem provozovatel deklaruje, že bude dodržovat zmírňující opatření provozu.

1.1.2.2 Standartní scénáře

Plánované standartní scénáře (STS) budou možností pro malé provozovatele, jak létat ve specifické kategorii. Provozovatelé sice nebudou splňovat podmínky kategorie OPEN, ale budou mít možnost vydat prohlášení, že upraví plánovaný provoz dle vybraného scénáře a budou dodržovat jeho podmínky. ÚCL po přijetí prohlášení vydá potvrzení o přijetí prohlášení. Až po jeho získání je možné provoz uskutečnit. Standartní scénáře jsou zatím definovány dva a na obrázku 2 jsou vypsány základní podmínky těchto scénářů.

STS#	Vydání/datum	Charakteristiky UAS	BVLOS/VLOS	Přelétávaná oblast	Maximální vzdálenost od dálkově řídícího pilota	Maximální výška	Vzdušný prostor
STS-01	červen 2020	Nesoucí označení třídy C5 (maximální charakteristický rozměr do 3 m a MTOM do 25 kg)	VLOS		VLOS	120 m	Řízený nebo neřízený s nízkým rizikem setkání s letadlem s pilotem na palubě
STS-02	červen 2020	Nesoucí označení třídy C6 (maximální charakteristický rozměr do 3 m a MTOM do 25 kg)	BVLOS		2 km s AO 1 km bez AO	120 m	Řízený nebo neřízený s nízkým rizikem setkání s letadlem s pilotem na palubě

Obrázek 2 Seznam standartních scénářů [6]

1.1.2.3 Oprávnění provozovatele lehkého bezpilotního systému

Zkušenější profesionální provozovatelé, kteří Úřadu prokáží, že jsou spolehliví, mají možnost získat oprávnění provozovatele lehkého bezpilotního systému (LUC). To jim umožní vlastní a individuální posuzování provozního rizika a díky tomu si budou moci sami schvalovat plánované lety [5]. 11. února 2022 získala společnost Primoco UAV SE jako první v ČR oprávnění k provozu LUC. V Evropě bylo těchto oprávnění vydáno zatím pouze pět. Primoco UAV SE je zároveň první provozovatel, který získal oprávnění LUC pro provoz UAV s pevným křídlem [7].

1.1.3 Kategorie CERTIFIED

V kategorii CERTIFIED se počítá s největší mírou rizika provozu. V budoucnu budou do této kategorie spadat bezpilotní systémy, které budou v rámci Urban air mobility převážet cestující

bezpilotními systémy ve městech. Nebude se jednat pouze o přepravu osob, ale i o přepravu jiného užitečného nákladu nebo nebezpečného nákladu jako převoz krve apod.

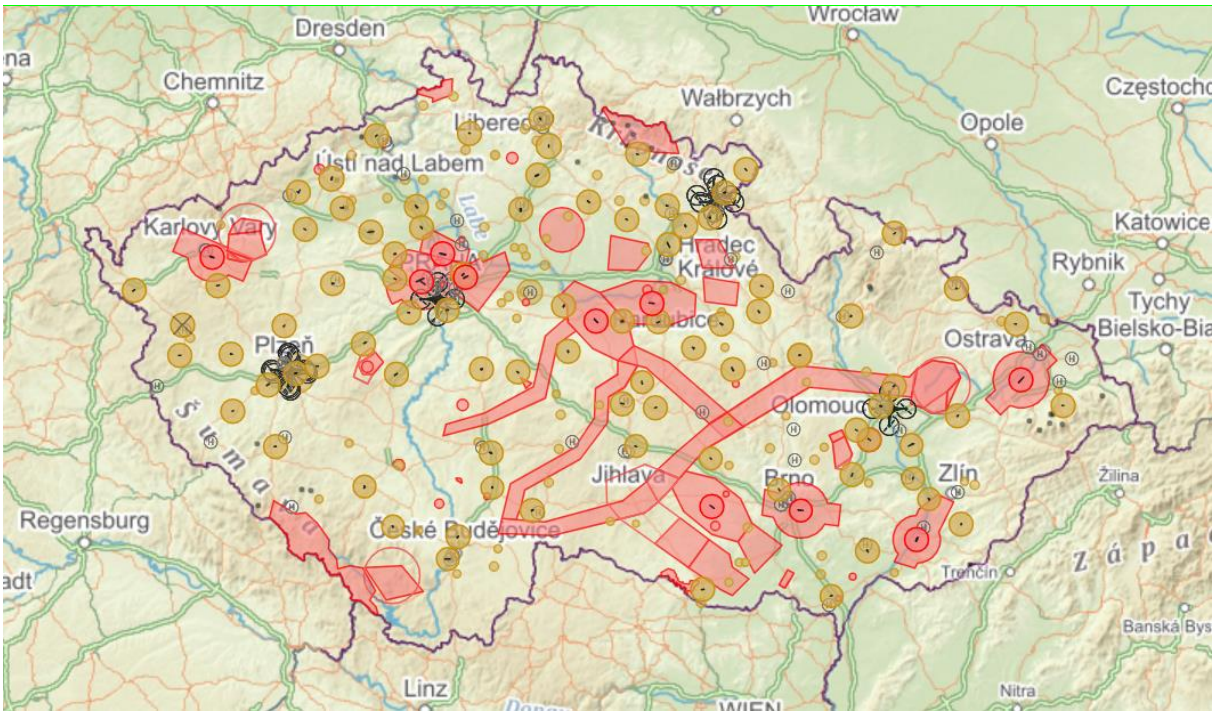
Tato kategorie bude mít největší požadavky na provozovatele, piloty i bezpilotní systémy. Veškerý letecký personál, bude muset být certifikován, stejně jako výroba, a samotné UAS taktéž bude muset projít procesem certifikace.

Již teď je známo, jaký provoz bude do této kategorie spadat. Budou to lety, kde bude let prováděn [5]:

a) nad shromážděním lidí s UAS o rozměrech 3 m a větších;
b) s osobami na palubě;
c) s nebezpečným zbožím, které by mohlo způsobit velké riziko v případě nehody.

1.1.4 Geo-zóny

Zásadní změnu, kterou nová legislativa přináší je definování geo-zón. Každý členský stát definuje zeměpisné zóny pro bezpilotní systémy, ve kterých platí speciální podmínky pro let. V minulosti (ale bohužel i v současnosti), často docházelo k narušení vzdušných prostorů bezpilotními letadly. Piloti UAS si před letem nezjistí, zdali v daném vzdušném prostoru mohou létat a dochází ke střetům s letadly s pilotem na palubě nebo narušením bezpečnosti provozu kolem letišť. Takovéto prostory vznikly v okolí měst, významných státních staveb, kritické infrastruktury, chráněných krajinných oblastí atd. Například v prostoru LKP1 kolem Pražského hradu je let povolen pouze s oprávněním ÚCL. Prostor LKP1 se zároveň nachází uvnitř prostoru LKR9, což je omezený vzdušný prostor nad centrem hlavního města Prahy, kde je taktéž let povolen pouze s oprávněním ÚCL. Povinností každého členského státu je zveřejnit mapu těchto zón. V ČR k tomuto účelu aktuálně slouží webová aplikace Dronview od Řízení letového provozu (ŘLP). Jak aplikace vypadá, je možné vidět na obrázku 3.



Obrázek 3 Aplikace DronView [8]

V budoucnu budou mapové podklady převedeny do datových souborů, které budou nahrány do navigačního systému UAS. Díky tomu bude možné aktivovat služby „geo-awareness“ a „geo-fencing“, které jsou klíčové pro koncept U-space. Služba „geo-awareness“ bude sloužit k upozornění pilota, že se blíží k omezenému prostoru. Oproti tomu služba „geo-fencing“ bude fungovat mnohem radikálněji a nedovolí pilotovi narušit omezený prostor, do kterého nemá oprávnění vletět. Zároveň může fungovat i opačně, to znamená, že nenechá pilota vyletět mimo vymezený prostor.

Podobným způsobem již fungují geo-mapy některých výrobců bezpilotních systémů. Tyto mapy ovšem fungují pouze pro UAS daného výrobce. Mapy nejsou publikovány státem a o zveřejnění omezeného vzdušného prostoru v této mapě je potřeba výrobce zažádat.

1.1.5 E-identifikace

E-identifikace je jeden z dalších kroků k bezpečnějšímu a organizovanějšímu provozu UAS. Každý bezpilotní systém bude muset vysílat alespoň základní údaje o letu, a to registrační číslo provozovatele, sériové číslo UAS a jeho aktuální polohu.

Bezpilotní systémy budou muset být vybaveny zařízením, které je schopné tyto údaje vysílat. Zabudované zařízení budou mít UAS, které budou vyrobeny dle požadavků na třídy. Ty, které

byly vyrobeny bez štítku, budou muset být vybaveny doplňkovým zařízením, které bude schopno údaje vysílat.

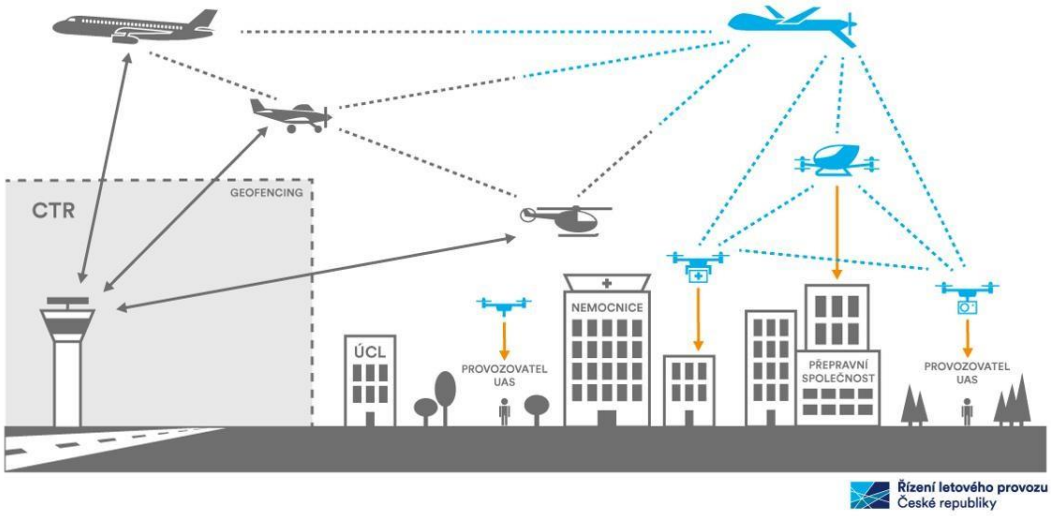
S e-identifikací se v budoucnu počítá jako s běžnou součástí v kategorii SPECIFIC, ale podmínky budou nejspíše upřesněny v nadcházejících nařízení evropské komise a novelizaci zákona o civilním letectví. Nicméně s povinnou e-identifikací pro všechna UAS počítá koncept společného vzdušeného prostoru pro bezpilotní i letadla s pilotem na palubě s názvem U-space.

1.2 U-space

Všechny výše zmíněné kroky implementování evropské legislativy vedou k tomu, aby ve všech členských státech platily stejné podmínky provozu. Některým státům to jde rychleji než jiným, ale v budoucnu budou všude platit stejná pravidla a bude možné zavést společný vzdušný prostor s kontrolovaným provozem bezpilotních systémů. K dosažení společného vzdušného prostoru pro UAS a letadla s pilotem na palubě nás čeká ještě dlouhá cesta, ale jeho výsledkem bude velmi efektivní a bezpečné využití vzdušného prostoru všemi jeho uživateli.

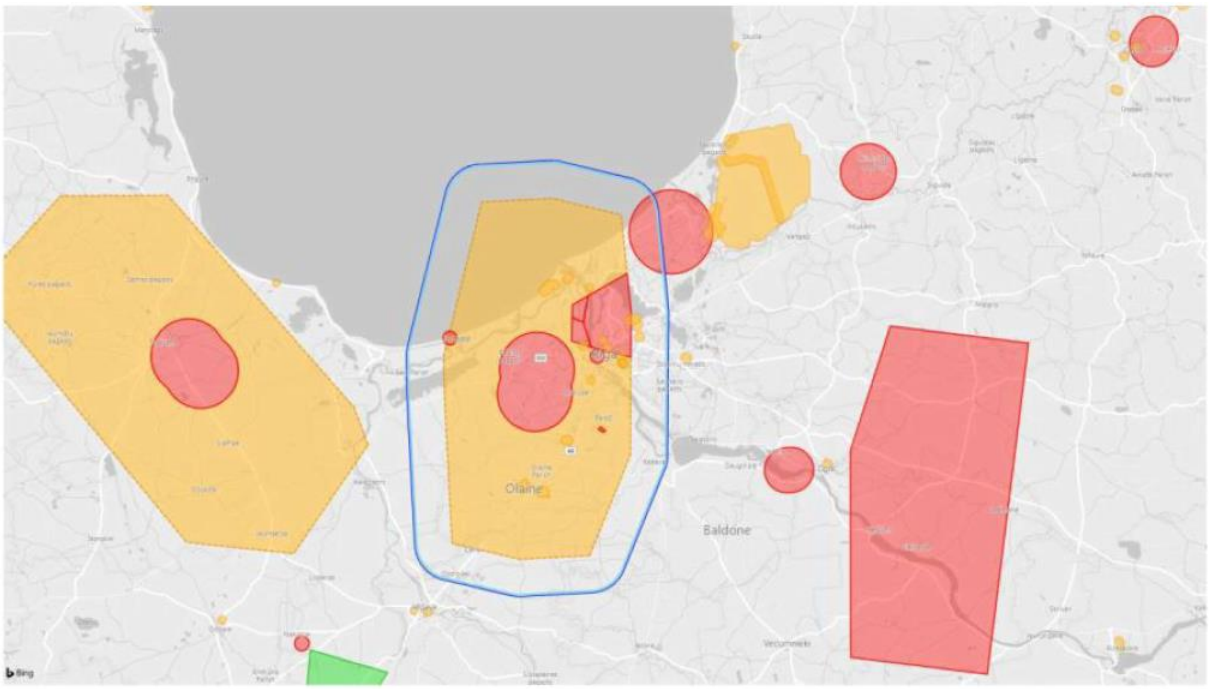
U-space představuje soubor nových služeb a postupů vedoucí k bezpečnému a efektivnímu vzdušnému prostoru pro UAS i letadla s pilotem na palubě. Společné prostředí bude moci fungovat díky kooperaci poskytovatelů ATM/ANS služeb, poskytovatelů aplikací potřebných pro samotný provoz UAS, kteří budou dodávat potřebné informace pilotům UAS, a jednotlivých autorit.

V rámci U-space bude možné provozovat všechny typy provozů a bezpilotních systémů. Ve městech budou povoleny VLOS i BVLOS lety. Výška 120 m nebude nadále limitující v řízeném, ani neřízeném vzdušném prostoru a umožněny budou automatické a zejména pak autonomní lety, které aktuálně není možné provozovat. Služby, které budou U-space podporovat spoléhají na vysokou úroveň automatizace a digitalizace pozemní infrastruktury i funkcí samotného UAS. Představa, jak by U-space mohl vypadat je znázorněná na obrázku 4.



Obrázek 4 Princip fungování U-space [5]

Na obrázku 5 je vyznačeno, jakým způsobem mohou vypadat geo-zóny společně s plánovanými prostory U-space. Červenou barvou jsou vyznačeny prostory, kde je provoz UAS zakázán. Po splnění podmínek daného prostoru (oprávnění k letu atd.), může být provozovateli dovoleno zde létat. Žlutou barvou jsou znázorněny zeměpisné zóny UAS, kde je provoz UAS omezen. Provoz je podmíněn splněním podmínek prostoru. Zelenou barvou jsou označeny prostory, které zjednodušují provoz UAS v kategorii OPEN. Modrou čarou je vyznačen vzdušný prostor U-space, s podporou U-space služeb



Obrázek 5 Příklad zeměpisných zón UAS zahrnující znázornění plánovaných prostorů U-space [6]

1.2.1 Fáze U-space

U-space má zatím definovány čtyři fáze U1 až U4. S každou další fází přichází vyšší míra automatizace a digitalizace. Tyto čtyři fáze definovaly výzkumné přístupy SESAR, které jsou podporovány agenturou EUROCONTROL [9].

V první fázi U1 je očekáváno zavedení počátečních služeb U-space, jejichž základními pilíři je e-registrace, e-identifikace a definování geo-zón. Jak již bylo zmíněno výše, zatím je zavedena e-registrace pilotů a provozovatelů, jsou definovány geo-zóny, ale na zavedení e-identifikace stále čekáme. První krůčky započaly v roce 2019 a dnes jsme se již měli nacházet ve fázi U2, ale kvůli složitosti implementovaných prvků a světové pandemii se stále nacházíme v první fázi [5].

V druhé fázi U2 se počítá s novými službami, které budou podporovat samotný provoz UAS. Budou dostupné služby k plánování letů, schválení letů, jejich sledování, dále služby umožňující poskytování informací o vzdušném prostoru a budou nastavena pravidla, jakým způsobem bude probíhat výměna dat s řízením letového provozu [5].

Ve třetím kroku U3 již budou v provozu služby, které budou zvládat velký počet letů a budou v provozu funkce schopné řídit kapacitu a umět detekovat konfliktní provoz. Jakmile začnou fungovat služby v této fázi, počítá se s významným nárůstem provozu v rámci U-space [5].

Čtvrtá fáze U4 již bude schopná plně integrovat UAS do U-space, všechny služby umožňující společný provoz UAS s provozem s pilotem na palubě již budou spuštěny a bude zavedena vysoká úroveň automatizace, digitalizace a konektivity [5].

1.2.2 Služby U-space

Provoz U-space bude zajišťovat šest základních služeb U-space, které jsou definovány jako *služby založené na digitálních službách a automatizaci funkcí navržené tak, aby podporovaly bezpečný, zabezpečený a účinný přístup velkého počtu bezpilotních systémů do vzdušného prostoru U-space* [10]. Poskytovatelé těchto služeb musí být certifikováni a k tomu, aby služby mohly být poskytovány, je třeba zajistit koordinaci činností a výměnu informací mezi poskytovateli U-space služeb (USSP) a letových provozních služeb.

1.2.2.1 Síťová identifikační služba

Tato služba bude umožňovat nepřetržité zpracování dálkové identifikace UAS po celou dobu letu a svým uživatelům bude poskytovat dálkovou identifikaci UAS v souhrnné podobě. Služba bude umožňovat svým uživatelům přijímat zprávy, které budou obsahovat [10]:

a) registrační číslo provozovatele UAS;
b) sériové číslo UAS;
c) zeměpisnou polohu UAS;
d) letová dráha měřená ve směru hodinových ručiček od skutečného severu a pozemní rychlost bezpilotního systému;
e) zeměpisnou polohu dálkově řídícího pilota nebo bod vzletu;
f) nouzový stav UAS;
g) čas generování zpráv.

Uživatelé, kteří budou moci využívat tuto službu jsou [10]:

a) široká veřejnost;
b) ostatní poskytovatelé služeb U-space;
c) poskytovatelé letových provozních služeb;
d) poskytovatel společných informačních služeb;
e) autority.

1.2.2.2 Služba „geo-awareness“

Služba „geo-awareness“ slouží zejména provozovatelům a pilotům v U-space prostoru. Hlavní účel služby je informovat pilota o provozních podmínkách omezených vzdušných prostorů. V případě, že se UAS bude blížit ke vzdušnému prostoru, do kterého nemá oprávnění vletět, bude na to upozorněn. Nejenže služba bude piloty upozorňovat, ale v případě, že pilot na upozornění nezareaguje a bude pokračovat v letu, služba „geo-awareness“ nenechá UAS vstoupit do daného prostoru. Poskytovatelé těchto služeb musí odesílat provozovatelům informace o zeměpisné orientaci včas, aby měl provozovatel možnost se podmínkám a omezením přizpůsobit.

Služba bude poskytovat hlavně tyto informace [10]:

a) informace o provozních podmínkách omezených vzdušných prostorů U-space;
b) významné zeměpisné zóny;
c) dočasná omezení na využívání vzdušného prostoru U-space.

1.2.2.3 Služba oprávnění k letu bezpilotního systému

Pomocí této služby budou poskytovatelé U-space služeb vydávat oprávnění k letu provozovatelům a stanoví podmínky provedení letu. Po obdržení žádosti USSP ověří, zdali žádost je podána v souladu s požadavky na žádost. Žádost musí obsahovat [10]:

a) jedinečné sériové číslo bezpilotního letadla, nebo je-li bezpilotní letadlo zhotoveno soukromě, jedinečné sériové číslo doplňkového zařízení;
b) provozní režim;
c) druh letu (zvláštní provoz);
d) kategorii provozu bezpilotního systému (OPEN, SPECIFIC, CERTIFIED) a případně třídu bezpilotního systému nebo typové osvědčení bezpilotního systému;
e) trajektorii 4D;
f) identifikační technologii;
g) očekávané metody konektivity;
h) výdrž;
i) příslušný nouzový postup v případě ztráty řídícího a kontrolního spoje;
j) registrační číslo provozovatele bezpilotního systému a případně bezpilotního letadla.

Jakmile USSP žádost přijmou, ověří, jestli nebyla podána jiná žádost o oprávnění k letu, která by se nacházela ve stejném vzdušném prostoru U-space a byla by naplánovaná na stejné časové období. Pokud jedna z žádostí bude pro UAS se zvláštním provozem, tato žádost bude

upřednostněna, jinak bude upřednostněna žádost, která byla podána dřív. Za zvláštní provoz se považují lety policejních a celních letadel, lety pátrání a záchrany, lety související s poskytováním lékařské péče, lety zajišťující hašení požárů atd. [11]. Taktéž žádost porovnají s podmínkami letu v omezených prostorech. Následně USSP informuje provozovatele o přijetí, či zamítnutí žádosti. V případě přijetí žádosti také uvedou odchylku od prahových hodnot od oprávnění k letu UAS, respektive do jaké míry se může reálný provoz lišit od schváleného provozu. Při vydávání oprávnění k letu USSP také nahlíží na informace poskytované informační službou o počasí. V případě zamítnutí žádosti může USSP navrhnou provozovateli alternativní oprávnění k letu, tedy možnost vzlétnout, ale za trochu jiných podmínek, než jaké žádal.

Dalším úkolem služby oprávnění k letu bezpilotního systému bude schvalovat aktivaci oprávnění k letu a dát provozovateli vědět, že provoz může začít. Pokud se během aktivovaného oprávnění k letu vyskytne ve stejném vzdušném prostoru U-space letadlo s posádkou, které se nachází ve stavu nouze, může USSP upravit či přerušit oprávnění k letu tak, aby byla zachována bezpečnost provozu [10].

1.2.2.4 Služba informací o provozu

Tato služba zajišťuje poskytování informací provozovateli o provozu jiných letadel, ať už s pilotem na palubě nebo bez, ve stejném vzdušném prostoru. Tyto informace poskytují USSP ve spolupráci se stanovištěm letových provozních služeb (ATSP neboli „Air Traffic Service Providers“). Jakmile se jiná letadla nacházejí v blízkosti provozu bezpilotního systému nebo by jeho provoz mohla ovlivnit, provozovatel je na tuto skutečnost upozorněn. Služba poskytne provozovateli informace o poloze, rychlosti, kurzu nebo směru jiného letadla společně s časem, kdy byla tato zpráva vydána a zprávu pravidelně aktualizuje. Po obdržení takovéto zprávy je provozovatel UAS povinen přijmout nezbytné kroky k tomu, aby bylo zabráněno kolizi [10].

1.2.2.5 Služba informací o počasí

Služba informací o počasí poskytuje informace o aktuálním počasí, na základě kterých provozovatel a USSP posoudí, zda je bezpečné let provést nebo ne. USSP shromažďují údaje o počasí od důvěryhodných zdrojů poskytující tyto informace a před letem či během něho je poskytují provozovateli.

Služba informací o počasí zahrnuje alespoň [10]:

a) směr větru měřený ve směru hodinových ručiček od zeměpisného severu a jeho rychlost v metrech za sekundu, včetně poryvů;
b) výšku nejnižší protrhané nebo souvislé oblačné vrstvy ve stovkách stop nad úrovní země;
c) dohlednost v metrech a kilometrech;
d) teplotu a rosný bod;
e) ukazatele konvekční aktivity a srážek;
f) místo a čas pozorování nebo platné časy a místa předpovědi;
g) vhodnou hodnotu QNH se zeměpisnou polohou její použitelnosti.

1.2.2.6 Služba monitorování souladu

Tato služba umožňuje provozovateli ověřit, zda letí tak, jak má a splňuje požadavky na UAS, jestli využívá nezbytné služby U-space k bezpečnému provozu UAS, což jsou všechny výše zmíněné služby U-space (kromě služby informací o počasí) a zda splňuje podmínky omezeného vzdušného prostoru.

Podstata této služby je následující. Jakmile služba monitorování souladu zjistí odchylku od oprávnění k letu, která překračuje i povolené odchylky od prahových hodnot, informuje ostatní USSP, ostatní provozovatele bezpilotních systémů a stanoviště letových provozních služeb o této skutečnosti pomocí výstrahy, kterou následně potvrdí [10].

1.2.3 Prvky U-space

Provoz U-space je založen na koordinaci a sdílení dat mezi jednotlivými prvky v daném vzdušném prostoru U-space. Role provozovatele bezpilotního systému je poměrně jasná. Provozovatel má zájem provozovat UAS v prostoru U-space. K tomu musí zajistit, aby bezpilotní systém splňoval určité požadavky na schopnosti a výkonnost, dále musí zajistit, že bude k provozu využívat nezbytné U-space služby a musí splňovat podmínky omezených prostorů. Před každým letem musí provozovatel předložit platné oprávnění k letu svému provozovateli služeb U-space a musí podmínky oprávnění dodržovat.

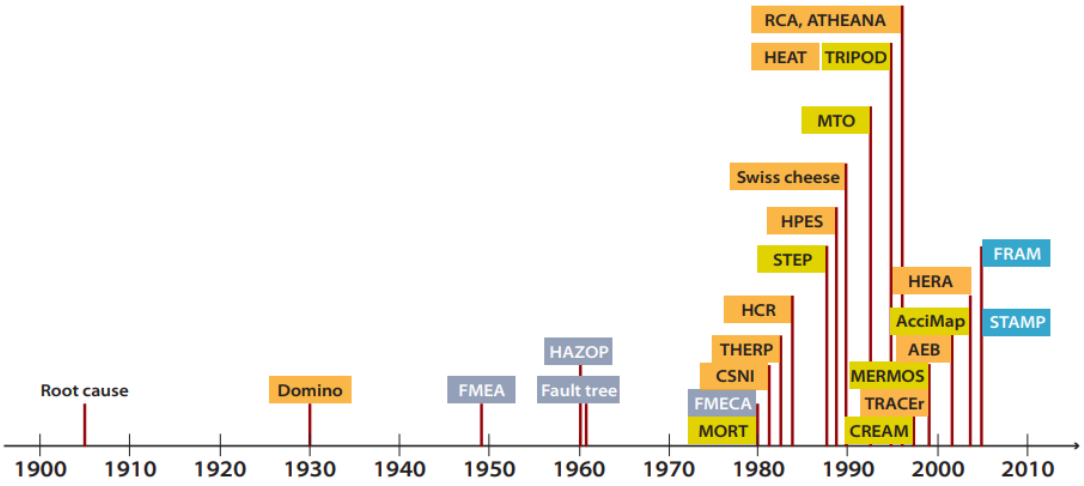
Role a činnosti poskytovatelů služeb U-space jsou popsány v předchozích kapitolách. Dalším z prvků je poskytovatel společných informačních služeb (CIS neboli „Common Information Service“). V legislativě je společná informační služba definována jako *služba založená na digitálních službách a automatizaci funkcí navržená tak, aby podporovala bezpečný, zabezpečený a účinný přístup velkého počtu bezpilotních systémů do vzdušného prostoru U-space.* [10] Jinými slovy, poskytovatel společných informačních služeb bude

zajišťovat výměnu statických a dynamických informací mezi U-space poskytovateli, státem a poskytovateli letových provozních služeb. Předpokládá se, že bude jeden poskytovatel společných informačních služeb na jeden U-space prostor. Členské státy, jakožto součást společných informačních služeb, budou mít na starost sdílení dat o hranicích prostoru U-space, informace o požadavcích na výkonnost U-space služeb, bezpilotních systémů a provozních podmínek daného vzdušného prostoru. Také budou muset poskytovat seznam certifikovaných USSP, jaké služby nabízejí a jejich kontaktní údaje. Zejména pro provozovatele UAS budou státy muset poskytovat data o všech vzdušných prostorech U-space, definované geo-zóny, případně jejich omezení. USSP pomocí společných informačních služeb nasdílí podmínky poskytování svých služeb [10].

Poskytovatelé letových provozních služeb (ATSP neboli „Air Traffic Service Providers“) sdílejí informace o provozu letadel s posádkou. Za poskytovatele letových služeb považujeme letištní a letové informační služby FIS („Flight Information Service“) a AFIS („Aerodrome Flight Information Service“). Díky těmto informacím může U-space služba poskytovat informace týkající se provozu letadel s pilotem na palubě. Poskytovatelé navigačních služeb (ANSP neboli „Air Navigation Service Provider“) mají za úkol poskytovat letové navigační služby a jsou zodpovědní za řízení letového provozu v daném státě nebo regionu.

2 Metody provozní bezpečnosti

Provozní bezpečnost je jedním z nejvíce sledovaných faktorů v letectví. Všichni výrobci, provozovatelé, úřady jsou tlačeni ke zvyšování bezpečnosti, ale zároveň sami mají zájem ji stále zvyšovat. Nahlížení na bezpečnost se v průběhu vývoje lidstva výrazně změnila. Zranění i úmrtí byly na pracovišti poměrně běžné. Následně si lidstvo uvědomilo, že s tím dá něco dělat a začalo bezpečnost řešit. Nejdříve se bezpečnost řešila pouze z pohledu technického stavu přístrojů a technického vybavení. Následně se řešil vliv člověka na bezpečnost, organizační mechanismy a řídící procesy. Nejmodernější systémové bezpečnostní modely se zabývají všemi uvedenými faktory. Obrázek 6 ukazuje, jak se vyvíjely bezpečnostní metody a modely v čase. Šedou barvou jsou znázorněny bezpečnostní metody, které řeší pouze technické faktory. Oranžovou barvou jsou znázorněny bezpečnostní metody, které se zabývají, jaký vliv na bezpečnost má lidský faktor. Žlutou barvou jsou vyznačeny ty metody, které řeší organizační faktory a modrou barvou jsou vyznačeny systémové modely/metody.



Obrázek 6 Vývoj bezpečnostních modelů a metod v čase [12]

Dnešní svět si již nevystačí pouze s bezpečnostními metodami a modely, které se zabývaly pouze technickými zařízeními. S vývojem nových technologií přichází komplexní systémy a vývoj nových hrozeb, které musíme řešit moderním přístupem k bezpečnosti. V následujících odstavcích budou některé z bezpečnostní metod popsány.

Jedna z technických metod je FTA neboli „Fault Tree Analysis“ (do češtiny překládáno jako analýza stromu poruchových stavů), který byl definován v roce 1961. FTA lze zjednodušeně popsat jako metodu, která specifikuje nežádoucí stav systému (obvykle stav, který je kritický z hlediska bezpečnosti nebo spolehlivosti), a systém je poté analyzován ve svém reálném prostředí a provozu, aby se našly všechny způsoby, jakými může dojít k nežádoucí události (vrcholové události). Ke znázornění systému a možného výskytu poruch slouží strom poruch neboli „fault tree“, což je grafický model různých kombinací poruch, které povedou k výskytu předem definované nežádoucí události. Poruchy mohou být události, které jsou spojeny se selháním hardwaru komponent, lidskými chybami, chybami softwaru. Jednotlivé prvky ve stromu poruch spojují logická hradla A a NEBO [12].

Metoda SHELL vystihuje problematiku lidského činitele a vlivy na něj působící. Uprostřed je subjekt (člověk, „lifeware“) a kolem něj se nacházejí vlivy ovlivňující jeho práci. Všechny prvky procesu musí zajišťovat žádanou úroveň bezpečnosti, protože ta je hlavním cílem. Prvním prvkem je software, který definuje programy nebo soubor informací, postupů (algoritmů), kterými se při práci řídíme. Druhým prvkem je hardware, čímž je myšlen stroj a všechno hmotné, s čím pracujeme, tedy technologie, ovládací prvky, pracovní nástroje atd. Třetím prvkem je „environment“ neboli okolní prostředí. To může být vnější, jako například viditelnost, povětrnostní podmínky atd., nebo vnitřní, jako teplota, hluk, vibrace, osvětlení apod. Posledními dvěma prvky je „lifeware“, čímž jsou myšleni lidé. Jeden z nich je osoba samotná, na kterou se analýza vztahuje. Ta má nějaké vlastnosti, schopnosti a vědomosti, které ovlivňují jeho práci, jako například vzdělání, zkušenosti, motivace, psychická a fyzická kondice. Posledním prvkem jsou osoby obklopující analyzovanou osobu, tedy kolegové, nadřízení, zákazníci atd [13].

Další kategorií modelů jsou organizační metody. Jedním z nich je například metoda MORT neboli „Management Oversight and Risk Tree“. Pomocí diagramu analýza vyšetřuje, jaké riziko působilo na jednotlivé části systému a jak je možné se jim vyvarovat díky změnám na organizační úrovni [14].

Základem všech výše zmíněných metod je dekompozice systému. Metody zkoumají jednotlivé části systému postupně. Nejsou tedy vhodné pro analyzování komplexních systémů, které nelze rozebrat na jednotlivé části a ty zvlášť analyzovat. Komplexní systémy je potřeba analyzovat jako celek. Komplexní systémy jsou takové systémy, u kterých nelze provést analytickou redukci, nelze je rozebrat na jednotlivé části, které by se daly jednoduše pochopit. Zdrojem komplexity je v těchto systémech člověk a software. Všechny výše zmíněné

bezpečnostní metody zastávají přístup tzv. Safety-I. Klasifikaci na Safety-I a Safety-II definoval profesor Erik Hollnagel. Tvrdí, že pomocí Safety-I lze analyzovat bezpečnost jednoduchých a složitých systémů, ale nikoli komplexních systémů. Profesor Hollnagel definoval Safety-I tak, jak je popsáno dále v tomto odstavci. Safety-I vnímá člověka jako zdroj nebezpečí v systému. Jakákoli variabilita v systému je škodlivá, protože se vždy jedná o odchylky od zavedených postupů, což je nežádoucí. Na odchylky v bezpečnosti reaguje, až když se stane událost, kde byla bezpečnost ohrožena. Zabývá se tím, kdo udělal chybu, nebo kde se stala chyba. Odpovědí na tuto otázku je často člověk. V Safety-I lze bezpečnost systému nastolit pouze tehdy, když je zamezeno vzniku lidské chyby. Tedy jsou vytvořeny bariéry, které v budoucnu zabrání vzniku lidského selhání. [15]

Poslední kategorií bezpečnostních modelů jsou ty, které jsou založeny na systémové teorii. Tyto modely byly vyvinuty jako reakce na rychle se rozvíjející svět, technologie, snahu vše automatizovat, tedy kvůli zvyšující se komplexitě systémů. Svět je čím dál tím komplexnější a na popsání systémů v něm se vyskytujících, již modely Safety-I nestačí. Nedokáže detailně vysvětlit nehody vznikající v komplexních systémech. Systémové metody umějí analyzovat systém jako celek. Nezaměřují se na selhání jednotlivých komponent, ale umějí identifikovat nebezpečí v systému jako celku. Dokáží implementovat vliv chování člověka. Systémový přístup má například metoda FRAM („Functional Resonance Analysis Method“), model STAMP („System-Theory Based Accident Model and Processes“), ze kterého vychází analýza STPA („Systems Theoretic Process Analysis“) a model RAG („Resilience Assessment Grid“). Metody FRAM a RAG využívají principy Safety-II.

Přístup Safety-II se výrazně liší od Safety-I. Safety-II vnímá člověka jako nutnou součást systému k jeho běžnému provozu. Je zdrojem komplexity a zároveň odolnosti systému, protože člověk dokáže odhalit nebezpečí a reagovat na něj. Tento přístup chápe, že se člověk nemůže chovat jako stroj. Říká, že člověk zapojený do systému neselhává, pouze reaguje na situaci. Safety-I vnímá člověka jako zdroj nebezpečných událostí. Safety-II na rozdíl od Safety-I vnímá odchylky od postupů (variabilitu) jako normální a nevyhnutelné, až nutné. I přístup k bezpečnosti je ve srovnání se Safety-I odlišný. Princip vzniku dobrých událostí je v Safety-II stejný, jako princip vzniku špatných událostí. Safety-II se snaží být proaktivnější a získává data nejen z negativních událostí, ale také z každodenních výsledků. Modely Safety-I pracují pouze s daty špatných událostí, zatímco modely Safety-II pracují s daty z každodenního provozu, respektive řeší, jak by systém fungovat měl, a je pomocí nich možné odhalit jeho slabá místa. Safety management je proaktivní, protože řeší i ty výjimečně dobré

události (úspěchy, výjimečně dobré události, které se běžně nestávají) a snaží se, aby jich bylo co nejvíce. Safety-II říká, že ty výjimečně dobré události vznikají stejným způsobem, jako ty špatné události.

Použití metod Safety-II je možné, pokud se v systému vyskytuje emergence. Emergencí je myšlen princip, kdy je možné pozorovat jednotlivé příčiny vzniku negativní události, ale není jisté spojení mezi nimi. Emergentní vlastnosti v systému je možné odhalit, když je na systém nahlíženo z pohledu interakcí v systému. Bezpečnost je v Safety-II zajištěna řízením výkonnosti člověka a sledováním variability. Díky emergenci může v systému vznikat rezonance, což je kombinace nakupených variabilit (odchylek od běžného chování systému). Jakmile kombinace variabilit překročí nastavené meze, může vzniknout rezonance, tedy neočekávaná událost, která může být negativní i pozitivní. Systémové metody se snaží snížit vzájemnou rezonanci a stabilizovat systém zpět do bezpečného stavu [15].

Pro účely této práce jsou vybrány právě metody založené na systémovém přístupu, a to z toho důvodu, že na vybraný systém působí mnoho různých faktorů dohromady, se kterými jen systémové metody dokáží pracovat. Dokáží do analýzy zahrnout lidského činitele, technické vybavení i organizační prvky. Komplexní přístup nahlížející na celý systém je jejich velkou výhodou. Nerozkládá systém na jednotlivé části, ale analyzuje jej jako celek. Zvolený systém je třeba vyhodnocovat proaktivním způsobem.

Systémové metody, které jsou vybrány pro proaktivní vyhodnocení systému jsou metody FRAM a STPA. Obě tyto metody dokáží proaktivně i reaktivně odhalit, jakým způsobem a kde v systému vznikají negativní události. Metoda RAG není pro tento systém vhodná, protože ta poskytuje návod, jak vytvořit odolný systém. Metoda FRAM se snaží pochopit, jak systém normálně funguje a díky tomu dokáže vysvětlit, jak se v systému stávají negativní události. Analýza STPA je analýza rizik, která umožňuje řídit negativní události v systému a díky zpětným vazbám je pochopit a poučit se z nich. U-space tak může být díky těmto dvěma metodám analyzován jako komplexní systém a jako celek. Metody FRAM a STPA, budou detailně popsány v následujících kapitolách.

2.1 STPA

Analýza STPA leží na základech bezpečnostního modelu STAMP. Ten vznikl v Americe pod vedením profesorky Nancy G. Levesonové. Profesorka Levesonová je americká odbornice na bezpečnost systémů a softwaru a profesorka letectví a astronautiky na MIT ve Spojených státech [16].

2.1.1 STAMP

STAMP vznikl k řešení komplexních problémů a uměle vytvořených systémů. Model je založený na systémové teorii. Systémová teorie popisuje komplexní sociotechnické problémy a snaží se vysvětlit jejich chování. Jejím cílem je analyzovat systém jako celek, ne analyzovat jednotlivé části systému zvlášť, jak tomu bylo u dříve vytvořených modelů. Systémová teorie je založena na dvou myšlenkách [17]:

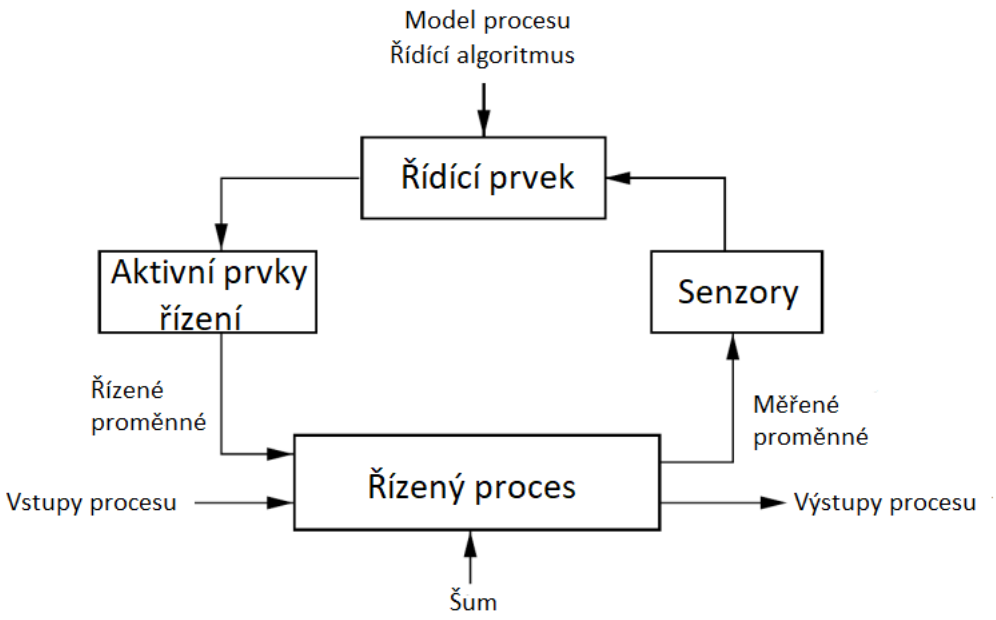
a) emergence a hierarchie

   Komplexní systémy se dají rozdělit na hierarchické úrovně. Každá úroveň je komplexnější než ta pod ní. Každá z vrstev má emergentní vlastnosti a emergence neexistuje v nejspodnějších úrovních.

b) komunikace a řízení

   Komplexní systémy jsou závislé na komunikaci a řízení. Spodní úrovně se řídí vrstvami nad nimi. Řízení v systémech znamená nutnost komunikace, protože každá úroveň potřebuje vědět, jak funguje úroveň pod ní. Nebezpečné procesy v nižších vrstvách vyplývají z vrstev nad nimi. Proto je nutné k identifikaci nebezpečného procesu znát vrstvy nad nimi.

Aby bylo možné získat informace o celém systému, je potřeba definovat a použít se z chování jedné specifické systémové úrovně. STAMP dokáže pracovat se systémem, který zahrnuje software, člověka, organizace, technické systémy, takzvanou „safety culture“, atd. Základní myšlenka modelu STAMP je, že nežádoucí stavy lze včas detekovat a řídit. Vnímá sociotechnické systémy jako komplexní, ze kterých není možné získat všechny potřebné informace. Podle STAMP se sociotechnický systém skládá z řídicích struktur a negativní události uvnitř těchto struktur mají dopad na bezpečnost systému. Řídicí struktura systému se skládá ze sítě řídících smyček, která je zobrazena na obrázku 7.



Obrázek 7 Řídící smyčka [17] (upraveno autorem)

Řídícím prvkem může být člověk nebo software. Řízeným procesem může být proces, obvykle technický, nebo nějaký jiný člověk v systému. Řídící prvek získává zpětnou vazbu (měřené proměnné) z řízeného procesu. Na základě zpětné vazby se řídící prvek rozhodne, jaký krok bude následovat a pomocí aktivních prvků řízení vyšle informace do řízeného procesu. Zpětná vazba významně ovlivňuje řídící prvky, protože je zásadním vstupem pro generování nových řídících akcí. Každý řídící prvek se skládá ze dvou částí: modelu procesu a řídícího algoritmu. Model procesu obsahuje informace o aktuálním stavu systému a jak může proces změnit stav systému. Řídící algoritmus je soubor pravidel pro řídící prvek, který popisuje, jakým způsobem má být proces řízen. Může to být buďto logika softwaru nebo vědomosti a informace, které člověk získal výcvikem či zkušenostmi.

STAMP dokáže odhalit selhání člověka i říct, proč k selhání došlo. Incidenty a nehody často vznikají, když model procesu používaný řídícím není vhodně aplikován na řízený proces nebo není poskytnuta žádná, nebo dostačující zpětná vazba nebo nejsou dostatečně zajištěny bezpečnostní opatření [17]. STAMP říká, že systém selhává na základě negativních událostí v kontrolních smyčkách. Dokáže analyzovat i systémy, ve kterých je více řídících prvků najednou. Více řídících prvků zároveň může znamenat kombinaci člověka i software jako řídící prvek v jednom systému. Tímto se vyznačují zejména systémy v reálném světě.

2.1.2 Metodika STPA

STPA je proaktivní analytická metoda, která je založena na modelu STAMP. Analyzuje potenciální příčiny nehod během vývoje, aby bylo možné eliminovat nebo kontrolovat nebezpečí. Kromě selhání komponent STPA předpokládá, že nehody mohou být způsobeny také nebezpečnými interakcemi komponent systému. Analýza může být aplikována už v ranném vývoji systému. Díky ní je možné odhalit požadavky na systém a jeho omezení již při vývoji systému. Tím pádem nebude nutné při jeho dokončení systém předělávat, což má pozitivní dopad na finanční náklady na vývoj systému. STPA poskytuje také funkční model, který je většinou náročné sestavit u komplexních systémů. Oproti tradičním metodám (založených na principech Safety-I) STPA odhalí navíc selhání způsobené softwarem či člověkem.

Čtyři hlavní kroky analýzy STPA jsou zobrazeny na obrázku 8 a jsou následující [18]:

1) Stanovit cíl analýzy.

   V prvním kroku analýzy je nutné stanovit cíl analýzy. Určení, k čemu analýza bude použita, pomůže analytikovi ujasnit si myšlenky. Následně bude jednodušší identifikovat systém, který bude rozebírán, a definovat jeho hranice či prostředí, ve kterém se nachází. Dále je v tomto kroku důležité identifikovat jaká nebezpečí se v systému mohou vyskytnout a k jakým ztrátám vedou. Následně se v tomto kroku určí omezení systému a případně jsou ponechána pouze ta nebezpečí, která má smysl rozebírat v dané analýze a ostatní mohou být zanedbána, jelikož se nachází mimo systém.

2) Namodelovat řídící strukturu systému.

   V druhém kroku má analytik za úkol namodelovat hierarchickou řídící strukturu systému. Řídící struktura je funkční model systému, což znamená, že se zobrazuje funkčními vztahy a funkčními interakcemi. Skládá se ze zpětnovazebních regulačních smyček, které jsou zobrazeny na obrázku 7. Řídící struktura obvykle začíná na velmi abstraktní úrovni a je postupně zpřesňována, aby zachytila více detailů o systému. V některých případech může pouhé nakreslení schématu řídící struktury se všemi definovanými prvky objasnit dříve neobjevené nedostatky.

   Model systému v STPA analýze má následující podobu. Jednotlivé řídící prvky systému jsou zobrazeny obdélníkovitými „boxy“. Řídící prvky jsou pod sebou

uspořádány hierarchicky. Směrem shora dolů směřují vazby, které jsou obvykle zobrazeny šipkami, od hierarchicky výše postavených prvků, k prvků, které jsou hierarchicky níže. Tyto vazby mají řídící funkci. Oproti tomu z hierarchicky níže postavených prvků vedou směrem zdola nahoru vazby, obvykle šipky, které předávají prvkům hierarchicky výš zpětnou vazbu potřebnou k řízení systému.

3) Identifikovat nebezpečnou řídící akci.

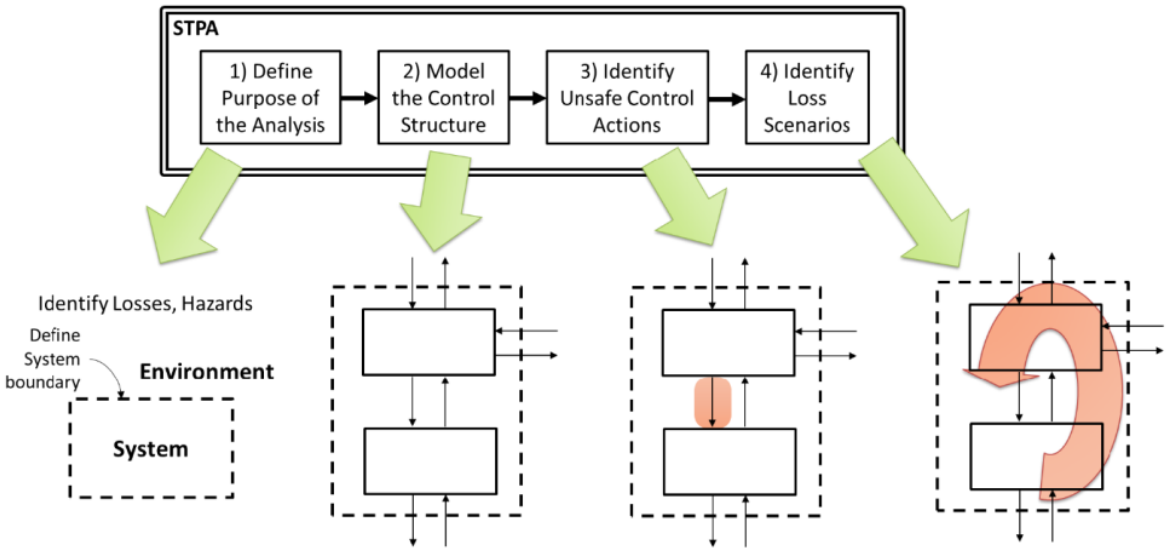
   Třetím krokem je analýza nebezpečných řídících akcí v řídící struktuře. Pomocí nich je možné zjistit, co vede vést ke ztrátám definovaným v prvním kroku. Tyto nebezpečné kontrolní akce jsou následně použity k definování funkčních požadavků a omezení pro systém. Řídící akce mohou být nebezpečné, pokud:

   a) řídící akce nebyla provedena pro bezpečný průběh procesu;
   b) provedená řídící akce nebyla vhodná pro bezpečný průběh procesu;
   c) řídící akce byla poskytnuta, ale příliš brzo nebo příliš pozdě, nebo ve špatném pořadí;
   d) řídící akce trvala déle, než bylo potřeba, nebo byla ukončena příliš brzy.

4) Identifikovat ztrátové scénáře.

   Posledním krokem analýzy je identifikovat důvody neboli ztrátové scénáře, které vedou ke ztrátovým událostem. Aktivace ztrátového scénáře začíná v řídící smyčce. Může být spuštěn nevhodným modelem procesu, nedostatečnou zpětnou vazbou, nevhodným řídícím algoritmem atd.

   Jakmile jsou scénáře identifikovány, je možné definovat další požadavky na systém, zmírnění, změny v řídící struktuře, vytváření doporučení a nových návrhových rozhodnutí (pokud se STPA používá během vývoje). Dále je díky nim možné upravit stávající návrhy, definovat nedostatky systému nebo například navrhnout testovací plány, pokud je STPA použita až po dokončení návrhu systému.



Obrázek 8 Základní čtyři kroky STPA [18]

2.2 FRAM

Základní principy metody FRAM profesor Erik Hollnagel definoval již v roce 2004. Profesor Hollnagel vyučuje na mnoha univerzitách po celé Evropě. Zabývá se zejména provozní bezpečností, dalším vývojem bezpečnostních modelů a teorií („resilience engineering“), vyšetřováním nehod a je autorem mnoha publikací [19].

Systémová metoda provozní bezpečnosti popisuje především vazby a závislosti mezi funkcemi systému. Byl vytvořen, stejně jako STPA, k popisu komplexních sociotechnických systémů, které v sobě zahrnují jak technické, tak organizační faktory, lidského činitele i tzv. „safety culture“. Z toho vyplývá, že je schopen pracovat se systémem jako s celkem a není potřeba jej rozdělovat na jednodušší části. Pomocí metody FRAM je možné definovat možné variability v systému a díky nim vyhodnotit rezonance v systému, které mohou vést k neočekávaným událostem, které mohou způsobovat nebezpečí, ale i k neočekávaně dobrým událostem. K tomu, aby variability a rezonance mohly být nalezeny, je důležité nejdříve správně identifikovat a detailně popsat funkce systému.

2.2.1 Čtyři principy

FRAM navrhuje, aby každodenní události a činnosti mohly být popsány z hlediska funkcí, aniž by bylo nutné předem definovat konkrétní vztahy, úrovně nebo struktury. Naopak říká, že chování funkcí je možné chápat následujícími čtyřmi principy [20]:

1) Selhání a úspěch vznikají stejným způsobem.

   To že výsledek těchto dvou událostí je rozdílný, ještě neznamená, že vznikají jiným způsobem. Jak selhání, tak úspěch jsou snahou organizací, skupin a jednotlivců se úspěšně přizpůsobit očekávaným i neočekávaným situacím. Každá reakce na konkrétní situaci je vykonána s úmyslem získání dobrého výsledku. Ale protože naše snaha přizpůsobit se situaci není úplně přesná, výsledky se mohou lišit od toho, co se očekávalo, nebo být dokonce zcela nepřijatelné. Zaměřováním se pouze na selhání v systému způsobuje, že nevíme, jak vznikají úspěchy. Předpokládá se, že úspěchy jsou docíleny dodržováním správných postupů, přitom se může stát, že úspěchy jsou výsledkem špatných reakcí a v budoucnu mohou způsobit neúspěch.

2) Výkonost sociotechnických systémů je proměnlivá, přizpůsobuje se prostředí.

   Tento princip poukazuje na to, že lidé ani organizace nejsou stroje a jejich výkony se přizpůsobují podmínkám, které je zrovna obklopují (čas, vybavení, informace, požadavky, únava atd.). Přizpůsobivost člověka je chápána jako pozitivní vlastnost.

3) Výstupy je potřeba popisovat jako emergentní.

   Protože většina výstupů, které zaznamenáme vznikly díky emergenci. Jakmile se objeví nečekaná událost, hledáme, jak událost vznikla například pomocí dekompozice a kauzality. V případě, kdy tímto způsobem příčina není odhalena, důvodem vzniku události je emergence. Právě proto, že předem není jasné, jak výstup vzniká, je potřeba je popisovat jako emergentní. Emergence se v systému mohla nacházet pouze v daný okamžik. FRAM říká, že variabilita jedné funkce není dostatečně velká k tomu, aby vedla k selhání. Ovšem kombinace variabilit dvou a více funkcí již mohou vést k neočekávaným událostem, ať už pozitivním nebo negativním.

4) Celý systém stojí na funkční rezonanci.

   Funkční rezonance je způsobena variabilitou výkonu v sociotechnickém systému, ke které může dojít, když se sejde více variabilit najednou. Vztahy mezi funkcemi jsou popsány právě pomocí rezonance podle toho, jak se vyvíjely v určité situaci. Systém může rezonovat s různě velkou amplitudou.

Funkční rezonance nabízí pohled na porozumění výstupů, které nejsou kauzální, tedy jsou emergentní.

2.2.2 Metoda FRAM

Metodou FRAM je možné analyzovat události, které se již staly (například letecké nehody), ale i systémy, u kterých je výhodné zjistit hrozící rizika dopředu ještě předtím, než se stanou. Tedy analýzu je možné provést reaktivně i proaktivně. V této práci je metoda FRAM využita proaktivně.

Metoda FRAM má čtyři základní kroky [20]:

1) Identifikace a popis funkcí systému.
   V prvním kroku analýzy je potřeba identifikovat hranice a funkce systému. Za funkci je považována činnost systému, která je vykonávaná v každodenním a normálním provozu systému. Funkce je nutné popsat co nejlépe a nejdetailněji. Protože funkce mají popisovat každodenní činnost systému je třeba funkci definovat tak, jak se opravdu děje, ne to, co je zamýšleno. Funkce tedy obvykle obsahuje sloveso. Pokud systém nemá žádnou funkci, kterou by činnost začínala, je možné začít jakoukoli funkcí, třeba tou nejdůležitější. Při definování dalších a dalších funkcí jsou postupně odhaleny všechny funkce, které zajišťují normální provoz systému.

   Každá funkce je definována šesti aspekty, které funkci popisují [20]:

   a) Vstup (input)
   Vstup je spouštěč funkce. Je to něco, co funkce přemění na výstup. Vstup může být něco hmotného, informace nebo energie. Vstup je vždy podstatné jméno nebo fráze, která obsahuje podstatné jméno. Jestliže je definován vstup jedné funkce, tento vstup musí být zároveň výstupem funkce jiné. Ne všechny funkce musí mít definovány vstup. Variabilita vstupu ovlivňuje variabilitu celé funkce.

   b) Výstup („output“)
   Výstup je výsledek funkce. To, co vznikne, jakmile je funkce dokončena. Výstup může být taktéž hmotný, informace nebo energie. Výstup je vždy podstatné jméno, nebo fráze, která obsahuje podstatné jméno. Definovaný výstup musí vstupovat do jiné funkce buďto jako vstup, podmínka, zdroj, řízení nebo čas. Jestliže je variabilita funkce nestálá, bude i její výstup nestálý. Tím přenese variabilitu na funkce, do kterých vstupuje jako vstup.

c) Podmínka („precondition“)

Podmínka musí být splněna, aby funkce mohla být provedena. Nicméně spouštěčem funkce je vstup. Podmínka musí být přítomna jen při spouštění funkce. Podmínka je výstupem jiné funkce. Může být definováno více podmínek pro jednu funkci. Podmínka také musí být definována podstatným jménem, nebo frází jej obsahující.

d) Zdroj („resource“)

Zdrojem funkce je něco, co je během provádění funkce spotřebováno. Podobným aspektem je realizační podmínka. Ta na rozdíl od zdroje není během provádění funkce spotřebována. Realizační podmínka musí být přítomna, po celou dobu realizace funkce. Podobně jako předchozí aspekty i zdroj může mít formu energie, informace, nebo hmotné věci. Na rozdíl od předchozích aspektů může mít také podobu softwaru, nástroje nebo lidské práci. Taktéž musí být definován podstatným jménem a musí být výstupem jiné funkce.

e) Řízení („control“)

Řízení je aspekt, který kontroluje nebo řídí danou funkci tak, aby bylo dosaženo zamýšleného výstupu. Řízení může představovat plán, pokyny, časový harmonogram nebo postup. Řízením mohou být i představy nadřízeného, spolupracovníků o provedené práci. Funkce musí mít řízení buďto vnější nebo vnitřní. Je popsáno podstatným jménem a je výstupem funkce jiné.

f) Čas („time“)

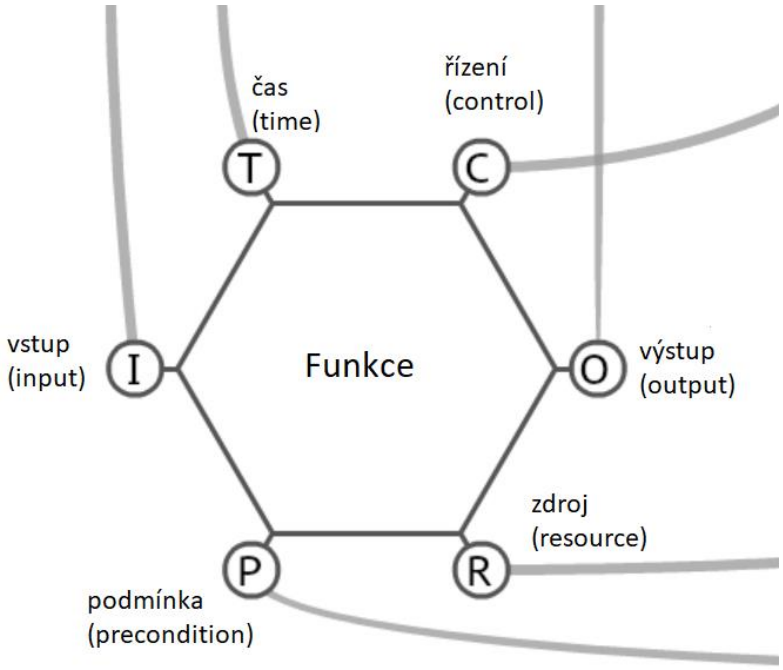
Představuje pořadí, v jakém má být funkce vykonána vzhledem k ostatním funkcím, nebo konkrétní čas, kdy má být funkce provedena. Může také představovat její trvání.

Ne všechny funkce musí mít definovány všech šest aspektů. Je potřeba definovat pouze ty, které vzhledem k popisované činnosti dávají smysl. Kolik aspektů funkce má závisí na povaze funkce a na zvolené rozlišovací úrovni. Funkce většinou mají definován alespoň vstup a výstup, ale ani to není podmínkou. Množství vstupů a výstupů funkce není omezeno. Jeden výstup může vést do několika funkcí jako vstup,

ale i několik výstupů může vést do několika funkcí jako vstup. Podobně to platí pro všechny ostatní aspekty

V případě, kdy funkce má pouze vstup nebo pouze výstup, jedná se tzv. „background“ funkci. Jakmile je na jedné funkci definován výstup a tento výstup vstupuje do jiné funkce v podobě aspektu, funkce se propojí a vzniká funkční toková vazba mezi dvěma funkcemi. Výstup definuje, jak se změní stav systému provedením dané funkce, zatímco ostatní aspekty popisují, co funkce potřebuje k jejímu provedení [20].

Taktéž model systému je vytvořen v prvním kroku analýzy. Funkce jsou zobrazeny jako hexagony, kde každý vrchol hexagonu představuje jeden z výše zmíněných aspektů. Hexagon funkce s jejími aspekty jsou zobrazeny na obrázku 9. Vazby mezi funkcemi tvoří propojení aspektů. Aspekty mohou být na hexagonu umístěny i v jiném pořadí.



Obrázek 9 Funkce a její aspekty

2) Identifikace variability.

Ve druhém kroku metody FRAM jsou identifikovány variability funkcí v systému. Protože FRAM analyzuje reálný stav systému, taktéž i variability, které zde mohou

vzniknout jsou reálné. Je třeba definovat okrajové hodnoty variability, aby bylo možné určit, když už je variabilita nadlimitní. Variabilita funkce je měřena na jejím výstupu a udává variabilitu samotné funkce.

Existují tři různé důvody, proč vzniká na výstupu funkce variabilita [20]:

a) variabilita výstupu má shodnou variabilitu jako funkce, tzv. vnitřní variabilita;
b) variabilita výstupu je ovlivněna okolním prostředím, respektive podmínkami, za kterých je funkce prováděna, tzv. vnější variabilita;
c) variabilita výstupu je způsobena vlivem předcházející funkce („upstream function“), která přenese variabilitu na aspekty následující funkce („downstream function“). Tento typ vazby je základem funkční rezonance a nazývá se funkční toková vazba.

Variabilita funkce může být způsobena i kombinací všech těchto důvodů.

Základem tohoto kroku je zjistit, jakým způsobem se variabilita projevuje. Jak variabilitu najít popisuje příručka od Erika Hollnagela [20]. Díky tomuto je možné variabilitu odhalit a zjistit, jak variabilita ovlivňuje další funkce. Variabilita je charakterizována na výstupu funkce z hlediska času a přesnosti. Z hlediska času se výstup může stát příliš brzy, na čas, příliš pozdě nebo vůbec. Z hlediska přesnosti může být výstup nepřesný přijatelný nebo přesný.

Existují tři druhy funkcí: technologická, lidská a organizační funkce. Jejich variabilita se mírně liší.

Technologické funkce jsou obvykle vykonávány stroji a technologií, například informační technologií. Variabilitu těchto funkcí FRAM považuje za poměrně stabilní, nevyznačují se žádnou výraznou variabilitou, ale i přes to zde variabilita může vznikat.

Lidské funkce vykonávají lidé nebo malé skupiny lidí. FRAM předpokládá, že variabilita těchto funkcí je vysoká, protože člověk reaguje poměrně rychle a v závislosti na události upravuje pružně své reakce. Jejich variabilita je závislá na mnoha faktorech.

Velké skupiny lidí vykonávají organizační funkce. Činnosti této skupiny mají určitý řád. I přesto, že jsou skupiny složeny z lidí, variabilita organizačních funkcí je za běžných podmínek pravděpodobně nízká a měla by taková skutečně být, aby organizaci umožnila působit jako regulátor variability. Variabilita organizačních funkcí se mění pomalu, ale výsledek má velký dopad.

3) Identifikace kombinací variabilit.

   V předposledním kroku jsou vyhledávány kombinace variabilit, čímž je sledována funkční rezonance. Negativní nebo pozitivní efekt mohou mít variability výstupu předcházející funkce na zkoumanou funkci. Aspekty sledované funkce taktéž ovlivňují působení na funkci. Obvykle hlediska „vůbec“ a „nepřesný“ z druhého kroku výrazně zvyšují variabilitu. Zatímco výstupy vykonané „na čas“ a „přesně“ velkou variabilitou nedisponují.

4) Návrh opatření, která snižují rezonanci.

   Pomocí předchozích kroků jsou odhalena problémová místa v systému, tedy místa, kde vzniká a kde se kombinuje negativní variabilita. V posledním kroku jsou navržena opatření, jak negativní variabilitě zabránit.

3 Aplikace metody STPA na provozní prostředí

Vzhledem k povaze systému U-space jsou ke zhodnocení bezpečnosti vybrány systémové metody. Pouze pomocí systémových metod je možné analyzovat tak komplexní systém jako je U-space jako celek. Protože od začátku zpracovávání této práce nebylo možné jasně určit, která systémová metoda je pro vybraný systém vhodnější, jsou zpracovány dvě systémové metody STPA a FRAM.

Cílem aplikování analýzy STPA je proaktivním způsobem zjistit, kde se v systému mohou nacházet ztrátové scénáře. Systém U-space je stále ve vývoji, proto je vhodné metodu aplikovat již teď. Pomocí ztrátových scénářů je identifikováno, jakým způsobem v systému může docházet ke ztrátovým událostem. Následně budou definovány požadavky na systém, které zamezí vznik ztrátových událostí.

3.1 Stanovení cíle analýzy

Cílem aplikování STPA analýzy na provozní prostředí bezpilotních systémů v U-space je ověření úrovně nastavené bezpečnosti.

Na začátku analyzování systému je nutné si stanovit, jaké hranice vybranému systému budou nastaveny. Do systému zahrnout pouze prvky, které mají zásadní význam v systému a nezabíhat do přílišných detailů. Na základě definovaných hranic jsou nalezeny možné ztráty („losses“). Za ztráty je možné považovat cokoli, co má pro prvky systému důležitou hodnotu. Ztráta může být například úmrtí člověka, poškození majetku, únik dat apod. V systému U-space jsou definovány následující ztráty:

- L1: Narušení vzdušného prostoru
- L2: Omezení ostatního provozu
- L3: Kolize s provozem s pilotem na palubě
- L4: Narušení bezpečnosti provozu
- L5: Ztráta dat registru
- L6: Ztráta spolupráce (s U-space airspace prvky, EASA, provozem, ...)
- L7: Majetková újma
- L8: Nemajetková újma

Následně jsou identifikována nebezpečí, která se mohou v systému vyskytnout. U všech nebezpečí jsou v závorce uvedeny odkazy na ztráty, které mohou způsobit. Nebezpečí jsou rozdělena do skupin, kde první skupina se týká samotného letu UAS, druhá skupina leteckých

nehod a třetí skupina se týká autorit a ostatních prvků U-space. Byla identifikována tato nebezpečí:

- H1.1: UAS bude létat v pro něj nepovoleném vzdušném prostoru (L1, L2, L3, L4, L7, L8)
- H1.2: UAS omezí ostatní účastníky provozu (L1, L2, L4)
- H1.3: UAS ohrozí ostatní účastníky provozu (L1, L2, L3, L4, L7, L8)
- H1.4: UAS naruší provoz neřízeného letiště (L1, L2, L3, L4, L7, L8)
- H1.5: UAS naruší provoz řízeného letiště (L1, L2, L3, L4, L7, L8)

- H2.1: Letecká nehoda s letadly s pilotem na palubě (L3, L4, L7, L8)
- H2.2: Letecká nehoda s UAS (L4, L7, L8)

- H3.1: USSP neplní své závazky (L4, L6)
- H3.2: USSP neposkytuje data v rámci smlouvy (L4, L6)
- H3.3: ÚCL poskytuje chybná data CIS (L4)
- H3.4: Dojde ke ztrátě dat registru (L5)

H1.1: nepovoleným vzdušným prostorem pro UAS je myšlen prostor, pro který provozovatel UAS nezískal povolení k letu, případně další potřebná povolení.

H1.2 a H1.3: ostatními účastníky provozu jsou myšleny jak ostatní bezpilotní systémy v daném vzdušném prostoru, tak letadla s pilotem na palubě.

H1.4 a H1.5: pokud by UAS narušilo provoz řízeného či neřízeného letiště, vyplývá z toho, že o provozu UAS letiště nebylo informováno a provoz s největší pravděpodobností není v souladu s legislativou. Kdyby UAS narušilo provoz letiště, mohlo by dojít k odklánění letů na jiná letiště, případně by byla aplikována jiná opatření.

H2.1 a H2.2: příkladem letecké nehody je střet UAS s letadlem s pilotem na palubě nebo jiným UAS.

H3.1: za neplnění závazků USSP je například neplnění legislativních požadavků.

H3.2: neposkytováním dat podle smluv je myšleno nezajištění sdílení dat mezi USSP a ostatními prvky U-space dle smluv.

H3.3: data, která ÚCL poskytuje CIS jsou data o geo-zónách a registru, tedy databázi registrovaných provozovatelů a pilotů.

H3.4: ztrátou dat z registru je myšlena ztráta dat z databáze registrovaných provozovatelů a pilotů.

V závěru prvního kroku jsou definována omezení na úrovni systému („system-level constraints“). Ta musí zajistit, že nedojde k výše uvedeným nebezpečím. Omezení jsou stejně jako nebezpečí rozdělena do skupin. Čísla uvedená u každého omezení se shodují s číslem nebezpečí, pro která jsou omezení vytvořena.

- C1.1 UAS nesmí létat v pro něj nepovoleném vzdušném prostoru
- C1.2 UAS nesmí omezit ostatní účastníky provozu
- C1.3 UAS nesmí ohrozit ostatní účastníky provozu
- C1.4 UAS nesmí narušit provoz neřízeného letiště
- C1.5 UAS nesmí narušit provoz řízeného letiště

- C2.1 UAS nesmí kolidovat ve vzduchu s letadly s pilotem na palubě
- C2.2 UAS nesmí kolidovat ve vzduchu s UAS

- C3.1 USSP musí plnit své závazky
- C3.2 USSP musí poskytovat dává v rámci smlouvy
- C3.3 ÚCL musí poskytovat správná data CIS
- C3.4 Nesmí dojít ke ztrátě dat registru

3.2 Modelování řídící struktury U-space

Řídící struktura systému U-space byla vytvořena na základě normálního fungování systému U-space. V řídící struktuře jsou obsaženy řídící prvky, které jsou v systému stěžejní. Při vytváření modelu jsou definovány tyto řídící prvky, které jsou vzájemně propojeny v hierarchické struktuře:

- EASA
- MD
- ÚCL
- CIS

- Poskytovatel U-space služeb
- FIS (AFIS)
- ANS ČR
- Neřízený provoz s pilotem na palubě
- Řízený provoz s pilotem na palubě
- Provozovatel
- Pilot
- Pozorovatel
- Operátor payloadu
- Stanice dálkově řídícího pilota
- UA
- Poskytovatel výcviku
- ÚZPLN
- Výrobce UAS

Tyto řídící prvky zajišťují běžný chod systému U-space. Každý z řídících prvků má v systému svou roli a odpovědnost podle nastavených postupů systému. Každý prvek se zodpovídá prvkům nad ním a má autoritu nad prvky pod ním.

V modelu jsou vybrané řídící prvky podbarveny buďto zelenou, žlutou, červenou nebo oranžovou barvou. Řídící prvky podbarveny zelenou barvou jsou prvky zastupující stát ČR. Jedná s konktrétně o MD (ministerstvo dopravy) a ÚCL (Úřad pro civilní letectví). Dále prvky podbarveny žlutou barvou jsou U-space airspace prvky, tedy prvky, které přímo zajišťují provoz U-space. Následují řídící prvky podbarveny červenou barvou. Tyto prvky jsou přímou součástí provozu UAS. Jako poslední jsou prvky podbarveny oranžovou barvou, které znázorňují samotné UAS. Řídící struktura je uvedena v příloze 1. K namodelování řídící struktury v analýze STPA byl využit program yEd Graph Editor, který je na internetu volně dostupný ke stažení.

3.2.1 Charakteristika jednotlivých řídících prvků

Většina řídících prvků, které přímo zajišťují fungování U-space jsou popsány výše v této práci v kapitolách 1.2.2. Služby U-space a 1.2.3. Prvky U-space. Ty, jejichž činnost zatím nebyla zmíněna, jsou popsány v této podkapitole.

EASA

Agentura Evropské unie pro bezpečnost letectví („European Aviation Safety Agency“) je agentura Evropské unie, která zajišťuje bezpečnost a ochranu životního prostředí v oblasti civilního letectví v Evropě. EASA má na starosti tvorbu předpisů a certifikaci, vývoj jednotného trhu EU v oblasti letectví, typové osvědčení letadel a komponentů, schvalování společností, které zajišťují konstrukci, výrobu a údržbu leteckých výrobků, prosazování evropských a světových bezpečnostních norem atd. Zároveň EASA zaštiťuje evropské úřady pro civilní letectví, provozovatele letecké dopravy a letecké společnosti, obchodní a soukromé piloty, letiště, schválené výcvikové organizace atd [21]. V systému U-space má na starosti hlavně tvorbu jednotné legislativy, certifikaci a dohlížení na dodržování stanovených pravidel. Jakožto nejvyšší orgán zajišťující bezpečnost letectví a jako hierarchicky nejvýše postavený řídící prvek je zodpovědný za nastavení provozní bezpečnosti v celé EU.

MD (Ministerstvo dopravy)

Ministerstvo dopravy ČR je úřední orgán státní správy zodpovědný za záležitosti týkající se dopravy. Jakožto nejvyšší orgán zodpovědný za letectví v ČR je taktéž zodpovědný za definování provozní bezpečnosti na území ČR. Je zodpovědný za tvorbu zákona o civilním letectví a implementování Evropských pravidel, což platí i pro U-space.

ÚCL (Úřad pro civilní letectví)

Úřad pro civilní letectví spadá jako organizační složka státu pod ministerstvo dopravy. Má na starosti dohled nad civilním letectvím v ČR, vydává certifikace letadel, leteckých technických zařízení, pilotů apod. V U-space zajišťuje dozor nad civilním letectvím, certifikaci zapojených subjektů, zajišťuje registrace provozovatelů a pilotů

Řízený provoz s pilotem na palubě

Řízený provoz s pilotem na palubě je provoz letadel v řízeném vzdušném prostoru. Pohybují se tedy v prostoru, kde je letadlům poskytována služba řízení letového provozu.

Neřízený provoz s pilotem na palubě

Neřízený provoz s pilotem na palubě se nachází v neřízeném vzdušném prostoru. V těch je povinnost separace mezi letadly přenechána na posádce letadla.

Pilot

Pilot je osoba pověřená provozovatelem UAS, která je zodpovědná za bezpečné provedení letu. Pilot zodpovídá za stav UAS, komunikaci s ostatními členy posádky, jako například s operátorem „payloadu“ nebo pozorovatelem. Úloha pilota je i ovládat stanici dálkově řídícího pilota.

Pozorovatel

Pozorovatel je osoba pověřená provozovatelem bezpilotního systému, která má za úkol asistovat pilotovi a udržovat oční kontakt s letícím bezpilotním letadlem. Pilot a pozorovatel spolu samozřejmě musí komunikovat.

Operátor „payloadu“

Operátor „payloadu“ neboli užitečného zatížení (nákladu) je osoba taktéž pověřená provozovatelem UAS a jeho zodpovědností je upevnit a zajistit „payload“ na bezpilotní letadlo tak, aby těžiště bylo co nejblíže letadlu a „payload“ během letu nespadl na zem, nebo nenarušoval průběh letu výkyvy apod.

Stanice dálkově řídícího pilota

Stanice dálkově řídícího pilota slouží k ovládání bezpilotního letadla, k zobrazování informací o letu, informací z kamery atd. Zařízení taktéž přijímá a zobrazuje data poskytovaná službami U-space.

UA

UA („Unmanned Aircraft“) neboli bezpilotní letadlo slouží k vykonání provozu. Je ovládáno pilotem pomocí stanice dálkově řídícího pilota. Většinou nese užitečné zatížení („payload“).

Poskytovatel výcviku

Společnost, či osoba, která je ÚCL certifikována k poskytování výcviku pilotům UAS a ostatním členům posádky.

ÚZPLN

Ústav pro odborné zjišťování příčin leteckých nehod je složka státu, která má na starost vyšetřování příčin vážných incidentů a leteckých nehod. Cílem vyšetřování není určit viníka události, nýbrž odhalit, co ke způsobení události vedlo. Po ukončení šetření nehody nebo

incidentu ÚZPLN vydá bezpečnostní doporučení, kde stanoví, jak je možné zabránit opakování události.

Výrobce UAS

Výrobce bezpilotních systémů je nejčastěji společnost, která komerčně vyrábí a následně poskytuje na trh bezpilotní systémy. Zajišťuje reklamaci výrobku a má možnost nechat svůj výrobek certifikovat, respektive zažádat o provedení „design verification“ agenturou EASA.

3.2.2 Charakteristika ostatních prvků

V systému se vyskytuje i prvek, který nelze považovat za řídící prvek. Je to vstup do procesu, a to Registr ČR.

Registr ČR

Registr slouží jako databáze registrovaných provozovatelů a dálkově řídících pilotů v České republice. Z něj čerpá informace například společná informační služba, která předává tato data dalším prvkům U-space, které na tato data mají oprávnění.

3.2.3 Popis vybraných řídící akcí a zpětných vazeb

Jelikož model obsahuje značné množství prvků, řídících akcí a zpětných vazeb, jsou v této podkapitole popsány pouze některé z nich a to ty, které nejvíce ovlivňují nebo jsou nejvíce zapojeny do fungování U-space.

EASA – MD

Vzájemná komunikace mezi agenturou EASA a Ministerstvem dopravy (MD) je klíčová pro zajištění legislativy a pravidel platných v každém členském státě, stejně tak i v ČR. Od legislativy definované agenturou EASA se odvíjí úroveň bezpečnosti provozu v systému U-space. Ministerstvo dopravy následně předává agentuře EASA zprávy postupu implementace EU předpisů a informace týkající se odvolání proti rozhodnutí MD.

MD – ÚCL

Vazba mezi Ministerstvem dopravy a Úřadem pro civilní letectví je na úrovni prvků zastupujících stát. Ministerstvo dopravy má povinnost tvořit leteckou legislativu na území ČR a zároveň implementovat předpisy platné pro celou EU. Úřad pro civilní letectví následně podává zpětnou vazbu Ministerstvu dopravy. Informace, které jsou předávány jsou následující: komentáře k legislativě, reportování postupu implementace, informace o odebrání certifikace a odvolání proti rozhodnutím ÚCL.

ÚCL – CIS

Řídící akce mezi Úřadem pro civilní letectví a CIS (společná informační služba) je zejména stanovení pravidel pro poskytování CIS. Dále ÚCL musí předat CIS data potřebná k tomu, aby služba mohla být zajištěna, tedy data o registracích a geo-zónách. CIS následně předá ÚCL informace o problémech týkajících se provozních situací a zároveň musí plnit pravidla.

ÚCL – Poskytovatel U-space služeb

ÚCL v prvé řadě certifikuje poskytovatele U-space služeb. Bez certifikace by nemohl provádět svou činnost. ÚCL také definuje za jakých podmínek a jakým způsobem může poskytovatel U-space služeb služby poskytovat. U-space služby jsou základem systému U-space. Bez nich by společný provoz bezpilotních letadel a letadel s pilotem na palubě ve společném prostoru nebyl možný. Poskytovatel služeb U-space musí dodržovat stanovená pravidla a být schopen to kdykoli dokázat.

ÚCL – Provozovatel

Spojení těchto dvou řídících prvků je další významná řídící smyčka. Řídících akcí je v této vazbě rovnou několik. První z nich je stanovení pravidel pro umožnění provozu. Dále ÚCL stanoví zodpovědnosti provozovatele. V neposlední řadě dohlíží, zda provozovatel dodržuje stanovená pravidla. Při provozu UAS může ÚCL přijít na místo provozu a zkontrolovat, jestli provoz probíhá dle pravidel a vydaných oprávnění. Provozovatel následně po skončení provozu informuje ÚCL o tom, jak let probíhal, a musí zajistit provoz dle stanovených pravidel.

ÚCL – Pilot

ÚCL má vůči pilotovi dvě řídící akce. Jednak pilotovi stanovuje pravidla pilotování, a také stanovuje, jaké zodpovědnosti má pilot během provozu na starosti. Pilot se ÚCL zodpovídá létáním dle pravidel.

Provozovatel – Pilot

Poslední vazbou je vazba provozovatel a pilot. Provozovatel musí pilotovi poskytnout instrukce k dosažení mise, které budou obsahovat provozní příručku, aby pilot věděl, jaké provozní postupy má provozovatel nastaveny. Dále provozovatel stanoví místo provozu a stanoví cíl mise. Provozovatel je taktéž zodpovědný za aktualizaci dat v bezpilotním letadle (UA). Pilot provozovateli předá potvrzení o tom, že pochopil pravidla provozu a ostatní informace. Pilot taktéž může provozovateli navrhovat úpravy mise. Předposlední zpětná vazba je v této vazbě

poskytnutí nasbíraných dat. Nasbíraná data mohou být například snímky, data ze senzorů apod. Pilot je také zodpovědný provozovateli za splnění mise.

3.3 Identifikace nebezpečných řídících akcí

V dalším kroku analýzy STPA jsou identifikovány nebezpečné řídící akce („Unsafe Control Actions“ neboli UCA). Nebezpečná řídící akce je akce, která v určitém kontextu a v nejhorším možném případě povede k nebezpečí. STPA definuje 4 situace, kdy řídící akce může být nebezpečná [18]:

a) neprovedení řídící akce vede k nebezpečí;
b) provedení řídící akce vede k nebezpečí;
c) provedení potenciálně bezpečné řídící akce, ale příliš brzy, pozdě nebo ve špatném pořadí vede k nebezpečí;
d) řídící akce tvá příliš dlouho nebo je přerušena příliš brzy vede k nebezpečí.

V některých případech, jak je znázorněno v tabulce 2, ne všechny řídící akce dávají smysl vzhledem k dané situaci. V těchto případech je políčko tabulky proškrtnuto. Každá nebezpečná řídící akce vede k nebezpečí. Nebezpečí, která mohou vzniknout v tomto systému byla definována v prvním kroku analýzy. Vzhledem k velkému množství identifikovaných nebezpečných řídících akcí v systému je v následující části popsána pouze jedna vybraná. Přehled všech nebezpečných řídících akcí je uveden v příloze 2.

Tabulka 2 Nebezpečná řídící akce

ID	***Řídící akce***	***Neprovedení řídící akce vede k nebezpečí***	***Provedení řídící akce vede k nebezpeční***	***Příliš brzy, pozdě, ve špatném pořadí***	***Trvá příliš dlouho, přerušena příliš brzy***	***Způsobená nebezpečí***
UCA-1.1	pokyny k zajištění dozoru nad impementací pravidel	neposkytne ÚCL pokyny k zajištění dozoru	poskytne neúplné pokyny k zajištění dozoru nad implementací pravidel	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2

3.3.1 Omezení řídícího prvku

Pro každou identifikovanou nebezpečnou řídící akci je potřeba definovat omezení řídícího prvku. Omezení řídícího prvku („constrain“ zkráceně c) říká, jakým způsobem se řídící prvek musí chovat, aby nedošlo k nebezpečné řídící akci. V této části textu jsou popsána omezení řídícího prvku související s řídící akcí, ke které byly definovány nebezpečné řídící akce

v předchozí podkapitole, viz tabulka 3. Přehled všech omezení řídících prvků je uveden v příloze 3.

Tabulka 3 Omezení řídícího prvku

ID	***Řídící akce***	***Omezení řídícího prvku 1***	***Omezení řídícího prvku 2***	***Omezení řídícího prvku 3***	***Omezení řídícího prvku 4***
C-1.2	pokyny k zajištění dozoru nad impementací pravidel	musí poskytnout ÚCL pokyny k zajištění dozoru	musí poskytnout kompletní pokyny k zajištění dozoru nad implementací pravidel	-	-

3.4 Identifikace ztrátových scénářů

V poslední části STPA analýzy jsou nalezeny ztrátové scénáře. Ztrátové scénáře popisují faktory, které mohou vést k nebezpečným řídícím akcím a k nebezpečím [18]. STPA definuje dvě možnosti, jak může ke ztrátovým scénářům dojít [18]:

a) nebezpečným chováním řídícího prvku;
b) nedostatečnou zpětnou vazbou.

V tabulce 4 jsou uvedeny ztrátové scénáře související s řídící akcí, která je zmíněna v předchozích podkapitolách. Zároveň jsou v posledním sloupci tabulky uvedeny požadavky na systém, které musí být splněny, aby nedošlo ke ztrátovým scénářům. Přehled všech ztrátových scénářů a požadavků na systém je uveden v příloze 4.

Tabulka 4 Ztrátové scénáře a požadavky na systém

ID	***UCA ref.***	***Nebezpečná řídící akce***	***Ztrátový scénář***	***Požadavky na systém***
Scenario 1.2	UCA-1.2	EASA neposkytne ÚCL pokyny k zajištění dozoru, nebo poskytne neúplné pokyny k zajištění dozoru nad implementací pravidel, protože...	– zajištění dozoru není definováno, nebo – neexistuje smlouva mezi EASA a ÚCL, nebo – pravidla pro zajištění dozoru jsou stará a nepostihují nový provoz, nebo – EASA neví, jak zajišťovat dozor	–EASA musí zajistit, že dozor nad provozem je definován –EASA musí zajistit, že je uzavřena smlouva mezi EASA a ÚCL – EASA musí zajistit aktuálnost pravidel pro vykonávání dozoru, aby postihovaly provoz –EASA musí vědět, jak dělat dozor

4 Aplikace metody FRAM na provozní prostředí

Druhou systémovou metodou aplikovanou na systém U-space je metoda FRAM. Cílem metody FRAM je odhalit pomocí variabilit vznik nežádoucí rezonance v systému, jejichž výsledkem mohou být nebezpečné neočekáváné situace, které mohou vést k nehodám.

4.1 Identifikace a popis funkcí systému

Na začátku aplikace metody FRAM je nutné určit rozlišovací úroveň systému. Je možné na systém nahlížet v různých úrovních detailu. Tyto úrovně jsou určeny pomocí tzv. abstrakční hierarchie, která pomáhá zjednodušit procesy. Některé procesy můžeme zařadit pod jiné „nadřazené“. Z komplexního procesu je vytvořen jednodušší proces. Abstrakční hierarchie má čtyři základní abstrakční úrovně: funkční účel, obecná funkce, fyzická funkce a fyzická forma [22]. Úroveň popisu funkčního účelu sleduje funkční efekt systému na své prostředí. Oproti tomu poslední úroveň fyzická forma se zaměřuje na popis těch největších detailů v systému a je zaměřená na fyzickou formu jednotlivých součástí systému. Další součástí abstrakční hierarchie jsou agenti, kteří představují skupiny funkcí v systému se stejným cílem. Agenty mohou být organizace, jednotlivci, technické vybavení apod.

Vybranými agenty pro systém U-space jsou EASA, ÚCL, provozovatel, pilot, poskytovatel služeb U-space, CIS, ATSP (ATC, FIS, AFIS) a ANSP. Bližší popis těchto agentů je možné nalézt výše v této práci.

Rozlišovací úroveň vybraná pro účely této práce je úroveň obecné funkce systému. Funkce, které byly pro tuto úroveň definovány jsou popsány dále. Aby bylo možné rozlišit mezi funkcemi a aspekty, funkce budou vždy začínat velkým písmenem. Celkem bylo na úrovni obecných funkcí definováno 20 funkcí. Jednotlivé funkce přiřazené k jejich agentům jsou vypsány v tabulce 5.

Tabulka 5 Agenti a jejich funkce

Agent	Funkce
EASA	Stanovit pravidla provozu Stanovit pravidla certifikace Stanovit pravidla pro poskytování U-space služeb
ÚCL	Stanovit pravidla pro registraci provozovatele Stanovit pravidla pro certifikaci zapojeného subjektu Stanovit pravidla pro poskytování U-space služeb v ČR
Provozovatel	Splnit registraci provozovatele Stanovit provozní postupy
Poskytovatel U-space služeb	Získat certifikaci poskytovatele U-space služeb Vyhodnotit přijímaná data Poskytovat specifickou U-space službu dle stanovených pravidel
Pilot	Získat certifikaci dálkově řídícího pilota Řídit se provozními postupy provozovatele Splnit teoretický a praktický výcvik posádky
CIS	Získat certifikaci CIS poskytovatele Sběr a dodání dat
ATSP (FIS, AFIS)	Získat certifikaci ATSP Poskytovat data o provozu letadel s pilotem na palubě
ANSP	Získat certifikaci ANSP Poskytovat data o poloze letadel s pilotem na palubě

4.1.1 Popis funkcí systému

První funkcí je *Stanovit pravidla provozu*. Tuto funkci lze považovat za výchozí bod systému. K tomu, aby mohl být zabezpečen vývoj U-space, musí nejdříve EASA definovat pravidla provozu v U-space., Musí tedy být vytvořeny předpisy, kterými se budou výrobci, uživatelé a příslušné úřady řídit. Na tuto funkci navazuje funkce *Stanovit pravidla certifikace.* Vzhledem k tomu, že prostředky a technologie, které budou využity v U-space musí splňovat vysoké nároky na jejich kvalitu, musí být veškeré technické vybavení certifikováno (např. bezpilotní letadla, software na sdílení dat, apod.). Certifikace se netýká pouze technického vybavení. Certifikovány budou muset být také veškeré zapojené osoby a subjekty, jako například dálkově řídící piloti nebo poskytovatelé služeb U-space. V neposlední řadě je nutné *Stanovit pravidla pro poskytování U-space služeb.* Jak již bylo zmíněno dříve, právě U-space služby dělají U-space tak výjimečným a bezpečným vzdušným prostorem, proto je nutné definovat pravidla, jak mají být služby poskytovány.

Pro všechny provozovatele, kteří chtějí létat se svými bezpilotními prostředky ve vzdušných prostorech U-space je potřeba *Stanovit pravidla pro registraci provozovatele.* Definovat tato pravidla a umožnit tím provozovatelům UAS létat v U-space je jedna z klíčových funkcí systému. ÚCL má dále na starost *Stanovit pravidla pro certifikaci zapojeného subjektu*. Na základě pravidel, které stanoví EASA, musí ČR stanovit svá pravidla. Tato pravidla musí být stejně přísná jako pravidla definovaná agenturou EASA nebo přísnější. To samé platí pro funkci *Stanovit pravidla pro poskytování U-space služeb v ČR.*

Provozovatelé musí *Splnit povinnosti provozovatele* k tomu, aby mohli využívat vzdušný prostor U-space. Splněním povinností je myšlena například registrace provozovatele nebo definování provozních postupů. Dále je nutné *Stanovit cíl mise.* To je nutné k tomu, aby poskytovatelé U-space služby věděli, jaká data provozovateli poskytovat.

Jak již bylo zmíněno výše, všechny subjekty zapojené do provozu v U-space musí být certifikovány, proto USSP musí *Získat certifikaci poskytovatele U-space služeb.* K tomu, aby mohl data poskytovat, musí nejdříve *Vyhodnotit přijímaná data.* Tím je myšleno vyhodnotit, zdali jsou data kompletní, aktuální, nepoškozená atd. V neposlední řadě musí *Poskytovat specifickou U-space službu dle stanovených pravidel*, aby mohla být zajištěna bezpečnost provozu v U-space.

Pilot, jakožto osoba zapojená do provozu, musí *Získat certifikaci dálkově řídícího pilota*. Typ certifikace se liší na základě druhu provozu a typu UAS, se kterým je provoz zamýšlen. Aby mohl provoz postupovat dle plánu, pilotovou povinností je *Řídit se provozními postupy provozovatele*. Tím se zamezí vzniku neočekávaných či nebezpečných situací, které by mohly vzniknou, pokud by se pilot provozními postupy neřídil. *Splnit teoretický a praktický výcvik posádky* je další předpoklad k bezpečnému provozu. Čím více zkušeností a znalostí osoby zapojené do provozu mají, tím větší bezpečnost provozu může být zajištěna. Povinností pilota je také *Seznámit se s cílem mise*. Díky tomu bude mít jasno, jak bude provoz probíhat a jakou techniku bude potřeba k letu zajistit.

Všichni tři zbývající agenti (subjekty) musí být certifikováni. Pro poskytovatele společné informační služby platí, že musí *Získat certifikaci CIS poskytovatele.* Důležitá úloha CIS je taktéž *Sběr a dodání dat.* Jelikož CIS má na starosti výměnu dat mezi ATSP, členským státem a USSP, musí zajistit sběr dat do své databáze a následné dodání dat ostatním subjektům.

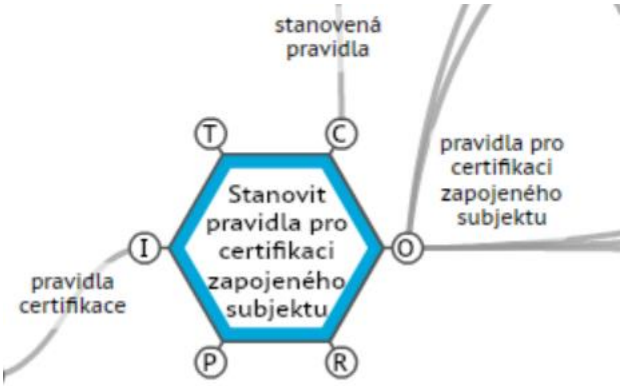
Získat certifikaci ATSP je nutnou podmínkou pro poskytování provozních informací nejen pro U-space, ale i pro ostatní druhy vzdušných prostorů. *Poskytovat data o provozu letadel*

s pilotem na palubě je důležitá funkce pro možnost sdílení prostoru U-space s letadly s pilotem na palubě. Na jejich základě bude možné sledovat a přizpůsobovat trasu všech letadel (s pilotem na palubě i bezpilotních) v U-space. Obdobným způsobem lze popsat funkce *Získat certifikaci ANSP* a *Poskytovat data o poloze letadel s pilotem na palubě*, jen se budou vztahovat na ANSP.

4.1.2 Aspekty funkcí

Každá funkce metody FRAM má definovány aspekty. Druhy aspektů jsou popsány v kapitole 2.2.2 Metodika FRAM. Vzhledem k množství definovaných aspektů bude následovat popis aspektů jedné vybrané funkce.

Funkce *Stanovit pravidla pro certifikaci zapojeného subjektu* má definovány tři aspekty a to vstup, výstup a řízení. Tato funkce je „foreground" funkcí, což znamená, že má definovaných více aspektů, nejen vstup nebo výstup. Vstupem této funkce jsou *pravidla certifikace,* což znamená, že k tomu, aby funkce *Stanovit pravidla pro certifikaci zapojeného subjektu* mohla být definována, musí být nejdříve definována *pravidla certifikace*, která jsou výstupem funkce *Stanovit pravidla certifikace.* Dalším aspektem je výstup funkce, a to *pravidla pro certifikaci zapojeného subjektu.* Jakmile je funkce dokončena, pravidla jsou definována. Tento aspekt, dále vstupuje do dalších funkcí v podobě jiných aspektů. Posledním aspektem je aspekt řízení *stanovená pravidla.* Podle *stanovených pravidel* jsou *stanovena pravidla pro certifikaci zapojeného subjektu*. Z tohoto důvodu je tento aspekt řídícím. Na obrázku 10 je znázorněna funkce *Stanovit pravidla pro certifikaci zapojeného subjektu* s jejími aspekty.



Obrázek 10 Funkce Stanovit pravidla pro certifikaci zapojeného subjektu s jejími aspekty

Jednotlivé funkce zde mají podobu hexagonu, jak je možné vidět na obrázku 10 a zároveň pomocí programu FRAM Model Vizualizer je možné vytvořit (díky definování aspektů) funkční tokové vazby. Kompletní podoba modelu FRAM je součástí přílohy 5. Kompletní model systému U-space je vytvořen pomocí programu FRAM Model Vizualizer (FMV). Ten je volně dostupný ke stažení na webových stránkách https://zerprize.co.nz/home/FRAM.

Vzhledem ke složitosti modelu a velkého počtu funkcí, aspektů a tokových vazeb je součástí přílohy 5 taktéž tabulka obsahující vypsané všechny funkce a jejich aspekty. Z této formy modelu nejsou jasně zřejmé funkční tokové vazby, nicméně je přehlednější. Protože nebyly definovány žádné aspekty času a zdroje, tyto aspekty v tabulce v příloze 5 nejsou uvedeny.

4.2 Identifikace variability

Identifikace variability funkcí vede k umožnění identifikace možných problémů v systému U-space. Prvním krokem k určení variability funkce je určení jejího typu. Funkce mohou být buďto technické, organizační nebo lidské. Druh funkce určuje, kdo nebo co vykoná danou funkci. Variabilitu v systému je možné definovat na základě dvou hledisek, a to hlediska času a přesnosti. Vzhledem k tomu, že je pomocí metody FRAM, zjišťován možný výskyt nebezpečí v systému proaktivně, tedy není rozebírána konkrétní událost, která již proběhla, není možné využít FMV k nalezení variability. Z tohoto důvodu byla vytvořena tabulka, která je součástí přílohy 6.

U určování variability je nutné se zamyslet, zdali je daná variabilita v tomto světě reálná (pokud není, je v tabulce v příloze 6 označena proškrtnutím políčka), a zdali by byla vnímána pozitivně, či negativně. Vzhledem k nastavenému cíli metody FRAM jsou zkoumány pouze negativní variability systému U-space.

V tabulce 6 jsou uvedeny variability funkce *Stanovit pravidla pro certifikaci zapojeného subjektu.* Typ této funkce je organizační, protože je vykonávána velkou skupinou lidí (ÚCL). Výstupem této funkce jsou *pravidla pro certifikaci zapojeného subjektu.* Pokud by pravidla byla stanovena příliš brzy, nemělo by to žádný negativní dopad na systém. V případě, kdy by pravidla byla stanovena na čas, taktéž by tento fakt neměl negativní vliv na systém. Stanovení pravidel příliš pozdě v tomto systému nedává smysl. Nejprve jsou pravidla stanovena, až poté jsou zavedeny další postupy. Dokud nebudou *Stanovena pravidla pro certifikaci zapojeného subjektu*, není možné certifikovat zapojený subjekt. Ovšem pokud by pravidla nebyla definována vůbec, pak už by to negativně systém ovlivnilo. Zapojené subjekty by nemohly být certifikovány, což by vedlo k nemožnosti provozu U-space, protože subjekty zde musí být

certifikovány. Nepřesně, nebo přijatelně stanovená pravidla by také vytvářela negativní variabilitu v systému. Pravidla musí být stanovena přesně, aby nebyl možný jejich špatný výklad.

Tabulka 6 Variabilita funkce Stanovit pravidla pro certifikaci zapojeného subjektu

			Čas				Přesnost		
Funkce	***Typ funkce***	***Výstup***	***příliš brzy***	***na čas***	***příliš pozdě***	***vůbec***	***nepřesné***	***přijatelné***	***přesné***
Stanovit pravidla pro certifikaci zapojeného subjektu	organizační	pravidla pro certifikaci zapojeného subjektu			-	negativní	negativní	negativní	

4.3 Identifikace kombinací variabilit

Třetím krokem metody FRAM je identifikace možné rezonance. Rezonance vzniká jako kombinace minimálně dvou potkávajících se variabilit. Existuje několik možností, jak rezonanci v systému odhalit. První z těchto možností je ta, kdy funkce, která má největší počet vstupů, může být nejvíce náchylná na rezonanci. Tato funkce bude kombinovat všechny variability, které do ní vstupují. Druhou možností, kde se může vyskytovat variabilita jsou funkce, které mají před sebou velký počet „upstream“ funkcí. Pokud by byly variability všech předcházejících funkcí kombinovány, došlo by tak k identifikaci rezonance. Zajímavé jsou ty kombinace variabilit, které by způsobily negativní rezonanci, tedy nejhorší dopad na fungování systému. Negativní rezonancí je vždy incident nebo nehoda. Jakmile jsou všechny možné rezonance odhaleny, jsou popsány scénáře, co by vedlo k narušení bezpečnosti a jakým způsobem.

4.3.1 První kombinace variabilit

V systému U-space na zvolené abstrakční úrovni byly identifikovány tři funkce s významnou variabilitou. První z těchto funkcí je funkce *Řídit se provozními postupy provozovatele.* Důvodem významné variability je velké množství aspektů vstupujících do funkce. Prvním vstupem jsou *provozní postupy*. Provozovatel musí definovat *provozní postupy*, aby personál zapojený do provozu věděl, jakým způsobem má provoz probíhat. Pokud by *provozní postupy* nebyly definovány, personál by nevěděl, jakým způsobem chce mít provozovatel nastavenou bezpečnost provozu, jak má být náklad k připoután k UAS apod. Kdyby *provozní postupy* byly definovány příliš pozdě, mohlo by dojít k situaci, že se s nimi personál nestihne seznámit a provozovatel by očekával, že provoz bude nějak probíhat, ale realita by se nepotkala

s očekáváním. Pokud by se vyskytovaly nepřesnosti v provozních postupech, personál by tím mohl být zmaten a nejspíš by došlo k porušení legislativy.

Podmínkou, která musí být splněna je *registrace provozovatele*. Jakmile provozovatel nebude registrován, nesplní pravidla platné pro provozovatele, kteří chtějí létat v U-space. V tomto případě by provozovatel nebyl oprávněn v U-space létat a nebyly by mu k dispozici služby U-space. Pokud by se i přes to pokusil provoz provést, vznikla by zde výrazná negativní variabilita.

Posledním vstupem do funkce je *certifikace dálkově řídícího pilota*. Dálkově řídící pilot musí mít platnou a náležitou certifikaci k tomu, aby mohl pilotovat daný provoz. Pokud by pilot neměl náležitou certifikaci mohlo by se stát, že nezvládne pilotování UAS.

Kombinací výše uvedených variabilit by zde vznikala rezonance, která by s největší pravděpodobností vedla k nebezpečné události. Pokud by provozovatel neměl k dispozici služby U-space a i přesto provoz zahájil, a ještě k tomu by provoz prováděl pilot bez náležité certifikace, byla by značně ohrožena bezpečnost vzdušného prostoru U-space. Mohlo by zde dojít k ohrožení životů zapojených i nezapojených osob do provozu, majetkovým škodám i ke sblížení letadel nebo jejich střetu. Další možností negativní rezonance je kombinace variabilit, kdy budou vydány nepřesné provozní postupy, tedy personál nebude mít dostatečné informace o provozu a pilot nebude držitelem náležité certifikace pilota. V tomto případě by mohlo dojít ke stejným nebezpečným událostem jako v předchozím případě.

4.3.2 Druhá kombinace variabilit

Druhou funkcí s významnou variabilitou je funkce *Poskytovat specifickou U-space službu dle stanovených pravidel.* Významná variabilita je zde způsobena velkým množstvím vstupujících aspektů do funkce a vysokým množstvím „upstream“ funkcí.

Aspekt řízení *pravidla poskytování U-space služeb* definuje, jakým způsobem mají být U-space služby poskytovány. Pokud by pravidla byla definována nepřesně, pak by systém nemusel fungovat správně, nebo vůbec. Mohlo by se stát, že nebude zajištěna kooperace mezi USSP a provozovatelem. Pokud by pravidla nebyla definována vůbec, pak by nemohlo dojít ke správnému a sjednocenému poskytování U-space služeb.

Podmínka *certifikace poskytovatele U-space služby* je nutná podmínka k tomu, aby služba mohla být poskytována. Pokud by poskytovatel nebyl certifikován, pak by nejspíš neposkytoval

správná data potřebná k bezpečnému provozu, nebo by je poskytoval, ale ne během provozu UAS, respektive ve špatný čas.

Vstup *vyhodnocená data* by mohl výrazně ovlivnit variabilitu funkce. V případě, kdy by vyhodnocená data nebyla poskytována, nebo by byla nepřesná, nebo by docházelo k jejich poskytování pozdě, poskytovatelé služeb U-space by neměli relevantní zdroj aktuálních informací a U-space služby by buďto nemohly být poskytovány, nebo by byly poskytovány nepřesně.

Posledním aspektem je vstup *cíl provozu definován*. Tento vstup zajišťuje, že poskytovatelé U-space služeb vědí, jaké jsou potřeby provozu, tedy jaké služby musí poskytovat. Pokud by cíl provozu nebyl definován vůbec, pak by USSP nevěděli, že má provoz proběhnout a provozu by nebyly poskytovány žádné U-space služby. Pokud by cíl provozu byl definován pozdě nebo nepřesně, mohlo by se stát, že provozu nebudou poskytovány všechny potřebné U-space služby.

V případě kombinace variabilit, kdy *vyhodnocená data* nebudou poskytována vůbec, a ještě k tomu by byla nepřesně nastavena *pravidla poskytování U-space služby*, mohlo by dojít k "nefunkčnosti" U-space. Pokud by U-space služby nebyly funkční, již by se nedalo hovořit o vzdušném prostoru U-space. Takový prostor by se ničím nelišil od okolního vzdušného prostoru. Pokud by se sešla variabilita v podobě špatně *vyhodnocených dat*, nepřesně nastavených *pravidel poskytování U-space služeb* a *cíl provozu* by byl nepřesně *definován*, pak by mohlo dojít ke sblížení letadel (ať už UAS s UAS, nebo UAS s letadlem s pilotem na palubě) a v nejhorším případě by mohlo dojít ke střetu letadel, nebo k pádu letadla (způsobeným např. špatným počasím).

Pokud by nebyla definována *pravidla poskytování U-space služeb* a poskytovatel U-space služby by nebyl certifikován, mohlo by dojít ke značně negativní rezonanci v systému, a to k nepovolenému elektronickému zásadu do dat poskytovatele U-space služeb.

4.3.3 Třetí kombinace variabilit

Poslední identifikovanou funkcí s výraznou variabilitou je funkce *Sběr a dodání dat.* Tato funkce disponuje velkým množstvím aspektů do ní vstupujících. Prvním vstupem jsou *data o provozu*, která když jsou nepřesná, kvalita U-space služeb je zhoršena a je možné, že by o tom piloti a provozovatelé UAS ani nebyli informováni. To samé platí, pokud by data byla poskytována pozdě, protože by nebyla k dispozici data aktuální. Pokud by data o provozu nebyla k dispozici vůbec, pak by nebyly k dispozici informace o provozu letadel kolem letišť.

Pro vstup *data o poloze* by vznikala stejná negativní variabilita jako u vstupu *data o provozu*, pokud by nebyla by k dispozici správná data o poloze letadel s pilotem na palubě ve vzdušném prostoru, nebo by nebyla k dispozici vůbec.

Vstupem řízení jsou *stanovená pravidla*, která také definují, jakým způsobem má ke *Sběru a dodání dat* docházet. Pokud by pravidla nebyla stanovena vůbec, pak by se tato funkce neměla čím řídit a sbírání a dodávaní dat by fungovalo nespolehlivě, což by ovlivňovalo bezpečnost U-space provozu. Piloti UAS i piloti letadel s pilotem na palubě by neměli dostatek správných dat o provozu. Pokud by pravidla byla definována příliš pozdě, nebo nepřesně, nebylo by jasné, jakým způsobem má sbírání a dodávání dat probíhat, nebo by to neprobíhalo tak, aby byla zajištěna bezpečnost U-space.

Kombinace variabilit, kdy nejsou k dispozici *data o provozu* a *data o poloze*, nebo pokud by byla nepřesná, či zpožděná, by způsobila nedostatek informací o letadlech s pilotem na palubě, jejich pohybu a poloze. V případě, že by tento významný nedostatek byl odhalen, došlo by k přerušení sdílení dat, kvůli čemuž by musel být zastaven provoz U-space. Pokud by nebyl odhalen, let letadla s pilotem na palubě by mohl zkřížit let UAS (nebo naopak) a mohlo by dojít ke sblížení až srážce dvou letadel. Kombinace všech těchto tří variabilit by způsobila významnou rezonanci v systému a situace by mohla vyústit až ve stejná nebezpečí, jaká byla definována pro předchozí rezonanci.

4.4 Návrh opatření snižující rezonanci

Pomocí scénářů, které jsou popsány v předchozím kroku je možné definovat návrhy opatření, které povedou ke snížení rezonance, případně k tomu, aby některá z identifikovaných rezonancí nenastala. Je potřeba se zaměřit na ty funkce, které způsobují největší rezonanci.

Pro první kombinaci variabilit jsou navržena následující opatření:

- Provozovatel musí definovat provozní postupy.
- Provozovatel musí být registrován.
- Pilot musí mít odpovídající licenci pro provoz.

Pro druhou kombinaci variabilit jsou navržena tato opatření:

- Data musí být poskytovatelům U-space služeb dodávána.
- Pravidla poskytování U-space služby musí být definována.
- Poskytovatel U-space služeb musí být certifikován.
- Data dodaná do USSP musí být správná a dodána ve správný čas

- Data dodaná do USSP musí odpovídat požadavkům na kvalitu.
- Provozovatel musí definovat cíl provozu.
- Poskytovatel U-space služeb musí zajistit ochranu dat.

Pro třetí a zároveň poslední kombinaci variabilit byla definována následující opatření:

- Data dodávaná do CIS musí být přesná.
- Data dodávaná do CIS musí být aktuální.
- Data do CIS musí být dodávaná včas.
- Musí být stanovena pravidla, jakým způsobem má sběr a následné dodání dat ostatním subjektům U-space probíhat.
- Data musí být dodávána dle uzavřených smluv.

5 Interpretace výsledků

Pomocí obou systémových metod byly definovány požadavky a opatření, které musí být splněny, aby v systému nedošlo k nebezpečným událostem. Pomocí analýzy STPA bylo nalezeno velké množství požadavků, zatímco metoda FRAM pomohla odhalit menší množství opatření. Výsledky jednotlivých metod jsou popsány v následujících kapitolách. Jelikož cílem této práce je zhodnotit bezpečnost U-space v ČR, výsledky metod jsou porovnány s platnou leteckou legislativou. Výsledky byly porovnány s následujícími dokumenty:

- Zákon o civilním letectví č. 49/1997 Sb.
- Prováděcí nařízení Komise (EU) 2019/945
- Prováděcí nařízení Komise (EU) 2019/947
- Prováděcí nařízení Komise (EU) 2021/664
- Prováděcí nařízení Komise (EU) 2021/665
- Prováděcí nařízení Komise (EU) 2017/373
- Nařízení Evropského parlamentu a Rady (ES) č. 550/2004
- Nařízení Evropského parlamentu a Rady (EU) č. 376/2014

Pokud bylo zjištěno, že nalezené opatření/požadavek je pokryt legislativou, je u něj odkaz zvýrazněný kurzívou na daný legislativní dokument. Opatření/požadavek, který není v legislativě zmíněn, je zvýrazněn tučně.

5.1 Výsledky metody STPA

Pomocí metody STPA bylo nelezeno 96 požadavků na systém U-space. Všechny požadavky, s odkazy na legislativní dokumenty, jsou uvedeny v příloze 7. Většinu požadavků je možné nalézt v legislativních dokumentech uvedených v předchozí kapitole. Byly ale nalezeny i požadavky, které se v legislativě nevyskytují. Jmenovitě to jsou:

- USSP musí dodržovat pravidla.
- USSP musí mít informaci o tom, že musí poskytovat hlášení události.
- Musí být stanovena pravidla na poskytnutí výcviku pro určitý provoz.
- Provozovatel musí poskytnout instrukce poskytovateli výcviku s dostatečným předstihem, aby ten se na výcvik mohl připravit.
- Provozovatel musí vědět, jaký standardní scénář chce využívat a tuto informaci poskytnout poskytovateli výcviku.

- Provozovatel musí definovat místa provozu a mise, aby podle nich definoval instrukce pro poskytovatele výcviku pilotovi.
- Ovládací stanice se nesmí porouchat.
- Poskytovatel výcviku musí mít schopnosti a možnosti vycvičit pilota.
- Poskytovatel výcviku musí dostat pokyny pro výcvik.
- Poskytovatel výcviku musí znát harmonizovaná pravidla.

5.2 Výsledky metody FRAM

Počet opatření, která byla nalezena pomocí metody FRAM, je 16. U každého opatření je kurzívou napsán odkaz na konkrétní legislativní dokument, ve kterém je uvedené opatření pokryto. Nalezená opatření jsou následující:

- Provozovatel musí definovat provozní postupy. *2019/947, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů 1) a 2019/947 UAS.SPEC.050 Povinnosti provozovatele bezpilotních systémů 1)a)*
- Provozovatel musí být registrován. *2019/947, článek 12, 4. s. 10*
- Pilot musí mít odpovídající licenci pro provoz. *2019/947, Příloha, část A, UAS.OPEN.020 Provoz bezpilotních systémů v podkategorii A1, 4)b) s. 16 a UAS.OPEN.030 Provoz bezpilotních systémů v podkategorii A2, 2), a), b), s. 17 a UAS.OPEN.040 Provoz bezpilotních systémů v podkategorii A3, 3) s. 18*
- Poskytovatel U-space služeby musí být certifikován. *2021/664, článek 7, 1., s. 8*
- Data musí být poskytovatelům U-space služeb dodávána. *2021/664, článek 5, 4. b) s. 6*
- Pravidla poskytování U-space služby musí být definována. *2021/664, (9), s. 2*
- Poskytovatel U-space služeb musí být certifikován. *2021/664, článek 7, 1., s. 8*
- Data dodaná do USSP musí být správná a dodána ve správný čas. *2021/664, článek 5, 4. b) s. 6*
- Data dodaná do USSP musí odpovídat požadavkům na kvalitu. *2021/664, článek 5, 4. b) s. 6*
- Provozovatel musí definovat cíl provozu. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 1), s. 18 a část B, UAS.SPEC.050 Povinnosti provozovatele bezpilotních systémů 1)a)*
- Poskytovatel U-space služeb musí zajistit ochranu dat. *2021/664, příloha III, s. 17*
- Data dodávaná do CIS musí být přesná. *2021/664, (16), s. 2 a článek 5, 4.*

- Data dodávaná do CIS musí být aktuální. *2021/664, článek 5, č., s. 6*
- Data do CIS musí být dodávaná včas. *2021/664, článek 5, č., s. 6*
- Musí být stanovena pravidla, jakým způsobem má sběr a následné dodání dat ostatním členům U-space probíhat. *2021/664, (16), s. 2*
- Data musí být dodávána dle uzavřených smluv. *2021/664, příloha V, 1., s. 19*

Všechna definovaná opatření byla v uvedených legislativních dokumentech nalezena.

5.3 Stanovení doporučení pro ČR

Na základě provedených studií je možné definovat doporučení pro zvýšení bezpečnosti provozu UAS v ČR. Většina požadavků identifikovaná pomocí metody STPA je spojena s výcvikem posádky. Legislativa v současné chvíli nedefinuje povinnosti poskytovatele výcviku, ani pokyny, jak by měl takový výcvik vypadat, ani jaké povinnosti z poskytnutého výcviku plynou pro provozovatele. Prováděcí nařízení Komise (EU) 2019/947 se zabývá pouze povinností výcviku v kategorii OPEN a SPECIFIC. V těchto kategoriích je výcvik posádky založen na on-line výcvikovém kurzu a absolvování praktického výcviku v provozních podmínkách shodných, jako jsou zamýšlené provozní podmínky provozu. Praktický výcvik má sice dané body, které musí dálkově řídící pilot zvládnout, respektive jsou definovány manévry a dovednosti, které musí pilot ovládat, nicméně praktický výcvik je ponechán na samostudiu dálkově řídícího pilota. Jako důkaz o absolvování výcviku postačuje čestné prohlášení o jeho absolvování. V kategorii CERTIFIED (do které bude spadat část provozu v U-space) ovšem musí veškeré organizace a osoby zapojeny do provozu, taktéž i výcvik všech těchto osob podléhat certifikaci. To znamená, budou muset být schváleni Agenturou Evropské unie pro bezpečnost letectví (EASA). Z praxe z provozu letadel s pilotem na palubě je v letectví běžné poskytovat odborný výcvik třetí stranou. Existují organizace, které poskytují výcvik pilotům, řídícím letového provozu, obsluze pozemního odbavení atd. Z toho vyplývá, že v budoucnu bude nutné, do legislativních dokumentů týkajících se bezpilotního letectví zahrnout nařízení, týkající se poskytování odborného výcviku. Proto jsou stanovena tato doporučení, která by bylo vhodné implementovat do legislativy pro Českou republiku:

- První doporučení je pro příslušný úřad stanovený Českou republikou implementovat a definovat pravidla stanovená v nařízeních EK týkající se výcviku leteckého personálu. Je nutné definovat, jak přesně má výcvik probíhat, co všechno musí výcvik obsahovat, jakým způsobem bude výcvik zakončen.

- Druhé doporučení se týká provozovatele bezpilotního systému. V legislativě musí být definováno, že provozovatel musí informovat poskytovatele výcviku, že bude potřebovat výcvik pro svůj personál. Jeho povinnost je také poskytnout poskytovateli výcviku informace o zamýšleném provozu a provozních postupech. Informace musí být poskytnuty s dostatečným předstihem tak, aby se poskytovatel výcviku mohl na výcvik připravit.
- Třetí doporučení se týká poskytovatele výcviku, který musí být certifikován k poskytování výcviku. Poskytovatel výcviku musí znát a dodržovat pravidla výcviku a musí mít zavedeny efektivní procesy pro výcvik pilota, potřebné vybavení a certifikovaný personál.

6 Diskuze

Dosažené výsledky vyplývající z aplikace metod STPA a FRAM ukazují, že současná regulace bezpilotního letectví je nastavena převážně správně. Při ověřování regulace bylo nezbytné nastavit hranice systému, který bude analyzován. Tento systém byl omezen na provoz pouze vnitrostátních letadel, který nepočítá s výskytem letadel zahraničních. Provoz zahraničních letadel by byl v systému umožněn přidáním prvku společné informační služby jiného státu. Taktéž by bylo nutné přidat prvek EU registr, ze kterého by bylo možné získat informace o zahraničních provozovatelích, pilotech, UAS apod. Do systému nejsou zapojeny některé organizace státu, jako například složky IZS, PČR, AČR apod., které budou v U-space také provozovat své lety. V analyzovaném systému je definován pouze jeden poskytovatel U-space služeb. Po definování systému v rámci těchto hranic bylo následně pomocí metod STPA a FRAM identifikováno celkem 112 požadavků a opatření, které když budou splněny, sníží možnost výskytu rezonance či výskyt nebezpečných řídících akcí v systému.

První požadavek, který byl identifikován pomocí metody STPA říká, že *USSP musí dodržovat pravidla.* Požadavek nebyl nalezen v legislativě z toho důvodu, že se obecně předpokládá, že veškeré organizace zapojené do letectví budou dodržovat stanovená pravidla. Nepředpokládá se, že by letecké organizace pravidla úmyslně porušovaly nebo nedodržovaly. Obdobné vysvětlení platí i pro druhý požadavek *USSP musí mít informaci o tom, že musí poskytovat hlášení události.* V Nařízení Evropského parlamentu a Rady (EU) č. 376/2014 je definováno následující nařízení [23]: *Každá organizace usazená v členském státě zřídí povinný systém podávání hlášení usnadňující shromažďování údajů o událostech (…).* Z tohoto nařízení vyplývá, že USSP musí poskytovat hlášení o událostech, a proto se předpokládá, že USSP zná své povinnosti a ví, že musí toto nařízení dodržovat. Proto není tato povinnost v legislativě napsána doslovně. Z těchto důvodů není první, ani druhý požadavek zmíněn jako doporučení v kapitole 5.3 Stanovení doporučení pro ČR.

Požadavky na systém týkající se praktického výcviku pilota, který by byl poskytován třetí stranou, zatím nejsou v legislativě definovány. Povaha provozu, který je aktuálně možné uskutečnit, nevyžaduje certifikovaný výcvik. V Prováděcím nařízení Komise (EU) 2019/947 jsou definovány pouze požadavky na výcvik pilota pro kategorii OPEN a SPECIFIC. Nicméně výcvik, který je vyžadován je ponechán na samotném pilotovi a nikdo nehodnotí, zdali pilot opravdu splňuje požadavky výcviku. Jakmile budou definována pravidla pro provoz v kategorii CERTIFIED, takovéto požadavky bude potřeba definovat.

Další požadavek je *Ovládací stanice se nesmí porouchat*. U ovládací stanice, stejně jako u jakéhokoli jiného výrobku není možné garantovat jeho naprostou bezporuchovost. Není možné zajistit, že se ovládací stanice nikdy neporouchá, ovšem je možné stanovit pravidla její konstrukce tak, aby s co nejmenší pravděpodobností došlo k její poruše. Musí být tedy stanovena pravidla konstrukce a údržby ovládací stanice. Ta již jsou definována ve čtvrté verzi eRules pro bezpilotní systémy [5]. Zde jsou definovány požadavky na konstrukci a vybavení bezpilotních systémů tříd C1, C2, C3, C4, C5 a C6. Zároveň je nutné, aby výrobce ovládací stanice k výrobku přiložil podrobný návod, jak ho ovládat, jak provádět údržbu, kde je možné výrobek reklamovat/servisovat apod.

Stanovená doporučení pro ČR je možné očekávat v nařízeních Evropské komise, která budou vydávána s postupem implementace dalších fází U-space.

Všechna z nalezených opatření pomocí metody FRAM jsou definována v legislativních dokumentech. Z tohoto výsledku je možné usoudit, že pravidla vyplývající z předpisů a zákonů, které jsou aktuálně platné, jsou definována na dostatečné úrovni bezpečnosti. Pokud ale porovnáme výsledky metody STPA a metody FRAM, je možné zjistit, že pomocí metody STPA bylo nalezeno mnohem více požadavků na systém než pomocí metody FRAM. Tento výsledek může být zapříčiněn zvolením příliš obecné úrovně abstrakční hierarchie. Je pravděpodobné, že pokud by byla zvolena nižší úroveň (např. fyzické funkce nebo fyzické formy), bylo by identifikováno větší množství požadavků na systém.

Není možné jasně určit, která z těchto dvou metod je pro analyzování bezpečnosti systému U-space vhodnější. Pomocí obou metod je možné nalézt, kde v systému mohou vzniknout nebezpečné situace. Obě metody by bylo možné využít pro posouzení provozní bezpečnosti i jiných komplexních systémů v letectví. Doporučení, která byla stanovena na základě výsledků metod STPA a FRAM, je možné aplikovat nejen v ČR, ale ve všech státech EU, jelikož se všechny řídí stejnými pravidly.

7 Závěr

Ve této diplomové práci jsem chtěla poukázat na problematiku bezpečnosti provozu bezpilotních systémů. Předtím, než jsou zavedeny nové systémy a postupy, je nutné ověřit jejich bezpečnost. Běžně používaným nástrojem pro definování bezpečnosti jsou právě safety metody. Tato práce ukazuje, že pomocí safety metod je možné identifikovat nedostatky v systému a díky nim definovat opatření, jak tyto nedostatky eliminovat.

Provoz bezpilotních systémů se řídí od roku 2020 novými pravidly provozu, která definovala Evropská komise. Pravidla jsou stejná pro všechny státy EU a dělí provoz UAS do třech kategorií dle míry rizika provozu. Také definuje povinnost registrace pilotů a provozovatelů a každý členský stát musí publikovat mapu omezených vzdušných prostorů. Všechny tyto novinky vedou k tomu, aby jednou vzdušný prostor nad osídlenými oblastmi sdílely bezpilotní letadla společně s letadly s pilotem na palubě. Tento vzdušný prostor se nazývá U-space.

Vzhledem k tomu, že U-space s sebou přináší velké množství nových technologií, postupů a služeb, je nutné zjistit, jestli provoz v něm bude bezpečný. Bezpečnost U-space, jakožto komplexního systému, který obsahuje techniku, lidi a organizace najednou, je možné analyzovat pomocí systémový metod provozní bezpečnosti STPA a FRAM. Tyto dvě metody umožní v systému identifikovat možné nebezpečné události, které mohou v systému nastat. Pomocí metod je následně možné nalézt opatření a požadavky na systém, které když budou splněny, tak nebude docházet k nebezpečným událostem. Vybrané systémové metody byly aplikovány na systém U-space a pomocí jejich výsledků bylo možné navrhnout opatření, která přispějí ke zvýšení bezpečnosti provozu bezpilotních systémů v ČR.

Práce obsahuje dvě limitace. První limitací je nastavení hranic systému pro provedení metody STPA, kdy může existovat další požadavek na legislativu, který ale nebyl odhalen. Druhou limitací je použitá abstrakční hierarchie v rámci metody FRAM, kdy při použití detailnějšího modelu by mohlo dojít k identifikaci nějakých, legislativou aktuálně neadresovaných požadavků.

I přes zmíněné limitace práce splnila svůj účel. Byly definovány celkem tři oblasti doporučení, které aktuálně chybějí v legislativě. Zároveň práce ukázala, že většina identifikovaných požadavků na systém je v rámci legislativy obsažena. Všechny tři oblasti pro doporučení se týkají výcviku dálkově řídícího pilota. Aktuálně platná legislativa nevyžaduje pilotův odborný výcvik. Výcvik pilota je založen na samostudiu a následném čestném prohlášení, že pilot výcvik absolvoval. Kategorie CERTIFIED, která zatím nemá jasně stanovaná pravidla provozu,

protože provoz v ní je zatím budoucností, bude odborný výcvik vyžadovat. Čím dále se bude postupovat v implementování jednotlivých fází U-space, tím větší bude potřeba kategorii CERTIFIED dospecifikovat a definovat její pravidla provozu.

Před každou nově implementovanou fází U-space by bylo vhodné ji analyzovat způsobem, jaký byl popsán v této práci a zjistit tak, jaké jsou nedostatky v definovaných pravidlech, případně jaké nebezpečné události by mohly vzniknout. Návazné práce by mohly zkusit rozšířit hranice systému pro modelování STPA a využít detailnější úroveň abstrakční hierarchie FRAM, čímž by mohlo dojít k potvrzení závěrů, nebo k identifikaci dalších požadavků na U-space, aby provoz v něm byl bezpečný.

Bibliografie

[1] *PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2019/947 ze dne 24. května 2019 o pravidlech a postupech pro provoz bezpilotních letadel*. In: . EU: Evropská komise, 2019. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019R0947&from=CS

[2] *NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2019/945 ze dne 12. března 2019 o bezpilotních systémech a o provozovatelích bezpilotních systémů ze třetích zemí*. In: . EU: Evropská komise, 2019. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019R0945&from=CS

[3] ČESKÁ REPUBLIKA. *Zákon č. 49/1997 Sb.: Zákon o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů*. In: . ČR, 1997. Dostupné také z: https://www.zakonyprolidi.cz/cs/1997-49

[4] Drone Laws: 1:1 rule. In: *INFRATEC* [online]. [cit. 2022-05-03]. Dostupné z: https://www.infratec-drones.com/post/drone-laws-1-1-rule

[5] ŘÍZENÍ LETOVÉHO PROVOZU ČESKÉ REPUBLIKY, S. P. Létejte zodpovědně. In: *Létejte zodpovědně* [online]. [cit. 2022-04-14]. Dostupné z: https://letejtezodpovedne.cz/

[6] *ERules pro bezpilotní systémy (UAS): (nařízení (EU) 2019/947 a (EU) 2019/945)*. In: . EASA, ÚCL, 2022, Verze 4.0.

[7] PRIMOCO UAV. ČESKÝ VÝROBCE BEZPILOTNÍCH LETOUNŮ PRIMOCO UAV SE ZÍSKAL EVROPSKÉ OPRÁVNĚNÍ K PROVOZU LUC. In: *PRIMOCO UAV* [online]. [cit. 2022-05-01]. Dostupné z: https://uav-stol.com/cs/media/primoco-uav-se-the-czech-unmanned-aircraft-manufacturer-has-received-a-european-luc-authorisation/

[8] *DronView* [online]. ČR: ŘLP ČR s.p. [cit. 2022-05-03]. Dostupné z: https://dronview.rlp.cz/

[9] EUROCONTROL, a EU. *Delivering drone solutions for smart and sustainable air mobility: U-space research and innovation portfolio* [online]. In: . Luxembourg: Publications Office of the European Union: SESAR Joint Undertaking, 2021 [cit. 2022-05-01]. Dostupné z: https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20RandI%20portfolio.pdf

[10] *PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2021/664: ze dne 22. dubna 2021 o regulačním rámci pro vzdušný prostor U-space*. In: . EU: Evropská komise, Generální ředitelství pro mobilitu a dopravu,

2021, ročník 2021. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32021R0664&from=CS

[11] *PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) č. 923/2012: ze dne 26. září 2012,*. In: . EU: Evropská komise, 2012, ročník 2012. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32012R0923

[12] EUROCONTROL. *A White Paper on Resilience Engineering for ATM* [online]. 16 [cit. 2022-04-28]. Dostupné z: https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf

[13] MOLLOY, Gerard a Ciarán O'BOYLE. The SHEL Model: A Useful Tool for Analyzing and Teaching the Contribution of Human Factors to Medical Error. *Academic Medicine* [online]. 2005, **80**(2) [cit. 2022-05-09]. Dostupné z: file:///C:/Users/evami/Downloads/The_SHEL_Model__A_Useful_Tool_for_Analyzing_and.9.pdf

[14] VINCOLI, Jeffrey W. *Management Oversight and Risk Tree: Basic Guide to System Safety* [online]. USA: John Wiley & Sons, 2014 [cit. 2022-04-28]. ISBN 9781118904589. Dostupné z: https://onlinelibrary.wiley.com/doi/10.1002/9781118904589.ch13

[15] HOLLNAGEL, Erik. *Safety-I and safety-II: The past and future of safety management* [online]. USA: Ashgate Publishing Company, 2014 [cit. 2022-04-30]. ISBN 9781472423061.

[16] NANCY LEVESON: Professor of Aeronautics and Astronautics. In: *AEROASTRO* [online]. [cit. 2022-05-01]. Dostupné z: https://aeroastro.mit.edu/people/nancy-leveson/

[17] LEVESON, Nancy G. *Engineering a safer world: systems thinking applied to safety* [online]. Cambridge: MIT Press, 2011, 463 s. [cit. 2022-05-01]. ISBN 9780262016629. Dostupné z: http://sunnyday.mit.edu/safer-world.pdf

[18] LEVESON, Nancy a John THOMAS. *STPA Handbook* [online]. 2018 [cit. 2022-05-02]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[19] Erik Hollnagel. In: *SKYbrary* [online]. [cit. 2022-05-02]. Dostupné z: https://skybrary.aero/contributors/erik-hollnagel

[20] HOLLNAGEL, Erik. *FRAM (The Functional Resonance Analysis Method): A brief Guide on how to use the FRAM* [online]. 2018 [cit. 2022-05-02]. Dostupné z: https://functionalresonance.com/onewebmedia/Manual%20ds%201.docx.pdf

[21] Agentura Evropské unie pro bezpečnost letectví (EASA). In: *Evropská unie* [online]. [cit. 2022-05-04]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/easa_cs

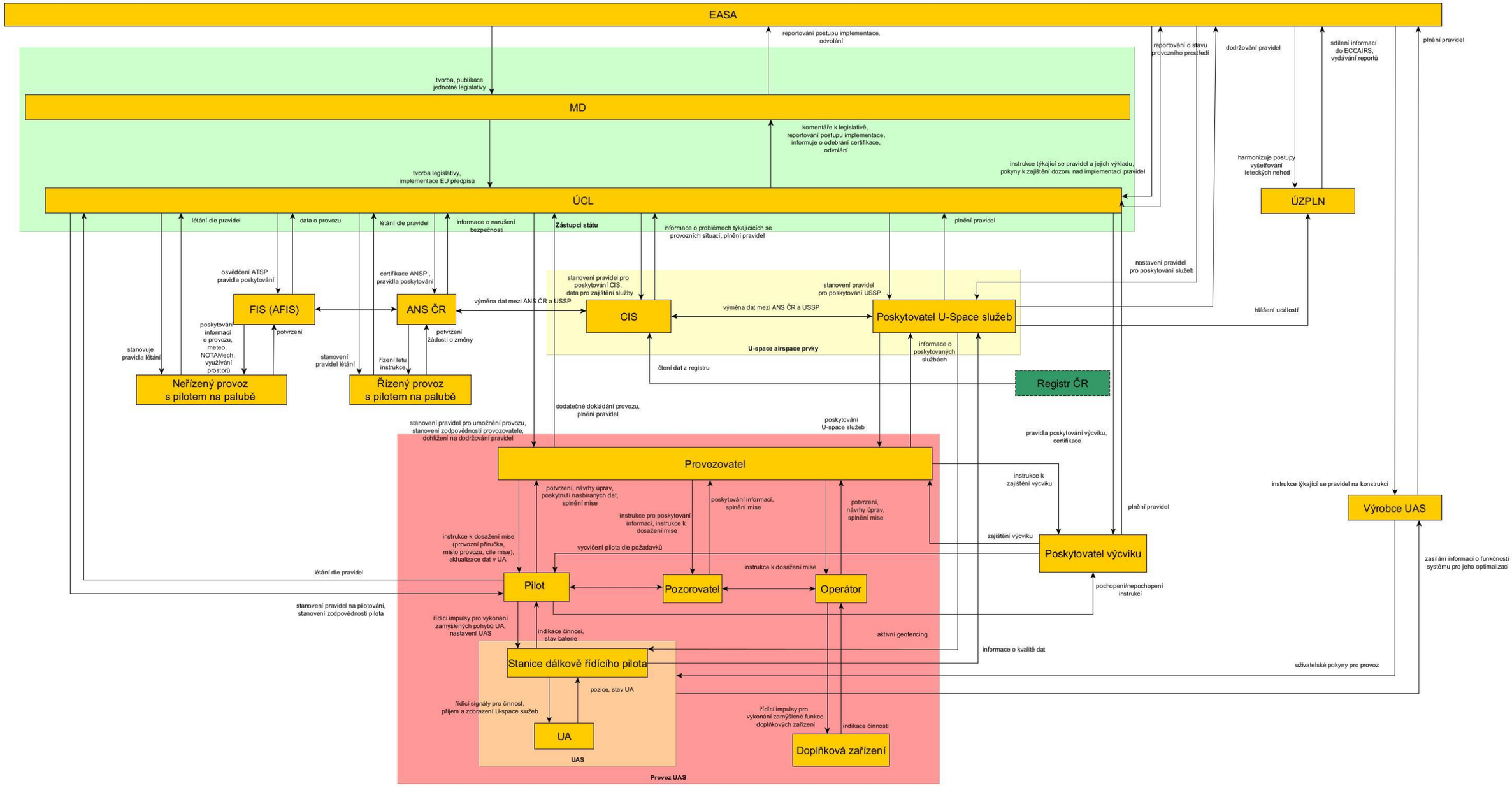
[22] PATRIARCA, Riccardo, Giulio DI GRAVIOA a Johan BERGSTRÖMB. *Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM* [online]. 15 [cit. 2022-05-06]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0951832016302514

[23] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 376/2014*. In: . EU: Evropský parlament a Rada, 2014. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0376&from=CS

Seznam tabulek

Seznam obrázků

Příloha 1 Řídící struktura



Příloha 2 Přehled nebezpečných řídících akcí

ID	*Řídící akce*	*Neprovedení řídící akce vede k nebezpečí*	*Provedení řídící akce vede k nebezpeční*	*Příliš brzy, pozdě, ve špatném pořadí*	*Trvá příliš dlouho, přerušena příliš brzy*	*Způsobená nebezpečí*
UCA-1.1	instrukce týkající se pravidel a jejich výkladu	neposkytne ÚCL instrukce a výklad pro aplikaci pravidel	poskytne neúplné instrukce a výklad pravidel poskytne instrukce a výklad pravidel, která nebudou jednoznačná	poskytne instrukce a výklad pravidel pozdě	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-1.2	pokyny k zajištění dozoru nad implementací pravidel	neposkytne ÚCL pokyny k zajištění dozoru	poskytne neúplné pokyny k zajištění dozoru nad implementací pravidel	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-1.3	instrukce týkající se pravidel na konstrukci	nenastaví pravidla pro konstrukci UAS nenastaví pravidla na manuál k UAS	stanoví pravidla pro konstrukci UAS, která nebudou bezpečná	-	-	H1.2, H1.3
UCA-1.4	stanovení pravidel pro poskytování USSP	neposkytne USSP pravidla pro poskytování USSP	stanoví USSP pravidla neúplně	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.1	stanovení pravidel pro umožnění provozu	nestanoví provozovateli pravidla pro umožnění provozu	stanoví provozovateli pravidla neúplně, nebo protichůdně	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.2	stanovení zodpovědnosti provozovatele	nestanoví provozovateli zodpovědnost	-	-	-	H1.2, H1.3
UCA-2.3	dohlížení na dodržování pravidel	nedohlíží na dodržování pravidel	-	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.4	stanovení pravidel pro poskytování CIS	nestanoví CIS poskytovateli všechna pravidla pro předávání informací	stanoví poskytovateli CIS pravidla neúplně	-	-	H3.3
UCA-2.5	data pro zajištění služby	neposkytne CIS poskytovateli data pro předávání informací	poskytne nesprávná data CIS poskytovateli	poskytuje data pozdě	přeruší poskytování dat	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.6	stanovení pravidel pro poskytování USSP	neposkytne USSP pravidla pro poskytování USSP	stanoví USSP pravidla neúplně	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.7	stanovení pravidel na pilotování	nestanovení pravidel na pilotování	stanoví pilotovi pravidla neúplně	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.8	stanovení zodpovědnosti pilota	nestanoví zodpovědnosti pilota	-	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.9	stanovení pravidel létání	nestanoví pravidla létání	stanoví pravidla létání neúplně			H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-2.10	certifikace ANSP a pravidla poskytování	ÚCL necertifikuje ANSP nebo nevydá pravidla poskytování	ÚCL certifikuje ANSP nesprávně			H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2

UCA-3.1	výměna dat z ANS ČR do USSP	k výměně dat nedojde i když jsou vyžadována	k výměně dojde, ale integrita dat bude narušena	k výměně dat dojde pozdě	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-3.2	výměna dat z USSP do ANS ČR	k výměně dat nedojde i když jsou vyžadována	k výměně dojde, ale integrita dat bude narušena	k výměně dat dojde pozdě	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2
UCA-4.1	aktivní geofencing	neposkytuje data pro aktivní geofencing	poskytuje nesprávná data pro aktivní geofencing	poskytuje data pro aktivní geofencing v čase, kdy nejsou aktuální	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2
UCA-4.2	hlášení událostí v případě nehody/incidentu	nenahlásí událost ÚZPLN	nahlásí událost ÚZPLN nesprávně	nahlásí událost ÚZPLN pozdě	-	H3.1, H3.2
UCA-5.1	instrukce k dosažení mise (provozní příručka, místo provozu, cíle mise)	nedá instrukce pilotovi k dosažení mise, když je třeba misi realizovat	dá instrukce pilotovi k plnění mise, které jsou protichůdné, když je třeba misi realizovat	dá instrukce pilotovi k plnění mise moc pozdě, když je třeba misi realizovat	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-5.2	aktualizace dat v UA	neaktualizuje data v UAS, když je třeba je aktualizovat	aktualizuje data v UAS neaktuální verzí	aktualizuje data v UAS moc brzy, tedy nebudou aktuální v době mise	aktualizuje data v UAS pouze částečně	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-5.3	instrukce k dosažení mise	nedá instrukce operátorovi k dosažení mise, když je třeba misi realizovat	dá operátorovi instrukce k dosažení mise, které jsou protichůdné	dá instrukce operátorovi k plnění mise moc pozdě	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-5.4	instrukce pro zajištění výcviku	nedá poskytovateli výcviku instrukce k zajištění potřebného výcviku pro definovaný provoz	dá poskytovateli výcviku instrukce k zajištění výcviku, které neodpovídají provozu	dá instrukce poskytovateli výcviku moc pozdě	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-5.5	instrukce pozorovateli pro poskytování informací	nedá pozorovateli instrukce k poskytování informací pilotovi pro definovaný provoz	dá pozorovateli instrukce k poskytování informací, které jsou nesprávné	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2
UCA-6.1	řídící impulsy pro vykonání zamýšlených pohybů UA	neposkytuje řídící impulsy pro vykonání potřebných pohybů UA, když je to potřebné pro let	poskytuje špatné řídící impulsy pro vykonání potřebných pohybů UA	poskytuje řídící impulsy moc brzy nebo moc pozdě	poskytuje řídící signály moc krátké, nebo moc dlouhé	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-6.2	nastavení UAS	nenastaví UAS před letem	nastaví UAS před letem v rozporu s misí, provozní příručkou, manuálem	-	nedokončí nastavení UAS	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-7.1	řídící impulsy pro vykonání zamýšlené funkce doplňkových zařízení	neposkytuje řídící impulsy pro zamýšlené funkce doplňkových zařízení	poskytuje špatné řídící impulsy pro doplňková zařízení	poskytuje řídící impulsy moc brzy nebo moc pozdě	poskytuje řídící signály moc krátké, nebo moc dlouhé	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-8.1	řídící signály pro činnost	neposkytne UA řídící signál pro činnost	poskytne UA špatný signál pro činnost	poskytne UA řídící signál pro činnost pozdě	přeruší poskytování řídícího signálu	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-8.2	příjem a zobrazení U-space služeb	nepřijme nebo nezobrazí U-space služby	přijme nebo zobrazí nesprávné informace	přijme nebo zobrazí informace pozdě	přestane přijímat nebo zobrazovat informace	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2
UCA-9.1	vycvičení pilota dle požadavků	nevycvičí pilota dle požadavků provozovatele nevycvičí pilota dle pravidel	poskytne neúplný výcvik poskytne výcvik, který není v souladu s pravidly	-	-	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2

Příloha 3 Omezení řídícího prvku

ID	*Omezení řídícího prvku 1*	*Omezení řídícího prvku 2*	*Omezení řídícího prvku 3*	*Omezení řídícího prvku 4*
C-1.1	musí poskytnout ÚCL instrukce a výklad pro aplikaci pravidel	musí poskytnout úplné instrukce a výklad všech pravidel musí poskytnout instrukce a výklad pravidel, který bude jednoznačný	musí poskytnout instrukce a výklad pravidel včas před započetím provozování	-
C-1.2	musí poskytnout ÚCL pokyny k zajištění dozoru	musí poskytnout kompletní pokyny k zajištění dozoru nad implementací pravidel	-	-
C-1.3	musí stanovit pravidla pro konstrukci UAS musí stanovit pravidla na manuál k UAS	musí stanovit pravidla pro konstrukci UAS, která budou bezpečná	-	-
C-1.4	musí poskytnout USSP pravidla pro poskytování USSP	musí stanovit USSP pravidla úplně	-	-
C-2.1	musí stanovit provozovateli pravidla pro umožnění provozu	musí stanovit provozovateli pravidla úplně a správně pro celý provoz	-	-
C-2.2	musí stanovit provozovateli zodpovědnost	-	-	-
C-2.3	ÚCL musí dohlížet na dodržování pravidel	-	-	-
C-2.4	musí stanovit CIS poskytovateli všechna pravidla pro předávání informací	musí stanovit poskytovateli CIS pravidla úplně	-	-
C-2.5	musí poskytnout CIS poskytovateli data pro předávání informací	musí poskytnout správná data CIS poskytovateli	musí poskytnout data pro CIS včasně	nesmí přerušit poskytování dat
C-2.6	musí poskytnout USSP pravidla pro poskytování USSP	musí stanovit USSP pravidla úplně	-	-
C-2.7	musí stanovit pravidla na pilotování	musí stanovit pilotovi pravidla úplně	-	-
C-2.8	musí stanovit zodpovědnosti pilota	-	-	-
C-2.9	musí stanovit pravidla létání	musí stanovit pravidla létání úplně		
C-2.10	ÚCL musí certifikovat ANSP	ÚCL musí certifikovat ANSP správně		
C-3.1	musí dojít k výměně dat mezi ANS ČR a USSP	nesmí být narušena integrita dat	k výměně dat nesmí dojít pozdě	
C-3.2	musí dojít k výměně dat mezi ANS ČR a USSP	nesmí být narušena integrita dat	k výměně dat nesmí dojít pozdě	
C-4.1	musí poskytnout data pro aktivní geofencing	musí poskytovat správná data pro aktivní geofencing	musí poskytovat data pro aktivní geofencing v čase, kdy jsou aktuální	-
C-4.2	musí nahlásit událost ÚZPLN	-	musí nahlásit událost ÚZPLN včasně	-
C-5.1	musí dát instrukce pilotovi k dosažení mise, když je třeba misi realizovat	musí dát instrukce pilotovi k plnění mise, které nejsou protichůdné, když je třeba misi realizovat	musí dát instrukce pilotovi k plnění mise v dostatečném předstihu, když je třeba misi realizovat	-
C-5.2	musí aktualizovat data v UAS, když je třeba je aktualizovat	musí aktualizovat data v UAS aktuální verzí	musí aktualizovat data v UAS v čase, kdy bude zajištěno, že budou aktuální v době mise	musí aktualizovat všechna potřebná data v UAS
C-5.3	musí dát instrukce operátorovi k dosažená mise, když je třeba misi realizovat	musí dát operátorovi instrukce k dosažení mise, které nejsou protichůdné	musí dát instrukce operátorovi k plnění mise v dostatečném předstihu před časem mise	-
C-5.4	musí dát poskytovateli výcviku instrukce k zajištění potřebného výcviku pro definovaný provoz	musí dát poskytovateli výcviku instrukce k zajištění výcviku, které odpovídají požadavkům provozu	musí dát instrukce poskytovateli výcviku v dostatečném předstihu před časem výcviku	-
C-5.5	musí dát pozorovateli instrukce k poskytování informací pilotovi pro definovaný provoz	musí dát pozorovateli instrukce k poskytování informací, které jsou správné	-	-
C-6.1	musí poskytnout řídící impulsy pro vykonání potřebných pohybů UA, když je to potřebné pro let	musí poskytovat správné řídící impulsy pro vykonání potřebných pohybů UA	musí poskytovat řídící impulsy v čase, kdy je provozní situace vyžaduje	musí poskytovat správně dlouhé řídící signály
C-6.2	musí nastavit UAS před letem	musí nastavit UAS před letem správně, dle provozní příručky, mise a manuálu	-	musí dokončit nastavení UAS
C-7.1	musí poskytovat řídící impulsy pro zamýšlené funkce doplňkových zařízení	musí poskytovat správné řídící impulsy pro zamýšlené funkce doplňkových zařízení	musí poskytovat řídící impulsy pro zamýšlené funkce v čase, kdy to provozní situace vyžaduje	musí poskytovat správně dlouhé řídící signály
C-8.1	musí poskytnout UA řídící signál pro činnost	musí poskytnout UA správný signál pro činnost	musí poskytnout UA řídící signál pro činnost okamžitě	nesmí přerušit poskytování řídícího signálu
C-8.2	musí přijímat a zobrazovat U-space služby	musí přijímat a zobrazovat správné informace	musí přijímat a zobrazovat informace okamžitě	nesmí přestat přijímat a zobrazovat informace

C-9.1	musí vycvičit pilota dle požadavků provozovatele musí vycvičit pilota dle pravidel	musí poskytnout úplný výcvik pilotovi dle požadavků provozovatele musí poskytnout výcvik pilotovi, který je v souladu s pravidly	-	-

Příloha 4 Ztrátové scénáře a požadavky na systém

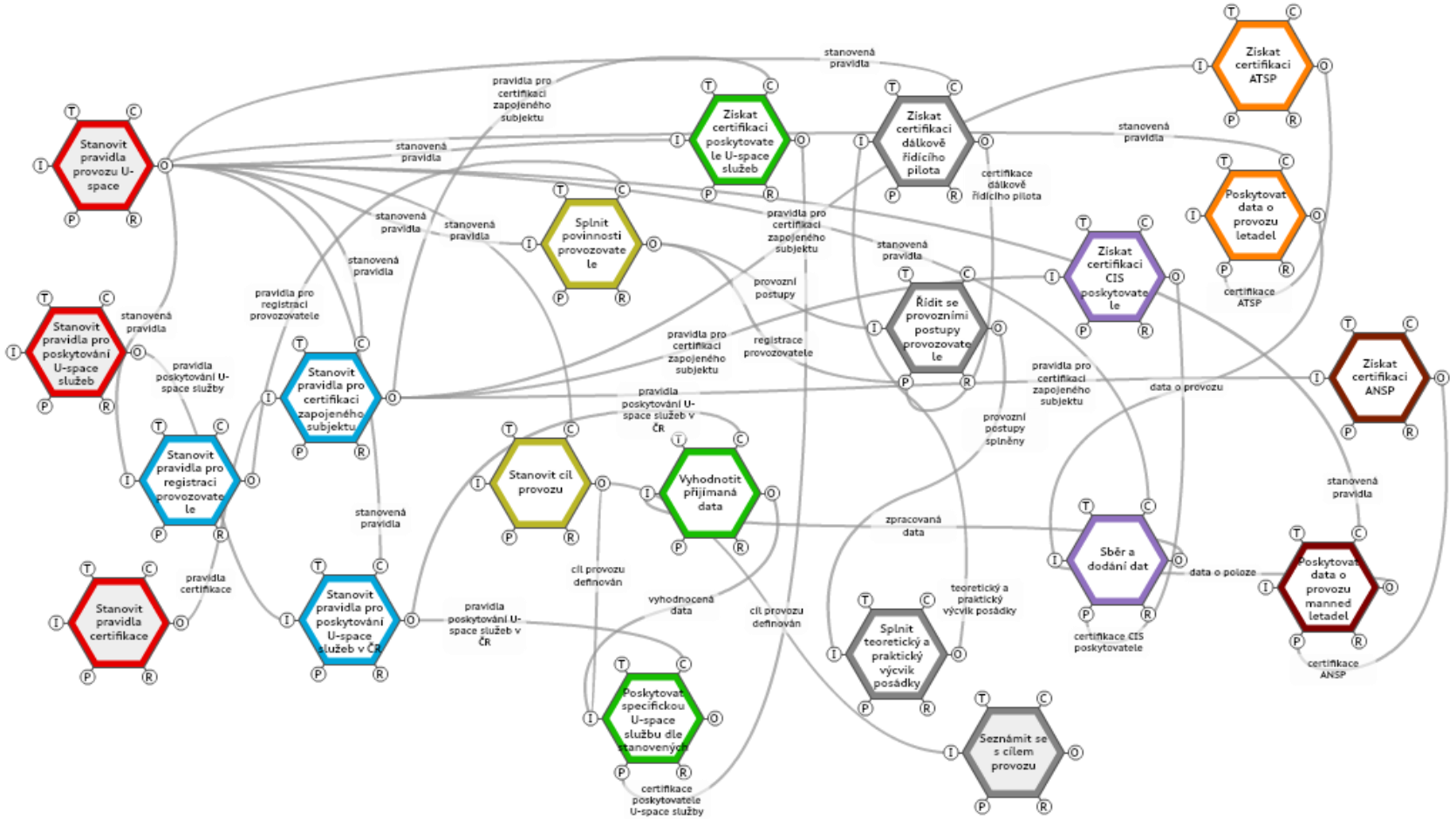
ID	*UCA reference*	*Nebezpečná řídící akce*	*Způsobená nebezpečí*	*Způsobené ztráty*	*Ztrátový scénář*	*Požadavky na systém*
Scenario 1.1	UCA-1.1	EASA neposkytne ÚCL instrukce a výklad pro aplikaci pravidel, nebo poskytne neúplné instrukce a výklad pravidel, nebo poskytne instrukce a výklad pravidel, které nebudou jednoznačné, nebo poskytne instrukce a výklad pravidel pozdě, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– pravidla nejsou definována, nebo –výklad pravidel neexistuje, nebo –nemá představu o reálné problematice létání, nebo –neví, jak vypadá provoz ve státech EU	–EASA musí definovat pravidla –EASA musí vytvořit výklad pravidel –EASA musí mít představu o reálné problematice létání –EASA musí vědět, jak vypadá provoz ve státech EU
Scenario 1.2	UCA-1.2	EASA neposkytne ÚCL pokyny k zajištění dozoru, nebo poskytne neúplné pokyny k zajištění dozoru nad implementací pravidel, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– zajištění dozoru není definováno, nebo – neexistuje smlouva mezi EASA a ÚCL, nebo – pravidla pro zajištění dozoru jsou stará a nepostihují nový provoz, nebo – EASA neví, jak zajišťovat dozor	–EASA musí zajistit, že dozor nad provozem je definován –EASA musí zajistit, že je uzavřena smlouva mezi EASA a ÚCL – EASA musí zajistit aktuálnost pravidel pro vykonávání dozoru, aby postihovaly provoz –EASA musí vědět, jak dělat dozor
Scenario 1.3	UCA-1.3	EASA nenastaví pravidla pro konstrukci UAS, nebo nenastaví pravidla na manuál k UAS, nebo stanoví pravidla pro konstrukci UAS, která nebudou bezpečná, protože...	H1.2, H1.3	L1, L2, L3, L4, L7, L8	–EASA nepovažuje pravidla za potřebná, nebo – EASA nepovažuje uživatelskou příručku/manuál za potřebný, nebo –EASA nemá expertízu na to posoudit možné dopady provozu	–EASA musí definovat všechna pravidla pro zajištění bezpečného provozu –EASA musí zajistit, že uživatelská příručka UAS je vytvořena správně u každého UAS – EASA musí mít expertní znalosti pro posouzení možných dopadů provozu
Scenario 1.4	UCA-1.4	EASA neposkytne USSP pravidla pro poskytování USSP, nebo stanoví USSP pravidla neúplně, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nepovažuje pravidla za potřebná, nebo – nezná přesnou roli USSP v ekosystému dronů	–EASA musí definovat všechna pravidla pro zajištění bezpečného provozu – EASA musí chápat roli USSP
Scenario 2.1	UCA-2.1	ÚCL nestanoví provozovateli pravidla pro umožnění provozu, nebo stanoví provozovateli pravidla neúplně, nebo protichůdně, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nezná harmonizovaná pravidla provozu, nebo – neví o provozovateli, nebo – neumí stanovit pravidla provozu, nebo – nezná provoz a neumí vyhodnotit, zdali postihlo všechna pravidla	–ÚCL musí znát harmonizovaná pravidla provozu –ÚCL musí mít přehled o provozovatelích – ÚCL musí stanovit pravidla provozu –ÚCL musí znát provoz a umět vyhodnotit, zdali jsou pravidla dostatečná
Scenario 2.2	UCA-2.2	ÚCL nestanoví provozovateli zodpovědnost, protože…	H1.2, H1.3	L1, L2, L3, L4, L7, L8	– neumí definovat zodpovědnosti, nebo – nemá představu o provozu a jeho potřebách	–ÚCL musí umět definovat zodpovědnosti a definovat je pro provoz – ÚCL musí mít představu o provozu a jeho potřebách
Scenario 2.3	UCA-2.3	ÚCL nedohlíží na dodržování pravidel, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nepovažuje dohled za potřebný – nepovažuje dodržování pravidel za potřebné – neví na co má dohlížet	– ÚCL musí dohlížet na dodržování pravidel
Scenario 2.4	UCA-2.4	ÚCL nestanoví CIS poskytovateli všechna pravidla pro předávání informací, nebo stanoví poskytovateli CIS pravidla neúplně, protože…	H3.3	L4	– nezná harmonizovaná pravidla provozu, nebo – neumí stanovit pravidla poskytování CIS, nebo – nechápe roli CIS	–ÚCL musí znát harmonizovaná pravidla provozu –ÚCL musí umět stanovit pravidla poskytování CIS –ÚCL musí chápat roli CIS
Scenario 2.5	UCA-2.5	ÚCL neposkytne CIS poskytovateli data pro předávání informací, nebo poskytne nesprávná data CIS poskytovateli, nebo poskytuje data pozdě, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– roli CIS si definovalo nesprávně, nebo – neví, co potřebuje CIS za data, nebo – nemá data pro CIS, nebo – neví, že poskytovaná data nejsou správná, nebo – nemá zavedeny efektivní procesy na poskytování dat	– ÚCL musí chápat roli CIS –ÚCL musí vědět, co potřebuje CIS za data –ÚCL musí zajistit všechna data pro CIS –ÚCL musí zajistit správnost dat poskytovaných pro CIS – ÚCL musí mít zavedeny efektivní procesy na poskytování dat
Scenario 2.6	UCA-2.6	ÚCL neposkytne USSP pravidla pro poskytování USSP, nebo stanoví USSP pravidla neúplně, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– neví o daném USSP, nebo – nezná pravidla pro a roli USSP, nebo – neumí definovat pravidla pro USSP	– ÚCL musí znát poskytovatele USSP – ÚCL musí chápat roli USSP –ÚCL musí definovat pravidla pro USSP

Scenario 2.7	UCA-2.7	ÚCL nestanoví pravidla na pilotování, nebo stanoví pilotovi pravidla neúplně, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– neví, co dělá pilot UAS	–ÚCL musí vědět, co dělá pilot UAS, jaká je jeho role
Scenario 2.8	UCA-2.8	ÚCL nestanoví zodpovědnosti pilota, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– neumí definovat zodpovědnosti, nebo – nemá představu o provozu a jeho potřebách	–ÚCL musí umět definovat zodpovědnosti a definovat je pro pilota –ÚCL musí mít představu o provozu a jeho potřebách
Scenario 2.9	UCA-2.10	ÚCL nestanoví pravidla létání, nebo stanoví pravidla létání neúplně, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	–nepovažuje stanovení pravidel létání za důležité, nebo – neumí stanovit pravidla provozu – nemá představu o provozu a jeho potřebách	–ÚCL musí správně stanovit pravidla provozu –ÚCL musí mít představu o provozu a jeho potřebách –musí umět stanovit pravidla provozu
Scenario 2.10	UCA-2.11	ÚCL necertifikuje ANSP, nebo nevydá pravidla poskytování, nebo ÚCL certifikuje ANSP nesprávně, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nepovažuje certifikaci za důležitou, nebo – nemá prostředky na certifikaci ANSP, nebo – necertifikuje dle daných pravidel	–ÚCL musí certifikovat ANSP dle daných pravidel –ÚCL musí mít prostředky na certifikaci ANSP
Scenario 3.1	UCA-3.1	K výměně dat z ANS ČR do USSP nedojde, nebo k výměně dat dojde, ale integrita dat bude narušena, nebo k výměně dat dojde pozdě, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– ANS ČR nepovažuje výměnu dat za důležitou, nebo – předání dat bylo přerušeno, nebo – neví, že poskytovaná data nejsou správná, nebo – nemají zavedeny efektivní procesy na poskytování dat	– musí vědět, co potřebuje USSP za data –musí zajistit všechna data pro USSP –musí zajistit správnost dat poskytovaných pro USSP –musí mít zavedeny efektivní procesy na poskytování da
Scenario 3.2	UCA-3.2	K výměně dat z USSP do ANS ČR nedojde, nebo k výměně dat dojde, ale integrita dat bude narušena, nebo k výměně dat dojde pozdě, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2	L1, L2, L3, L4, L7, L6, L8	– USSP nepovažuje výměnu dat za důležitou, nebo –předání dat bylo přerušeno, nebo – neví, že poskytovaná data nejsou správná, nebo – nemají zavedeny efektivní procesy na poskytování dat	–musí vědět, co potřebuje ANS ČR za data –musí zajistit všechna data pro ANS ČR –musí zajistit správnost dat poskytovaných pro ANS ČR –musí mít zavedeny efektivní procesy na poskytování dat
Scenario 4.1	UCA-4.1	Poskytovatel U-space služeb neposkytuje data pro aktivní geofencing, poskytuje nesprávná data pro aktivní geofencing, nebo poskytuje data pro aktivní geofencing v čase, kdy nejsou aktuální, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2	L1, L2, L3, L4, L7, L6, L8	– nemá informaci o tom, že má poskytovat data, nebo – nemá aktuální data k dispozici, nebo – neví, jak a kdy poskytovat správná data, nebo – nemá dostatečnou infrastrukturu pro poskytování dat v místě mise, nebo – si špatně vyložil pravidla	–poskytovatel U-space služeb musí poskytovat data dle smluv –poskytovatel U-space služeb musí mít k dispozici aktuální data – poskytovatel U-space služeb musí mít nastaveny procesy, jak a kdy poskytovat data –poskytovatel U-space služeb musí mít dostatečnou infrastrukturu pro poskytování dat v místě mise –poskytovatel U-space služeb musí poskytovat data dle pravidel
Scenario 4.2	UCA-4.2	Poskytovatel U-space služeb nenahlásí událost ÚZPLN, nebo nahlásí událost ÚZPLN nesprávně, nebo nahlásí událost ÚZPLN pozdě, protože...	H3.1, H3.2	L4, L6	– nemá informaci o tom, že má poskytovat hlášení o události, nebo – si špatně vyložil pravidla, nebo – nemá zavedeny efektivní procesy na poskytování hlášení	–musí mít informaci o tom, že musí poskytovat hlášení události –musí dodržovat pravidla –musí mít zavedeny efektivní procesy na poskytování hlášení –musí hlásit události
Scenario 5.1	UCA-5.1	Provozovatel nedá instrukce operátorovi k dosažení mise, když je třeba misi realizovat, nebo dá operátorovi instrukce k dosažení mise, které jsou protichůdné, nebo dá instrukce operátorovi k plnění mise moc pozdě, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– provozovatel neví, že má dát operátorovi instrukce, nebo –provozovatel neumí dát operátorovi správné instrukce, jelikož nezná pravidla/prostředí/techniku	– musí být doloženo, že provozovatel má jasně nastaveno, že každý člen podílející se na provozu má své instrukce pro všechny typy provozu provozovatele – provozovatel musí předat operátorovi správné instrukce
Scenario 5.2	UCA-5.2	Provozovatel neaktualizuje data v UAS, když je třeba je aktualizovat, nebo aktualizuje data v UAS neaktuální verzí, nebo aktualizuje data v UAS moc brzy, tedy nebudou aktuální v době mise, nebo aktualizuje data v UAS pouze částečně, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– provozovatel neví, že je třeba aktualizovat data v UAS, nebo - provozovatel neumí aktualizovat data v UAS, nebo – provozovatel neví, kdy je třeba aktualizovat data, nebo – provozovatel z pravidel nepochopil, že je třeba aktualizovat data v UAS	–provozovatel musí mít jasně stanovenu zodpovědnost za aktualizaci dat v UAS –v manuálu k UAS musí být popsáno, jak aktualizovat data v UAS –musí být stanoveno, jak často/kdy je nutné aktualizovat data v UAS

Scenario 5.3	UCA-5.3	Provozovatel nedá poskytovateli výcviku instrukce k zajištění potřebného výcviku pro definovaný provoz, nebo dá poskytovateli výcviku instrukce k zajištění výcviku, které neodpovídají provozu, nebo dá instrukce poskytovateli výcviku moc pozdě, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– provozovatel neumí dát poskytovateli výcviku správné instrukce, jelikož nezná pravidla/prostředí/techniku, nebo – provozovatel nezná pravidla standardního scénáře a nemůže dát poskytovateli výcviku správné instrukce, nebo – provozovatel pracuje neefektivně a nepředává včas informace	–musí být stanovena pravidla na poskytnutí výcviku pro určitý provoz, –provozovatel musí definovat místa provozu a mise, aby podle nich definoval instrukce pro poskytovatele výcviku pilotovi, –provozovatel musí vědět, jaký standardní scénář chce využívat a tuto informaci poskytnout poskytovateli výcviku, –provozovatel musí poskytnout instrukce poskytovateli výcviku s dostatečným předstihem, aby ten se na výcvik mohl připravit,
Scenario 5.4	UCA-5.4	Provozovatel nedá pozorovateli instrukce k poskytování informací pilotovi pro definovaný provoz, nebo dá pozorovateli instrukce k poskytování informací, které jsou nesprávné, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– provozovatel neví, že má dát pozorovateli instrukce, nebo – provozovatel neumí dát pozorovateli správné instrukce, jelikož nezná pravidla, nebo – provozovateli nebyla poskytnuta pravidla, a tedy je nemůže předat pozorovateli, nebo – pravidla jsou protichůdně nastavena, nebo – pravidla nejsou provozovatelem správně pochopena	– provozovatel musí mít povinnost dát pozorovateli instrukce, –provozovatel musí znát pravidla a dle nich dát pozorovateli správné instrukce –musí být stanovena pravidla pro provozovatele, jak začlenit pozorovatele
Scenario 5.5	UCA-5.5	Provozovatel nedá poskytovateli U-space služeb instrukce k poskytování služeb při provozu, nebo dá poskytovateli U-space služeb špatné/nedostatečné instrukce k poskytování služeb, nebo instrukce k poskytování služeb dá moc pozdě, nebo instrukce k poskytování služeb nezajistil na dost dlouho, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2, H3.1 H3.2	L1, L2, L3, L4, L7, L6, L8	– provozovatel neví, že musí využívat U-space služby, nebo –provozovatel nemá představu o místě provozu, nebo – provozovatel nezajistil poskytování U-space služeb včas, nebo – provozovatel uzavřel špatný smluvní vztah s poskytovatelem U-space služeb, nebo – provozovatel nepovažuje služby U-space za potřebné	–musí být definováno kdy a kde je povinností využívat jaké služby U-space –musí být k dispozici informace, kdo je certifikovaným poskytovatelem služeb U-space –provozovatel musí být zodpovědný za provoz a za definování místa provozu – provozovatel musí zajistit, aby služby U-space byly dostupné při celém trvání mise
Scenario 6.1	UCA-6.1	Pilot neposkytuje řídící impulsy pro vykonání potřebných pohybů UA, když je to potřebné pro let, nebo poskytuje špatné řídící impulsy pro vykonání potřebných pohybů UA, nebo poskytuje řídící impulsy moc brzy nebo moc pozdě, nebo poskytuje řídící signály moc krátké, nebo moc dlouhé, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– není vycvičen pro daný provoz, nebo –není seznámen s provozní příručkou provozovatele, nebo – není seznámen s manuálem k UAS, nebo – není seznámen s misí, nebo – nemá schopnosti pro pilotování UAS, nebo – neprovedl koordinaci s pozorovatelem a chybí mu správné informace	– pilot musí být vycvičen pro daný provoz – pilot musí být seznámen s provozní příručkou provozovatele – pilot musí být seznámen s misí – pilot musí mít schopnosti pro pilotování UAS – pilot musí provést koordinaci s pozorovatelem ohledně výměny informací
Scenario 6.2	UCA-6.2	Pilot nenastaví UAS před letem, nebo nastaví UAS před letem v rozporu s misí, provozní příručkou, manuálem, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– není seznámen s provozní příručkou, manuálem UAS, misí, nebo – nezná pravidla pro nastavení UAS, nebo – neví, že je nutné nastavit UAS před letem, nebo – nepovažuje nastavení UAS před letem za potřebné	– pilot musí být vycvičen pro daný UAS – pilot musí být seznámen s provozní příručkou provozovatele – pilot musí být seznámen s manuálem k UAS pro nastavení UAS – pilot musí být seznámen s misí – pilot musí mít schopnosti pro nastavení UAS – pilot musí být seznámen s nutností nastavení UAS před letem
Scenario 7.1	UCA-7.1	Operátor neposkytuje řídící impulsy pro zamýšlené funkce doplňkových zařízení, nebo poskytuje špatné řídící impulsy pro doplňková zařízení, nebo poskytuje řídící impulsy moc brzy nebo moc pozdě, nebo poskytuje řídící signály moc krátké, nebo moc dlouhé, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– není vycvičen pro daný provoz, nebo – není seznámen s provozní příručkou provozovatele, nebo – není seznámen s manuálem k zařízení, nebo – není seznámen s misí, nebo – nemá schopnosti pro ovládání zařízení	– operátor musí být vycvičen pro daný provoz –operátor musí být seznámen s provozní příručkou provozovatele – operátor musí být seznámen s manuálem k zařízení – operátor musí být seznámen s misí –operátor musí mít schopnosti pro ovládání zařízení
Scenario 8.1	UCA-8.1	Ovládací stanice neposkytne UA řídící signál pro činnost, nebo poskytne UA špatný signál pro činnost, nebo poskytne UA řídící signál pro činnost pozdě, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nedetekuje vstupní impulsy, nebo – došlo k poruše při přenosu do UA, nebo – došlo k poruše ovládací stanice a ta vysílá řídící signál omezeně	– ovládací stanice musí být bezpečná při poruše – ovládací stanice se nesmí porouchat –přenos signálů do UAS musí být funkční – UAS se štítkem musí být vyroben v souladu s požadavky třídy,

Scenario 8.2	UCA-8.2	Ovládací stanice nepřijme nebo nezobrazí U-space služby, nebo přijme nebo zobrazí nesprávné informace, nebo přijme nebo zobrazí informace pozdě, nebo přestane přijímat nebo zobrazovat informace, protože...	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– došlo k poruše ovládací stanice a ta nepřijímá U-space služby, – došlo k poruše při zobrazování U-space služeb, – došlo k poruše ovládací stanice a ta zobrazuje nesprávné informace	– ovládací stanice se nesmí porouchat
Scenario 9.1	UCA-9.1	Poskytovatel výcviku nevycvičí pilota dle požadavků provozovatele, nebo nevycvičí pilota dle pravidel, nebo poskytne neúplný výcvik, nebo poskytne výcvik, který není v souladu s pravidly, protože…	H1.1, H1.2, H1.3, H1.4, H1.5, H2.1, H2.2	L1, L2, L3, L4, L7, L8	– nezná harmonizovaná pravidla, nebo – neobdržel definované pokyny pro výcvik, nebo –neumí vycvičit pilota	–poskytovatel výcviku musí znát harmonizovaná pravidla – poskytovatel výcviku musí dostat pokyny pro výcvik –poskytovatel výcviku musí mít schopnosti a možnosti vycvičit pilota

Příloha 5 Model FRAM



	Aspekty			
Funkce	***Vstup***	***Výstup***	***Řízení***	***Podmínka***
Stanovit pravidla provozu U-space		stanovená pravidla		
Stanovit pravidla pro poskytování U-space služeb		pravidla poskytování U-space služby		
Stanovit pravidla certifikace		pravidla certifikace		
Stanovit pravidla pro registraci provozovatele	stanovená pravidla	pravidla pro registraci provozovatele		
Stanovit pravidla pro certifikaci zapojeného subjektu	pravidla certifikace	pravidla pro certifikaci zapojeného subjektu	stanovená pravidla	
Stanovit pravidla pro poskytování U-space služeb v ČR	pravidla poskytování U-space služby	pravidla poskytování U-space služeb v ČR	stanovená pravidla	
Splnit povinnosti provozovatele	stanovená pravidla	-provozní postupy -registrace provozovatele	pravidla pro registraci provozovatele	
Stanovit cíl provozu		cíl provozu definován	stanovená pravidla	
Získat certifikaci poskytovatele U-space služeb	stanovená pravidla	certifikace poskytovatele U-space služby	pravidla pro certifikaci zapojeného subjektu	
Vyhodnotit přijímaná data	zpracovaná data	vyhodnocená data	pravidla poskytování U-space služeb v ČR	
Poskytovat specifickou U-space službu dle stanovených pravidel	- vyhodnocená data - cíl provozu definován	*U-space služba*	pravidla poskytování U-space služeb v ČR	certifikace poskytovatele U-space služby
Získat certifikaci dálkově řídícího pilota	teoretický a praktický výcvik posádky	certifikace dálkově řídícího pilota	pravidla pro certifikaci zapojeného subjektu	
Řídit se provozními postupy provozovatele	provozní postupy	provozní postupy splněny		- registrace provozovatele - certifikace dálkově řídícího pilota
Splnit teoretický a praktický výcvik posádky	provozní postupy splněny	teoretický a praktický výcvik posádky		
Seznámit se s cílem mise	cíl mise definován	*požadavky na techniku*		
Získat certifikaci CIS poskytovatele	pravidla pro certifikaci zapojeného subjektu	certifikace CIS poskytovatele		
Sběr a dodání dat	- data o poloze - data o provozu	zpracovaná data	stanovená pravidla	certifikace CIS poskytovatele
Získat certifikaci ATSP	pravidla pro certifikaci zapojeného subjektu	certifikace ATSP		
Poskytovat data o provozu letadel s pilotem na palubě		data o provozu	stanovená pravidla	certifikace ATSP
Získat certifikaci ANSP	pravidla pro certifikaci zapojeného subjektu	certifikace ANSP		

Poskytovat data o poloze letadel s pilotem na palubě		data o poloze	stanovená pravidla	certifikace ANSP

Příloha 6 Identifikace variability

			Čas				Přesnost		
Funkce	***Typ funkce***	***Výstup***	***příliš brzy***	***na čas***	***příliš pozdě***	***vůbec***	***nepřesné***	***přijatelné***	***přesné***
Stanovit pravidla provozu U-space	organizační	stanovená pravidla			-	negativní	negativní	negativní	
Stanovit pravidla pro poskytování U-space služeb	organizační	pravidla poskytování U-space služby			-	negativní	negativní	negativní	
Stanovit pravidla certifikace	organizační	pravidla certifikace			-	negativní	negativní	negativní	
Stanovit pravidla pro registraci provozovatele	organizační	pravidla pro registraci provozovatele			negativní	negativní	negativní	negativní	
Stanovit pravidla pro certifikaci zapojeného subjektu	organizační	pravidla pro certifikaci zapojeného subjektu			-	negativní	negativní	negativní	
Stanovit pravidla pro poskytování U-space služeb v ČR	organizační	pravidla poskytování U-space služeb v ČR			-	negativní	negativní	negativní	
Splnit povinnosti provozovatele	lidská	provozní postupy			negativní	negativní	negativní		
		registrace provozovatele			negativní	negativní	negativní	-	
Stanovit cíl provozu	lidská	cíl provozu definován			negativní	negativní	negativní		
Získat certifikaci poskytovatele U-space služeb	organizační	certifikace poskytovatele U-space služby			negativní	negativní	-	-	
Vyhodnotit přijímaná data	organizační	vyhodnocená data	-		negativní	negativní	negativní		
Poskytovat specifickou U-space službu dle stanovených pravidel	organizační	*U-space služba*			negativní	negativní	negativní		
Získat certifikaci dálkově řídícího pilota dle ÚCL	lidská	licence dálkově řídícího pilota			negativní	negativní	-	-	
Řídit se provozními postupy provozovatele	lidská	provozní postupy splněny			negativní	negativní	negativní		
Splnit teoretický a praktický výcvik posádky	lidská	teoretický a praktický výcvik posádky			negativní	negativní	negativní		
Seznámit se s cílem mise	lidská	požadavky na techniku			negativní	negativní	negativní	negativní	
Získat certifikaci CIS poskytovatele	organizační	certifikace CIS poskytovatele			negativní	negativní	-		
Sběr a dodání dat	organizační	zpracovaná data	-		negativní	negativní	negativní		

Poskytovat data o provozu letadel s pilotem na palubě	organizační	data o provozu	negativní		negativní	negativní	negativní	negativní	
Získat certifikaci ATSP	organizační	certifikace ATSP			negativní	negativní	-		
Získat certifikaci ANSP	organizační	certifikace ANSP			negativní	negativní	-		
Poskytovat data o poloze letadel s pilotem na palubě	organizační	data o poloze	negativní		negativní	negativní	negativní	negativní	

Příloha 7 Požadavky na systém U-space

- EASA musí definovat pravidla. *2019/947, článek 19, 3., s. 14*
- EASA musí vytvořit výklad pravidel. *2019/947, článek 19, 3., s. 14*
- EASA musí mít představu o reálné problematice létání. *2019/947, článek 19, 3., s. 14*
- EASA musí vědět, jak vypadá provoz ve státech EU. *2019/947, článek 19, 3., s. 14*
- EASA musí zajistit, že dozor nad provozem je definován. *2019/947, článek 18, h), s. 13*
- EASA musí zajistit, že je uzavřena smlouva mezi EASA a ÚCL. *49/1997, § 3, (3), s. 3*
- EASA musí zajistit aktuálnost pravidel pro vykonávání dozoru, aby postihovaly provoz. *2019/947, článek 19, 3., s. 14*
- EASA musí vědět, jak dělat dozor. *2019/947, článek 19, 3., s. 14*
- EASA musí definovat všechna pravidla pro zajištění bezpečného provozu. *2019/947, článek 19, 3., s. 14*
- EASA musí zajistit, že uživatelská příručka UAS je vytvořena správně u každého UAS. *2019/945 článek 6, 7., s. 9*
- EASA musí mít expertní znalosti pro posouzení možných dopadů provozu. *2019/947 článek 19, 3., s. 14*
- EASA musí definovat všechna pravidla pro zajištění bezpečného provozu. *2019/947 článek 19, 3., s. 14*
- EASA musí chápat roli USSP. *2019/947 článek 19, 3., s. 14*
- ÚCL musí znát harmonizovaná pravidla provozu. *2019/947 článek 18, 1., s. 13*
- ÚCL musí mít přehled o provozovatelích. *2019/947 článek 14, 1. a 4., s. 11*
- ÚCL musí stanovit pravidla provozu. *2019/947 článek 18, 1., s. 13*
- ÚCL musí znát provoz a umět vyhodnotit, zdali jsou pravidla dostatečná. *2019/947 článek 12, 1.,2.,3., s. 9 (platí pro specific a certified)*
- ÚCL musí umět definovat zodpovědnosti a definovat je pro provoz. *2019/947, článek 18 , s. 13*
- ÚCL musí mít představu o provozu a jeho potřebách. *2021/664, článek 17, 1. s. 13*
- ÚCL musí dohlížet na dodržování pravidel. *49/1997 zákon o civilním letectví, § 3, (5), s. 3*
- ÚCL musí znát harmonizovaná pravidla provozu. *2019/947 článek 18, s. 13*
- ÚCL musí umět stanovit pravidla poskytování CIS. *2021/664 (12) s. 2*
- ÚCL musí chápat roli CIS. *2021/664 článek 18, s. 13*
- ÚCL musí chápat roli CIS. *2021/664 článek 18, s. 13*
- ÚCL musí vědět, co potřebuje CIS za data. *2021/664 (14) s. 2*
- ÚCL musí zajistit všechna data pro CIS. *2021/664 (14) s. 2*
- ÚCL musí zajistit správnost dat poskytovaných pro CIS. *2021/664 (14) s. 2*

- ÚCL musí mít zavedeny efektivní procesy na poskytování dat. *2021/664 (14) s. 2*
- ÚCL musí znát USSP. *2021/664, článek 18 a), s. 13*
- ÚCL musí chápat roli USSP. *2021/664, článek 18, s.13*
- ÚCL musí definovat pravidla pro USSP. *2021/664 (12) s. 2*
- ÚCL musí vědět, co dělá pilot UAS, jaká je jeho role. *2019/947, článek 16, 2) b) i) s. 12 a 2019/947 článek 18 b), c) s. 13*
- ÚCL musí umět definovat zodpovědnosti a definovat je pro pilota. *2019/947, příloha, část A, UAS.OPEN.060 Povinnosti dálkově řídícího pilota a 2019/947 část B, UAS.SPEC.060 Povinnosti dálkově řídícího pilota*
- ÚCL musí mít představu o provozu a jeho potřebách. *2021/664, článek 17, 1. s. 13*
- ÚCL musí chápat roli ATSP a důležitost vydání osvědčení. *550/2004 článek 7 odst. 1*
- ÚCL musí vydat osvědčení včas. *2019/947, příloha, část B, UAS.SPEC.040, 1) s. 21*
- ÚCL musí správně stanovit pravidla provozu. *2019/947 článek 18, a)., s. 13*
- ÚCL musí mít představu o provozu a jeho potřebách. *2021/664, článek 17, 1. s. 13*
- ÚCL musí umět stanovit pravidla provozu. *2019/947 článek 18, a), s. 13*
- ÚCL musí certifikovat ANSP dle daných pravidel. *550/2004 článek 7 odst. 1*
- ÚCL musí mít prostředky na certifikaci ANSP. *550/2004 článek 7 odst. 1*
- ANS ČR musí vědět, co potřebuje USSP za data. *2021/665 článek I, 2), a), s. 2*
- ANS ČR musí zajistit všechna data pro USSP. *2021/665 článek I, 2), a), s. 2*
- ANS ČR musí zajistit správnost dat poskytovaných pro USSP. *2021/665 článek I, 2), a), s. 2*
- ANS ČR musí mít zavedeny efektivní procesy na poskytování dat. *2021/665 článek I, 2), b), s. 2*
- USSP musí vědět, co potřebuje ANS ČR za data. *2021/664, článek 7, 3., s. 8*
- USSP musí zajistit všechna data pro ANS ČR. *2021/664, příloha V, 1., s. 19*
- USSP musí zajistit správnost dat poskytovaných pro ANS ČR. *2021/664, článek 7, 3., s. 8*
- USSP musí mít zavedeny efektivní procesy na poskytování dat. *2021/664, článek 7, 3., s. 8*
- Poskytovatel U-space služeb musí poskytovat data dle smluv. *2021/664, článek 5, 4. s. 7*
- Poskytovatel U-space služeb musí mít k dispozici aktuální data. *2021/664 (15) s. 2*
- Poskytovatel U-space služeb musí mít nastaveny procesy, jak a kdy poskytovat data. *2021/664 článek 7, 2., s. 8, a 2021/664, příloha III, s. 17*
- Poskytovatel U-space služeb musí mít dostatečnou infrastrukturu pro poskytování dat v místě mise. *2017/ 373, hlava B, ATM/ANS.OR.B.001, s. 33*
- Poskytovatel U-space služeb musí poskytovat data dle pravidel. *2021/664, článek 5, 4. s. 7*
- **USSP musí mít informaci o tom, že musí poskytovat hlášení události.**
- **USSP musí dodržovat pravidla.**
- USSP musí mít zavedeny efektivní procesy na poskytování hlášení. *376/2014, článek 4, 2., s. 10*
- USSP musí hlásit události. (vyplývá z) *376/2014, článek 4, 8., s. 10*

- Musí být doloženo, že provozovatel má jasně nastaveno, že každý člen podílející se na provozu má své instrukce pro všechny typy provozu provozovatele. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 4), s. 18*
- Provozovatel musí předat operátorovi správné instrukce. *2019/ 947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 4), s. 18*
- Provozovatel musí mít jasně stanovenu zodpovědnost za aktualizaci dat v UAS. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 5), s. 18*
- V manuálu k UAS musí být popsáno, jak aktualizovat data v UAS. *2019/945, příloha, část 2, 18) c) s. 26 a následně v částech 3 i 4*
- Musí být stanoveno, jak často/kdy je nutné aktualizovat data v UAS. *2019/947, příloha, část A, UAS.OPEN.060 Povinnosti dálkově řídícího pilota 1)b) s. 19, a část B, UAS.OPEN.060 Povinnosti dálkově řídícího pilota 2)a) s. 23,*
- **Musí být stanovena pravidla na poskytnutí výcviku pro určitý provoz.**
- **Provozovatel musí definovat místa provozu a mise, aby podle nich definoval instrukce pro poskytovatele výcviku pilotovi.**
- **Provozovatel musí vědět, jaký standardní scénář chce využívat a tuto informaci poskytnout poskytovateli výcviku.**
- **Provozovatel musí poskytnout instrukce poskytovateli výcviku s dostatečným předstihem, aby ten se na výcvik mohl připravit.**
- Provozovatel musí mít povinnost dát pozorovateli instrukce. *eRules Dodatek 1, UAS.STS-01.030, 9b),*
- Provozovatel musí znát pravidla a dle nich dát pozorovateli správné instrukce. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 4), s. 18*
- Musí být stanovena pravidla pro provozovatele, jak začlenit pozorovatele. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 4), s. 18*
- Musí být definováno kdy a kde je povinností využívat jaké služby U-space. *2021/664, článek 3, 2., 3. s. 5*
- Musí být k dispozici informace, kdo je certifikovaným poskytovatelem služeb U-space. *2021/664, Článek 5, 1. (c)*
- Provozovatel musí být zodpovědný za provoz a za definování místa provozu. *2019/947, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů 1) a 2019/947, UAS.SPEC.050 Povinnosti provozovatele bezpilotních systémů 1)a)*
- Provozovatel musí zajistit, aby služby U-space byly dostupné při celém trvání mise. *2019/947, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů 1) a 2019/947, UAS.SPEC.050 Povinnosti provozovatele bezpilotních systémů 1)a)*
- Pilot musí být vycvičen pro daný provoz. *2019/947 UAS.SPEC.050 1)d) s. 22 (zodpovědnost provozovatele)*

- Pilot musí být seznámen s provozní příručkou provozovatele. *2019/947 UAS.SPEC.050 1)d)v) s. 22 (zodpovědnost provozovatele)*
- Pilot musí být seznámen s misí. *2019/947 UAS.SPEC.060 2)a) s. 23*
- Pilot musí mít schopnosti pro pilotování UAS, vychází z povinnosti výcviku. *2019/947 UAS.SPEC.050 1)d) s. 22 (zodpovědnost provozovatele)*
- Pilot musí provést koordinaci s pozorovatelem ohledně výměny informací. *2019/947 UAS.STS-01.040, 2)(b) s. 233*
- Pilot musí být vycvičen pro daný UAS. *2019/947 UAS.SPEC.050 1)d) s. 22 (zodpovědnost provozovatele)*
- Pilot musí být seznámen s provozní příručkou provozovatele. *2019/947 UAS.SPEC.050 1)d)v) s. 22 (zodpovědnost provozovatele)*
- Pilot musí být seznámen s manuálem k UAS pro nastavení UAS, vychází z povinnosti výcviku. *2019/947 UAS.SPEC.050 1)d) s. 22 (zodpovědnost provozovatele)*
- Pilot musí být seznámen s misí. *2019/947 UAS.SPEC.050 1)d)vi) s. 22 (zodpovědnost provozovatele)*
- Pilot musí mít schopnosti pro nastavení UAS. *2019/947 UAS.SPEC.050 1)d) s. 22 (vychází z povinnosti výcviku)*
- Pilot musí být seznámen s nutností nastavení UAS před letem. *2019/947, UAS.SPEC.060 2)c), s. 23*
- Operátor musí být vycvičen pro daný provoz. *2019/947, UAS.SPEC.050 1)e), s. 22*
- Operátor musí být seznámen s provozní příručkou provozovatele. *2019/947 UAS.SPEC.050 1)e), s 22*
- Operátor musí být seznámen s manuálem k zařízení. *2019/947, příloha UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů 4), s. 18*
- Operátor musí být seznámen s misí. *2019/947 UAS.SPEC.050 1)e), s. 22*
- Operátor musí mít schopnosti pro ovládání zařízení. *2019/947, příloha UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů 4) a) s. 18*
- Ovládací stanice musí být bezpečná při poruše. *2019/947 UAS.SPEC.050 1)h), s. 22*
- **Ovládací stanice se nesmí porouchat.**
- Přenos signálů do UAS musí být funkční. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 2), s. 18*
- UAS se štítkem musí být vyroben v souladu s požadavky třídy. *2019/947, příloha, část A, UAS.OPEN.050 Povinnosti provozovatele bezpilotních systémů, 6), s. 18*
- **Ovládací stanice se nesmí porouchat.**
- **Poskytovatel výcviku musí znát harmonizovaná pravidla.**
- **Poskytovatel výcviku musí dostat pokyny pro výcvik.**

- **Poskytovatel výcviku musí mít schopnosti a možnosti vycvičit pilota.**