ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

ÚSTAV LETECKÉ DOPRAVY

SYSTÉMOVÉ ŘÍZENÍ NEPLÁNOVANÝCH ZMĚN V RÁMCI STÁTNÍHO PROGRAMU BEZPEČNOSTI

DIPLOMOVÁ PRÁCE

BC. KATEŘINA ŠKODOVÁ

VEDOUCÍ PRÁCE: DOC. ING. ANDREJ LALIŠ, PH.D.

PRAHA 2022

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

K621.....Ústav letecké dopravy

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Kateřina Škodová

Studijní program (obor/specializace) studenta:

navazující magisterské –PL– Provoz a řízení letecké dopravy

Název tématu (česky): **Systémové řízení neplánovaných změn v rámci státního programu bezpečnosti**

Název tématu (anglicky): **Systemic Change Management of Unplanned Changes in State Safety Programme**

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je navrhnout postup a klíčové prvky státního programu bezpečnosti pro identifikaci a řízení neplánovaných změn v leteckém provozu s využitím systémového přístupu k bezpečnosti.
- Analyzujte legislativní rámec a standardy pro státní programy bezpečnosti v kontextu řízení neplánovaných změn
- Analyzujte současné metody systémového přístupu k bezpečnosti
- Vyberte a specifikujte systém dozoru státu nad konkrétním typem letecké organizace v kontextu řízení neplánovaných změn
- Navrhněte postup dozorové činnosti státu a klíčové prvky pro státní program bezpečnosti založený na systémovém přístupu k bezpečnosti pro identifikaci a řízení neplánovaných změn
- Navržené řešení ověřte a vyhodnoťte

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

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

Seznam odborné literatury: ICAO Doc 9859: Safety Management Manual. 4. Edition, 2018.
Leveson, Nancy. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.

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

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. -3-

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. Kateřina Škodová
jméno a podpis studenta

V Praze dne 16. července 2021

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 16.5.2022

Bc. Kateřina Škodová

Poděkování

Ráda bych poděkovala vedoucímu mé diplomové práce Doc. Ing. Andreji Lališovi, Ph.D. za jeho cenné rady a připomínky a za jeho vstřícnost a trpělivost, kterou mi poskytl během psaní této práce.

Abstrakt

Cílem této diplomové práce bylo vytvoření návrhu pro řízení neplánovaných změn v rámci SSP (Státní program bezpečnosti) s využitím systémového přístupu. Teoretická část práce se věnuje popisu neplánovaných změn v rámci provozní bezpečnosti, SSP a současným přístupům k řízení neplánovaných změn včetně systémového přístupu modelu STAMP (Systémově-teoretický model nehod a procesů) a současného přístupu k neplánovaných změnám v rámci ÚCL (Úřad pro civilní letectví). V praktické části byl na základě výběru vhodného způsobu k řízení neplánovaných změn vytvořen návrh pro řízení neplánovaných změn v rámci SSP, který využívá myšlenky systémového přístupu modelu STAMP a jeho analýz. Závěr práce byl věnován validaci stanoveného návrhu na procesu technického odbavení a nehodě, která se stala během technického odbavení.

Klíčová slova: provozní bezpečnost, neplánované změny, řízení neplánovaných změn, státní program bezpečnosti, Systémově-teoretický model nehod a procesů, Systémově-teoretická analýza procesů, Analýza příčin na základě Systémové teorie, Aktivní Systémově-teoretický model nehod a procesů, systémový přístup, dozorový orgán nad civilním letectvím, systém státní správy a dozoru civilního letectví

Abstract

The objective of the master's thesis is to create a proposal of systemic change management of unplanned changes within SSP (State Safety Programme). The theoretical part of the thesis is dedicated to explanation of unplanned changes in safety, SSP and nowadays approaches to change management of unplanned changes including the systemic approach of STAMP (System-Theoretic Accident Model and Processes) and nowadays approach of CAA (Civil Aviation Authority) of the Czech Republic. In the practical part of the thesis proposal of change management of unplanned changes within SSP is created with usage of systemic approach of STAMP and its analysis. Final part of the thesis is dedicated to validation of the proposal, where process of ground handling and accident of ground handling are used.

Keywords: safety, unplanned changes, management of unplanned changes, State Safety Programme, System-Theoretic Accident Model and Processes, System-Theoretic Process Analysis, Causal Analysis based on System Theory, Active System-Theoretic Process Analysis, systemic approach, Civil Aviation Authority, civil aviation safety oversight system

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AAII	Air Accident Investigation Institute	Institut pověřený šetřením leteckých nehod
ADREP	Accident/Incident Data Reporting	-
AHAI	Active Hazard Analysis Input	Vstup aktivní analýzy nebezpečí
ALoSP	Acceptable Level of Safety Performance	Přijatelná úroveň výkonnosti bezpečnosti
ARMS	Aviation Risk Management Solutions	Řešení pro řízení rizik v letectví
CAST	Causal Analysis based on System Theory	Analýza příčin na základě Systémové teorie
CAA	Civil Aviation Authority	Dozorový orgán nad civilním letectvím
D3M	Data-driven decision-making	Rozhodování na základě dat
EASA	European Union Aviation Safety Agency	Evropská agentura pro bezpečnost letectví
ECCAIRS	European Co-ordination Centre for Accident and Incident Reporting Systems	Evropské koordinační středisko pro nahlašování nehod a incidentů
ERC	Event Risk Classification	Klasifikace rizika události
EU	European Union	Evropská unie
FHA	Functional Hazard Assessment	Vyhodnocování funkčních nebezpečí
FOD	Foreign Object Damage	Poškození cizím předmětem
IB	-	Inspektor bezpečnosti
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
JRC	Joint Research Centre	Společné výzkumné středisko
LAA	-	Letecká amatérská asociace
LGAV	Athens International Airport	Mezinárodní letiště Athény
LGPA	Paros National Airport	Národní letiště Paros
MCAS	Maneuvering Characteristics Augmentation System	Systém rozšiřování charakteristik manévrování

MD ČR	Ministry of Transport of the Czech Republic	Ministerstvo dopravy ČR
M/MS	-	Manažer systému řízení
MoC	Management of Change	Řízení změn
NFC ČR	National Facilitation Committee of the Czech Republic	-
OOP	-	Osobní ochranné prostředky
PSSA	Preliminary System Safety Assessment	Předběžné vyhodnocování bezpečnosti systému
SAG	Safety Action Group	Skupina pro řešení otázek bezpečnosti
SAM	Safety Assessment Methodology	Metodika vyhodnocování bezpečnosti
SISeI	Safety Intelligence System	Bezpečnostní informační systém ÚCL
SMM	Safety Management Manual	Příručka pro řízení bezpečnosti
SMS	Safety Management System	Systém řízení bezpečnosti
SRBS	Safety Risk-Based Surveillance	Dozor založený na bezpečnostním riziku
SRM	Safety Risk Management	Řízení bezpečnostního rizika
SSA	System Safety Assessment	Vyhodnocování bezpečnosti systému
SSp	State Safety Plan	Státní plán bezpečnosti
SSP	State Safety Program	Státní program bezpečnosti
STAMP	System-Theoretic Accident Model and Processes	Systémově-teoretický model nehod a procesů
STPA	System-Theoretic Process Analysis	Systémově-teoretická analýza procesů
TRA	Temporary Reserved Area	Dočasně rezervovaný prostor
UCA	Unsafe Control Action	Nebezpečná řídicí akce
ÚCL	Civil Aviation Authority of the Czech Republic	Úřad pro civilní letectví ČR
ÚZPLN	Air Accidents Investigation Institute of the Czech Republic	Ústav pro odborné zjišťování příčin leteckých nehod ČR

1 Úvod

Systém letecké dopravy a zejm. té civilní je složitý socio-technický systém, který se skládá z mnoha subsystémů dozorových orgánů, provozovatelů letišť, údržbových organizací, leteckých společností atd. Tyto subsystémy se skládají zejm. z moderní a složité techniky, infrastruktury a také kvalifikovaného personálu, který se společně podílí na denním provozu letecké dopravy. Spojením těchto subsystémů vzniká dynamické prostředí letecké dopravy, které neustále vyvíjí tlak na inovace v tomto systému. Ať už se v letecké dopravě jedná o alternativní paliva, nové postupy v rámci řízení leteckého provozu, úspornější motory nebo vyšší požadavky na provozní bezpečnost, které jsou vytvářeny na základě velmi nízké úrovně tolerance společnosti v tomto století vůči nehodám a incidentům letecké dopravy.

V systému civilní letecké dopravy, stejně jako ve všech ostatních v čase se vyvíjejících systémech, se dějí určité změny. Ty mohou být plánované, tedy změny prováděné s vědomím a úmyslem něco změnit (např. výstavba nového terminálu), anebo jsou změny neplánové neboli ty, které probíhají nekoordinovaně bez jakéhokoliv záměru. Druhý typ změny je obvykle vyvolán špatně implementovanou plánovanou změnou, dlouhodobým příznivým stavem provozní bezpečnosti nebo nečekanou událostí, na kterou systém není připraven. Jedním z důkazů, že neplánované změny hrají významnou roli v provozní bezpečnosti, mohou být např. letecké nehody spojené s letadlem B-737 MAX, ve kterém byl nově implementován systém MCAS (Systém rozšiřování charakteristik manévrování). Plánovaná změna vyvolala v systému letecké dopravy neplánované změny, na které systém nebyl připravený, a jejich vlivem se poté staly dvě katastrofální nehody se ztrátami na lidských životech. Plánované i neplánované změny ovlivňují provozní bezpečnost, a proto je nutné se jimi zabývat.

Nástroj, který je v současnosti využíván subjekty civilního letectví pro řízení, měření a zlepšování provozní bezpečnosti, se nazývá SMS (Systém řízení bezpečnosti). Na úrovni státu a dozorových orgánů je SMS zahrnut v dokumentu SSP (Státní program bezpečnosti), který popisuje přístup a řízení provozní bezpečnosti daného státu. Součástí SSP je rovněž řízení změn, které se zabývá zejm. plánovanými změnami a dozorovou činností nad tímto procesem. Neplánované změny jsou řízeny nepřímo pomocí měření a hodnocení výkonnosti v bezpečnosti, kdy na základě zvýšených ukazatelů se zvažuje, zda jedním z důvodů nebyla nějaká neplánovaná změna.

Tento způsob identifikace a řízení neplánovaných změn v rámci SSP není efektivní mimo jiné proto, že mnohdy zachytí neplánovanou změnu až v případě, kdy zapříčinil leteckou nehodu nebo incident. S pomocí modelu STAMP (Systémově-teoretický model nehod a procesů) lze přistupovat k provozní bezpečnosti (i k neplánovaným změnám) systémově, a neplánované změny tak zachytit předtím, než vznikne jejich důsledkem nějaká ztráta.

Tato práce je zaměřena právě na výše zmíněnou problematiku identifikace a řízení neplánovaných změn v rámci SSP. Cílem práce je vytvořit návrh pro identifikaci a řízení neplánovaných změn v rámci SSP na základě vybraného systémového přístupu. Návrh by měl pomoci dozorovým orgánům k efektivnější identifikaci a řízení neplánovaných změn, což může v důsledku včasného provedení předejít závažným leteckým nehodám a incidentům, a pozitivně tak ovlivnit provozní bezpečnost.

2 Bezpečnost a změny

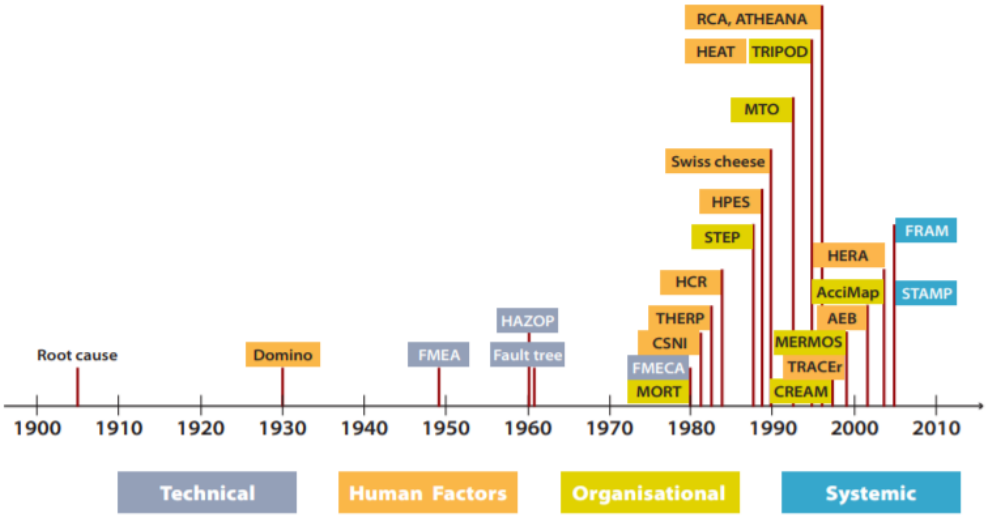
Bezpečnost v letecké dopravě je řešena již od počátků vzniku obchodní letecké přepravy a zvyšování objemu přepravovaných cestujících. I přes nespočet bezpečnostních modelů, analýz a postupů je třeba se bezpečnosti stále aktivně věnovat a snažit se ji vést kupředu pomocí nových metod, které budou lépe reflektovat aktuální problémy bezpečnosti. Důvodů, proč i v dnešní době je tak důležité se zabývat zlepšováním úrovně bezpečnosti, je několik. Patří mezi ně např. nové hrozby, které vznikají rychlým technologickým pokrokem, snížená možnost učit se z určitých událostí vlivem jejich nízké četnosti, snižování tolerance nehodovosti nebo celkově navyšující se komplexnost systémů a jejich problémů. [1]

2.1 Provozní bezpečnost

Provozní bezpečnost se zaměřuje na události z běžného provozu letecké dopravy kromě událostí, kterými se zabývá ochrana před protiprávními činy. Toto odvětví bezpečnosti se snaží zamezit událostem vedoucím k jakékoliv nepřijatelné ztrátě pro společnost a leteckou dopravu, nejčastěji se jedná o poškození/ztrátu např. lidských životů, majetku nebo úrovně životního prostředí. Události, které tyto ztráty vyvolávají, a příčiny samotných událostí se provozní bezpečnost snaží identifikovat, predikovat a zamezit, či je odstranit úplně pomocí bezpečnostních modelů a analýz. Bezpečnostní modely a analýzy jsou tedy nástrojem provozní bezpečnosti pro zvyšování její úrovně.

Historie přístupu k provozní bezpečnosti, bezpečnostních modelů a jejich využívání je velmi obsáhlá, a doposud se tyto aspekty neustále mění. Od úplných počátků až do konce 20. století se provozní bezpečnost zaměřovala zejména na události způsobené lidským a technickým faktorem. Modely z této doby se zaměřují pouze na selhání techniky nebo působení člověka v systému a jeho chyb. Dalším přístupem, který byl nejvíce rozvinut ke konci 20. století, je přístup organizační. Bezpečnostní modely, které vychází z tohoto přístupu, se zaměřují zejména na organizační politiku a kulturu daného systému. Modely zaměřené na lidský, technický a organizační faktor jsou primárně určeny pro využití v oblasti daného faktoru, a proto je není doporučeno používat pro jinou oblast z důvodu omezených výsledků jejich aplikace takovýmto způsobem. Posledním a nejnovějším přístupem je systémový přístup, který není tak úzce zaměřen na konkrétní oblast jako předchozí modely. Lze jej využít na celý systém a jeho rozhraní s ostatními systémy bez nutnosti využití dalších modelů. Tento fakt činí ze systémového přístupu a jeho modelů nejvyspělejší způsob analýzy komplexních systémů, jakým

letecká doprava je. [2] Průběh vývoje a příklady bezpečnostních modelů a analýz znázorňuje obrázek 1.



Obrázek 1: Historický vývoj bezpečnostních modelů a analýz [3]

Technical-Technický, Human Factors-Faktor lidského činitele, Organisational-Organizační, Systemic-Systémový

Přístupy k provozní bezpečnosti se však nedělí pouze na 4 výše uvedené kategorie, kterými se modely daného přístupu zabývají. Další a zároveň nejnovější rozdělení provozní bezpečnosti přinesly publikace a modely Prof. Erika Hollnagela. Jeho myšlenka odolnosti systému vůči rezonanci rozdělila provozní bezpečnost na Safety II., která zahrnuje veškeré modely pracující s myšlenkou rezonance a odolnosti (na obrázku 1 pouze model FRAM), a Safety I., která zahrnuje zbylé modely, které byly vyvinuty před modely Prof. Hollnagela. Ten definoval Safety I. jako přístup, který analyzuje situace ve kterých dojde k nebezpečí, a Safety II. jako ten, který se zaměřuje a zkoumá běžný provoz, kdy žádné nebezpečí neproběhlo. Nejnovější publikace Prof. Nancy Leveson Safety III: A Systems Approach to Safety and Resilience však doplňuje toto rozdělení o Safety III., která obsahuje pouze systémový model STAMP. Dle Prof. Leveson se Safety II. nezabývá systémovým přístupem, a proto nebyly modely Prof. Hollnagela zařazeny do Safety III. Ta přistupuje k provozní bezpečnosti jako ke svobodě od všech nepřijatelných ztrát. Tento přístup je dle Prof. Leveson jediným systémovým přístupem k provozní bezpečnosti a nezabývá se tak pouze vybranými částmi systému jako předchozí modely. [4]

2.2 Provozní bezpečnost a změny

Jak již bylo zmíněno v kapitole výše, provozní bezpečnost se zabývá událostmi, které mohou vyvolat nějakou z identifikovaných ztrát. Příčiny těchto událostí mohou být různorodé a jedna událost může mít mnoho příčin, které se provozní bezpečnost snaží identifikovat. Cílem identifikování příčin je porozumění situaci a případné odstranění/snížení pravděpodobnosti výskytu některých příčin. Jednou ze skupin příčin mohou být změny v systému.

Změny v systému lze rozdělit na plánované a neplánované. Oba typy změn jsou v bezpečnosti stejně důležité a je třeba se jimi zabývat. Plánované změny jsou typy změn, které probíhají vědomě, řízeně a za určitého postupu. Tento typ změn je typický tím, že je třeba jej nahlašovat, nebo o něm alespoň informovat dozorový orgán, probíhá v přesně daném rozsahu a jeho implementace se podrobuje určité kontrole. Často na něj dopadá také nutnost provedení bezpečnostní studie ještě před samotným zahájením implementace. Plánované změny, které musí být schváleny dozorovým orgánem, se většinou týkají změn většího charakteru, konkrétně do nich patří např. stavební úpravy, změny vrcholového managementu nebo změny postupů daných certifikační základnou. Ostatní plánované změny stačí pouze dozorovému orgánu nahlásit. Druhým typem změn jsou neplánované změny. Ty naopak od plánovaných změn probíhají v systému nekoordinovaně a nepozorovaně. Neplánované změny zahrnují změny, které jsou vyvolány nečekanými událostmi jako např. vliv pandemie Covid-19 na leteckou dopravu, nebo změny, které jsou vyvolány plánovanou změnou, která není provedena bezpečně. Plánovaná změna poté vyvolá další změnu v systému, která není podchycena při jejím implementování. Poslední typ situace vyvolávající neplánovanou změnu nastává při dlouhodobém příznivém stavu bezpečnosti. Ten může vyvolat v zaměstnancích pocit, že riziko nebezpečí kleslo i přes to, že tomu tak není. Zaměstnanci poté začnou postupy provádět např. rychlejším nebo jednodušším způsobem, který je ovšem mimo stanovená pravidla, s pocitem, že neovlivní bezpečnost negativně. [5]

Všechny tyto změny, plánované i neplánované, mohou znamenat bezpečnostní riziko, a je proto třeba se změnami v systému počítat a mít na ně připravené postupy. Řízení změn je součástí Příručky pro řízení bezpečnosti (SMM) a Mezinárodní organizace pro civilní letectví (ICAO) jej doporučuje zahrnout jako součást Státního programu bezpečnosti (SSP). [2]

3 SSP

Státní program bezpečnosti (SSP) je dokument, který obecně udává předpisy, pravidla a činnosti, které by společně měly zvyšovat úroveň bezpečnosti letecké dopravy. Povinnost vytvořit SSP vznikla pro Českou republiku jakožto člena organizace ICAO vydáním Annexu 19, který tuto povinnost zmiňuje. SSP byl vydán jako Dodatek N letového předpisu L 19, a je nutné, aby pokrýval klíčové oblasti, které udává Annex 19 a ICAO Dokument 9859. SSP je rovněž nutné udržovat aktuální dle uvedených standardů. V České republice vydává a aktualizuje SSP Úřad pro civilní letectví (ÚCL). [6]

Cílem SSP je zajištění [2]:

- Využívání platné legislativy
- Koordinace a spolupráce mezi dozorovými orgány civilního letectví
- Podpory pro spolupráce se subjekty civilního letectví[1]
- Usnadnění monitorování a měření výkonnosti v bezpečnosti
- Udržení a zlepšování výkonnosti v bezpečnosti daného státu

Pro úspěšnou implementaci SSP je třeba spolupráce veškerých orgánů státní správy civilního letectví. [2]

SSP tedy obsahuje obecný popis platné legislativy, struktury dozorových orgánů, sběr bezpečnostních dat a požadavky na všechny subjekty civilního letectví. Konkrétní cíle v oblastech provozní bezpečnosti zahrnují státní plány bezpečnosti (SSp), které jsou standardně vydávány na určitá časová období. [6]

SSP ČR je vytvořen na základě Annexu 19 a ICAO Dokumentu 9859. SMM. Tyto dokumenty udávají členským státům postupy, jak SSP vytvořit a udržovat aktuální. SMM navíc pokrývá i Systém řízení bezpečnosti (SMS) pro subjekty civilního letectví a dává tak ucelený pohled na problematiku řízení bezpečnosti. Struktura SSP je standardně rozdělena dle SMM na 4 kapitoly [2]:

1) Bezpečnostní politika státu a její cíle
2) Řízení bezpečnostního rizika na úrovni státu
3) Zajištění bezpečného provozu na úrovni státu
4) Prosazování bezpečného provozu na úrovni státu

[1] Mezi subjekty civilního letectví patří veškeří poskytovatelé služeb v oblasti civilního letectví, mezi které patří např. letiště, provozovatelé obchodní letecké přepravy nebo poskytovatelé letových služeb. [6]

3.1 Bezpečnostní politika státu a její cíle

V první kapitole SSP dle SMM by měl každý stát určit, jakým způsobem bude řídit bezpečnost civilního letectví na svém území pomocí dozorových orgánů se stanovenými pravomocemi a odpovědností. V této kapitole je vždy nezbytné definovat legislativní rámec civilního letectví a jeho bezpečnosti pomocí národní a patřičné mezinárodní legislativy a standardů, které se na daný stát vztahují. Dále by zde měla být popsána struktura systému státního dozoru, jeho orgánů a pravomocí, které dané orgány mají. Jeden z orgánů musí být pověřen odpovědností za implementaci a aktualizaci SSP. Stát by si měl rovněž definovat základní stanovisko bezpečnostní politiky neboli státní záměr a vize bezpečnosti a nastavit bezpečnostní cíle a nebezpečí, které určují, čeho stát dosáhnout chce a naopak. [2]

3.2 Řízení bezpečnostního rizika na úrovni státu

Zde by stát měl vytvořit efektivní systém na identifikování nebezpečí na úrovni státu, který by měl kromě tradičního reaktivního přístupu identifikovat nebezpečí i proaktivně na základě sbíraných dat. Zdrojem dat pro stát jsou data, která sbírají subjekty civilního letectví, výsledky šetření leteckých nehod a incidentů nebo data, která sbírá některý z dozorových orgánů (např. data z bezpečnostních auditů). Data jsou poté doporučena analyzovat pomocí vybraného modelu, který pomáhá identifikovat nebezpečí systému. Nebezpečí poté musí být ohodnocena číselnou pravděpodobností a závažností následků, které dohromady tvoří bezpečnostní riziko. [2] Zde SMM doporučuje využití ICAO matici rizik, která je znázorněna na obrázku 2.

Bezpečnostní riziko		Vážnost				
Pravděpodobnost		Katastrofická A	Nebezpečná B	Významná C	Méně významná D	Zanedbatelná E
Častá	1	5A	5B	5C	5D	5E
Občasná	2	4A	4B	4C	4D	4E
Velice slabá	3	3A	3B	3C	3D	3E
Nepravděpodobná	4	2A	2B	2C	2D	2E
Velice nepravděpodobná	5	1A	1B	1C	1D	1E

Obrázek 2: Matice rizik dle ICAO [7]

Události se poté dělí dle hodnoty bezpečnostního rizika na 3 hlavní kategorie, podle kterých je s rizikem dále pracováno. [2] Kategorie bezpečnostního rizika jsou znázorněny na obrázku 3.

Míra indexu rizika	Popis rizika	Doporučená kritéria
5A, 4A, 3A, 5B, 4B, 5C	Nepřijatelná oblast	Není požadování zmírnění rizik
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Snesitelná oblast	Může být tolerováno dle snížení bezpečnostních rizik. Může vyžadovat rozhodnutí vedení k akceptování rizik
3E, 2D, 2E, 1B, 1C, 1D, 1E	Přijatelná oblast	Není požadování zmírnění rizik

Obrázek 3: Kategorie bezpečnostního rizika dle ICAO [7]

Dále by systém řízení bezpečnostního rizika (SRM) měl zahrnovat i spouštěče identifikovaných nebezpečí, mezi které patří např. i výše zmiňované systémové změny. Oba tyto seznamy by měly být pravidelně aktualizovány. Cílem SRM je tedy zajištění kontroly identifikovaných bezpečnostních rizik a dosažení přijatelné úrovně výkonnosti v bezpečnosti (ALoSP). [2]

3.3 Zajištění bezpečného provozu na úrovni státu

Cílem této kapitoly, jak její název vypovídá, je zajištění, že stát plní svou funkci v řízení bezpečnosti a jeho bezpečnost dosahuje stanovených limitů a cílů. Nástrojem pro zajištění bezpečného provozu je implementování měření a monitorování výkonnosti v bezpečnosti jak jednotlivých subjektů civilního letectví, tak i celkově státního aparátu. V rámci SMM je v tomto kroku doporučeno využívat dozor založený na bezpečnostním riziku (SRBS), který umožňuje definovat v rámci státního dozoru prioritní oblasti, na které je třeba se zaměřit. Součástí SRBS je rovněž vytvoření rizikových profilů pro danou oblast nebo konkrétní subjekty civilního letectví. Tyto profily jsou tvořeny na základě dlouhodobého sledování dané oblasti/subjektu, v rámci subjektů zejm. jejich přístupu k řízení bezpečnostního rizika a úrovně výkonnosti v bezpečnosti. [2] Mezi informace zobrazované v rizikových profilech subjektů civilního letectví patří např. [2]:

- Finanční situace subjektu
- Počet let v provozu
- Kompetence a výkonnost odpovědných vedoucích pracovníků
- Výsledky předchozích auditů
- Ukazatele výkonnosti v bezpečnosti týkající se provozu subjektu
- Úroveň identifikace bezpečnostního rizika a zajišťování bezpečnosti
- Výkonnost v bezpečnosti dle analýzy používané orgánem státního dozoru

Stát tedy musí k již vytvořeným bezpečnostním cílům identifikovat rovněž ukazatele a cíle výkonnosti v bezpečnosti, které představují konkrétní cílové hodnoty daného ukazatele, a pomáhají tak k ověření situace v kratším časovém měřítku. Mezi ukazateli výkonnosti v bezpečnosti by měly být zastoupeny reaktivní i proaktivní ukazatele jejichž nasbírané hodnoty jsou následně znázorněny pomocí grafů, tabulek, obrázků nebo „safety dashboards" neboli bezpečnostních panelů. Ty jsou využívány pro vizualizaci vybraných dat a trendů ukazatelů výkonnosti v bezpečnosti pomocí jednoho grafického rozhraní, které má za cíl zvýšit přehlednost daných informací. [2]

Dále si musí stát pomocí ukazatelů výkonnosti v bezpečnosti a jejich cílů nastavit ALoSP, která reprezentuje určitý limit, který stát očekává od všech dozorových orgánů i subjektů civilního letectví. Cílem ALoSP je k ujištění dosažení nastavených státních požadavků na provozní bezpečnost. Celý systém monitorování a měření výkonnosti v bezpečnosti by měl být v určité periodě aktualizován, aby nedocházelo např. k nastavení nedosažitelných cílů či ALoSP. [2]

Do této kapitoly je dle SMM také doporučeno zahrnout i řízení změn (MoC), které by mělo zahrnovat aktivní vyhodnocování možných dopadů změn dle SRM na státní úroveň bezpečnosti. V MoC by měly být zahrnuty zejm. takové změny, které mohou výrazně ovlivnit bezpečnost (dle ICAO jsou to změny organizační, provozní nebo kombinace těchto dvou). Na identifikované změny by měly být vypracovány postupy pro stanovení možných důsledků a provedení těchto změn bezpečným způsobem. [2]

3.4 Prosazování bezpečného provozu na úrovni státu

V poslední kapitole by stát měl vytvořit účinný mechanismus pro předávání bezpečnostních informací, jakými jsou např. bezpečnostní politika, stanovené bezpečnostní cíle, rizika a ostatní důležité částí SSP. Důvodem pro vytvoření tohoto mechanismu je vzbudit zejm. v zaměstnancích dozorových orgánů pocit odpovědnosti a osvojení si pozitivního přístupu k bezpečnosti. Tento přístup zaměstnanců je poté přenášen na subjekty civilního letectví při vykonávání dozorových činností a společně tak vytváří prostředí úspěšné pro implementování SSP. Mechanismus pro předávání informací by měl být zaměřen na interní a externí komunikaci. Interní komunikací je myšlena výměna informací zejména mezi jednotlivými dozorovými orgány a rovněž uvnitř jich samotných, která většinou probíhá např. pomocí seminářů, tréninků, informačních publikací nebo pomocí webové stránky. Externí komunikace probíhá mezi dozorovými orgány a subjekty civilního letectví např. pomocí příruček, poradního

materiálu, bulletinů nebo oběžníků. Pomocí výročních zpráv dozorových orgánů probíhá externí komunikace i s širokou veřejností. [2]

3.5 SSP ČR

Jak již bylo zmíněno výše, SSP ČR byl vydán jako dodatek N předpisu L 19, a jeho zhotovení a aktualizaci má na starosti ÚCL. Byl vypracován na základě výše zmíněných dokumentů ICAO (Annex 19 a SMM) a národní legislativy. Jeho poslední aktualizace proběhla 14.11. 2013. [6] Strukturu SSP ČR shrnuje tabulka 1.

Tabulka 1: Struktura SSP ČR [6]

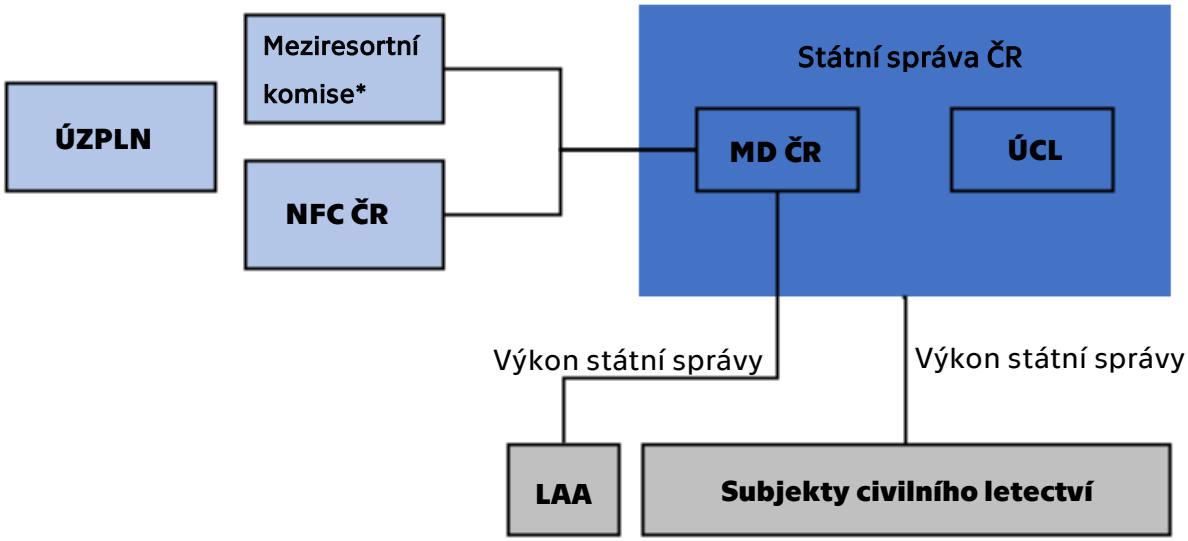
Kapitola	Obsah
1. Bezpečnostní politika státu a její cíle	1.1. Právní předpisy v oblasti bezpečnosti
	1.2. Povinnosti a odpovědnost státu v oblasti bezpečnosti
	1.3. Zjišťování příčin leteckých nehod
	1.4. Prosazování bezpečnosti
2. Řízení bezpečnostního rizika na úrovni státu	2.1. Požadavky na vnitřní systémy řízení bezpečnosti subjekty působícími v civilním letectví
	2.2. Výkonnost řízení bezpečnosti poskytovateli služeb v civilním letectví
3. Zajištění bezpečného provozu na úrovni státu	3.1. Dohled nad bezpečností
	3.2. Sběr, rozbor a šíření bezpečnostních údajů
	3.3. Zaměření dohledu, založeného na sběru údajů, na oblasti vyžadující zvýšenou pozornost
4. Prosazování bezpečného provozu na úrovni státu	4.1. Interní výcvik, komunikace a šíření informací o bezpečnosti
	4.2. Externí výcvik, komunikace a šíření informací o bezpečnosti

První kapitola SSP se týká nejprve legislativního rámce, který je platný pro ČR. Jsou tu zahrnuty jak národní zákony a standardy ICAO, tak i evropská legislativa, která pro ČR jako členský stát EU, rovněž platí. Poté je zde popsána odpovědnost dozorových orgánů ČR a jejich závazku vůči agentuře EASA. Jako poslední je zde popsána povinnost a odpovědnost šetření leteckých nehod a odpovědnost dozorových orgánů v oblasti

prosazování bezpečnosti. Druhá kapitola se zabývá povinností implementace SMS dle SMM pro subjekty civilního letectví a povinností státu tuto implementaci kontrolovat. Dále je zde popsáno, jakým způsobem by si subjekty civilního letectví měly měřit výkonnost v bezpečnosti a jaká data ohledně výkonnosti v bezpečnosti musí poskytnout ÚCL. Ve třetí kapitole je nejprve popsán systém dozoru v ČR a zejm. role a odpovědnost ÚCL při klíčových událostech pro subjekty civilního letectví, jakými jsou osvědčování a průběžný dozor. Dále je zde popsán systém sběru dat, který probíhá jak z povinných, tak z dobrovolných hlášení. Pro tento účel je zde popsán i systém ECCAIRS, který plní funkci pro nahlašování povinných i dobrovolných hlášení pro EU. Nakonec je zde popsán systém dozoru zaměřeného na problematické oblasti, kterými jsou např. zahraniční letadla. Poslední kapitola shrnuje požadavky na vypracování plánu výcviku a systému předávání informací o bezpečnosti. Požadavky se dělí na oblast interního výcviku, který se týká zaměstnanců dozorových orgánů (např. ÚCL nebo ÚZPLN), a externího výcviku týkajícího se zaměstnanců subjektů civilního letectví. [6]

4 Státní orgány správy civilního letectví v ČR

Jak již bylo zmíněno v kapitole výše, SSP udává obecný postup, jak zajišťovat bezpečnost a zvyšovat její úroveň. K dosažení tohoto cíle je nutné, aby fungoval stanovený systém správy nad subjekty civilního letectví pomocí orgánů daného státu, které tuto funkci zaopatřují, a fungovala mezi nimi kontinuální spolupráce. Mezi státní orgány správy civilního letectví ČR se řadí zejm. MD ČR, ÚCL a ÚZPLN. Jejich nynější uskupení stanovuje zákon č. 49/1997 Sb. o civilním letectví a zákon č. 455/1991 Sb., o živnostenském podnikání. Struktura systému správy je znázorněna na obrázku 4. [6]



Obrázek 4: Struktura systému správy civilního letectví ČR, upraveno z [8]

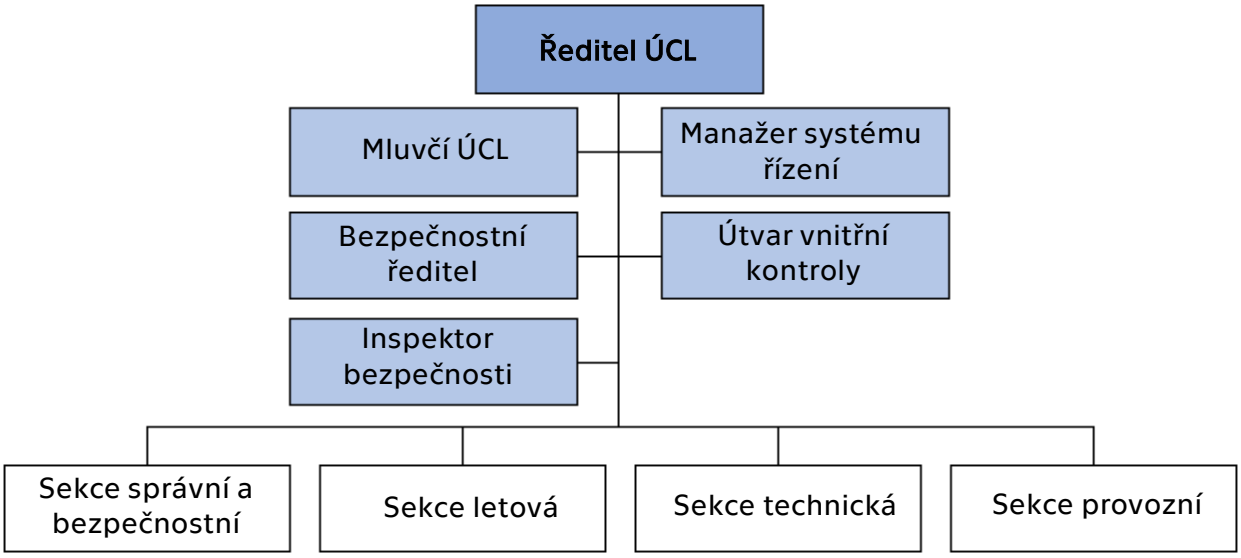
** Meziresortní komise pro bezpečnost civilního letectví*

4.1 MD ČR

Ministerstvo dopravy ČR (MD ČR) je organizačně nejvyšším orgánem státní správy civilního letectví v ČR v jehož čele stojí ministr. MD ČR se organizačně dělí na sekce a odbory, z nichž civilním letectvím se zabývá sekce nesilniční dopravy a mezinárodních vztahů konkrétně odbor civilního letectví. Tento odbor se dále dělí na oddělení letecké dopravy, infrastruktury letišť a oddělení leteckého provozu, techniky a rozvoje. Odbor civilního letectví obecně zodpovídá za implementaci patřičné legislativy, vydává nejdůležitější dokumenty týkající se civilního letectví (např. povolení k provozu pravidelné/nepravidelné obchodní letecké dopravy) uděluje přepravní práva leteckým dopravcům, zajišťuje reprezentaci ČR v mezinárodních organizacích a zastává funkci odvolávacího úřadu při vedení správního řízení ostatními dozorovými orgány. [9] [10]

4.2 ÚCL

Úřad pro civilní letectví (ÚCL) zastává funkci Dozorového orgánu nad civilním letectvím (CAA) v České republice neboli vykonává státní dozor nad veškerými subjekty civilního letectví (mimo SLZ, kde tuto funkci zastává LAA). Touto funkcí bylo ÚCL pověřeno MD ČR, kterému je také přímo podřízeno, od roku 1997 kdy ÚCL vzniklo. Mezi hlavní aktivity ÚCL patří zejm. vydávání licencí, průkazů, povolení pro subjekty civilního letectví a provádění dozoru, tj. vynucování dodržování zákonů, standardů a dokumentů české i mezinárodní legislativy, která je platná pro ČR, a případně podniká kroky k nápravě (např. zadržení průkazů/licencí nebo jejich odebrání). ÚLC se organizačně dělí na 4 samostatné sekce dle oblasti jejich působení, a to na sekci bezpečnostní a správní, letovou, provozní a technickou. [6] [11] Strukturu ÚCL znázorňuje obrázek 5.



Obrázek 5: Organizační struktura ÚCL, upraveno z [12]

V čele ÚCL stojí ředitel, který ÚCL reprezentuje a zodpovídá za jeho chod. Mezi ním a řediteli jednotlivých sekcí, se nachází funkce přímo podřízené řediteli ÚCL, které jsou rovněž znázorněny na obrázku 5. Manažer systému řízení zodpovídá za implementaci SSP, stojí v čele skupiny pro řešení otázek bezpečnosti (SAG), monitoruje účinnost opatření navržených touto skupinou, vede seznam bezpečnostních rizik ÚCL a společně s inspektorem bezpečnosti vede evidenci hlášení o událostech a závěrečných analýz. Inspektor bezpečnosti zabezpečuje komunikaci mezi ÚCL a ÚZPLN, analyzuje hlášené události a závěrečné zprávy ÚZPLN a jak již bylo řečeno vede databázi těchto událostí. Útvar vnitřní kontroly se zabývá dodržování stanovených předpisů na ÚCL pomocí interních auditů. Bezpečnostní ředitel se zabývá krizovými plány a agendou utajovaných

informací. Poté jsou již jednotlivé sekce, které mají v čele ředitele sekcí. Sekce správní a bezpečnostní zajišťuje chod logistických a právních potřeb ÚCL a rovněž pod její odpovědnost spadá ochrana před protiprávními činy. Sekce letová obstarává zejm. certifikaci a průběžný dozor provozovatelů obchodní letecké dopravy a také leteckého personálu civilního letectví. Sekce technická má v odpovědnosti činnosti spojené s prokázáním a zachování letové způsobilosti letadel, leteckých motorů, vrtulí nebo letadlových částí a zařízení, které spadají do kompetence ÚCL. Poslední sekcí je sekce provozní, která zajišťuje osvědčování a průběžný dozor např. provozovatelů letišť, poskytovatelů navigačních služeb nebo meteorologických služeb. Také vykonává funkci stavebního úřadu pro civilní letecké stavby a podílí se s MD ČR na návrzích letových předpisů. [12]

4.3 ÚZPLN

Ústav pro odborné zjišťování příčin leteckých nehod (ÚZPLN) zastává funkci Institutu pověřeného šetřením leteckých nehod (AAII) v České republice a patří do rozpočtové kapitoly MD ČR. Tento úzce profilovaný orgán státní správy šetří letecké nehody a vážné incidenty z povinných nebo dobrovolných hlášení, která se staly v ČR, nebo se týkají českého subjektu civilního letectví operujícího v zahraničí, a které nejsou v kompetenci daných subjektů civilního letectví[2]. Hlášení ÚZPLN sbírá pomocí evropského systému ECCAIRS nebo systému, který ÚZPLN musel zavést na základě leteckého předpisu L 19 a nařízení Evropské parlamentu a Rady č. 376/2014. Nahlášenou událost poté na ÚZPLN posoudí, a pro závažné události vypracují závěrečné zprávy a stanoví bezpečnostní doporučení pro snížení rizika identifikovaných příčin. Proces šetření vede ÚZPLN dle leteckého předpisu L 13 a zahrnuje využití bezpečnostních modelů pro zjištění příčin hlášené události. Závěr procesu šetření ÚZPLN konzultuje s ÚCL a dotčenými stranami a následně předá kopii závěrečné zprávy ÚCL, MD ČR a Evropské komisi. ÚZPLN se organizačně dělí na oddělení letových inspektorů, technických inspektorů a oddělení správy, rozvoje a analýz. Každé oddělení vede vedoucí a v čele ÚZPLN stojí ředitel. [6] [13] [14]

[2] ÚZPLN může rovněž povinnost šetření přenést na daný subjekt civilního letectví na základě žádosti o pověření dle zákona č. 49/1997 Sb. v oblasti uvedené v předmětu požadovaného pověření. Pokud ÚZPLN žádost schválí, tak šetření událostí vymezené předmětem žádosti spadá do kompetencí subjektu. Subjekt poté musí při šetření postupovat dle dané legislativy, plnit povinnost o hlášení událostí a informovat ÚZPLN o výsledcích šetření. Seznam subjektů a předměty pověření vede ÚZPLN na jejich webových stránkách. [15]

5 Přístupy k řízení neplánovaných změn

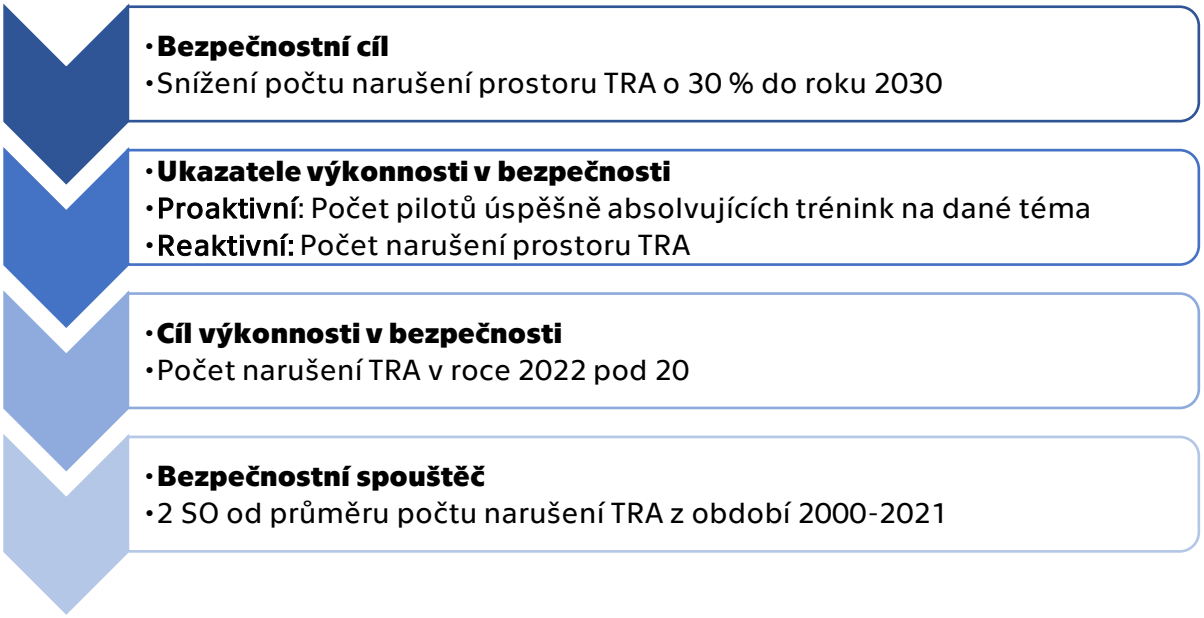
Neplánované změny, jak již bylo řečeno výše, mohou znamenat pro systém určité bezpečnostní riziko, a proto je nutné, aby na ně daný systém byl schopen reagovat a vyhodnocovat je, jako tomu je i u ostatních bezpečnostních rizik identifikovaných pomocí bezpečnostních modelů. U neplánovaných změn tkví problematika v samotné podstatě těchto změn, a totiž v jejich těžké identifikaci. Pro identifikování těchto změn je nutné systém dlouhodobě sledovat a situaci vyhodnocovat, na rozdíl od plánovaných změn, které v systému probíhají kontrolovaně.

Jednotlivé CAA mají doporučeno v rámci SSP dle SMM zahrnout i přístup k neplánovaným změnám, který je rovněž doporučeno zahrnout do SMS pro všechny subjekty civilního letectví. Tato kapitola se bude zaměřovat na 2 nejpoužívanější přístupy v civilním letectví. [2]

5.1 Přístup ICAO

Přístup, který doporučuje ICAO, je popsán v SMM jako součást SMS i SSP. Řízení neplánovaných změn je zde založeno na sledování a hodnocení výkonnosti v bezpečnosti (viz kapitola 3), které se provádí pomocí identifikovaných ukazatelů, cílů a spouštěčů výkonnosti v bezpečnosti. Ukazatele výkonnosti v bezpečnosti jsou taktické parametry reflektující nastavené cíle, které představují obecné tvrzení o určitém stavu, kterého je v úmyslu dosáhnout. Ukazatele jsou definovány na základě těchto cílů a představují parametry, které ovlivňují dosažení daného cíle. Obvykle jsou v systému rozdělovány na reaktivní a proaktivní. Reaktivní ukazatele monitorují výstup systému, tedy stav již ovlivněný provozem, a proaktivní se zaměřují na vstup systému. Jelikož stanovené cíle jsou obvykle obecně definované, bylo by těžké v průběhu času určit, zda se čísla ukazatelů pohybují dostatečně rychle a zda se podaří stanovený cíl naplnit. Proto se stanovují cíle výkonnosti v bezpečnosti. Ty reflektují cíle bezpečnosti v kratším časovém měřítku pro usnadnění kontroly, zda je cíl bezpečnosti průběžně plněn. Stanovují se zejm. pro reaktivní ukazatele, pro které se stanoví cílová hodnota za dané časové období. Pro účely ověření, zda se naopak hodnoty daného ukazatele nevzdalují od stanovených cílů, se vytváří bezpečnostní spouštěč, který většinou pracuje s myšlenkou směrodatné odchylky (SO). Ta představuje vychýlení hodnot, které je způsobené běžným provozem, a je odvozována od průměru historických dat daného ukazatele. Bezpečnostní spouštěč poté určuje násobek směrodatné odchylky určující

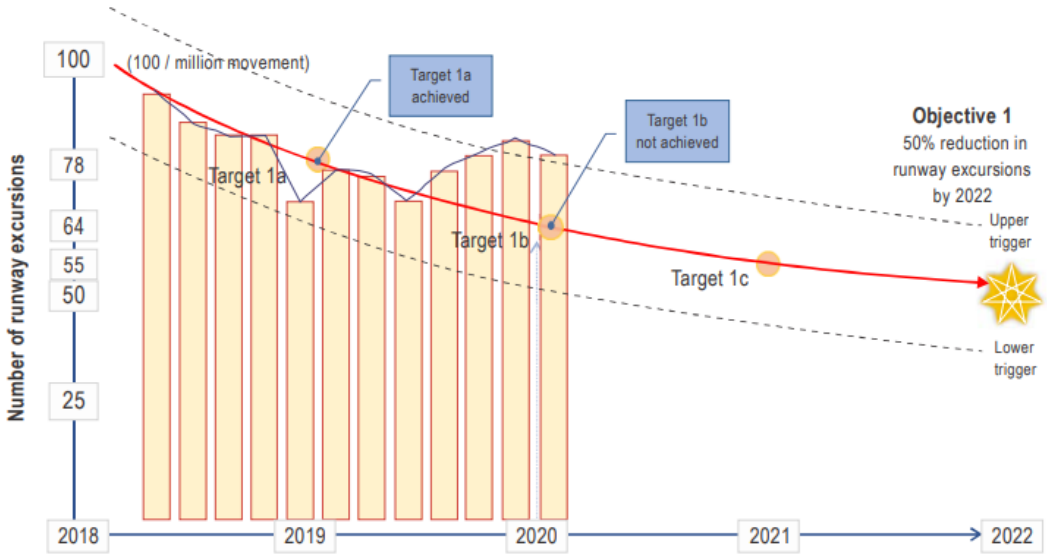
vychýlení hodnot, které již není běžné, a je třeba na něj reagovat. [2] Příklady těchto parametrů jsou znázorněny na obrázku 6.



Obrázek 6: Příklad nastavených parametrů výkonnosti v bezpečnosti dle ICAO

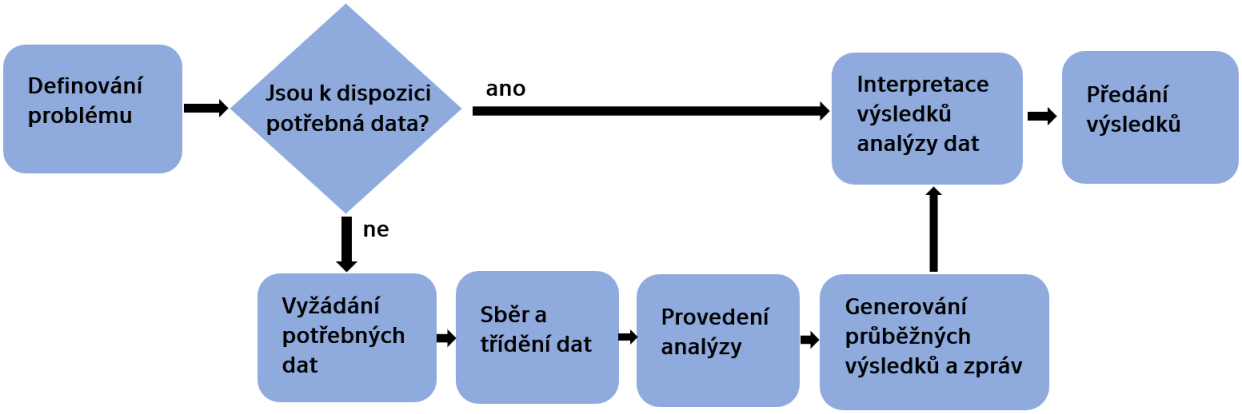
Po nastavení všech nutných parametrů pro sledování a hodnocení výkonnosti v bezpečnosti nastává již samotný sběr dat a prezentace průběžných výsledků nejčastěji v podobě grafů, tabulek nebo bezpečnostních panelů. [2] Příklad znázornění sbíraných dat pomocí grafu je na obrázku 7.

Data se poté průběžně vyhodnocují v čase pomocí deskriptivní, inferenční a prediktivní analýzy. Pokud hodnoty ukazatelů korespondují s nastavenými cíli výkonnosti v bezpečnosti, tak se dále pokračuje ve sběru dat a případné aktualizaci nastavených parametrů. V případě, že hodnoty překračují násobek směrodatné odchylky, je třeba rozhodnout na základě dat o dalším postupu. Tento způsob rozhodování bývá v literatuře označován jako Rozhodování na základě dat (D3M), a umožňuje zaměřit se na rozhodnutí orientované na splnění cíle v bezpečnosti, které mnohdy zahrnuje i myšlenky změn a jejich řízení. Pomocí analýz se identifikuje příčina odchylky, kde často mohou figurovat právě neplánované změny, a pomocí D3M se poté stanovují patřičné kroky k nápravě. [2] D3M je způsob rozhodování doporučovaný organizací ICAO a jeho proces je znázorněn na obrázku 8.



Obrázek 7: Příklad znázornění dat výkonnosti v bezpečnosti dle ICAO [2]

Number of runway excursion-Počet vyjetí z dráhy, Target 1a achieved/not achieved-Cíl výkonnosti v bezpečnosti 1a splněn/nesplněn, Upper/Lower trigger-Horní/Dolní spouštěč, Objective 1: 50% reduction in runway excursion by 2022: -Bezpečnostní cíl 1: Snížení počtu vyjetí z dráhy o 50% do roku 2022



Obrázek 8: Proces D3M, upraveno z [2]

5.2 SAM

Metodika vyhodnocování bezpečnosti (SAM) byla vydána organizací EUROCONTROL primárně pro řízení plánovaných a částečně neplánovaných změn. Původně byla tato metodika určena pro použití v procesech řízení letového provozu, avšak její použití není limitováno pouze pro tyto procesy a může být využita pro všechny procesy, ve kterých plánované a neplánované změny hrají roli. SAM byl založen na metodikách ARP4754/4761 a ED79 a je zaměřen na 3 elementy systému, kterými jsou lidé, vybavení

a postupy a interakce v daném prostředí. EUROCONTROL k této metodice vydal rovněž elektronickou verzi, která je označována jako e-SAM. [16]

Metodika SAM se provádí pomocí 3 kroků, kterými jsou [16]:

1. Vyhodnocování funkčních nebezpečí (FHA)
2. Předběžné vyhodnocování bezpečnosti systému (PSSA)
3. Vyhodnocování bezpečnosti systému (SSA)

Celá metodika SAM je založena na iterativním procesu, který je prováděn vždy při vytváření nového systému nebo změny toho stávajícího. Kroky se rovněž periodicky opakují pro aktualizaci, aby stanovené parametry reflektovaly současnou situaci systému. [16]

5.2.1 FHA

FHA je prvním krokem metodiky SAM, ve kterém je cílem stanovit, jak bezpečný systém musí být, a to s pomocí stanovení nebezpečí a bezpečnostních cílů. Tento krok se aplikuje na systém v počátku jeho vývoje nebo jeho modifikace, tj. v procesu definice systému. FHA je prováděna pomocí 5 kroků, kdy prvním z nich je iniciace FHA. V tomto kroku je cílem prvotní porozumění systému, jeho komponentům a prostředí ve kterém působí za pomocí kompletace veškeré dokumentace týkající se tohoto tématu. Rovněž se zde tvoří tzv. předpoklady o daném systému. Druhým krokem je plánovaní, ve kterém se definují rozsah a cíle FHA, a vytvoření plánu činností, které musí být provedeny na základě plánu daného projektu. Třetím krokem je specifikace bezpečnostních cílů, které byly vytvořeny v prvním kroku FHA. Stanovují se zde rovněž nebezpečí systému, jejich závažnost, výsledný efekt, který mohou v systému vyvolat, a jejich limitní četnost výskytu. Dále se provádí ověření a validace stanovených bezpečnostních cílů, ve které se analyzují výsledky předchozích kroků FHA, a proces ověřování, ve kterém dochází k ověření, zda je dodržen plán z druhého kroku. Posledním krokem je kompletace dosažených výsledků. [16]

5.2.2 PSSA

PSSA se aplikuje ve fázi návrhu systému, a to pokaždé při tvoření nového systému nebo při provedení plánované změny, k čemuž využívá výstupy z FHA. Jejím cílem je tedy stanovit, jak bezpečná je navržená architektura systému a zda je tato architektura schopna v daném návrhu splnit parametry stanovené v předchozím kroku. Pokud by zde došlo ke zjištění, že některý z parametrů (např. předpoklad) nelze splnit, je nutno opět provést FHA. Jinak se struktura postupu PSSA víceméně shoduje s FHA, a proto prvním

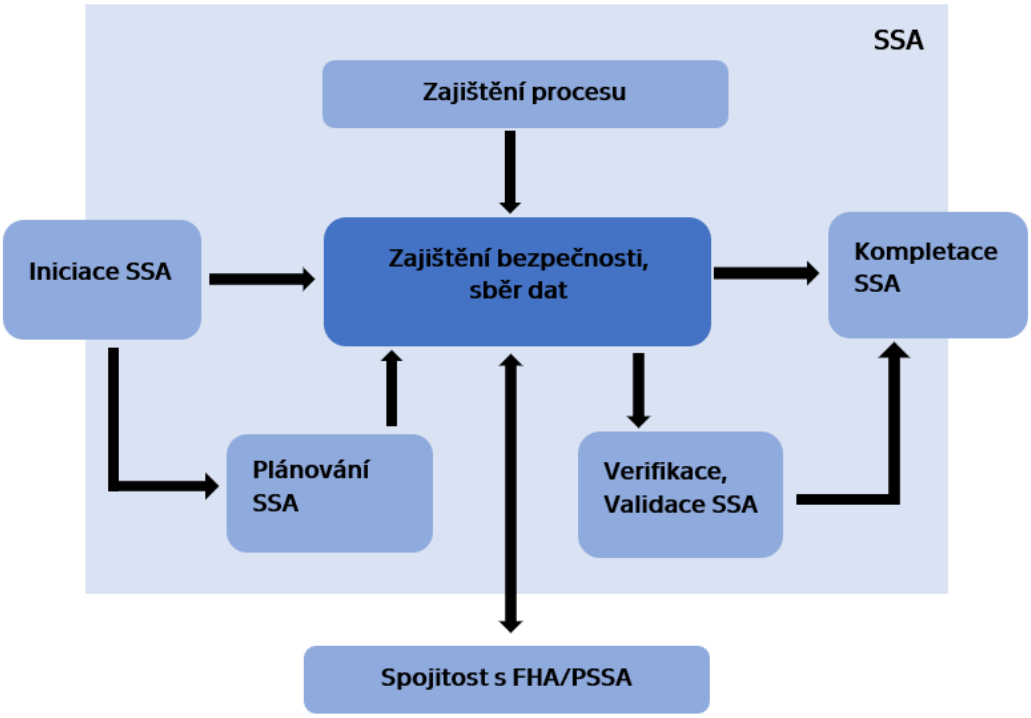
krokem je porozumění architektuře systému a celkovému popisu systému a jeho okolí z tohoto pohledu. Dále následuje identifikování rozsahu PSSA a plánování jednotlivých činností potřebných k dosažení cíle PSSA. Třetím krokem je stanovení specifických požadavků pro 3 základní elementy metodiky SAM, a totiž pro lidi, vybavení a postupy, které se definují na základě bezpečnostních cílů. Rovněž se zde aktualizují prozatímní dosažené výstupy, jakými jsou např. seznam nebezpečí, předpokladů nebo bezpečnostních cílů. Následně jsou výsledky PSSA (zejm. bezpečnostní požadavky) podrobeny procesu ověření a validace a činnosti plánu PSSA jsou podrobeny procesu ověřování. Na závěr je opět provedena kompletace dosažených výsledků. [16]

5.2.3 SSA

SSA se spouští při uvedení systému nebo jeho změny do provozu a tvoří tedy poslední krok metodiky SAM. Cílem SSA je dokázat, že takto nastavený systém je schopen dosáhnout cíleného (nebo alespoň akceptovatelného) rizika, a zda splňuje bezpečnostní cíle identifikované v FHA a bezpečnostní požadavky na základní elementy stanovené v PSSA. SSA je stěžejní částí pro řízení neplánovaných změn. V rámci tohoto kroku dochází ke sběru dat z provozu, monitorování a vyhodnocování výkonnosti v bezpečnosti. SSA je částí SAM, která je prováděna kontinuálně po dobu, co daný systém funguje, není-li nutné provést celou metodiku SAM znovu kvůli jeho změně nebo aktualizaci, jak již bylo řečeno výše. První dva kroky SSA se shodují s již výše uvedenými u FHA a PSSA. Nejdůležitější částí SSA a celkového řízení neplánovaných změn je třetí krok, ve kterém se provádí sběr a vyhodnocování dat z provozu na základě bezpečnostních cílů a bezpečnostních požadavků. [16] Jednotlivé kroky SSA jsou znázorněny na obrázku 9.

Na počátku při implementaci se znovu přehodnocují nastavené parametry. Pokud některý z nich neodpovídá, je doporučeno vypracovat SAM znovu dalším iteračním procesem. Během provozu již probíhá sběr dat dle identifikovaných ukazatelů výkonnosti v bezpečnosti na jejichž základě probíhá sledování a vyhodnocování výkonnosti v bezpečnosti. Pomocí výkonnosti v bezpečnosti metodika SAM sleduje vývoje trendu a dle nastavených limitních četností výskytu, popř. proběhne vyhodnocení důvodů způsobujících nadlimitní četnost, do čehož se zahrnují právě i neplánované změny. Ty mohou být i součástí analýzy událostí týkajících se daného ukazatele, které EUROCONTROL v metodice SAM rovněž doporučuje použít. Sledování a vyhodnocování výkonnosti v bezpečnosti v SSA končí pouze tehdy, když systém ukončí svou činnost. I na

tuto fázi je nutné mít připravený seznam bezpečnostních cílů a požadavků, který bude reflektovat bezpečné ukončení činnosti daného systému. [16]



Obrázek 9: Postup SSA, upraveno z [16]

Obě metody (metodika SAM i metoda doporučována ICAO) přistupují k neplánovaným změnám pomocí ukazatelů výkonnosti v bezpečnosti, jejich dlouhodobému sledování, vyhodnocování dle stanovených limitních hodnot a provedených opatření v případě překročení těchto hodnot. Čím se metody liší je zejm. způsob, pomocí kterého dané ukazatele a jejich limitní hodnoty stanovují, a rovněž přístup k aktualizaci stanovených parametrů. Metoda ICAO je, jak již bylo řečeno, součástí SMM a její rozpracování vůči neplánovaným změnám je detailnější zejm. co se týče stanovení vhodných ukazatelů, jejich limitních hodnot a průběžného vyhodnocování. Na rozdíl od této metody byla metodika SAM cíleně vytvořena pro řízení plánovaných změn a chybí zde větší detail pro zmíněné parametry, které jsou klíčové pro neplánované změny. Co ovšem má metoda SAM vypracováno lépe je iterativní proces, díky kterému probíhá aktualizace systému v průběhu času, která je důležitá pro případnou identifikaci nových nebezpečí a následně i ukazatelů výkonnosti v bezpečnosti. [2] [16]

6 STAMP

Jak již bylo řečeno výše, současné nejpoužívanější přístupy k řízení neplánovaných změn jsou zejm. ty, které jsou uvedeny v kapitole 5. Jejich velkou nevýhodou je však nerozpracovanost těchto postupů zejm. ve smyslu identifikace a aktivního vyhodnocování neplánovaných změn a nesystémový přístup[3] k celé problematice. Jediným systémovým přístupem k provozní bezpečnosti založeným na Systémové teorii je Safety III. a její Systémově-teoretický model nehod a procesů (STAMP).

STAMP je bezpečnostní model (obdobně jako je např. známý model švýcarského sýra), který byl poprvé představen prof. Nancy Leveson v roce 2004 jako součást nového přístupu k provozní bezpečnosti, který je založen na Systémové teorii, a navazuje na model AcciMap od prof. Rasmussena. STAMP analyzuje a popisuje chování systému jako celku na rozdíl od všech předchozích modelů z obrázku 1, které se zabývaly pouze konkrétními částmi systému. Aplikace modelu STAMP tak pokrývá veškeré faktory a vazby mezi nimi, na které není třeba aplikace dalších modelů. Touto vlastností STAMP tvoří nejvhodnější bezpečnostní model pro složité socio-technické systémy, jakými letectví bezpochyby je. STAMP je tedy model, který popisuje, jak dochází k nechtěným výstupům daného systému (např. nehodě), a jak těmto výstupům co nejvíce zabránit v jejich vzniku. K tomu je třeba detailní analýza daného systému, které STAMP dociluje pomocí jeho dvou analýz a to Systémově-teoretické analýzy procesů (STPA),Analýzy příčin na základě Systémové teorie (CAST). [17]

Výhody použití tohoto modelu jsou zejm. [17]:

- STAMP lze aplikovat i na komplexní systémy díky jeho přístupu shora dolů.
- Zahrnuje všechny důležité části systému (např. software, lidi, organizaci nebo kulturu bezpečnosti).
- Vytváří prostředí pro využití vyspělejších analýz (CAST a STPA).

6.1 STPA

STPA je, jak již bylo řečeno výše, jednou ze dvou analýz založených na modelu STAMP a jeho myšlenkách. Cílem aplikace STPA je analýza nebezpečí daného systému. Tato analýza se označuje jako proaktivní neboli jejím obsahem je identifikování nebezpečí již

[3] Nesystémový přístup znamená, že daný model/analýza nepřistupuje k systému jako k celku, systém rozděluje na více částí, kterými se poté zabývá samostatně. Tento přístup byl využíván v modelech a analýzách Safety I..

při návrhu daného systému, která se poté dále sledují a predikují v určitém časovém měřítku. V celém procesu STPA se systém nerozděluje a analýza je aplikována na celý model se všemi jeho komponenty současně, a je proto vhodná i pro komplexní systémy. Naopak využití předchozích metod např. lineárního sekvenčního modelu není pro tyto účely vhodné, jelikož jeho využití problematiku u složitých až komplexních systémů nepřiměřeně zjednodušuje a jeho výstup se tak stává zkreslený. [5]

Celá analýza STPA zahrnuje následující kroky [5]:

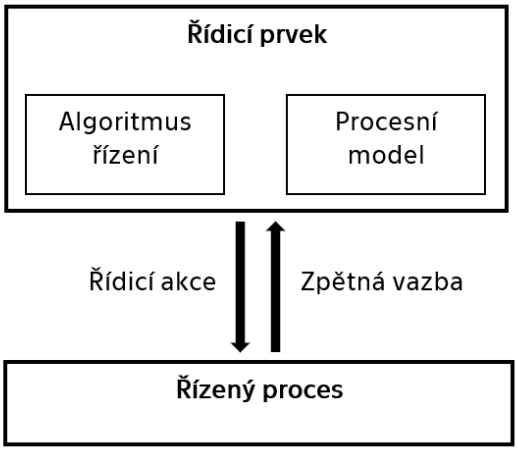
1. Definování účelu analýzy
2. Modelování řídicí struktury daného systému
3. Identifikování nebezpečných řídicích aktivit
4. Stanovení scénářů, ve kterých dochází ke ztrátě

6.1.1 Definování účelu analýzy

V prvním kroku STPA je nutné stanovit proč a za jakým cílem se analýza na systém aplikuje. Cíl je stanoven pomocí identifikovaných ztrát, nebezpečí a omezení, které se vztahují na celý systém. Pro identifikování ztrát je nutné se zaměřit na to, co je pro zúčastněné strany v systému (např. vlastníka společnosti) cenné a nutné pro zachování. Zde se většinou jedná o ztráty na životech, zdraví nebo majetku (viz kapitola 2.1). Nebezpečí jsou poté podmínky, které by mohly vést společně s vlivem prostředí k jedné nebo více ztrátám. Jako poslední se stanovují omezení, která představují podmínky pro prevenci nebezpečí a ztrát. Všechny tři parametry mají svůj daný syntax a značení, které napomáhá k unifikaci a lepší přehlednosti celé analýzy. Součástí tohoto kroku rovněž může být rozdělení nebezpečí do jednotlivých dílčích nebezpečí, která mohou ještě přidat větší detail analýzy. Tato část prvního kroku je volitelná a není třeba ji provádět. [5]

6.1.2 Modelování řídicí struktury daného systému

Druhým krokem je vytvoření hierarchické řídicí struktury systému. Tento krok se tvoří pomocí řídicích zpětnovazebních smyček, které jsou tvořeny na základě toho, jak je proces řízen řídicími prvky. [5] Příklad takové řídicí zpětnovazební smyčky je znázorněn na obrázku 10.



Obrázek 10: Základní řídicí zpětnovazební smyčka STAMP, upraveno z [5]

V řídicí zpětnovazební smyčce vždy figuruje řídicí prvek a řízený proces. Řídicí prvek může být např. osoba nebo skupina, která pomocí algoritmu řízení vytváří řídicí akci na daný proces. Daný algoritmus řízení tedy představuje proces rozhodování řídicího prvku a řídicí akce způsob, jak si řídicí prvek vynucuje, aby proces zůstal v bezpečných mezích. Daná řídicí akce poté vyvolává v procesu zpětnou vazbu, kterou řídicí prvek přijímá pomocí senzorů a zpracovává ji pomocí procesního modelu. Ten představuje vnitřní přesvědčení a záměr řídicího prvku, který dále ovlivňuje proces rozhodování o adekvátní řídicí akci na danou zpětnou vazbu. Společně s dalšími vstupy a výstupy (např. okolního prostředí systému) tvoří tyto prvky základní typy elementů řídicích smyček dle STAMP. Jako poslední se v tomto kroku stanovují zodpovědnosti jednotlivých řídicích prvků, které jsou odvozeny z bezpečnostních omezení, a představují co jednotlivé řídicí prvky musí udělat, aby systém zůstal v jeho bezpečných hranicích, a nedocházelo tak k nebezpečí. [5]

6.1.3 Identifikování nebezpečných řídicích akcí

Třetím krokem analýzy STPA je identifikování nebezpečných řídicích akcí (UCA), což jsou akce, které by v důsledku mohly vést k jednomu nebo více nebezpečím. [5]

STPA rozlišuje 4 způsoby, jak řídicí akce může být nebezpečná. Jedná se o [5]:

- Neprovedení řídicí akce vede k nebezpečí
- Provedení řídicí akce vede k nebezpečí
- Provedení řídicí akce příliš brzo, pozdě nebo ve špatném pořadí vede k nebezpečí
- Provedení řídicí akce trvalo příliš dlouho nebo skončilo příliš brzy, a to vyvolalo nebezpečí

V tomto kroku se rovněž identifikují omezení řídicího prvku, což jsou podmínky pro chování řídicího prvku, které musí být splněny, aby nedocházelo ke stanoveným UCA. [5]

6.1.4 Stanovení scénářů, ve kterých dochází ke ztrátě

Posledním krokem je stanovení ztrátových scénářů neboli scénářů, při kterých dochází k UCA, které dále mohou vyvolat nebezpečí. STPA stanovuje 2 typy scénářů, které musí být vždy zváženy [5]:

- Proč by vznikla daná UCA?
- Proč by nebyla řídicí aktivita správně provedena/ nebyla provedena, a to následně vedlo k nebezpečí?

Vytvoření 1. typu ztrátového scénáře je postaveno na vysvětlení proč řídicí prvek provedl UCA. Důvody, které nejčastěji vedou k tomuto typu scénáře, jsou faktory související s řídicím prvkem (např. fyzické selhání), neadekvátní/chybný algoritmus řízení, nebezpečný řídicí vstup nebo neadekvátní procesní model (např. přijetí chybné zpětné vazby nebo její špatná interpretace). U 2. typu ztrátového scénáře nemusí nutně dojít k UCA ale pouze ke špatnému provedení jinak správné řídicí akce, což může být vyvoláno chybou v její cestě (např. řídicí akce nebyla přijata akčním prvkem[4]) nebo chybou řídicího procesu (např. řídicí akce je provedena ale řízený proces na ni nereaguje). [5]

6.1.5 Využití výstupu STPA

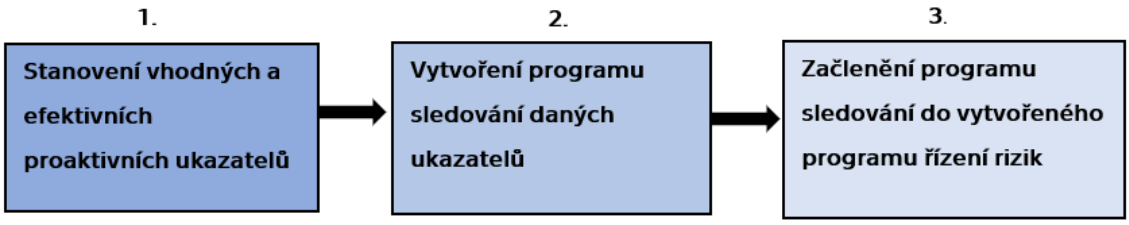
Výsledkem analýzy STPA je zejm. vytvořená řídicí struktura a identifikované parametry jako ztráty, nebezpečí, systémová omezení, UCA a ztrátové scénáře, které jsou vytvořeny na základě obecných předpokladů o systému a jeho fungování. Příkladem takového předpokladu může být např. tvrzení, že v systému je dostatečně implementován SMS. S těmito obecnými předpoklady se tvoří analýza STPA a během jejího procesu mohou vyplynout další předpoklady, které mohou být rovněž dále využívány. Identifikování předpokladů slouží pro stanovení proaktivních ukazatelů výkonnosti v bezpečnosti založených na předpokladech, které jsou kritické z hlediska bezpečnosti. [5] [18] Pro tvorbu proaktivních ukazatelů jsou uvažovány obecně 3 typy předpokladů, kterými jsou [5]:

- Modely a předpoklady použité během návrhu daného systému byly pravdivé.
- Systém bude vytvořen a provozován dle požadavků těch, kteří jej navrhli.

[4] Akční prvek se nachází mezi řídicím prvkem a řízeným procesem na cestě řídicí akce. Akčním prvkem řídicí prvek provádí řídicí akci (např. pedál, volant atd.) [5]

- Modely ani předpoklady nebudou narušeny vlivem změn systému nebo prostředí, ve kterém se nachází.

Pomocí výstupů STPA (zejm. proaktivních ukazatelů založených na předpokladech) lze řídit neplánované změny. Cílem ukazatelů je sledování sociálních a manažerských předpokladů a předpokladů o službách/produktech. Stanovení, co přesně by měl proaktivní ukazatel představovat, jak a kdy by se ukazatel měl měřit, je dosáhnuto dle STPA pomocí programu pro proaktivní ukazatele. [5] Tento program má definované 3 kroky, které jsou znázorněny na obrázku 11.



Obrázek 11: Program proaktivních ukazatelů výkonnosti v bezpečnosti založených na předpokladech, upraveno z [5]

Prvním krokem je stanovení vhodných a efektivních ukazatelů na základě již zmíněných předpokladů. Pro tento krok je nezbytné identifikovat hlavní oblasti příčin nehod, kterými jsou dle STPA management, provoz a návrh a výroba. V těchto oblastech se poté identifikují předpoklady pomocí již vytvořených výstupů STPA a na základě nich se stanoví i proaktivní ukazatele. [5] Zdroje pro vytvoření předpokladů mohou být např. [5]:

- Systémové bezpečnostní cíle
- Předpoklady o prostředí, v němž se systém nachází
- Řídicí struktura
- Nebezpečné řídicí akce
- Ztrátové scénáře
- Limitace předchozích bodů

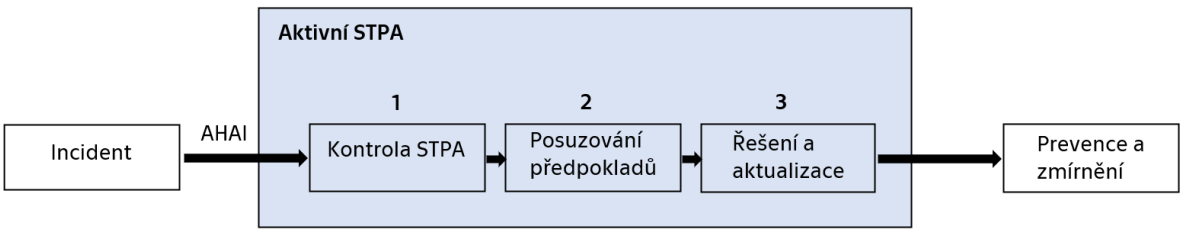
Ve druhém kroku se stanoví tzv. formovací a zajišťovací akce. Formovací akce mají za cíl udržet předpoklad daného proaktivního ukazatele pravdivý a zajišťovací akce mají za cíl systém připravit na eventualitu, že předpoklad přestane být pravdivý. Příkladem formovací akce může být např. fyzické zabránění nebezpečného stavu, navržení úkonů prováděných lidmi tak, aby jejich provedení bylo snadné a zároveň obtížné je neprovést nebo vytvoření zvláštní nezávislé pracovní skupiny s kompetencí vydávat kritická

rozhodnutí z hlediska bezpečnosti. Příkladem zajišťovací akce je např. systém „fail-safe“. V tomto bodě se rovněž řeší kontrola identifikovaných předpokladů. Ty se prověřují a aktualizují v čase kontinuálně/periodicky (např. pomocí auditů, dotazníků nebo sbíraných dat) nebo na základě tzv. směrových bodů, což jsou stanovené situace nebo časové mezníky, které vyvolávají nutné prověření a aktualizaci předpokladů. Příkladem směrových bodů mohou být např. plánované změny týkající se daného systému. [5]

Posledním bodem je začlenění všech definovaných parametrů zejm. proaktivních ukazatelů do již vytvořeného systému řízení rizik. V daném systému je nutné zajistit, že proaktivní ukazatele budou používány na základě platných předpokladů se všemi dále stanovenými parametry (formovací a zajišťovací akce, směrové body), které jsou vytvořeny pomocí daných předpokladů. Pro řízení rizik pomocí těchto ukazatelů je nezbytné rizika řídit nejen během návrhu systému, ale i během jeho provozu. Toho je dosaženo pomocí proaktivního kontinuálního vyhodnocování stavu daného ukazatele, které zajistí v systému včasnou detekci počínajícího nechtěného stavu neboli situace, kdy stanovený předpoklad přestane být platný. Díky včasné detekci je možno provést předem stanovené řízení, které zajistí nápravu tohoto stavu předtím, než se v systému stane některá z nechtěných událostí, na rozdíl od přístupu využívaného v SMM. [5]

6.1.6 Aktivní STPA

Aktivní STPA byla poprvé popsána v roce 2019 a tvoří tak nejnovější část celého modelu STAMP. Jedná se o doplnění analýzy STPA o potřebnou aktualizaci systému v průběhu času, která se provádí pomocí prověření a případné změny předpokladů zmíněných v předchozí kapitole. Předpokladem pro využití Aktivní STPA je již aplikovaná analýza STPA se všemi jejími kroky. [19] Aktivní STPA se provádí pomocí kroků znázorněných na obrázku 12.



Obrázek 12: Aktivní STPA, upraveno z [19]

Celý proces Aktivní STPA se spouští po bezpečnostní události, která v systému proběhla. Jako vstup pro Aktivní STPA se používá Vstup aktivní analýzy nebezpečí (AHAI), který obsahuje popis daného incidentu zapsaného pomocí určeného formátu. Poté se spustí Aktivní STPA, kdy v rámci prvního kroku „Kontrola STPA" se prochází výstupy z již provedené STPA, hledá se odpověď na otázku „Co se stalo?" a na základě toho se dále určují prvky systému, které měly nechtěnému výstupu zabránit. V druhém kroku se určí, které předpoklady byly porušeny, a stanoví se důvod jejich porušení a faktory, které k porušení přispěly. Pokud byl předpoklad porušen poprvé, tak dle Aktivní STPA je to proaktivním ukazatelem, že v systému došlo k nějaké změně. Pokud je předpoklad porušen opakovaně, je zřejmé, že předchozí výstupy Aktivní STPA nebyly efektivní, a s touto informací je poté nutno pracovat v posledním kroku „Řešení a aktualizace". V tomto kroku se pomocí poznatků s předchozích kroků stanoví řešení (ve složitých systémech obvykle více než jedno), které mají za cíl udělat systém bezpečnější, než byl předtím. Objektivním cíle Aktivní STPA, jak již vyplývá z předchozího textu, je tedy schopnost poučit se z chyb, které v systému mohou nastat. [19]

6.2 CAST

Analýza příčin na základě Systémové teorie (CAST) je druhá analýza, která je součástí modelu STAMP. Na rozdíl od analýzy STPA je CAST reaktivní analýzou, která se zabývá situacemi, které se již staly. Tato analýza se používá retrospektivně na identifikování příčin nehod a incidentů, ve kterých došlo k nějaké ztrátě, a k navržení opatření pro snížení jejich výskytu. Příčinami nehod a incidentů se zabývaly již mnohé analýzy, avšak ty často vedly k závěru jedné kořenové příčiny, zjednodušení reality a přisuzování viny lidskému selhání, což rozhodně není vhodný závěr zejm. u složitých/komplexních socio-technických systémů. Cílem analýzy CAST je zjistit jaké všechny příčinné faktory vedly k nehodě/ incidentu z pohledu celého systému, poučit se z vlastních chyb a podniknout na jejich základě patřičné kroky k prevenci. CAST a celý model STAMP nevnímá nehodu/incident jako selhání někoho/něčeho ale jako chybu řízení. [20]

Analýza CAST se provádí dle následujících kroků [20]:

1. Shromáždění základních informací
2. Modelování řídicí struktury
3. Analyzování jednotlivých komponentů ohledně ztráty
4. Identifikování nedostatků řídicí struktury
5. Vytvoření plánu zlepšení

Kroky uvedené výše kopírují částečně kroky STPA s rozdílem posledních dvou kroků a celkového zaměření na jednu konkrétní událost. Rovněž oproti STPA mají všechny kroky jako součást vytváření otázek „*Proč?*“ a hledání jejich odpovědí. [20]

6.2.1 Shromáždění základních informací

V prvním kroku se obecně popisuje, jaká událost se stala, a co je cílem analýzy CAST. Je zde nutné popsat systém a jeho hranice, ve kterém se nehoda stala, k lepšímu pochopení události. Dále se stanoví, jaká systémová nebezpečí se vyskytla, a jaká bezpečnostní omezení byla porušena. [20]

6.2.2 Modelování řídicí struktury

Druhým krokem je vytvoření modelu řídicí struktury a stanovení zodpovědností řídicích prvků stejně jako ve druhém kroku STPA. Pokud se v systému využívají analýzy CAST a STPA simultánně, není třeba zde řídicí strukturu ani zodpovědnosti opětovně vytvářet, ale využít již ty vytvořené z analýzy STPA. [20]

6.2.3 Analyzování jednotlivých komponentů ohledně ztráty

Ve třetím kroku se prochází celá řídicí struktura zdola nahoru, analyzují se role jednotlivých řídicích prvků v události dle jejich zodpovědností a jejich podíl na vzniklé události (např. neprovedení určité řídicí akce) a proč tomu tak bylo, pokud nějaký podíl řídicí prvek na události má. Tento krok odpovídá čtvrtému kroku STPA, kdy se vytvářely ztrátové scénáře. [20]

6.2.4 Identifikování nedostatků řídicí struktury

Všechny předchozí kroky analýzy CAST se víceméně zaměřovaly na jednotlivé části systému, čímž se zabývaly i starší modely bezpečnosti např. již výše zmíněný model švýcarského sýra. Předposlední krok se již zaměřuje na celý systém a na systémové faktory, které působí na řídicí prvky, a přispěly k dané události. A právě tento krok dělá z CAST jedinou systémovou analýzu. [20]

Systémové faktory, které mohou přispět k nehodě/incidentu jsou např. [20]:

- Komunikace a koordinace
- Bezpečnostní informační systém
- Bezpečnostní kultura
- Design SMS
- Změny a dynamika v čase
- Interní a externí ekonomika a s ní spojené faktory

Z hlediska zaměření této diplomové práce jsou nejdůležitějším systémovým faktorem změny a dynamika v čase, které často působí jako katalyzátory nehody/ incidentu. V této části jsou opět změny rozděleny na plánované a neplánované. Pro neplánované změny, které ovlivňují bezpečnost, musí být v systému stanovený postup pro jejich detekci, který je založený na proaktivních ukazatelích výkonnosti v bezpečnosti (viz kapitola 6.1.5), bezpečnostně zaměřených auditech a periodické revizi předpokladů o systému. [20]

6.2.5 Vytvoření plánu zlepšení

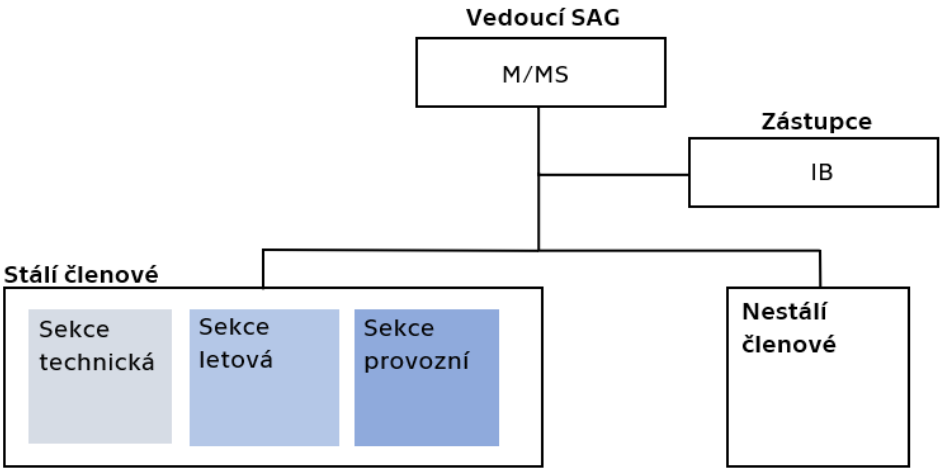
Na základě veškerých výstupů této analýzy je cílem posledního kroku vytvoření doporučení ohledně změn řídicí struktury, na jejichž základě by mělo dojít ke zmírnění nebo odstranění rizik, které přispěly k dané události. [20]

7 Současný přístup k řízení neplánovaných změn v rámci SSP ČR

Jak již bylo řečeno, funkci výkonného dozorového orgánu zastává ve státní správě České republiky ÚCL . Tento úřad je dle stanov SSP ČR pověřen odpovědností ve věcech dozoru nad subjekty civilního letectví, vytváření a vedení SSP ČR a v rámci jeho pravomocí je rovněž řízení plánovaných i neplánovaných změn. Přístup, jakým ÚCL přistupuje a řídí neplánované změny, je popsán ve směrnici ÚCL-331 „Zpracování informací o bezpečnosti", která byla uvedena v platnost v roce 2019 na návrh ředitele ÚCL. [21]

7.1 Složení SAG

Řízením neplánovaných změn se na ÚCL zabývá skupina pro řešení otázek bezpečnosti (SAG) , která byla vytvořena jako poradní skupina ředitele ÚCL. Cílem zřízení této skupiny je, jak již z jejího názvu vyplývá, řešení implementace principů SMS a vytváření a předkládání návrhů s cílem zvýšení bezpečnosti řediteli ÚCL. Rovněž SAG zajišťuje sjednocení postupů napříč sekcemi ÚCL a komunikace s ÚZPLN či jinými orgány. Hlavní náplní skupiny SAG je tedy průběžné posuzování a hodnocení bezpečnostních rizik a vytváření návrhů k jejich zmírnění/prevenci. [21] Struktura skupiny SAG je znázorněna na obrázku 13.



Obrázek 13: Složení skupiny SAG [21]

Skupina SAG se skládá z vedoucího, kterým je manažer systému řízení (M/MS), jeho zástupce, kterým je inspektor bezpečnosti (IB) a stálých a nestálých členů. Vedoucí skupiny SAG zodpovídá za plánování a řízení jednání SAG, zpracování informací pro účely

těchto jednání, vedení agendy a předávání závěrečných ustanovení jednotlivých jednání. Pevný počet zbylých členů není pro SAG dán, avšak jsou stanoveny nutné oblasti pokrytí, které jsou určeny pro sekci technickou, letovou a provozní, jak je vidno z obrázku 13. Za sekci letovou musí být pokryty oblasti letového provozu, obchodní letecké dopravy, neobchodního/zvláštního provozu a letových posádek. Za sekci provozní jsou to oblasti letišť, poskytovatelů navigačních služeb a regulace. Za sekci technickou musí být pokryta oblast letové způsobilosti. Nestálí členové slouží k pokrytí dalších oblastí, které mají nižší četnost než výše uvedené (např. oblast parašutismu) a účastní se jednání SAG pouze v jejich nutnosti. Jednání SAG obvykle probíhá jednou za kalendářní měsíc nebo častěji, pokud situace vyžaduje jednání dříve. [21]

7.2 Informační zdroje činnosti SAG

Jednání jsou vždy vedena na základě přijatých informací z daných informačních zdrojů povinných a dobrovolných hlášení. Do povinných hlášení se řadí veškeré události popsané ve článku 4 „Povinná hlášení" Nařízení Evropského parlamentu a Rady (EU) č. 376/2014. Mezi ně se řadí např. události spojené s provozem letadla, údržbou, opravou letadla nebo navigačních služeb. Seznam dobrovolných hlášení je shrnut ve článku 5 „Dobrovolná hlášení" téhož nařízení a jeho hlavním cílem je zachytit informace neobsažené v prvotním povinném hlášení. Dobrovolná hlášení rovněž slouží pro zachycení informací o události/situaci, které nahlašující identifikoval jako ohrožující bezpečnost. [21] [22]

Mezi zdroje informací, která slouží pro jednání SAG, patří [21]:

- Systém povinného a dobrovolného hlášení EU
- Dobrovolná hlášení událostí v civilním letectví ÚCL
- Podněty prezentované zaměstnanci ÚCL

7.2.1 Systém povinného a dobrovolného hlášení EU

Systémem povinného a dobrovolného hlášení EU je myšlen systém, který vznikl a je veden na základě nařízení Evropského parlamentu a Rady (EU) č.996/2010 a č. 376/2014. [21] Pro účely tohoto systému slouží platforma nesoucí název Evropské koordinační středisko pro systémy hlášení nehod a incidentů (ECCAIRS), která byla vytvořena za pomoci Společného výzkumného střediska (JRC). Od roku 2020 je v používání ECCAIRS 2, který již plně využívá webového rozhraní[5]. ECCAIRS (jak nová, tak i jeho starší verze)

[5] www.aviationreporting.eu

využívá taxonomii ECCAIRS[6], která byla vytvořena rozšířením taxonomie ADREP od ICAO. Systém ECCAIRS 2 tedy umožňuje podat hlášení jak ze stran jednotlivých CAA nebo AAII, tak i fyzických osob pomocí internetového formuláře. Data z podaných formulářů jsou poté sdílena mezi členskými státy. [23] Hlášení z tohoto zdroje jsou sdílena mezi ÚCL a ÚZPLN na základě Dohody o spolupráci pomocí komunikace přes inspektora bezpečnosti. ÚCL jsou rovněž sdíleny závěrečné zprávy šetření a závěrečná doporučení vyplývající z šetření. [21]

7.2.2 Dobrovolná hlášení událostí v civilním letectví ÚCL

Dobrovolná hlášení v rámci ÚCL jsou sbírána pomocí elektronického formuláře[7]. Tento formulář slouží pro dobrovolná hlášení, která jsou definována v této kapitole, a je určen zejm. pro jakýkoliv subjekt civilního letectví, jejich zaměstnance a širokou veřejnost. Tento systém již nevyužívá žádné taxonomie, nýbrž využívá pouze textové pole pro popis události, její čas, místo a případně kontakt na osobu, která hlášení podává. [25]

7.2.3 Podněty prezentované zaměstnanci ÚCL

Posledním zdrojem jsou podněty od zaměstnanců ÚCL, a to jak od členů SAG, tak i ostatních zaměstnanců, kteří nejsou členy. Ti používají k podání podnětu jakéhokoliv člena SAG. [21]

7.3 Zpracování dat z informačních zdrojů

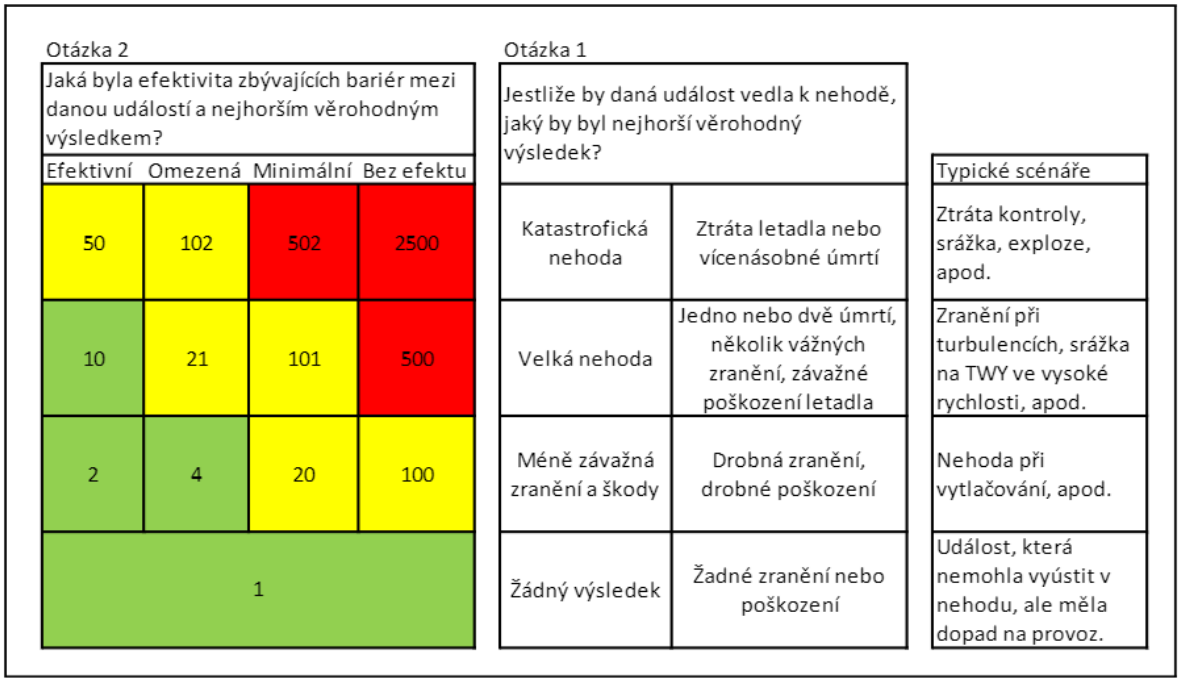
Jak již bylo řečeno výše, hlavním koordinátorem informací z uvedených informačních zdrojů je inspektor bezpečnosti. Ten zodpovídá za prvotní příjem a zpracování informací, který zajišťuje pomocí bezpečnostního informačního systému (SISel). Účelem systému SISel je zabezpečení evidence a zpracování hlášení a momentálně slouží jako podpůrný nástroj pro činnost skupiny SAG. Povinná i dobrovolná hlášení jež jsou podávána ve formátu, který je kompatibilní se systémem ECCAIRS, SISel přijímá automaticky. Ovšem hlášení dle leteckého předpisu L13 nebo dobrovolná hlášení ÚCL obvykle tento formát nesplňují a je třeba jejich ruční zadání do systému, které provede vedoucí SAG nebo jeho zástupce. Ruční zadání se provádí na základě přijatého prvotního hlášení prostřednictvím e-mailu, který je rozesílán inspektorem bezpečnosti manažerovi systému řízení, ředitelům sekcí a odborů a zaměstnancům, jež jsou členy skupiny SAG.

[6] Taxonomie v letectví obecně slouží pro standardizovaný zápis incidentů, nehod a faktorů, které k nim přispěly. Každý faktor a typ události má své dané číslo pomocí kterého se identifikuje. Seznam veškerých faktorů a událostí je dostupný např. na www.aviationreporting.eu. [24]

[7] Elektronický formulář je dostupný na stránce ÚCL www.caa.cz.

Na prvotní hlášení se vztahuje princip ochrany ohlašovatele, který udává nařízení Evropského parlamentu a Rady (EU) č. 376/2014, neboť toto hlášení stále obsahuje neanonymizované informace. V případě dalšího rozesílání je nutno seznámit zaměstnance s náležitostmi, které práce s těmito daty obnáší. [21]

Poté co jsou v systému SISel zaneseny již anonymizované informace, tedy dojde k vymazání informací o osobách podílejících se na události, vedoucí SAG událost dále zpracuje ve smyslu doplnění veškerých faktorů pomocí taxonomie ECCAIRS, které k události přispěly, a vazeb mezi nimi. Každá událost má v systému SISel svoje referenční číslo a příznak udávající kategorii události, o kterou se jedná např. zkratka PARA pro událost spojenou s parašutismem. V systému SISel je rovněž již zavedený systém na hodnocení prvotního rizika, který je založen na metodologii ARMS-ERC (Řešení pro řízení rizik v letectví-Klasifikace rizika události). [21] Proces číselného ohodnocení rizika dané události je znázorněn na obrázku 14.



Obrázek 14: Matice ERC [26]

Jak je patrné na obrázku výše, číselné hodnocení se stanoví na základě odpovědí na otázky nejhoršího možného výsledku dané situace a efektivity nastavených bariér pro zabránění takového výsledku. [26] Informace se poté dále aktualizují na základě informací poskytnutých ÚZPLN, vnitřního šetření ÚCL nebo informací z dozorové činnosti. SAG ve svém posuzování rozděluje 4 základní kategorie událostí dle číselného ohodnocení, které jsou znázorněny v tabulce 2. [21]

Tabulka 2: Kategorie ARMS-ERC dle ÚCL [21]

Typ události	ARMS index	Reakce SAG
Zelené události	≤10	Není řešeno
Žluté události	<100	Sledování vývoje trendu dané události
	≥100	Projednáváno na jednání SAG, stanovení reakce ÚCL
Červené události	≥500	Okamžité řešení

7.4 Reakce SAG na hlášené události

Jak již vyplývá z tabulky 2, SAG dělí události na 4 kategorie dle indexu ARMS a dle této klasifikace následně SAG rozhoduje o případných dalších krocích, které bude třeba učinit. Obecně nejmenší závažnost mají události, při kterých by došlo v nejhorším možném výsledku k méně závažným škodám a efektivita nastavených bariér byla vysoká. Tyto události mívají ARMS index 10 a méně a SAG tyto události, pokud není rozhodnuto jinak, dále neřeší a pouze vede jejich evidenci. Události, které již neměly tak efektivní bariéry nebo by v jejich důsledku mohlo dojít nehodě, spadají dle SAG do druhé kategorie s ARMS indexem do 100. Tyto události jsou zkoumány s větším detailem a rovněž je sledován vývoj trendu. Opět ale platí, že blíže se těmito událostmi SAG na jednání nezabývá, pokud není rozhodnuto inspektorem bezpečnosti o nutnosti konkrétní událost projednat více. Největší prioritou skupiny SAG jsou poslední dvě kategorie událostí, a totiž události nabývající hodnoty indexu ARMS 100 a více, které jsou projednávány jednotlivě na jednání SAG. [21]

Pokud událost mohla vyvolat vážnou nehodu a bariéry v tomto případě byly již značně omezené/ minimální, jedná se o událost a indexem 100 a více (nejvyšší hodnota 102), která odpovídá třetí kategorii událostí. Poslední kategorií událostí jsou ty ohodnocené indexem 500 a výše, do kterých patří události s možnou velmi vážnou nehodou a s bariérami bez efektu. Pro obě tyto kategorie je zpracována vedoucím skupiny SAG přehledová tabulka, ve které je rovněž uvedena předpokládaná sekce mající kompetenci v dané oblasti. Pro události s indexem 500 a výše jsou tyto informace zpracovány okamžitě a o dalším postupu a řešení rozhoduje vedení ÚCL. Členové SAG jsou v tomto případě pouze informování o závěru prostřednictvím vedoucího skupiny SAG. Události s indexem 100-102 jsou řešeny na jednáních skupiny SAG, které jsou vedeny na základě stanoveného programu jednání. Přehledová tabulka je zaslána pro tyto události vždy alespoň 1 týden před datem jednání. [21]

7.4.1 Program jednání SAG

Před každým jednáním vypracuje vedoucí SAG program jednání, dle kterého se následující jednání vede. Program vždy reflektuje hlášené a kategorizované události, které proběhly mezi jednotlivými jednání SAG. Standardní interval jednání je jeden měsíc, pokud nenastala nutnost svolat jednání dříve. [21]

Mezi nejdůležitější body programu patří [21]:

- Počet událostí za období v daných kategoriích
- Události s možnou prevencí
- Stanovení a posouzení možných bezpečnostních problémů
- Stanovení návrhů pro zvýšení výkonnosti v bezpečnosti
- Trendy ukazatelů výkonnosti v bezpečnosti (data exportovaná ze systému SISeI)

Dále se do programu mohou zařadit body ohledně příležitostí pro členy skupiny SAG (např. školení), důležité informace (např. změna legislativy), diskuse ohledně předchozích bodů nebo body, které chtějí projednat někteří členové. Návrh programu zašle vedoucí členům SAG, kteří jej mohou připomínkovat ohledně jeho obsahu. [21]

7.4.2 Jednání SAG

Obecně jednání SAG začíná oficiálním schválením programu jednání, ve kterém probíhá opětovné možné vznesení připomínek k stanovenému návrhu. Poté již jednání probíhá dle schválených bodů programu, kdy každý bod musí mít svůj oficiální závěr nebo alespoň úkol, který má stanovenou pevnou dobu jeho splnění. Jeden z hlavních bodů celého jednání SAG je řešení událostí s indexem 100 a výš. Pro každou takovou událost je projednávána správnost ARMS indexu a stanovených faktorů přispívajících k dané události. Rovněž je projednáváno, jaký je závěr pověřené sekce neboli zda se budou událostí nadále zabývat a popř. způsob, který k tomu příslušná sekce zvolila (např. formou mimořádného dozoru, sankčním řízením nebo požádáním o vyjádření provozovatele). V případě dalšího řešení dané události ji SAG sleduje do jejího uzavření. Z průběhu jednání je vytvořen zápis, který se podepsaný přítomnými členy skupiny SAG odesílá řediteli ÚCL ke schválení. [21]

Během jednání SAG jsou probrány závažné události předchozího období, které SAG v kompetenci má. Projednávání událostí, faktorů a trendů ukazatelů výkonnosti v bezpečnosti vede k určitým závěrům, pomocí kterých se ÚCL snaží těmto událostem předcházet. V rámci diskuse nad nimi jsou právě i neplánované změny, které SAG může ve svých závěrech zvážit, a navrhnout další postup. [21] Přístup, který je na ÚCL v tomto

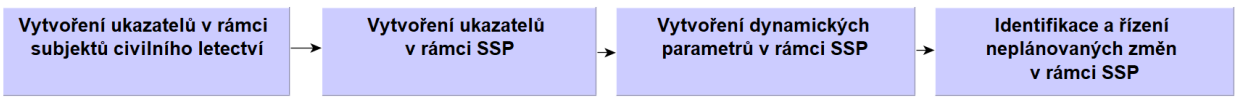
smyslu využíván, je založen zejména na reaktivním přístupu, tedy uvažování o proběhnutí a řízení neplánované změny až poté, co se určitá událost stala. Tento přístup je založen na tom, jak řízení neplánovaných změn popisuje ICAO v SMM.

8 Návrh systémového řízení neplánovaných změn v rámci SSP

Současný přístup k řízení neplánovaných změn v rámci SSP, který v uvedeném příkladu je popsán pro Českou republiku (viz kapitola 7), není systémový a pracuje zejm. pomocí výkonnosti v bezpečnosti, ke které využívá staršího přístupu ICAO vyplývajícího z myšlenek Safety I.. Řízení neplánovaných změn dle ICAO a celý dokument SMM, který udává doporučenou strukturu SSP i postup, jak jej tvořit, je stále nejdůležitějším dokumentem pro tvorbu SSP jak v České republice, tak i v ostatcích členských státech ICAO. Tento dokument ovšem sám neudává konkrétní způsob, jak pracovat dynamicky a proaktivně s identifikováním a řízením neplánovaných změn, a v současném přístupu tento fakt tvoří významné limitace. Dalším možným řešením je metodika SAM, která již změny řeší systematicky, avšak neudává přesný postup (konkrétní analýzu), a neplánované změny řeší oproti plánovaným změnám velmi okrajově.

Pro návrh řízení neplánovaných změn byl proto vybrán systémový model STAMP, který je popsán v kapitole 6. Pomocí analýz modelu STAMP byl navržen postup, jak v rámci SSP proaktivně identifikovat neplánované změny, a jak je dynamicky řídit s využitím systémového přístupu. Pro návrh řešení této problematiky byly využity všechny analýzy modelu STAMP z důvodu jejich vzájemného propojení a jejich simultánní používání je vhodné nejen v rámci řízení neplánovaných změn, ale i v rámci celého potenciálního systémového SSP. Obecně byla v návrhu využita analýza CAST jako nezbytný nástroj pro systémové šetření událostí, STPA pro stanovení parametrů nezbytných pro identifikaci neplánovaných změn a Aktivní STPA byla využita jako nástroj pro samotnou identifikaci a řízení neplánovaných změn v provozu a nutnou aktualizaci systému v čase.

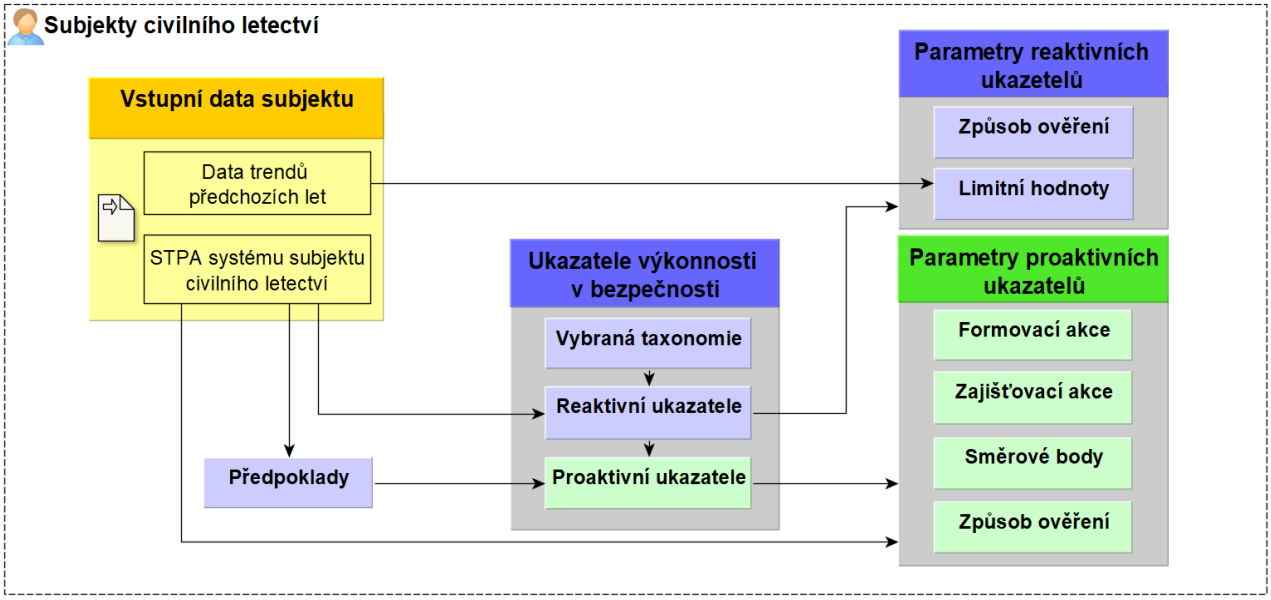
Tato kapitola se bude věnovat detailnějšímu popisu návrhu řešení pro systémovou identifikaci a řízení neplánovaných změn, jehož kroky znázorňuje obrázek 15.



Obrázek 15: Základní schéma systémového řízení neplánovaných změn v rámci SSP

8.1 Vytvoření ukazatelů v rámci subjektů civilního letectví

Prvním krokem nezbytným pro systémovou identifikaci a řízení neplánovaných změn je vytvoření ukazatelů v rámci subjektů civilního letectví. Jednotlivé části tohoto procesu jsou znázorněny na obrázku 16.



Obrázek 16: Vytvoření ukazatelů v rámci subjektů civilního letectví

Základem pro vytvoření ukazatelů výkonnosti v bezpečnosti, nejen pro subjekty civilního letectví, je vytvoření analýzy STPA se všemi jejími kroky. Pomocí výstupů analýzy zejm. identifikovaných systémových ztrát a nebezpečí jsou určeny patřičné reaktivní ukazatele z vybrané taxonomie. Pro účely tohoto návrhu lze využít současnou taxonomii ECCAIRS, která je popsána v kapitole 7.2.1. Dále je nutné pro reaktivní ukazatele stanovit jejich parametry znázorněné na obrázku 16. Je tedy nutné stanovit způsob jejich ověření, který představuje nějaký zavedený systém nebo řídicí akci, pomocí které jsou zjišťovány skutečné hodnoty daného ukazatele. Rovněž je vhodné stanovit limitní hodnoty k daným reaktivním ukazatelům, které slouží jako nástroj pro zajištění adekvátních reakcí při příliš dlouhém přehlížení zvýšených hodnot ukazatele. Jako limitní hodnoty budou využity násobky směrodatných odchylek, které jsou stanoveny na základě hodnot dat z předchozích období.

Pro proaktivní ukazatele je třeba stanovit kritické předpoklady, které mohou být vytvořeny např. na základě systémových omezení, ztrátových scénářů nebo UCA z STPA subjektu. Pomocí těchto předpokladů jsou potom vytvořeny proaktivní ukazatele, které mají za cíl monitorovat faktory ovlivňující reaktivní ukazatele. Dle STPA je třeba ke

každému takovému ukazateli stanovit formovací a zajišťovací akce, směrové body (viz kapitola 6) a stejně jako u reaktivních ukazatelů také způsob jejich ověření.

8.2 Vytvoření ukazatelů v rámci SSP

Po kroku kapitoly 8.1 následuje dle obrázku 15 druhý krok návrhu znázorněný na obrázku 17, kterým je vytvoření ukazatelů v rámci SSP. Tento krok již obstarává systém státní správy a dozoru, a to konkrétně jednotlivé CAA, které již určité ukazatele výkonnosti v bezpečnosti monitorují a hodnotí. Výběr těchto ukazatelů v rámci SSP je však nyní primárně zaměřen na reaktivní ukazatele, které ovšem v tomto případě potenciální neplánovanou změnu neindikují včas, a v systému se projeví až nějakou nechtěnou bezpečnostní událostí. V rámci systémového SSP by bylo vhodné, aby si obdobně jako subjekty civilního letectví v předchozím kroku vytvořily STPA orgány systému státní správy a dozoru (zejm. jednotlivé CAA.) z důvodu celkového systémového přístupu k civilnímu letectví.

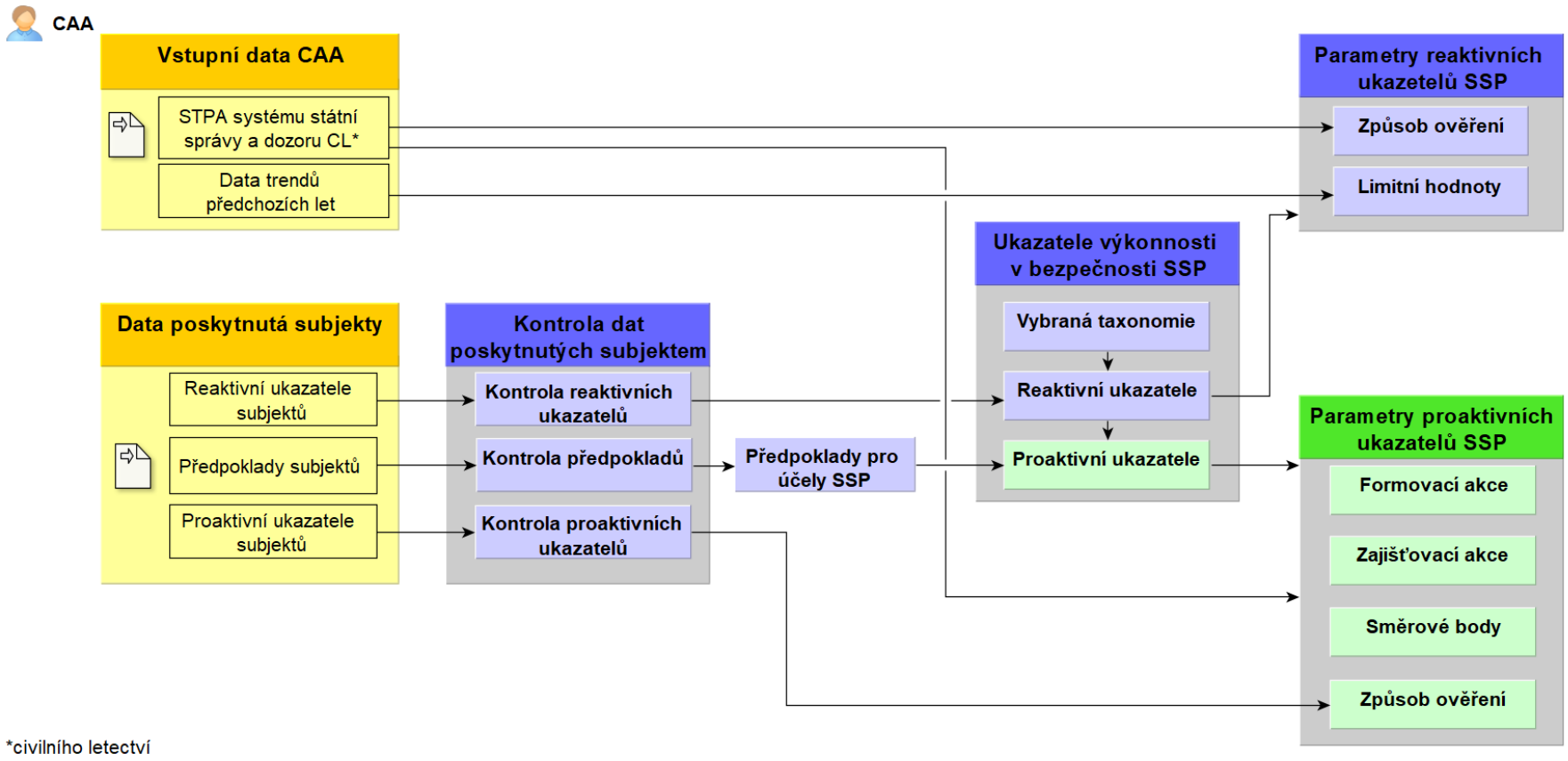
Pro stanovení ukazatelů výkonnosti v bezpečnosti a jejich parametrů v rámci SSP je nejdůležitější, aby si subjekty civilního letectví vytvořily předpoklady a proaktivní a reaktivní ukazatele dle kapitoly 8.1, a následně je poskytly CAA. Po zaslání výše uvedených dat je třeba ze strany CAA provést kontrolu jejich kompletnosti a správnosti. U reaktivních ukazatelů je třeba zkontrolovat zejm. to, zda jsou uvedeny veškeré ukazatele týkající se daného subjektu a zda jsou správně formulovány, tedy že odpovídají ukazatelům z vybrané taxonomie. U předpokladů je třeba posoudit, zda jsou stanoveny v náležitém detailu a jsou stanoveny pro všechny procesy, které mohou vyvolat nějaké nebezpečí. Pokud jsou proaktivní ukazatele shodné s předpoklady, tj. proaktivní ukazatele jsou brány jako tvrzení hodnocené kvalitativně (např. splněno nebo nesplněno), postačí pouze kontrola předpokladů, a není třeba provádět kontrolu i proaktivních ukazatelů. Pokud tomu tak není, je třeba provést i kontrolu proaktivních ukazatelů, při které se zkontroluje, zda jsou ukazatele stanoveny pro veškeré předpoklady a odpovídají jim. Pokud CAA uzná, že data poskytnutá subjektem nesplňují tyto kritéria, zašle je zpět subjektu, který musí zjednat nápravu označených dat. Tento postup je znázorněn na obrázku 18. Teprve, když CAA obdrží od subjektu správné a kompletní reaktivní a proaktivní ukazatele a předpoklady, je možné v procesu 2. kroku návrhu pokračovat.

CAA poté na základě stanovených reaktivních ukazatelů subjektu stanoví reaktivní ukazatele na úrovni SSP dle taxonomie, která bude využívaná v rámci SSP (v tomto návrhu taxonomie ECCAIRS). Při využití stejné taxonomie subjektu i CAA budou při

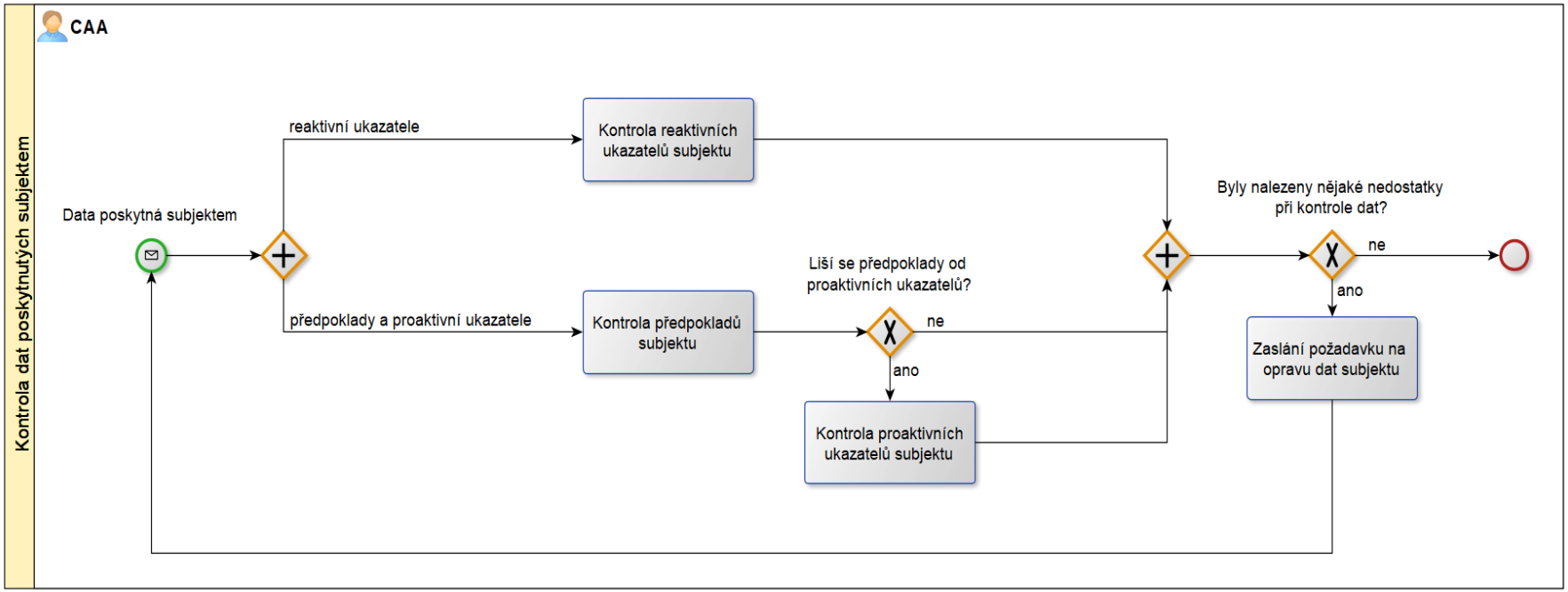
kompletnosti a správnosti reaktivních ukazatelů subjektu reaktivní ukazatele CAA i subjektu shodné . Dále se pomocí STPA CAA a částečně i STPA AAII k reaktivním ukazatelů stanoví způsob jejich ověření a získání jejich reálných hodnot, což v případě reaktivních ukazatelů tvoří zejm. systém pro povinná/dobrovolná hlášení a šetření nehod a incidentů. Rovněž se pro reaktivní ukazatele nastaví pomocí dat trendů předchozích let hodnoty směrodatných odchylek a jejich násobky, které budou sloužit jako záchytné body pro vyvolání reakce CAA při dlouhodobém přehlížení zvýšených hodnot daného reaktivního ukazatele.

Pro proaktivní ukazatele je třeba nejprve stanovit kritické předpoklady na úrovni SSP, které budou vytvořeny na základě předpokladů subjektu, tak, aby odpovídaly systémové úrovni tvrzení, u kterého je CAA schopno ověřit jeho platnost. Na základě takto vytvořených předpokladů CAA dále vytvoří proaktivní ukazatele, které budou v systému civilního letectví pomáhat k identifikaci neplánované změny dříve, než se tato skutečnost projeví v trendech jednoho z reaktivních ukazatelů. I pro proaktivní ukazatele v rámci SSP musí být stanoveny čtyři již výše zmíněné parametry viz obrázek 17. Formovací akce představují způsoby, jakými CAA jakožto dozorový orgán pomáhá udržet předpoklady v rámci SSP pravdivé a zároveň jimi tuto platnost prověřuje[8]. Zajišťovací akce jsou již reakce na situaci, kdy předpoklady přestanou platit. Oba typy akcí jsou tedy určité řídicí akce CAA vůči subjektu, které vycházejí z řídící struktury STPA CAA. Dále je nutné určit směrové body určující události, které by mohli ovlivnit platnost předpokladů a je tedy třeba jejich aktuální platnost ověřit formovací akcí. Směrové body většinou tvoří plánované změny subjektu, legislativy vztahující se na daný subjekt, nebo jakákoliv jiná událost/situace mající vliv na platnost předpokladu. Posledním parametrem pro proaktivní ukazatele je na obrázku 17 zmíněn způsob ověření. Ty vycházejí z proaktivních ukazatelů subjektu, které v tomto případě stanovují oblasti, ve kterých subjekt aktivně sbírá data. Znalost oblastí aktivního sběru dat je poté využita právě pro stanovení způsobu ověření neboli jaká data bude CAA kontrolovat při formovacích akcích a pomocí ostatních datových zdrojů.

[8] Příkladem takové formovací akce ze strany ÚCL může být provádění pravidelných auditů. Pomocí auditů nejen ÚCL zjišťuje hodnoty ukazatelů, tj. platnost předpokladů na jejichž základě byly ukazatele vytvořeny, ale rovněž se prováděním auditů a jejich závěry snaží udržet předpoklady pravdivé, protože vytváří určitý tlak na subjekt, aby on sám udržoval platnost daných předpokladů



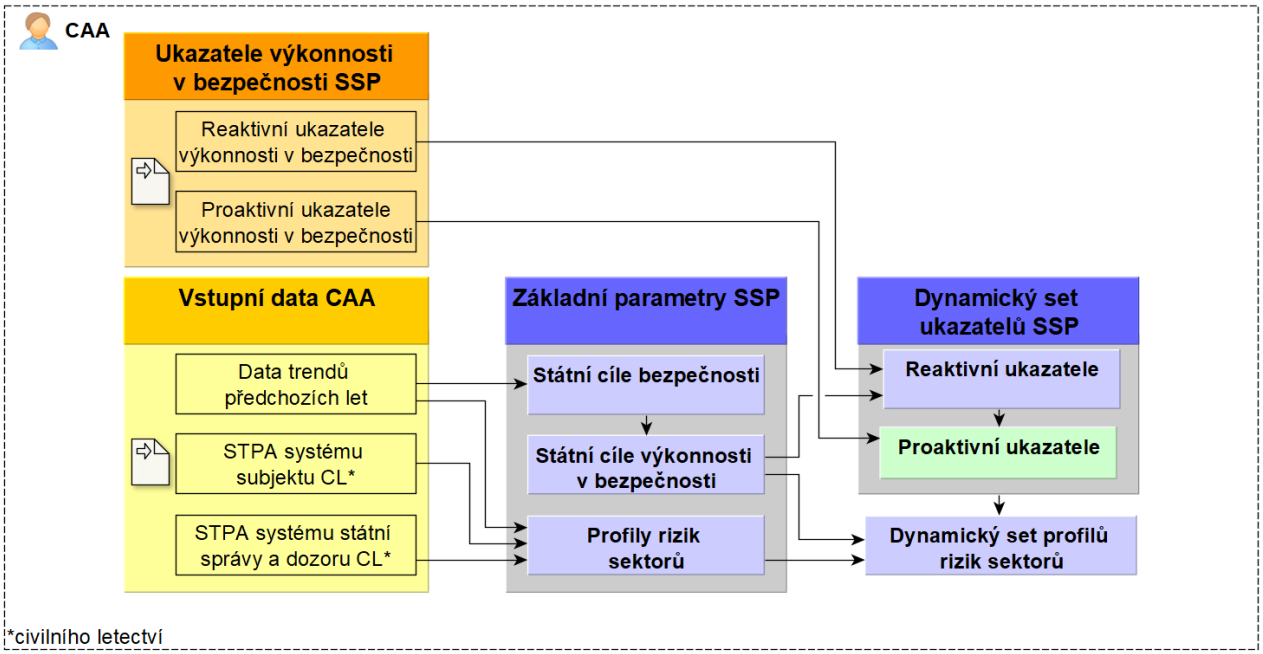
Obrázek 17: Vytvoření ukazatelů v rámci SSP



Obrázek 18: Kontrola dat poskytnutých subjektem

8.3 Vytvoření dynamických parametrů v rámci SSP

Ve třetím kroku systémového řízení neplánovaných změn je řešen proces vytvoření dynamických parametrů, které jsou dále využity v tzv. bezpečnostních panelech (viz kapitola 3.3). Mezi dynamické parametry v tomto návrhu patří dynamické sety ukazatelů a dynamické sety profilů rizik dle sektorů civilního letectví, které dále určují, jaká data budou znázorněna na bezpečnostních panelech. Ty mají za cíl znázornit vybraná nejdůležitější data z hlediska provozní bezpečnosti a vytvořit tak přehledný nástroj pro jejich sledování. Dynamické parametry a bezpečnostní panely jsou dnes již běžně využívány, nicméně zobrazované parametry nejsou systémově vytvářeny, a proto je v návrhu zahrnut i tento krok. Proces vytvoření dynamických parametrů v rámci SSP je zobrazen na obrázku 19.



Obrázek 19: Vytvoření dynamických parametrů v rámci SSP

Nejprve je nutné stanovit státní cíle bezpečnosti a cíle výkonnosti v bezpečnosti, které se v rámci SSP momentálně stanovují dle SMM ve 3. kapitole SSP. Pro stanovení aktuálně nejdůležitějších oblastí, které výše zmíněné cíle představují, jsou využita data trendů předchozích let, jako je tomu i doposud. Stanovené cíle představují většinou nějaký progres hodnot reaktivního ukazatele za určité časové období, kterého je v systému zamýšleno dosáhnout. Státní cíle výkonnosti v bezpečnosti se od státních cílů bezpečnosti liší pouze v kratším časovém měřítku a o tento časový rozdíl poměrně zkrácenou hodnotou, které chceme dosáhnout, což pomáhá při kontrole jejich plnění. Jako poslední jsou v této části návrhu (viz obrázek 19) zmíněny profily rizik. Ty jsou

současně většinou využívány pro jednotlivé subjekty. V takovýchto profilech jsou trendy a ostatní informace vztaženy na vybraný subjekt civilního letectví. V systémovém přístupu jde ale především o zacházení se systémem jako s celkem. Sledovat tak trendy určitých ukazatelů pouze v kontextu jednoho subjektu se zdá jako méně efektivní. Rovněž to může působit zjednodušeně, protože na procesech civilního letectví, a tedy i na ukazatelích výkonnosti v bezpečnosti, se většinou podílí alespoň 2 subjekty současně (např. spolupráce letiště, handlingové společnosti a letecké společnosti při odbavení). Proto je z tohoto důvodu v návrhu využita myšlenka profilů rizik sektorů, které se týkají určité oblasti civilního letectví a všech subjektů v ní působící. Tyto profily jsou vytvořeny na základě STPA subjektů a orgánů systému státní správy a dozoru. Dynamické parametry v rámci SSP tedy stanovují primární ukazatele, které jsou v zájmu systému státní správy a dozoru, a rovněž kdo se na těchto ukazatelích podílí dle rizikových profilů sektorů civilního letectví.

8.4 Identifikace a řízení neplánovaných změn v rámci SSP

Poslední částí dle obrázku 15 je již samotný proces identifikace a řízení neplánovaných změn, který je znázorněn na obrázku 20. Jednou z nejdůležitějších částí tohoto kroku je sběr dat z datových zdrojů. Sběr dat probíhá pomocí ověřování platnosti stanovených předpokladů v rámci SSP. Platnost těchto předpokladů je ověřována na základě způsobů ověření a formovacích akcí daných ukazatelů v rámci SSP neboli akcí, které státní orgány provádí pro udržení ale i zjištění platnosti daných předpokladů. Pomocí tohoto ověřování získává CAA nejen reálné hodnoty proaktivních i reaktivních ukazatelů, ale z hlediska neplánovaných změn i informace o směrových bodech, které byly popsány ve 2. kroku tohoto návrhu.

Mezi hlavní datové zdroje ověřování předpokladů pro neplánované změny v rámci SSP patří:

1) Systém pro dobrovolná/povinná hlášení
2) Provádění auditů, kontrol a inspekcí
3) Šetření leteckých nehod a incidentů
4) Proces plánovaných změn
5) Ostatní data poskytována subjekty

Všechny výše uvedené datové zdroje se v současnosti již využívají. Jediné, co by se v tomto případě změnilo, je možný způsob ověřování v daném datovém zdroji neboli formovací akce, kterými se předpoklady ověřují. Pro plné využití potenciálu

systémového přístupu by bylo vhodné např. pro šetření leteckých nehod a incidentů využívat analýzu CAST nebo posuzovat plánované změny pomocí STPA.

Sbíraná data popsána výše jsou dále vyhodnocována dle stanovených ukazatelů a jejich parametrů. Pokud se navíc jedná o některý z ukazatelů dynamického setu, tato data budou navíc zobrazena na bezpečnostním panelu z důvodu jejich důležitosti. Postup vyhodnocování dat je popsán dále.

8.4.1 Vyhodnocování dat

Proces vyhodnocování dat je aktivován, jak je patrné z obrázku 21, příchozí informací z datového zdroje. Tato informace je nejprve zařazena dle sektoru/oddělení CAA, které se daná informace týká. Po zařazení je informace patřičnou osobou sektoru/oddělení vyhodnocena, nebo v případě pokud se informace týká více oblastí, může vyhodnocení proběhnout za spolupráce dalších osob CAA. Primární otázkou při vyhodnocení z hlediska neplánovaných změn je, zda se informace týká nějkého ze stanovených ukazatelů výkonnosti v bezpečnosti. Pokud tomu tak není, je nutné zjistit, zda se nejedná o informaci o nějakém ze směrových bodů pro případné ověření platnosti předpokladů, které jsou s daným směrovým bodem spjaty. Pokud se informace netýká žádného ukazatele ani směrového bodu pravděpodobně se jednalo o méně důležitou informaci[9] a v takovém případě se dále pokračuje ve sběru dat bez dalších kroků dle obrázku 20.

Pokud se informace týkala nějakého ze stanovených ukazatelů, je nejprve nutné určit, zda se jednalo o reaktivní ukazatel (bezpečnostní událost) nebo o proaktivní (porušení předpokladu v rámci SSP). V případě reaktivního ukazatele a překročení jeho limitní hodnoty je stav situace již vážný, daná nehoda nebo incident se staly vícekrát bez adekvátní reakce, a je třeba situaci řešit okamžitou reakcí na daný bezpečnostní problém, které CAA již provádí v podobných situacích. Dále tato situace vede k vytvoření AHAI, který je nutné vytvořit i v případě, kdy limitní hodnota reaktivního ukazatele překročena ještě nebyla. V případě informace týkající se proaktivního ukazatele je nejprve nutné rozhodnout, zda došlo k porušení jeho předpokladu. Pokud předpoklad nebyl porušen tak se pravděpodobně jednalo o informaci potvrzující jeho aktuální platnost a toto zjištění nevyžaduje další kroky a pokračuje se pouze ve sběru dat. Pokud předpoklad porušen byl, tak je provedena zajišťovací akce konkrétního proaktivního

[9] Příkladem takové informace mohou být méně důležité plánované změny, pro které má subjekt vytvořený systém posouzení a schvalování, a který je schválen patřičným orgánem (CAA). Takové změny má subjekt pouze povinnost ohlásit CAA a z důvodu jejich rozsahu není třeba ze strany CAA podnikat další kroky.

ukazatele. Dále tato situace rovněž ústí ve vytvoření AHAI. Nutnost vytvoření AHAI záleží na podobě hlášení ze systému pro jejich sběr. Pokud budou datové zdroje již odpovídat potřebám modelu STAMP a jeho analýzám, AHAI bude odpovídat popisu události z datových zdrojů. V současnosti jsou ovšem podmínky kladené na detail jednotlivých datových zdrojů rozdílná, a proto je nutné AHAI vytvořit. Jak je patrno z obrázku 20, po vytvoření AHAI následuje proces Aktivní STPA.

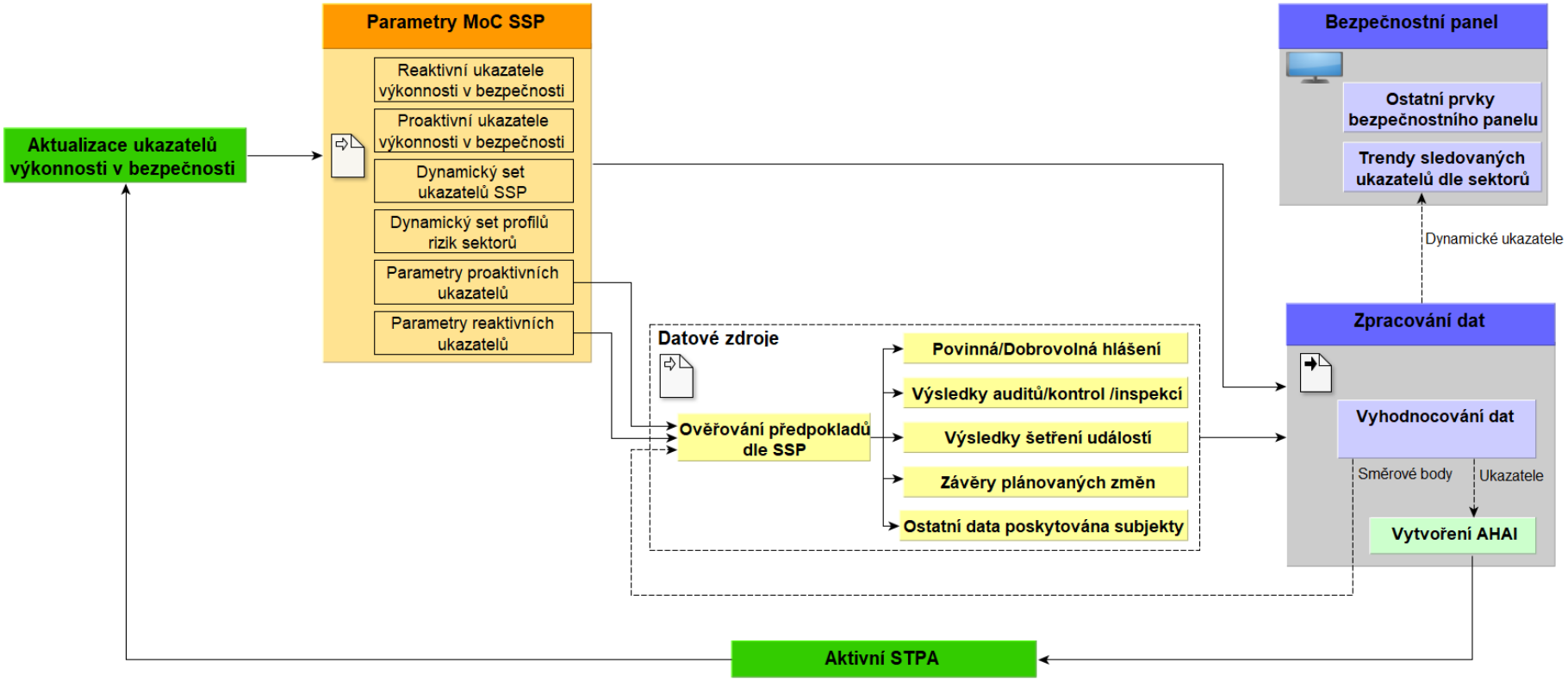
8.4.2 Aktivní STPA

Po vytvoření AHAI nastává proces Aktivní STPA, jehož cílem je identifikace veškerých proušených předpokladů, důvody tohoto porušení a následná aktualizace STPA dle nově nastavených předpokladů. Proces Aktivní STPA je znázorněn na obrázku 22 a tuto část vykonává dle návrhu CAA. Z hlediska CAA je nejdůležitější posouzení na základě dat předchozích let, ve kterém CAA posuzuje, zda byl konkrétní předpoklad porušen poprvé, anebo došlo k opakovanému porušení. Na základě tohoto posouzení informuje CAA daný subjekt o jeho závěru, a dle toho pokračuje proces porušení předpokladu znázoněný na obrázku 23 nebo proces opakovaného porušování předpokladu na obrázku 24.

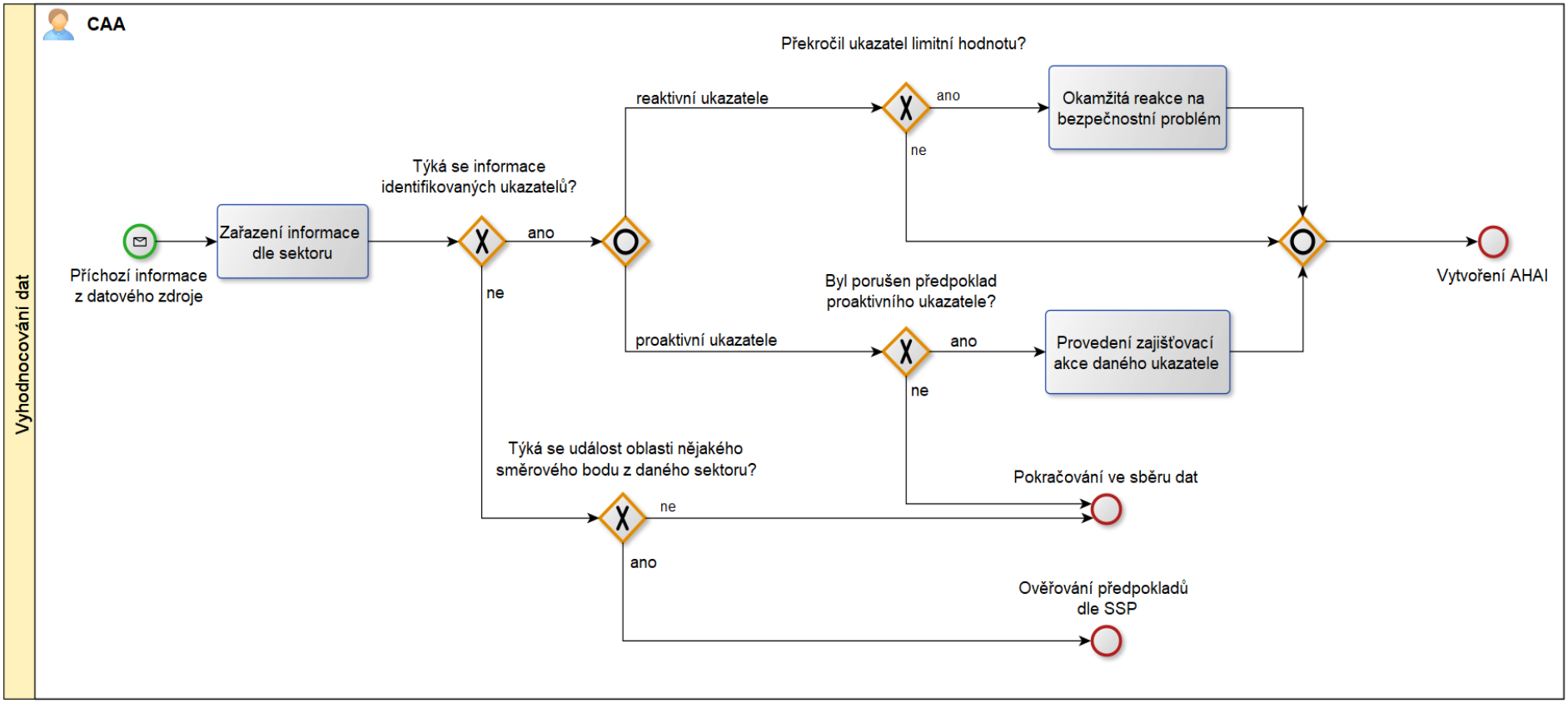
Oba procesy na obrázcích 23 a 24 mají podobný průběh, jehož hlavní podstatou je již provést kroky Aktivní STPA a zjistit tak, co vedlo k porušení předpokladu, jaké bariéry tomu měli zabránit, a zda nedošlo k porušení i jiného předpokladu. Tomuto procesu odpovídají první dva kroky, kterými jsou „Kontrola STPA“ a „Posouzení předpokladů“. Tedy v prvním kroku je důležité pro subjekt projít vytvořenou analýzu a všechny její kroky (systémová omezení, UCA, ztrátové scénáře atd.) na základě nálezu o porušeném/opakovaně porušeném předpokladu. Ve druhém kroku obrázku 23 a 24 jsou poté již na základě prvního kroku identifikovány ostatní porušené předpoklady, pokud k nějakým dalším došlo. Na základě toho subjekt vypracuje návrh řešení a aktualizace STPA, který je zaměřen na změny STPA (zejm. změny předpokladů a proaktivních ukazatelů), které se porušeným předpokladem musí provést. Hlavním rozdílem při prvním porušení daného předpokladu (viz obrázek 23) je nutnost subjektu identifikovat neplánovanou změnu, která vedla k dané situaci, a s touto skutečností poté pracovat při úpravách STPA v návrhu. Opakované porušení předpokladu poté značí špatné řešení při předchozích porušení, což by měl subjekt rovněž zapracovat do návrhu úpravy STPA. Návrh řešení podléhá kontrole ze strany CAA jako je tomu i nyní např. při řešení nápravných opatření. Zaslané předpoklady a proaktivní ukazatele se budou kontolovat obdobně jako je tomu v kapitole 8.2. Na základě schváleného návrhu musí subjekt

přepracovat a zaslat zpět CAA změněné předpoklady a prokativní ukazatele, aby mohlo dojít k atualizaci i na této straně.

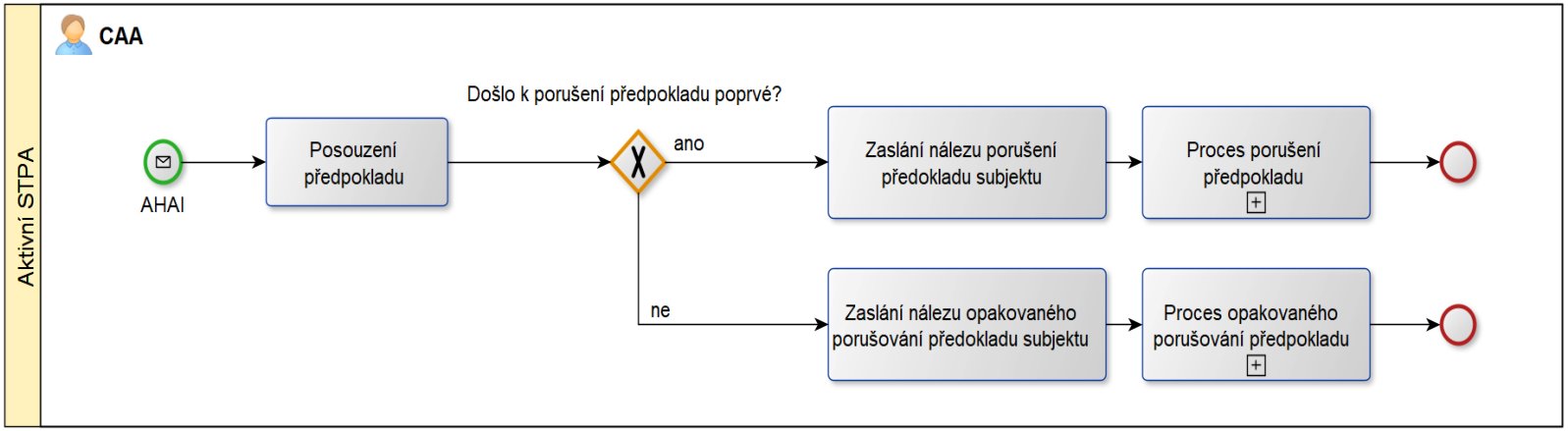
Oba procesy mají v kompetenci již samotné subjekty civilního letectví, neboť k takto konkrétním závěrům je třeba detailnějších znalostí systému subjektu než je dozorový orgán v rámci SSP schopen dosáhnout. V tomto procesu CAA primárně udávají subjektu nutnost se neplánovanou změnou zabývat a vykonávají dozorovu činnost nad jejím řešením.



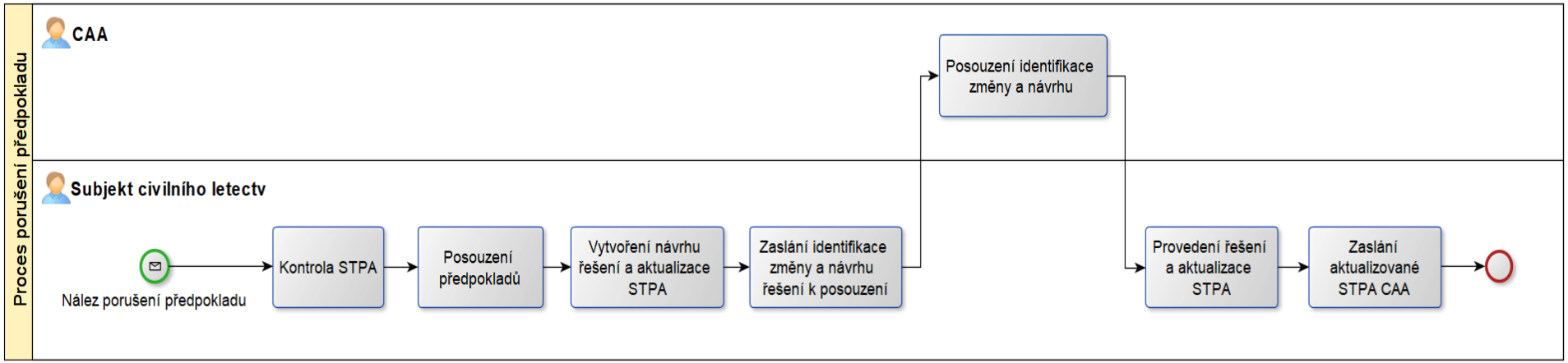
Obrázek 20: Identifikace a řízení neplánovaných změn v rámci SSP



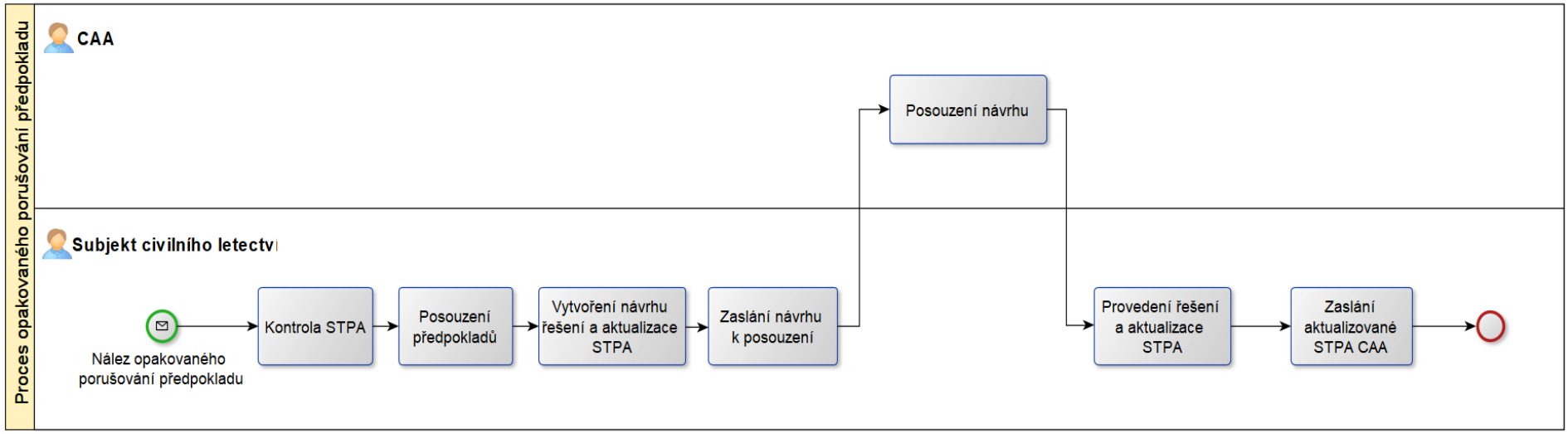
Obrázek 21: Proces vyhodnocování dat



Obrázek 22: Proces Aktivní STPA



Obrázek 23: Proces porušení předpokladu



Obrázek 24: Proces opakovaného porušování předpokladu

9 Validace

Cílem práce bylo vytvoření návrhu na identifikaci a řízení neplánovaných změn v rámci SSP s využitím systémového přístupu. Tento návrh je popsaný v kapitole 8 a zahrnuje procesy prováděné jak subjekty, tak i orgány systému státní správy a dozoru civilního letectví. Návrh umožňuje snadnější a efektivnější identifikaci neplánovaných změn, které v civilním letectví vznikají. Součástí této práce je ovšem nejen vytvořit samotný návrh, ale rovněž ověřit, zda je tento návrh proveditelný, a parametry, které se v něm identifikují, lze identifikovat i na datech z provozu. V této kapitole bude popsán proces validace návrhu, která se sestává ze 2 hlavních částí. První část validace je popsána v kapitolách 9.1 a 9.2 a je zaměřena na ověření proveditelnosti stanovení veškerých parametrů zmíněných v kapitole 8 na datech z provozu. Druhá část validace, která je popsána v kapitole 9.3, je zaměřena na ověření správnosti a proveditelnosti návrhu v rámci současného SSP.

9.1 Validace stanovení parametrů pro neplánované změny

Nejprve je v rámci validace třeba ověřit, zda je dle návrhu možné stanovit parametry potřebné pro systémovou identifikaci a řízení neplánovaných změn. Tato část validace je tedy zaměřená na první 3 kroky návrhu (viz obrázek 15) a je založená na výstupech bakalářské práce Bc. Ondřeje Vašaty nesoucí název „Návrh proaktivních indikátorů bezpečnosti pro letiště s využitím modelu STAMP“. [27] Ve zmíněné práci byla použita analýza STPA na proces technického odbavení na letišti, kdy na základě jejích výstupů byly vytvořeny předpoklady a proaktivní ukazatele. Celá tato práce je popsána z pozice subjektu civilního letectví poskytující službu technického odbavení, a odpovídá tedy prvnímu kroku návrhu popsaného v kapitole 8.1. Na základě výstupů této práce následuje 2. krok návrhu. Ten je již v kompetenci jednotlivých CAA a jeho cílem je navrhnout tyto parametry v rámci SSP.

Mezi hlavní vstupy pro tento krok návrhu dle obrázku 17 patří reaktivní a proaktivní ukazatele subjektu civilního letectví a jejich předpoklady, které subjekt zašle CAA. CAA data poskytnutá subjektem podrobí kontrole dle obrázku 18. V práci Bc. Vašaty jsou předpoklady shodné s proaktivnímu ukazateli a kontrola předpokladů tedy bude dostačující. Příklady předpokladů stanovených pro proces technického odbavení v práci Bc. Vašaty jsou shrnuty v tabulce 3.

Tabulka 3: Předpoklady pro proces technického odbavení [27]

ID	Proaktivní ukazatele
P-1	Odbavení letadla probíhá za dodržení odbavovacích procedur
P-2	Odbavení probíhá za vyhovujících pracovních podmínek
P-3	Pracovníci odbavení mají výcvik na odbavovaný typ letadla
P-4	Letadla určená pro odbavení splňují technické normy pro bezpečné odbavení

Jelikož práce Bc. Vašaty nebyla vytvořena pro splnění záměru této práce, předpoklady neodpovídají svým detailem pro účely CAA. V reálném provozu by si CAA od subjektu vyžádal zaslání předpokladů s menším detailem. V tomto případě byl potřebný detail předpokladů vytvořen na základě ostatních výstupů práce Bc. Vašaty, mezi které se řadí nebezpečí a systémová omezení. Z již zmíněných důvodů byla práce Bc. Vašaty vytvořena s jiným detailem, a proto musely být částečně upraveny i nebezpečí a systémová omezení, kterým byl dodán pouze jiný detail. U nebezpečí byla upravena pouze dílčí a systémová byla ponechána. Na základě toho byla upravena systémová omezení. Příklady systémových nebezpečí, které byly vybrány pro tuto kapitolu, shrnuje tabulka 4.

Tabulka 4: Příklad systémových nebezpečí subjektu [27]

ID	Systémová nebezpečí	Ztráty
H-1	Odbavení letadla probíhá na kontaminované stojánce	L-1, L-2, L-3, L-4, L-5, L-6
H-3	Při odbavení letadla dojde k nepředepsané manipulaci s odbavovací technikou nebo částmi letadla	L-1, L-2, L-3, L-4, L-6
H-4	Odbavovací technika, pracovníci odbavení nebo letadlo během odbavení překročí minimální bezpečné rozestupy vzhledem k jiné odbavovací technice/letadlu	L-1, L-2, L-3, L-4, L-5, L-6

Systémová nebezpečí H-3 a H-4 jsou složena z dílčích nebezpečí, u kterých byl upraven původní detail z práce Bc. Vašaty. Systémové nebezpečí H-1 bylo ponecháno bez dílčího nebezpečí stejně jako bylo uvedeno původně ve zmíněné práci. Dílčí nebezpečí pro H-3 a H-4 jsou shrnuta v tabulce 5. Na identifikovaná nebezpečí jsou dále vázána systémová omezení, které zamezují vzniku daného nebezpečí. Příklady systémových omezení shrnuje tabulka 6.

Tabulka 5: Příklad dílčích nebezpečí subjektu, upraveno z [27]

ID	Dílčí nebezpečí	Ztráty
H-3	**Při odbavení letadla dojde k nepředepsané manipulaci s daným objektem**	**L-1, L-2, L-3, L-4, L-6**
H-3.1	Při odbavení letadla dojde k nepředepsané manipulaci s odbavovací technikou	L-1, L-2, L-3, L-4, L-6
H-3.2	Při odbavení letadla dojde k nepředepsané manipulaci s částmi letadla	L-1, L-2, L-3, L-4, L-6
H-4	**Při odbavení dojde k porušení minimálních rozestupů**	**L-1, L-2, L-3, L-4, L-5, L-6**
H-4.1	Při odbavení dojde k porušení minimálních rozestupů letadla vůči letadlu	L-1, L-2, L-3, L-4, L-5, L-6
H-4.2	Při odbavení dojde k porušení minimálních rozestupů odbavovací techniky vůči letadlu	L-1, L-2, L-3, L-4, L-5, L-6
H-4.3	Při odbavení dojde k porušení minimálních rozestupů personálu vůči částem letadla	L-1, L-2, L-3, L-4, L-5, L-6

Tabulka 6: Příklady systémových omezení subjektu, upraveno z [1]

ID	Systémová omezení	Nebezpečí
SC-1	Odbavení letadla nesmí probíhat na stojánce kontaminované FOD	H-1
SC-3	Při odbavení letadla nesmí dojít k nepředepsané manipulaci s daným objektem	H-3
SC-3.1	Při odbavení letadla nesmí dojít k nepředepsané manipulaci s odbavovací technikou	H-3.1
SC-3.2	Při odbavení letadla nesmí dojít k nepředepsané manipulaci s částmi letadla	H-3.2
SC-4	Při odbavení nesmí dojít k porušení minimálních rozestupů	H-4
SC-4.1	Při odbavení nesmí dojít k porušení minimálních rozestupů letadla vůči letadlu	H-4.1
SC-4.2	Při odbavení nesmí dojít k porušení minimálních rozestupů odbavovací techniky vůči letadlu	H-4.2
SC-4.3	Při odbavení nesmí dojít k porušení minimálních rozestupů personálu vůči částem letadla.	H-4.3

Na základě výše uvedených systémových omezení jsou stanoveny předpoklady z pohledu subjektu, jejichž příklady shrnuje tabulka 7.

Tabulka 7: Příklady předpokladů subjektu

ID		Předpoklady subjektu
SC-1	P-1	V rámci technického odbavení existuje seznam, který definuje objekty kontaminující stojánku (FOD).
	P-2	Pracovníci technického odbavení pracují s kompletním a aktuálním seznamem předmětů definovaných jako FOD.
SC-3.1	P-3	V rámci technického odbavení existují postupy pro manipulaci s odbavovací technikou.
	P-4	Pracovníci technického odbavení pracují s platnými postupy pro manipulaci s odbavovací technikou.
SC-3.2	P-5	V rámci technického odbavení existují postupy pro manipulaci s částmi letadla.
	P-6	Pracovníci technického odbavení pracují s platnými postupy pro manipulaci s částmi letadla.
SC-4.1	P-7	V rámci technického odbavení existují požadavky na minimální rozestup letadel.
	P-8	Pracovníci technického odbavení pracují s kompletními a aktuálními požadavky na minimální rozestup letadel.
SC-4.2	P-9	V rámci technického odbavení existují požadavky na minimální rozestup letadla a odbavovací techniky.
	P-10	Pracovníci technického odbavení pracují s kompletními a aktuálními požadavky na minimální rozestup letadla a odbavovací techniky.
SC-4.3	P-11	V rámci technického odbavení existují požadavky na minimální rozestup personálu technického odbavení a částí letadla.
	P-12	Pracovníci technického odbavení pracují s kompletními a aktuálními požadavky na minimální rozestup personálu vůči částem letadla.

Předpoklady pro účely subjektu jsou stanoveny zejm. na omezení vycházejících z dílčích nebezpečí s výjimkou omezení SC-1 vycházejícího ze systémového nebezpečí H-1, které žádná dílčí nebezpečí nemá. Je to z toho důvodu, že z pozice subjektu je možné měřit více konkrétních proaktivních ukazatelů vycházejících z těchto předpokladů než naopak poté u CAA. Detail, se kterým bude subjekt pracovat při vytváření předpokladů může být

ještě vyšší, než je ten uvedený v tabulce 7 (např. P-4 a P-5 by mohl být rozveden do předpokladů pro jednotlivé typy odbavovací techniky). Toto již záleží na jednotlivých subjektech a jejich možnostech. Výše uvedené předpoklady se dále využijí pro vytvoření proaktivních ukazatelů. V tomto případě mohou být proaktivní ukazatele ponechány ve formách tvrzení jednotlivých předpokladů, která jsou buď pravdivá či nikoliv.

V práci Bc. Vašaty byly uvažovány dle zadání pouze předpoklady a proaktivní ukazatele, a proto byly reaktivní ukazatele doplněny pro účely této práce na základě ostatních výstupů STPA (zejm. identifikovaných ztrát a nebezpečí) s využitím taxonomie ECCAIRS. Příklad identifikovaných reaktivních ukazatelů shrnuje tabulka 8.

Tabulka 8: Příklady reaktivních ukazatelů procesu technického odbavení

ID ECCAIRS	Reaktivní ukazatele
2060200	Poškození letadla cizím předmětem (FOD)
2150300	Zranění způsobená vrtulí/ vlivem tzv. „jet blast“[10]
2150400	Zranění způsobená částí/částmi letadla
2200302	Narušení odbavovací plochy/rampy vozidlem/vybavením
2200303	Narušení odbavovací plochy/rampy osobou
5030701	Kolize- Vozidlo s jiným vozidlem
5030702	Kolize- Vozidlo s osobou
99010060	Kolize- Tažené letadlo s předmětem
99012402	Poškození pozemních vozidel/ pozemního vybavení vlivem tzv. „jet blast“
99012404	Kolize/ Poškození nárazem pozemních vozidel/pozemního vybavení

Takto vytvořené předpoklady, proaktivní a reaktivní ukazatele již odpovídají požadavkům kontroly CAA viz kapitola 8.2. To znamená, že reaktivní ukazatele korespondují s vybranou taxonomií a pokrývají veškeré možné incidenty nebo nehody, které by se v procesu mohou vyskytnout. Pro předpoklady to znamená, že jsou v patřičném detailu pro další využití CAA a jsou vytvořeny pro všechny procesy, které mohou způsobit nebezpečí.

[10] Termínem „jet blast“ je označován proud vzduchu, který je vytvářen za proudovým motorem při jeho spuštění. Tento jev je nebezpečný zejm. v procesu technického odbavení, kdy prudký náraz vzduchu může způsobit např. zranění pracovníků nebo škody na vybavení. [28]

Pomocí informací obsažených v tabulkách může CAA dle obrázku 17 již začít proces vytvoření ukazatelů v rámci SSP. Nejprve je nutné stanovit předpoklady, které budou již vytvořeny pro účely SSP. V zájmu CAA budou zejm. předpoklady, které nejsou v takovém detailu jako jsou např. předpoklady vytvořené na základě omezení pro dílčí nebezpečí. Pokud by některý ze CAA chtěl sledovat proces detailněji je možné stanovit předpoklady pro CAA i na základě omezení pro dílčí nebezpečí. Pro validaci v této práci budou vytvořeny předpoklady na základě omezení systémových nebezpečí, neboť lze předpokládat, že v současné situaci, kdy se proaktivní ukazatele na základě předpokladů příliš nepoužívají, bude jako prvním krokem pro CAA vytvořit alespoň ty méně detailní. Předpoklady v rámci SSP, které jsou vytvořeny na základě výše uvedených předpokladů subjektu v tabulce 7, budou rovněž sloužit jako kvalitativní proaktivní ukazatele v rámci SSP. Příklady předpokladů/proaktivních ukazatelů v rámci SSP jsou shrnuty v tabulce 9.

Tabulka 9: Příklady předpokladů/proaktivních ukazatelů v rámci SSP

ID	Předpoklady/Proaktivní ukazatele v rámci SSP	Předpoklady subjektu
P-1	V rámci technického odbavení existuje seznam, který definuje objekty kontaminující stojánku (FOD).	P-1
P-2	Pracovníci technického odbavení pracují s kompletním a aktuálním seznamem předmětů definovaných jako FOD.	P-2
P-3	V rámci technického odbavení existují postupy pro manipulaci s odbavovací technikou a částmi letadla.	P-3, P-5
P-4	Pracovníci technického odbavení pracují s platnými postupy pro manipulaci s odbavovací technikou a částmi letadla.	P-4, P-6
P-5	V rámci technického odbavení existují požadavky na minimální rozestup.	P-7, P-9, P-11
P-6	Pracovníci technického odbavení pracují s kompletními a aktuálními požadavky na minimální rozestup.	P-8, P-10, P-12

Pro proaktivní ukazatele je nutné stanovit veškeré parametry zmíněné na obrázku 17, kterými jsou formovací a zajišťovací akce, směrové body a způsob ověření. První tři parametry pro předpoklady z tabulky 9 jsou shrnuty v tabulce 10.

Tabulka 10: Formovací a zajišťovací akce a směrové body předpokladů v rámci SSP

ID	Formovací akce	Zajišťovací akce	Směrové body
P-1	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna postupů ohledně FOD, seznamu FOD, rozložení odbavovací plochy
P-2	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna postupů ohledně FOD, seznamu FOD, rozložení odbavovací plochy
P-3	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna postupů manipulace s odbavovací technikou, s částmi letadla, odbavovací techniky (nákup nové), odbavovaných letadel (nový typ letadla)
P-4	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna postupů manipulace s odbavovací technikou, s částmi letadla, odbavovací techniky (nákup nové), odbavovaných letadel (nový typ letadla)
P-5	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna požadavků na minimální rozestupy při technickém odbavení, odbavovací techniky (nákup nové), odbavovaných letadel (nový typ letadla)
P-6	Vedení programu dozoru Provedení kontrol/inspekcí/auditů	Notifikace a doporučení pro řešení nastalé situace Zvýšení frekvencí auditů, inspekcí a kontrol Kontrola nápravných opatření	Plánovaná změna požadavků na minimální rozestupy při technickém odbavení, odbavovací techniky (nákup nové), odbavovaných letadel (nový typ letadla)

Posledním parametrem pro stanovení u proaktivních ukazatelů je způsob ověření, který shrnuje pro uvedené předpoklady v rámci SSP tabulka 11.

Tabulka 11: Způsob ověření proaktivních ukazatelů v rámci SSP

ID	Způsob ověření		
	Způsob hodnocení	**Oblasti ověření**	**Zdroje ověření**
P-1	Kvalitativní	Proaktivní ukazatel subjektu P-1	Datové zdroje viz obrázek 20
P-2	Kvalitativní	Proaktivní ukazatel subjektu P-2	Datové zdroje viz obrázek 20
P-3	Kvalitativní	Proaktivní ukazatele subjektu P-3, P-5	Datové zdroje viz obrázek 20
P-4	Kvalitativní	Proaktivní ukazatele subjektu P-4, P-6	Datové zdroje viz obrázek 20
P-5	Kvalitativní	Proaktivní ukazatele subjektu P-7, P-9 a P-11	Datové zdroje viz obrázek 20
P-6	Kvalitativní	Proaktivní ukazatele subjektu P-8, P-10 a P-12	Datové zdroje viz obrázek 20

Dle obrázku 17 je ke stanovení parametrů reaktivních a proaktivních ukazatelů třeba STPA systému státní správy a dozoru civilního letectví. V rámci této práce nebyla využita konkrétní STPA ÚCL ke stanovení např. formovacích a zajišťovacích akcí vůči provozovatelům technického odbavení. Je to z toho důvodu, že STPA ÚCL (zde konkrétně část STPA ÚCL dozorové činnosti technického odbavení) nebyla v rámci této práce vykonána z důvodů jejího rozsahu a zaměření. Rovněž limitem k jejímu vytvoření je omezený přístup k informacím potřebným pro vytvoření STPA ÚCL. Tyto parametry byly stanoveny na základě veřejně přístupných informací (např. legislativních dokumentů nebo směrnic a postupů ÚCL) týkající se dozorové činnosti ÚCL. Řídící akce dozorové činnosti ÚCL (obecně CAA) vůči subjektům civilního letectví jsou rámcově pro všechny procesy civilního letectví stejné[11] a mění se pouze detaily a osoby CAA, které dle specializovaných oddělení dozorovou činnost vykonávají. Z těchto důvodů nejsou

[11] Řídicí akce CAA vůči jakémukoliv subjektu civilního letectví neboli způsoby, jakými CAA může působit na subjekt, jsou omezené, a i přes měnící se detaily zůstává základ řídící akce stejný. Toto platí jak pro řídící akce vůči subjektu, který poskytuje službu technického odbavení, tak i např. pro provozovatele letiště (vykonávání auditů, inspekcí nebo kontrol, odebrání, omezení nebo pozastavení platnosti oprávnění atd.)

možné chybějící detaily dozorové činnosti překážkou, neboť pro účely validace návrhu této práce je tato úroveň detailu dostačující.

Takto mohly být stanoveny patřičné parametry (formovací a zajišťovací akce, směrové body a způsob ověření) pro proaktivní ukazatele P-1 až P-6, které budou dále napomáhat identifikaci neplánované změny. U formovacích akcí jsou uvedeny řídící akce pravidelné dozorové činnosti. Obě uvedené formovací akce v tabulce 10, které se pro všechny předpoklady opakují, probíhají na CAA v určitých legislativou stanovených periodách. Pro zajišťovací akce je stanoveno více řídících akcí, kterými CAA může reagovat na porušený předpoklad. Výběr odpovídající zajišťovací akce bude v odpovědnosti CAA a osoby příslušné sekce/oddělení. U způsobu ověření je třeba určit o jaký typ ukazatele se jedná (kvalitativní/kvantitativní), na základě jakých dat se bude jeho hodnota stanovovat (oblast ověření) a jak se tato data budou získávat (zdroj ověření).

V uvedených příkladech byly všechny proaktivní ukazatele stanoveny jako kvalitativní ve formě tvrzení, a proto hodnocení může probíhat jednoduchou formou, zda je tvrzení pravdivé či nepravdivé. Pomocí oblastí ověření v tabulce 11 se definují data, pomocí kterých se stanoví, zda je tvrzení pravdivé či nikoliv. Oblasti většinou korespondují s dílčími proaktivními ukazateli sledovanými subjektem, ze kterých se skládá systémový proaktivní ukazatel sledovaný CAA. Pokud ukazatel nemá žádný dílčí ukazatel (P-1 a P-2), tak sám tvoří oblast ověření, neboť jeho pravdivost nezáleží na žádném jiném dílčím ukazateli. Jeho hodnota pak přímo vyplývá z hodnoty P-1 nebo P-2. V případě ostatních proaktivních ukazatelů, které mají více než jednu oblast ověření, se celková hodnota ukazatele v rámci SSP stanoví tak, že pokud jedna z oblastí nesplňuje kritérium (není pravdivá), tak celý systémový předpoklad daného proaktivního ukazatele (P-3 nebo P-4) je porušen. Informace o pravdivosti proaktivních ukazatelů se získávají pomocí datových zdrojů, které jsou uvedeny v obrázku 20, zejm. pomocí auditů, inspekcí a kontrol ale i pomocí jiných zdrojů např. systému povinného/dobrovolného hlášení.

V rámci SSP musí CAA rovněž stanovit reaktivní ukazatele, ke kterým se vážou dále stanovené proaktivní ukazatele. Pokud proběhla kontrola reaktivních ukazatelů a subjekt používá stejnou taxonomii jako CAA, CAA pouze převezme reaktivní ukazatele subjektu. V ostatních případech je CAA vybere z taxonomie, kterou používá, na základě reaktivních ukazatelů subjektu. V tomto případě reaktivní ukazatele subjektu vypsané v tabulce 8 odpovídají i těm v rámci SSP. Dle obrázku 17 se k reaktivním ukazatelům stanoví ještě způsob ověření a limitní hodnoty, se kterými již CAA na základě postupů

uvedených v SMM pracují. Hlavními způsoby ověření pro veškeré reaktivní ukazatele, a tedy i pro ty týkající se technického odbavení, jsou šetření leteckých nehod využívající optimálně analýzu CAST (viz kapitola 8.2) a systémy povinného/ dobrovolného hlášení. Hodnocení reaktivních ukazatelů je kvantitativní ve všech výše uvedených příkladech a způsob stanovení limitních hodnot se shoduje se způsobem využívaným v současnosti. Z tohoto důvodu limitní hodnoty v této práci nejsou stanoveny, neboť tento proces oproti tomu současnému nepřináší nic nového.

Dle návrhu je možno po definování ukazatelů a jejich parametrů v rámci SSP začít 3. krok, kde se vytváří dynamické parametry. Cílem tohoto kroku je pouze výběr nejdůležitějších ukazatelů z pohledu bezpečnostních cílů. Jejich stanovení ovšem není jednoduchý proces vyžadující robustní datovou sadu předchozích let ke konkrétní organizaci, která nebyla pro účely této práce k dispozici. Z těchto důvodů nebyly bezpečnostní cíle v rámci validace 3. kroku návrhu vytvořeny. Rovněž stanovení bezpečnostních cílů již CAA provádí, a tak tento krok není třeba blíže specifikovat. Jediné, co se zde mění, jsou proaktivní ukazatele vázané na reaktivní ukazatele, které bezpečnostní cíle reflektují.

Druhým dynamickým parametrem jsou profily rizik. Ty CAA v současnosti taktéž využívají a dle návrhu změna nastane pouze k jakému celku se profily vztahují. V současnosti se využívají profily spíše pro jednotlivé subjekty. Dle návrhu by se subjekty pouze zařadily do větších celků (sektorů) podle procesů, na kterých se podílí. Pro případ technického odbavení by se tedy jednalo zejm. o provozovatele technického odbavení a dále např. o provozovatele letiště. Pomocí stanovených parametrů lze přistoupit na poslední krok návrhu, jehož validace je popsána v další kapitole.

9.2 Validace identifikace a řízení neplánovaných změn

V posledním kroku návrhu probíhá již samotná identifikace a řízení neplánovaných změn v provozu (viz obrázek 20). Jelikož návrh vytvořený v této práci nemohl být z důvodu časové náročnosti uveden do provozu, validace tohoto kroku proběhne pomocí vybrané události z letiště LGAV (Mezinárodní letiště Athény) ze 7.října roku 2017, která byla vybrána z webových stránek ECCAIRS[12]. Během této události byl zraněn pracovník společnosti SKYSERV S.A. při provádění technického odbavení letadla ATR 42-500 mířícího na letiště LGPA (Národní letiště Paros) společnosti SKY EXPRESS S.A.. Toto zranění nastalo dle závěrečné zprávy vlivem ztráty situačního povědomí, kdy pracovník při smotávání kabelů v závěrečné fázi technického odbavení nacouval příliš blízko

[12] https://sris.aviationreporting.eu/safety-recommendations

k vrtuli již spuštěného motoru č. 2, která ho zranila. Po vypnutí motorů byl pracovník převezen do nemocnice a zůstal mimo službu 19 dní. Jako hlavní příčina byl identifikován pohyb pracovníka technického odbavení a jako přispívající faktor byla identifikována již zmíněná ztráta situačního povědomí. Na základě těchto nálezů bylo stanoveno bezpečnostní doporučení pro společnost SKYSERV S.A., ve kterém bylo doporučeno přepracování prvotního a opakovacího výcviku pracovníků technického odbavení s ohledem na nastalou situaci. Společnost SKY EXPRESS S.A. vydala i bez bezpečnostního doporučení bezpečnostní bulletin, který reflektoval spuštění motorů po technickém odbavení a kontrolu odbavovací plochy před touto činností. [29]

Na základě závěrečné zprávy, jejíž výstupy jsou popsány výše, byl šetřením identifikován jeden reaktivní ukazatel z tabulky 8 „Zranění způsobené vrtulí/ vlivem tzv. „jet blast““. Při použití návrhu systémové identifikace a řízení neplánovaných změn by závěrem nebyl pouze tento reaktivní ukazatel, ale rovněž některý z proaktivních ukazatelů vytvořených v předchozí kapitole, jehož porušení k nehodě vedlo. Reaktivní ukazatel „Zranění způsobené vrtulí/ vlivem tzv. „jet blast““ se dle závěrečné zprávy stal vlivem porušení minimální vzdálenosti pracovníka technického odbavení od motoru letadla, čímž se dostal do přílišné blízkosti vrtule, která ho zranila. Faktor, který vedl k reaktivnímu ukazateli, a tedy k nehodě, jsou minimální rozestupy během technického odbavení, které reflektují proaktivní ukazatele P-5 a P-6. Důležité je v této části zjistit, zda došlo k porušení jednoho z těchto ukazatelů. To je stanoveno na základě posouzení, zda byl porušen předpoklad nějaké z jejich oblasti ověření uvedené v tabulce 11 (konkrétně pro proaktivní ukazatel P-5 by to byla oblast „V rámci technického odbavení existují požadavky na minimální rozestup personálu technického odbavení a částí letadla“ a pro P-6 oblast „Pracovníci technického odbavení pracují s kompletními a aktuálními požadavky na minimální rozestup personálu vůči částem letadla“).

I přesto, že v závěru šetření nebylo přesně stanoveno, zda se nehoda stala z důvodu chybějících požadavků na minimální rozestup personálu vůči částem letadla (oblast ověření pro P-5) nebo z důvodu, že pracovník nepracoval s kompletními a aktuálními požadavky této problematiky (oblast ověření pro P-6), lze porušení předpokladu P-5 ve výše uvedené oblasti odvodit z bezpečnostního doporučení, které bylo vydáno. Obě zúčastněné strany (SKYSERV S.A. a SKY EXPRESS S.A.) přepracovaly své postupy ohledně minimální vzdálenosti pracovníka technického odbavení vůči motoru letadla při jeho spuštění. Lze tedy předpokládat, že požadavky na minimální rozestup pracovníka a

letadlových částí nebyly zcela stanoveny, a oblast předpokladu P-5 byla porušena. Tím došlo k porušení i proaktivního ukazatele P-5 v rámci SSP.

Po zjištění těchto výsledků je nutné posoudit, zda nedošlo u reaktivního ukazatele k překročení limitní hodnoty. Toto posouzení by proběhlo na základě dat z předchozích let, které v tomto případě nejsou k dispozici. Následně by v případě překročení limitní hodnoty byla vyvolána okamžitá reakce na bezpečnostní problém, jak je patrno z obrázku 21. Při porušení proaktivního ukazatele P-5 by byla provedena CAA zajišťovací akce z tabulky 10, přičemž výběr vhodné zajišťovací akce je ponechán na odpovědné osobě CAA. Závěrem této fáze je vytvoření AHAI, které bude dále sloužit v procesu Aktivní STPA. AHAI pro tuto událost může být dle Aktivní STPA napsán např. takto:

„ATC na základě domluvy s vedoucím nakládky povolilo posádce spustit oba motory. Kapitánem letadla bylo po spuštění motorů zažádáno o odstranění veškerého vybavení ze stání. Jeden z pracovníků technického odbavení při odklízení kabelů z plochy nacouval příliš blízko spuštěného motoru, kde ho zranila vrtule motoru č.2. Pracovník byl poté převezen do nemocnice.“

Na základě AHAI je spuštěn proces Aktivní STPA, kde je nejprve nutné posouzení CAA, zda k porušení předpokladu došlo poprvé nebo porušení již nastalo. Toto posouzení probíhá pomocí dat předchozích let. Na základě tohoto posouzení, které nelze kvůli chybějícím datům v této oblasti utvořit, by CAA zaslalo poskytovateli služby technického odbavení nález o porušeném nebo opakovaně porušovaném předpokladu. Na základě typu nálezu je spuštěn proces obrázku 23 nebo 24, na jehož začátku by subjekt prošel vytvořenou analýzu STPA (viz kapitola 8.4.2) a identifikoval by další porušené předpoklady, pokud by porušením předpokladu z nálezu byly porušeny další. U prvně porušeného předpokladu musí navíc subjekt identifikovat neplánovanou změnu, která vedla k jeho porušení. Subjekt poté zašle CAA návrh na změnu předpokladů a proaktivních ukazatelů, který podléhá jeho schválení. Po schválení návrhu provede subjekt úpravu STPA a zašle CAA nové předpoklady a proaktivní ukazatele, na jejichž základě provede CAA aktualizaci parametrů v rámci SSP.

9.3 Validace správnosti a proveditelnosti návrhu v rámci současného SSP

Celý návrh pro systémovou identifikaci a řízení neplánovaných změn v rámci SSP byl vytvořen na základě modelu STAMP. Proveditelnost identifikace všech jeho parametrů byla validována pomocí obhájené bakalářské práce Bc. Vašaty (viz kapitola 9.1) a závěrečné zprávy šetření letecké nehody (viz kapitola 9.2). Validace správnosti návrhu,

která by byla provedena pomocí jeho implementace a následného sběru a vyhodnocení dat, nešla provést kvůli časové náročnosti. Nicméně všechny analýzy modelu STAMP (CAST, STPA a Aktivní STPA), které byly v návrhu použity, jsou již využívány nejen ve světě letectví a byly prokázány jako správné a efektivní z hlediska bezpečnosti. V návrhu jsou využity pouze tyto analýzy, které jsou vzájemně propojeny tak, jako je to popsáno např. v Aktivní STPA. Proto lze návrh a všechny jeho části z hlediska využitých analýz považovat za správný i bez nutnosti časově náročné validace pomocí implementace. Návrh této práce je rovněž zasazen do struktury již validovaného dokumentu SMM, dle kterého se SSP vytváří již mnoho let.

Práce vznikla v koordinaci s projektem CK01000073 „Digitalizace integrovaného dozoru nad bezpečností leteckých organizací“ s podporou Technologické agentury ČR, která zajistila její ověření z pohledu požadavků a technických možností dozorových institucí.

.

10 Diskuze

Neplánované změny patří mezi faktory negativně ovlivňující provozní bezpečnost, která je pro civilní letectví klíčová. Z tohoto důvodu je třeba se neplánovaným změnám věnovat a předcházet jejich negativnímu vlivu pomocí jejich včasné identifikace a řízení. Současně využívány přístup v této problematice je zejm. přístup pomocí výkonnosti v bezpečnosti, který je pospán v SMM od ICAO. Tento dokument ovšem neudává v oblasti neplánovaných změn příliš velké detaily a obecně se neplánovaným změnám věnuje okrajově a nepřisuzuje jim dostatečnou významnost v oblasti provozní bezpečnosti.

Nejnovějším přístupem k provozní bezpečnosti je systémový přístup modelu STAMP založený na Systémové teorii. Tento model obsahuje analýzu CAST, STPA a Aktivní STPA, které tvoří nástroje pro dosáhnutí myšlenek systémového přístupu modelu STAMP. Současné využívání systémového přístupu se v systému civilního letectví pomalu rozšiřuje z důvodu jeho prokázané vhodnosti a efektivity na socio-technické systémy, kterým systém civilního letectví je. Využití systémového přístupu v rámci SSP je z těchto důvodů určitě správným krokem, který usnadní a urychlí implementaci systémového přístupu v celém systému civilního letectví.

Jeho využití pro účely neplánovaných změn, které jsou součástí SSP, je nezbytné pro budoucí využití systémového přístupu v rámci celého SSP. I přesto, že problematika neplánovaných změn netvoří primární zaměření analýz modelu STAMP, byl na jejich základě v této práci vytvořen návrh pro systémovou identifikaci řízení neplánovaných změn. Návrh umožňuje efektivnější identifikaci a řízení neplánovaných změn z pozice CAA jakožto nejdůležitějšího orgánu systému státní správy a dozoru civilního letectví. K vytvoření návrhu byly využity všechny analýzy modelu STAMP, které se při jejich společném využívání vhodně doplňují.

Validace návrhu na základě jeho implementace do provozu nebyla možná z časových důvodů, což může tvořit limitaci této práce. Pro validaci byla proto využita bakalářská práce Bc. Vašaty věnující se STPA a proaktivním předpokladům procesu technického odbavení, jejíž výstupy byly pro účely této práce upraveny. Pomocí těchto výstupů mohly být podrobeny validaci první 3 kroky návrhu, ke kterým byla potřeba rovněž STPA ÚCL. Ta nebyla kvůli zaměření této práce a chybějícím informacím vytvořena, a místo ní byly využity volně dostupné informace o dozorové činnosti ÚCL. Parametry stanovené na těchto informacích mohou postrádat větší detail, ale pro účely validace tohoto návrhu byl menší detail dostačující.

Validace posledního kroku návrhu byla demonstrována na nehodě nastalé při technickém odbavení letadla. Z důvodu chybějících dat ohledně proaktivních ukazatelů z šetření této nehody byl v této části validace pouze naznačen další průběh při identifikaci neplánované změny, což tvoří druhou limitaci této práce.

Každá implementace něčeho nového může ze začátku přinést určité obtíže a stejně tomu je i v případě implementace a využití tohoto návrhu. Jako počáteční překážka pro využívání systémového přístupu se může jevit nutné proškolení zaměstnanců (v rámci SSP zejm. zaměstnance CAA) na využívání jednotlivých analýz. V tomto návrhu se zaměstnanců CAA týká především práce s předpoklady a proaktivními ukazateli a jejich parametry, a navíc školení by museli absolvovat pouze vybraní zaměstnanci (z vybraných oddělení pouze určitý počet zaměstnanců), kteří se budou na této problematice podílet.

Jako další překážka se může jevit časová náročnost nejen implementace ale i řízení neplánovaných změn dle návrhu. Při implementaci se samozřejmě větší časová náročnost může objevit stejně jako u každé implementace něčeho nového. Ovšem při řízení neplánovaných změn dle návrhu lze očekávat spíše časovou úsporu s ohledem na současně využívaný přístup např. na ÚCL. Svolávání a řízení diskuzí ohledně možných příčin zvýšených hodnot reaktivních ukazatelů se jeví jako způsob mnohem méně efektivní. Z důvodu včasného nepodchycení neplánované změny se mohou nehody a incidenty vyskytovat častěji a stejně tak budou muset probíhat i diskuze častěji. Oproti tomu systémové řízení neplánovaných změn sice vyžaduje pravidelnější činnost ohledně vyhodnocování proaktivních ukazatelů, ale neplánované změny jakožto možné příčiny nehod a incidentů budou zachyceny dříve, než se stanou, a tím lze předpokládat nižší počet nehod a incidentů, kterými se ÚCL musí zabývat. V současném přístupu se neplánovanými změnami zabývají až poté, co se nějaká bezpečnostní událost stala, což je možné spatřit v uvedeném příkladu nehody ve validaci. Pomocí proaktivního systémového přístupu k neplánovaným změnám navrženého v této práci lze neplánované změny identifikovat pomocí proaktivních ukazatelů, které lze měřit, aniž by se nějaká bezpečnostní událost stala. Proaktivními ukazateli lze velmi dobře odhalit systémovou příčinu, která ovlivňuje celou řadu dalších na první pohled spolu nesouvisejících událostí. Díky včasnému podchycení systémové příčiny a její nápravě lze předcházet mnohým bezpečnostním událostem. Možnost měření proaktivních ukazatelů bez bezpečnostních událostí a předcházení těchto událostí tvoří nejdůležitější výhody systémového přístupu a návrhu této práce.

Vytvořený návrh se zaměřuje na řízení neplánovaných změn v rámci SPP, ale jeho využití je možné i mimo rámec SSP např. subjektem civilního letectví, neboť udává parametry potřebné k identifikaci neplánovaných změn i postupy pro jejich řízení. Udává tedy nejen detailní návrh pro systémovou identifikaci a řízení neplánovaných změn v rámci SSP, ale i obecný návrh, jak k neplánovaným změnám přistupovat mimo SSP, čemuž se současné dostupné zdroje zatím nevěnovaly.

Součástí zadání práce bylo rovněž stanovení klíčových prvků SSP pro systémovou identifikaci a řízení neplánovaných změn. V případě zachování struktury SSP dle dokumentu SMM od ICAO, by postup pro identifikaci a řízení neplánovaných změn byl zahrnut v rámci 3. kapitoly SSP s názvem „Zajištění bezpečného provozu na úrovni státu“, konkrétně v klíčovém prvku „Měření a hodnocení výkonnosti v bezpečnosti“. V tomto klíčovém prvku jsou popsány reaktivní a proaktivní ukazatele a jejich využití pro měření a hodnocení výkonnosti v bezpečnosti. V současném přístupu se řeší neplánované změny právě pomocí měření a hodnocení ukazatelů výkonnosti v bezpečnosti. V klíčovém prvku ovšem není přistupováno k neplánovaným změnám systémově a ohledně této problematiky chybí v SMM mnoho potřebných detailů. Z tohoto důvodu je potřeba doplnit tento klíčový prvek o všechny 4 kroky vytvořeného návrhu pro systémovou identifikaci a řízení neplánovaných změn v rámci SSP.

Závěr

Cílem této práce bylo vytvoření návrhu pro identifikaci a řízení neplánovaných změn v rámci SSP s využitím systémového přístupu. Pro splnění cíle bylo nejprve potřeba nastudovat veškeré potřebné dokumenty a materiály dané problematiky. Jako první proběhlo obecné seznámení s problematikou neplánovaných změn v rámci provozní bezpečnosti, které vedlo k vytvoření rozhraní, co přesně neplánované změny zahrnují pro další postup v práci. Jelikož v této práci se jedná o problematiku neplánovaných změn v rámci SSP, jako druhý bod bylo nutné nastudovat SSP jak z pozice SMM, tak pro srovnání současně využívaný SSP pro Českou republiku, který ze SMM vychází. V návaznosti na SSP byla nastudována struktura systému státní správy a dozoru pro ČR, jejíž orgány jsou součástí SSP a neplánovanými změnami se zabývají. Jako poslední byly pro účely návrhu nastudovány přístupy k řízení neplánovaných změn. Mezi současné přístupy využívané v letecké dopravě byl zahrnut přístup popsaný v dokumentu SMM a metodika SAM, které nejsou založeny na systémovém přístupu. Jako poslední přístup k neplánovaným změnám byl nastudován systémový model STAMP a jeho analýzy CAST, STPA a Aktivní STPA, které v současnosti stále nejsou využívány tolik, jako je tomu např. u přístupu ze SMM od ICAO. Pro srovnání byl také nastudován způsob identifikace a řízení neplánovaných změn, který využívá ÚCL.

Pro vytvoření návrhu této práce byl vybrán systémový model STAMP, který se jeví jako nejefektivnější pro socio-technické systémy, kterým civilní letectví je. Model STAMP ani jeho analýzy nejsou specificky zaměřeny na neplánované změny. Obecně ale udávají způsob, jak k systému přistupovat, a co přesně na něm analyzovat pro účely identifikace jakýchkoliv bezpečnostních problémů. Nejblíže se zabývá změnami analýza Aktivní STPA, která byla v návrhu využita pro proces, který nastává po porušení předpokladů proaktivních ukazatelů. Analýza STPA byla využita pro stanovení předpokladů a proaktivních ukazatelů a analýza CAST pro šetření leteckých nehod a incidentů, které patří mezi jeden ze zdrojů, jak porušení předpokladu zjistit.

V prvním kroku vytvořeného modelu bylo potřebné definovat jaké parametry budou muset stanovovat subjekty civilního letectví, aby na jejich základě byly CAA schopny stanovit si tytéž parametry v rámci SSP. Pro tyto účely musí subjekt vytvořit předpoklady a proaktivní a reaktivní ukazatele, které zašle CAA. Ten na zaslaných datech dále stanoví tytéž parametry již v rámci SSP. Ve třetím kroku se pomocí stanovených bezpečnostních cílů SSP stanoví dynamický set ukazatelů a dynamické profily rizik sektorů, které se dále

využívají v bezpečnostních panelech pro zpřehlednění nejdůležitějších dat z pohledu SSP. Posledním krokem je již samotná identifikace a řízení neplánovaných změn, které jsou založeny na sběru dat z provozu pomocí datových zdrojů a jejich následnému vyhodnocení. Pomocí vyhodnocení dat se identifikuje případná neplánovaná změna, která se vyznačuje prvním porušením předpokladu. V zodpovědnosti daného subjektu je poté provést Aktivní STPA, která má za cíl posoudit, zda nedošlo k porušení dalších předpokladů, a nakonec provést aktualizaci STPA dle závěru Aktivní STPA. Poslední část tohoto kroku tvoří aktualizace předpokladů a proaktivních ukazatelů v rámci SSP, která je provedena dle aktualizace subjektu.

Tento návrh má za cíl zavést systémový přístup do problematiky neplánovaných změn, díky kterému je identifikace a řízení neplánovaných změn jednodušší a efektivnější. Rovněž lze s jeho pomocí předcházet závažnějším důsledkům neplánovaných změn jako jsou letecké nehody a incidenty. Cílem tohoto návrhu není zahltit CAA jakožto hlavní orgán systému státní správy a dozoru civilního letectví veškerou zodpovědností nad neplánovanými změnami, ale rovnoměrně rozdělit tuto zodpovědnost mezi CAA a subjekty civilního letectví. V rámci SSP je primární roli CAA identifikace porušení předpokladu jakožto neplánované změny, upozornění subjektu o nastalé situaci a provádění dozorové činnosti nad nápravnými opatřeními této situace.

Jednou z hlavních limitací implementace tohoto návrhu a celkově systémového přístupu je nutné proškolení pracovníků systému státní správy a dozoru civilního letectví (zejm. CAA) ohledně problematiky systémového přístupu a jeho analýz. Tuto limitaci lze částečně omezit určením klíčových pracovníků z každého oddělení, kteří se podrobí školení. Druhou limitaci návrhu tvoří prvotní časová náročnost při implementaci zejm. při vytváření předpokladů a proaktivních ukazatelů v rámci SSP. Časová náročnost nastává ovšem pouze při implementaci návrhu. Při již vytvořených předpokladech a proaktivních ukazatelích v rámci SSP lze pomocí pravidelného vyhodnocování proaktivních ukazatelů identifikovat neplánovanou změnu včas, a předejít tak bezpečnostním událostem s mnohdy velmi závažnými ztrátami. Systémový přístup využitý v návrhu rovněž umožňuje mnohem efektivnější způsob identifikace neplánované změny než ten, který je v současnosti využíván. Současná forma diskuze nad možnými důvody již zvýšených reaktivních ukazatelů není efektivní ani z časové náročnosti, ale ani z hlediska včasnosti identifikace neplánované změny.

Model STAMP a jeho analýzy jsou založeny na systémovém přístupu. Ten je vhodný jak pro neplánované změny, tak pro veškeré ostatní problémy, se kterými se v bezpečnosti

potýkáme. Dle mého názoru je budoucí využití systémového přístupu ve všech aspektech provozní bezpečnosti v letecké dopravě žádoucí a velmi pravděpodobné. Otázkou pouze zůstává, kdy se tomu tak stane, neboť přechod ze staršího přístupu , který využívá spíše reaktivní přístup, může být obtížný pro některé subjekty civilního letectví. Faktem ale zůstává, že přístup modelu STAMP a jeho analýz je tím nejefektivnějším, který může letecká doprava a provozní bezpečnost využívat. Z tohoto důvodu je dle mého názoru vhodné nejprve z pozice CAA zvážit obměnu současného postupu ohledně neplánovaných změn s postupem založeným na systémovém přístupu, který je popsán v této práci. Pokud chce CAA přistupovat k neplánovaným změnám efektivně, proaktivně je v systému letecké dopravy identifikovat a zamezovat tak jejich negativnímu vlivu na provozní bezpečnost, je třeba přistoupit k systémovému přístupu. Ten je dále potřeba zakomponovat i do SSP, a to nejen z hlediska neplánovaných změn.

Seznam zdrojů

[1] LEVESON, Nancy. Engineering a Safer World: Systems Thinking Applied to Safety [online]. MIT: The MIT Press, 2012. ISBN 9780262016629.

[2] ICAO. Doc. 9859: Safety Management Manual. Montréal, Quebec, 2018. ISBN 978-92-9258-552-5

[3] A White Paper on Resilience Engineering for ATM. EUROCONTROL [online]. Září 2009 [cit. 2021-10-24]. Dostupné z: https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf

[4] LEVESON, Nancy. Safety III: A Systems Approach to Safety and Resilience [online]. MIT ENGINEERING SYSTEMS LAB, 7/1/2020 [cit. 2021-10-31]. Dostupné z: http://sunnyday.mit.edu/safety-3.pdf

[5] LEVESON, Nancy a John THOMAS. STPA Handbook [online]. 2018 [cit. 2021-10-30]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[6] MINISTERSTVO DOPRAVY ČR, ÚŘAD PRO CIVILNÍ LETETCVÍ. Předpis L 19: Dodatek N. In: Česká republika, 2013. [cit. 2021-10-30] Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm

[7] ŽIŽKOVSKÁ, Aneta. Analýza rizik v letecké dopravě z pohledu regulátora. Praha, 2018. Diplomová práce. České vysoké učení technické v Praze.

[8] Organization of civil aviation in the Czech Republic. Civil Aviation Authority of the Czech Republic [online]. Česká republika, 2021 [cit. 2021-11-07]. Dostupné z: https://www.caa.cz/en/authority/organization-of-civil-aviation-in-the-czech-republic/

[9] Vedení ministerstva: Odbor civilního letectví, O činnosti oddělení. Ministerstvo dopravy České republiky [online]. Česká republika, 2021 [cit. 2021-11-07]. Dostupné z: https://www.mdcr.cz/Ministerstvo/Vedeni-ministerstva

[10] Poskytnuté informace: Vznik a činnost Odboru civilního letectví Ministerstva dopravy ČR. Ministerstvo dopravy České republiky [online]. Česká republika, 2021 [cit. 2021-11-07]. Dostupné z: https://www.mdcr.cz/Ministerstvo/Zadost-o-poskytnuti-informace-(1)/Poskytnute-informace/Vznik-a-cinnost-Odboru-civilniho-letectvi-Minister

[11] Povinně zveřejňované informace. Úřad pro civilní letectví [online]. Česká republika, 2021 [cit. 2021-11-07]. Dostupné z: https://www.caa.cz/urad-pro-civilni-letectvi/povinne-zverejnovane-informace/

[12] Organizační struktura. Úřad pro civilní letectví [online]. Česká republika, 2021 [cit. 2021-11-09]. Dostupné z: https://www.caa.cz/wp-content/uploads/2020/11/organizacnistruktura.pdf?cb=30c38131a598d7123a0697f9162dd02c

[13] Průvodce hlášením v civilním letectví. Ústav pro odborné zjišťování příčin leteckých nehod [online]. 2021 [cit. 2021-11-09]. Dostupné z: https://uzpln.cz/pruvodce-hlaseni

[14] Povinně zveřejňované informace. Ústav pro odborné zjišťování příčin leteckých nehod [online]. 2021 [cit. 2021-11-11]. Dostupné z: https://uzpln.cz/povinne-informace

[15] Pověření právnických osob šetřením leteckých nehod a incidentů. Ústav pro odborné zjišťování příčin leteckých nehod [online]. 2021 [cit. 2021-11-11]. Dostupné z: https://uzpln.cz/povereni

[16] EUROCONTROL. E-SAM [online]. 2nd ed. 2006 [cit. 2021-12-05].

[17] LEVESON, Nancy. A New Accident Model for Engineering Safer Systems [online]. MIT [cit. 2021-12-14]. Dostupné z: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[18] LEVESON, Nancy. A systems approach to risk management through leading safety indicators. Reliability Engineering & System Safety [online]. Elsevier, 2014-10, (136), 17-34 [cit. 2021-12-19]. ISSN 0951-8320. Dostupné z: https://dspace.mit.edu/handle/1721.1/108601

[19] SILVA CASTILHO, Diogo. Active STPA: integration of hazard analysis into a Safety Management System Framework. 2019. Disertační práce. Massachusetts Institute of Technology, Department of Aeronautics and Astronautics.

[20] LEVESON, Nancy. CAST Handbook: How to Learn More from Incidents and Accidents [online]. 2019 [cit. 2021-12-14]. Dostupné z: http://sunnyday.mit.edu/CAST-Handbook.pdf

[21] ÚŘAD PRO CIVILNÍ LETECTVÍ. Směrnice ÚCL-331: Zpracování informací o bezpečnosti. Praha, 2019, 1. vydání.

[22] Nařízení Evropského parlamentu a Rady (EU) č. 376/2014. In: . Úřední věstník Evropské unie, 2014, L 122/18. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0376&from=CS

[23] About us. ECCAIRS 2 [online]. 2020 [cit. 2022-02-27]. Dostupné z: https://aviationreporting.eu/en/eccairs

[24] VITTEK, Peter, Slobodan STOJIĆ a Milan LÁNSKÝ. ADREP Events and Factors Contribution to Definition of Safety Performance Indicators for Airports. Aeronautica. 2015, XV.(1), 59-63. ISSN 978-83-7947-149-2.

[25] Dobrovolné hlášení událostí v civilním letectví. Úřad pro civilní letectví [online]. 2022 [cit. 2022-02-27]. Dostupné z: https://www.caa.cz/dokumenty/formulare/dobrovolne-hlaseni-udalosti-v-civilnim-letectvi/

[26] VITTEK, Peter, Jakub KRAUS a Stanislav SZABO. Moderní přístup k hodnocení provozní bezpečnosti v letectví. Brno: Akademické nakladatelství CERM, 2016. ISBN 978-80-7204-944-8.

[27] VAŠATA, Ondřej. Návrh proaktivních indikátorů bezpečnosti pro letiště s využitím modelu STAMP. Praha, 2021. Bakalářská práce. České vysoké učení technické v Praze.

[28] Jet Efflux Hazard. In: SKYbrary [online]. 2021-22 [cit. 2022-05-03]. Dostupné z: https://skybrary.aero/articles/jet-efflux-hazard

[29] Accident Investigation Report Aircraft ATR 42-500 SX-GRI at Athens International Airport on October 07, 2017 [online]. Nea Philadelphia: AIR ACCIDENT INVESTIGATION AND AVIATION SAFETY BOARD, 17.2.2022 [cit. 2022-04-29]. Dostupné z: https://aaiasb.gr/en/-2022/487-01-2022.html