ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Ústav letecké dopravy

Systémové řízení plánovaných změn v rámci státního programu bezpečnosti

Diplomová práce

Bc. Michaela Fukalová

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. Michaela Fukalová

Studijní program (obor/specializace) studenta:

navazující magisterské –PL– Provoz a řízení letecké dopravy

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

Název tématu (anglicky): **Systemic Change Management of Planned 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 řízení plánovaných změn v leteckém provozu s využitím systémového přístupu k bezpečnosti.
- Analyzujte legislativní rámec a standardy pro státní programy bezpečnosti v kontextu řízení plánovaných změn
- Analyzujte současné metody systémového přístupu k bezpečnosti
- Vyberte a specifikujte systém dozoru státu nad konkrétním typem letecké organizace v kontextu řízení plánovaných změn
- Navrhněte postup dozorové činnosti státu a klíčové prvky pro státní program bezpečnosti založený na systémovém přístupu k bezpečnosti pro řízení plánovaných 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

L. S.

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

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

Potvrzuji převzetí zadání diplomové práce.

Bc. Michaela Fukalová
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 etické přípravě vysokoškolských závěrečných pracích.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu zákona § 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 13. 5. 2022 .....

Bc. Michaela Fukalová

Poděkování

Tímto bych ráda poděkovala svému vedoucímu doc. Ing. Andreji Lališovi, Ph.D. za jeho ochotu, podporu a zejména cenné rady při psaní této diplomové práce. Také bych ráda poděkovala zaměstnancům Úřadu pro civilní letectví za poskytnutí potřebných materiálů pro účely této práce.

V neposlední řadě bych chtěla poděkovat své rodině a přátelům za neutuchající podporu během celého mého studia.

Abstrakt

Cílem této diplomové práce je navržení postupu a klíčových prvků státního programu bezpečnosti pro řízení plánovaných změn v leteckém provozu s využitím systémového přístupu k bezpečnosti. První část práce přibližuje legislativní stránku státních programů bezpečnosti (SSP) spolu se zaměřením na dozorový orgán civilního letectví. Následuje popis přístupů k řízení plánovaných změn, především přístupu ICAO dle Safety Management Manual a metodiky SAM (Safety Assessment Methodology) a dále vysvětlení systémového přístupu k bezpečnosti s bližší specifikací STPA, Active STPA a CAST. Současný přístup dozorového orgánu k řízení plánovaných změn je demonstrován na konkrétních příkladech dozoru nad subjekty civilního letectví, na což navazuje navržený postup spolu s klíčovými prvky pro řízení plánovaných změn ze strany dozorového orgánu s využitím systémového přístupu, kde dochází ke kombinaci metodiky SAM spolu s STPA a Active STPA. V závěru práce je navržený postup patřičně validován.

Klíčová slova: řízení plánovaných změn, státní program bezpečnosti, dozorový orgán civilního letectví, Metodika posouzení bezpečnosti, Systémově-teoretická analýza procesů, Aktivní Systémově-teoretická analýza procesů, předpoklad, proaktivní indikátor

Abstract

The objective of the master's thesis is to design the procedure and key elements of the state safety program for the management of planned changes in air traffic using a systemic approach to safety. The first part approaches the legislative side of state safety programs (SSP) together with a focus on the civil aviation authority. The following is a description of approaches to managing planned changes, especially the ICAO approach according to the Safety Management Manual and the SAM (Safety Assessment Methodology), as well as an explanation of the systemic approach to safety with more detailed specification of STPA, Active STPA and CAST. The current approach of the civil aviation authority to the management of planned changes is demonstrated on specific examples of supervision of civil aviation entities, followed by the proposed procedure together with key elements for the management of planned changes by the civil aviation authority using a systemic approach where the SAM methodology is combined with STPA and Active STPA. At the end of the work, the proposed procedure is properly validated.

Keywords: Management of Planned Changes, State Safety Programme, Civil Aviation Authority, Safety Assessment Methodology, System-Theoretic Process Analysis, Active System-Theoretic Process Analysis, Assumption, Leading Indicator

Obsah

Seznam obrázků

Seznam tabulek

Seznam příloh

Seznam použitých zkratek

AHAI	Active Hazard Analysis Input	Vstup aktivní analýzy nebezpečí
ALoS	Acceptable Level of Safety	Přijatelná úroveň bezpečnosti
ALoSP	Acceptable Level of Safety Performance	Přijatelná úroveň výkonnosti v bezpečnosti
AMC	Acceptable Means of Compliance	Přijatelné způsoby průkazu
BEK	-	Bezpečnostní kontrola
BPMN	Business Process Modeling Notation	Notace pro modelování podnikových procesů
CAST	Causal Analysis based on STAMP	Analýza příčin založená na STAMP
CE	Critical element	Kritický prvek
CMES	CMES – Combined Mitigation Effectiveness Score	Kombinované skóre účinnosti zmírnění
CPMS	Combined Post-Mitigation Severity	Kombinovaná závažnost po zmírnění
ČR	-	Česká republika
DoC	Declaration of Conformity	Prohlášení o shodě
DoV	Declaration of Verification	Prohlášení o verifikaci
DSU	Declaration of Suitability for Use	Prohlášení o vhodnosti k použití
EASA	European Union Aviation Safety Agency	Agentura Evropské unie pro bezpečnost letectví
EU	European Union	Evropská unie
EUROCONTROL	European Organisation for the Safety of Air Navigation	Evropská organizace pro bezpečnost leteckého provozu
FHA	Functional Hazard Assessment	Funkční posouzení nebezpečí
FMEA	Failure Mode and Effects Analysis	Analýza možného výskytu a vlivu vad
FTA	Fault Tree Analysis	Analýza stromu poruchových stavů
GM	Guidance Material	Poradenský materiál
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví

LAA	Light Aircraft Association	Letecká amatérská asociace
MES	Mitigation Effectiveness Score	Skóre účinnosti zmírnění
MIT	Massachusetts Institute of Technology	Massachusettský technologický institut
MoC	Management of Change	Řízení změn
PMS	Pre-Mitigation Severity	Závažnost před zmírněním
PPMS	PPMS – Post-Potential Mitigation Severity	Závažnost po potenciálním zmírnění
PSSA	Preliminary System Safety Assessment	Předběžné posouzení bezpečnosti systému
SAM	Safety Assessment Methodology	Metodika posouzení bezpečnosti
SLZ	-	Sportovní létající zařízení
SMS	Safety Management System	Systém řízení bezpečnosti
SPI	Safety Performance Indicator	Indikátor výkonnosti v bezpečnosti
SRM	STPA-Informed Risk Matrix	STPA-informovaná matice rizik
SSA	System Safety Assessment	Posouzení bezpečnosti systému
SSO	State Safety Oversight	Systém státního dozoru nad bezpečností
SSP	State Safety Programme	Státní program bezpečnosti
STAMP	System-Theoretic Accident Model and Process	Systémově-teoretický model nehody a proces
STPA	System-Theoretic Process Analysis	Systémově-teoretická analýza procesů
SW	Software	-
TCAS	Traffic Alert and Collision Avoidance System	Palubní protisrážkový systém
UCA	Unsafe Control Action	Nebezpečné řízení
ÚCL	Civil Aviation Authority of the Czech Republic	Úřad pro civilní letectví
ÚZPLN	-	Ústav pro odborné zjišťování příčin leteckých nehod

Úvod

Letecká doprava je dynamicky se rozvíjející způsob dopravy, který je hojně využíván lidmi po celém světě. Není to jen z důvodu komfortu, rychlosti či finanční dostupnosti, ale rovněž z hlediska bezpečnosti, která je považována za důležitý aspekt. Pokud není zajištěna požadovaná úroveň bezpečnosti, neprojeví se to pouze na reputaci letectví, ale může to také negativně ovlivnit ekonomickou stránku letectví v případě vzniku incidentů a nehod. Proto by mělo být hlavním zájmem neustále zvyšovat úroveň bezpečnosti.

Obecně je bezpečnost považována za stav, kdy jsou eliminovány podmínky, které by mohly způsobit smrt, zranění, poškození majetku apod. Prvotní přístup k bezpečnosti byl především reaktivní. Bezpečnost byla hodnocena na základě nežádoucích událostí (incidentů a nehod) a až poté byla navržena preventivní opatření na základě zjištěných příčin, aby již k podobným situacím nedocházelo. Ačkoliv je nutné poučit se z chyb, není rozhodně dostačující čekat pouze na to, až chyby nastanou. Je důležité uplatňovat zároveň proaktivní přístup a snažit se do určité míry předvídat, k čemu by u daného systému mohlo dojít a jak by bylo možné tomu předcházet. Skutečností však je, že nikdy není možné předvídat veškeré situace, a proto je nutné, aby oba přístupy (reaktivní a proaktivní) fungovaly ruku v ruce.

Zároveň se neustále zvyšuje komplexita a provázanost veškerých systémů, na což je nutné rovněž reagovat. Dosavadní bezpečnostní modely a metody jsou v tomto směru pro velmi komplexní systémy nedostatečné, navíc obvykle neberou v úvahu veškeré úrovně systému. Stále více skloňovaný je systémový přístup k bezpečnosti, v rámci něhož je vyzdvižena myšlenka, že systém by měl být uvažován jako celek. Bezpečnostní model STAMP a související analýzy STPA a CAST přináší nový pohled na to, jak uvažovat nad bezpečnostní systému.

Z hlediska prosperity a posouvání hranic úrovně bezpečnosti je zároveň nezbytné vypořádat se s neustálými změnami. Pokud má být systém aktuální vzhledem k současným trendům v provozu, je potřeba uvažovat nad plánovanými změnami, které však z hlediska bezpečnosti znamenají výzvu a jsou zcela jistě kritickou fází v životním cyklu každého systému. Ať už se jedná o zavedení nového systému do letadla, výstavbu nového terminálu letiště či změnu postupů při odbavení, vše jsou to příklady plánovaných změn, nad kterými je nejčastěji uvažováno z toho důvodu, že se například vyvíjí nové technologie nebo že došlo k nárůstu počtu odbavených cestujících apod.

Vždy se jedná o cíl posunout systém vpřed, avšak aby bylo tohoto cíle dosaženo, je nezbytné zvážit bezpečnostní stránku plánovaných změn. Do systému mohou nejen přinášet nová nebezpečí, ale také měnit nebezpečí stávající.

Vzhledem k faktu, že je letecká doprava odvětvím, které vyžaduje patřičnou regulaci ze strany státu, rovněž problematika plánovaných změn subjektů civilního letectví musí být adekvátně regulována ze strany Úřadu pro civilní letectví dle státního programu bezpečnosti (SSP). Zároveň při uvážení neustále se zvyšující komplexity systémů subjektů civilního letectví je nutné vhodně přizpůsobit dozorové činnosti, aby reflektovaly systémový přístup k bezpečnosti.

Cílem této diplomové práce je navrhnout postup a klíčové prvky v rámci SSP pro řízení plánovaných změn s využitím systémového přístupu k bezpečnosti a tím představit dozorovému orgánu (ÚCL) způsob, jak zakomponovat tento nový přístup do dozorové činnosti a neustále tak zvyšovat úroveň bezpečnosti civilního letectví.

1 Státní program bezpečnosti

Státní program bezpečnosti (State Safety Programme – SSP) je soubor předpisů a činností zaměřených na zvyšování úrovně bezpečnosti. Podklad pro vytvoření a realizaci státního programu bezpečnosti dává svým členským státům Mezinárodní organizace pro civilní letectví (ICAO), a to skrze dokument ICAO Doc. 9859: Safety Management Manual. Pro členské státy ICAO platí, že pro dosažení přijatelné úrovně výkonnosti v bezpečnosti v civilním letectví musí vytvořit a zavést státní program bezpečnosti. V České republice je SSP vydáváno Ministerstvem dopravy ve formě Dodatku N k leteckému předpisu L19. [1] [2]

Tabulka 1 představuje základní strukturu SSP, která je tvořena čtyřmi hlavními komponenty. [1]

Tabulka 1: Komponenty státního programu bezpečnosti (upraveno z [1])

Komponenty SSP
Bezpečnostní politika státu a její cíle
Řízení bezpečnostního rizika na úrovni státu
Zajištění bezpečného provozu na úrovni státu
Prosazování bezpečného provozu na úrovni státu

Mimo jiné má SSP plnit funkci spojujícího prvku mezi bezpečnostními procesy na úrovni státu a bezpečnostními procesy subjektů činných v oblasti civilního letectví. Zásadní účel, který má SSP plnit, je dosažení přijatelné úrovně bezpečnosti (Acceptable Level of Safety – AloS). Podstatou konceptu určení ALoS je doplnění přístupu založeného na principu posuzování shody organizací s platnými legislativními požadavky o přístup zaměřený na posuzování skutečné výkonnosti v bezpečnosti daného subjektu v civilním letectví. [1]

Aby mohly být zásady SSP patřičně implementovány, je důležitá koordinace všech orgánů, které jsou zodpovědné za státní správu v letectví v daném státě. Cílem implementace SSP je pak neustálé zdokonalování procesů a činností pro zvyšování úrovně bezpečnosti a také účinné provádění SMS (Safety Management System) subjekty činnými v oblasti letectví. [2]

SSP má svým obsahem pokrývat 8 kritických prvků (Critical elements – CE) systému státního dozoru nad bezpečností (State Safety Oversight – SSO), jež jsou uvedené v tabulce 2.

Tabulka 2: Kritické prvky systému státního dozoru nad bezpečností (upraveno z [2])

CE-1	Primární letecká legislativa
CE-2	Specifické provozní předpisy
CE-3	Systém civilního letectví státu a jeho funkce
CE-4	Kvalifikace odborného technického personálu
CE-5	Technické pokyny, nástroje a poskytování informací důležitých pro bezpečnost
CE-6	Průkazy způsobilosti, osvědčení, oprávnění a schvalování
CE-7	Povinnosti v oblasti dozoru
CE-8	Řešení bezpečnostních problémů

1.1 Bezpečnostní politika státu a její cíle

První komponent SSP má popisovat, jakým způsobem bude příslušný stát řídit bezpečnost v celém svém systému letectví. Měl by zahrnovat povinnosti, funkce a činnosti správních orgánů daného státu, stejně tak jako stanovené bezpečností cíle, kterých chce stát dosáhnout. [2]

Bezpečnostní politika státu by měla jasně popisovat bezpečnostní záměry a směřování státu v oblasti bezpečnosti. Jejím úkolem by mělo být stanovení klíčových postupů nezbytných pro řízení bezpečnosti a zároveň to, jaké přístupy budou využity pro plnění odpovědností z hlediska bezpečnosti. [2]

Bezpečnostní cíle státu pak mají určovat směr státním úřadům v letectví a představovat požadované výsledky. Pro jejich stanovení je však potřeba nejprve si uvědomit hlavní bezpečnostní rizika v daném systému letectví konkrétního státu a rovněž to, do jaké míry je stát schopen ovlivnit požadované výsledky. Definování bezpečnostních cílů mimo jiné pomáhá pro následné určení ALoS a především určuje priority státu pro řízení bezpečnosti, což dále ovlivňuje řízení a přidělování potřebných zdrojů. [2]

1.2 Řízení bezpečnostního rizika na úrovni státu

Další část SSP se týká požadavku, aby státy byly schopny identifikovat případná bezpečnostní rizika a byly je schopny adekvátně řídit. Dle ICAO by měly být postupně

zaváděny proaktivní procesy pro identifikaci příčin incidentů či nehod. V návaznosti na to by měly jednotlivé státy apelovat na subjekty působící v civilním letectví, aby zavedly ve svých organizacích SMS. Zároveň je doporučeno kontrolovat účinnost těchto SMS a posuzovat, zda dané subjekty vhodně řídí bezpečnostní rizika. [2]

Řízení bezpečnostních rizik (Safety Risk Management) se však týká i státních dozorových orgánů. Především by měly na základě zásad řízení bezpečnostních rizik vyvíjet příslušné předpisy a podle vyhodnocených rizik určovat priority pro následnou dozorovou činnost. Poměrně zásadní je v rámci řízení bezpečnostních rizik na úrovni státu také vydávání licencí, certifikátů a povolení. Procesy související s tímto vydáváním totiž státu umožňují posoudit, zda dané subjekty dosahují požadovaných standardů pro bezpečný provoz v rámci letectví. [2]

Dalším velmi podstatným procesem je proces šetření nehod. Jeho důležitost tkví především v tom, že umožňuje státu nejen zjišťovat příčiny nehod či přispívající faktory, ale také umožňuje stanovit případná nápravná opatření, aby se takovým situacím do budoucna předcházelo. Vedením tohoto procesu má být pověřen úřad pro šetření nehod (v ČR se jedná o ÚZPLN), který bude zcela nezávislý na jiné organizaci a stejně tak i nezávislý na úřadu pro civilní letectví daného státu (v ČR je tímto úřadem Úřad pro civilní letectví – ÚCL). V případě, že se jedná o událost, která nepodléhá šetření na úrovni státu, je žádoucí, aby proběhlo šetření na úrovni konkrétního subjektu, kterého se událost týká. [2]

Ať už zmíněné oficiální šetření nehod a incidentů či šetření na úrovni jednotlivých poskytovatelů služeb v civilním letectví poskytuje státu významný zdroj dat a informací, se kterými je v rámci řízení bezpečnostních rizik dále nakládáno. Dalšími zdroji mohou být zprávy a případné nálezy z auditní činnosti dozorových orgánů, zprávy ze systémů pro hlášení událostí (ať už se jedná o povinný či dobrovolný systém), případně také bezpečnostní studie apod. Data a informace z uvedených zdrojů umožní leteckým úřadům jednotlivých států identifikovat a posuzovat případná nebezpečí a zároveň vznikající trendy v systému letectví daného státu. [2]

1.3 Zajištění bezpečného provozu na úrovni státu

Účelem činností spadajících pod zajištění bezpečného provozu na úrovni státu je zejména ujištění, že bezpečnostní procesy státu umožňují dosáhnout požadovaných bezpečnostních cílů, které si stát nastavil. Zároveň se vyžaduje zakomponování procesu zajištění bezpečného provozu i do SMS jednotlivých subjektů letectví, aby mohlo být

zajištěno efektivní fungování všech bezpečnostních procesů a tím i dosaženo stanovených bezpečnostních cílů. [2]

Aby měl stát kontrolu nad úrovní bezpečnosti, musí zajistit potřebný dohled nad civilním letectvím. V rámci tohoto dohledu by mělo docházet ke shromažďování, rozboru, sdílení a výměně bezpečnostních dat a informací. Díky těmto správně nastaveným krokům může stát vhodně cílit své zdroje a aktivity, konkrétně například právě již zmíněný dozor, na oblasti vyžadující zvýšenou pozornost. S dozorovou činností souvisí i to, že by měl stát pravidelně vyhodnocovat výkonnost v bezpečnosti jednotlivých poskytovatelů služeb v civilním letectví. Výkonnost v bezpečnosti může vyhodnocovat na základě sledování indikátorů výkonnosti v bezpečnosti (Safety Performance Indicator – SPI). Jedná se o určité parametry, které umožňují jak jednotlivým subjektům, tak státu, sledovat, jaký je vývoj výkonnosti v bezpečnosti. Zásadní je, aby tyto indikátory byly vhodně stanoveny a aby souvisely s určenými bezpečnostními cíli. [2]

V rámci hodnocení výkonnosti v bezpečnosti mají státy stanovit tzv. přijatelnou úroveň výkonnosti v bezpečnosti (Acceptable Level of Safety Performance – ALoSP). Splnění této nastavené úrovně výkonnosti v bezpečnosti se má očekávat od všech subjektů tvořících systém letectví daného státu. [2]

1.3.1 Řízení změn

Součástí zajištění bezpečnosti na úrovni státu by mělo být také řízení změn. Prozatím není výslovně požadováno, aby stát stanovil konkrétní činnosti pro řízení změn v SSP. I přes to je doporučeno, aby stát zavedl postupy pro řízení změn, neboť ke změnám dochází v dnešním světě stále častěji. S každou změnou mohou vznikat nová nebezpečí a může mít tak i vliv na dosavadní identifikovaná bezpečnostní rizika. Proto by měly být implementovány postupy, které by sloužily pro posuzování vlivu změn na stávající systém a v rámci procesu řízení bezpečnostních rizik by měla být nová či dosavadní bezpečnostní rizika ovlivněná změnou patřičně analyzována a případně zmírněna. [2]

1.4 Prosazování bezpečného provozu na úrovni státu

Pokud si budou mezi sebou orgány státní správy a jednotlivé subjekty sdělovat své priority, osvědčené bezpečnostní postupy, rizika a způsoby, jakým je řídí, bude pro ně snazší a účinnější dosažení nastavených bezpečnostních cílů a spolu s tím i jednodušší nastavení přijatelné úrovně bezpečnosti v rámci celého systému letectví daného státu. Dá se tak říct, že zlepšení výkonnosti v bezpečnosti do určité míry závisí na kultuře bezpečnosti. Pro rozvoj pozitivní kultury bezpečnosti by bylo vhodné, aby úřad pověřený

dozorovou činností nad civilním letectvím v určitém státě zavedl mechanismy pro komunikaci na interní i externí úrovni a umožnil tak výměnu příslušných bezpečnostních informací. [2]

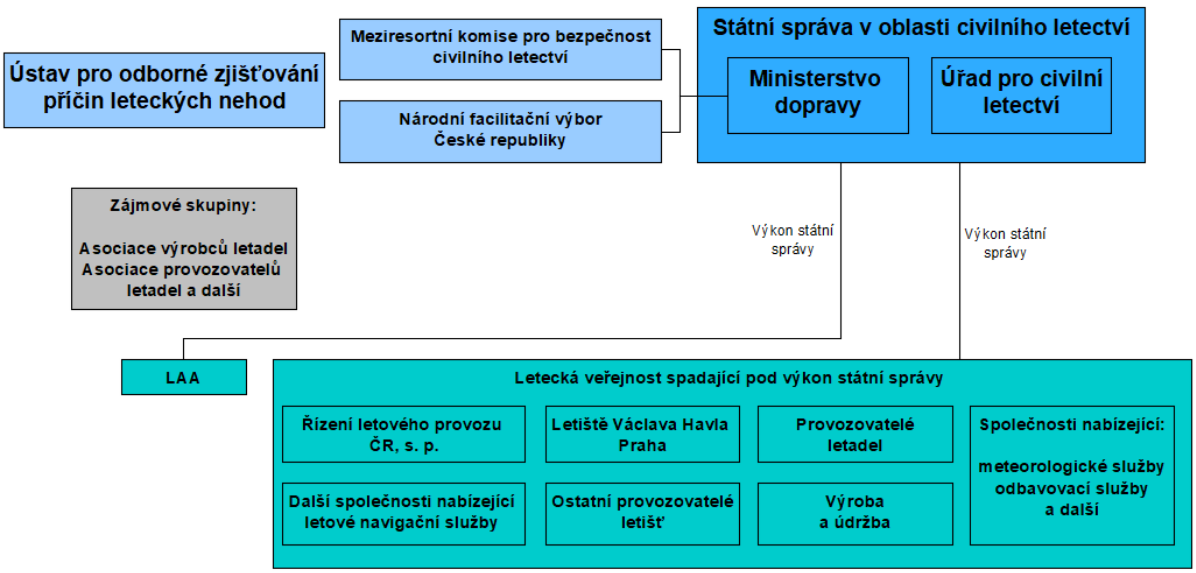
Z pohledu interního šíření informací o bezpečnosti je podstatný nejprve sběr a zpracování těchto informací, které jsou například získávány prostřednictvím systémů pro hlášení událostí. Následně musí existovat efektivní spolupráce mezi orgány státní správy, a to především mezi dozorovým úřadem a úřadem, který je pověřen šetřením nehod. Existuje mnoho způsobů, jakými lze komunikaci v rámci těchto orgánů i mezi nimi zajistit. Ať už se však jedná o komunikaci přes různé publikace, bulletiny, e-maily či osobně v rámci školení, zasedání nebo formou diskuze apod., vždy by měl být způsob interní komunikace zvolen podle povahy konkrétní sdělované informace. [2]

Neméně důležitá je komunikace na externí úrovni mezi orgány státní správy a subjekty působícími v civilním letectví. I zde by měla být vždy vhodně zvolena komunikační platforma na základě typu konkrétního sdělení. Použity mohou být způsoby komunikace uvedené výše pro komunikaci interní, nicméně u externí komunikace obvykle platí, že informace jsou sdělovány většímu počtu adresátů, tudíž se jako vhodnější způsoby pro výměnu informací jeví například sociální média, semináře či vytvoření komunit zaměřených přímo na výměnu bezpečnostních informací. [2]

2 Dozor nad bezpečností civilního letectví

Civilní letectví je značně složitým a provázaným odvětvím, které musí být patřičně regulováno a dozorováno. Na evropské úrovni se oblastí dozoru nad bezpečností civilního letectví zabývá Agentura Evropské unie pro bezpečnost letectví (EASA). Jejím cílem je především harmonizace předpisů a procesů s nimi spojených, dále pak bezpečnostní dohled nad členskými státy Evropské unie (EU) společně s prosazováním bezpečnostních norem. Pro členské státy EU však platí povinnost regulovat a dozorovat letectví rovněž na národní úrovni.

Regulační a dozorovou činnost zastávají příslušné orgány státní správy (obrázek 1), v České republice konkrétně Ministerstvo dopravy a Úřad pro civilní letectví. Ministerstvo dopravy je ústředním orgánem státní správy v oblasti dopravy. Připravuje novely zákonů a zároveň k nim vydává prováděcí právní předpisy. Na obrázku 1 jsou uvedeny další odpovědné subjekty činné v civilním letectví, například Ústav pro odborné zjišťování příčin leteckých nehod (ÚZPLN), jehož činnost zahrnuje zejména šetření incidentů a nehod a následné stanovení příčin těchto událostí. Letecká amatérská asociace (LAA) je zodpovědná za výkon správní činnosti v oblasti sportovních létajících zařízení (SLZ). Dále jsou zde uvedeny subjekty civilního letectví, nad kterými je státní správa vykonávána – provozovatelé letišť, poskytovatelé letových provozních služeb, provozovatelé letadel apod. [1]



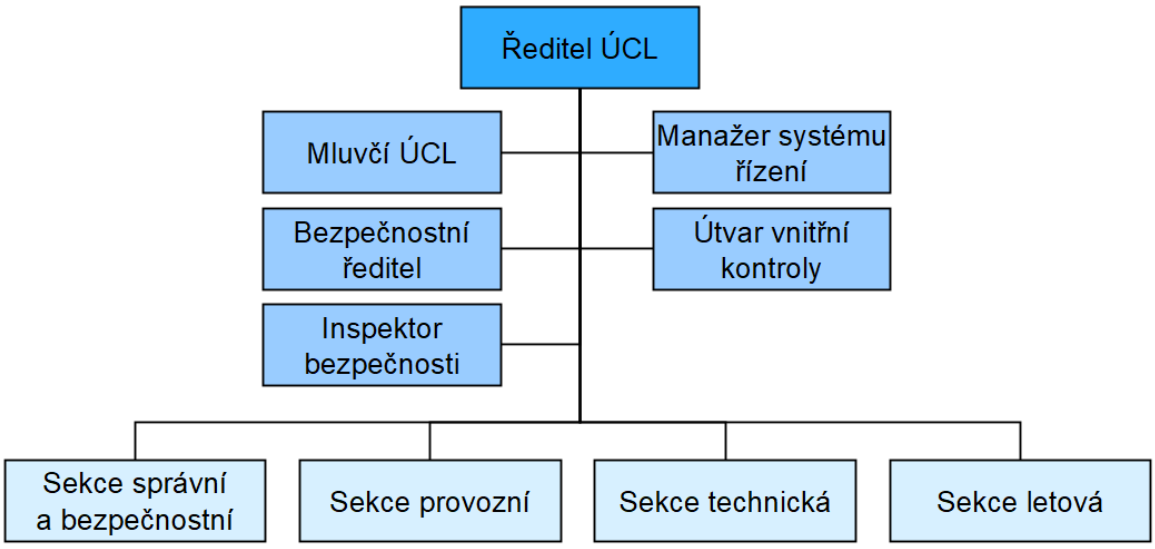
Obrázek 1: Státní správa civilního letectví v České republice (upraveno z [5])

2.1 Úřad pro civilní letectví

Úřad pro civilní letectví je výkonným orgánem státní správy v letectví pro Českou republiku, který je přímo podřízený Ministerstvu dopravy. Oba tyto správní orgány jsou povinny vykonávat činnosti uvedené v zákoně č. 49/1997 Sb., o civilním letectví. Z pohledu ÚCL se jedná především o odpovědnosti ve sféře schvalování organizací činných v oblasti civilního letectví, stejně tak jako ve schvalování personálu těchto organizací, dále odpovědnosti ve směru certifikace a letové způsobilosti letadel, letadlových částí, zařízení a rovněž zachování letové způsobilosti. [1]

2.1.1 Organizační struktura ÚCL

Vedením ÚCL je pověřen ředitel, jehož pravomocí je zejména rozhodovat v klíčových otázkách týkajících se například organizačního rozvržení ÚCL či pracovněprávních záležitostí, vytyčit koncepci činností ÚCL, schvalovat rozpočet a plány činností ÚCL atd. Další funkce vykonávají osoby, které přímo spadají pod ředitele ÚCL a jsou jimi – mluvčí ÚCL, manažer systému řízení, bezpečnostní ředitel, útvar vnitřní kontroly a inspektor bezpečnosti. Mimo zmíněné pozice tvoří organizační strukturu čtyři sekce sestávající se z odborů, které se dále rozdělují na jednotlivá oddělení. Základní organizační struktura ÚCL je zobrazena na obrázku 2. [3]



Obrázek 2: Základní organizační struktura ÚCL (upraveno z [3])

Sekce technická

Hlavní činnost sekce technické spočívá ve výkonu státní správy a státního dozoru nad dokazováním a zachováním typové způsobilosti letadel, motorů, vrtulí, letadlových částí a zařízení, mimo jiné pak také opravňování organizací k činnostem spojeným

s vývojem, projektováním, zkouškami, výrobou, údržbou apod. S tím navíc souvisí posuzování případných hlášení o událostech se zaměřením na letovou způsobilost. [4]

Sekce letová

Výkon státní správy u sekce letové se zaměřuje na osvědčování a průběžný dozor českých provozovatelů obchodní letecké dopravy, neobchodního a zvláštního provozu a dále v omezeném rozsahu na dozor nad zahraničními provozovateli letadel. Navíc je sekce letová pověřena vedením rejstříku letadel, dozorovou činností nad sportovními létajícími zařízeními a v neposlední řadě posuzuje způsobilosti leteckého personálu. [4]

Sekce správní a bezpečnostní

Klíčovým úkolem sekce správní a bezpečnostní je výkon právních služeb ÚCL, státní správa v oblasti ochrany civilního letectví před protiprávními činy a mimo to obstarání logistických záležitostí pro chod úřadu. Zároveň má pod svou správou celý proces ověřování spolehlivosti. [4]

Sekce provozní

Sekce provozní vykonává státní správu a dozor nad způsobilostí a provozem civilních a vojenských letišť a nad oblastí týkající se rozdělování a řízení vzdušného prostoru ČR. Dále je zodpovědná za dohled nad provozní bezpečností v okruhu letových navigačních služeb, uspořádání toku letového provozu a uspořádání vzdušného prostoru. V neposlední řadě je pověřena osvědčováním poskytovatelů letových navigačních služeb a organizací zaštiťujících výcvik řídících letového provozu. [4]

I přes rozdílné odpovědnosti sekcí zde existuje významná spolupráce nejen mezi dílčími odděleními či odbory v rámci jedné sekce, ale i spolupráce mezi jednotlivými sekcemi, což je pro správný chod tohoto výkonného orgánu státní správy klíčové.

2.1.2 Činnosti ÚCL

Vzhledem k faktu, že je ÚCL hlavním výkonným orgánem státní správy v letectví v České republice, je rozsah činností, které ÚCL vykonává, poměrně obsáhlý. ÚCL vydává oprávnění, povolení a souhlasy konkrétním subjektům figurujícím v oblasti letecké dopravy, kdy v rámci těchto procesů posuzuje jejich způsobilost k vykonávání daných aktivit. Tím však jeho odpovědnost vůči zmíněným subjektům nekončí. V průběhu jejich fungování provádí ÚCL průběžný dozor ve formě inspekcí či auditů, jehož účelem je především posouzení shody s platnými legislativními požadavky, implementace těchto požadavků v provozu a zhodnocení, zda je daný subjekt schopen identifikovat případná

nebezpečí a efektivně řídit bezpečnostní rizika. V případě nevyhovění stanoveným požadavkům či závažného pochybení má ÚCL pravomoc vydaná oprávnění pozastavit nebo odebrat. [1]

Pro činnost ÚCL je rovněž důležitý sběr dat od subjektů v letectví. Tato data získává jak během prvotních schvalovacích procesů při vydávání oprávnění, tak i během pravidelné dozorové činnosti. Dalším významným zdrojem externích dat jsou také systémy pro hlášení událostí v letectví. Systém pro povinné hlášení událostí v letectví má pod svou správou ÚZPLN. V případě, že se nejedná o událost, která spadá pod povinně nahlašované události, je možné využít systém pro dobrovolné hlášení událostí pod ÚZPLN nebo ÚCL. [1]

Kromě činností spojených s certifikací, vydáváním průkazů apod., je ÚCL zároveň orgánem posuzujícím případné plánované změny v organizacích. Jedná se tak o další proces spjatý s dozorovou činností ÚCL, který je z hlediska bezpečnosti velmi důležitý, neboť v neustále se rozvíjejícím letectví dochází často ke změnám, které musí být nejen prvotně vhodně posouzeny, ale následně především adekvátně implementovány do provozu. [1]

Ať už se jedná o vydávání oprávnění organizacím v letectví či leteckému personálu, certifikaci letišť, vykonávání dozoru nad těmito organizacemi apod., veškeré postupy pro uvedené procesy popisuje ÚCL v rámci své dokumentace, konkrétně ve směrnicích a příručkách. Tyto dokumenty obsahují jak postupy ÚCL, tak i požadavky na danou organizaci, které musí být splněny, a to na základě standardů a regulačních požadavků ze strany ICAO, EASA a zároveň musí být v souladu s národními legislativními požadavky. [1]

3 Změny v kontextu provozní bezpečnosti

Letectví je obor, který se neustále vyvíjí, na což musí subjekty působící v civilním letectví, a stejně tak orgány státní správy neustále reagovat. Nejde pouze jen o zavádění nových postupů, technologií, ale rovněž o změny v objemech dopravy v závislosti na různých aspektech. Příkladem může být situace spojená s pandemií COVID-19, která významným způsobem ovlivnila celý svět. Je tedy patrné, že téměř jakékoliv změny hrají v letectví velmi významnou roli a jsou téměř nezbytné, pokud má být daný systém neustále prosperující. Nicméně i přes pozitivní úmysly při zavádění změn může často docházet i k negativním dopadům, které s sebou mohou změny přinášet. Každá změna by tak měla být vždy s ohledem na svou povahu řádně posouzena, vhodně implementována do provozu a následně i dostatečně sledována a řízena. [1] [6] [7]

Změny se dají dělit podle toho, zda se jedná o změny plánované, které jsou do provozu vnášeny s určitým záměrem, a změny neplánované, které vznikají v závislosti na provozu bez předchozího záměru a mohou být také odrazem zavedení změn plánovaných. Je tedy zřejmé, že ačkoliv se jedná o dva odlišné typy změn, jsou vzájemně provázané a daný systém by měl být připraven na jakoukoliv z nich. Oba typy změn mohou jistě znamenat pro daný systém velký přínos, ale musí být vhodně nastaveny postupy pro jejich řízení, jinak mohou znamenat problém z hlediska bezpečnosti. [6] [7]

3.1 Plánované změny

Plánované změny jsou změny, které jsou důležité pro každý systém s ohledem na jeho neustálý vývoj, a jsou tak předem plánovány s konkrétním cílem. Zpravidla se může jednat o změny provozní, změny v infrastruktuře, změny organizačního charakteru apod. Ať už se však jedná o jakýkoliv typ plánované změny, každá obvykle ovlivní nejen část systému, ve které má být zavedena, ale také jeho další části v závislosti na provázanosti daného systému. [6] [7]

Ačkoliv se může zdát, že při plánovaných změnách jsou vždy dopředu promyšleny veškeré situace, které mohou s jejich zavedením nastat, mnohdy tomu tak není a plánované změny se tím pádem stávají, místo pozitivním směrováním daného systému, spíše potenciální příčinou následných incidentů či nehod. K tomu dochází především z toho důvodu, že bezpečnostní analytici dnes nejsou schopni předpovědět zdaleka vše, co může změna přinést.

Každý systém by měl být ve svém provozu připraven na plánované změny, které zcela jistě během jeho životního cyklu nastanou. To stejné pak platí jak pro subjekty civilního

letectví v rámci jejich SMS, tak i pro státní správu v civilním letectví v rámci SSP. Měly by být stanoveny postupy pro řízení plánovaných změn, které by každou změnu vyhodnocovaly s ohledem na její dopady na bezpečnost. [6] [7]

3.2 Neplánované změny

Jako neplánované změny, jsou označovány změny, které jsou do provozu systému zaváděny bez předchozího záměru. Jedná se především o výsledek provozu systému v určitých podmínkách, kdy tento výsledek nebyl dopředu očekáván, respektive plánován. Jako příklad může být uvedena situace, která nastala v souvislosti s pandemií COVID-19. Rok 2019 byl z hlediska počtu odbavených cestujících velice příznivý a s vidinou takto příznivého průběhu vkročilo letectví do roku 2020, ve kterém došlo k velmi výrazné neplánované změně – pandemii onemocnění COVID-19, jež ovlivnila cestování včetně letecké dopravy a došlo tak ke značnému snížení počtu odbavených cestujících.

Zároveň je častým důvodem vzniku neplánovaných změn přehodnocení rizik. Jako příklad může být uvedena situace, kdy pracovníci konkrétní organizace civilního letectví po určitou dobu nezaznamenávají žádné nežádoucí situace v provozu, a tudíž nesprávně přehodnocují své vnímání rizik. Začínají porušovat nastavená pravidla v domnění, že tím nebude bezpečnost ovlivněna a mohou tak celý systém vystavit vzniku nežádoucí ztrátové události.

Stejně tak mohou být neplánované změny vedlejším produktem změn plánovaných, pokud nejsou dopředu řádně promyšleny veškeré dopady plánovaných změn. V takovém případě se může jednat o změnu určité části systému, při jejíž návrhu a následném zavedení do provozu nebyl uvážen veškerý vliv na ostatní části tohoto systému. Ve většině případů jsou neplánované změny změnami negativními, které s sebou vnáší do systému bezpečnostní problémy. Prvotním problémem je samotný vznik příslušné neplánované změny. Je proto velmi důležité mít stanoven postup pro identifikaci neplánovaných změn, pro který bude zásadní sběr dat z provozu. Na základě sběru a vyhodnocení dat z provozu mohou být zjištěny určité trendy, které mohou poukazovat na případnou neplánovanou změnu. Následovat by mělo vyhodnocení identifikované neplánované změny s posouzením jejího dopadu na bezpečnost konkrétního systému. Konečným výsledkem by měla být adekvátní reakce na tuto změnu a potenciální zmírnění bezpečnostních rizik. [6] [7]

4 Přístupy pro řízení plánovaných změn

Řízení změn neboli Management of Change (MoC) je proces, který by měl být zaveden pro adekvátní posouzení dané plánované změny z hlediska bezpečnosti. Součástí tohoto procesu by tak měla být především systematická a proaktivní identifikace případných nebezpečí, která mohou být vedlejším produktem změny, a stejně tak stanovení, implementace a následné vyhodnocení opatření pro řízení bezpečnostních rizik. Zároveň by však měla být stejným způsobem znovu posouzena dosavadní nebezpečí a strategie pro řízení rizik, neboť i zde může dojít k ovlivnění při zavádění dané změny. Stejně tak jako v případě řízení jiných procesů i v případě plánovaných změn existují různé přístupy, jak tyto změny adekvátně řídit. [6] [8]

4.1 ICAO Safety Management Manual – The Management of change

Dle ICAO dochází ke změnám v důsledku řady faktorů. Může se jednat například o expanzi dané organizace, změny v interních systémech a procesech či v provozním prostředí organizace, vnější regulační a ekonomické změny apod. S každou změnou může dojít k zavedení nových nebezpečí a souvisejících bezpečnostních rizik do systému a zároveň ke změně stávajících nebezpečí. Proto by mělo být cílem zejména identifikovat nová nebezpečí, posoudit nebezpečí stávající a související bezpečnostní rizika by měla být posouzena a sledována podle zavedeného řízení bezpečnostních rizik konkrétní organizace. [2]

V procesu řízení změn by mělo být vzato v úvahu několik aspektů. Jde například o kritičnost příslušné změny, tedy o to, jakou roli bude hrát změna v rámci celého systému. Dále by mělo být posouzeno, zda má organizace dostatečný počet odborníků, kteří se budou řízením změn zabývat. V neposlední řadě je důležitá dostupnost informací a dat o výkonnosti v bezpečnosti organizace, aby bylo možné zhodnotit současný stav organizace z pohledu bezpečnosti a zároveň využít tyto informace a data pro následnou analýzu změny. Navíc by měla být změna diskutována s ostatními pracovníky, kteří jsou procesu, jehož se změna týká, součástí, stejně tak jako zvážení dopadů, které na ně může změna mít. [2]

Obvyklým problémem bývá, že se v případě malé změny zdá, že její vliv na bezpečnost je téměř zanedbatelný. Ačkoliv tomu tak může v některých případech být, i malé změny mohou znamenat v závěru velké ovlivnění popisu konkrétního systému, a může tak být vyžadována jeho úprava. Vzhledem k tomu, že v některých systémech dochází

k pravidelným či kontinuálním změnám, je vhodné popis systému pravidelně posuzovat, aby byl neustále platný. [2]

Pro proces řízení změny je žádoucí určit, co bude spouštěčem tohoto procesu. Po jeho zahájení by měly následovat níže uvedené činnosti [2]:

- **Pochopení a definování změny**. To zahrnuje popis změny a vysvětlení, proč bude změna zavedena.
- **Porozumění a stanovení, na co a na koho bude mít změna vliv**. Změna může mít vliv nejen na lidi, systémy a procesy uvnitř organizace, ale může ovlivnit také externí organizace. Navíc může dojít k situaci, kde vlivem zaměření se na zmírnění určitých rizik může dojít ke zvýšení rizika v jiných oblastech, kde to nebylo hned zřejmé. Zároveň může vzniknout potřeba revidovat popis konkrétního systému.
- **Provedení identifikace nebezpečí, které souvisí se změnou a posouzení bezpečnostních rizik**. Tento krok má sloužit k identifikaci veškerých nebezpečí, která mohou vzniknout se zavedením změny a spolu s tím má být vyhodnocen dopad změny na dosavadní nebezpečí a související bezpečnostní rizika.
- **Vypracování akčního plánu změny**. V rámci tohoto plánu by mělo být definováno, jaké činnosti se musí splnit, kdo bude za ně odpovědný a jaký je termín pro jejich splnění. Jedná se tak o plán s jasně stanoveným popisem implementace změny, odpovědnostmi za jednotlivé úkony, pořadím a harmonogramem těchto úkonů.
- **Podepsání změny** znamená potvrzení, že zavedení změny je bezpečné. Plán změny by tak měl být podepsán příslušnou osobou, která nese odpovědnost za implementaci změny.
- **Vytvoření plánu zajištění** by mělo zahrnovat stanovení toho, jaké následné činnosti budou potřeba. Především by mělo být zváženo, jakým způsobem bude změna komunikována a jestli budou po jejím zavedení do provozu nutné další aktivity, jako například provedení auditu.

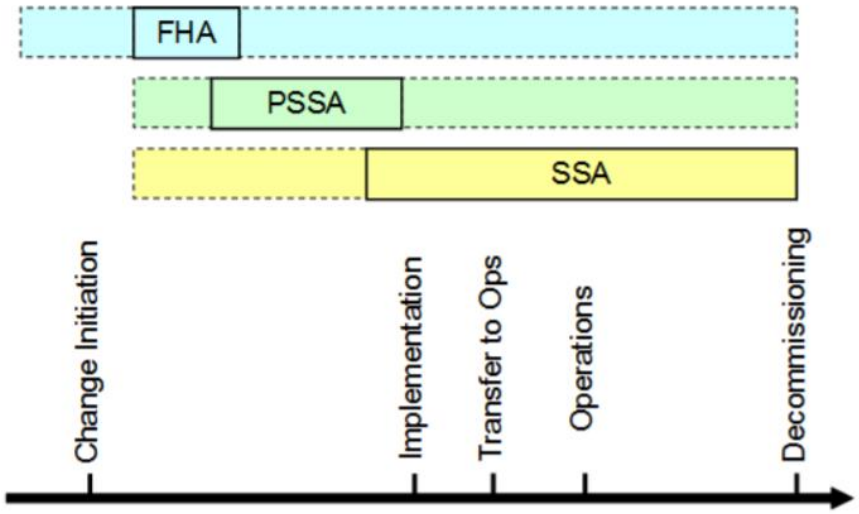
4.2 Safety Assessment Methodology (SAM)

Metodika posouzení bezpečnosti (Safety Assesment Methodology – SAM) byla vyvinuta organizací EUROCONTROL za účelem stanovení procesů pro posouzení bezpečnosti letových navigačních systémů. Zároveň se zaměřuje na určení postupů a technik pro posouzení bezpečnosti změn systémů poskytovatelů letových navigačních služeb. [9] [10] [12]

Proces posouzení bezpečnosti, který je metodikou SAM popsán, zahrnuje 3 hlavní fáze [9]:

- **Functional Hazard Assessment (FHA)** – Posouzení funkčních nebezpečí
- **Preliminary System Safety Assessment (PSSA)** – Předběžné posouzení bezpečnosti systému
- **System Safety Assessment (SSA)** – Posouzení bezpečnosti systému

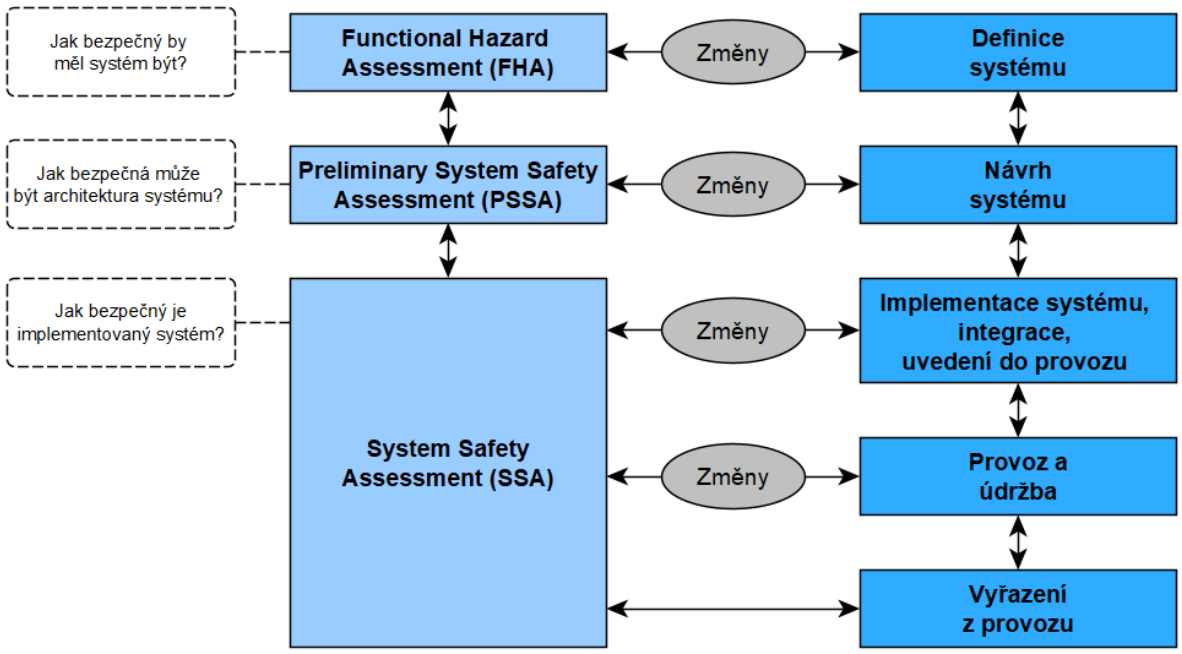
Výše uvedené fáze probíhají zhruba podle časové osy, jak je zobrazeno na obrázku 3. Avšak nejsou vždy nutně vykonávány separátně. Obvykle se vzájemně prolínají a dochází i k případům, kdy je potřeba vrátit se z fáze SSA do fáze PSSA, případně až do fáze FHA. V případě posuzování plánovaných změn jsou v prvotním stádiu podstatné zejména fáze FHA a PSSA, které se zaměřují na posouzení změny před tím, než je zavedena do provozu. Fáze SSA je zahájena při implementaci změny do provozu.



Obrázek 3: Časová osa SAM [11]

(Change Initiation – *zahájení změny*, Implementation – *implementace*, Transfer to Ops – *přechod do provozu*, Operations – *provoz*, Decommissioning – *vyřazení z provozu*)

SAM se zaměřuje na 3 typy elementů systému, a to na člověka, zařízení, postupy a jejich vzájemné působení v konkrétním provozním prostředí, ale nezabývá se organizačními a řídícími aspekty souvisejícími s posouzením bezpečnosti. Je provázán s celým životním cyklem daného systému, od počáteční definice a návrhu systému až po konečné vyřazení z provozu. Obrázek 4 znázorňuje vztah mezi jednotlivými fázemi procesu SAM a celkovým životním cyklem systému. [9] [12]



Obrázek 4: Vztah mezi fázemi procesu SAM a životním cyklem systému (upraveno z [9])

4.2.1 Functional Hazard Assessment

Functional Hazard Assessment (FHA) je fáze SAM, jejíž hlavním cílem je určit, jak musí být daný systém bezpečný. Jedná se o proces, který je zahájen na počátku vývoje systému nebo v případě jeho změny. V rámci tohoto procesu jsou identifikována potenciální selhání a nebezpečí a jsou posouzeny jejich možné důsledky na bezpečnost provozu v konkrétním provozním prostředí. Výstupem mají být celkové bezpečnostní cíle systému, které reflektují, jaké úrovně bezpečnosti by měl systém dosáhnout. [9] [12]

FHA – Zahájení

Počátečním úkolem FHA je porozumění danému systému a provoznímu prostředí, ve kterém se nachází, a případně i regulačnímu rámci, aby bylo možné adekvátně provádět činnosti spojené s posouzením bezpečnosti. Ke splnění tohoto úkolu je potřeba shromáždit a analyzovat následující vstupy. [9] [12]

Zásadním vstupem pro zahajovací fázi FHA je popis systému. Součástí tohoto popisu by měla být definice účelu systému, popis fungování systému a prostředí, ve kterém bude provozován, dále určení jednotlivých funkcí systému a jejich vzájemné provázání (například pomocí vývojových či blokových diagramů) a definování hranic systému. Dalším podstatným vstupem je popis provozního prostředí, který má zahrnovat informace o prostředí, do kterého bude daný systém integrován. Dále by neměl chybět regulační rámec obsahující regulační požadavky na systém (mezinárodní i národní)

a platné normy. Využity však mohou být i jiné vstupy, jako například výstupy z FHA a posouzení bezpečnosti pro podobné systémy nebo výsledky FHA, která byla provedena na vyšší funkční úrovni, případně výstupy ze zkoušek a simulací provedených u podobných systémů apod. [9] [12]

Informace ze všech shromážděných vstupů by měly být následně posouzeny a na jejich základě by měly být odvozeny předpoklady o systému. Veškeré zjištěné či odvozené informace tvoří výstup ze zahajovací fáze FHA a budou využity v následujících krocích. [9] [12]

FHA – Plánování

Účelem plánování FHA je stanovení cílů a rozsahu FHA, definování činností, jež budou v rámci FHA provedeny, jejich posloupnost a potřebné zdroje pro jejich vykonání. Součástí této fáze by tak měla být identifikace a specifikace každého kroku FHA a po vytvoření strukturovaného plánu by mělo následovat jeho předložení zúčastněným stranám. [9] [12]

FHA – Specifikace bezpečnostních cílů

Na základě předchozích kroků může být vytvořena nejdůležitější část fáze FHA, a to specifikace bezpečnostních cílů. Tento krok zahrnuje identifikaci všech potenciálních nebezpečí, identifikaci dopadů konkrétních nebezpečí na provoz, posouzení závažnosti dopadů nebezpečí a na závěr stanovení bezpečnostních cílů. [9] [12]

V prvním kroku při identifikaci všech případných nebezpečí je nutné zvážit, jak mohou jednotlivé funkce systému selhat a zároveň vzít v potaz, že nebezpečí nevznikají pouze uvnitř daného systému, ale rovněž při interakci s jinými systémy či okolním prostředím. Pro jejich stanovení se tak doporučuje kombinace systematické metody pro identifikaci selhání funkcí systému, dále tzv. „Brainstorming“ metody, která hledá nebezpečí skrze posouzení různých kombinací scénářů událostí, a využití získaných poznatků, analýzy databáze rizik, informace z jiných FHA či zpráv z incidentů a nehod. Po stanovení veškerých nebezpečí je potřeba určit, jaký efekt budou mít na provoz. Není myšlen pouze efekt na systém samotný. V úvahu musí být brán širší kontext, a tak i vliv nebezpečí na systémy, se kterými dochází k interakci. Například v případě letových navigačních systémů by měl být brán v úvahu dopad na poskytování služby řízení letového provozu, na pracovní podmínky řídících letového provozu i posádky, efekt na funkční schopnosti letadla apod. Poté může být určena závažnost zjištěných dopadů nebezpečí. Zde by

mělo být vzato v potaz několik ukazatelů, jako například to, jak dlouhou dobu je daný subjekt vystaven nebezpečí. Závěrečným a hlavním úkolem je specifikování bezpečnostních cílů. Tyto cíle udávají, jaká je maximální frekvence výskytu nebezpečí v závislosti na stanovené závažnosti. [9] [12]

FHA – Hodnocení

Cílem tohoto kroku je prokázání, že proces FHA splňuje své celkové cíle a požadavky. To je provedeno prostřednictvím ověřování, validace a zajištění procesu. Během ověřování je podstatné zjistit, zda stanovené bezpečnostní cíle korespondují s bezpečnostními cíli organizace. Validace má pomoci k ujištění, že celkové výstupy z fáze FHA (bezpečnostní cíle a předpoklady) jsou správné a zároveň úplné. Na závěr by mělo dojít k posouzení, zda veškeré činnosti provedené během FHA byly v souladu s plánem FHA a mělo by být zajištěno, že celkový proces FHA uvedený v tomto plánu je vyhovující a úplný. [9] [12]

FHA – Dokončení

Při dokončení FHA by měly být shromážděny a zaznamenány všechny výsledky vystupující z procesu FHA. Výsledky by následně měly být šířeny mezi všechny zainteresované subjekty. [9] [12]

4.2.2 Preliminary System Safety Assessment

Úkolem fáze Preliminary System Safety Assessment (PSSA) je určit, jak je bezpečná architektura daného systému, tedy jestli se dá předpokládat, že tato architektura systému bude dosahovat bezpečnostních cílů, jež byly specifikovány během fáze FHA. V této fázi dokonce může být zjištěno, že bezpečnostních cílů z FHA dosáhnout nelze, což by vedlo ke změně celého návrhu systému a následně k opětovnému provedení fáze FHA. [9] [12]

PSSA – Zahájení

Součástí prvního kroku PSSA je detailnější pochopení návrhu systému, aktualizace popisu provozního prostředí a pokud je to nutné, tak rovněž identifikace regulačních požadavků a norem, které se týkají daného systému. Vstupy jsou v tomto případě z velké části tvořeny výstupy z předchozí fáze FHA. Jedná se tak především o definici systému, která kromě funkcí systému již zahrnuje předpoklady, nebezpečí a bezpečnostní cíle z FHA, dále návrh systému popisující architekturu systému a jeho omezení, upřesněný popis provozního prostředí, regulační požadavky a platné normy a mimo to mohou být

využity i další podklady, jako například zpráva FHA, zprávy z šetření incidentů a nehod. [9] [12]

Získané informace mohou být následně přezkoumány a zároveň může být provedena aktualizace popisu provozního prostředí systému, neboť popis vytvořený v FHA již nemusí být zcela vyhovující a může být vyžadována jeho úprava či bližší specifikace. [9] [12]

PSSA – Plánování

Obdobně jako u FHA je i v případě PSSA potřeba vytvořit ucelený plán, který reflektuje cíle a rozsah PSSA společně s popisem jednotlivých činností, posloupností jejich provedení a zdroji, které jsou pro jejich vykonání potřebné. Rovněž by měl zahrnovat popis strategie zmírňování rizik a popis metod a technik, které budou v PSSA použity pro hodnocení bezpečnosti. Po schválení vytvořeného plánu PSSA by mělo dojít k jeho distribuci mezi zainteresované subjekty. [9] [12]

PSSA – Specifikace bezpečnostních požadavků

Klíčovým krokem PSSA je odvození bezpečnostních požadavků pro každý prvek systému. Jedná se o proces s jasně stanoveným postupem. [9] [12]

První část tohoto postupu je upřesnění, jak každá dílčí funkce přispívá k dosažení bezpečnostních cílů. K tomu je nejprve potřeba provést rozbor jednotlivých funkcí a postupně je rozkládat na další dílčí funkce nižší úrovně. Členění funkcí se provádí až do doby, kdy jsou všechny jednotlivé funkce přiřazeny k prvkům systému, kterými mohou být lidé, postupy či zařízení. Následně může být stanoveno, jaké dílčí funkce přispívají k dosažení jednotlivých bezpečnostních cílů. Navíc mohou být při členění funkcí zjištěna nová nebezpečí, což vyžaduje aktualizaci seznamu nebezpečí, který byl vytvořen v FHA a spolu s tím i aktualizaci bezpečnostních cílů. [9] [12]

Další částí je vyhodnocení architektury systému z pohledu toho, zda systém přispívá k nebezpečím identifikovaným v FHA. Nebezpečí pak mohou vzniknout v důsledku následujících typů situací [12]:

- Normální provoz systému
- Selhání prvků systému
- Instalace a přechod do provozu

Zde tak může dojít k vytvoření a následnému posouzení potenciálních scénářů, které by mohly vést k nebezpečím. [12]

Třetí částí je aplikace strategie pro zmírňování rizik. Strategie by měla být uplatňována na základě jejího popisu uvedeného v plánu PSSA a jejím cílem je snížit rizika na přijatelnou úroveň. K jejich snížení může dojít třemi způsoby. Jedním je odstranění nebezpečí, které může být provedeno například omezením používání v provozu. Dále se jedná o snížení nebezpečí ve smyslu snížení frekvence, se kterou se může toto nebezpečí vyskytovat. Nakonec může být využita možnost řízení nebezpečí. V tomto případě jde o to, aby systém zajistil, že při výskytu nebezpečí nebudou tato nebezpečí znamenat nepřijatelné riziko. Toho lze dosáhnout například snížením následků nebezpečí. [9] [12]

Následovat by měla část, ve které budou bezpečnostní cíle přiřazeny příslušným bezpečnostním požadavkům ke konkrétním prvkům systému. Přidělování bezpečnostních cílů k bezpečnostním požadavkům by mělo být přizpůsobeno popisu provozního prostředí. [9] [12]

Finální částí je vyvážení bezpečnostních požadavků. Vzhledem k tomu, že v rámci systému může docházet k překrývání jednotlivých bezpečnostních požadavků, je žádoucí postupovat od funkcí na nižší úrovni k funkcím na vyšší úrovni, aby došlo k přizpůsobení požadavkům a zabránění jejich překrývání. [9] [12]

PSSA – Hodnocení

Ve fázi PSSA dochází rovněž při hodnocení k ověření, validaci a zajištění procesu. Cílem ověření je zajištění, že stanovené bezpečnostní požadavky splňují bezpečnostní cíle. Validace posuzuje úplnost výstupů z PSSA a část zajištění procesu se zabývá posouzením souladu procesu PSSA s předem vytvořeným plánem PSSA. [9] [12]

PSSA – Dokončení

V závěru PSSA dochází k seskupení veškerých poznatků a výsledků procesu PSSA a jejich distribuce zúčastněným stranám. [9] [12]

4.2.3 System Safety Assessment

Fáze Systém Safety Assessment je zahájena na začátku implementace systému či změny do provozu a jejím cílem je prokázat, že systém dosahuje přijatelného rizika, že splňuje stanovené bezpečnostní cíle, které byly specifikované ve fázi FHA, a rovněž to, že prvky

systému splňují bezpečnostní požadavky definované v PSSA. Celkově tak proces SSA shromažďuje důkazy o tom, zda jsou tyto aspekty splněny, a to během všech fází životního cyklu systému – implementace a integrace systému, zavedení do provozu, provoz, údržba a vyřazení z provozu. To zahrnuje sledování bezpečnostní výkonnosti systému během jeho provozu. Během procesu SSA může být také zjištěno, že bezpečnostní cíle z FHA nebo bezpečnostní požadavky z PSSA nemohou být dosaženy, a to může vést ke změně návrhu systému či změny a k opětovnému provedení FHA či PSSA. [9] [12]

SSA – Zahájení

Během prvního kroku SSA je účelem zejména získat poznatky o vývoji, implementaci, provozu systému, jeho údržbě, případně o vyřazení systému z provozu, a zjistit tak důvody pro tyto úkony. Podobně jako ve fázi FHA by měl být aktualizován popis provozního prostředí, případně identifikovány regulační požadavky a normy týkající se dané fáze životního cyklu systému. [9] [12]

Požadovanými vstupy pro proces SSA jsou definice a návrh systému zahrnující popis architektury systému a výstupy z předchozích fází FHA a PSSA (předpoklady, bezpečnostní cíle, bezpečnostní požadavky, omezení návrhu), dále upřesněný popis provozního prostředí, regulační požadavky, normy a v neposlední řadě také schéma organizace pro klasifikaci rizika, zpráva FHA a PSSA, zprávy z šetření incidentů a nehod, případně zpětná vazba k předchozí aplikaci SSA. [9] [12]

SSA – Plánování

Podobně jako v předchozích fázích FHA a PSSA je i zde nejprve potřeba stanovit cíle a rozsah SSA, činnosti, harmonogram těchto činností a zdroje, které pro jejich vykonání budou využity. Rovněž by měl zahrnovat bezpečnostní aspekty strategií, které budou použity, dále identifikace metod a technik potřebných pro posouzení bezpečnosti a také popis vzájemných závislostí s fázemi vývoje, implementace, uvedením do provozu, provozu, údržby a vyřazením z provozu. Výstupem by měl být ucelený plán kroků SSA, jež bude distribuován mezi dotčené strany. [9] [12]

SSA – Zajištění bezpečnosti a shromažďování důkazů

Podstatou celé fáze SSA je především ujištění a shromáždění důkazů o tom, zda každý prvek systému (lidé, postupy, zařízení) splňuje určené bezpečnostní požadavky, jestli systém jako celek po celou dobu své provozní životnosti vyhovuje stanoveným

bezpečnostním cílům a jestli dosahuje přijatelného rizika. Postup, jakým toto posuzování a dokazování probíhá, závisí na fázi životního cyklu systému. [9] [12]

Při SSA ve fázi implementace a integrace systému by měly být přehodnoceny výstupy z FHA a PSSA a zároveň by mělo dojít k ověření, že prvky systému splňují bezpečnostní požadavky a že jsou splněny bezpečnostní cíle. V případě fáze přechodu systému do provozu se jedná zejména o hodnocení bezpečnosti tohoto přechodu, dále ověření plnění bezpečnostních cílů a bezpečnostních požadavků i po přechodu systému do provozu a validace systému s ohledem na bezpečnostní očekávání uživatelů. Zároveň by mělo být součástí obou těchto fází ověření přijatelnosti rizika. [9] [12]

Během SSA ve fázích provozu a údržby je stěžejní průběžné shromažďování dat a sledování výkonnosti v bezpečnosti, a to s ohledem na bezpečnostní cíle, bezpečnostní požadavky, předpoklady a přijatelnost rizika. [12]

V případě jakýchkoliv změn, ať už jde o změny systému jako celku či změny jeho prvků, dochází k opakování celkového procesu posouzení bezpečnosti prostřednictvím všech tří fází – FHA, PSSA, SSA. [12]

Ve fázi vyřazení systému z provozu je důležité, aby byl posouzen dopad vyřazení tohoto systému na celkový provoz, do něhož byl systém původně zasazen a plnil zde určitou roli. Zároveň musí být posouzena bezpečnost této fáze. [12]

Finálním výstupem by měly být aktualizované seznamy předpokladů a nově identifikovaných nebezpečí, seznamy bezpečnostních cílů a bezpečnostních požadavků souvisejících s jednotlivými fázemi životního cyklu systému, ujištění a důkazy, že jsou splněny bezpečnostní cíle a přijatelnost rizika. Dále by neměly chybět výsledky a závěry průběžného sběru dat a také výsledky posouzení, že dopad jakékoliv změny je z pohledu bezpečnosti přijatelný. [12]

SSA – Hodnocení

Účelem hodnocení SSA je prokázání, že proces SSA splňuje stanovené cíle a požadavky. Stejně jako ve fázích FHA a PSSA je také u SSA nutné provést ověření, validaci a zajištění procesu. Během ověření by mělo dojít k posouzení, zda proces SSA prokázal, že jsou splněny bezpečnostní požadavky, a to přezkoumáním a analýzou výsledků SSA. Prostřednictvím validace SSA by mělo dojít k zajištění, že výstupy z procesu SSA jsou úplné a vyhovující. Zajištění procesu zahrnuje posouzení souladu činností procesu SSA se stanoveným plánem SSA. [9] [12]

SSA – Dokončení

Finálním krokem je dokončení SSA, během kterého mají být zaznamenány výsledky celého procesu SSA. Poté by měly být tyto výsledky sdíleny se všemi zainteresovanými subjekty. [12]

5 Systémový přístup k bezpečnosti

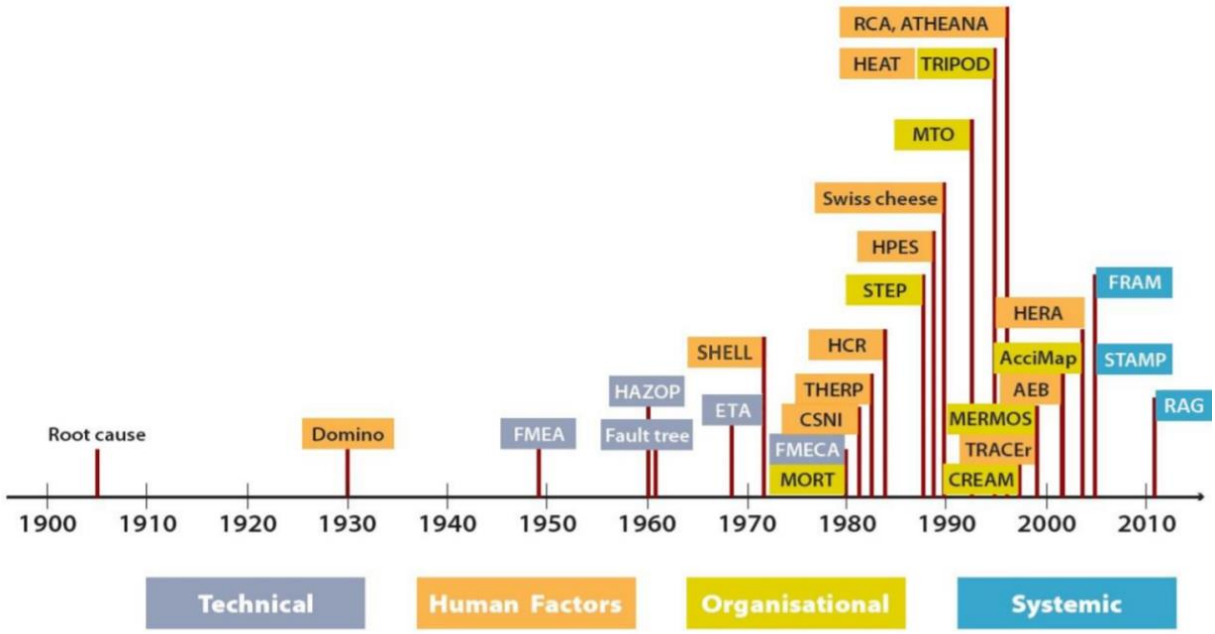
Letectví se v průběhu času vyvíjí a na to musí patřičně reagovat přístupy k bezpečnosti. Zpočátku převažoval technický přístup k bezpečnosti, který se zaměřoval na selhání technických částí systémů, tedy díval se na bezpečnostní nedostatky jako na důsledky nesprávného fungování určitých technických komponentů. Na tomto technickém přístupu jsou založeny například metody FMEA (Failure Mode and Effects Analysis) či FTA (Fault Tree Analysis). Zhruba od 70. let minulého století se však začal brát více v potaz lidský faktor. Pokroky při šetření nehod a incidentů totiž ukázaly, že je důležité se mimo technické stránky systému zabývat také člověkem, který v mnoha systémech figuruje. Začalo se tak více uvažovat nad interakcemi člověka s ostatními prvky systému. V souvislosti s tím začaly vznikat modely a metody bezpečnosti, které se rolí člověka v systému zabývaly. Příkladem může být model SHELL, Reasonův model (Swiss cheese). Třetím přístupem k bezpečnosti je přístup organizační. Zde se začaly brát v úvahu i vyšší úrovně systému, které mají rovněž vliv na konečné výstupy činností lidí a strojů. Rovněž se začal zvažovat dopad organizační kultury a účinnost řízení bezpečnostních rizik. Organizační přístup k bezpečnosti využívá například metoda AcciMap. Poslední a v současnosti patrně nejdiskutovanější je přístup systémový. Tento přístup reaguje na problém, který většina systémů měla, a to sice na to, že se obvykle zaměřovaly individuální výkonnost v bezpečnosti a téměř nebraly v potaz širší kontext celého systému letectví. Systémový přístup tak věnuje pozornost rozhraním mezi zúčastněnými subjekty v letectví, která mohou přispívat ke vzniku nežádoucích událostí. Vývoj metod analýzy nehod a hodnocení rizik vztahujících se ke konkrétním přístupům k bezpečnosti je uveden na obrázku 5. [2]

5.1 Teorie Safety-I, Safety-II a Safety-III

Safety-I, Safety-II a Safety-III jsou teorie bezpečnosti, které se vzájemně v mnoha ohledech liší. Jejich rozdíly tkví především v tom, jak vykládají pojem bezpečnost, jak vysvětlují podstatu vzniku incidentů a nehod nebo jakým způsobem se dívají na roli variability výkonnosti.

S prvním rozdělením na Safety-I a Safety-II přišel profesor Erik Hollnagel, podle jehož názoru Safety-I bere bezpečnost spíše jako absenci nepříznivých událostí. Tedy zvýšení úrovně bezpečnosti znamená snížení počtu nepříznivých výsledků, respektive toho, co měříme a analyzujeme. Tento přístup je tak spíše reaktivní, zaměřuje se na to, jak došlo k případným událostem nebo zda by k nějaké mohlo dojít a prostřednictvím omezení a různých opatření se snaží těmto událostem do budoucna předcházet.

Problémem zároveň je, že cílením na neustálé snižování událostí, ze kterých jsou získávány informace a data, se postupně mohlo dojít pouze k tomu, že by časem nebylo co měřit a analyzovat. Mimo to teorie Safety-I bere flexibilitu a variabilitu systémů jako nežádoucí jev, který je potřeba eliminovat. Oproti tomu Safety-II se snaží vidět bezpečnost skrze pozitivní výsledky v provozu. Jedná se o proaktivní přístup k bezpečnosti, který se neustále snaží předvídat budoucí vývoj a potenciální události. Zároveň ve srovnání s teorií Safety-I, která považuje člověka jako zdroj problému v systémech, Safety-II bere člověka jako nedílnou součást systémů, neboť jsou to právě lidé, kdo zajišťuje flexibilitu a odolnost systémů a tyto dvě vlastnosti jsou podle tohoto přístupu pro správný provoz nezbytné. [14] [15]



Obrázek 5: Vývoj metod analýzy nehod a hodnocení rizik dle přístupů k bezpečnosti [13]

(Technical – *technický*, Human Factors – *lidský faktor*, Organisational – *organizační*, Systemic – *systémový*)

Safety-III je teorie, jež v sobě kombinuje prvky teorií Safety-I a Safety-II, nicméně oproti nim je podle profesorky Nancy Leveson S-III založena na systémovém přístupu. Bezpečnost je podle této teorie osvobození od nežádoucích ztrát a cílem by tak mělo být zejména eliminovat, zmírňovat a řídit nebezpečí, která právě mohou vést k těmto ztrátám. Kromě soustředění se na prevenci vzniku nebezpečí a případných ztrát by měl být kladen důraz také na učení se z nehod, incidentů a zejména z toho, jak daný systém funguje. Nehody a incidenty podle Safety-III vznikají v důsledku neadekvátního řízení nebezpečí a nemá být o nich uvažováno jako o lineární sekvenci událostí. Podstata

vzniku události by měla být hledána už v samotném návrhu systému. Pokud tedy už určitá nežádoucí událost nastala, mělo by být zjištěno, proč bezpečnostní řídicí struktura nezabránila ztrátě. V případě nového systému musí být tento systém navržen tak, aby předcházel vzniku nebezpečí, a tak i případným ztrátám. Zároveň musí být navržen takovým způsobem, aby umožňoval lidem být flexibilní, odolný a aby byli schopni zvládat neočekávané události. [16]

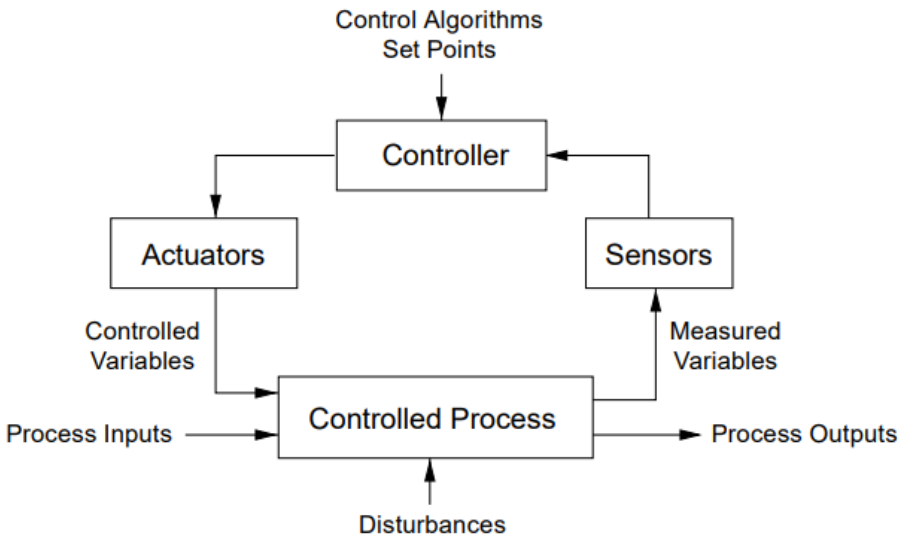
5.2 STAMP

STAMP (System-Theoretic Accident Model and Process) je bezpečnostní model založený na systémové teorii. Podle systémové teorie má být systém považován za celek spíše než jako součet jeho částí a bezpečnost systému jako celku by tak měla být to nejdůležitější. Zároveň systémová teorie uvádí do popředí tzv. emergentní vlastnosti, což jsou vlastnosti celků a vznikají tak ze vztahů mezi částmi systému tím, jak se vzájemně ovlivňují a zapadají do sebe. Emergentními vlastnostmi jsou například safety, security, udržitelnost a provozuschopnost a pro jejich řízení je vyžadováno řízení chování jednotlivých komponent systému a řízení interakcí mezi těmito komponenty. [6] [7]

Na základě modelu STAMP lze sociotechnický systém popsat jako tzv. řídicí strukturu, která je uspořádána do úrovní dle hierarchie systému. Pro každý systém navíc platí, že je charakterizován řízením v rámci jednotlivých úrovní. Dle STAMP dochází k nežádoucím událostem v provozu, pokud řídicí prvek systému nesprávně reaguje na vnější vlivy, poruchy komponentů systému nebo na chybnou interakci mezi komponenty. Proto je důležité, aby byla pro každý systém definována bezpečnostní omezení, jejichž cílem by mělo být zabránění vzniku nežádoucích událostí. Udržení dynamické rovnováhy systému se v řídicí struktuře popisuje pomocí tzv. zpětnovazebních řídicích smyček (Feedback Control Loops). [6] [7]

Na obrázku 6 je zobrazena standardní řídicí smyčka, která se skládá ze čtyřech hlavních prvků – řídicí prvek, řízený proces, aktivní prvky řízení a senzory. Řídicím prvkem je zde myšlen například člověk, nebo počítač. Podstatné je, že tento řídicí prvek řídí konkrétní proces. K provedení takové řídicí činnosti potřebuje řídicí prvek model daného procesu a řídicí algoritmus. Aby získával potřebné informace o stavu procesu, musí zde figurovat senzory, které zaznamenávají naměřené proměnné reflektující tento stav. Následně může být stav procesu řídicím prvkem vyhodnocen, a může tak přejít k řídicí akci. Akční členy zde vnáší do procesu řídicí proměnné, které spustí daný proces. Zároveň platí,

že řízený proces potřebuje příslušné vstupy a následně generuje výstupy. Navíc je jeho průběh ovlivněn okolním rušením. [7]



Obrázek 6: Standardní řídicí smyčka [7]

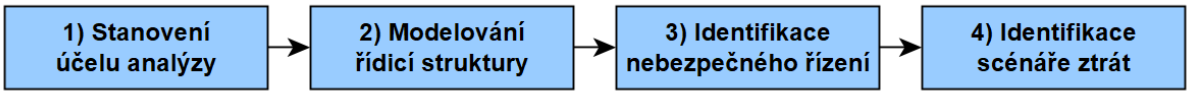
(Controller – *řídicí prvek*, Control Algorithms – *řídicí algoritmy*, Set Points – *nastavené body*, Sensors – *senzory*, Measured Variables – *měřené proměnné*, Controlled Process – *řízený proces*, Process Outputs – *výstupy procesu*, Disturbances – *rušení*, Process Inputs – *vstupy procesu*, Controlled Variables – *řízené proměnné*, Actuators – *akční členy*)

Na základě modelu STAMP byly profesorkou Nancy Leveson definovány metody STPA (System-Theoretic Process Analysis) a CAST (Causal Analysis based on Systems Theory).

5.2.1 STPA

STPA (System-Theoretic Process Analysis) je proaktivní metoda analýzy nebezpečí. Vychází z principů systémové teorie a řízení v rámci systémů. Bere tak v potaz spíše interakce mezi jednotlivými komponenty systému, než aby se zabývala separátně každým prvkem. Vzhledem k tomu, že se jedná o proaktivní metodu, může být využita už při samotném návrhu daného systému, kdy umožňuje definování bezpečnostních požadavků a omezení a mimo to také analýzu potenciálních nebezpečí. Rovněž však může být využita pro již zavedené systémy. Zde může pomoci najít kritická místa v řízení, která by mohla znamenat potenciální problém pro systém a mohla by vést k definovaným nebezpečím či případně až ke ztrátám na úrovni systému. Díky tomu je možné včas zareagovat a tato kritická místa patřičným způsobem řídit, v lepším případě eliminovat tak, aby nedošlo k nežádoucí události (incidentu či nehodě).

Následující obrázek 7 představuje čtyři základní části STPA.



Obrázek 7: Základní části STPA (upraveno z [6])

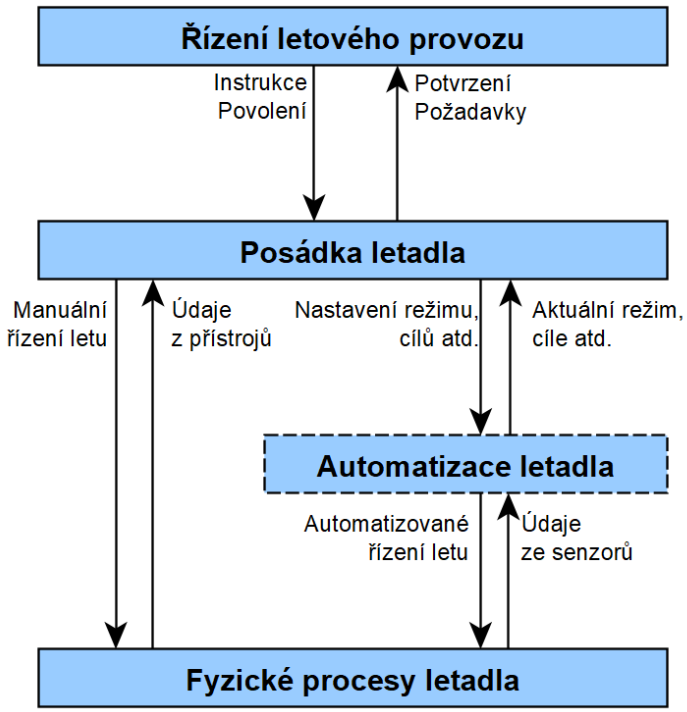
Stanovení účelu analýzy

Podstatou první části STPA je stanovení, k jakému účelu analýza slouží. To především znamená objasnění, jakým ztrátám bude pomocí analýzy předcházeno, a popis analyzovaného systému spolu s definováním jeho hranic. Pro splnění první části STPA jsou stěžejní kroky – identifikace ztrát, identifikace nebezpečí na úrovni systému, identifikace bezpečnostních omezení na úrovni systému a v případě potřeby upřesnění nebezpečí. [6]

Počátečním krokem je identifikace ztrát, které představují stav, jež je nepřijatelný pro daný systém, a měla by být vyvinuta co největší snaha, aby ztrátám bylo zabráněno. Může se jednat o ztrátu lidského života, zranění člověka, únik informací, poškození majetku apod. Vždy záleží na povaze konkrétního systému. Stanovené ztráty dále poslouží pro identifikaci systémových nebezpečí, která jsou s nimi spojena. K tomu je však nejprve nutné definovat daný systém a určit jeho hranice. Pro snadnější vytyčení hranic systému je výhodné si zprvu určit, nad jakými částmi může probíhat řízení. Následně mohou být stanovena příslušná nebezpečí, která popisují stavy a podmínky systému, jež spolu s konkrétním souborem nejhorších podmínek prostředí povedou ke ztrátě. Na základě tohoto kroku mohou být dále definována bezpečnostní omezení na úrovni systému specifikující podmínky či chování, které je třeba splnit, aby se předešlo vzniku nebezpečí, a tím nakonec i ztrátám. V závěru první části STPA je možné upřesnit stanovená nebezpečí, respektive je rozdělit na dílčí nebezpečí. [6]

Modelování řídicí struktury

Druhou částí STPA je vytvoření hierarchické řídicí struktury. Hierarchická řídicí struktura složitých systémů se skládá z několika zpětnovazebních řídicích smyček, které zahrnují komponenty – řídicí prvek, řídicí algoritmus, procesní model, řídicí akce, zpětnou vazbu a řízený proces. [6]



Obrázek 8: Ukázka hierarchické řídicí struktury (upraveno z [6])

Hierarchická řídicí struktura popisuje, jakým způsobem probíhá řízení v rámci systému, které je důležité z hlediska dosažení požadovaných hodnot a cílů systému. Vertikální osa řídicí struktury určuje řízení a autoritu v daném systému a vertikální rozmístění komponentů představuje hierarchii řízení od řídicích prvků nejvyšší úrovně po prvky na nejnižší úrovni. Každý prvek řídí prvky stojící v řídicí struktuře pod ním a zároveň každý prvek podléhá řízení prvků, které stojí bezprostředně nad ním. [6]

Z obrázku 8 je patrné, že například *Automatizace letadla* figuruje v řídicí struktuře jako řídicí prvek ovlivňující *Fyzické procesy letadla* pomocí řídicí akce *Automatizované řízení letu*. Mimo to je ale zároveň *Automatizace letadla* také řízeným procesem, který je řízen skrze řídicí akci *Nastavení režimu, cílů atd.* od *Posádky letadla*, které rovněž posílá zpětnou vazbu ve formě *Aktuálního režimu, cílů atd.*

Identifikace nebezpečného řízení

Cílem třetí části STPA je identifikace potenciálního nebezpečného řízení (Unsafe Control Action – UCA). Jedná se o řízení, které v určitém kontextu a nejhorších podmínkách prostředí může vést ke vzniku nebezpečí. Řízení může být nebezpečné čtyřmi způsoby [6]:

- Neprovedení řízení povede k nebezpečí.
- Provedení řízení povede k nebezpečí (nesprávné provedení řízení).

- Řízení bylo provedeno, ale příliš brzo, příliš pozdě nebo v nesprávném pořadí.
- Řízení trvalo příliš dlouho nebo příliš krátce.

Při identifikaci nebezpečných řízení je zároveň důležité stanovit kontext neboli podmínky, za jakých je konkrétní řízení považováno za nebezpečné. To může být využito zejména při návrhu systému, kdy mohou být tyto případy eliminovány. Navíc by měl být u každého nebezpečného řízení uveden odkaz na konkrétní nebezpečí, ke kterému se nebezpečné řízení váže. Jakmile jsou nebezpečná řízení identifikována, je možné na jejich základě formulovat bezpečnostní omezení řídicího prvku, která je třeba splnit, aby se nebezpečným řízením dalo vyvarovat. [6]

Identifikace scénáře ztrát

Finálním krokem je stanovení scénářů ztrát. Tyto scénáře popisují příčinné faktory, které mohou vést ke vzniku nebezpečného řízení a následně k nebezpečím. Zde je důležité zaměřit se zejména na to, zda je nebezpečné řízení způsobené nebezpečným chováním řídicího prvku, nebo nedostatečnou zpětnou vazbou či jinými vstupy. Aby bylo možné tento krok provést, je dobré si nejprve řídicí strukturu doplnit o senzory a aktivní prvky řízení. Zpětná vazba totiž musí být určitým způsobem měřena či detekována, aby mohla řídicímu prvku předávat informace o stavu procesu, k čemuž slouží senzory. Oproti tomu řídicí akce musí být něčím zprostředkovány, aby ovlivnily řízený proces, což pomohou zajistit právě aktivní prvky řízení. [6]

5.2.2 Proaktivní indikátory založené na předpokladech

Proaktivní indikátory se využívají k identifikaci potenciálu nehody dříve, než k ní dojde, aby bylo možné přijmout adekvátní opatření k jejímu zabránění. Profesorka Nancy Leveson navrhuje vytvoření proaktivních indikátorů, které budou založené na předpokladech (assumption-based leading indicators). Jedná se o varovné signály, jež je možné použít při monitorování daného procesu ke zjištění, kdy je konkrétní předpoklad porušen, oslaben nebo kdy se mění platnost tohoto předpokladu. Dle této myšlenky jsou předpoklady o chování daného systému základem už při samotném návrhu systému. Může se jednat o předpoklady související se způsobem používání a fungování systému, předpoklady o poruchovosti některých komponentů systému v průběhu času apod. Jako příklad může být uveden protisrážkový systém TCAS (Traffic Alert and Collision Avoidance System). Jedním z předpokladů o prostředí, ve kterém může TCAS adekvátně fungovat, je to, že letadlo vybavené systémem TCAS je zároveň

vybaveno odpovídačem módu S. Dalším příkladem může být předpoklad, že všechna letadla mají funkční odpovídače. [6] [17]

Ke stanovení proaktivních indikátorů založených na předpokladech lze využít STPA. Cílem je využít řídicí strukturu společně s řídicími prvky k identifikaci předpokladů o daném systému a následně k vytvoření odpovídajících proaktivních indikátorů. V provozu systému je následně důležité, aby byla vyvinuta snaha o zachování předpokladů, k čemuž by měly být stanoveny tzv. formovací akce (shaping actions). Formovací akce mají ve struktuře systému za úkol udržovat platnost předpokladů. Příkladem formovacích akcí u různých typů systémů může být použití vysoušedel, aby se zabránilo korozi, nebo navrhování lidských činností tak, aby bylo jejich provedení snadné, ale zároveň aby bylo těžké je opomenout. Kromě formovacích akcí by měly být určeny také tzv. zajišťovací akce (hedging actions), jejichž podstatou je příprava na možnost, že dojde k selhání předpokladu, a proto přijmou odpovídající opatření. Jako příklad může být uvedena konstrukce bezpečná při poruše (fail-safe), která předvídá, že v určitých případech mohou být formovací akce neúspěšné v prevenci porušení předpokladů. Důležité je také zmínit, že není žádoucí ani proveditelné, aby byly předpoklady prostřednictvím proaktivních indikátorů kontrolovány nepřetržitě. K porušení některých předpokladů dochází pouze v případě konkrétních změn v systému či jeho prostředí. Proto je vhodné stanovit body v čase či konkrétní budoucí události (tzv. signposts), které spustí kontrolu platnosti předpokladů. Obvykle se jedná o různé změny, jako například změny ve vzdušném prostoru (zvýšená hustota provozu, snížení rozstupů apod.), které mohou být stanoveny pro již zmíněný TCAS. V rámci provozu systému mohou být předpoklady kontrolovány skrze audity, průzkumy či automaticky shromažďovaná data. [6]

Ačkoliv by měly být proaktivní indikátory založené na předpokladech stanoveny již v návrhu daného systému, dá se očekávat, že během životního cyklu systému může docházet ke změnám, během kterých může být zjištěno, že některé dříve stanovené předpoklady již pozbyly platnosti, zároveň mohou vznikat předpoklady nové a s tím je spjata i změna souvisejících proaktivních indikátorů. Proto by mělo v rámci řízení rizik docházet k přehodnocování proaktivních indikátorů, aby byly stále aktuální vzhledem ke stavu daného systému. [6]

5.2.3 Active STPA

Active STPA je proces využívající provozní data ke kontrole proaktivních indikátorů založených na předpokladech. Slouží k neustálé aktualizaci stávající STPA, aby byla

aktuální vzhledem k současnému stavu systému, a to na základě identifikace proaktivních indikátorů zvyšujícího se rizika pomocí zpětné vazby z provozu (sledování dat, analýzy incidentů a nehod, Management of Change apod.) po celou dobu životnosti systému. [17]

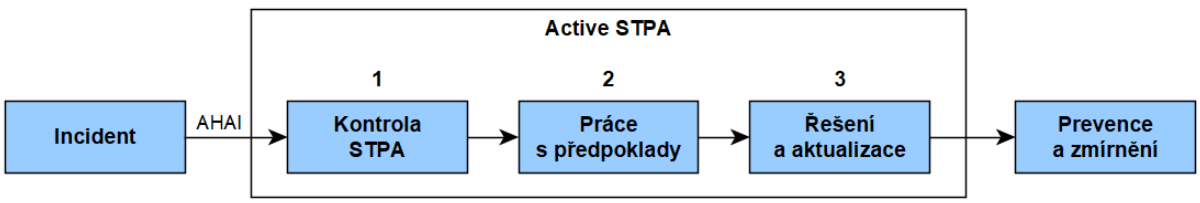
Aby mohla daná organizace využívat Active STPA, musí [17]:

1. Vytvořit STPA nebo použít již existující STPA
2. Implementovat řízení doporučené STPA
3. Shromažďovat provozní data
4. Provést Active STPA

Active STPA začíná analýzou vstupní zprávy, například dobrovolného hlášení, aby bylo zjištěno, zda byla analýza nebezpečí neúplná nebo jsou postupy v praxi neúčinné. Ať už se však jedná o kterýkoliv z těchto dvou případů, je potřeba metoda ke stanovení akcí, které jsou nezbytné pro to, aby se v budoucnu podobným situacím předešlo. Popis incidentu se stane zprávou pro bezpečnostního analytika, která se zde nazývá vstup aktivní analýzy nebezpečí – AHAI (Active Hazard Analysis Input). Tento vstup používá k popisu dané události specifický formát, který začíná popisem kontextu, jenž je následován popisem veškerých řídicích akcí každého řídicího prvku. Účelem je, aby popis incidentu vysvětloval všechny akce nebo absence akcí v chronologickém pořadí. [17]

Proces Active STPA je rozdělen do tří fází (kontrola STPA, práce s předpoklady, řešení a aktualizace), které jsou názorně zobrazeny na obrázku 9. První fáze hledá neúčinné postupy a kontroluje STPA, aby identifikovala nesprávné nebo chybějící části analýzy nebezpečí. Druhá fáze se týká zejména předpokladů, které byly při provozních incidentech porušeny. Třetí fáze pomáhá řídit rozhodovací proces, který se týká identifikace optimálních řešení pro obranu systému, jejich implementace a aktualizace STPA. [17]

Výstupem Active STPA je soubor nových opatření pro prevenci a zmírnění, která budou prosazovat požadavky a omezení generovaná STPA. [17]



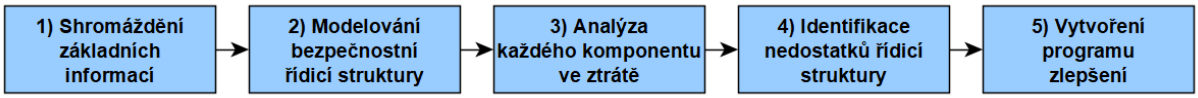
Obrázek 9: Fáze Active STPA (upraveno z [17])

5.2.4 CAST

CAST (Causal Analysis based on Systems Theory) je metoda retrospektivní analýzy příčiny nehod či incidentů. Dosavadní přístupy k šetření incidentů a nehod byly zaměřeny zejména na výsledný popis události a stanovení příčiny vzniku události. Často tak docházelo ke stanovení jednoho viníka, čímž byla událost uzavřena. CAST má oproti tomuto přístupu za cíl prozkoumat návrh daného systému, pochopit způsob jeho fungování, identifikovat jeho nedostatky a v konečné fázi navrhnout opatření, která by do budoucna eliminovaly výskyt takových událostí. Zásadní tedy podle CAST je zahrnout v závěrečných zprávách o nehodách systémové faktory, aby bylo do budoucna nedocházelo k nežádoucím ztrátám. [18]

Důležité je také to, že CAST není využitelný pouze v případech, kdy dojde k incidentu či nehodě. Může být použit pro pochopení jakékoliv nepříznivé události, která může vést ke ztrátě. [18]

Obrázek 10 představuje pět základních částí CAST.



Obrázek 10: Základní části CAST (upraveno z [18])

Shromáždění základních informací

Úkolem první části CAST je především seskupení veškerých informací o události a stanovení účelu analýzy. Základem je tedy definování systému, kterého se analýza týká, respektive vytyčení hranic tohoto systému. Následovat by měl popis ztráty a rovněž identifikace nebezpečí, která ke vzniku této ztráty vedla. Z nebezpečí mohou být stanovena bezpečnostní omezení na úrovni systému, která jsou nutná pro zabránění vzniku nebezpečí. V dalším kroku by mělo být popsáno, co se stalo (události), a to bez vyvozování závěrů a případného obviňování. Z toho mohou být následně vytvořeny otázky, na které je potřeba odpovědět, aby bylo vysvětleno, proč k událostem došlo. V závěru první části by měly být analyzovány fyzické ztráty z hlediska vybavení a ovládání, požadavky na fyzický návrh sloužící pro vyvarování se nebezpečí, fyzické řídicí prvky zahrnuté v návrhu, aby se předešlo tomuto typu nehody, selhání a nebezpečné interakce vedoucí k nebezpečí, chybějící nebo nepřiměřené fyzické řízení a jakékoliv další faktory, které událost ovlivnily. [18]

Modelování bezpečnostní řídicí struktury

Druhou částí CAST je vytvoření řídicí struktury pomocí zpětnovazebních řídicích smyček. Vytvoření řídicí struktury by obecně mělo pomoci pochopit, proč nebylo řízení v systému účinné. Zde je možnost, že je řídicí struktura pro daný systém již vytvořena (v rámci STPA). Pokud tomu tak není, doporučuje se nejprve začít na vyšší úrovni s abstraktní řídicí strukturou a poté ji upřesnit a identifikovat řízení. [18]

Analýza každého komponentu ve ztrátě

Podstatou třetí části CAST je prozkoumání komponentů řídicí struktury, aby mohlo být zjištěno, proč nebylo zabráněno ztrátě. Začít by se mělo ve spodní části řídicí struktury specifikací role, kterou každý řídicí prvek sehrál při nehodě. Dále by mělo být vysvětleno jeho chování – proč řídicí prvek udělal to, co udělal, proč to v tu chvíli vyhodnotil jako správnou věc apod. [18]

Identifikace nedostatků řídicí struktury

Ve čtvrté části CAST je hlavním cílem identifikace nedostatků v řídicí struktuře jako celku skrze prozkoumání obecných systémových faktorů, které přispěly ke ztrátě. Předchozí krok se zaměřoval na jednotlivé komponenty systému a jejich řízení nad ostatními komponenty. Jednalo se především o zkoumání toho, proč každý z řídicích prvků nebyl schopen prosadit řízení a omezení, která mu byla přidělena. Oproti tomu tato část se zabývá řídicí strukturou jako celkem a dále systémovými faktory, které vedly k neúčinnosti navrženého řízení, neboť ovlivňují chování a interakce všech komponentů řídicí struktury. V úvahu lze v tomto kroku vzít například následující faktory. [18]

- Komunikace a koordinace
- Bezpečnostní informační systém
- Kultura bezpečnosti (Safety culture)
- Návrh systému řízení bezpečnosti (SMS)
- Změny a dynamika v čase
- Vnitřní a vnější ekonomické a související faktory v prostředí systému

Vytvoření programu zlepšení

Cílem poslední části CAST je vytvoření doporučení pro změny v řídicí struktuře, které by měly zabránit dalším podobným ztrátám do budoucna. A pokud je to vhodné, je žádoucí vytvořit program neustálého zlepšování daného nebezpečí jako součást programu řízení rizik. Při vytváření doporučení je rovněž podstatné určit postup jejich implementace.

Všechna pravděpodobně nebudou zavedena okamžitě, tudíž by mělo být na základě stanovených priorit definováno, která doporučení budou implementována přednostně. [18]

6 Současný přístup ÚCL k řízení plánovaných změn

ÚCL má jako přední dozorový orgán pod svou správou rovněž procesy související se schvalováním příslušných plánovaných změn subjektů civilního letectví. Každé oddělení ÚCL řeší schvalování změn podle svých kompetencí v daném spektru subjektů civilního letectví a mají v rámci svých směrnic tyto postupy vždy alespoň částečně přiblíženy. Obecně se dá konstatovat, že vždy záleží na povaze konkrétní změny. Některé z dokumentů hovoří o rozdílu mezi změnami, které mohou být ÚCL pouze oznámeny a které vyžadují podrobné posouzení a následné schválení ze strany ÚCL. Rovněž u těchto změn, které vyžadují předchozí souhlas ÚCL, jsou rozdíly především v tom, o jak zásadní změnu se v rámci daného systému jedná. S tím jsou následně spjaty požadavky, které musí splnit daný subjekt, ale také ÚCL. V případě menších změn ze strany konkrétního subjektu zpravidla vystačí bezpečnostní posouzení ve formě identifikace nebezpečí, analýzy a hodnocení rizik a případně stanovení nápravných opatření. V případě složitějších změn je obvykle využíváno bezpečnostní posouzení ve formě studie bezpečnosti (safety study). Ze strany ÚCL se jedná především o posouzení veškerých skutečností, které s danou změnou souvisí, a to zejména se zaměřením na přezkum bezpečnostního posouzení změny a shodu s legislativními požadavky. Zároveň však může ÚCL provést audit, který bude omezený na rozsah příslušné změny.

V následujících podkapitolách budou přiblíženy některé postupy pro řízení plánovaných změn, které v současné době ÚCL uplatňuje. Prvním z nich je proces zavádění změn na letištích certifikovaných podle EASA, druhým je pak dohled nad řízením změn u poskytovatelů služeb.

6.1 Zavádění změn na letištích certifikovaných podle EASA

Celý proces popisující zavádění změn na letištích certifikovaných podle EASA je uveden ve směrnici CAA/S-SP-005-0/2017: Směrnice pro zavádění změn na letištích certifikovaných podle EASA. Hlavním účelem tohoto dokumentu je poskytování vedení v procesu vyrozumění ÚCL o změnách na letištích provozovatelům letišť, certifikovaných dle nařízení Komise (EU) č.139/2014, aby tak byla zajištěna trvalá způsobilost letiště k provádění bezpečného provozu v souladu s platnými požadavky a spolu s tím, aby byla sledována trvalá shoda s certifikační předpisovou základnou. [19]

Základní proces je zobrazen na obrázku 11, který byl vytvořen ve formě diagramu s využitím standardu BPMN. Z tohoto diagramu je patrné, že celý proces je započat

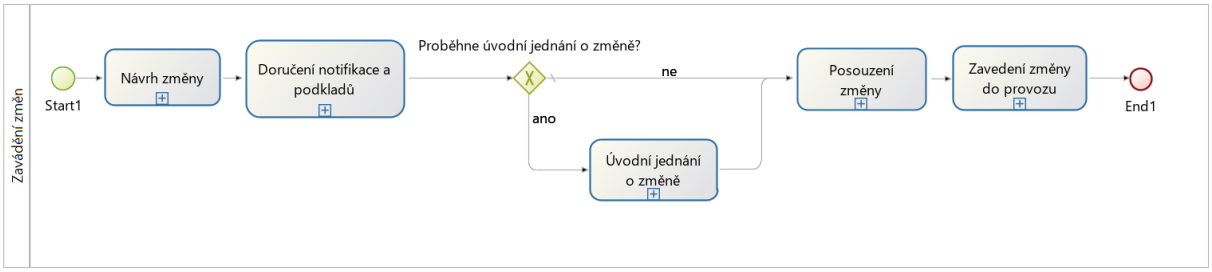
Návrhem změny od provozovatele. Zde se po provozovateli požaduje, aby důsledně zvážil veškeré dopady uvažované změny na provoz. Klíčovým krokem celého procesu je odhad všech potenciálních nebezpečí spojených s danou změnou a provedení bezpečnostní analýzy, jež bude přiblížena v následující podkapitole. Mimo to musí provozovatel v případě dopadu změny na postupy třetích stran koordinovat postup s těmito účastníky dle příslušných smluv a legislativy a zároveň je musí informovat o způsobu zachování bezpečnosti. V návrhu změny musí být provozovatelem zhodnoceno, zda se jedná o změnu vyžadující/nevyžadující předchozí souhlas ÚCL. Nicméně jedná se pouze o předběžné zhodnocení, které může být následně přehodnoceno pověřeným pracovníkem ÚCL.

Po *Návrhu změny* následuje *Doručení notifikace změny a podkladů*, což zahrnuje zejména vyplnění notifikace dané změny, přiložení příslušné dokumentace a následné podání těchto podkladů na ÚCL fyzicky, nebo elektronickou cestou.

Může být rovněž provedeno *Úvodní jednání o změně*, při němž provozovatel letiště seznámí pracovníky ÚCL s možnými dopady, postupy a dalšími souvislostmi, které změna vyvolá.

Jedním z nejzásadnějších kroků v tomto procesu je *Posouzení změny* ze strany ÚCL. Zde musí dojít k detailnímu posouzení veškeré dokumentace, která byla dodána provozovatelem, včetně zhodnocení významnosti změny – tedy zda se jedná o změnu, jež vyžaduje předchozí souhlas ÚCL, nebo o změnu, která předchozí souhlas ÚCL nevyžaduje a postačí pouze její oznámení. Co je však v celém procesu *Posouzení změny* klíčové, je zhodnocení, zda provozovatel posoudil veškeré možné dopady uvažované změny na bezpečnost provozu. Celý proces *Posouzení změny* je ukončen vydáním potvrzujícího dokumentu – Rozhodnutí o změně v případě změny vyžadující předchozí souhlas a Evidence změny v případě změny nevyžadující předchozí souhlas. Pokud poté vznikne požadavek o doplnění či úpravu dané změny, je nutné, aby tuto skutečnost provozovatel nahlásil ÚCL a je tak vyvolán nový proces posouzení změny.

Završením celého procesu je v případě schválení změny ze strany ÚCL následné *Zavedení změny do provozu*. Jedná se o kritický krok, který vyžaduje pečlivé naplánování ze strany provozovatele. Zároveň je po provozovateli vyžadováno, aby v případě, že dojde k ovlivnění údajů v letištní příručce a certifikační předpisové základně, aktualizoval po zavedení změny do provozu dotčené části příslušných dokumentů a vyměnil si s ÚCL aktualizované verze těchto dokumentů.



Obrázek 11: Základní model procesu Zavádění změn

6.1.1 Bezpečnostní posouzení změny ze strany provozovatele letiště

V rámci posouzení bezpečnosti změny s ohledem na její vliv na provoz se od provozovatele požaduje, aby provedl odhad potenciálních nebezpečí spojených s danou změnou a v návaznosti na to provedl jejich bezpečnostní analýzu. Jedná se o nezbytný krok pro ohodnocení potenciálu nebezpečí a rizik, která konkrétní změna přináší z hlediska provozu, infrastruktury, ale také z hlediska ostatních zúčastněných stran.

Podle dokumentu Přijatelné způsoby průkazu (AMC) a poradenský materiál (GM) k požadavkům na úřady, organizace a provoz pro letiště, na který se směrnice CAA/S-SP-005-0/2017 odkazuje, by mělo mít bezpečnostní posouzení změny následující náležitosti.

„GM1 ADR.OR.B.040(f) Změny

POSOUZENÍ ZMĚN

(a) Bezpečnostní posouzení změny

Bezpečnostní posouzení změny by mělo zahrnovat:

(1) identifikaci rozsahu změny;

(2) identifikaci nebezpečí;

(3) stanovení kritérií bezpečnosti použitelných pro změnu;

(4) analýzu rizik ve vztahu k nepříznivým účinkům nebo zlepšením v oblasti bezpečnosti v souvislosti se změnou;

(5) zhodnocení rizika a, v případě potřeby, snížení rizika, aby změny splňovaly příslušná kritéria bezpečnosti;

(6) ověření, že změna odpovídá rozsahu, jenž byl předmětem posouzení bezpečnosti, a splňuje kritéria bezpečnosti před tím, než je změna zavedena do provozu; a

(7) specifikace požadavků na sledování, které je nezbytné k zajištění toho, že letiště a jeho provoz bude po zavedení změny i nadále splňovat kritéria bezpečnosti.

(b) Rozsah posouzení bezpečnosti

Rozsah posouzení bezpečnosti by měl zahrnovat následující prvky a jejich vzájemné posouzení:

(1) letiště, provoz, vedení, a vyvolané personální změny;

(2) rozhraní a vzájemné vazby mezi měněnými a zbývajícími prvky systému;

(3) rozhraní a vzájemné vazby mezi měněnými prvky a prostředím, v němž je provoz zamýšlen; a

(4) celý životní cyklus změny od jejího záměru po uvedení do provozu;

(c) Kritéria bezpečnosti

Použitá kritéria bezpečnosti by měla být definována v souladu s postupy pro řízení změn, které jsou obsaženy v letištní příručce.

V závislosti na dostupnosti dat by použitá kritéria bezpečnosti měla být specifikována s odkazem na explicitní kvantitativní přijatelné úrovně bezpečnostních rizik, uznávané standardy a/nebo platné předpisy, výkonnost v oblasti bezpečnosti stávajícího nebo podobného systému.“ [20]

Provozovatelům je v této souvislosti pro posouzení bezpečnosti změny k dispozici Formulář bezpečnostního posouzení na webových stránkách ÚCL. V rámci tohoto dokumentu se po provozovateli požaduje vyplnění následujících informací. [21]

- Název změny
- Identifikace rozsahu změny
- Identifikace nebezpečí, analýza rizik, hodnocení rizik
- Kritéria bezpečnosti použitelných pro změnu
- Ověření, že změna odpovídá rozsahu, jenž byl předmětem posouzení bezpečnosti a splňuje kritéria bezpečnosti předtím, než je změna zavedena do provozu

- Specifikace požadavků na sledování, které je nezbytné k zajištění toho, že letiště a jeho provoz bude po zavedení změny i nadále splňovat kritéria bezpečnosti
- Preventivní opatření

Hlavním výstupem bezpečnostního posouzení, který je ve zmíněném dokumentu obsažen, je tabulka, jejíž část je uvedena v tabulce 5. Z ukázky tabulky je patrné, že nejprve je nutné identifikovat případná nebezpečí spojená se změnou, dále související rizika a již zavedená zmírňující opatření. Poté musí být vyhodnocena stávající úroveň rizika dle ICAO matice pro hodnocení rizik (z hlediska závažnosti a pravděpodobnosti), která je uvedena v tabulce 3. Na základě výsledného indexu bezpečnostního rizika je možné určit, zda je riziko považováno ze přijatelné, tolerovatelné, nebo nepřijatelné (tabulka 4) a podle toho mohou být požadována další nápravná opatření, po jejichž stanovení se vyžaduje opětovné posouzení úrovně rizika. [21]

Tabulka 3: ICAO matice bezpečnostních rizik (upraveno z [2])

Bezpečnostní riziko		**Závažnost**				
Pravděpodobnost		Katastrofální	Nebezpečná	Významná	Méně významná	Zanedbatelná
		A	B	C	D	E
Častá	5	5A	5B	5C	5D	5E
Příležitostná	4	4A	4B	4C	4D	4E
Malá	3	3A	3B	3C	3D	3E
Nepravděpodobná	2	2A	2B	2C	2D	2E
Krajně nepravděpodobná	1	1A	1B	1C	1D	1E

Tabulka 4: Snášenlivost bezpečnostního rizika (upraveno z [2])

Rozsah indexu bezpečnostního rizika	**Popis bezpečnostního rizika**	**Doporučená akce**
5A, 5B, 5C, 4A, 4B, 3A	Nepřijatelné	Proveďte okamžitá opatření ke zmírnění rizika nebo pozastavte činnost. Proveďte prioritní zmírnění bezpečnostních rizik, abyste zajistili, že budou zavedeny další nebo vylepšené preventivní kontroly, aby se index bezpečnostních rizik snížil na přijatelnou úroveň.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Tolerovatelné	Lze tolerovat na základě zmírnění bezpečnostních rizik. Může vyžadovat rozhodnutí vedení, aby přijalo riziko.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Přijatelné	Přijatelné tak, jak je. Není nutné žádné další zmírňování bezpečnostních rizik.

Identifikované nebezpečí	Související rizika (následky)	Zavedená zmírňující opatření (současná)	Stávající úroveň rizika	Další zmírňující opatření	Revidovaná úroveň rizika	Opatření zajišťuje: Ke dni:
1.	1. 2.	1. 2. 1. 2.	Závažnost: **A** Pravděpodobnost: **1** □ přijatelné □ tolerovatelné □ nepřijatelné	1. 2. 1. 2.	Závažnost: **A** Pravděpodobnost: **1** □ přijatelné □ tolerovatelné □ nepřijatelné	Jméno a funkce: Dne:

Tabulka 5: Identifikace nebezpečí, analýza a hodnocení rizik (upraveno z [21])

6.1.2 Přezkum bezpečnostního posouzení změny ze strany ÚCL

Jak již bylo zmíněno výše, zásadním bodem celého procesu řízení změn je posouzení změny z hlediska provozní bezpečnosti ze strany ÚCL. Ve směrnici CAA/S-SP-005-0/2017 není blíže specifikováno, jakým způsobem ÚCL postupuje při přezkumu bezpečnostního posouzení změny. Nicméně dokument Přijatelné způsoby průkazu (AMC) a poradenský materiál (GM) k požadavkům na úřady, organizace a provoz pro letiště popisuje kroky, které by měl ÚCL splnit při tomto přezkumu, následovně.

„GM3 ADR.AR.C.035(a) Vydávání osvědčení

VYHODNOCENÍ POSOUZENÍ BEZPEČNOSTI, KTERÁ DODAL PROVOZOVATEL LETIŠTĚ PŘI PRVOTNÍ CERTIFIKACI NEBO KTERÁ PROVÁZÍ ŽÁDOST O PŘEDCHOZÍ SOUHLAS SE ZMĚNOU V SOULADU S ADR.OR.B.040.

(a) Příslušný úřad by měl vyhodnotit závěry doloženého posouzení bezpečnosti poskytnutého provozovatelem letiště za účelem zajištění vyhovění relevantnímu požadavku pro provozovatele o tom, jak posuzovat změny ADR.OR.B.040(f).

(b) Příslušný úřad by měl vyhodnotit posouzení bezpečnosti a zejména se ujistit, že:

(1) identifikované bezpečnostní problémy byly posouzeny prostřednictvím procesu posouzení bezpečnosti a jsou dostatečně zdokumentovány.

(2) došlo k příslušné koordinaci mezi stranami dotčenými bezpečnostním(i) problémem(y);

(3) posouzení zahrnuje celý systém a vzájemné působení jeho součástí;

(4) nebezpečí byla řádně určena a úroveň rizika posouzena;

(5) navržená zmírňující opatření jsou úměrná a konzistentní s cílem snížit identifikovanou úroveň rizika a cíli bezpečnosti, je-li to relevantní;

(6) časový rámec pro plánovanou implementaci navrhovaných souvisejících činností je přiměřený.

(c) Po vyhodnocení by měl příslušný úřad buď:

(1) souhlasit s navrženými souvisejícími činnostmi, jako jsou zmírňující opatření; nebo

(2) koordinovat s provozovatelem letiště na dosažení dohody ohledně revidovaných zmírňujících opatření, pokud byla některá rizika podceněna nebo nebyla identifikována; nebo

(3) zavést dodatečná opatření; nebo

(4) zamítnout návrh, pokud nelze dosáhnout žádné dohody.

(d) Příslušný úřad by měl definovat a podniknout činnosti dozoru, které zajistí, že jsou zmírňující a/nebo dodatečná opatření správně implementována tak, že daná opatření splňují cíle snížení rizika, a že jsou využity plánované časové rámce.

(e) Je-li to nezbytné, měl by příslušný úřad vyžadovat, aby provozovatel letiště uveřejnil příslušné informace pro použití v rámci organizace letiště, různými zainteresovanými osobami a především poskytovateli letových navigačních služeb a provozovateli letadel.“ [20]

6.2 Dohled nad řízením změn u poskytovatelů služeb

Proces dohledu nad řízením změn u poskytovatelů služeb je popsán ve směrnici CAA/S-SP-009-3/2019: Dohled nad řízením změn u poskytovatelů služeb a u organizací pro výcvik řídících letového provozu. Konkrétně se jedná o proces týkající se změn funkčních systémů poskytovatelů služeb a je započat oznámením změny ze strany poskytovatele služeb dle příslušných náležitostí. Mimo to musí uvážit, na které další subjekty (poskytovatele služeb, letecké organizace) může mít změna dopad a musí je o této skutečnosti patřičně informovat. ÚCL po obdržení dokumentace od poskytovatele služeb provede její prvotní posouzení za účelem rozhodnutí, zda bude proveden přezkum argumentů změny spojených s novým funkčním systémem nebo se změnou stávajícího funkčního systému. Pro rozhodování o přezkumu argumentů změny jsou zároveň použita kritéria zahrnující kombinaci pravděpodobnosti, zda je argument pro poskytovatele služeb složitý nebo neznámý, a závažnosti možných důsledků změny. Pokud je rozhodnuto, že změna podléhá přezkumu ze strany ÚCL, podá poskytovatel služeb na ÚCL žádost o přezkum platnosti argumentu oznámené změny a o jeho schválení společně s následující dokumentací. [22]

„1. Identifikace poskytovatele, včetně kontaktní osoby.

2. Identifikace změny.

3. Identifikace dotčené předpisové základny.

4. Identifikace dotčených postupů a směrnic poskytovatele.

5. Dokumentované posouzení podpory bezpečnosti a zajištění změn funkčního systému dle ustanovení ATM/ANS.OR.C.005 prováděcího nařízení Komise (EU) 2017/373 ve formě **STUDIE NA PODPORU BEZPEČNOSTI**, vypracované a předkládané poskytovateli jiných než letových provozních služeb (NON-ATS), které zahrnuje minimálně:

A. Posouzení podpory bezpečnosti,

B. Úplný, dokumentovaný a platný argument změny, zahrnující:

(1) přesný popis rozsahu změny

(2) specifikaci služby a její změny

(3) provozní kontext změny

(4) ověřování

(5) Specifikaci kritérií pro monitorování

6. Dokumentované posouzení bezpečnosti a zajištění změn funkčního systému dle ustanovení ATS.OR.205 nařízení EU 2017/373 ve formě **STUDIE BEZPEČNOSTI**, vypracované a předkládané poskytovateli letových provozních služeb (ATS), které zahrnuje minimálně:

A. Posouzení bezpečnosti,

B. Úplný, dokumentovaný a platný argument změny, zahrnující:

(1) úplnou identifikaci nebezpečí a rizik

(2) stanovení a zdůvodnění konkrétních a ověřitelných bezpečnostních kritérií

(3) analýzu rizik účinků souvisejících se změnou

(4) hodnocení rizik a v případě, že je požadováno, opatření ke zmírnění rizik pro danou změnu

(5) ověření

(6) identifikovaná a zdokumentovaná monitorovací kritéria

V souladu s čl. ATS.OR.210 poskytovatel letových provozních služeb zaručuje, že jsou stanovena pro danou změnu bezpečnostní kritéria. Je

požadováno, aby splnění požadavků ATS.OR.210 bylo v předkládané dokumentaci explicitně doloženo a dokumentováno.

Pokud je změna funkčního systému implementována poskytovatelem služeb, který poskytuje i jiné služby současně s poskytováním letových provozních služeb, musí být v případě, že změna zahrnuje změnu ve funkčních systémech poskytujících tyto služby, zajištěno, aby Studie bezpečnosti splňovala požadavky kladené na poskytovatele jiných než letových provozních služeb s ohledem na zpracování Studie na podporu bezpečnosti. Tento požadavek může být splněn například doplněním Studie bezpečnosti o specifikaci služby, doplněním kontextu služby apod., či připojením Studie na podporu bezpečnosti. Způsob, jak je tento soulad splněn, definuje poskytovatel ve svých postupech.

7. Případná identifikace potřeby změn do leteckých předpisů nebo potřeby nových standardů.

8. Doklad o definici a zajištění SW bezpečnosti, pokud se dotčená změna týká změny SW.

9. Doklady o zajištění proškolení provozního a technického personálu k provoznímu využití dotčené změny v rámci poskytovaných služeb, včetně bezpečnostního posouzení dle ATCO.D.085 (Přeškolovací výcvik), pokud je toto pro konkrétní změnu relevantní.

10. Vyjádření odpovědného pracovníka provozovatele k provoznímu zavedení změny, pokud není již obsahem výše uvedených dokumentů.

11. Přechodový plán k zavedení změny, pokud není již obsahem výše uvedených dokumentů.

12. Směrnice poskytovatele služeb pro dotčená pracoviště.

13. Odkaz na platné Prohlášení ES o ověření systému, včetně Souboru technické dokumentace (obsahující mimo jiné DSU/DoC) ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2018/1139, pokud je aplikovatelné.

14. Ostatní dokumentace předkládaná ve smyslu souvisejících postupů ÚCL (jen v případě, že je současné podávána žádost ve smyslu těchto souvisejících postupů).

15. Důkazy o splnění konkrétních požadavků bezpečnosti, uváděných v souvisejících nařízeních EU, DSU nebo DoV, pokud jejich plnění není zahrnuto v dokumentu deklarujícím bezpečnostní posouzení změny, dle platných zásad předkladatele.“ [22]

Po získání všech potřebných dokumentů souvisejících se změnou, musí ÚCL určit hodnotitele, který musí mimo jiné zkontrolovat úplnost předložené dokumentace a přezkoumat studii bezpečnosti/studii na podporu bezpečnosti a ostatní předloženou dokumentaci. [22]

Během přezkumu studie bezpečnosti/studie na podporu bezpečnosti musí hodnotitel posoudit, zda studie prokazuje, že lze zavedení změny realizovat s akceptovatelným rizikem, respektive zda bude bezpečné. Jedná se o nejdelší fázi procesu přezkumu argumentu změny. Zároveň jsou zde žádoucí případné konzultace hodnotitele s ostatními specialisty, které mohou pomoci při následném rozhodnutí, zda lze změnu schválit, či nikoliv. [22]

Postupy pro přezkoumání studie na podporu bezpečnosti a studie bezpečnosti jsou následující.

„Při přezkoumávání **studie na podporu bezpečnosti** (AMC1 ATM/ANS.OR.C.005(a)(2)) používá hodnotitel tzv. „Checklist" obsahující kontrolní otázky pro posouzení následujících oblastí a přijatelnosti argumentu:

1) Rozsah změny

2) Úplnost argumentu

3) Stanovení specifikace změněné služby

4) Stanovení provozního kontextu změny

5) Ověření

6) Monitoring

7) Soustavné dodržování předpisů

Při přezkoumávání **studie bezpečnosti** používá hodnotitel tzv. „Checklist" obsahující kontrolní otázky pro posouzení následujících oblastí a přijatelnosti argumentu:

1) Rozsah změny

2) Úplnost argumentu

3) Úplnost identifikace nebezpečí a rizik

4) Určení bezpečnostních kritérií použitelných pro změnu

5) Úplnost analýzy rizik účinků souvisejících se změnou

6) Hodnocení a zmírňování rizik

7) Ověření

8) Monitorování změny zavedené změny

9) Soustavné dodržování předpisů – provádí se rámcové posouzení s cílem zjištění, zda je nezbytné ověřit soustavné dodržování předpisů poskytovatelem služeb.“ [22]

Na základě provedeného přezkumu argumentu změny vypracuje hodnotitel závěrečnou zprávu, na jejímž základě je následně vypracováno Rozhodnutí ÚCL o schválení/neschválení argumentu změny funkčního systému. Schválené a zavedené změny mohou být dále prověřovány v rámci auditů prováděných inspektory ÚCL. Cílem jejich provedení je zejména dohled nad plněním dalších podmínek provozní bezpečnosti souvisejících se zaváděním změn funkčních systémů, které byly stanoveny ÚCL ve výrokové části rozhodnutí a dohled nad monitorováním zavedené změny. [22]

6.3 Zhodnocení současného přístupu ÚCL k řízení plánovaných změn

V předchozích podkapitolách byly krátce přiblíženy ukázky současných postupů ÚCL pro řízení plánovaných změn. Ačkoliv ÚCL má těchto postupů popsáno více v závislosti na subjektu civilního letectví, kterého se změna týká, obvykle se o řízení změn píše podrobněji pouze to, jaká dokumentace a jaké kroky se vyžadují od daného subjektu a že dodaná dokumentace bude následně příslušným zaměstnancem posouzena. Bohužel se zde často vytrácí detail toho, jakým způsobem je tato dokumentace následně přezkoumána z hlediska bezpečnosti. Směrnice týkající se dohledu nad řízením změn u poskytovatelů služeb alespoň popisuje, na co se má hodnotitel zaměřit při přezkumu studie bezpečnosti/studie na podporu bezpečnosti, nicméně směrnice pro zavádění změn na letištích certifikovaných podle EASA postrádá postup, jak příslušný pracovník provádí přezkum bezpečnostního posouzení změny. Ačkoliv byly příslušné kroky pro přezkum dohledány v odpovídajícím dokumentu AMC a GM, bylo by žádoucí, aby byl postup přímo specifikován v dané směrnici, neboť bez těchto informací působí postup neuceleně.

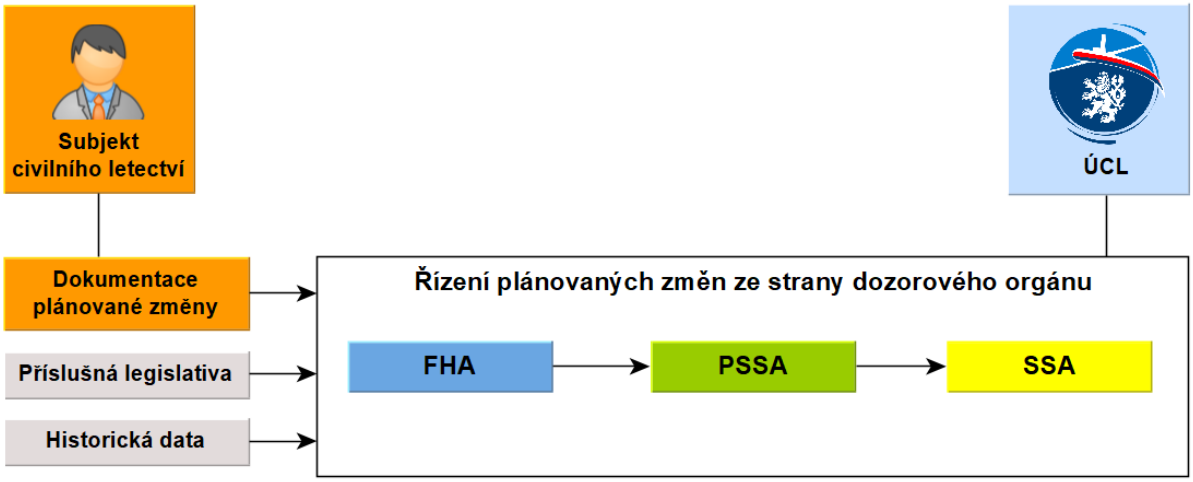
Navíc se při srovnání několika postupů pro řízení změn jeví tyto postupy už v základní rovině poněkud rozdílně. Může to být z důvodu nejednotné formy zpracování směrnic.

Ačkoliv se postupy pro řízení změn vždy specifikují podle subjektu, jehož se týkají, dá se předpokládat, že alespoň základní kroky postupů řízení změn budou v rámci celého ÚCL téměř totožné a rozdíly budou pouze v požadavcích na některou dokumentaci. Nicméně to, co je při řízení změn klíčové (přezkum bezpečnostního posouzení změny), by mělo být sjednoceno.

Zároveň ÚCL v současnosti neuplatňuje systémový přístup k bezpečnosti, který přináší výhody především ve využití podrobných systémových analýz (STPA, Active STPA, CAST).

7 Postup pro řízení plánovaných změn s využitím systémového přístupu k bezpečnosti

Základem pro navržený postup pro řízení plánovaných změn s využitím systémového přístupu k bezpečnosti je kombinace metodiky SAM spolu s metodami STPA a Active STPA. SAM dodává postupu jasně danou strukturu, neboť dělí posouzení bezpečnosti změny do 3 základních fází, z nichž každá má své jasně dané vstupy, procesní kroky a také výstupy. STPA a Active STPA vnášejí do postupu systémový přístup k bezpečnosti a určují tak způsob provedení jednotlivých kroků v rámci SAM. V následujících podkapitolách je přiblížen návrh postupu pro řízení plánovaných změn, který je rozdělen na 3 základní fáze dle metodiky SAM – FHA, PSSA, SSA. Ukázka základní roviny procesu řízení plánovaných změn ze strany dozorového orgánu je uvedena na obrázku 12.

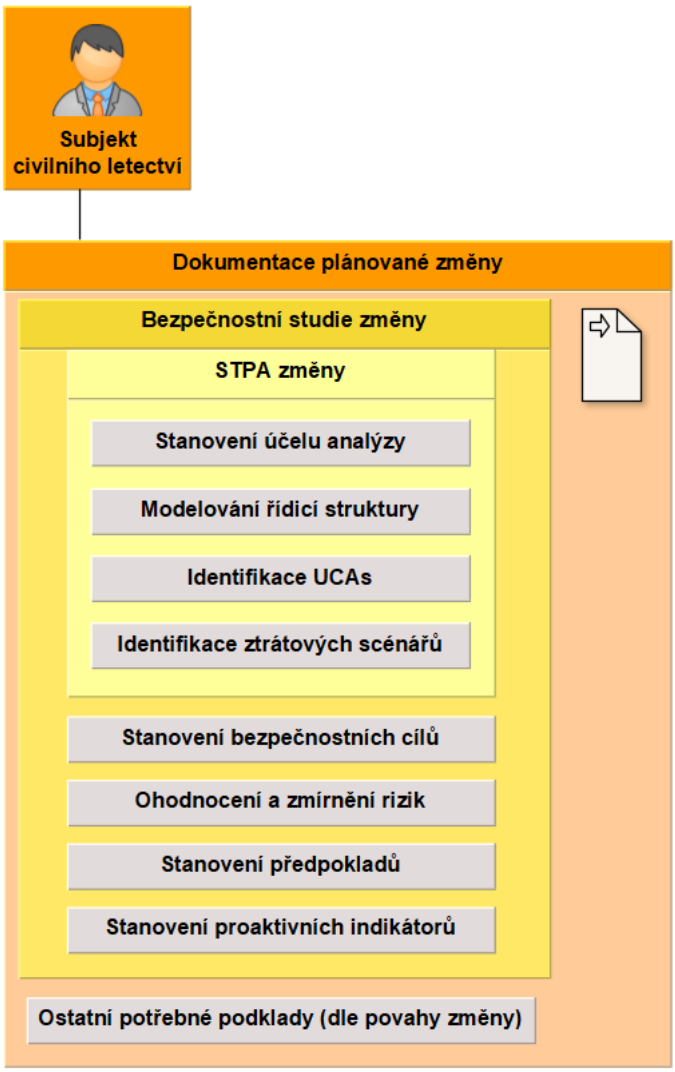


Obrázek 12: Základní rovina procesu řízení plánovaných změn ze strany ÚCL

7.1 Vstupy od subjektu civilního letectví

Vzhledem k tomu, že hlavním vstupem do řízení plánovaných změn je podnět od konkrétního subjektu, který chce danou změnu zavést do provozu, měly by být i požadavky na tyto subjekty pozměněny vzhledem k využití systémového přístupu. O změnu by se pak jednalo především v části dokumentace, která se zabývá bezpečnostním posouzením změny. Další podklady, které jsou dle typu změny po subjektu požadovány (např. výkresová dokumentace, formuláře apod.), by dle své povahy buď měly stávající podobu, nebo by mohly být upraveny, aby rovněž reflektovaly systémový přístup. Nicméně co se týká právě bezpečnostního posouzení změny, ze strany subjektů civilního letectví by bylo nejlepší využití STPA (doposud ÚCL subjektům nedoporučoval konkrétní metodu pro bezpečnostní posouzení). Vzhledem k předpokladu, že subjekt bude rovněž využívat systémový přístup k bezpečnosti

a související STPA, potřebné vstupy by měly mít podobu znázorněnou na obrázku 13 a jsou podrobně přiblíženy v následujících podkapitolách.



Obrázek 13: Vstupy od subjektu civilního letectví

7.1.1 STPA plánované změny

V rámci STPA jsou identifikovány ztráty, související systémová nebezpečí a omezení, dále je provozovatelem vytvořena potřebná řídicí struktura, která poskytuje vstup ve formě řídicích prvků a řídicích akcí pro stanovení odpovídajících nebezpečných řízení (UCA), k nimž jsou určeny ztrátové scénáře. Použití STPA je výhodné především z hlediska detailnosti této analýzy, protože kromě stanovení systémových ztrát a nebezpečí umožňuje podrobný popis toho, jak by k těmto ztrátám a nebezpečím mohlo dojít skrze ztrátové scénáře.

Výstupy z STPA mohou být následně využity pro ohodnocení a zmírnění rizik, což je přiblíženo v následující podkapitole.

7.1.2 Ohodnocení a zmírnění rizik s využitím STPA

S využitím výstupů z STPA může být následně subjektem provedeno posouzení a zmírnění rizik. Doposud bylo subjektům doporučeno hodnocení rizik s využitím ICAO matice, která aplikuje hodnocení závažnosti a pravděpodobnosti. Nicméně v případě zavádění nových systémů či změn stávajících systémů je objektivní kvantifikace pravděpodobnosti náročná, neboť je závislá na historických datech. A vzhledem k tomu, že v těchto případech tato data nejsou obvykle dostupná, jedná se tak často o subjektivní hodnocení pravděpodobnosti ze strany daného hodnotitele, což ve výsledku může zkreslit celkové ohodnocení rizik a tím i celou bezpečnostní studii. Proto je ve vytvořeném návrhu pracováno s novou maticí rizik, tzv. STPA-Informed Risk Matrix (SRM), která byla navržena autory Yoo a Grigorian [23] na univerzitě MIT (Massachusetts Institute of Technology). Výhodou použití této nové matice je rovněž to, že byla tvořena za účelem využití výstupů z STPA pro její aplikaci.

Podstatou SRM je převedení výsledků STPA do hodnocení rizik bez nutnosti zaměřovat se zejména na pravděpodobnost, která odhaduje výskyt rizik. Místo toho se zdá být smysluplnější zaměřit se především na účinnost zmírnění (mitigation effectiveness) daného rizika. Účinnost zmírnění rizika reprezentuje to, jak dobře navržené zmírnění řídí riziko. Tímto je pozornost přesunuta na přímé zmírnění rizik spíše než na to, kdy tato rizika mohou nastat. V rámci hodnocení účinnosti zmírnění je nejprve důležité stanovit jednotlivá opatření. Zde se jedná o 5 úrovní zmírnění rizik, které jsou názorně zobrazeny v tabulce 6. Ke každé úrovni zmírnění rizik je následně přiřazeno tzv. skóre účinnosti zmírnění (MES – Mitigation Effectiveness Score). Z tabulky 6 je patrné, že nejvyššího skóre lze dosáhnout opatřením, které eliminuje riziko, případně opatřením, které sníží riziko prostřednictvím návrhu systému. Oba tyto způsoby jsou považovány za proaktivní, proto je jejich skóre vyšší, než je tomu u detekce s odezvou, případně u školení a postupů, jež jsou považovány za reaktivní. Zároveň platí, že pro každé riziko může být stanoveno více než jedno zmírňující opatření, což výslednou účinnost zmírnění může zvýšit. To je zřejmé z tabulky 7, která zobrazuje finální SRM, nicméně místo hodnoty MES zahrnuje hodnotu CMES – Combined Mitigation Effectiveness Score, což je tzv. kombinované skóre účinnosti zmírnění. Rozsah CMES je od „Nejméně efektivní“ s hodnotou 0 po „Eliminováno“. CMES s hodnotou 6 (tedy „Nejefektivnější) lze dosáhnout v případě, kdy jsou pro zmírnění rizika využity všechny tři úrovně zmírnění (Snížení prostřednictvím návrhu systému + Detekováno s odezvou + Školení a postupy = 3 + 2 + 1 = 6). Mimo to je hodnota CMES založena na předpokladu, že více zmírňujících opatření

na stejné úrovni neznamená vyšší výslednou hodnotu CMES. Pokud jsou tak ke konkrétnímu riziku stanovena dvě zmírňující opatření úrovně „Snížení prostřednictvím návrhu systému“, každé s hodnotou MES = 3, finální hodnota CMES by byla stále 3 místo 6. Důraz je zde tedy kladen především na kvalitu zmírnění, nikoli na kvantitu. Rovněž jsou zde možné případy, kdy budou navržena například dvě opatření, kdy jedno bude „Snížení prostřednictvím návrhu systému“ s MES = 3 a druhé „Detekováno s odezvou“ s MES = 2, ale kombinované účinky v dané situaci mohou riziko přímo eliminovat (CMES = ELIM). Vždy tak záleží na konkrétním kontextu a kombinaci typů zmírnění. [23]

Tabulka 6: Úrovně účinnosti zmírnění rizik (upraveno z [23])

Úroveň zmírnění	Popis zmírnění	Skóre účinnosti zmírnění (MES)
Eliminováno	Kauzální faktor lze eliminovat pomocí návrhu nebo specifickou kombinací níže uvedených zmírnění (proaktivní).	ELIM
Snížení prostřednictvím návrhu systému	Výskyt kauzálního faktoru lze snížit, popřípadě řídit prostřednictvím návrhu systému (proaktivní).	3
Detekováno s odezvou	Kauzální faktor lze detekovat a vyžaduje reakci ke zmírnění (reaktivní).	2
Školení a postupy	Kauzální faktor lze zmírnit dodatečným školením a postupy (reaktivní).	1
Žádné	Neexistuje žádné možné zmírnění nebo zmírnění nebude použito.	0

Co však v tomto případě v hodnocení rizik zůstává, je hodnocení závažnosti (severity). Zde se nejedná o tak závažný problém z pohledu hodnocení tohoto parametru, neboť při hodnocení závažnosti by měly být brány v potaz nejhorší možné scénáře, což je podrobně rozebráno v rámci STPA, a proto je stanovení závažnosti poměrně jednoznačné. Rozdělení závažnosti do jednotlivých kategorií je znázorněno v tabulce 8. Prvotně je každému riziku přiřazena závažnost před zmírněním (PMS – Pre-Mitigation Severity) a dále se hodnotí závažnost po stanovení potenciálních zmírňujících opatření (PPMS – Post-Potential Mitigation Severity). Jak ukazuje tabulka 9, kromě hodnot PMS a PPMS se zároveň určuje výsledná hodnota tzv. CPMS – Combined Post-Mitigation Severity, neboli kombinovaná závažnost po zmírnění. Hodnota CPMS se určuje tak, že se vypočítá průměr všech PPMS pro určité riziko a poté se zaokrouhlí dolů na nejbližší

celé číslo. Výsledné CPMS se rovněž jako výše zmíněné CMES zaznamenává do finální SRM, která je znázorněna v tabulce 7. [23]

Tabulka 7: STPA-Informed Risk Matrix – SRM (upraveno z [23])

Dílčí nebezpečí					
Nejméně efektivní	**0**				
Mírně efektivní	**1**				
Středně efektivní	**2-3**				
Velmi efektivní	**4-5**				
Nejefektivnější	**6**				
Eliminováno	**N/A**				
CMES		**1**	**2**	**3**	**4**
	CPMS	Katastrofická	Kritická	Nízká	Zanedbatelná

Tabulka 8: Rozdělení závažnosti (upraveno z [23])

Závažnost	**Kategorie závažnosti**
Katastrofická	1
Kritická	2
Nízká	3
Zanedbatelná	4

Tabulka 9: Příklad hodnocení závažnosti (upraveno z [23])

ID rizika	**PMS**	**ID zmírnění**	**PPMS**	**CPMS**
R1	1	RM01	4	3
		RM02	3	
		RM03	3	

Jak již bylo zmíněno, SRM pracuje s výstupy z provedené STPA. Existují zde dva přístupy, jak riziko hodnotit. Prvním z nich je přístup založený na scénářích (Scenario-Based Approach), jehož podstatou je využití identifikovaných ztrátových scénářů z STPA jako rizik, která mají být ohodnocena a zmírněna způsobem, který byl popsán výše. Jedná se tak o velmi podrobné hodnocení, neboť výčet scénářů z STPA bývá dost rozsáhlý. Ačkoliv je detailnost hodnocení důležitá, z pohledu dozorového orgánu by se jednalo o velkou časovou zátěž při posuzování těchto výstupů, pokud by se subjekt rozhodl pro přístup založený na scénářích. Proto se jeví jako smysluplnější druhý přístup, který je založen na

nebezpečích (Hazard-Based Approach). Jedná se tak o rizika reprezentující dílčí nebezpečí, jež specifikují systémová nebezpečí definovaná v rámci STPA. Ačkoliv je dílčích nebezpečí značně méně než ztrátových scénářů, nelze říci, že se jedná o nekompletní seznam rizik, neboť ztrátové scénáře spadají pod tato dílčí nebezpečí, tudíž při stanovení zmírňujících opatření dojde zároveň ke zmírnění všech scénářů, které spadají pod dané dílčí nebezpečí. Přístup založený na nebezpečích zahrnuje kroky uvedené v tabulce 10.

Tabulka 10: Kroky pro přístup založený na nebezpečích (upraveno z [23])

Přístup založený na nebezpečích	
Krok 1	Kompletace STPA
Krok 2	Stanovení dílčích nebezpečí
Krok 3	Ohodnocení závažnosti před zmírněním (PMS) každého dílčího nebezpečí
Krok 4	Stanovení dílčích omezení
Krok 5	Stanovení zmírňujících opatření, aby bylo splněno každé dílčí omezení
Krok 6	Kompletní ohodnocení CMES a CPMS
Krok 7	Zanesení každého dílčího nebezpečí do matice rizik na základě CMES a CPMS

7.1.3 Stanovení bezpečnostních cílů

S využitím nové matice rizik založené na výstupech STPA by se zároveň přizpůsobilo to, jak subjekt stanoví své bezpečnostní cíle. Vzhledem k využití přístupu založeného na nebezpečích by nejprve subjekt sepsal veškerá dílčí nebezpečí spolu s ohodnocením PMS. K tomu by následně z matice rizik určil, jakou nejnižší hodnotu CMES může riziko ve formě dílčích nebezpečí při dané hodnotě PMS mít, aby bylo bráno jako tolerovatelné.

7.1.4 Stanovení předpokladů a proaktivních indikátorů

Kromě ohodnocení a zmírnění rizik a stanovení bezpečnostních cílů je rovněž u subjektu civilního letectví důležité, aby stanovil, jakým způsobem bude následně plánovanou změnu sledovat, pokud bude ze strany ÚCL schválena a bude zavedena do provozu. V tomto směru se jeví jako přínosné určit předpoklady o dané plánované změně a posléze proaktivní indikátory, které budou z těchto předpokladů vycházet. Předpoklady a na ně navázané proaktivní indikátory budou také určeny na základě

výstupů z STPA, konkrétně mohou vycházet z identifikovaných dílčích nebezpečí, respektive z dílčích omezení.

7.2 FHA

V kapitole 4.2.1, která se věnovala fázi FHA, bylo zmíněno, že jejím hlavním cílem je stanovení toho, jak bezpečný musí být daný systém či v tomto případě změna systému. Zde se jedná o případ, kdy je potřeba, aby změna byla posouzena a následně schválena ÚCL, a proto hlavním úkolem ÚCL v této fázi bude posouzení potřebné dokumentace od subjektu civilního letectví za účelem stanovení, zda byla správně identifikována nebezpečí a na základě toho, zda byly adekvátně stanoveny bezpečnostní cíle změny určující požadovanou úroveň bezpečnosti změny. Na obrázku 14 je zobrazena vizualizace fáze FHA se zaměřením na její vstupy, kroky a výstupy, na obrázku 15 je následně demonstrována procesní rovina fáze FHA s přiblížením posloupnosti jednotlivých kroků.

ÚCL nejprve obdrží veškerou dokumentaci k plánované změně od subjektu, která již byla zmíněna v předchozí kapitole 7.1. Nicméně ve fázi FHA jsou stěžejními vstupy pro ÚCL zejména kompletní STPA plánované změny, ohodnocení PMS dílčích nebezpečí společně s následným stanovením bezpečnostních cílů a stanovené předpoklady a proaktivní indikátory. Mimo uvedené vstupy od subjektu využije ÚCL k jejich posouzení příslušnou legislativu, která se daným systémem zabývá, případně může využít historická data, pokud už byla plánovaná změna stejného charakteru posuzována u jiného subjektu a mohla by tato data pomoci při procesu posuzování dokumentace.

Prvotním krokem ÚCL ve chvíli, kdy má kompletní vstupy, je posouzení STPA změny. Dá se předpokládat, že STPA změny od subjektu bude velmi rozsáhlá s ohledem na fakt, do jaké míry detailu se v rámci STPA dostáváme, neboť se jedná o velmi podrobnou analýzu. Avšak z pohledu dozorového orgánu to může přinést značné výhody, neboť zde nevidí pouze identifikovaná nebezpečí, ale rovněž řídicí strukturu, která znázorňuje řídicí, zpětné a koordinační vazby mezi jednotlivými prvky, což umožní lepší orientaci ve vztazích mezi těmito prvky. Nehledě na následné určení nebezpečných řízení spolu se ztrátovými scénáři, které jasně demonstrují to, jakým způsobem může dojít k následným nebezpečím a posléze ztrátám. Nicméně není v možnostech ÚCL posoudit STPA do největší míry detailu, a to ať už z hlediska časových možností či z hlediska znalostí o jednotlivých systémech, které nemohou být rozsáhlé tak, jak je tomu u subjektu, pod jehož provoz systém spadá. I přesto může ÚCL adekvátně posoudit

kompletnost a správnost STPA. Postupovalo by při tom stejným způsobem jako při vytváření STPA, tedy od ztrát a nebezpečí až po ztrátové scénáře. Ztráty by měly být posouzeny zejména z toho hlediska, zda subjekt dle úsudku ÚCL zmínil veškeré ztráty, ke kterým by u daného systému mohlo dojít. Následovat by mělo posouzení systémových a případně i dílčích nebezpečí. V tomto bodě by ÚCL měl být schopen zhodnotit, jestli subjekt zvážil všechna možná nebezpečí, k čemuž mu mohou pomoci i případná data z již dříve schválených změn stejného charakteru. Důležité je, aby případná dílčí nebezpečí byla skutečně podmnožinou souvisejících systémových nebezpečí. Zároveň by měla být posouzena omezení a dílčí omezení, a to především proto, aby v STPA skutečně mělo každé nebezpečí své stanovené omezení. V rámci řídicí struktury se lze zaměřit na veškeré řídicí prvky a vazby mezi nimi. Podkladem pro hodnocení řídicí struktury mohou být i legislativní požadavky, neboť mohou určovat, jaké řídicí prvky jsou v daném systému požadovány společně s tím, jaké vazby mezi sebou jednotlivé prvky mají. Následuje posouzení nebezpečných řízení (UCAs). Pro nebezpečná řízení platí, že by měla být stanovena pro každou řídicí akci, což lze zkontrolovat na základě řídicí struktury, ve které by měly být všechny řídicí akce zaznamenány, čímž může být případně zjištěno, zda nebyla některá z řídicích akcí opomenuta při stanovení UCAs. Rovněž platí, že každá UCA by měla zahrnovat odkaz na související nebezpečí a měla by mít stanoveno omezení řídicího prvku. Posledním krokem posouzení STPA je zaměření se na ztrátové scénáře. V tomto kroku by mělo být zhodnoceno, zda subjekt formuloval scénáře ke každé UCA.

Po celkovém posouzení STPA plánované změny může být pozornost přesunuta na posouzení závažnosti jednotlivých dílčích nebezpečí před zmírněním (PMS – Pre-Mitigation Severity). V tomto směru se může ÚCL zaměřit především na to, jestli subjekt nepodceňuje závažnost nebezpečí, respektive zda neudává vyšší hodnotu PMS, která následně ovlivňuje výsledné bezpečnostní cíle. Zároveň lze následně zhodnotit správnost dále určených bezpečnostních cílů, a to s využitím příslušné matice rizik, která udává nejnižší možnou hodnotu CMES pro tolerování nebezpečí.

Ve fázi FHA by měl ÚCL také zvážit subjektem vytyčené předpoklady a související proaktivní indikátory, které by v případě schválení změny ze strany ÚCL sloužily subjektu pro sledování změny v provozu. Pokud subjekt při vytváření předpokladů vycházel z dílčích omezení, měly by být předpoklady stanoveny ke každému z nich a nemělo by se jednat o pouze jinak formulovaná omezení. K proaktivním indikátorům by měl mít subjekt definováno, jakým způsobem je bude měřit či sledovat a neměl by opomenout

určení formovacích a zajišťovacích akcí (shaping actions, hedging actions) a bodů pro spuštění kontroly předpokladů (signposts). Na základě předpokladů subjektu může ÚCL stanovit prvotní předpoklady, které by zajímaly ÚCL v následné dozorové činnosti po případném schválení změny. Nicméně může tento krok aplikovat až v nadcházející fázi PSSA, která ÚCL přinese více důkazů o tom, zda vůbec bude plánovaná změna schválena.

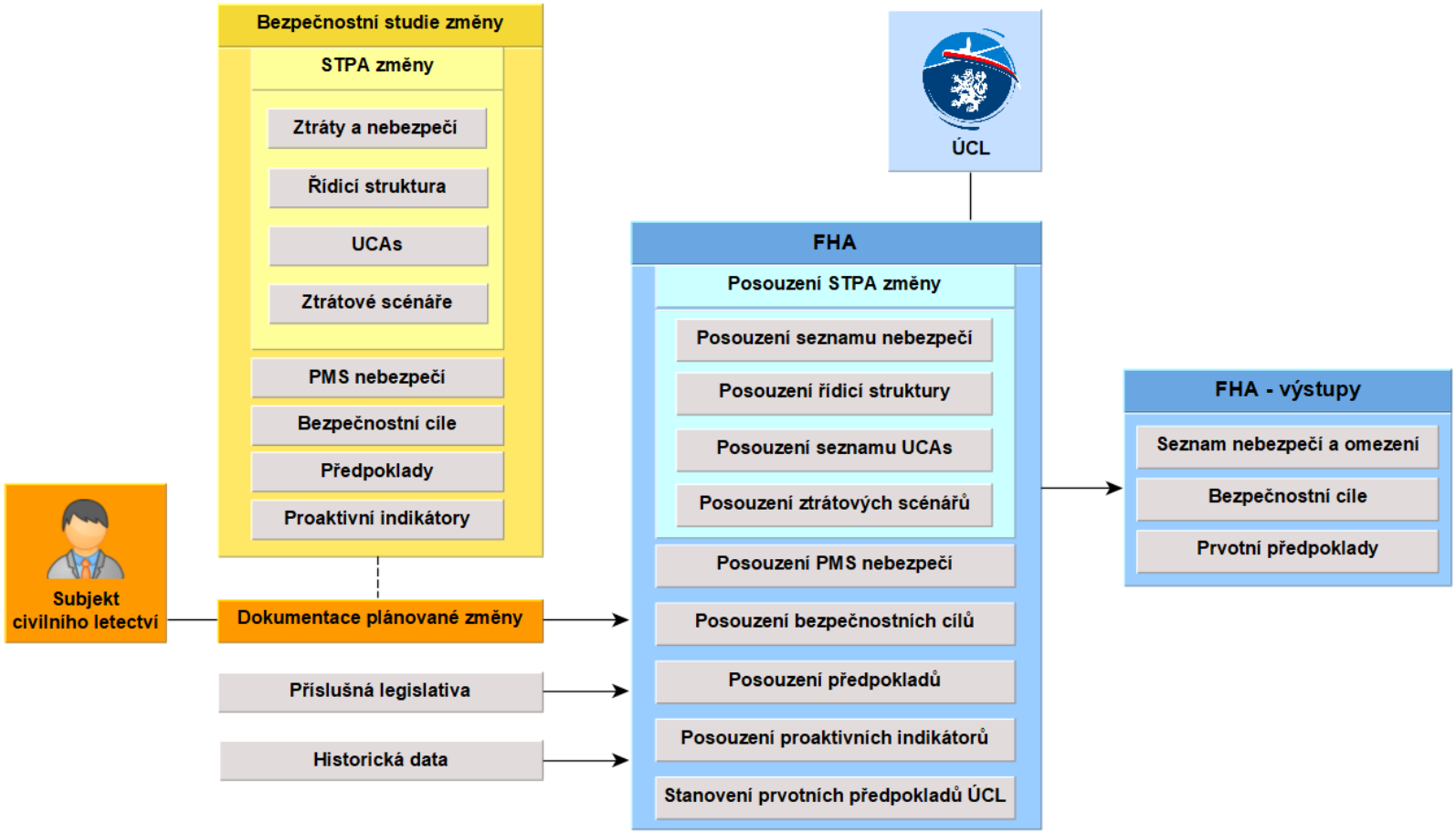
Z FHA jsou pro ÚCL nejdůležitějšími výstupy nebezpečí a omezení z STPA, dále bezpečnostní cíle subjektu a případné prvotní předpoklady pro dozorovou činnost ÚCL.

7.3 PSSA

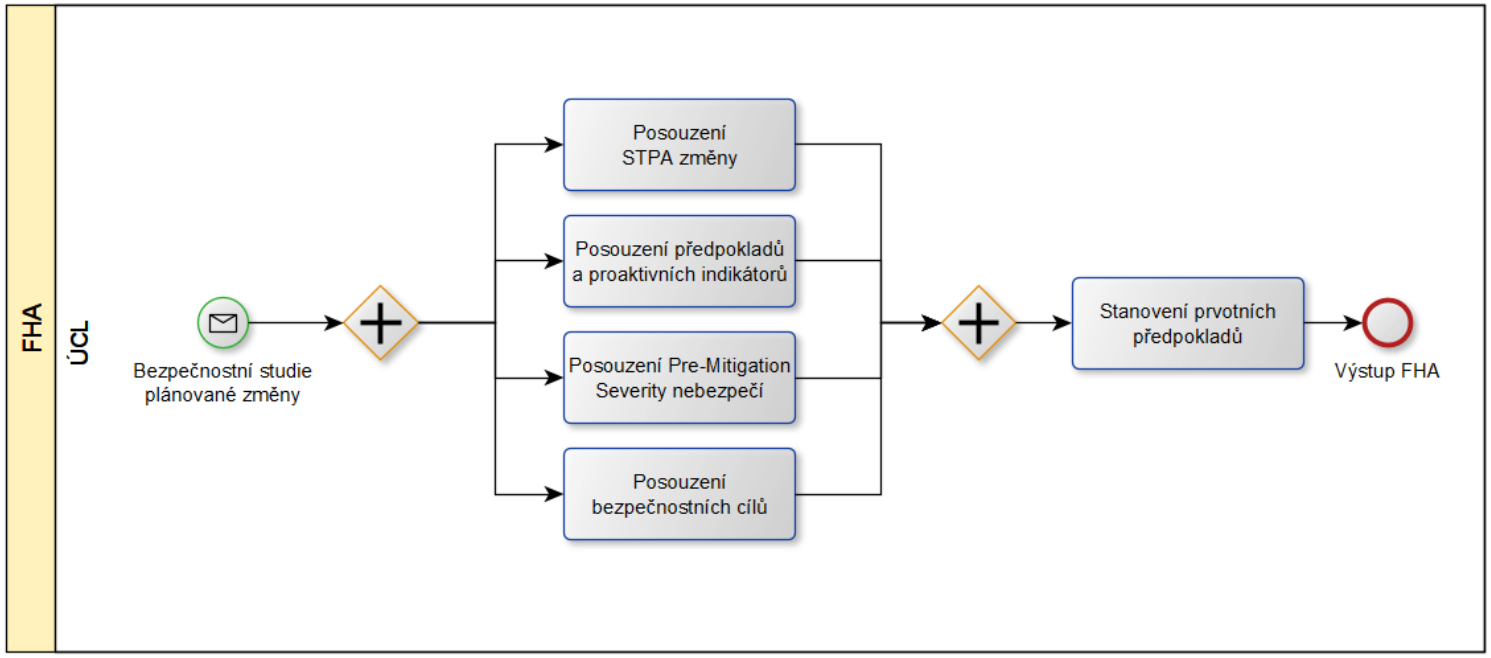
Pro fázi PSSA je stěžejní určení, jak je daný systém bezpečný, což lze poznat zejména z toho, zda systém dosahuje stanovených bezpečnostních cílů, jež byly určeny v předchozí fázi FHA. Z pohledu ÚCL se jedná o zásadní krok celého posouzení, neboť zde budou posuzovány důkazy o tom, jestli je subjekt schopen naplnit stanovené bezpečnostní cíle, případně jakým způsobem toho chce dosáhnout. V této fázi zároveň dojde k rozhodnutí o schválení, či neschválení plánované změny. Na obrázku 16 je uvedena ukázka fáze PSSA s vymezením příslušných vstupů, kroků a výstupů a následně obrázek 17 demonstruje procesní rovinu fáze PSSA.

Stejně jako tomu bylo ve fázi FHA, i zde jsou nejpodstatnější vstupy od subjektu civilního letectví, a to konkrétně ohodnocení a zmírnění rizik. Zmíněný vstup si lze představit například ve formě tabulky. V rámci tohoto kroku subjekt předvede nejen to, jak rizika ohodnotil, ale především způsob, jakým hodlá daná rizika zmírnit na alespoň tolerovatelnou úroveň, což reflektují bezpečnostní požadavky ve formě zmírňujících opatření. Tím dokáže, že je systém schopen dosáhnout svých bezpečnostních cílů. Spolu s ohodnocením a zmírněním rizik vstupují do procesu výstupy předchozí fáze FHA, které rovněž ÚCL pomohou při posouzení bezpečnosti změny a mimo to může dojít k situaci, kdy až ve fázi PSSA budou zjištěny některé nesrovnalosti, které mohly být v FHA přehlédnuty. Jako další možný zdroj potřebných informací pro posouzení plánované změny ze strany ÚCL bude i v tomto případě příslušná legislativa společně s případnými historickými daty, pokud existují.

V kapitole 7.1.2 byl představen návrh nové matice rizik od MIT. Vzhledem k tomu, že tato matice využívá výstupy z STPA a jeví se jako přínosnější pro ohodnocení rizik u systémů, z jejichž provozu nemáme dostatek dat pro hodnocení pravděpodobnosti, je posouzení hodnocení a zmírnění rizik demonstrováno s uvážením právě této navržené matice.



Obrázek 14: Vstupy, kroky a výstupy FHA



Obrázek 15: Proces FHA

I když se nejedná o výlučnou variantu pro hodnocení rizik a lze využít například dnes stále hojně aplikovanou ICAO matici rizik, byla zde přiblížena její omezení ve smyslu zaměření na pravděpodobnost, která se u nových dosud neprovozovaných systémů odhaduje jen stěží. Její využití by se tak dalo předpokládat spíše pro systémy, u nichž jsou dostupná historická data pro adekvátní stanovení pravděpodobnosti.

ÚCL začíná svou činnost ve fázi PSSA tím, že v tabulce pro hodnocení a zmírnění rizik zkontroluje kompletnost dílčích omezení, která byla specifikována během STPA. Ke každému dílčímu omezení musí být uveden odkaz na dílčí nebezpečí, k němuž se omezení vztahuje. Dále je žádoucí, aby zde byly uvedeny odkazy na ztrátové scénáře, které pod příslušné nebezpečí spadají. Poté se ÚCL zaměří na kontrolu PMS. Ačkoliv tuto činnost již provedl v FHA, zde se bude pravděpodobně jednat o jinou tabulku oproti té, která zahrnovala hodnocení PMS pro stanovení bezpečnostních cílů, tudíž zde může dojít k nesprávnému přepisu hodnoty do tabulky pro ohodnocení a zmírnění rizik. Dále je potřeba zvážit stanovená zmírňující opatření. Z pohledu ÚCL není možné do detailu zhodnotit, zda jsou opatření správná, nicméně jak bylo zmíněno v kapitole 7.1.2, v případě využití nové matice rizik se zde bude pracovat s konkrétními druhy zmírnění (eliminace, snížení prostřednictvím návrhu systému, detekce s odezvou, školení a postupy). K nim má být vždy přiřazena příslušná hodnota MES. V tomto směru může ÚCL provést kontrolu toho, zda subjekt správně přiřadil hodnoty k jednotlivým opatřením. Pokud by totiž subjekt například k opatření, které se bude týkat školení, přiřadil hodnotu MES = 3, jež odpovídá snížení prostřednictvím návrhu systému, došlo by k nesprávnému určení finální hodnoty CMES daného rizika, což by mohlo mít posléze negativní vliv na bezpečnost, kdyby tato skutečnost byla přehlédnuta. Následně by mělo dojít k posouzení správnosti výsledných hodnot CMES. V kapitole 7.1.2 byl přiblížen způsob určení hodnoty CMES, a proto by na základě této logiky mělo dojít ke kontrole, zda subjekt neurčil vyšší hodnotu CMES, než jaká je skutečná hodnota dle stanovených MES jednotlivých opatření. Poté by měla být pozornost zaměřena na hodnoty PPMS. U některých opatření může být zjištěno, že se závažnost po nastavení opatření nijak nemění, nebo to, že subjekt hodnotu stanovil vyšší, než by skutečně měla být. Takové posouzení může ÚCL udělat například s využitím dat z předchozích procesů posuzování a schvalování změn. Z hodnot PPMS jednotlivých rizik byla určena výsledná hodnota CPMS, u níž by měla být posouzena správnost výpočtu, aby opět ani zde nedošlo k určení chybné hodnoty závažnosti, neboť právě hodnoty CPMS a CMES jsou nakonec subjektem zaneseny do finální matice rizik, která představuje ucelený obraz všech rizik. Díky tomuto

konečnému vyjádření ve formě matice rizik se všemi ohodnocenými riziky získá ÚCL kompletní představu o tom, zda splňují bezpečnostní cíle. Avšak i v tomto kroku by mělo dojít ke kontrole ze strany ÚCL, jestli jsou v matici uvedena veškerá dílčí nebezpečí a zároveň, jestli odpovídá jejich umístění v matici tomu, jaké hodnoty CMES a CPMS byly stanoveny v tabulce pro ohodnocení a zmírnění rizik.

Po provedení posouzení ohodnocení a zmírnění rizik ÚCL vyhodnotí, zda je možné plánovanou změnu schválit, či nikoliv. Pokud usoudí, že je potřeba bezpečnostní studii upravit či doplnit, aby změna mohla být schválena, informuje o této skutečnosti dotčený subjekt civilního letectví, který seznámí s důvody, jež vedly k tomuto rozhodnutí. Pokud subjekt nesrovnalosti v bezpečnostní studii změny napraví, je nutné ze strany ÚCL navrácení do fáze FHA.

Pokud je bezpečnostní studie změny v pořádku a ÚCL ji schválí, je pro ÚCL důležité, aby měl o plánované změně přehled i po jejím zavedení do provozu. I když změna byla řádně posouzena s ohledem na bezpečnost, neznamená to naprostou jistotu v tom, že v provozu nevzniknou žádné situace, ve kterých by mohla změna znamenat problém z hlediska bezpečnosti. Proto by bylo ze strany ÚCL žádoucí stanovit si podobně jako subjekt své předpoklady o daném systému a na základě toho proaktivní indikátory. Nicméně pro účely ÚCL nemusí být předpoklady a související proaktivní indikátory tak detailní, jako tomu bylo u subjektu. Vzhledem k tomu, že má ÚCL pod svou správou velký počet subjektů s různými předměty zájmu, nebylo by ani možné sledovat a vyhodnocovat pro každý systém tak velký počet proaktivních indikátorů. Důležité je, aby předpoklady a proaktivní indikátory pro následnou dozorovou činnost ÚCL vystihovaly to, co je u konkrétního systému podstatné a co je celkově stěžejní u tohoto systému pro zajištění požadované úrovně bezpečnosti. Pro subjekt bylo navrhováno, aby předpoklady vycházely z dílčích omezení daného systému. Pro Úřad, který nemusí v provozu sledovat takový detail, by stačilo formulovat předpoklady na základě systémových nebezpečí, respektive na základě systémových omezení. Zároveň by nemělo být opomenuto nastavení odpovídajících zajišťovacích a formovacích akcí společně s body pro spuštění kontroly předpokladů. Je však podstatné, aby Úřad myslel na to, že předpoklady (a následně proaktivní indikátory) musí mít pro jejich dozorovou činnost nad daným systémem skutečně smysl. Nesprávně zvolené předpoklady a nevhodně nastavené indikátory mu neumožní efektivní sledování plánované změny v provozu.

Nejdůležitějšími výstupy z PSSA jsou pro ÚCL především bezpečnostní požadavky ve formě zmírňujících opatření, na které se může následně více zaměřit při auditech či inspekcích, a dále pak stanovené předpoklady a proaktivní indikátory ÚCL, které budou využity pro sledování a vyhodnocování plánované změny v provozu.

7.4 SSA

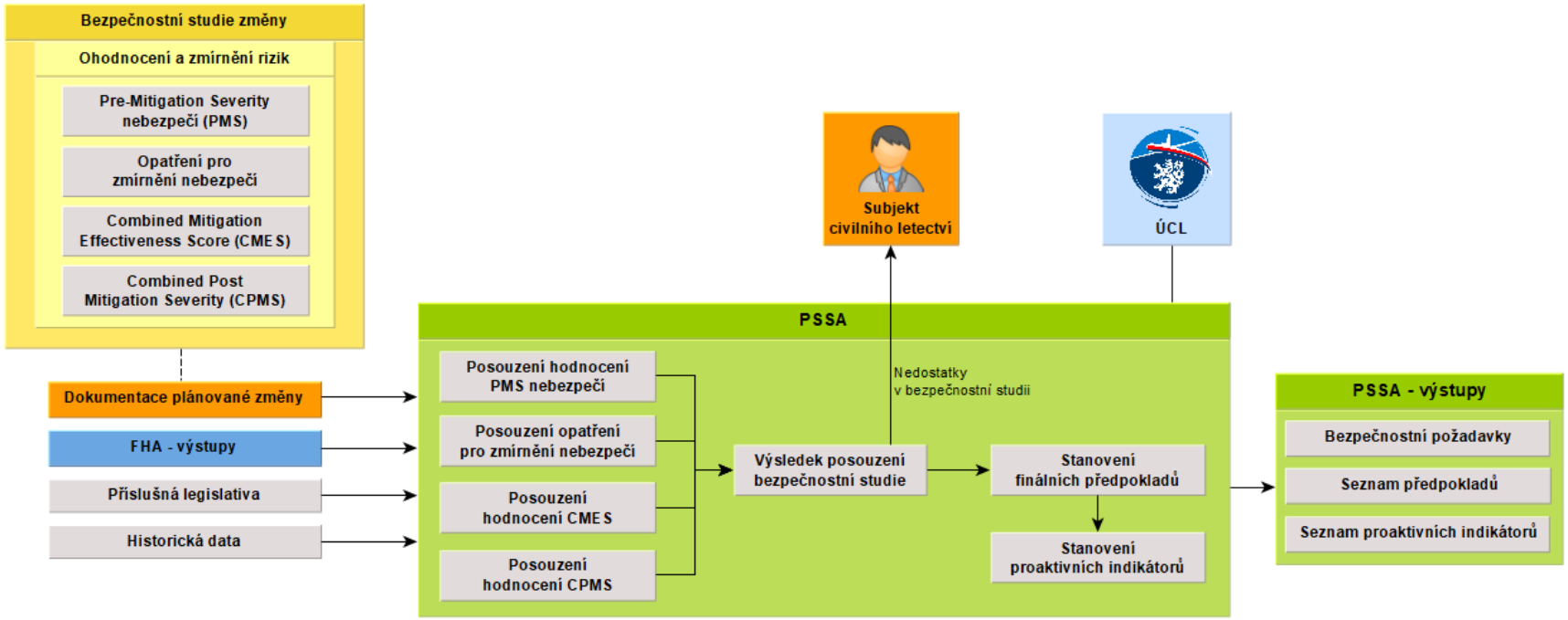
Účelem fáze SSA je prokázání, že plánovaná změna i po svém zavedení do provozu splňuje stanovené bezpečnostní cíle a stejně tak bezpečnostní požadavky. Jedná se zejména o shromažďování důkazů o tom, zda jsou tyto náležitosti splněny. Ačkoliv stěžejní sledování změny v provozu musí provádět daný subjekt, do jehož provozu je změna zavedena, role ÚCL v tomto směru nekončí. V rámci svého zájmu by měl ÚCL změnu rovněž v provozu sledovat, aby případně mohl včas zasáhnout, pokud by byl zjištěn nesoulad, který by mohl mít vliv na bezpečnost provozu. Obrázek 18 představuje vstupy, kroky a výstupy fáze SSA a obrázky 19 a 20 následně ukazují její procesní rovinu.

Mezi vstupy fáze SSA se řadí dokumentace plánované změny od subjektu, která již byla využita v předchozích fázích FHA a PSSA. Dále se jedná o výstupy z těchto předchozích fází společně s příslušnou legislativou a historickými daty. Legislativní požadavky v tomto případě stanoví, co je po daném systému z hlediska provozu požadováno a rovněž může stanovit, co je naopak nežádoucí. A pokud existují historická data ve smyslu již dříve prováděné SSA u plánované změny odpovídajícího charakteru, mohou být použita jako poradní vstup, když dojde k nejasnostem.

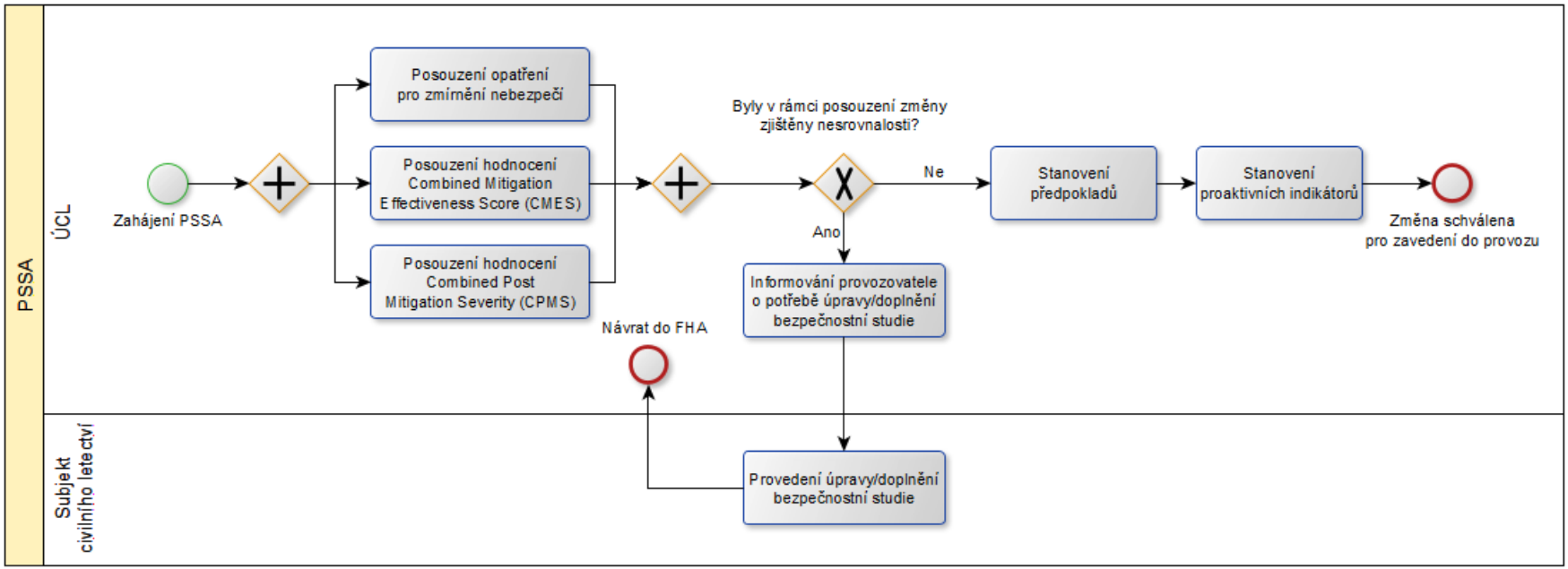
Ve chvíli, kdy jsou dostupné všechny zmíněné vstupy, je potřeba začít sbírat data, která nám upřesní, jak si změna z pohledu bezpečnosti vede. Způsobů, jakými může ÚCL konkrétní plánovanou změnu sledovat v provozu a sbírat tak potřebná data, je hned několik. Může se jednat o sběr dat z povinných či dobrovolných hlášení z provozu, která se od subjektů požadují, nebo data z šetření incidentů a nehod či data auditů a inspekcí, které ÚCL pravidelně provádí. Z těchto datových zdrojů by následně měla být s využitím proaktivních indikátorů vyhodnocena platnost stanovených předpokladů ÚCL. Pokud by bylo odhaleno porušení některého z předpokladů, bude ze strany ÚCL nutné provedení odpovídající zajišťovací akce, která byla k předpokladu stanovena ve fázi PSSA. Posléze by měl ÚCL zvážit, zda přispěl k porušení předpokladu například neadekvátním plněním vlastních odpovědností a vlastních řídicích akcí vůči subjektu, které by měl Úřad zahrnout ve své STPA popisující dozorovou činnost nad subjekty. Může se jednat například o podcenění potřeby provádění častějších auditů či inspekcí u konkrétního

subjektu, pokud se jedná o plánovanou změnu, jež je v provozu zásadní a vyžaduje ze strany ÚCL větší pozornost. Pokud by tato skutečnost byla zjištěna, Úřad by v rámci svých interních procesů měl provést Active STPA, během níž by nejen provedl kontrolu STPA své dozorové činnosti, ale především by se zaměřil na to, proč z jeho strany došlo k přispění porušení předpokladu. Následně by bylo navrženo řešení, aby k podobným situacím ze strany ÚCL nedocházelo a byla by aktualizovaná stávající STPA. Nicméně patrně častějším případem bude to, že předpoklad bude porušen především ze strany daného subjektu civilního letectví, neboť v jeho provozu se plánovaná změna vyskytuje, a tím má na její počínání mnohem větší vliv než dozorový orgán. Proto je tato možnost více rozpracována i ve zmíněných ukázkách návrhu na obrázcích 18, 19 a 20. V takovém případě bude provedení Active STPA požadováno právě po subjektu, jehož se plánovaná změna týká (viz obrázek 20). Subjekt by nejprve zkontroloval STPA příslušné změny, aby vyhodnotil, zda nedošlo k opomenutí či nesprávnému určení některých skutečností STPA. Dále by zvážil veškeré možné důvody porušení konkrétního předpokladu a vzápětí by navrhl potřebná opatření, aby byly splněny veškeré požadavky a omezení a provedl by aktualizaci STPA změny. Výstupy z Active STPA by byly předány ÚCL, kde by bylo provedeno jejich posouzení. Na základě výstupů by poté Úřad provedl případnou aktualizaci svých předpokladů a proaktivních indikátorů změny. Pokud by se však jednalo o rozsáhlé změny v původní STPA změny, které by se výrazným způsobem promítly v ostatních částech bezpečnostní studie změny, bylo by ze strany ÚCL nutné opětovné provedení fází FHA a PSSA.

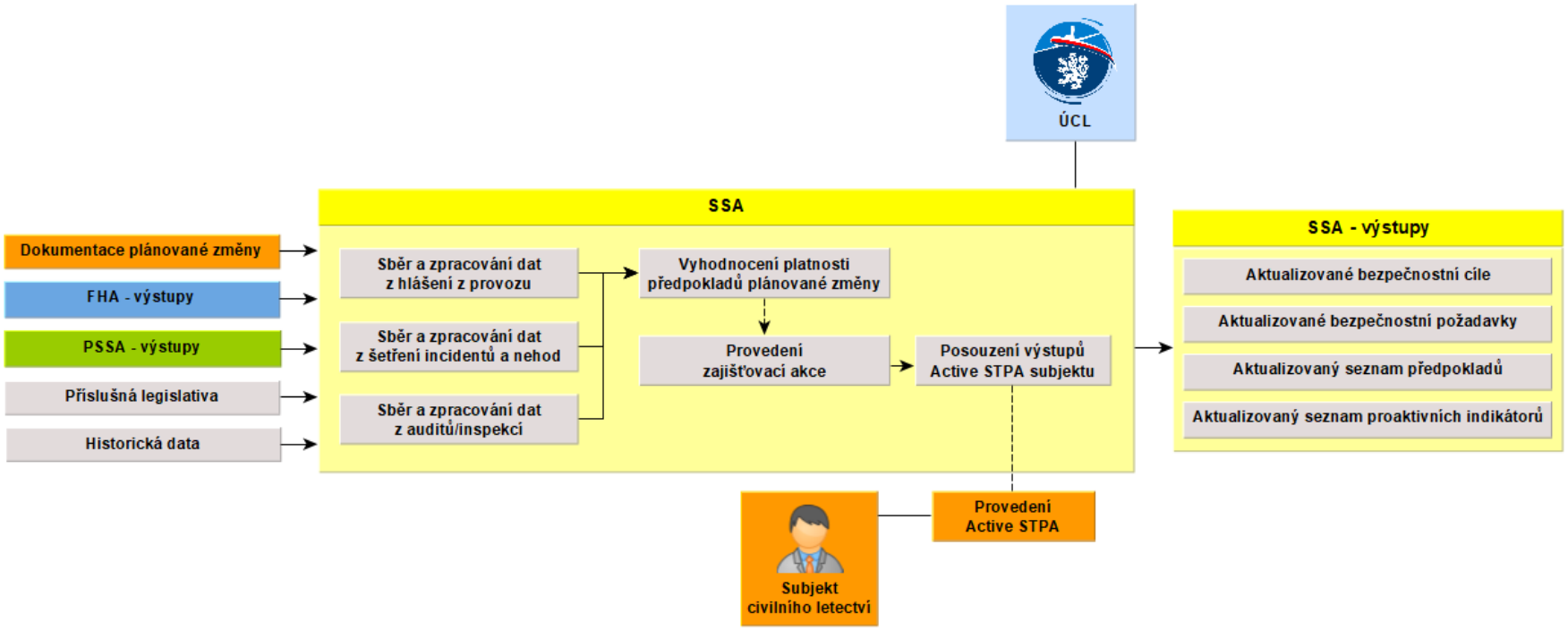
Důležitými výstupy z SSA jsou veškeré aktualizované informace o změně, z pohledu ÚCL se však jedná zejména o aktualizované bezpečnostní cíle a bezpečnostní požadavky změny a rovněž o aktualizované předpoklady a proaktivní indikátory stanovené pro dozorovou činnost ÚCL. Všechny tyto parametry dotčené změny musí být neustále aktuální. Proto je také nutné dodat, že SSA je kontinuální proces, který probíhá až do doby, kdy je systém vyřazen z provozu. V tu chvíli se dá hovořit o ukončení fáze SSA.



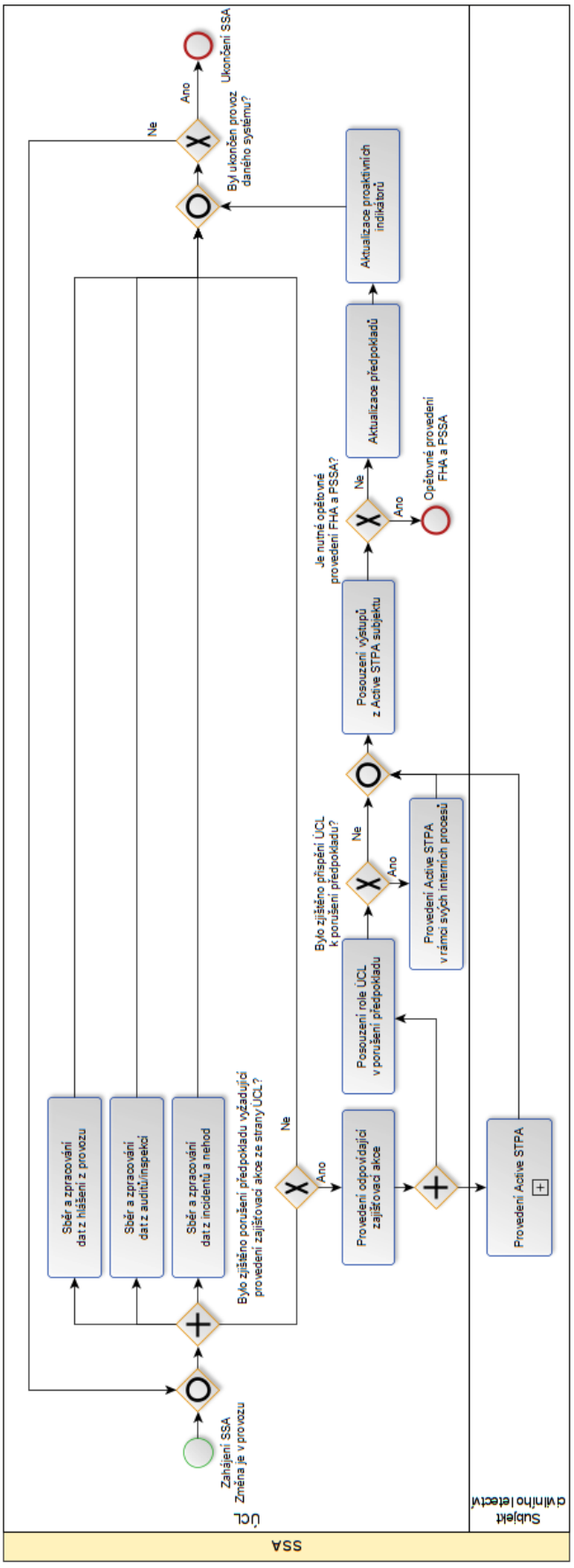
Obrázek 16: Vstupy, kroky a výstupy PSSA



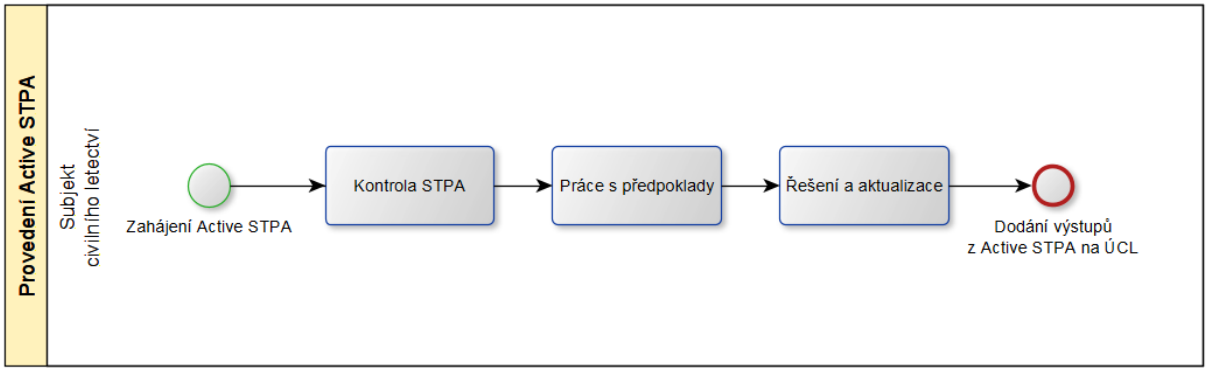
Obrázek 17: Proces PSSA



Obrázek 18: Vstupy, kroky a výstupy SSA



Obrázek 19: Proces SSA



Obrázek 20: Proces Active STPA subjektu

8 Ověření navrženého postupu

Ověření postupu navrženého v předchozí kapitole se jeví jako nejlepší s využitím reálné již schválené změny některého ze subjektů civilního letectví. Nicméně v současnosti nejen že ÚCL nepožaduje po subjektech využití systémového přístupu ve formě aplikace analýzy STPA na plánovanou změnu, ale především sám Úřad tento přístup v rámci své činnosti dosud neaplikoval. Proto k ověření postupu nebyla využita již schválená plánovaná změna, neboť by zde nebyla dostupná ani STPA dané změny. Místo toho bylo záměrem najít již vytvořenou STPA na určitý systém a na ní demonstrovat, jakým způsobem by s tímto vstupem Úřad pracoval.

Konkrétně byla vybrána STPA z diplomové práce Ing. Adama Kohoutka (Ověření modelu STAMP v procesech bezpečnostní kontroly [24]), která je zaměřena na procesy bezpečnostní kontroly na letišti. Jejím účelem bylo ověření správnosti nastavených procesů pro zabezpečení dostatečného počtu pracovníků pro provoz bezpečnostní kontroly (BEK). Sice se jedná o použití STPA na již zavedené procesy BEK, což není přímo příklad plánované změny, nicméně lze na to tímto způsobem pohlížet, neboť kroky STPA zde budou aplikovány stejným způsobem, ať už se jedná o zavedený proces, nebo plánovanou změnu. Zároveň je v praxi možné, že některá letecká organizace bude chtít své postupy měnit právě na ty, které jsou uvedeny ve zmíněné diplomové práci, což by znamenalo plánovanou změnu, která by musela být schválena ÚCL. Co zde však muselo být doplněno, jsou zbylé vstupy od daného subjektu civilního letectví, neboť diplomová práce Ing. Kohoutka byla zaměřena na vytvoření kompletní STPA, což je jen část požadovaných vstupů od subjektu, které byly uvedeny v kapitole 7.1.

V rámci této diplomové práce tak došlo ke stanovení bezpečnostních cílů, ohodnocení a zmírnění rizik s využitím matice rizik z MIT a dále k návrhu předpokladů a proaktivních indikátorů, které by letiště mohly zajímat v souvislosti s procesy pro zabezpečení dostatečného počtu pracovníků BEK. Je však nutné zmínit, že dotvořené vstupy jsou orientační z důvodu omezené znalosti analyzovaných procesů BEK.

Následně je na kompletním vstupu demonstrováno, jak by ÚCL postupovalo v posuzování STPA ve fázi FHA. Nabízí se použít tento vstup rovněž pro demonstraci posouzení ohodnocení a zmírnění rizik ve fázi PSSA. Nicméně v tomto případě bylo ohodnocení a zmírnění rizik dotvořeno na základě STPA z diplomové práce Ing. Kohoutka. Takové hodnocení by nedovolilo nezávislý pohled, a proto byl v této práci použit jiný vstup. Vzhledem k uvážení nové matice rizik z MIT byla pro ukázku posouzení

v rámci PSSA využita publikovaná práce MIT (A System-Theoretic Approach to Risk Analysis [23]), jež představovala ohodnocení a zmírnění rizik na příkladu hypotetického budoucího letounu s rotujícími nosnými plochami.

V závěru ověření je představeno, jakým způsobem by Úřad mohl tvořit předpoklady o systémech společně s proaktivními indikátory. To je opět demonstrováno na STPA bezpečnostní kontroly, neboť v rámci této diplomové práce byly dotvářeny předpoklady a indikátory pro letiště, tudíž je možné na tomto příkladu ukázat, jak by se předpoklady a indikátory lišily pro subjekty a pro ÚCL z hlediska míry detailu.

8.1 Doplnění potřebných vstupů

Jak již bylo zmíněno v předchozí kapitole, základním vstupem od subjektu je v tomto případě STPA na procesy bezpečnostní kontroly na letišti vytvořená Ing. Kohoutkem. Ve své diplomové práci provedl kompletní analýzu – identifikaci ztrát a systémových nebezpečí společně se systémovými omezeními, vytvoření řídicí struktury, identifikaci nebezpečných řízení spolu s omezeními řídicích prvků a v závěru stanovení ztrátových scénářů.

Na základě výstupů z vytvořené STPA od Ing. Kohoutka byly stanoveny bezpečnostní cíle, nicméně i pro následné hodnocení a zmírnění rizik bylo přínosnější specifikovat systémová nebezpečí na dílčí nebezpečí a následně určit dílčí omezení, neboť ta v původní STPA Ing. Kohoutka stanovena nebyla. Příklad vytvořených dílčích nebezpečí pro systémové nebezpečí *H-3: Nedodržení pravidel pro plánování* je představen v tabulce 11, a jejich dílčí omezení v tabulce 12. Celkový výčet dílčích nebezpečí a dílčích omezení je k nahlédnutí v příloze 1. Poté až došlo v této práci k určení bezpečnostních cílů, jejichž ukázka je uvedena v tabulce 13 a kompletní přehled v příloze 2.

Tabulka 11: Dílčí nebezpečí k systémovému nebezpečí H-3

Systémové nebezpečí		Dílčí nebezpečí		Odkaz na ztráty
H-3	Nedodržení pravidel pro plánování	H-3.1	Nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	[L-1, L-4]
		H-3.2	Překročení maximálního počtu směn na jednoho pracovníka BEK	[L-1, L-4]
		H-3.3	Překročení maximálního počtu přesčasů na jednoho pracovníka BEK	[L-1, L-4]
		H-3.4	Překročení maximálního počtu nočních směn jdoucích za sebou na jednoho pracovníka BEK	[L-1, L-4]

Tabulka 12: Dílčí omezení pro dílčí nebezpečí k H-3

Dílčí nebezpečí	Dílčí omezení	
H-3.1	SC-3.1	Musí být dodržen minimální počet přestávek na jednoho pracovníka BEK
H-3.2	SC-3.2	Nesmí být překročen maximální počet směn na jednoho pracovníka BEK
H-3.3	SC-3.3	Nesmí být překročen maximální počet přesčasů na jednoho pracovníka BEK
H-3.4	SC-3.4	Nesmí být překročen maximální počet nočních směn jdoucích za sebou na jednoho pracovníka BEK

Tabulka 13: Bezpečnostní cíle pro dílčí nebezpečí k H-3

ID nebezpečí	Popis	Závažnost (PMS)	Bezpečnostní cíl (dle CMES)
H-3.1	Nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	2	4-5
H-3.2	Překročení maximálního počtu směn na jednoho pracovníka BEK	2	4-5
H-3.3	Překročení počtu přesčasů na jednoho pracovníka BEK	2	4-5
H-3.4	Překročení maximálního počtu nočních směn jdoucích za sebou na jednoho pracovníka BEK	2	4-5

Následně zde došlo k ohodnocení a zmírnění rizik, a to s využitím SRM. To bylo provedeno s využitím přístupu založeném na nebezpečích (v tomto případě dílčích nebezpečích), jenž byl přiblížen v kapitole 7.1.2. Příklad ohodnoceného a zmírněného rizika je představen v tabulce 14 a celkové ohodnocení a zmírnění rizik je zahrnuto v příloze 3. Každé dílčí omezení má uvedeno odkaz na související dílčí nebezpečí, dále je k dílčímu nebezpečí přiřazena příslušná hodnota PMS. Dále byla stanovena zmírňující opatření ke každému riziku, přičemž zde docházelo ke kombinaci alespoň dvou úrovní zmírnění, k nimž bylo vždy přiřazeno odpovídající skóre účinnosti zmírnění (MES). Z těchto hodnot byly dále určeny výsledné hodnoty CMES pro každé riziko. Následovalo ohodnocení PPMS na základě každého zmírňujícího opatření a posléze stanovení výsledné hodnoty CPMS. Posléze byla na základě hodnot CMES a CPMS začleněna dílčí nebezpečí do finální SRM (tabulka 15) pro lepší vizualizaci a představu, zda jsou díky navrženým opatřením dosaženy stanovené bezpečnostní cíle. V tomto případě je při uvážení bezpečnostních cílů v tabulce 13 patrné, že došlo k jejich splnění.

Tabulka 14: Hodnocení a zmírnění rizika H-3.1

Odkaz na nebezpečí	PMS	RM ID	Doporučené zmírnění (Recommended Mitigation)	Úroveň zmírnění (Mitigation Level)	MES	CMES	PPMS	CPMS
H-3.1	2	RM09	Navržení programu, který zabrání tomu, aby během plánování došlo k nedodržení/překročení stanovených limitů (nedodržení minimálního počtu přestávek apod.)	Eliminováno	ELIM	ELIM	4	3
		RM10	Kontrola ze strany pracovníků BEK a případné upozornění dispečera DEP v případě zjištění nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	Detekováno s odezvou	2		4	
		RM07	Školení dispečera DEP ohledně jeho odpovědností (přiřazení pracovníků k jednotlivým pracovním úlohám apod.)	Školení a postupy	1		2	

Tabulka 15: Finální SRM

Dílčí nebezpečí					
Nejméně efektivní	0				
Mírně efektivní	1				
Středně efektivní	2-3			H-4.1, H-4.2, H-5.1, H-5.2	
Velmi efektivní	4-5		H-2.1		
Nejefektivnější	6			H-1.1, H-1.2	
Eliminováno	N/A	H-3.1, H-3.2, H-3.3, H-3.4			
CMES		**1**	**2**	**3**	**4**
	CPMS	Katastrofická	Kritická	Nízká	Zanedbatelná

Další krokem bylo stanovení předpokladů a proaktivních indikátorů založených na těchto předpokladech. K určení předpokladů byla využita dílčí omezení a jeden z příkladů je uveden v tabulce 16. Nad předpokladem bylo uvažováno tak, že ačkoliv dílčí omezení SC-3.1 (*Musí být dodržen minimální počet přestávek na jednoho pracovníka BEK*) může být splněno, stále je zde možnost, že dojde k nežádoucí události. Způsobeno to může být tím, že požadavky na minimální počty přestávek nejsou dostačující, a to například v tom smyslu, že i když je legislativně daný požadavek subjektem splněn, pro potřeby odpočinku pracovníků se jeví jako nedostačující a je nutné jeho zpřísnění ve formě vyššího počtu přestávek na jednoho zaměstnance. Druhým příkladem může být to, že požadavky na minimální počet přestávek jsou dostačující, ale při plánování

směn jsou využívány zastaralé či nedostačující požadavky. Na základě této úvahy byly stanoveny dva předpoklady, jeden vztahující se na dostatečnost požadavků (*Požadavky na minimální počet přestávek na jednoho pracovníka BEK jsou dostačující pro odpočinek pracovníka.*) a druhý vztahující se na využití aktuálních a dostačujících požadavků (*Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na minimální počet přestávek na jednoho pracovníka BEK.*). Ačkoliv tomu tak být vždy nemusí a záleží vždy na konkrétním předpokladu, v tomto případě se předpoklad rovná proaktivnímu indikátoru. Je to z toho důvodu, že při následném vyhodnocování platnosti je zde vhodné využít pouze variantu kvalitativního hodnocení, konkrétně hodnocení, jestli je tvrzení pravdivé, nebo ne. Způsoby, jakými mohou být předpoklady, respektive proaktivní indikátory, vyhodnocovány, jsou například *Kontroly/inspekce/audity BEK* a *Hlášení pracovníků BEK*. Formovací akce (shaping actions) sloužící k udržení platnosti předpokladu zde byly určeny jako *Pravidelné přezkoumání požadavků* a *Provádění kontrol/inspekcí/auditů BEK*. Zajišťovací akce (hedging actions) byly stanoveny 3 a vždy bude záležet na konkrétní situaci, která z nich bude použita. Pokud se jedná o nefunkční požadavky, bylo by žádoucí provést *Úpravu požadavků na minimální počet přestávek dle potřeby*. Dále by mělo dojít k *Doplňujícímu školení pracovníků*, aby byly pracovníkům vysvětleny případné nesrovnalosti nebo úpravy požadavků, či *Zvýšení frekvence kontrol/inspekcí/auditů*, které zajistí ověření plnění odpovědností. Události, které budou spouštět kontrolu předpokladů (signposts), jsou stanoveny jako *Plánované změny postupů BEK*. Veškeré předpoklady a proaktivní indikátory jsou k nahlédnutí v příloze 4.

Tabulka 16: Předpoklady (proaktivní indikátory) k SC-3.1

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování	Hedging action
SC-3.1	Požadavky na minimální počet přestávek na jednoho pracovníka BEK jsou dostačující pro odpočinek pracovníka.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Úprava požadavků na minimální počet přestávek dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
		Shaping action	**Signposts**
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na minimální počet přestávek na jednoho pracovníka BEK.	Pravidelné přezkoumání požadavků. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)

8.2 Posouzení STPA změny

V rámci fáze FHA by ÚCL nejprve posuzoval STPA dané změny. Konkrétní postup, který přibližoval, na co by se Úřad měl při posuzování zaměřit, byl popsán v kapitole 7.2. V STPA na BEK byly identifikovány 4 ztráty – finanční náklady (L-1), poškození nebo zničení majetku letiště (L-2), ztráta života či zranění (L-3), ztráta reputace (L-4) [24]. Při uvážení systému bezpečnostní kontroly v kontextu provozu celého letiště je zřejmé, že se jedná o kompletní výčet ztrát. V dalším kroku došlo k posouzení systémových nebezpečí uvedených v tabulce 17. Systémová nebezpečí se zde jeví rovněž jako kompletní, nicméně je lehce v rozporu úroveň detailu jednotlivých nebezpečí, konkrétně H-1 a H-2. Nebezpečí H-2 působí jako dílčí nebezpečí k H-1, totiž ve chvíli, kdy bezpečnostní kontrola nezaručí dostatek pracovníků BEK, tak může dojít k tomu, že nebude pokryt provoz. Přesně z tohoto důvodu je přínosné specifikovat systémová nebezpečí na dílčí nebezpečí, aby byl zjištěn případný rozpor v úrovni detailu. Zároveň by u nebezpečí H-1 měla být doplněna ztráta L-3, která se týká ztráty života či zranění. Dále byla posouzena systémová omezení k jednotlivým systémovým nebezpečím. Ačkoliv jsou všechna omezení v pořádku, autor zde opět uvádí odkazy na ztráty, nicméně u nebezpečí H-3 (respektive omezení SC-3) zmiňuje ztráty L-2 a L-4, kdežto v předchozím kroku, při kterém definoval systémová nebezpečí, uvedl u nebezpečí H-3 ztráty L-1 a L-4. Ačkoliv se může zdát, že se nejedná o zásadní pochybení, v STPA je kladen důraz na dodržení správnosti v odkazování se na jednotlivé části analýzy, aby v celkovém kontextu dávala smysl. Pokud by podobných pochybení bylo více, analýza by byla nekonzistentní.

Tabulka 17: Systémová nebezpečí (upraveno z [24])

Systémové nebezpečí		Odkaz na ztráty
H-1	Bezpečnostní kontrola nepokryje provoz	[L-1, L-2, L-4]
H-2	Bezpečnostní kontrola nezaručí dostatek pracovníků BEK	[L-1, L-2, L-3, L-4]
H-3	Nedodržení pravidel pro plánování	[L-1, L-4]
H-4	Při plánování dojde k překročení FPD (Fond pracovní doby)	[L-1]
H-5	Nedostatečná bezpečnostní kontrola	[L-1, L-2, L-3, L-4]

Řídicí struktura se jeví jako úplná, avšak nebyla nalezena legislativa, která by určovala, kdo všechno v tomto procesu figuruje. I přesto ale řídicí struktura splňuje potřebné náležitosti ve smyslu uvedení řídicích akcí a zpětných vazeb, rovněž jsou zde zahrnuty externí vstupy a v některých případech konkrétní akční členy. Jediné, co by bylo vhodné sjednotit, jsou formulace řídicích akcí. Některé jsou formulované včetně uvedení příslušné aktivity, jako například *Poskytnutí požadavku na minimální počet BEK*. Velká

část z nich je ale formulována bez aktivity, například *Strategické cíle, Limity práce s ročním FPD, Měsíční plán apod*.

Následně byla posouzena nebezpečná řízení spolu s omezeními řídicích prvků. Nebezpečná řízení byla určena pro všechny řídicí akce, nebyla zde žádná řídicí akce opomenuta, což je v pořádku. Zároveň autor dodržel syntaxi nebezpečných řízení, která má zahrnovat – řídicí prvek, typ UCA, řídicí akci, kontext a odkaz na nebezpečí. Pro omezení řídicího prvku platí, že by měla být formulována pro všechna nebezpečná řízení, což je v tomto případě splněno. Nicméně některá omezení nejsou vhodně formulována a působí tak, jako by patřila k jiné řídicí akci, než ke které se vztahují. Příklad je uveden v následující tabulce 18. Hned u UCA-22 chybí odkaz na nebezpečí, který však autor uvedl v tabulce, která se týkala výhradně UCAs, avšak i zde by měly být odkazy zahrnuty. Navíc omezení C-22 se zdá být vztaženo spíše k aktivitě, jež se týká procházení MPS, místo toho, aby byla zaměřena na možnost zastavení schválení MPS až po dokončení jeho kontroly. Podobnými případy jsou další dvě omezení C-27 a C-36, která se zaměřují na to, co musí mít vedoucí stanoviště k dispozici, ale nezahrnují nutnost předání MPS/požadavků na přesčas.

Tabulka 18: Příklad UCAs a omezení řídicích prvků (upraveno z [24])

UCA	Omezení řídicího prvku
UCA-22: VP (vedoucí provozu) zastaví schvalování MPS (měsíční plán směn) před dokončením kontroly celého MPS	C-22: VP musí projít celý MPS před jeho schválením
UCA-27: Vedoucí stanoviště nepředá MPS pracovníkům BEK během doby pro předání [H-1, H-2, H-5]	C-27: Vedoucí stanoviště musí mít k dispozici MPS pro pracovníky BEK během doby pro předání
UCA-36: VS (vedoucí stanoviště) nepředá požadavky na přesčas mezi pracovníky BEK, když jsou přesčasy potřebné [H-1, H-2, H-5]	C-36: VS musí mít k dispozici požadavky na přesčasy

Posledním krokem v posouzení STPA bylo posouzení ztrátových scénářů. Zde se dostáváme už do značných podrobností a ze strany dozorového orgánu nebude možné vždy prozkoumávat veškeré scénáře do detailu. I přesto mohlo být v této STPA posouzeno, zda byly scénáře stanoveny pro všechny UCAs. Tento požadavek splněn byl, dokonce většina UCAs má hned několik ztrátových scénářů a je tak patrné, že se autor pokusil jít skutečně do hloubky daného procesu BEK.

Celkově se posuzovaná STPA jeví jako zdařilá i přes zmíněné nedostatky. Často se jednalo o vynechání či chybné uvedení odkazů, pravděpodobně se však jedná pouze o přehlédnutí při přepisu mezi tabulkami v STPA. Dále by bylo žádoucí upravit některé formulace u řídicích akcí v řídicí struktuře. Nejzásadnějším nedostatkem jsou však některá nevhodně stanovená omezení řídicích prvků. Omezení mají být vztažena k řídicí akci, ke které je vytvořena konkrétní UCA. A jelikož je přesné stanovení bezpečnostních omezení kritické z pohledu bezpečnosti, jedná o skutečnost, u níž by ÚCL vyžadovalo nápravu od subjektu.

8.3 Posouzení ohodnocení rizik

Předchozí kapitola byla zaměřena na přiblížení posouzení STPA změny. Zde bude demonstrováno posouzení ohodnocení a zmírnění rizik na publikované práci MIT (A System-Theoretic Approach to Risk Analysis [23]). Ta aplikuje na ohodnocení rizik již zmíněnou SRM, která využívá výstupy STPA. Konkrétně byl posuzován přístup založený na nebezpečích. Ačkoliv na tomto příkladu již nemuselo být znovu představeno posouzení STPA, vzhledem k tomu, že jsou v tomto případě výstupy STPA využívány k ohodnocení a zmírnění rizik, některé kroky STPA zde musely být rovněž posouzeny. Jelikož se jedná o přístup založený na nebezpečích, prvotně muselo být posouzeno, zda se v tabulce pro ohodnocení a zmírnění rizik nachází všechna dílčí nebezpečí (respektive dílčí omezení). STPA byla vytvořena na příkladu hypotetického budoucího letounu s rotujícími nosnými plochami a bylo určeno 7 systémových nebezpečí. Ta byla dále specifikována na dílčí nebezpečí. V dalším kroku došlo k definování systémových omezení a dílčích omezení a právě v tomto místě byl nalezen nesoulad. Jak je patrné z tabulky 19, pro systémové nebezpečí H1.0 bylo určeno 8 dílčích nebezpečí a pro H2.0 pak 6 dílčích nebezpečí. Ačkoliv by mělo platit, že každé dílčí nebezpečí bude mít své dílčí omezení, v následující tabulce 20 je možné spatřit, že chybí dílčí omezení C1.8, C2.5 a C2.6. Stejný nedostatek byl identifikován u dílčích omezení pro nebezpečí H6.0, kde schází omezení C6.11 a C6.12. Při následném zhodnocení tabulky pro ohodnocení a zmírnění rizik bylo zjištěno, že tato dílčí omezení (respektive dílčí nebezpečí) tu byla rovněž vynechána.

Poté proběhla kontrola veškerých náležitostí ohodnocení a zmírnění rizik, jež byly popsány v kapitole 7.3. Pro dílčí omezení byl splněn požadavek, aby se v tabulce nacházely odkazy na související dílčí nebezpečí a u některých i příslušné ztrátové scénáře, které pod ně spadají. Při kontrole PMS, nebylo identifikováno, že by autoři hodnocení závažnosti podcenili, u rizik se vyskytovalo pouze PMS=1 (katastrofická) nebo

PMS=2 (kritická). Dále byla pozornost zaměřena na hodnoty MES přiřazené k jednotlivým zmírňujícím opatřením. Vzhledem k formulacím jednotlivých opatření se zdálo, že hodnoty MES byly správně určeny. Několik nesrovnalostí se však vyskytlo u hodnot CMES, což je znázorněno v tabulce 21. V prvním případě u C1.7 byla určena nižší hodnota CMES, než jaká skutečně měla být. Podle logiky vysvětlené v kapitole 7.1.2 se výsledná hodnota CMES určuje tak, že se sčítají hodnoty MES podle úrovně zmírnění. Tudíž v tomto případě by místo CMES=3 mělo být CMES=4. Ačkoliv zde došlo pouze k tomu, že si autoři zhoršili CMES z „Velmi efektivní" na „Středně efektivní", mělo by se to projevit i ve finální matici rizik, kde ještě při uvážení CPMS=2 spadá riziko do oranžového spektra matice, a tudíž do části, která již není z hlediska rizikovosti akceptovatelná. V druhém případě se jednalo o C7.5, kde naopak došlo k navýšení hodnoty CMES. Ačkoliv jsou zde dvě opatření s hodnotou MES=3, v úvahu se bere pouze jednou. Dále je tu opatření s MES=1, tudíž ve výsledku vychází CMES=4. Hodnoty PPMS se zdají být v pořádku nejen u C1.7 a C7.5, ale i u všech ostatních rizik. Stejně je tomu u výsledných hodnot CPMS, které byly spočítány správně. V závěru byla provedena kontrola finální SRM. Kontrola byla zaměřena na to, zda jsou v matici uvedena veškerá dílčí nebezpečí a jestli odpovídá jejich umístění v matici tomu, jaké jim byly určeny hodnoty CMES a CPMS. Finální SRM tak, jak byla uvedena ve zdrojovém dokumentu, je zobrazena v tabulce 22. Pouze do ní bylo doplněno dílčí nebezpečí H1.7, neboť v původní matici bylo opomenuto (proto je vyznačeno odlišnou barvou). Nicméně při zaměření na správnost umístění jednotlivých nebezpečí bylo zjištěno, že některá jsou umístěna v rozporu s hodnotami CMES nebo CPMS, které byly určeny v rámci ohodnocení a zmírnění rizik. Konkrétně se jednalo o H1.4, H2.3, H7.5. Opravená SRM je uvedena v tabulce 23 společně s barevným odlišením nebezpečí, která byla přemístěna. Nebezpečí H1.7 bylo přemístěno z důvodu nesprávně určené hodnoty CMES, což bylo rozebráno výše.

Celkově bylo nalezeno v ohodnocení a zmírnění rizik hned několik nedostatků. Jednalo se zprvu o vynechání některých dílčích omezení, která by zde rozhodně měla být stanovena, protože už v této fázi může být ohodnocení a zmírnění rizik bráno jako nekompletní. Dále se objevovaly nesprávně určené hodnoty CMES, které mohou konečné výsledky zkreslit. To samé platí o vynechání, případně špatném umístění dílčích nebezpečí do finální SRM. Jelikož je finální SRM uceleným obrazem všech rizik, je nutné, aby reflektovala kompletní a správné výsledky celého ohodnocení a zmírnění rizik. Z ní je na první pohled patrné, jaký je stav rizik po navržení zmírňujících opatření a jestli dojde ke splnění stanovených bezpečnostních cílů.

Tabulka 19: Dílčí nebezpečí pro systémová nebezpečí H1.0 a H2.0 (upraveno z [23])

Systémové nebezpečí		Dílčí nebezpečí		Odkaz na ztráty
H1.0	Letadlo je neovladatelné (S posádkou/Bezpilotní)	H1.1	Operátor je během letu nezpůsobilý	L1.0, L2.0, L3.0
		H1.2	Během bezpilotního letu jsou řídicí vstupy nedostatečné	L1.0, L2.0, L3.0
		H1.3	Zpětná vazba řídicího prvku/hardwaru je neadekvátní/nesprávná pro zachování ovladatelnosti	L1.0, L2.0, L3.0
		H1.4	Výkon komponent ovlivňuje funkce řídicího prvku	L1.0, L2.0, L3.0
		H1.5	Činnost nepřítele ohrožuje ovladatelnost	L1.0, L2.0, L3.0
		H1.6	Saturace/fixace/nepozornost úkolu operátora	L1.0, L2.0, L3.0
		H1.7	Nesprávná výměna řídicí pravomoci	L1.0, L2.0, L3.0
		H1.8	Konfigurace je pro letový provoz nevhodná	L1.0, L2.0, L3.0
H2.0	Je porušena strukturální integrita letadla	H2.1	Nedostatečný sběr/hlášení údajů o zdraví	L1.0, L2.0, L3.0
		H2.2	Neadekvátní řídicí algoritmy umožňují manévry přesahující strukturální omezení	L1.0, L2.0, L3.0
		H2.3	Saturace/fixace/nepozornost úkolu operátora	L1.0, L2.0, L3.0
		H2.4	Mentální model řídicích vstupů operátora je nesprávný	L1.0, L2.0, L3.0
		H2.5	Činnost nepřítele narušuje strukturální integritu	L1.0, L2.0, L3.0
		H2.6	Výkon součásti ovlivňuje strukturální integritu	L1.0, L2.0, L3.0

Tabulka 20: Dílčí omezení pro dílčí nebezpečí k H1.0 a H2.0 (upraveno z [23])

Dílčí nebezpečí	Dílčí omezení	
H1.1	C1.1	Vstupy do řízení musí být přiměřené k udržení řiditelnosti letadla pro let s posádkou
H1.2	C1.2	Vstupy řízení musí být přiměřené k udržení řiditelnosti letadla pro bezpilotní let
H1.3	C1.3	Zpětná vazba řídicího prvku/hardwaru musí být přiměřená pro udržení ovladatelnosti
H1.4	C1.4	Architektura řízení letadla nesmí být citlivá na činnost nepřítele
H1.5	C1.5	Řídicí pravomoc pro letové systémy musí být řádně vyměněna
H1.6	C1.6	Konfigurace musí být vhodná pro letový provoz
H1.7	C1.7	Bezpečnostní opatření letadla nesmí ovlivnit ovladatelnost během letového provozu
H1.8	C1.8	-
H2.1	C2.1	Postupy údržby/shromažďování údajů o zdraví musí být přiměřené pro zachování strukturální integrity
H2.2	C2.2	Řídicí algoritmy musí zabránit tomu, aby manévry překročily strukturální omezení
H2.3	C2.3	Zpětná vazba řídicího prvku/hardwaru musí být přiměřená pro zachování strukturální integrity
H2.4	C2.4	Konstrukce letadla nesmí být náchylná k činnosti nepřítele
H2.5	C2.5	-
H2.6	C2.6	-

Tabulka 21: Hodnocení a zmírnění rizik H1.7 a H7.5 (upraveno z [23])

Dílčí omezení		Dílčí nebezpečí	PMS	RM ID	Doporučené zmírnění (Recommended Mitigation)	MES	CMES	PPMS	CPMS
C1.7	Bezpečnostní opatření letadla nesmí ovlivnit ovladatelnost během letového provozu	H1.7	1	RM07	Poskytnout FO (Flight Operator - operátor letu) přímé ovládání hardwaru, který obchází ASEC (Aircraft Software Enabled Controller) a/nebo umožňuje FO resetovat systém (panely jističů, vypínače atd.)	3	3	2	2
				RM04	FO vyškolit ve správných předletových/letových/nouzových postupech a technikách (např. správné používání kontrolního seznamu, výcvik na simulátoru, letové manévry, stanovení priorit v případě nouze, týmové postupy, údržba, zbrojní postupy atd.)	1		2	
C7.5	Kritické informace musí být chráněny proti nepřátelské akci	H7.5	1	RM18	Vyžadovat ruční vstup od FO k ověření/potvrzení doporučené odezvy systému pro všechny funkce související s kritickými informacemi	3	6	2	2
				RM06	Navrhnout autonomní řídicí systém tak, aby byl odolný proti zaseknutí a falšování	3		3	
				RM04	FO vyškolit ve správných předletových/letových/nouzových postupech a technikách (např. správné používání kontrolního seznamu, výcvik na simulátoru, letové manévry, stanovení priorit v případě nouze, týmové postupy, údržba, zbrojní postupy atd.)	1		2	

Tabulka 22: Původní SRM (upraveno z [23])

Dílčí nebezpečí					
Nejméně efektivní	0				
Mírně efektivní	1				
Středně efektivní	2-3		1.7	4.4, 4.5, 6.1, 6.3,	
Velmi efektivní	4-5			1.2, 1.3, 2.3, 2.4, 3.3, 4.1, 6.7, 6.10,	
Nejefektivnější	6		6.2, 6.4, 7.4, 7.5,	1.4, 2.1, 4.2, 5.1, 5.2, 6.8,	
Eliminováno	N/A	1.1, 1.5, 1.6, 2.2, 3.1, 3.2, 3.4, 4.3, 5.3, 6.5, 6.6, 6.9, 7.1, 7.2, 7.3, 7.6,			
CMES		1	2	3	4
	CPMS	Katastrofická	Kritická	Nízká	Zanedbatelná

Tabulka 23: Opravená SRM (upraveno z [23])

Dílčí nebezpečí					
Nejméně efektivní	**0**				
Mírně efektivní	**1**				
Středně efektivní	**2-3**			4.4, 4.5, 6.1, 6.3,	
Velmi efektivní	**4-5**		1.7, 2.3, 7.5,	1.2, 1.3, 2.4, 3.3, 4.1, 6.7, 6.10,	
Nejefektivnější	**6**		1.4, 6.2, 6.4, 7.4,	2.1, 4.2, 5.1, 5.2, 6.8,	
Eliminováno	**N/A**	1.1, 1.5, 1.6, 2.2, 3.1, 3.2, 3.4, 4.3, 5.3, 6.5, 6.6, 6.9, 7.1, 7.2, 7.3, 7.6,			
CMES		**1**	**2**	**3**	**4**
	CPMS	Katastrofická	Kritická	Nízká	Zanedbatelná

8.4 Stanovení předpokladů a proaktivních indikátorů pro účely ÚCL

Ačkoliv je u plánovaných změn zásadní jejich prvotní posouzení před schválením pro zavedení do provozu, podstatné rovněž je, aby bylo dále sledováno a vyhodnocováno, jak si změna vede v provozu. K tomu by měly ÚCL sloužit předpoklady o daném systému a na ně navázané proaktivní indikátory, což bylo přiblíženo v kapitole 7.3. Pro představu byly vytvořeny předpoklady na základě STPA na bezpečnostní kontrolu z diplomové práce Ing. Kohoutka (Ověření modelu STAMP v procesech bezpečnostní kontroly [24]), které jsou uvedeny v příloze 5. Předpoklad k systémovému omezení SC-2 byl vynechán z toho důvodu, že systémové nebezpečí H-2 bylo v kapitole 8.2 v rámci posouzení STPA určeno jako dílčí nebezpečí k H-1.

V tabulce 24 je představen příklad předpokladů, které byly vytvořeny na základě systémového omezení *SC-3* (*Pravidla plánování musí být vždy dodržena*). Podobně jako u vytváření návrhu předpokladů (respektive proaktivních indikátorů) pro subjekt, i zde se vycházelo z úvahy, že zmíněné omezení může být splněno, i přesto však může dojít k nežádoucí události, pokud jsou požadavky pro plánování směn bezpečnostní kontroly nedostatečné z hlediska vytížení pracovníků, nebo pokud jsou dostačující, ale nejsou využity při plánování směn. Na základě toho byly stanoveny dva předpoklady ke zmíněnému omezení (*Požadavky pro plánování směn bezpečnostní kontroly jsou dostačující z hlediska vytížení pracovníků*, *Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky*). Při srovnání uvedených předpokladů pro ÚCL s předpoklady, které byly stanoveny pro subjekt v kapitole 8.1 k SC-3.1 (*Požadavky na minimální počet přestávek na jednoho pracovníka BEK jsou dostačující*

pro odpočinek pracovníka. Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na minimální počet přestávek na jednoho pracovníka BEK.) je patrný rozdíl v detailu předpokladů (proaktivních indikátorů) pro subjekt a pro ÚCL. V tomto případě je u subjektu blíže specifikováno, o jaký se jedná požadavek v rámci plánování směn (zde minimální počet přestávek). Pro ÚCL jsou předpoklady formulovány obecněji a pokrývají veškeré požadavky pro plánování směn z hlediska vytížení pracovníků, tudíž kromě minimálního počtu přestávek rovněž maximální počet směn (dle SC-3.2), maximální počet přesčasů (dle SC-3.3) a maximální počet nočních směn jdoucích za sebou (dle SC-3.4). Pro vyhodnocení takto nastavených obecnějších předpokladů však ÚCL může využít výsledky vyhodnocení detailnějších předpokladů od subjektu. Pokud by byl alespoň jeden z těchto detailních předpokladů subjektu porušen, obecnější předpoklad ÚCL by byl brán rovněž jako porušený. Ačkoliv zde byl ukázán možný rozdíl v detailu předpokladů pro subjekt a ÚCL, vždy záleží na konkrétní situaci a na systému, kterého se dozorová činnost bude týkat. Neboť i ÚCL může mít své proaktivní indikátory nastaveny ve větším detailu, pokud to uzná za vhodné.

Co se týká způsobu sledování proaktivního indikátoru a tím zároveň sledování platnosti daného předpokladu, Úřad může využít *Kontroly, inspekce či audity*, které na bezpečnostní kontrole provádí. Vzhledem k faktu, že ÚCL provádí dozorovou činnost nad subjekty, jeho přímý vliv na udržení platnosti předpokladu skrze formovací akce (shaping action) bude ve většině případů opět prostřednictvím *Provádění kontrol/inspekcí a auditů*. Zajišťovací akcí (hedging action) může být *Upozornění/doporučení dle příslušné situace*, ve smyslu informování subjektu o zjištěné skutečnosti a vyžádání nápravy, dále *Zvýšení frekvence kontrol/auditů/inspekcí BEK* a případná *Kontrola nápravné činnosti*, pokud byla doporučena. Kontroly předpokladů by měly být spuštěny během *Plánovaných změn postupů BEK*.

Tabulka 24: Předpoklady (proaktivní indikátory) pro účely ÚCL k SC-3

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování	Hedging action
SC-3	Požadavky pro plánování směn bezpečnostní kontroly jsou dostačující z hlediska vytížení pracovníků.	Kontroly/inspekce/audity BEK ze strany ÚCL	Upozornění/doporučení dle příslušné situace. Zvýšení frekvence kontrol/auditů/inspekcí BEK. Kontrola nápravné činnosti.
		Shaping action	**Signposts**
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky.	Provádění kontrol/inspekcí/auditů BEK	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)

8.5 Validace ve spolupráci s ÚCL

Práce byla vytvořena v koordinaci s projektem CK01000073 „Digitalizace integrovaného dozoru nad bezpečností leteckých organizací“ s podporou Technologické agentury ČR. Navíc byly od ÚCL poskytnuty podklady potřebné pro přiblížení jejich současného přístupu k řízení plánovaných změn. Z důvodu časové náročnosti nebylo možné navržený postup zavést do praxe a ověřit v reálných procesech SSP. Zároveň je zde veliký krok mezi současným přístupem státního dozoru a tím, jakým způsobem je řízení plánovaných změn navrženo v této práci. Nicméně i přesto, že ÚCL v současné době nevyužívá systémový přístup k bezpečnosti a ani ho nevyžaduje po subjektech civilního letectví, staví se k tomuto přístupu pozitivně.

9 Diskuze

Pro dnešní neustále se dynamicky rozvíjející svět letecké dopravy je z hlediska prosperity nezbytné, aby docházelo k plánovaným změnám. Zároveň se neustále zvyšuje komplexita systémů, což činí značnou výzvu nejen z hlediska porozumění systémům, které se tak jeví jako náročnější, ale rovněž v kontextu toho, že jakákoliv plánovaná změna v komplexním systému znamená kritickou fázi z pohledu bezpečnosti daného systému. Kombinace zvyšující se komplexity systémů a nutnosti dokázat se vypořádat s plánovanými změnami adekvátním způsobem vytváří značné nároky na oblast bezpečnosti v letectví, a to nejen na jednotlivé subjekty civilního letectví, ale především také na dozorové orgány.

Systémový přístup k bezpečnosti je obecně poměrně nový přístup, jehož využití v praxi je nutné stále více rozvíjet. Vzhledem k tomu, že se zaměřuje na systém jako celek, jeví se jako ideální pro provázané a komplexní systémy, které jsou pro letectví typické. Navíc související systémové analýzy, jako například STPA, umožňují velmi podrobné pochopení konkrétního systému, což z hlediska bezpečnosti přináší značné výhody, neboť v rámci identifikace nebezpečí je možné s využitím řídicí struktury, identifikovaných nebezpečných řízení a ztrátových scénářů porozumět širšímu kontextu případného problému. Ačkoliv se však může zdát, že takto podrobné analýzy vyžadují značně více času na provedení, než je tomu u jiných analýz, u systémového přístupu jde zejména o pochopení jeho podstaty a o porozumění jednotlivým analýzám. Následná časová náročnost je s jinými analýzami srovnatelná, nicméně vždy je ovlivněna především složitostí konkrétního systému.

Využití systémových analýz, konkrétně STPA a Active STPA, se jeví jako přínosné i v rámci řízení plánovaných změn. Plánované změny mohou do systémů vnášet nová nebezpečí, měnit stávající nebezpečí, a proto vyžadují detailní posouzení z hlediska bezpečnosti ještě před tím, než jsou zavedeny do provozu. Avšak jak z pohledu subjektů civilního letectví, tak z pohledu dozorového orgánu, představuje systémový přístup a zejména analýzy STPA a Active STPA způsob, jak nejen posoudit plánované změny do detailu v kontextu celého systému, ale také jak sledovat a vyhodnocovat chování plánované změny v provozu například skrze předpoklady a související proaktivní indikátory.

V rámci státního dozoru má ÚCL odpovědnost za schvalování konkrétních plánovaných změn subjektů. Pro demonstraci jejich současného přístupu k řízení plánovaných změn byly využity směrnice, které problematiku schvalování plánovaných změn popisovaly.

Bylo zjištěno, že se sepsané postupy pro schvalování plánovaných změn u různých subjektů lišily, ačkoliv tomu v reálném provozu tak nemusí být. Sjednocení postupů společně s aplikací systémového přístupu k bezpečnosti se zde zdá být žádoucí, neboť by právě ÚCL mělo být tím, kdo půjde v tomto směru ostatním subjektům civilního letectví příkladem. Proto byl vytvořen postup, který zasazuje systémový přístup k bezpečnosti (především STPA a Active STPA) do metodiky SAM.

Ačkoliv se využití metodiky SAM dá předpokládat především u samotných subjektů, které ji mohou využít pro posouzení bezpečnosti dané změny, z pohledu ÚCL je využití SAM rovněž praktické. Jedním z důvodů je zejména struktura této metodiky s jasně vymezeným postupem. Její jednotlivé fáze (FHA, PSSA, SSA) mají své dané vstupy, procesní kroky a výstupy, což vytváří logicky uspořádaný ucelený proces, který v kombinaci s analýzami STPA a Active STPA umožňuje systémovou práci s plánovanými změnami.

Nad rámec práce byla zároveň představena nová matice rizik od MIT, která využívá výstupy z STPA. I zde se jedná o perspektivní návrh, neboť bere v úvahu to, že často nejsou dostupná historická data pro konkrétní typ změny, a tím pádem v případě hodnocení pravděpodobnosti převažuje obvykle subjektivní pohled hodnotitele, což může konečné výsledky značně zkreslit. Matice rizik s využitím výstupů z STPA místo toho upřednostňuje hodnocení účinnosti zmírnění konkrétního rizika. Z pohledu ÚCL by posuzování výstupů z nového způsobu hodnocení a zmírnění rizik nepřineslo zásadní změny. Pouze by se jednalo o nastudování nové matice rizik.

Mimo to se v navrženém postupu pracuje i s tím, jakým způsobem má být plánovaná změna řízena následně v provozu, pokud je dozorovým orgánem schválena. Neboť i když je pro plánovanou změnu stěžejní její posouzení ze strany subjektu i ÚCL před zavedením do provozu, nemohou být subjektem předvídány veškeré situace, které mohou v kontextu dané změny nastat. Stejně tak není možné, aby ÚCL při posuzování dokumentace od subjektu identifikovalo veškeré případné skutečnosti, které subjekt mohl opomenout. ÚCL má zodpovědnost za dozor nad celým civilním letectvím České republiky, a tudíž nemůže znát každý detail systémů spadajících do činnosti jednotlivých subjektů. I přesto však může být zajištěno sledování a vyhodnocování změny v provozu skrze stanovené předpoklady a proaktivní indikátory, a to jak pro subjekt, tak pro ÚCL. Lišily by se mírou detailu, neboť pro ÚCL by postačily předpoklady a proaktivní indikátory vycházející z nejvyšší úrovně daného systému.

Celkově se navržený postup řízení plánovaných změn jeví jako přínosný pro dozorovou činnost ÚCL. Je strukturovaný, logicky uspořádaný a využívá systémový přístup k bezpečnosti, čím umožňuje lepší pochopení plánované změny v kontextu celého systému. Systémové analýzy jsou zde přínosné především díky míře detailu, do které se v systému dostávají, a díky svým jasně stanoveným krokům, které začínají na nejvyšší úrovni systému a končí až v úplném detailu. Každý, kdo s výstupy analýz pracuje, si tak najde svou potřebnou míru detailu.

Pro ÚCL zároveň může přijetí nového postupu pro řízení plánovaných změn znamenat určité překážky, které je potřeba vzít v potaz. Jednou z nich je zcela jistě pochopení podstaty systémového přístupu a souvisejících analýz, což se může jevit jako časově náročné. Z hlediska počtu pracovníků se dá předpokládat, že nebude nutné navýšit jejich počet, nicméně tento aspekt může být zhodnocen až při skutečném zavedení navrženého postupu do provozu. Největší výzvou však pro dozorový orgán nebude přijetí systémového přístupu k bezpečnosti, neboť k němu se staví pozitivně, ale především jeho zavedení do každodenní činnosti.

Je však důležité vyzdvihnout výhody, které tato změna přinese. ÚCL získá větší kontrolu nad subjekty civilního letectví ve smyslu lepšího porozumění tomu, jakým způsobem by v kontextu dané plánované změny mohlo u subjektu dojít k nežádoucím událostem (incidentům, nehodám) a v souvislosti s tím, na co by se měl Úřad v rámci dozorové činnosti u konkrétního subjektu zaměřit. Celkově tak systémový přístup umožní včasnou detekci případných slabin plánované změny, a tím předejít vzniku incidentů a nehod, což je žádoucí nejen z hlediska snížení výdajů za případné nežádoucí události, ale zcela jistě se to pozitivně odrazí na úrovni bezpečnosti civilního letectví.

Součástí návrhu bylo navíc navržení klíčových prvků SSP pro řízení plánovaných změn. Pokud by byla zachována současná struktura SSP dle dokumentu ICAO Doc. 9859, postup pro řízení plánovaných změn by byl popsán v komponentu „Zajištění bezpečného provozu na úrovni státu“ v rámci prvku „Řízení změn“. Z vytvořeného návrhu vyplývají stěžejní kroky pro adekvátní systémové posouzení plánovaných změn z hlediska bezpečnosti a jejich následné sledování a vyhodnocování v provozu, a tudíž by bylo žádoucí tyto kroky do SSP zakomponovat. Neboť plánované změny jsou zcela jistě kritickou fází z pohledu bezpečnosti a měla by jim být věnována v rámci SSP patřičná pozornost.

10 Závěr

Diplomová práce byla zaměřena na vytvoření návrhu postupu a klíčových prvků státního programu bezpečnosti pro řízení plánovaných změn v leteckém provozu s využitím systémového přístupu k bezpečnosti. K dosažení tohoto cíle však bylo nutné nastudovat příslušnou teorii k dané problematice. Nejprve byla prozkoumána legislativní stránka státních programů bezpečnosti, na což navázalo přiblížení ÚCL jako dozorového orgánu se zaměřením na jeho činnosti.

Vzhledem k zaměření na problematiku řízení plánovaných změn byly prostudovány přístupy k jejich řízení s bližší specifikací přístupu ICAO popsaném v Safety Management Manual a dále metodiky SAM. V rámci SAM došlo k podrobnému seznámení s jednotlivými fázemi FHA, PSSA a SSA.

Následně byla řešena problematika systémového přístupu k bezpečnosti. Zde byly rozebrány teorie Safety-I, Safety-II a Safety-III a poté byl přiblížen bezpečnostní model založený na systémové teorii – STAMP. V kontextu STAMP byly prostudovány související analýzy STPA, Active STPA a CAST. V návaznosti na STPA došlo k bližší analýze problematiky stanovení předpokladů a proaktivních indikátorů.

Pro přiblížení současného přístupu ÚCL k řízení plánovaných změn byly vybrány pouze dva konkrétní příklady dozoru nad subjekty civilního letectví, neboť vzhledem k rozsahu práce nebylo možné prostudovat veškerou dokumentaci zahrnující řízení plánovaných změn (směrnice, příručky). Byl vybrán proces zavádění změn na letištích certifikovaných podle EASA a jako druhý proces týkající se dohledu nad řízením změn u poskytovatelů služeb. Na těchto příkladech byla představena úskalí současného přístupu a možný prostor pro zlepšení.

Na základě zjištění potřebných informací a pochopení současného přístupu ÚCL mohl být následně vytvořen návrh postupu pro řízení plánovaných změn ze strany ÚCL s využitím systémového přístupu k bezpečnosti. Podstatou byla kombinace metodiky SAM společně s metodami STPA a Active STPA. Metodika SAM vnesla do postupu pevně danou logicky uspořádanou strukturu, STPA a Active STPA představovaly systémový přístup k bezpečnosti. V rámci navrženého postupu byla vyzdvižena potřeba zakomponování systémového přístupu rovněž do požadavků po subjektech civilního letectví. V tomto směru byla doporučena aplikace STPA pro analýzu plánované změny. V kontextu využití STPA byla představena nová matice rizik, která používá výstupy z STPA. Dále byly popsány jednotlivé fáze postupu pro řízení změn – FHA, PSSA, SSA.

Během představení fáze FHA bylo především popsáno, jakým způsobem by ÚCL posuzovalo výstupy z STPA změny a bezpečnostní cíle. Fáze PSSA se zaměřovala zejména na posouzení ohodnocení a zmírnění rizik (rovněž s uvážením nové matice rizik) a v případě schválení plánované změny také na stanovení předpokladů a proaktivních indikátorů k dané změně. V SSA došlo k vysvětlení, jakým způsobem by ÚCL sledovalo a vyhodnocovalo změnu v provozu prostřednictvím sběru dat z příslušných datových zdrojů a skrze následné vyhodnocování platnosti stanovených předpokladů. Dále je zde zmíněna případná potřeba provedení Active STPA, ať už pouze ze strany subjektu nebo také ze strany ÚCL, pokud je to dle situace nutné.

V závěru práce bylo nezbytné ověřit použití navrženého postupu. To bylo provedeno s využitím již vytvořené STPA na bezpečnostní kontrolu na letišti od Ing. Kohoutka a publikované práce z MIT, která představovala na praktickém příkladu aplikaci nové matice rizik. Na vytvořené STPA bylo představeno dotvoření potřebných vstupů od subjektu – stanovení bezpečnostních cílů, ohodnocení a zmírnění rizik a nastavení předpokladů a proaktivních indikátorů. Následně bylo přiblíženo, jakým způsobem by tuto STPA hodnotil Úřad. Posouzení hodnocení a zmírnění rizik na dotčené STPA nemohlo být demonstrováno, neboť v této práci bylo hodnocení a zmírnění rizik teprve dotvářeno, a tudíž by zde chyběl nezávislý pohled. Proto bylo posouzení hodnocení a zmírnění rizik představeno na publikované práci z MIT. Poté mohlo dojít k ukázce stanovení předpokladů a proaktivních indikátorů pro Úřad, k čemuž opět byla využita STPA na BEK, neboť k ní byly vytvořeny také předpoklady a proaktivní indikátory pro letiště a mohlo tak dojít ke srovnání předpokladů a proaktivních indikátorů subjektu a dozorového orgánu. V neposlední řadě bylo vysvětleno, jakým způsobem proběhla validace ve spolupráci s ÚCL.

Nakonec došlo k diskuzi dosažených výsledků společně s hodnocením, jaké jsou přínosy navrženého postupu pro dozorový orgán a limitace této práce. Za přínos se dá považovat zejména vytvoření postupu, který je oproti současnému jasně strukturovaný a může být použitý pro řízení plánovaných změn napříč všemi odděleními ÚCL bez ohledu na to, o jaký subjekt se v daném případě jedná. Zároveň byl do postupu zakomponován systémový přístup k bezpečnosti, který umožňuje neustále posouvat hranice úrovně bezpečnosti v letectví.

Na druhou stranu zde vzniká značná výzva pro dozorový orgán a tou je právě aplikace systémového přístupu k bezpečnosti do řízení plánovaných změn. Navržený postup

pracuje se systémovými analýzami (STPA, Active STPA), které doposud ÚCL nevyužívá. Zároveň postup přichází s myšlenkou stanovení a vyhodnocování předpokladů a souvisejících proaktivních indikátorů plánované změny, což vytváří požadavek na dodatečné aktivity v rámci řízení plánovaných změn, které doposud vykonávány nebyly.

Z výše uvedených limitací je zjevné, že prvotním krokem ze strany ÚCL by měla být aplikace principů systémového přístupu k bezpečnosti společně se souvisejícími analýzami v rámci dozorových činností dle SSP. Ačkoliv v této práci byla řešena problematika řízení plánovaných změn, dozorových činností, které mají být dle SSP Úřadem vykonávány, je znatelně více a jsou všechny propojeny. Tudíž by bylo žádoucí aplikovat systémový přístup nejen do procesu řízení plánovaných změn v rámci SSP, ale také do souvisejících činností, jako je sběr a zpracování dat, auditní činnost apod. Mimo to by bylo vhodné navržený postup pro řízení plánovaných změn ověřit v reálných procesech ÚCL, neboť to nemohlo být z důvodu časové náročnosti provedeno v rámci této práce.

Zdroje

[1] MINISTERSTVO DOPRAVY ČR. Předpis L19. Řízení bezpečnosti. 2013 [online]. [cit. 22.10.2021]. Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm

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

[3] ÚŘAD PRO CIVILNÍ LETECTVÍ. Organizační struktura ÚCL 02/2019 [online]. [cit. 22.10.2021]. Dostupné z: https://www.caa.cz/wp-content/uploads/2020/11/organizacnistruktura.pdf?cb=30c38131a598d7123a0697f9162dd02c

[4] ÚŘAD PRO CIVILNÍ LETECTVÍ. Organizační struktura [online]. [cit. 22.10.2021]. Dostupné z: https://www.caa.cz/urad-pro-civilni-letectvi/organizacni-struktura/

[5] Organization of civil aviation in the Czech Republic - Civil Aviation Authority of the Czech Republic. Úřad pro civilní letectví [online]. 2020 [cit. 29.11.2021]. Dostupné z: https://www.caa.cz/en/authority/organization-of-civil-aviation-in-the-czech-republic/

[6] LEVESON, Nancy G. a John P. THOMAS. STPA handbook [online]. [cit. 03.11.2021]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[7] LEVESON, Nancy G. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. [cit. 03.11.2021]. ISBN 978-0-262-01662-9.

[8] Management of Change. SKYbrary Aviation Safety [online]. [cit. 2021-11-04]. Dostupné z: https://www.skybrary.aero/index.php/Management_of_Change

[9] Review of techniques to support the EATMP safety assessment methodology. EUROCONTROL: EUROCONTROL EXPERIMENTAL CENTRE [online]. 2004 [cit. 2021-11-28]. Dostupné z: https://www.eurocontrol.int/sites/default/files/library/001a_Techniques_to_Support_EATMP_SAM.pdf

[10] EUROCONTROL Safety Assessment Methodology (SAM). SKYbrary Aviation Safety [online]. [cit. 2021-11-28]. Dostupné z: https://skybrary.aero/articles/eurocontrol-safety-assessment-methodology-sam

[11] Air Navigation System Safety Assessment Methodology-SAM: Guidance Material for the application of SAM. Civil Aviation Authority of Kosovo [online]. 2011 [cit. 2021-11-28]. Dostupné z: https://caa.rks-gov.net/wp-content/uploads/2016/04/TP-12-Guidance-material-for-the-application-of-SAM-1.pdf

[12] Air Navigation System Safety Assessment Methodology. EUROCONTROL Safety Assessment Methodology Task Force (SAMTF), 2006.

[13] A White Paper on Resilience Engineering for ATM [online]. EUROCONTROL [online]. 2009 [cit. 2021-12-04]. Dostupné z: https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf

[14] HOLLNAGEL, Erik. Safety-I and Safety-II. The Past and Future of Safety Management. Taylor & Francis Group, 2014 [cit. 2021-12-05]. ISBN 978-1-4724-2306-1

[15] HOLLNAGEL, Erik, Robert L WEARS a Jeffrey BRAITHWAITE. From Safety-I to Safety-II: A White Paper [online]. [cit. 2021-12-05]. Dostupné z: https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf

[16] LEVESON, Nancy G., Safety III: A Systems Approach to Safety and Resilience. MIT, Cambridge, 2020 [online]. [cit. 2021-12-05]. Dostupné z: http://sunnyday.mit.edu/safety-3.pdf

[17] 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. Vedoucí práce Prof. Nancy G. Leveson.

[18] LEVESON, Nancy G. CAST Handbook: How to Learn More from Incidents and Accidents [online]. 2019 [cit. 2021-12-16]. Dostupné z: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[19] ÚŘAD PRO CIVILNÍ LETECTVÍ. Směrnice CAA/S-SP-005-0/2017: Směrnice pro zavádění změn na letištích certifikovaných podle EASA. 2. vydání. Praha, 2018.

[20] ÚŘAD PRO CIVILNÍ LETECTVÍ. Evropská agentura pro bezpečnost letectví. Přijatelné způsoby průkazu (AMC) a poradenský materiál (GM) k požadavkům na úřady, organizace a provoz pro letiště. 2021.

[21] ÚŘAD PRO CIVILNÍ LETECTVÍ. Formulář bezpečnostního posouzení. Bezpečnostní posouzení. 2019.

[22] ÚŘAD PRO CIVILNÍ LETECTVÍ. Směrnice CAA/S-SP-009-3/2019: Dohled nad řízením změn u poskytovatelů služeb a u organizací pro výcvik řídících letového provozu. 4. vydání. Praha, 2021.

[23] GREGORIAN, Dro J. a Sam M. YOO. A System-Theoretic Approach to Risk Analysis. 2021. Diplomová práce. Massachusetts Institute of Technology. Vedoucí práce Prof. Nancy G. Leveson.

[24] KOHOUTEK, Adam. Ověření modelu STAMP v procesech bezpečnostní kontroly. Praha, 2021. České vysoké učení technické v Praze. Diplomová práce. Vedoucí práce: Ing. Roman Vokáč, Ph.D. a doc. Ing. Andrej Lališ, Ph.D.

Příloha 1 – Dílčí nebezpečí a dílčí omezení

Systémové nebezpečí		Dílčí nebezpečí		Odkaz na ztráty
H-1	Bezpečnostní kontrola nepokryje provoz	H-1.1	Neprovedení přerozdělení kapacit v případě zpoždění některého z letů	[L-1, L-2, L-4]
		H-1.2	Neobsazení požadovaných pozic v případě nouzové situace.	[L-1, L-2, L-4]
H-2	Bezpečnostní kontrola nezaručí dostatek pracovníků BEK	H-2.1	Přiřazení pracovníků bez provedení kontroly dostatečnosti jejich počtu	[L-1, L-2, L-3, L-4]
H-3	Nedodržení pravidel pro plánování	H-3.1	Nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	[L-1, L-4]
		H-3.2	Překročení maximálního počtu směn na jednoho pracovníka BEK	[L-1, L-4]
		H-3.3	Překročení maximálního počtu přesčasů na jednoho pracovníka BEK	[L-1, L-4]
		H-3.4	Překročení maximálního počtu nočních směn jdoucích za sebou na jednoho pracovníka BEK	[L-1, L-4]
H-4	Při plánování dojde k překročení FPD (Fond pracovní doby)	H-4.1	Plánování bude provedeno bez přizpůsobení stanovenému FPD	[L-1]
		H-4.2	Čerpání FPD neproběhne s uvážením veškerých náležitostí (křivka cestujících během roku apod.)	[L-1]
H-5	Nedostatečná bezpečnostní kontrola	H-5.1	Vykonání bezpečnostní kontroly bez dodržení veškerých stanovených postupů a pravidel	[L-1, L-2, L-3, L-4]
		H-5.2	Opomenutí některých úkonů v rámci bezpečnostní kontroly	[L-1, L-2, L-3, L-4]

Dílčí nebezpečí	Dílčí omezení	
H-1.1	SC-1.1	V případě zpoždění některého z letů musí být provedeno přerozdělení kapacit
H-1.2	SC-1.2	V případě nouzové situace musí být možné obsadit požadované pozice
H-2.1	SC-2.1	Přiřazení pracovníků musí proběhnout spolu s provedením kontroly dostatečnosti jejich počtu
H-3.1	SC-3.1	Musí být dodržen minimální počet přestávek na jednoho pracovníka BEK
H-3.2	SC-3.2	Nesmí být překročen maximální počet směn na jednoho pracovníka BEK
H-3.3	SC-3.3	Nesmí být překročen maximální počet přesčasů na jednoho pracovníka BEK
H-3.4	SC-3.4	Nesmí být překročen maximální počet nočních směn jdoucích za sebou na jednoho pracovníka BEK
H-4.1	SC-4.1	Plánování musí být provedeno s připůsobením stanovenému FPD
H-4.2	SC-4.2	Čerpání FPD musí proběhnout s uvážením veškerých náležitostí (křivka cestujících během roku apod.)
H-5.1	SC-5.1	Vykonání bezpečnostní kontroly musí proběhnout s dodržením veškerých stanovených postupů a pravidel
H-5.2	SC-5.2	Nesmí být opomenuty žádné úkony v rámci bezpečnostní kontroly

Příloha 2 – Bezpečnostní cíle

ID nebezpečí	Popis	Závažnost (PMS)	Bezpečnostní cíl (dle CMES)
H-1.1	Neprovedení přerozdělení kapacit v případě zpoždění některého z letů	1	6
H-1.2	Neobsazení požadovaných pozic v případě nouzové situace	1	6
H-2.1	Přiřazení pracovníků k jednotlivým úlohám bez provedení kontroly dostatečnosti jejich počtu pro danou úlohu	1	6
H-3.1	Nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	2	4-5
H-3.2	Překročení maximálního počtu směn na jednoho pracovníka BEK	2	4-5
H-3.3	Překročení počtu přesčasů na jednoho pracovníka BEK	2	4-5
H-3.4	Překročení maximálního počtu nočních směn jdoucích za sebou na jednoho pracovníka BEK	2	4-5
H-4.1	Plánování bude provedeno bez přizpůsobení stanovenému FPD	2	4-5
H-4.2	Čerpání FPD neproběhne s uvážením veškerých náležitostí (křivka cestujících během roku apod.)	2	4-5
H-5.1	Vykonání bezpečnostní kontroly bez dodržení veškerých stanovených postupů a pravidel	1	6
H-5.2	Opomenutí některých úkonů v rámci bezpečnostní kontroly	1	6

Příloha 3 – Hodnocení a zmírnění rizik

Odkaz na nebezpečí	PMS	RM ID	Doporučené zmírnění (Recommended Mitigation)	Úroveň zmírnění (Mitigation Level)	MES	CMES	PPMS	CPMS
H-1.1	1	RM01	Zavedení algoritmu pro vyhodnocení přerozdělení kapacit v případě zpoždění některého z letů.	Snížení prostřednictvím návrhu systému	3	6	4	3
		RM02	Dvojí kontrola možnosti přerozdělení kapacit v případě zpoždění některého z letů.	Detekováno s odezvou	2		3	
		RM03	Školení pracovníků ohledně jejich odpovědností (přerozdělení kapacit v případě zpoždění letů, obsazení pozic v případě nouzové situace apod.)	Školení a postupy	1		2	
H-1.2	1	RM04	Zavedení algoritmu pro vyhodnocení obsazení pozic v případě nouzové situace.	Snížení prostřednictvím návrhu systému	3	6	4	3
		RM05	Dvojí kontrola schopnosti obsadit požadované pozice v případě nouzové situace.	Detekováno s odezvou	2		3	
		RM03	Školení pracovníků ohledně jejich odpovědností (přerozdělení kapacit v případě zpoždění letů, obsazení pozic v případě nouzové situace apod.)	Školení a postupy	1		2	
H-2.1	1	RM06	Zavedení přímé zpětné vazby pracovníků BEK na dispečera DEP, aby bylo pracovníkům umožněno v případě nedostatečného počtu pracovníků informovat dispečera DEP o této skutečnosti.	Snížení prostřednictvím návrhu systému	3	4	3	2
		RM07	Školení dispečera DEP ohledně jeho odpovědností (přiřazení pracovníků k jednotlivým pracovním úlohám apod.)	Školení a postupy	1		2	
		RM08	Vytvoření podkladů pro dispečera DEP za účelem individuální kontroly plnění jeho odpovědností (kontrola dostatečnosti počtu pracovníků v rámci jednotlivých úloh apod.)	Školení a postupy	1		3	
H-3.1	2	RM09	Navržení programu, který zabrání tomu, aby během plánování došlo k nedodržení/překročení stanovených limitů (nedodržení minimálního počtu přestávek apod.)	Eliminováno	ELIM	ELIM	4	3
		RM10	Kontrola ze strany pracovníků BEK a případné upozornění dispečera DEP v případě zjištění nedodržení minimálního počtu přestávek na jednoho pracovníka BEK	Detekováno s odezvou	2		4	
		RM07	Školení dispečera DEP ohledně jeho odpovědností (přiřazení pracovníků k jednotlivým pracovním úlohám apod.)	Školení a postupy	1		2	
H-3.2	2	RM09	Navržení programu, který zabrání tomu, aby během plánování došlo k nedodržení/překročení stanovených limitů (nedodržení minimálního počtu přestávek apod.)	Eliminováno	ELIM	ELIM	4	3
		RM11	Kontrola ze strany pracovníků BEK a případné upozornění vedoucího stanoviště/dispečera SUP v případě zjištění překročení maximálního počtu směn na jednoho pracovníka BEK	Detekováno s odezvou	2		4	
		RM12	Školení vedoucího stanoviště/dispečera SUP ohledně jeho odpovědností (vytváření měsíčního plánu s využitím FPD/úprava směn apod.)	Školení a postupy	1		2	

Odkaz na nebezpečí	PMS	RM ID	Doporučené zmírnění (Recommended Mitigation)	Úroveň zmírnění (Mitigation Level)	MES	CMES	PPMS	CPMS
H-3.3	2	RM09	Navržení programu, který zabrání tomu, aby během plánování došlo k nedodržení/překročení stanovených limitů (nedodržení minimálního počtu přestávek apod.)	Eliminováno	ELIM	ELIM	4	3
		RM13	Kontrola ze strany pracovníků BEK a případné upozornění vedoucího stanoviště v případě zjištění překročení maximálního počtu přesčasů na jednoho pracovníka BEK	Detekováno s odezvou	2		4	
		RM14	Školení vedoucího stanoviště ohledně jeho odpovědností (vytváření měsíčního plánu s využitím FPD apod.)	Školení a postupy	1		2	
H-3.4	2	RM09	Navržení programu, který zabrání tomu, aby během plánování došlo k nedodržení/překročení stanovených limitů (nedodržení minimálního počtu přestávek apod.)	Eliminováno	ELIM	ELIM	4	3
		RM11	Kontrola ze strany pracovníků BEK a případné upozornění vedoucího stanoviště/dispečera SUP v případě zjištění překročení maximálního počtu nočních směn jdoucích za sebou.	Detekováno s odezvou	2		4	
		RM12	Školení vedoucího stanoviště/dispečera SUP ohledně jeho odpovědností (vytváření měsíčního plánu s využitím FPD/úprava směn apod.)	Školení a postupy	1		2	
H-4.1	2	RM15	Kontrola a následné potvrzení ze strany plánovače směn k ověření, že v měsíčním plánu byly zakomponovány požadavky na FPD.	Detekováno s odezvou	2	3	4	3
		RM14	Školení vedoucího stanoviště ohledně jeho odpovědností (vytváření měsíčního plánu s využitím FPD apod.)	Školení a postupy	1		2	
		RM16	Vytvoření podkladů pro vedoucího stanoviště za účelem individuální kontroly plnění jeho odpovědností (plánování spolu s přizpůsobením stanovenému FPD apod.)	Školení a postupy	1		3	
H-4.2	2	RM17	Dvojí kontrola v rámci čerpání FPD před předáním požadavků na FPD (mezi plánovačem a vedoucím stanoviště)	Detekováno s odezvou	2	3	4	3
		RM18	Školení plánovače směn ohledně jeho odpovědností (čerpání FPD, vyhodnocení a zpracování dat o letech atd.)	Školení a postupy	1		2	
		RM19	Vytvoření podkladů pro plánovače směn za účelem individuální kontroly plnění jeho odpovědností (čerpání FPD, vyhodnocení a zpracování dat o letech atd.)	Školení a postupy	1		3	
H-5.1	1	RM20	Provádění pravidelných inspekcí/auditů ze strany vedení za účelem ověření splňování veškerých odpovědností (dodržování pravidel a postupů, legislativních požadavků apod.)	Detekováno s odezvou	2	3	4	3
		RM21	Vytvoření podkladů pro pracovníky BEK za účelem individuální kontroly plnění veškerých odpovědností (dodržování pravidel a postupů, legislativních požadavků apod.)	Školení a postupy	1		3	
		RM22	Pravidelná školení pracovníků BEK ohledně jejich odpovědností (pravidla a postupy, legislativní požadavky apod.)	Školení a postupy	1		2	
H-5.2	1	RM20	Provádění pravidelných inspekcí/auditů ze strany vedení za účelem ověření splňování veškerých odpovědností (dodržování pravidel a postupů, legislativních požadavků apod.)	Detekováno s odezvou	2	3	4	3
		RM21	Vytvoření podkladů pro pracovníky BEK za účelem individuální kontroly plnění veškerých odpovědností (dodržování pravidel a postupů, legislativních požadavků apod.)	Školení a postupy	1		3	
		RM22	Pravidelná školení pracovníků BEK ohledně jejich odpovědností (pravidla a postupy, legislativní požadavky apod.)	Školení a postupy	1		2	

Příloha 4 – Předpoklady a proaktivní indikátory BEK

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování Shaping action	Hedging action Signposts
SC-1.1	V rámci procesů plánování bezpečnostní kontroly existují příslušné postupy pro přerozdělení kapacit.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK Stížnosti dopravců	Úprava postupů pro přerozdělení kapacit. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Během příslušných činností plánování bezpečnostní kontroly jsou využívány postupy pro přerozdělení kapacit.	Pravidelné přezkoumání postupů. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-1.2	V rámci procesů plánování bezpečnostní kontroly existují příslušné postupy pro obsazení požadovaných pozic při nouzových situacích.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK Stížnosti dopravců	Úprava postupů pro obsazení pozic při nouzových situacích. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Během příslušných činností plánování bezpečnostní kontroly jsou využívány postupy pro obsazení požadovaných pozic při nouzových situacích.	Pravidelné přezkoumání postupů. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-2.1	V rámci procesů plánování bezpečnostní kontroly existují postupy pro přiřazení pracovníků k jednotlivým úlohám.	Kontroly/inspekce/audity BEK	Úprava postupů pro přiřazení pracovníků k úlohám. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Během příslušných činností plánování bezpečnostní kontroly jsou využívány postupy pro přiřazení pracovníků k jednotlivým úlohám.	Pravidelné přezkoumání postupů. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-3.1	Požadavky na minimální počet přestávek na jednoho pracovníka BEK jsou dostačující pro odpočinek pracovníka.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Úprava požadavků na minimální počet přestávek dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na minimální počet přestávek na jednoho pracovníka BEK.	Pravidelné přezkoumání požadavků. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování Shaping action	Hedging action Signposts
SC-3.2	Požadavky na maximální počet směn na jednoho pracovníka BEK jsou dostačující z hlediska vytížení pracovníků.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Úprava požadavků na maximální počet směn dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na maximální počet směn na jednoho pracovníka BEK.	Pravidelné přezkoumání požadavků. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-3.3	Požadavky na maximální počet přesčasů na jednoho pracovníka BEK jsou dostačující z hlediska vytížení pracovníků.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Úprava požadavků na maximální počet přesčasů dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na maximální počet přesčasů na jednoho pracovníka BEK.	Pravidelné přezkoumání požadavků. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-3.4	Požadavky na maximální počet nočních směn jdoucích za sebou na jednoho pracovníka BEK jsou dostačující z hlediska vytížení pracovníků.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Úprava požadavků na maximální počet nočních směn jdoucích za sebou dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky na maximální počet nočních směn jdoucích za sebou na jednoho pracovníka BEK.	Pravidelné přezkoumání požadavků. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-4.1	Fond pracovní doby (FPD) je adekvátní.	Kontroly/inspekce/audity BEK	Aktualizace FPD. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	V rámci plánování směn bezpečnostní kontroly je využíván adekvátní FPD.	Pravidelné přezkoumání FPD. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování Shaping action	Hedging action Signposts
SC-4.2	Náležitosti pro účely čerpání FPD (křivka cestujících během roku apod.) jsou kompletní a aktuální.	Kontroly/inspekce/audity BEK	Aktualizace a doplnění náležitostí. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při čerpání FPD jsou využívány kompletní a aktuální náležitosti (křivka cestujících během roku apod.).	Pravidelné přezkoumání náležitostí pro čerpání FPD. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-5.1	Postupy a pravidla pro bezpečnostní kontrolu jsou adekvátní.	Testování pracovníků BEK Kontroly/inspekce/audity BEK	Úprava postupů a pravidel dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při bezpečnostní kontrole jsou využívány adekvátní postupy a pravidla.	Pravidelné přezkoumání postupů a pravidel. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-5.2	Úkony pro provedení bezpečnostní kontroly jsou kompletní.	Kontroly/inspekce/audity BEK Hlášení pracovníků BEK	Doplnění úkonů BEK dle potřeby. Doplňující školení pracovníků. Zvýšení frekvence kontrol/inspekcí/auditů.
	Při bezpečnostní kontrole jsou vykonávány kompletní potřebné úkony.	Pravidelné přezkoumání kompletnosti úkonů BEK. Provádění kontrol/inspekcí/auditů BEK.	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)

Příloha 5 – Předpoklady a proaktivní indikátory pro účely ÚCL

Zdroj	Předpoklad (proaktivní indikátor)	Způsob sledování Shaping action	Hedging action Signposts
SC-1	V rámci procesů plánování bezpečnostní kontroly existují postupy pro zajištění pokrytí provozu.	Kontroly/inspekce/audity BEK ze strany ÚCL	Upozornění/doporučení dle příslušné situace. Zvýšení frekvence kontrol/auditů/inspekcí BEK. Kontrola nápravné činnosti.
	Během činností plánování bezpečnostní kontroly jsou využívány postupy pro zajištění pokrytí provozu.	Provádění kontrol/inspekcí/auditů BEK	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-3	Požadavky pro plánování směn bezpečnostní kontroly jsou dostačující z hlediska vytížení pracovníků.	Kontroly/inspekce/audity BEK ze strany ÚCL	Upozornění/doporučení dle příslušné situace. Zvýšení frekvence kontrol/auditů/inspekcí BEK. Kontrola nápravné činnosti.
	Při plánování směn bezpečnostní kontroly jsou využívány aktuální a dostačující požadavky.	Provádění kontrol/inspekcí/auditů BEK	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-4	Postupy pro práci s FPD jsou adekvátní.	Kontroly/inspekce/audity BEK ze strany ÚCL	Upozornění/doporučení dle příslušné situace. Zvýšení frekvence kontrol/auditů/inspekcí BEK. Kontrola nápravné činnosti.
	Při plánování směn jsou využívány adekvátní postupy pro práci s FPD.	Provádění kontrol/inspekcí/auditů BEK	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)
SC-5	Požadavky pro vykonání bezpečnostní kontroly jsou kompletní a adekvátní.	Kontroly/inspekce/audity BEK ze strany ÚCL	Upozornění/doporučení dle příslušné situace. Zvýšení frekvence kontrol/auditů/inspekcí BEK. Kontrola nápravné činnosti.
	Při bezpečnostní kontrole jsou využívány kompletní a adekvátní požadavky pro její vykonání.	Provádění kontrol/inspekcí/auditů BEK	Plánované změny postupů BEK (rozdělování kapacit, plánování směn, provádění bezpečnostní kontroly)