ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ
Ústav letecké dopravy

REGISTR NEBEZPEČÍ A RIZIK ZALOŽENÝ NA SYSTÉMOVÉM PŘÍSTUPU V MRO

Diplomová práce

Studijní program: Technika a technologie v dopravě a spojích

Studijní obor: Provoz a řízení letecké dopravy

Vedoucí práce: Ing. Natalia Guskova
Ing. Andrej Lališ, Ph.D.

Bc. Michaela Víznerová

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 Víznerová

Studijní program (obor/specializace) studenta:

navazující magisterský – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Registr nebezpečí a rizik založený na systémovém přístupu v MRO**

Název tématu (anglicky): Systemic Hazard and Risk Register at MRO

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cílem práce je navrhnout architekturu registru nebezpečí a rizik systému řízení provozní bezpečnosti (SMS) založeném na systémovém přístupu pro uchovávaní dat o řídící struktuře, nebezpečí, rizicích a nápravných opatření.
- Analyzujte současné registry nebezpečí a rizik v organizacích provádějící údržbu letadel.
- Analyzujte systémový model STAMP a jeho metodiky.
- Vytvořte vzorek dat o bezpečnosti z provozu údržbových organizací pomocí systémového modelu STAMP.
- Navrhněte architekturu registru nebezpečí a rizik založeném na systémovém přístupu a postup pro využití navrženého registru v praxi.
- Vyhodnoťte a ověřte navržené řešení.

ČVUT FD

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, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N., Thomas, J. CAST Handbook, 2018.

Vedoucí diplomové práce: **Ing. Natalia Guskova**
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: **30. listopadu 2022**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

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

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

prof. Ing. Ondřej Přibyl, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Michaela Víznerová
jméno a podpis studenta

V Praze dne 17. května 2022

Abstrakt

Diplomová práce se zabývá návrhem architektury registru nebezpečí a rizik systému řízení provozní bezpečnosti (SMS) založeném na systémovém přístupu pro uchování dat o řídící struktuře, nebezpečí, rizik a nápravných opatření. Pomocí systémového modelu STAMP a jeho metodiky CAST se provede analýza na nehodě způsobenou organizací MRO. Tímto postupem se získá vzorek bezpečnostních dat z provozu údržbových organizací, která následně poslouží jako vstup pro návrh nové architektury registru nebezpečí a rizik, který je založeném na systémovém přístupu. Poté se navrhne aplikační model a postup pro využití navrženého registru v praxi.

Klíčová slova: údržba letadel, MRO, Systems-Theoretic Accident Model and Processes, Causal Analysis based on STAMP, registr rizik a nebezpečí, Safety Management System, systémový přístup

Abstract

The thesis deals with the design of a hazard and risk register architecture for an operational safety management system (SMS) based on a systemic approach for storing data on the control structure, hazards, risks and corrective actions. Using the STAMP system model and its CAST methodology, an analysis is performed on an accident caused by an MRO organization. This process will provide a sample of safety data from the MRO operations, which will then serve as input for the design of a new hazard and risk register architecture that is based on a systems approach. An application model and procedure for the use of the proposed registry in practice will then be proposed.

Keywords: aircraft maintenance, MRO, Systems-Theoretic Accident Model and Processes, Causal Analysis based on STAMP, risk and hazard register, Safety Management System, Systemic Approach to Safety

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Registr nebezpečí a rizik založený na systémovém přístupu v MRO vypracovala samostatně a použila k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

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

Praze dne 17. května 2022 .....

Bc. Michaela Víznerová

Poděkování

Ráda bych zde poděkovala mým vedoucím Ing. Natalii Guskove a doc. Ing. Andreji Lališovi, Ph.D. za odborné vedení a konzultování mé diplomové práce a za jejich čas a trpělivost. Dále děkuji panu Ing. Slobodanu Stojićovi, Ph.D. za poskytnutí užitečných rad.

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

ATC	Air Traffic Control	Řízení letového provozu
ATS	Air Traffic Service	Letové provozní služby
CAST	Causal Analysis based on STAMP	Analýza příčin založená na STAMP
CAMO	Continuing Airworthiness Management Organisation	Organizace k řízení zachování letové způsobilosti
CAO	Combined Airworthiness Organisation	Organizace s kombinovaným oprávněním k řízení zachování letové způsobilosti
CC	Cabin Crew	Posádka palubních průvodčí
CMES	Combined Mitigation Effectivness Score	Kombinace hodnot sil zmírnění
CPMS	Combined Post Mitigation Score	Kombinace hodnot po zmírnění
E/WD	Engine/Warning Display	-
FC	Flight Crew	Letová posádka
FK	Foreign key	Cizí klíč
FO	First Officer	První důstojník
GA	General Aviation	Všeobecné letectví
GPIAA	Gabinete de Prevenção e Investigação de Acidentes	Portugalské oddělení prevence a vyšetřování leteckých nehod
MCC	Maintenance Control Center	Řídící středisko údržby
MES	Mitigation Effectivness Score	Hodnota síly zmírnění
MIT	Massachusetts Institute of Technology	Massachusettský technologický institut
MRO	Maintenance, Repair and Overhaul	Údržba, opravy a revize
PK	Primary key	Primární klíč
PMS	Pre-Mitigation Severity	Závažnost před zmírněním
PPMS	Post-Potential Mitigation Severity	Potenciální dopad změny závažnosti zmírnění
SB	Service Bulletin	Servisní bulletin

SDCPS	Safety data collection and processing system	Systém sběru a zpracování bezpečnostních dat
SMS	Safety Management System	Systém řízení provozní bezpečnosti
SSP	State safety programme	Státní program bezpečnosti
STAMP	System-Theoretic Accident Model and Process	Systémově-teoretický model nehod a procesů
STPA	Systems-Theoretic Process Analysis	Systémově-teoretická analýza procesů
UCA	Unsafe Control Actions	Nebezpečné řídící akce
UI	User Interface	Uživatelské rozhraní

Úvod

Nárůst využití letecké dopravy, především v posledních letech, s sebou přináší neustále rychlý rozvoj technologií a systémů v letectví. Tím se kladou větší nároky i na bezpečnost v letectví. K tomu je zavedené řízení provozní bezpečnosti (SMS), které se zabývá práci s riziky a jeho proaktivním zmírňováním určené k předcházení nehodám. Jeden z klíčových aspektů, jak předcházet leteckým nehodám, je správně provedená údržba. Tím přirozeně vznikají mnohem větší nároky na údržbu letadel. Všechny procesy a postupy v údržbových organizacích musí být přesně dodržovány, neboť i menší chyba či přehlédnutí může vést spolu s dalšími faktory k nehodě. Z těchto důvodů se tato práce soustředí na procesy spojené s údržbou letadel, kde takových procesů je nespočet a je zapotřebí proaktivně pracovat s nebezpečími a riziky.

S rozvojem letecké dopravy se mění vzhled dnešních systémů; vznikají nové komplexní socio-technické systémy, které jsou složitější na pochopení, nové druhy nebezpečí a nárůst komplexity systémů, ke které je zapotřebí přistupovat jiným pohledem, než bylo doposud zvykem.

Cílem této diplomové práce je navrhnout vhodnou architekturu registru nebezpečí a rizik v organizacích provádějící údržbu. Návrh architektury je založen na systémovém přístupu dle modelu STAMP, který lépe chápe dnešní nově vzniklé systémy a obsahuje všechna relevantní data, kterými jsou nebezpečí, rizika, data o řídící struktuře, a nápravná opatření. Použitím modelu STAMP lze proaktivně přistupovat k řízení rizik pomocí jeho dvou metod.

K tomu je zapotřebí nejprve analyzovat současný stav a získat tak přehled o nynějších metodách vedení a následné použití registrů, během kterých lze odhalit nedostatky, které mohou být poučným vstupním aspektem při návrhu nové architektury.

Pro účely této práce, jak navrhnout vhodnou architekturu, je zvolena metodika CAST založená na modelu STAMP, která funguje jako retroaktivní nástroj. Pomocí této detailní analýzy, která je aplikována na nehodu způsobenou nedostatečnou údržbou, se získá širší přehled o faktorech přispívající k nehodě, které by pouhým šetření a investigací nehod nebyly odhaleny. Na základě těchto dat lze navrhnout nová architektura registru nebezpečí a rizik, která proaktivně přistupuje k řízení rizika.

V poslední kapitole je zohledněna aplikační fáze a navržen model, na kterém je demonstrováno, jak by tento návrh byl implementován v praxi, a jak by byl následně využit. Požadavky na aplikační návrh jsou především přehlednost a jednoduché uživatelské využití za účelem rychlé a efektivní práce s ním.

Ověření celého návrhu proběhne použitím bezpečnostních dat získané analýzou CAST z šetřené nehody. Ty se zanesou do navrženého modelu a výsledkem je výstup, jak pracovat s rizikem, aby se předcházelo nehodám.

1. Bezpečnost v civilním letectví

Provozní bezpečnost („Safety") v letectví je definována organizací ICAO jako *stav, ve kterém jsou rizika spojená s činnostmi letectví související s provozem letadel nebo s přímou podporou provozu letadel řízena a snížena na přijatelnou úroveň.* [1]. To s sebou přirozeně přináší i potřebu řídit procesy spojené s bezpečností, a proto by každý stát měl řízení bezpečnosti implementovat. [1]

Řízení bezpečnosti („Safety management") je zavedené za účelem proaktivního zmírňování rizik ještě předtím, než povedou k leteckým nehodám či incidentům. Pro účinnější řízení bezpečnosti je zaveden *Státní program bezpečnosti (SSP)* a *Systém řízení bezpečnosti (SMS)*. (Obojí je detailně popsáno v Annexu 19 – příloha Chicagské úmluvy – a jeho českém znění L19.) [1][2]

Řízení bezpečnosti přispívá k mnoha faktorům, které mají kladný vliv na výslednou bezpečnost v civilním letectví. Takovými faktory mohou být: kultura bezpečnosti, včasná detekce rizik, finanční úspora, komunikace v organizaci a mnoho dalších. [1]

1.1 Státní program bezpečnosti (SSP)

SSP je definováno jako integrovaný soubor předpisů a činností zaměřených na zlepšení bezpečnosti. [1] Obsah a rozsah působnosti vypracovaného SSP musí být úměrný rozsahu a komplexitě státního systému civilního letectví. [3] *Systémem je myšlená organizovaná, účelná struktura, která se skládá ze vzájemně souvisejících a vzájemně závislých prvků a složek a souvisejících politik, postupů a praktik vytvořených za účelem provádění konkrétní činnosti nebo řešení problému.* [1]

Dle Annexu 19 by SSP měl obsahovat čtyři základní pilíře, těmi jsou:

a) *státní politika a cíle bezpečnosti;*
b) *řízení bezpečnostních rizik na úrovni státu;*
c) *zajištění bezpečnosti na úrovni státu; a*
d) *prosazování bezpečnosti na úrovni státu.* [3]

1.2 Systém řízení provozní bezpečnosti (SMS)

Systém řízení bezpečnosti je definován jako systematický přístup k řízení provozní bezpečnosti, včetně nezbytných organizačních struktur, odpovědností, zásad a postupů.

[1] Annex 19 dále uvádí *důležitost vývoje a udržování SMS v důsledku zlepšování identifikací nebezpečí*[1]*, shromažďováním a analýzou dat a nepřetržitým hodnocením a řízením rizik*[2]. [1] Tak jako SSP, tak i SMS musí odpovídat velikosti a rozsahu provozu vykonávaným provozovatelem, avšak minimální obsah SMS je v Annexu 19 jasně definován; je to především:

- *proces identifikace potenciálních nebezpečí a souvisejících rizik,*
- *zavádění nápravných opatření; a*
- *průběžné sledování všech činností spojených s řízením bezpečnosti.* [3]

Aby SMS správně fungovalo, je zapotřebí zajistit integraci všech komponentů SMS a tím zajistit správné řízení a zajišťování bezpečnosti systémovým přístupem. SMS je postavené na 4 základních pilířích. Těmi jsou:

- **Politika bezpečnosti a její cíle** – v organizaci spravující SMS musí být jasně stanovená zodpovědnost managementu za bezpečnost. Management musí plnit své závazky a přijmout odpovědnost za veškeré procesy a činnosti týkající se bezpečnosti.
- **Řízení bezpečnostních rizik** („Safety Risk Management" – SRM) – pro správné řízení SMS je potřeba určit popis patřičného systému, analyzovat, posuzovat a řídit rizika a identifikovat nebezpečí.
- **Zajištění bezpečnosti** – je potřeba předem definovat cíle na základě požadavků managementu. Tyto cíle by se především měly týkat sběru dat, konkrétně shromažďování, analýzy a následného vyhodnocování informací. Management tyto cíle musí plnit a kontrolovat, zda cíle skutečně zajišťují vlastní účel.
- **Prosazování bezpečnosti** – bezpečnost se musí neustále prosazovat; programy či procesy by měly být neustále zlepšovány a tím zajišťovat i zlepšování SMS v rámci vlastní organizace. [3]

[1] Nebezpečí = jakákoliv existující, nebo potencionální podmínka, která může způsobit ztrátové události [1]
[2] Riziko = pravděpodobnost a závažnost následku nebezpečí [1]

Řízení bezpečnostních rizik (SRM)

SRM je jedna z nejdůležitějších součástí SMS pro správné zajišťování bezpečnosti. Mezi procesy spadající pod SRM spadá:

- *identifikace nebezpečí*
- *hodnocení rizik*
- *zmírňování rizik*
- *přijímání rizik.*

Vzhledem k rychlosti vývoje letectví, se přirozeně mění i nebezpečí a rizika spojená s ním. Proto SRM je samotný systém, ve kterém neustále probíhají činnosti spojené s řízením rizik. [1]

Prvním samotným procesem SRM je **identifikace nebezpečí.** Nebezpečí se může vyskytovat v různých formách, například jak v přirozeně vyskytující se, tak i uměle vytvořené. Letectví však může fungovat i s existencí takovýchto nebezpečí, ale jen za předpokladu, že jsou tyto nebezpečí bedlivě řízeny a kontrolovány. To ale spočívá v detailní identifikaci nebezpečí a jejich následků. Následky mohou mít taktéž jakoukoliv formu od těch nejméně vážných (diskomfort cestujících) až po extrémně vážných (ztráta na lidských životech). Popis těchto následků je základem pro hodnocení rizik a následné nakládání s nimi. *Proto detailní identifikace nebezpečí vede k přesnějšímu posouzení rizik.* [1]

Druhým procesem SRM je **hodnocení rizik**; to se skládá z pravděpodobnosti a závažnosti. ***Pravděpodobnost rizika*** je míra očekávání toho, že dojde k nějakému následku. Jak lze vidět v Tabulka 1, ICAO navrhlo alfanumerické hodnocení rizika, které se následně zapisuje do tabulky. Škála pravděpodobnosti se pohybuje od 1 do 5, kde:

- 1 = extrémně nepravděpodobná,
- 2 = nepravděpodobná,
- 3 = vzdáleně pravděpodobná,
- 4 = občasná,
- 5 = častá. [1]

Dále se posuzuje ***závažnost rizika***. Ta je definovaná jako očekávaný rozsah poškození, který nastane jako následek identifikovaného nebezpečí. Pro klasifikaci závažnosti se musí zvážit všechny možné následky, tedy od poškození letadla či letiště, jakákoliv újma

způsobená ATS až po lidská zranění či dokonce úmrtí. Škála závažnosti se pohybuje od A do E, kde:

- A = katastrofální,
- B = hazardní,
- C = významná,
- D = méně významná,
- E = zanedbatelná. [1]

Bezpečnostní riziko		*Závažnost*				
Pravděpodobnost		*Katastrofální A*	*Hazardní B*	*Významná C*	*Méně významná D*	*Zanedbatelná E*
Častá	5	5A	5B	5C	5D	5E
Občasná	4	4A	4B	4C	4D	4E
Vzdáleně pravděpodobná	3	3A	3B	3C	3D	3E
Nepravděpodobná	2	2A	2B	2C	2D	2E
Extrémně nepravděpodobná	1	1A	1B	1C	1D	1E

Tabulka 1 – Příklad matice bezpečnostních rizik [1 – upraveno autorem]

Tímto posouzením vznikne tabulka hodnocení rizik, viz Tabulka 1, kde jsou stanovené 3 kategorie rizika. 1. kategorie je přijatelné riziko (podbarvené zeleně), 2. kategorie je tolerovatelné riziko (podbarvené žlutě) a 3. kategorie je riziko nepřijatelné (podbarvené červeně). Management následně posoudí, jak moc jsou rizika přijatelná či nepřijatelná pro danou organizaci a přijme potřebná opatření, která sníží rizika na přijatelnou úroveň. Toho lze docílit pomocí snížení závažnosti, či pravděpodobnosti, či kombinací obojího zároveň. [1]

Dalším procesem je **zmírňování rizik**. To je proces začleňování nápravných opatření nebo preventivních kontrol, které vedou ke snížení závažnosti a/nebo pravděpodobnosti předpokládaných následků nebezpečí. Za všech okolností je vždy mnohem snadnější (také častější) snížit pravděpodobnost oproti snižování závažnosti. Zmírňování rizik často vyžadují změny určitých procesů a postupů. Dělí se do tří kategorií:

a) **Vyhnutí se** riziku („avoidance") – riziku se dá přímo vyhnout, pokud se zamýšlená operace vůbec neprovede. To může nastat v případech, kdy riziko a následky převyšují benefity plynoucí ze zamyšlené operace. (Příkladem by mohlo být

nevyužívání určitého letiště v dané lokalitě, pokud by tato lokalita mohla jakýmkoliv způsobem negativně ovlivnit provoz letadel.)

b) **Snížení** rizika („reduction") – riziko se dá snížit, pokud se sníží pravděpodobnost či závažnost. V praxi to znamená, že se sníží frekvence vykonávané činnosti nebo jsou navržena (a následována) taková opatření, které pomohou k snížení následků rizika. (Příkladem by mohlo být snížení frekvence letů na letišti/ z letiště v lokalitě, které by negativně mohlo jakýmkoliv způsobem ovlivnit provoz letadel.)

c) **Segregace** rizika („segregation") – od rizika se dá segregovat tím způsobem, že se přijmou taková opatření, která sníží následky. (Příkladem, který navazuje na příklady ‚a' a ‚b', by mohlo být přijmutí takových opatření, která již nebudou negativně ovlivňovat provoz letadla na daném letišti.) [1]

Posledním procesem SRM je **přijímání rizik**, kdy management dle svých kritérií stanoví, že riziko je přijatelné a nemá hrubý negativní vliv a následný impakt na procesy spojené s bezpečností. [1]

2. Registr nebezpečí a rizik v MRO

MRO (Maintenance, Repair and Overhaul) představuje údržbu, opravy a revize. Tato organizace zahrnuje všechny procesy spojené s jakoukoliv činností, které pomáhají udržovat či obnovit letadlo či letadlovou část do funkčního či původního stavu. MRO tedy zajišťuje zachování letové způsobilosti letadla a zároveň i jeho bezpečnost. Tyto procesy typicky probíhají v dílně či hangáru, kde technici využívají patřičné vybavení. [4]

Pro zachování bezpečnosti během činností provozovanými organizacemi MRO je důležité právě řízení rizik, které je důležitým pilířem SMS. SRM pomáhá organizacím identifikovat případná rizika a nebezpečí a mít je tak pod kontrolou. *K neustálému sledování potenciálních nebezpečí a souvisejících rizik je zapotřebí vést pravidelnou dokumentaci zahrnující předpoklady, na nichž je založeno posouzení* ***pravděpodobnosti*** *a* ***závažnosti,*** *přijatá rozhodnutí a přijatá opatření ke zmírnění bezpečnostních rizik.* [1] K tomu je určen právě registr nebezpečí a rizik. [1]

V současnosti běžně užívané registry nebezpečí a rizik jsou reprezentovány jako množina dat rozdělených do několika položek. Mezi tyto položky zejména patří **typ/kategorie** nebezpečí, samotné potenciální **nebezpečí, pravděpodobnost** a **závažnost** nebezpečí určující **míru rizika**. Jakmile je riziko přijatelné či tolerovatelné, žádná významná opatření neprobíhají, pokud však je riziko nepřijatelné, je nutné navrhnout **snížení rizika** či přijmout **nápravná opatření**.

V případě identifikace nebezpečí se lze podívat do takového registru a dohledat související rizika. V případě absence nebezpečí v registru se musí doplnit související dokumentace. Identifikace nového nebezpečí je prvním krokem SRM, který musí vypracovat management organizace. Systém, ve kterém se identifikují nebezpečí a rizika, zahrnuje vybavení, všechna zařízení a systémy, které jsou ovlivněny provozem a činnostmi spojené s MRO. Dále se musí zvážit i nebezpečí hrozící vzhledem ke spolupráci s externími organizacemi. [1]

K identifikaci nebezpečí se využívají interní a externí zdroje. **Interními zdroji** mohou být:

- Monitorování běžného provozu
- Automatizované monitorovací systémy
- Dobrovolné a povinné systémy hlášení událostí

- Audity
- Zpětná vazba ze školení
- Bezpečnostní vyšetřování poskytovatelů služeb [1]

Externími zdroji mohou být:

- Zprávy o leteckých nehodách
- Státní povinné a dobrovolné systémy hlášení událostí
- Audity státního dozoru a audity třetích stran
- Obchodní sdružení a systémy výměny informací [1]

2.1 Sběr a analýza bezpečnostních dat

SDCPS („Safety Data Collection and Processing Systems“) představuje název pro systém sběru a zpracování bezpečnostních dat. Jak je uvedeno v Annexu 19, státy jsou povinny zavést SDCPS za účelem ukládání bezpečnostních dat, procesů s nimi a jejich analýz. [3]

Jak již bylo zmíněno, systém pro hlášení událostí se dělí na **povinný** a **dobrovolný**. Povinný systém je zpravidla využíván k nahlášení incidentů, ke kterým již v minulosti došlo. Zatímco dobrovolný systém je spíše využíván k identifikaci potenciálních nebezpečí (skoronehody) či bezpečnostním problémům, kterým systém čelí. [1]

V případě dobrovolného systému management cílí pouze na využití informací k předcházení nebezpečí a nezneužívá tyto informace k postihu pracovníků (např. za porušení z bezpečnostních opatření). Při zachování důvěrnosti pracovníci nepociťují strach nadále hlásit jakékoliv další incidenty. Přístup k hlášení událostí musí být snadno dostupný pro všechny zaměstnance. Příkladem možností hlášení událostí je **papírový, webový** či **jakýkoliv jiný formulář**. Každý zaměstnanec by měl dostat zpětnou vazbu (pokud tento systém není anonymní) ohledně přijmutí následných opatření. [1]

Jelikož se systémy potýkají s velkým množstvím hlášení událostí, tato bezpečnostní data[3] se musí nějakým způsobem filtrovat. K tomu je určena **taxonomie** či **klasifikační systém**. Taxonomie taktéž slouží k použití těch správných definic a termínů. Tím se zvýší efektivita komunikace a správné pochopení informace. Některé taxonomie zahrnují např. model letadla, letiště (kód ICAO či IATA) a typ události. [1]

[3] **Bezpečnostní data** = Definovaný soubor faktů nebo soubor bezpečnostních hodnot shromážděných z různých zdrojů souvisejících s letectvím, který se používá k udržení nebo zlepšení bezpečnosti. [1]

Příklady taxonomií:

- ICAO ADREP (Accident/Incident Data Reporting) [5]
- CAST/ICAO CICTT (Common Taxonomy Team) [6]
- ECCAIRS (European Coordination Centre for Accident and Incident Reporting Systems) [7]
- ASRS (Aviation Safety Reporting System) [8]
- ASN Aviation Safety Database [9]
- Boeing MEDA (Maintenance Error Decision Aid) [10]

2.2 Legislativa související s bezpečností v MRO

Všechny části organizace MRO se musí řídit *Nařízením Komise (EU) č. 1321/2014 ze dne 26. listopadu 2014 o zachování letové způsobilosti letadel a leteckých výrobků, letadlových částí a zařízení a schvalování organizací a personálu zapojených do těchto úkolů*. [11]

Z tohoto nařízení vycházejí všechny legislativní požadavky na organizace, personál, prostory a vybavení. V březnu v roce 2020 se do tohoto nařízení implementovaly významné změny, které mají dopad především na všeobecné letectví (GA). V tomto znění přibyly nové části, konkrétně Part-ML, Part-CAMO a Part-CAO. [11]

Struktura Nařízení Komise (EU) č. 1321/2014 je následovná:

- Příloha I Part-M
- Příloha II Part-145
- Příloha III Part-66
- Příloha IV Part-147
- Příloha Va Part-T
- Příloha Vb Part-ML
- Příloha Vc Part-CAMO
- Příloha Vd Part-CAO

Part-ML

Part-ML stanovuje pravidla zachování letové způsobilosti letadel jiných než složitých a mimo obchodní dopravu s licencí dle Nařízení ES č. 1008/2008 („licence ES"), s omezením:

- *letounů do MTOM 2730 kg včetně,*
- *rotorových letadel do MTOM 1200 kg, včetně pro max. 4 osoby na palubě,*
- *všech dalších letadel ELA2. [11]*

Part-ML tedy pokrývá naprostou většinou GA; pro všechna ostatní letadla platí ***Part-M****.* [11]

Part-CAMO

Part-CAMO je nová příloha tohoto nařízení, která je vyčleněna jako samostatná část z původního Part-M, Subpart-G pro jakákoliv letadla. Obsahuje požadavky na organizace k řízení zachování letové způsobilosti (CAMO). [11]

Organizace, které byly oprávněné dle Part M, Subpart G se musely změnit buď na organizace oprávněné k řízení zachování letové způsobilosti dle Part CAMO, nebo na organizace s kombinovaným oprávněním dle Part CAO. Pokud by o tuto změnu nezažádaly, považovaly by se za oprávněné dle Part CAMO. [11]

Part-CAO

Parto-CAO je zcela nová část, která v sobě zahrnuje kombinované oprávnění jak k řízení zachování letové způsobilosti, tak k údržbě letadel jiných než složitých a mimo obchodní dopravu s licencí ES, nahrazující dosavadní Part M, Subpart F i G zároveň. CAO s oprávněním k údržbě může udržovat pouze letadla jiná než složitá a mimo obchodní dopravu s licencí ES (dle rozsahu svého oprávnění). [11]

Rozdíl mezi organizacemi oprávněnými dle Part CAMO a dle Part CAO je mimo jiné v tom, že CAMO budou muset zavést **systém řízení založený na SMS**, kdežto CAO jako doposud zavedou **systém jakosti (Quality System)**, resp. malé organizace s rozsahem práce omezeným jen na letadla, která spadají pod Part ML, mohou provádět pouze kontroly organizace (Organization Review). [11]

2.3 QMS a SMS

Systémy řízení jakosti[4] (QMS = „Quality Management System“) je systém zahrnující soubor zásad, procesů a postupů, které jsou vyžadovány za účelem koordinované činnosti pro vedení a řízení organizace, pokud se jedná o jakost. [12]

Systém řízení jakosti a systém řízení bezpečnosti mají velmi podobné metody a techniky, avšak mají odlišné cíle. Zatímco QMS je zaměřován na jakost, spolehlivost, a především uspokojení potřeb zákazníka, SMS je zaměřovaný na bezpečnost v letectví. Zavedení QMS v organizace není ani z daleka dostatečné z pohledu bezpečnosti, jelikož kvalita a spolehlivost není záruka bezpečnosti. QMS může sloužit jako základ pro sestavení SMS, avšak nesmí to nijak omezovat řízení provozní bezpečnosti. Dalším rozdílem mezi těmito dvěma systémy je, že QMS se nesoustředí na analýzy nehody a incidentů za účelem nalezení rizik a nebezpečí. [13]

[4] Jakost (Quality) = Stupeň splnění požadavků souborem inherentních charakteristik (ČSN EN ISO 9000*) [12]

3. Systémový přístup v letectví

Rychle rozvíjející se odvětví letectví s sebou přináší komplexní systémy, ke kterým se musí přistupovat jiným způsobem, než doposud bylo zapotřebí. Tento systémový přístup se začal ve 21. století aktivně implementovat do modelů a metodik provozní bezpečnosti. *„Abychom porozuměli a zlepšili způsob, jakým organizace fungují, musíme přemýšlet v systémech."* [14] Tento výrok jednoduše pojednává o tom, že je zapotřebí posuzovat systémy jako celek a nepřemýšlet nad nimi jako nad jednotlivými částmi. Musí se brát v úvahu i okolní aspekty, které kooperují s částmi systému. Takovými interakcemi mohou být interakce lidské, sociální, technické, informační, politické, ekonomické a organizační a další. Postupem času tedy vznikla **systémová teorie**, kterou lze definovat jako *soubor principů, které lze použít k pochopení chování komplexních systémů, ať už se jedná o přirozeně vyskytující se systémy nebo člověkem vytvořené.* [15] *Teorie komplexity popisuje přirozeně vyskytující se systémy, kde se zdánlivě nezávislí činitelé spontánně uspořádávají a přeskupují do koherentního systému pomocí přírodních zákonů, kterým ještě plně nerozumíme.* [15] Systémová teorie se zdá být nejvhodnější pro inženýrsky sestrojené či navržené systémy, zatímco teorie komplexity je nejvhodnější pro sociologické a přirozeně vyskytující se systémy, kde je návrh neznámý. [15][16]

Systémová teorie přistupuje i jiným způsobem ke vzniku nehod. Myšlenka je založená na tom, že nehody vznikají právě na základě probíhajících interakcí mezi jednotlivými komponenty systému. Zatímco průmyslové bezpečnostní modely se spíše zaměřují na nebezpečné úkony a podmínky, systémové modely se zaměřují na to, co se pokazilo celkově v organizaci systému. [16]

3.1 Model STAMP

STAMP svojí zkratkou představuje název pro Systems-Theoretic Accident Model and Processes, tedy je to systémově-teoretický model nehod a procesů. Autorkou tohoto modelu je profesorka Nancy G. Leveson pracující na univerzitě MIT. STAMP je první model, který se zabývá organizovanou komplexitou. Je navržen tak, že rozšiřuje lineární sekvenční model na více komplexní. Na nehody se už nepohlíží jako selhání jednotlivých částí systému, ale jako důsledek nedostatečného řízení systému. Na základě modelu STAMP jsou založeny dvě metodiky zvané STPA (System-Theoretic Process Analysis) a CAST (Causal Analysis based on STAMP), které budou později popsány. [16]

Základ systémové teorie, se kterým pracuje model STAMP, spočívá na dvou dvojicích myšlenek:

a) **Vznik (emergence) a hierarchie**

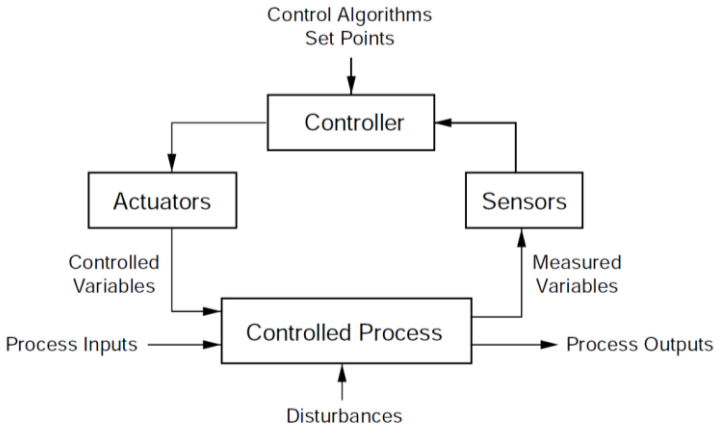
Komplexní systémy lze vyjádřit pomocí hierarchie úrovní organizace, z nichž každá úroveň je komplexnější než ta níže. Na vrcholu hierarchie je tedy přirozeně ta nejkomplexnější část celého systému. Dále zde hraje roli i zamýšlení o emergenci. Tu lze definovat jako myšlenku, která pojednává o tom, že na dané úrovni komplexity jsou vlastnosti charakterizované právě pro tuto úroveň. Různé úrovně organizace mají tedy různý popis vlastností. Jednoduše řečeno, každá úroveň se vyznačuje tím, že má nové vlastnosti. [16]

b) **Komunikace a řízení**

Další dvojicí je komunikace a řízení. Řízení je vždy spojeno se zavedením bezpečnostních požadavků. Jakýkoli popis řídícího procesu znamená vyšší úroveň zavedení požadavků na nižší. V hierarchii organizaci existují řídící procesy, které fungují mezi jednotlivými úrovněmi. Dále je třeba rozlišovat na systémy otevřené a uzavřené. Tak je právě rozlišoval Karl Ludwig von Bertalanffy – rakouský biolog a filozof, který již ve 20. století vyvíjel myšlenku systémové teorie. Uzavřené systémy obsahují neměnné komponenty, které jsou základem pro jistý balanc systému, zatímco otevřené systémy mohou být z rovnováhy vyvedeny, jakmile kooperují s okolními aspekty. A právě řízení v otevřených systémech vyžaduje jistou nutnost komunikace. [16]

Jak lze vidět na Obrázek 1, pro správnou funkci řízeného procesu je nutné splnit tyto čtyři základní podmínky:

- cíle – řídící prvek musí mít jistý cíl či jasně nastavené cílové hodnoty (***řídící prvek/kontrolor***),
- činu – řídící prvek musí být schopen ovlivnit stav systému (pomocí ***aktivních řídících prvků***),
- modelu – řídící prvek musí být modelem systému, nebo ho obsahovat (***řídící/kontrolovaný proces***),
- pozorovatelnosti – řídicí prvek musí být schopen zjistit stav systému (pomocí ***senzorů***). [16]



Obrázek 1 – „Standardní regulační smyčka" [16]

Obrázek 1 ukazuje proces nazývající se „standardní regulační smyčka", která popisuje veškerou hierarchii organizace. Řídící prvek („Controller") – může to být člověk či přístroj – má již předem definované meze či nastavené hodnoty („Control Algorithms Set Points"), ve kterých proces bude fungovat. Řídící prvek dále dostává informace o aktuálním stavu procesu ze senzorů („Sensors"), které je mohou získávat v určitých intervalech. Tyto informace se získávají z naměřených dat („Measured Variables"). K zajišťování funkčního procesu se využívají aktivní řídící prvky („Actuators"), které mají za úkol kontrolovat proměnné hodnoty („Controlled Variables"), tak aby řídící prvek byl schopen ovlivnit stav systému, tedy probíhající proces („Controlled Process"). Samotný proces obsahuje jak vstupy („Process Inputs"), tak výstupy („Process Outputs"). Proces může být ovlivňován rušivými elementy – šumem („Disturbances"). [16]

3.2 Systémový přístup a riziko

Jedním z rozdílů mezi bezpečnostním inženýrstvím a systémovým přístupem je v posuzování **rizika**. Bezpečnostní inženýrství pracuje s rizikem, které je spočteno jako součin pravděpodobnosti a závažnosti, avšak systémová teorie považuje tento způsob výpočtu rizika za nerelevantní. Pravděpodobnost události nelze u komplexních systémů snadno spočíst, vzhledem k mnoha probíhajícím interakcím v systému mezi jednotlivými komponenty, a především vzhledem k zpětným vazbám, které následně vyvolávají těžce předvídatelné události. Se závažností se naopak pracuje jako s nejvyšším možným důsledkem nebezpečné události. [16]

Metoda, jak hodnotit riziko, byla vyvinuta na univerzitě MIT a je detailně popsána v publikaci „A System-Theoretic Approach to Risk Analysis", kterou publikovali autoři Dro

J. Gregorian a Sam M. Yoo. [17] Dle této metody se na riziko již nepohlíží jako na problém selhání komponentu, ale spíše jako na **problém kontroly**. V dnešních komplexních systémech nelze určit pravděpodobnost následku nebezpečí, protože neexistují žádná relevantní historická data, ze kterých by se dalo vycházet. Pokud by se organizace pokoušela určit pravděpodobnost takového výskytu, riziko by mohlo být špatně odhadnuto a organizace by ve výsledku mohla utrpět ztrátami. Proto je pravděpodobnost nahrazena **účinností zmírňování rizika**. Z toho vyplývá i nová definice rizika, která je nyní popsána jako *"kombinace závažnosti nebezpečí a účinnosti zmírňování během řízení nebezpečí"*. [17]

K hodnocení účinnosti zmírnění rizika se zavedla hodnota **MES** („Mitigation effectivness score"), která se dá také nazvat jako **síla potenciálních způsobů zmírnění rizika**. V Tabulka 2 lze vidět přiřazení úrovně způsobu zmírnění rizika ke každé hodnotě MES. [17]

Úroveň způsobu zmírnění rizika	Popis zmírnění rizika	MES
Eliminováno	Příležitostný faktor lze eliminovat pomocí návrhu nebo specifickou kombinací níže uvedených zmírnění (proaktivní)	ELIM
Redukce vlivem návrhu systému	Výskyt kauzálního faktoru lze omezit nebo kontrolovat pomocí návrhu systému (proaktivní)	3
Reakce na riziko	Kauzální faktor lze detekovat a vyžaduje reakci na zmírnění (reaktivní)	2
Školení a instruktáž	Příčinný faktor lze zmírnit dodatečným školením a postupy (reaktivní)	1
Žádná	Neexistuje žádný způsob zmírnění rizika nebo způsob zmírnění není aplikován	0

Tabulka 2 – MES [17 – upraveno autorem]

V této metodice se dále uvažuje hodnota **CMES** („Combined Mitigation Effectiveness Score"), neboli **dopad kombinace způsobů snižující riziko**. Hodnota CMES je vlastně kombinací hodnot MES, avšak důležitá je kvalita zmírnění, nikoliv kvantita. To znamená, že při zavedení dvou způsobů snížení rizika se stejnou hodnotu MES bude hodnota CMS stále stejná, jako kdyby se zavedl způsob jeden. [17]

Dalším předpokladem je, že všechny způsoby zmírnění rizika jsou zavedeny současně. [17] Pokud tak není učiněno, hodnocení rizika musí odpovídat reálné implementaci zavedených způsobů zmírnění rizika. [17]

Pro následné hodnocení rizika je zapotřebí znát závažnost. Ta se nejdříve přiřazuje pomocí hodnoty **PMS** („Pre-Mitigation Severity"), což znamená **hodnota před zavedením jakéhokoliv způsobu zmírnění rizika**. Vždy se počítá s nejhorší možnou hodnotou závažnosti výsledné ztráty. Na tuto hodnotu se následně vztahuje zavedená hodnota **PPMS** („Post-Potential Mitigation Severity"), která znázorňuje ***potenciální dopad změny závažnosti každého jednotlivého zmírnění.*** [17] Po ohodnocení jednotlivých způsobů zmírnění hodnotou PPMS, spočte se hodnota **CPMS** („Combined Post Mitigation Severity"), která je kombinací všech PPMS. Spočte se průměrem všech hodnot PPMS a následně se zaokrouhlí dolů na celé číslo.

Po určení hodnoty CMES a CPMS lze určit výsledné riziko pomocí Tabulka 3. Jeden ze způsobů, jak určit riziko, je hodnotit kauzální scénáře pomocí zavádění způsobů zmírnění rizika. Všechna ID UCA se následně vepíšou do matice.

STPA-Informed Risk Matrix					
Least [A]	0				
Somewhat [B]	1				
Moderate [C]	2-3				
Very [D]	4-5				
Most [E]	6				
Eliminated [F]	N/A				
CMES		**1**	**2**	**3**	**4**
	CPMS	Catastrophic	Critical	Marginal	Negligible

Tabulka 3 – Hodnocení rizika dle metody založené na STPA

3.3 CAST

Metodika CAST (Causal Analysis based on STAMP) je analýza příčin založená na modelu STAMP. Tato metoda je retroaktivní, která se používá především k analýze nehod a

incidentů. (Metodika CAST bude popsána v samostatné kapitole vzhledem k detailnímu popisu kroků, který je zapotřebí k porozumění této analýzy.)

3.4 STPA

STPA (System-Theoretic Process Analysis) je systémově-teoretická analýza procesů založená na modelu STAMP. Je to proaktivní metoda, která zkoumá potenciální příčiny nehod během jejich vývoje, čímž umožňuje tyto příčiny řídit nebo eliminovat. Tato metoda byla vyvinuta po 2. světové válce, vzhledem k narůstající složitosti systémů. Do své analýzy zahrnuje jak lidského činitele, tak i software. STPA zajišťuje, že analýza rizik zahrnuje všechny potenciální příčinné faktory, které by mohly vést ke ztrátám. [18]

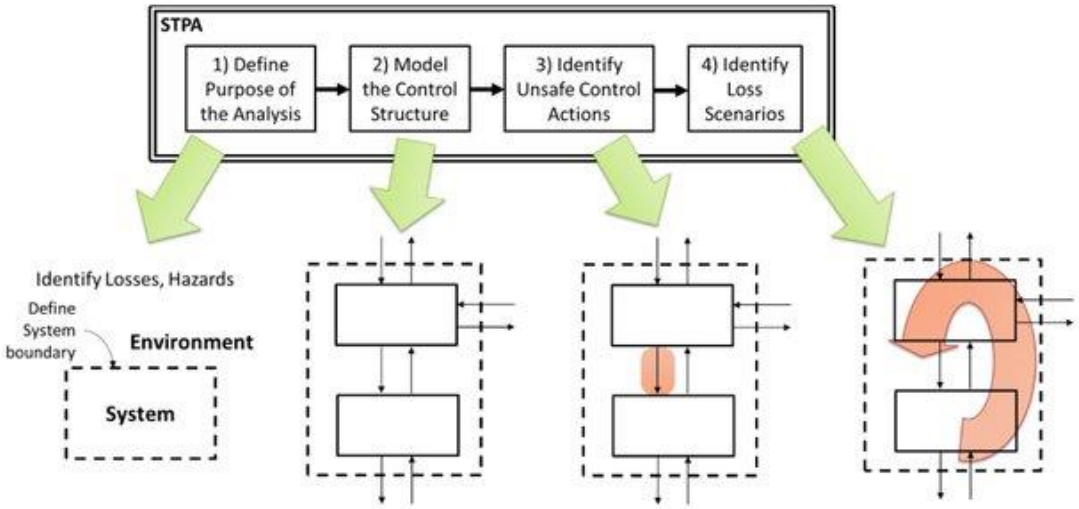
STPA se skládá ze 4 kroků, které jsou zobrazeny na oObrázek 2. Těmito kroky jsou:

1. Definování účelu analýzy – V tomto kroku se definuje účel analýzy. Identifikují se ztráty, systémová nebezpečí a jak vypadá systém. Vytyčují se hranice systému a definuje se, jak systém vypadá a jak do hloubky se systém bude zkoumat. Definuje se, zda systém má i nějaké podsystémy a popisuje se i prostředí celého systému a jak na systém působí.

2. Modelování řídící struktury systému – V tomto kroku se modeluje celá řídící struktura systému hierarchicky seřazená, která zachycuje funkční vztahy a interakce mezi komponenty. Tato struktura se skládá ze smyček řízení a zpětné vazby, kde musí být zaneseny řídící prvky, řídící akce, zpětné vazby, další vstupy a výstupy z komponentů a kontrolované procesy.

3. Identifikace nebezpečného řízení – V tomto kroku se analyzují kontrolní akce v celé řídicí struktuře. Zkoumá se, jak by kontrolní akce mohly vést ke ztrátám, které se předem definovaly. S těmito nebezpečnými kontrolními akcemi se nadále pracuje a díky nim se definují bezpečnostní požadavky pro daný systém.

4. Identifikace scénářů ztrát – V tomto kroku se identifikují všechny možné scénáře, které by vedly ke ztrátám. V potaz se berou jakékoliv nesprávné zpětné vazby, neadekvátní požadavky, selhání jednotlivých komponentů systému, chyby v návrhu či další faktory negativně ovlivňující systém. [18]



Obrázek 2 – Kroky STPA metody [18]

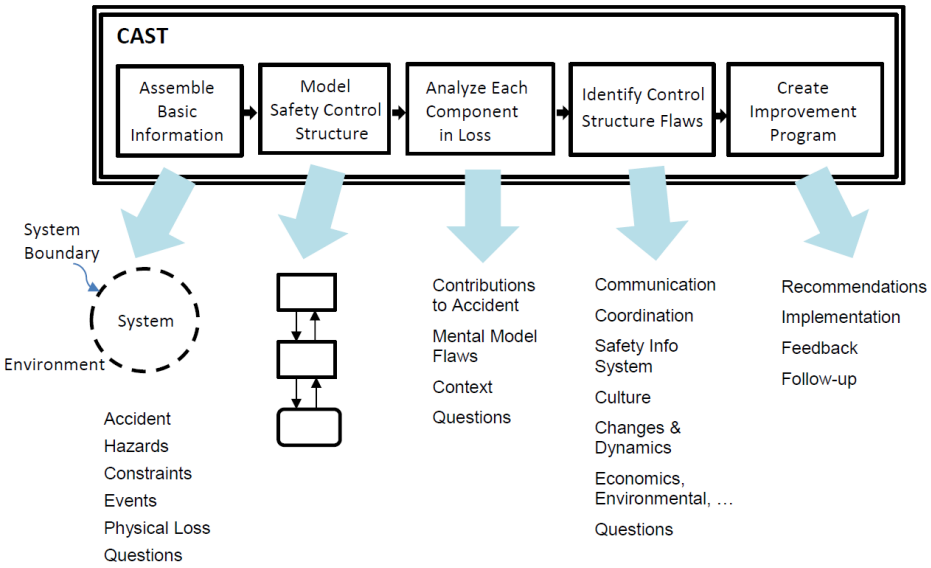
4. CAST

Tato retroaktivní metoda zkoumá nehody a incidenty, které si již staly v minulosti. Na rozdíl od STPA se CAST nezaměřuje na všechny potenciální scénáře, nýbrž pouze na konkrétní scénář, který vedl k nehodě. Avšak analýzy CAST mohou být velmi nápomocný při sestavování scénářů během analýzy STPA. [15]

Při provedení povrchní analýzy nehod (či incidentu) je vysoké riziko, že nehoda se bude stávat opakovaně, proto je zapotřebí zkoumat nehody do hloubky a neodkazovat se pouze na jeden či dva faktory vedoucí ke ztrátám. *Proto CAST rozebírá detailně celý systém a snaží se nalézt všechny příčiny nehod. CAST je ale pouze analytická metoda, a ne vyšetřovací technika.* [15] Z každého kroku vyplyne plno otázek, na které lze odpovědět až později. Cílem analýzy je zodpovědět všechny otázky či určit, že na danou otázku neexistuje odpověď. [15]

CAST se skládá z 5 kroků, které jsou zobrazeny na Obrázek 3, těmito kroky jsou:

1. Základní informace k provedení analýzy
2. Modelování řídící struktury systému
3. Analýza každého prvku řídící struktury
4. Identifikace nedostatků v řídící struktuře
5. Bezpečnostní doporučení



Obrázek 3 – Kroky CAST metody [15]

4.1 Základní informace k provedení analýzy

Tento krok obsahuje 5 částí. Nejdříve se shromažďují všechny dostupné informace o nehodě a určují se cíle prováděné analýzy.

4.1.1. Definují se **hranice systému,** dále co přesně do systému spadá a hranice prováděné analýzy. Také se definuje okolní prostředí, které ovlivnilo systém.

4.1.2. Dále se identifikují všechna **nebezpečí** („Hazards"), která následně vedla ke ztrátám. Z jednotlivých nebezpečí vyplývají i porušené bezpečnostní požadavky, jejichž identifikace je nedílnou součástí analýzy. Při identifikaci nebezpečí se musí brát v potaz vliv na celý systém, a ne pouze vliv na samotnou část systému či komponent, protože pak by to znamenalo pouze nalezenou příčinu nebezpečí, a ne nebezpečí jako takové. [15]

4.1.3. Ke každému systémovému nebezpečí je definováno **bezpečnostní omezení** („Safety constraints"). *Bezpečnostní omezení je definováno jako omezení na úrovni systému, které specifikuje systémové podmínky nebo chování, které je třeba splnit, aby se předešlo nebezpečím (a nakonec i ztrátám).* [18]

4.1.4. Následně se identifikují **ztráty** („Losses"), které mohou mít jakoukoliv podobu; *příklady jsou finanční ztráty, znečištění životního prostředí, nezdařená mise, poškození pověsti společnosti a v podstatě jakýkoli následek v podobě investice do obnovy původního stavu.* [15]

4.1.5. V poslední části se kladou **otázky,** proč vůbec k těm událostem došlo. S těmito otázky se pak bude pokračovat v dalších krocích analýzy. [15]

Dále je možnost libovolného provedení další části, kdy se popisují (bez jakýchkoliv závěrů či obviňování) všechny události, ke kterým došlo během nehody a které vedly ke ztrátám. Během **sledu všech událostí** vznikají otázky, proč k nim vůbec došlo. Tento krok je lepší k pochopení celého sledu situací. [15]

4.2 Modelování řídící struktury systému

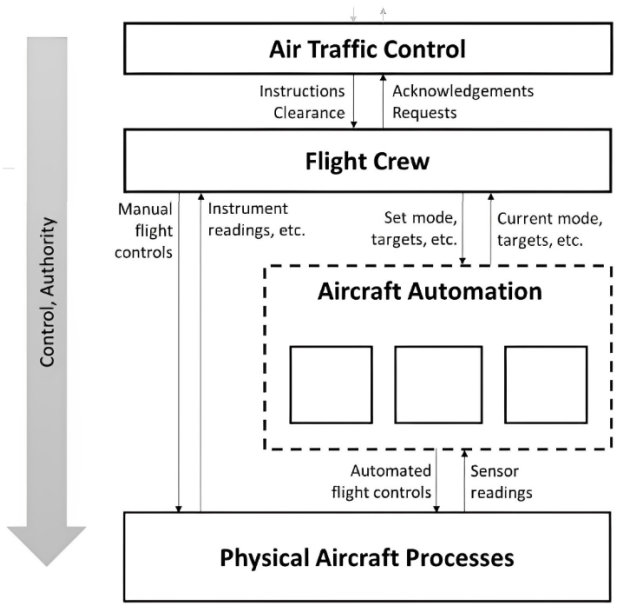
K identifikaci bezpečnostních požadavků je potřeba namodelovat řídící strukturu systému. [15] Jelikož se pomocí CAST analýzy na nehody přihlíží jako na vyskytnutý problém v řídící struktuře, a nikoliv jako selhání nějaké části systému, je zapotřebí namodelovat takovou strukturu. Vlivem modelování lze odhalit, proč nebylo předcházení nebezpečí efektivní a jak takovou strukturu vylepšit. [15]

Nejjednodušším a také nejrychlejším řešením pro vytvoření modelu řídící struktury je aplikace **analýzy STPA** na danou nehodu. Tím se tento krok výrazně ulehčí, jelikož řídící strukturu lze využít i v analýze CAST. [15]

Dalším způsobem je **inspirace u jiných nehod**, které jsou již zpracované pomocí analýzy CAST, jelikož ve většině případů se řídící struktura tak podstatně nemění.

Pokud neexistuje žádná STPA analýza na nehodu a nelze se inspirovat ani u jiných CAST analýz, řídící struktura se musí **namodelovat již od samého začátku**. Nejjednodušší je začít abstraktně od nejvyšší úrovně a postupně je konkretizovat a namodelovat ty řídící prvky, které souvisely se známým nebezpečím. Základní prvek řídící struktury je regulační (řídící) smyčka, která je již výše popsána a zobrazena na Obrázek 1. Model se může měnit i během prováděné analýzy s postupem nárůstu získaných informací. [15]

Na Obrázek 4, lze vidět příklad řídící struktury, která by se mohla vyskytovat v letectví. V nejvyšší úrovni je řízení letového provozu (ATC – „Air Traffic Control“), která dává instrukce letové posádce („Flight Crew“), ta reaguje zpětnou vazbou v podobě žádostí či potvrzení hlášení. Letová posádka řídí letadlo („Physical Aircraft Processes“), buď manuálně či pomocí autopilota.



Obrázek 4 – Příklad modelu řídící struktury v letectví [18]

4.3 Analýza každého prvku řídící struktury

Po vytvoření řídící struktury se důkladně celá analyzuje za účelem zjištění, proč řídící prvky nezabránily nehodě. Nejdříve se rozebere celá řídící struktura a zaměří se na všechny jednotlivé řídící prvky, které měly co do činění s ovlivněním nehody. Doporučovaný postup je začít od spodní části řídící struktury a postupovat směrem nahoru. Tento třetí krok se skládá ze dvou částí. [15]

V *první* části se popíše jejich **funkce či role** (v případě fyzického komponentu i lidského činitele) a jejich zodpovědnost související s nehodou. Dále se popíše, **jak prvky přispěly** k nehodě, ať už nějakým provedeným úkonem či rozhodnutím, či naopak vůbec neprovedeným úkonem či rozhodnutím. [15]

V *druhé části* kroku se kladou otázky, **proč** se tak stalo. Váže se k tomu další série, které souvisí s jistými nedostatky během rozhodování či plnění své funkce. Na to se vytvoří další sada odpovědí, které jsou ve formě různých **odůvodnění** vysvětlující provedené úkony a rozhodnutí řídících prvků. Na vše se po celou dobu musí hledět objektivně bez předčasných závěrů a obviňování. [15]

4.4 Identifikace nedostatků v řídící struktuře

Od tohoto kroku se už systém zkoumá jako celek a nezkoumají se jednotlivé komponenty, které přispěly k nehodě, to vede k jednodušší identifikaci kauzálních faktorů, které ovlivňují to, jak mezi sebou kooperují různé komponenty v řídící struktuře. Tyto faktory se nazývají systémové. Tento krok je jediný, který se nevyskytuje svým přístupem k analýze nehod v jiných bezpečnostních modelech. [15]

Takovými důležitými systémovými faktory jsou:

- Komunikace a koordinace
- Bezpečnostní informační systém
- Kultura bezpečnosti
- Návrh systému řízení bezpečnosti
- Změny v systému a jeho prostředí v průběhu času
- Vnitřní a vnější ekonomické, které stále nebyly zahrnuty v analýze [15]

Komunikace a koordinace

Mezi jedny z nejdůležitějších faktorů bezesporu patří komunikace a koordinace. Nedostatek jednoho z nich může vést k nevhodnému činu či dokonce k žádnému činu, který je právě vyžadován. K analýze komunikace je potřeba pochopení kritických komunikačních kanálů, které lze nalézt v řídící struktuře či naopak zjistit, že zde nějaké chybí. Tato skutečnost je signalizovaná absencí zpětné vazby u regulačních smyček. Dalším nedostatkem v komunikaci je nepoužívání systémů pro hlášení událostí či jeho nefunkčnost nebo dokonce úplně chybějící. [15]

Bezpečnostní informační systém

Bezpečnostní informační systém je druhý nejdůležitější faktor hrající roli v nehodovosti. *Je to systém, který zahrnuje ukládání a předávání informací o nebezpečích, zjišťování trendů a odchylek, které předpovídají nehodu, hodnocení účinnosti bezpečnostních kontrol a norem, porovnávání modelů a hodnocení rizik se skutečným chováním, identifikaci a kontrolu nebezpečí za účelem zlepšení návrhů a standardy atd. [15]*

Bezpečnostní informační systém musí být navržen tak, aby byl užitečný, a především využívaný. Mohou vznikat odchylky i shromažďováním dat, například zkreslení pohledu na nehodu. Ze zpráv o nehodách se na ně nepohlíží systémově, tudíž nejsou v systému zaneseny systémové faktory. Velmi často jsou vynechávány či nedostatečně popsány i softwarové chyby. Naopak nevýhodou může být i velké množství dat, které není zpracováno a zanalyzováno za účelem získání vhodného množství výsledků k práci s těmito výstupy. [15]

Kultura bezpečnosti

Kultura bezpečnosti jsou hodnoty a předpoklady ve společnosti, které se používají k rozhodování, a proto dokáže taktéž velmi ovlivnit chování komponentů v řídící struktuře. [15]

Aspekty kultury bezpečnosti jsou:

- *Kultura přijímání rizika* – Tato kultura spočívá v tom, že nehody jsou nevyhnutelné a jsou důsledkem nezodpovědnosti lidí a lze ji snížit či odstranit pouze zvýšenou opatrností.
- *Kultura popírání* – Management ve společností nechce slyšet negativní zprávy, a tak se rizika hodnotí velmi nízkými hodnotami.
- *Kultura dodržování předpisů* – Dodržování vládních nařízení vede dle managementu k lepším výsledkům, avšak management klade spíše důraz na to, aby se bezpečnostní návrhy dokončily a shledaly spolu s předpisy, než aby se implementovaly do reálného provozu.
- *Kultura papírování* – Společnost je přesvědčená, že větší množství dokumentace zajišťuje bezpečnější systém. Avšak dokumentace má velmi malý reálný dopad na provoz ve společnosti.
- *Kultura „swagger"* – Tato kultura spočívá v tom, že je zapotřebí pracovat v riziku a není důvod zvýšené bezpečnosti. [15]

Návrh SMS

Návrhů funkčního SMS může být spousta, avšak všechny mají stejný princip. Důležité je přiřazení zodpovědnosti a pravomocí. SMS musí být ve společnosti řádně dodržována, proto existují organizace, které kontrolují správného zavedení SMS ve firmě a zda jsou postupy vhodně implementovány a řádně dodržovány. [15]

Změny v systému a jeho prostředí v průběhu času

K většině nehod dochází právě po nějaké změně v systému, ať už jsou plánované či neplánované. Změnou může být implementace nové části či odebrání staré, změny v postupech, změny v řídící struktuře, změna prostředí atp. Jelikož změny jsou ale nutné a nevyhnutelné, musí se zavést takové procesy, kdy systém bude pružně reagovat na jakékoliv druhy změn. [15]

Vnitřní a vnější ekonomické faktory (doposud nezahrnuty v analýze)

I tyto systémové faktory dokážou znatelně ovlivnit systém. Reálným příkladem může být působení vnější konkurence na trhu či klesající zisky. To může vést ke snížení rozpočtu, který je určen na zavedení bezpečnostních opatření. [15]

4.5 Bezpečnostní doporučení

Posledním krokem je návrh bezpečnostních doporučení, aby se předešlo dalším podobným nehodám a následným ztrátám. Celkový proces bezpečnostního doporučení se skládá ze 4 kroků: Bezpečnostní doporučení → Implementace → Zpětná vazba → Dodržování bezpečnostních opatření.

Některá doporučení jsou složitější k implementaci a vyžadují rozsáhlejší změny než jiná, avšak jsou nezbytně nutná, aby se předcházelo nehodám. Aby se předcházelo zanedbávání bezpečnostních doporučení, musí se určit osoba/osoby, které budou zodpovídat za následnou implementaci. Dále proběhne kontrola, zda doporučení byla opravdu implementována a následně je zapotřebí zpětné vyjádření, zda implementace vskutku napomohla systému. Zpětná vazba může pocházet z auditů či pozdějších inspekcí. [15]

5. Přehled odborné publikace

Pro tuto práci je stěžejním zdrojem *ICAO doc. 9859*, který se nazývá Safety Management Manual. Tento dokument je soustředěn na implementaci SMS ve všech organizacích hrající roli v letectví. Jsou zde detailně popsány pilíře SMS, pod které spadá řízení rizik a jejich dokumentace. Manuál se také zabývá sběrem a využitím bezpečnostních dat, jaké procesy a analýzy s nimi probíhají a jak se s nimi pracují.

Pro pochopení systémového přístupu je ideální publikace od paní profesorky *Nancy G. Leveson – Engineering a Safer World,* kde autorka popisuje, jak implementovat systémové myšlení do světa inženýrství. Představuje zde systémovou teorii a model STAMP a jeho využití a jejich výhody oproti modelům tradičního bezpečnostního inženýrství.

K použití analýzy CAST jsou zapotřebí dvě příručky vydané taktéž paní profesorkou Nancy G. Leveson. Publikace *CAST Handbook* a *STPA Handbook*, které popisují, jak postupovat krok po kroku. Přestože STPA analýza je proaktivní, zatímco CAST analýza je retroaktivní, velmi často se odkazují na sebe navzájem, tudíž při použití obou příruček je analýza efektivnější; především při sestavování řídící struktury je popis kroku mnohem obsáhlejší v STPA příručce, díky čemuž lze detailněji namodelovat systém a více mu tak porozumět.

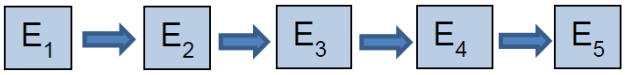
Publikací, které se zabývají registry nebezpečí a rizik v letectví, je dostupných mnoho, avšak registry související s údržbou je obtížné dohledat. Pro porozumění současného stavu registrů jsou velmi nápomocné publikace *„Case Study of Metrojet Flight 9268 to Research the Risks Register" [19]* a *„The development of the sector risk profiling methodology for Australian CAA and its application to the small aeroplane transport sector"*.[20]

Velmi názorným příkladem, který ukazuje, jak aplikovat analýzu CAST na reálnou leteckou nehodu, je publikace z roku 2019 pod názvem *Increasing Learning from Accidents: A Systems Approach Illustrated by the UPS Flight 1354 CFIT Accident,* na které se taktéž podílela Nancy G. Leveson. [21]

6. Limitace současného stavu

Organizace ICAO udává jisté standardy, jak řídit bezpečnostní rizika a jak vést dokumentaci související s riziky a nebezpečími, avšak všechny tyto standardy jsou zaměřeny tradičním bezpečnostním inženýrstvím, a ne systémovým přístupem.

Přístup bezpečnostního inženýrství na nehody pohlíží jako na lineární řetězec poruchových událostí (viz Obrázek 5). Vyšetřování nehod se provádí pouze za účelem sestavení kauzálního lineárního řetězce a nalezení prvotní události, od které se řetězec následně vyvíjí. V současném stavu se bezpečnost zaměřuje především na lidskou chybu, a ne na systém, ve kterém člověk figuruje.



Obrázek 5 – Lineární řetězec událostí [15]

Systémový přístup naopak vůbec nepracuje s lineární kauzalitou. Dle tohoto přístupu, se kterým pracuje například prof. Nancy Leveson, neexistuje žádná prvotní poruchová událost, jelikož nehoda je způsobená nedostatečným řízením v systému a nedostatečnou kontrolou nad nebezpečími. Účel vyšetřování nehody je identifikování nedostatků v řídící struktuře a předcházet dalším ztrátám do budoucna. [15]

Lineární kauzalita je vhodná k použití na jednoduché nehody, avšak ne na dnešní komplexní sociotechnické systémy. Metody tradičního přístupu přestávají stačit reagovat na změny vzhledem k rychle se rozvíjejícím technologiím. S dobou se mění příčiny nehod, vytvářejí se nové druhy nebezpečí a narůstá komplexita systémů, ke kterým je zapotřebí přistupovat s novými předpoklady.

Využití STAMP modelu pomáhá pochopit, jak systém ve skutečnosti opravdu funguje, jelikož velmi často se pracuje s modely, které pohlíží na systém tak, jak byl navržen. K tomu je vhodný právě model STAMP, který je základem CAST metody. To ale ve skutečnosti není reálný model systému. Pomocí modelu STAMP lze odhalit, jak systém reálně funguje a poukazuje na nedostatky v řídící struktuře.

7. Metodika

Cílem práce je návrh architektury registru nebezpečí a rizik v organizacích provádějící údržbu založený na modelu STAMP. V údržbových organizacích probíhá mnoho procesů zároveň a celý systém by byl časově náročný namodelovat. Při nvárhu nové architektury registru nebezpečí a rizik se stačí zaměřit na nehodové události, které již v minulosti proběhly, a aplikovat na ně CAST analýzu. Výstupy CAST analýzy pomohou odkrýt nová systémová nebezpečí a rizika spojená s nimi. Dále se získají další bezpečnostní data z provozu údržby, která napomůžou zjistit, zda současné registry vyhovují dnešním potřebám v bezpečnosti v letectví.

Pro účely CAST analýzy je zvolena nehoda letu 236 společnosti Air Transat, jelikož se na této nehodě z velké části podílela především údržba prováděná na letounu několik dní před nehodou. Před aplikací samotné analýzy je zapotřebí nashromáždit všechna dostupná data a informace týkající se nehody z ověřených zdrojů. Pro tuto analýzu se vychází především ze závěrečné zprávy vydanou portugalským oddělení prevence a vyšetřování leteckých nehod. [22]

7.1 Let 236 společnosti Air Transat

Let TSC236 kanadské společnosti Air Transat se konal 24. 8. 2001 letounem A330. Let byl naplánován s odletem z letiště Toronto, Kanada (CYYZ) v 0010 UTC1 a příletem na letiště Lisabon, Portugalsko (LPPT). Na palubě bylo 13 lidí z letové posádky a 293 cestujících. [22]

V 0503 UTC1 letová posádka zpozorovala výstražná varování indikující nízkou teplotu a vysoký tlak oleje u pravého motoru (č. 2), načež posádka tento stav sdělila MCC („Maintenance Control Conter“) v Quebecu v Kanadě. V 0533 UTC1 se objevilo další varování na displeji Engine/Warning (E/WD), který znázorňoval nerovnováhu paliva v palivových nádržích. Vzhledem k těmto neobvyklým dvěma indikacím se posádka řídila manuálem, který se odkazoval na přečerpání paliva. Posádka zvolila zapnutí ventilu přečerpání paliva („Cross Feed Valve“) a zároveň vypnula pravá palivová čerpadla, aby pravý motor získal přísun paliva z levých palivových nádrží.

V 0545 UTC1 se úroveň paliva na palubě snížila pod minimum, které bylo potřeba k dokončení letu do Lisabonu. Kapitán vzápětí zvolil odklon na letiště Lajes (LPLA) na ostrově

Terceira na Azorských ostrovech. V 0554 UTC1 posádka reagovala na abnormální únik paliva zapnutím palivových čerpadel v pravém křídle a čerpadla v levém křídle vypnula.

Posádka opět kontaktovala MCC v 0559 UTC1, jelikož palivo abnormálně unikalo, načež MCC mělo podezření, zda by to nemohl být únik paliva v levém křídle. Na to kapitán reagoval vypnutím ventilu přečerpání paliva („Cross Feed Valve“) a opět zapnul čerpadlo v levém křídle.

V 0613 UTC ve FL 390 a 150 NM od letiště Lajes pravý motor ztratil tah. V 0623 UTC1 vyhlásil FO „Mayday“ určené Santa Maria Oceanic Control. V 0626 UTC1 v FL 345 a 65 NM od letiště Lajes vypadnul i levý motor. Posádka následně zahájila klesání s vypnutými motory směrem k letišti Lajes. V 0631 UTC byl let převeden na Lajes Approach Control. [22]

Posádka zahájila sestup a za pomocí radarových vektorů a světel přistávací dráhy se přiblížila k letišti Lajes. Letadlo bylo ve výšce 13 000 stop, když kapitán provedl sérii zatáček za účelem ztráty výšky. V 0645 UTC1 letoun přistál na dráhu 33 za maximálního brždění. Během prudkého dosednutí ve velké rychlosti prasklo 8 pneumatik z 12 a způsobilo menší požáry u levého podvozku. Po uhašení požáru kapitán nařídil nouzovou evakuaci. [22]

Celkově 14 pasažérů a 2 členové palubního personálu utrpěli lehké zranění, 2 pasažéři byli těžce zraněni. Letoun utrpěl strukturální poškození trupu a hlavního podvozku. [22]

7.2 Vliv údržby na nehodu

Portugalské oddělení prevence a vyšetřování leteckých nehod (GPIAA) uvedlo, že před nehodou údržba prováděla výměnu motoru, která by mohla být relevantní. [22]

Při rutinní inspekci letounu dne 15. 8. 2001 nalezla kovové třísky v pravém motoru (č. 2) od společnosti Rolls-Royce. Dne 17. 8. 2001 se tyto třísky nalezly opět a vzhledem k nejasné identifikaci původu se společnost Air Transat rozhodla vyměnit motor. K tomu byl použit motor zapůjčený od společnosti Rolls-Royce, který již dříve byl použit společností Air Transat. [22]

Během výměny motoru se zjistilo, že motor zaslaný společností Rolls Royce byl dodán bez hydraulické pumpy. Vedoucí technik se zmínil pracovníkům z oddělení „engineeringu“, kteří mu poradili použít součástku z nahrazovaného motoru. [22]

Během procházení dokumentace Airbus IPC se nalezl vydaný Servis Bulletin (SB). Technici zjistili, že zapůjčený motor byl v konfiguraci před vydaným SB a nahrazovaný motor byl v konfiguraci po vydaném SB. Technik, který vedl výměnu motoru, neměl přístup k vydanému SB, proto se nakonec řídil radou od pracovníků z oddělení „engineeringu". Podle techniků mezi palivem a přilehlou hydraulickou trubkou byla dostatečná vůle. Po dokončení výměny motoru byly provedeny kontroly jak vedoucím technikem, tak dalším technikem a nebyly zjištěny žádné nesrovnalosti. [22]

7.3 Závěr šetření

V závěru šetření GPIAA bylo zjištěno, že únik paliva byl způsoben prasknutím přívodové palivové trubky čerpadla na pravém motoru. Tření vzniklo následkem nedostatečnou vůlí v řádu milimetrů mezi hydraulickým potrubím a palivovým potrubím. V závěru taktéž byla uvedena série chyb spojená s výměnou motoru. Dále byla uvedena chyba letové posádky jako jedna z hlavních příčin nehody z důvodu neschopnosti identifikovat únik paliva, opomenutí vypnout „Cross Feed Valve" po zhasnutí prvního motoru a nedodržení standardních provozních postupů v možná více než jednom případě. [22]

8. CAST analýza nehody letu 236

Celá CAST analýza se aplikuje na nehodu přesně dle příručky „CAST Handbook" od paní profesorky Nancy G. Leveson. Všechny kroky jsou detailněji popsány v kapitole č. 4.

8.1 Základní informace k provedení analýzy

V prvním kroku analýzy CAST se definují hranice systému a prostředí, identifikují se systémová nebezpečí, bezpečnostní omezení a ztráty.

Systém je zacílen na p*rocesy v údržbě a postupy spojené s ní* a *letová posádka provádějící let.*

Systémové nebezpečí je definováno jako nebezpečí na úrovni systému. Takzvaná systémová nebezpečí se rozlišují na základě 3 kritérií:

- *Nebezpečí jsou stavy nebo podmínky systému (nikoli příčiny na úrovni komponentu nebo stavy okolního prostředí)*
- *Rizika povedou v nejhorším případě ke ztrátě*
- *Nebezpečí musí popisovat stavy nebo podmínky, kterým je třeba zabránit* [18]

Při definování systémového nebezpečí je důležité, aby nebezpečí bylo opravdu na úrovni celého systému, a ne uvažováno jako potenciální příčina nebezpečí. To se docílí definováním nebezpečí nevztahující se pouze k jednomu komponentu systému či k jedné části, kdežto k celému celkovému systému. [18]

Ke každému systémovému nebezpečí připadají **bezpečnostní omezení**, díky kterým se předchází nebezpečí a nakonec ztrátám. V řídící struktuře to znamená, že nadřazená úroveň přiřadí jistá omezení úrovni podřazené. [18]

Systémovým nebezpečím je v tomto případě *uvolnění letadla, které je nezpůsobilé letu*. Nebezpečí rozdělují na další dvě dílčí nebezpečí, které jsou blíže specifikovány.

Systémová nebezpečí a bezpečnostní omezení, která jsou relevantní k nehodě jsou:

H1: *uvolnění letadla, které je nezpůsobilé letu*

H1.1: *uvolnění letadla s nepovolenou konfigurací motoru a potrubí*

SC: Letadlo musí být uvolněno se správnou konfigurací motoru i potrubí

H1.2*: žádný z motorů nemá přísun paliva*

SC: Úroveň paliva musí být po určitých úsecích zkontrolována

SC: Únik paliva musí být detekován

SC: Hmotnost paliva odpovídající délce letu musí být předem efektivně spočtena

SC: Palivové nádrže musí mít rovnovážný stav paliva

Dále se definují **ztráty,** kterými utrpěly všechny zúčastněné strany, těmi jsou:

L1: *Ztráta některých funkcí potřebných k letu*

L2: *Ztráta tahu*

V poslední části prvního kroku se kladou **otázky** spojené s událostmi, které následně vedly ke ztrátám. jsou klíčové pro další kroky, kde se s těmito otázkami bude nadále pracovat. Otázkami, vyplývající ze sledu událostí, jsou:

- *Proč letadlu došlo palivo?*
- *Pokud to způsobila nevhodná špatná konfigurace motoru a potrubí, proč k tomu vůbec došlo?*
- *Proč se letadlo uvolnilo do provozu se špatnou konfigurací?*
- *Proč posádka zareagovala pozdě?*

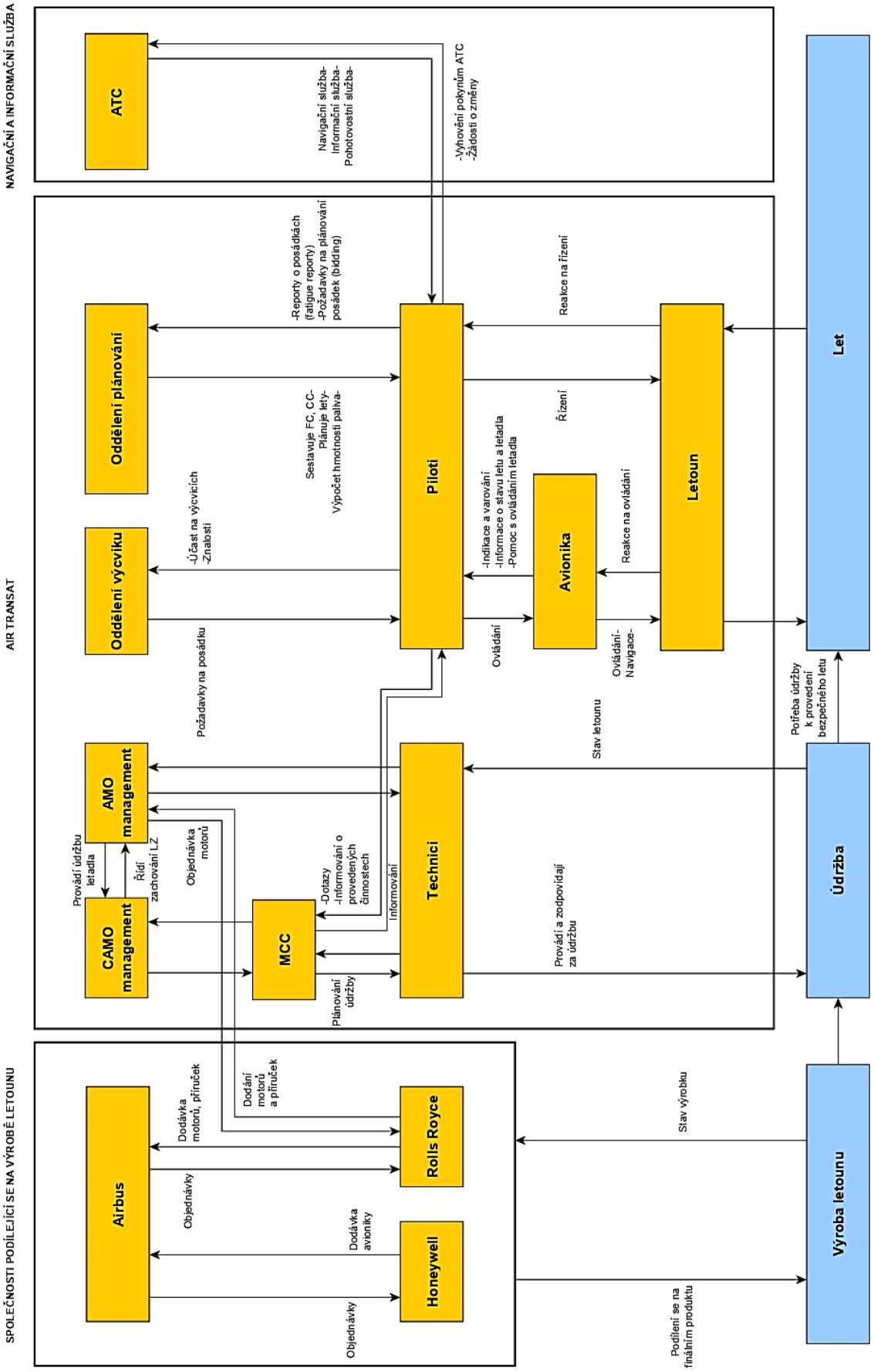
8.2 Modelování řídící struktury systému

Systémový přístup pohlíží na nehody jako na nedostatečné řízení, proto je zapotřebí namodelovat řídící strukturu v analyzovaném systému. K namodelování řídící struktury je zapotřebí znát procesy probíhající v systému, řídicí prvky a jejich odpovědnosti, řídicí akce a zpětné vazby.

V původním návrhu řídící struktury bylo zaimplementováno mnohem více prvků ve formě jednotlivých oddělení, které byla blíže specifikována, avšak při následné práci s analýzou se ukázalo, že tato oddělení nijak významně nezasahovala do procesů týkající se nehody či jejich činnosti nebyli relevantní k prováděné analýze, proto se řídící struktura zúžila na méně řídicích prvků.

V současné namodelované řídící struktuře, která lze vidět na Obrázek 6, působí tyto organizace:

- **Společnost Air Transat** – pod společnost následně spadá i organizace AMO a CAMO, kde nejdůležitějšími prvky v této analýze je MCC a technici
- **Společnosti podílející se na výrobě letounu** – pod tyto společnosti spadá společnost Airbus, který vyrábí letouny série A330; společnost Honeywell, který dodává avioniku do těchto letounů; společnost Rolls Royce, která dodává motory a zároveň zasílala náhradní motor společnosti Air Transat
- **Navigační a informační služba** – ATC



Obrázek 6 – Řídící struktura nehody letu 236 společnosti Air Transat

8.3 Analýza každého prvku řídící struktury

V tomto kroku se detailně analyzuje každý krok řídící struktury. Dále se definují jejich odpovědnosti, které jsou nějakým způsobem relevantní k nehodě.

Tento krok je rozdělen na dvě části. V části první se popíše řídicí prvek a jeho odpovědnost. V části druhé se zaměří na nebezpečné řídicí akce spojené s odpovědností řídicího prvku. K tomu je zapotřebí identifikovat vady v modelu systému a znát kontextuální faktory, které vychází ze závěrečné zprávy nehody. Po těchto identifikacích následuje sada otázek, kterýma lze odhalit systémové faktory přispívající k nehodě.

První část

Společnost Air Transat

Letoun

- Plnění všech svých funkcí – ovládání a řízení

Avionika

- Řízení letadla
- Varování a indikace
- Poskytnutí zadávání dat do NAV a PFD displejů
- Sledování letového plánu
- Zásah do rychlosti, výšky a polohy přední části letadla (kurz)

Piloti

Kapitán

- Řízení letadla dle postupů
- Ovládání autopilota
- Rozhoduje před odletem, zda výpočet hmotnosti paliva sedí na daný let
- Žádání ATC o případné změny
- Rozhoduje o odklonění či přistání

FO

- Kontrola operačních systémů a navigačního vybavení
- Analýza letových plánů a povětrnostních podmínek
- Monitorování trajektorie letu, nadmořské výšky, polohy, výkony, spotřeby paliva
- Listování v manuálech v případě potřeby
- Povinnosti na pokyn kapitána

Oddělení výcviku

- Výcvik posádek (FC, CC)
- Školení
- Předletová příprava posádek (briefing)

Oddělení plánování

- Zařazení posádek do provozu v souladu s letovým řádem
- Výpočet hmotnosti paliva
- Plánování, řízení, zabezpečování a vyhodnocování letů
- Odpovídá za sběr dat z letů

MRO organizace společnosti Air Transat

Technici

- Údržba systémů a zařízení
- Pravidelné kontroly systému
- Oprava nebo výměna poškozených dílů letadla
- Odstraňování problémů
- Uchovávání protokolů o údržbě a opravách

MCC

- Koordinace technických záležitostí se všemi ostatními provozními odděleními
- Koordinace zpětné vazby od letové posádky, organizací údržby atd.
- Sledování letové způsobilosti letadel
- Plánování úkolů údržby podle schváleného programu údržby letadla

CAMO management

- Vedení záznamů zachování letové způsobilosti
- Řízení příkazů zachování letové způsobilosti
- Poskytování údajů k údržbě
- Přejímka/předání letadel

AMO management

- Dohled nad prováděním údržby letadla
- Vydávání osvědčení o uvolnění do provozu po dokončení údržby

Společnosti podílející se na výrobě letounu

Airbus/Honeywell/Rolls Royce

- Výroba bezpečného produktu – letounu/avioniky/motorů
- Poskytnutí dokumentace zákazníkům a školicích materiálů

Navigační a informační služba

ATC

- Zajišťování rozestupů mezi letadly
- Monitorování trajektorie letu letadla a poskytování navádění pro přiblížení
- Poskytování informací o aktuálním počasí

Druhá část

Avionika

UCA: Neobjevila se žádná jasná jednoznačná indikace nebo varování, že by mohl nastat kritický únik paliva

Vady v procesním modelu a kontextuální faktory	Otázky
Avionika neměla žádný systém, který by jasně detekoval únik paliva a následně vydal jednoznačné varování.	*Proč avionika nemá žádný systém detekce úniku paliva s jasnou indikací?*

Tabulka 4 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „Avionika“

Doporučení:

- Zavést systém detekce úniku paliva do avioniky s jasně znějící indikací.

Piloti

UCA: Letová posádka nezjistila, že by mohl být problém s únikem paliva, dokud se nezobrazilo upozornění, že byla zaznamenána nerovnováha paliva.

UCA: Letová posádka zapnula ventil přečerpání paliva („Cross Feed Valve“)

Vady v procesním modelu a kontextuální faktory	**Otázky**
Posádka nebyla schopna porozumět varováním, které nejsou v této kombinaci časté.	*Proč posádka neporozuměla těmto indikacím? Není dostatečně vyškolená? Nebo se tyto indikace v této kombinaci nikdy nevyskytují? Indikoval systém varování nejednoznačným způsobem?*
Letová posádka si myslela, že je chyba v počítačích.	*Co vedlo piloty si toto myslet? Stalo se to už někdy předtím?*
Letová posádka provedla postup přečerpání paliva dle manuálu.	*Byl postup v manuálu napsán srozumitelně? Byl postup v manuálu správný? Měli správný manuál? Měli dostatek času přemýšlet nad více možnými scénáři či jinými postupy?*
Posádka nerozpoznala únik paliva, jelikož tomu nic z informací nenasvědčovalo.	*Měli správné informace? Jsou správně vyškoleni na takový kritický scénář? Měli postupy o úniku paliva zahrnuté ve výcviku?*

Tabulka 5 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „Piloti“

Doporučení:

- Implementovat simulace takovýchto kritických scénářů do výcviku pilota včetně školení na „únik paliva“.
- Dále zahrnout zřetelný postup týkající se úniku paliva do manuálů.

Technici

UCA: Vedoucí technik se během postupu výměny motoru řídil ústní radou pracovníka „engineeringu“

UCA: Vedoucí technik se neřídil SB

UCA: Technici použili hydraulickou pumpu z vyměňovaného motoru, který konfigurovali s motorem zapůjčeným

Vady v procesním modelu a kontextuální faktory	**Otázky**
Vedoucí technik se řídil ústní radou pracovníka z „engineeringu“	*Proč spoléhal na ústní radu? Proč se neřídil postupy? Měl vůbec k dispozici nějaké postupy? Nebyl to spíše nátlak ze strany „engineeringu“?*
Vedoucí technik byl v časové tísni	*Proč byli v časové tísni? Kdo nařídil rychle uvolnit letadlo do provozu?*
Vedoucí technik neměl momentálně přístup k SB. V počítači s přístupem k SB byla chyba v systému, kdy systém třikrát odmítl přístup technikovi. MCC mělo CD se všemi SB od firmy Rolls Royce, které nebyly využity.	*Proč technik neměl přístup k SB? Pokoušel se vůbec přístup k SB získat? Snažil se technik SB získat jiným způsobem? Věděl vůbec o jiném způsobu? Pokud ano, proč nevyužil CD s SB?*
Technici implementovali komponent silou z nahrazovaného motoru, aby seděl s ostatními komponenty.	*Proč použil starou součástku? Nebyla k dispozici jiná? Pokud nebyla, proč? Věděl vedoucí technik, že konfigurace je nesprávná? Pročetl si manuál o takové konfiguraci? Věděl, že tam není dostatečná vůle? Pokud ano, věděl, co to může způsobit? Měli tyto postupy ve školení?*

Tabulka 6 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „Technici“

Doporučení:

- Přezkoumání programu údržby a provozu, který povede ke zlepšení výkonu jeho činnosti zajišťování bezpečnosti
- Přezkoumání Safety Culture ve vedení aerolinky
- Zavedení školení o přesných postupech při nové instalaci pro veškerý technický personál

AMO management

UCA: Management trval na použití „starých" komponentů z vyměňovaného motoru

UCA: Oddělení kvality nevyžadovalo kontrolu instalace hydraulické pumpy, hydraulické trubky a palivové trubky

Vady v procesním modelu a kontextuální faktory	**Otázky**
Management trval na použití komponentů z vyměňovaného motoru, jelikož potřebovali uvolnit letadlo do provozu.	*Proč se spěchalo na uvolnění letadla do provozu?*
Oddělení uvolnilo letadlo s nezkontrolovanou instalací	*Proč se instalace neprověřila více detailněji? Pokud vše vypadalo v pořádku, co je k tomu vedlo?*

Tabulka 7 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „AMO management"

Doporučení:

- Zavést školení pro oddělení kontroly kvality v případě změny v systému

CAMO management

UCA: Uvolnění letadla s nepovolenou konfigurací motoru a palivového potrubí

Vady v procesním modelu a kontextuální faktory	Otázky
Uvolnění letadla s nepovolenou konfigurací	*Proč letadlo bylo uvolněné i přes nepovolenou konfiguraci? Věděla organizace, že je konfigurace nepovolená? Byla organizace v časové tísni?*

Tabulka 8 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „CAMO management“

Doporučení:

- Přezkoumání Safety Culture ve vedení aerolinky

MCC

UCA: Neposkytnutí CD s SB firmy Rolls Royce vedoucímu technikovi

Vady v procesním modelu a kontextuální faktory	Otázky
MCC nezvážili využití CD jako přístup k SB	*Proč pracovníci MCC nezvážili využití CD? Věděli, že technik nemá přístup k SB? Byli zaneprázdněni něčím jiným?*

Tabulka 9 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „MCC“

Doporučení:

- Přezkoumání Safety Culture ve vedení aerolinky

Rolls Royce

UCA: Dodání motoru bez hydraulické pumpy

Vady v procesním modelu a kontextuální faktory	Otázky
Motor byl zaslán společnosti Air Transat bez hydraulické pumpy a bez postupů a širších informací o konfiguraci nahrazovaných komponentů	*Proč společnost nezaslala hydraulickou pumpu? Měla vůbec hydraulickou pumpu k dispozici? Plánovala společnost zaslat hydraulickou pumpu se zpožděním? Proč se k motoru nezaslaly postupy s možnými konfiguracemi?*

Tabulka 10 – Vady v procesním modelu, kontextuální faktory a otázky pro prvek „Rolls Royce“

Doporučení:

- Vydání dokumentace specifikující konfiguraci motoru a ostatních komponentů

8.4 Identifikace nedostatků v řídící struktuře

V tomto kroku se už řídící struktura analyzuje jako celek, kdy se hledají systémové faktory, které přispěly k nehodě. K této analýze, avšak nejsou ve zprávě z šetření nehody všechny potřebné informace; ze zprávy lze alespoň využít co nejvíce relevantních dat, která by mohla být nápomocná k odhalení systémových faktorů. Lze si alespoň položit otázky, jejichž případným zodpovězením by se tak odhalily systémové faktory.

Komunikace a koordinace

- Jakým způsobem funguje komunikace mezi jednotlivými organizacemi v systému?
- Jakým způsobem funguje komunikace v organizaci Air Transat?
- Spolupracují jednotlivá oddělení spolu napříč systémem?

Návrh systému řízení bezpečnosti

- Byl již v té době zavedený SMS systém ve společnosti?
- Pokud ano, jak tento systém fungoval?
- Stalo se již něco podobného ve společnosti Air Transat?

Kultura bezpečnosti

- Naslouchá vedení pracovníkům v údržbových organizacích společnosti Air Transat?

Změny v systému a jeho prostředí v průběhu času

- Předcházely nějaké změny nehodě v systému?

Vnitřní a vnější ekonomické faktory

- Měla finanční tíseň nějaký vliv na nehodu?

8.5 Návrh doporučení a celková analýza

Všechna doporučení jsou navržena pod tabulkami z druhé části třetího kroku. Následuje celková analýza systému a nalezení systémových faktorů.

Během zpracování kauzálních scénářů a popisu vad v procesu včetně kontextuálních faktorů se zjistilo, že nejčastější vadou v řídící struktuře byl právě **nedostatek informací**, který následně způsobil nedostatečné řízení.

S tímto výstupem se nadále bude pracovat s jako důležitým aspektem při celkovém návrhu architektury registru rizik, kde se bude cílit především na **vazby mezi prvky**, zohledňovat **kauzální scénáře** spolu s vytvořenou **sadou otázek** vyplývající z identifikací vad v procesním modelu.

9. Návrh nové architektury registru nebezpečí a rizik

Jak již bylo zmíněno, v současnosti jsou běžně užívané registry nebezpečí a rizik reprezentovány tabulkou s množinou dat rozdělených pod jednotlivé položky. Vzhledem k současné práci s registry, kdy je posuzování jednotlivých položek individuální a bez dalšího kontextu, se nabízí zvolit systémový přístup, který využívá takové principy, které lépe chápou komplexní systémy.

Při návrhu nové architektury registru se stále uvažuje s jádrem stávajícího registru. Nadále se posuzují nebezpečí a rizika spojená s nimi, avšak v tomto návrhu jsou posuzovány z pohledu úrovně systému.

Výstupem z analýzy CAST, která byla aplikována na leteckou nehodu letu 236 společnosti Air Transat, bylo odhalení nedostatečného řízení, které následně vedlo k nebezpečným událostem. Primární příčinou byl především nedostatek informací, který opakovaně způsobil nedostatečnou zpětnou vazbu v systému na mnoha místech v řídící struktuře. Nedostatek informací způsobil neuspokojivě provedený proces údržby, který měl za následek několik nebezpečných událostí. Proto se implementace těchto aspektů do aplikačního návrhu soustředí především na řídící akce a zpětnou vazbu, které při správném řízení předchází kauzálním scénářům.

9.1 Registr nebezpečí a rizik

Nový návrh architektury registru nebezpečí a rizik lze vidět v Tabulka 11. Ve sloupcích jsou nově navržené atributy a data zanesená v registru jsou převzaté výstupy z analýzy CAST provedené na nehodě letu 236 společnosti Air Transat.

K zpřehlednění tabulky jsou data podbarvená; data modře podbarvená jsou všechny související aspekty náležící k systémovému nebezpečí H1 a data růžově podbarvená náleží k systémovému nebezpečí H2.

Registr nebezpečí a rizik											
ID	Systémová nebezpečí (H)	Ztráty (L)	Bezpečnostní omezení (SC)	Řízený proces	Řídící prvek	Odpovědnost	Řídící akce	Zpětná vazba	Kauzální scénář (UCA)	Hodnocení rizika	Datum zápisu do registru
1	Uvolnění letadla s nepovolenou konfigurací motoru a potrubí	Ztráta některých funkcí potřebných k letu	Letadlo musí být uvolněno se správnou konfigurací motoru i potrubí	Provádění údržby na letadle	Technici	Provádí údržbu dle ověřených a schválených postupů a předpisů	Instalace motoru do letounu	Stav letounu odpovídajícímu vykonanému procesu	UCA 1	Elim.	15.02.2022
2	Žádný z motorů nemá přísun paliva	Ztráta tahu	Úroveň paliva musí být po určitých úsecích zkontrolována	Kontrola stavu paliva	Pilot	Kontroluje stav paliva po určitých úsecích letu	Kontroluje stav paliva	FMS vykazuje aktuální stav paliva	UCA 2	Elim.	15.02.2022
									UCA 3	Elim.	
			Únik paliva musí být detekován	Detekce úniku paliva	ADIRU	Zpracovává data o úniku paliva	Vydá varování při úniku paliva	Potenciometry v nádrži poskytují data o hladině paliva	UCA 4	Elim.	
									UCA 5	Elim.	
									UCA 6	Elim.	
			Hmotnost paliva odpovídající délce letu musí být předem efektivně spočtena	Výpočet hmotnosti paliva	Oddělení plánování letů	Plánování výpočtů paliva	Zasílá pilotovi vypočtenou hmotnost paliva na daný let	Souhlas/ nesouhlas ze strany pilota s plánem	UCA 7	Nízké	
			Palivové nádrže musí mít rovnovážný stav paliva	Kontrola stavu palivových nádrží	Pilot	Kontroluje rovnovážnost paliva v palivových nádržích	Pilot manipuluje s přečerpáním paliva v případě potřeby	Palivo se přečerpává mezi nádržemi	UCA 8	Nízké	

Tabulka 11 – Návrh nové architektury registru nebezpečí a rizik

Registr může být použit jak retroaktivním způsobem, tak způsobem proaktivním. V případě, že se stane nehoda či incident, aplikací CAST analýzy se získají potřebná data, která lze následně implementovat do navržené architektury registru. Organizace musí k řízení rizik přistupovat ale také proaktivně, proto se doporučuje aplikovat STPA analýzu na řízené procesy v organizaci, aby se odhalila nebezpečí a posílilo řízení v organizaci, zavedla se nová bezpečnostní omezení a tím se tak předcházelo nehodám. Proto je v tomto návrhu popsáno, jak lze využít data v praxi jak z STPA analýzy, tak z analýzy CAST.

Vzhledem k rozsáhlému počtu dat vztahující se k nějakým z atributů navržené architektury registru je zapotřebí provést úpravu databáze. K tomu poslouží databázový relační model, kde jsou jednotlivé tabulky (databáze) vzájemně propojeny, kde výchozí databází je registr nebezpečí. (Celkový návrh databáze je detailněji popsán níže.)

Systémové nebezpečí

Celý návrh architektury registru se odvíjí od identifikace systémového nebezpečí. Aby již opětovně nedocházelo k nedostatečnému řízení v systému, návrh architektury registru obsahující jednotlivé atributy musí být zacíleny na celý systém, nikoliv na jednotlivé komponenty systému. Aby se tohoto přístupu dosáhlo, nestačí pracovat s nebezpečím tak, jak ho chápe bezpečnostní inženýrství, ale s nebezpečím systémovým.

Definice systémových nebezpečí je základem jak pro analýzy CAST, tak i pro analýzu STPA. Od tohoto atributu se následně odvíjí i celý registr s nově navrženou architekturou. *Cílem je začít od nebezpečí a určit, jaké podmínky v řízeném procesu by mohly přispět k tomuto nebezpečnému stavu.* [18]

Při práci s registrem je definice systémového nebezpečí velice klíčová, kdy je zapotřebí zacílit na úroveň celého systému, nikoliv ji uvažovat jako potenciální příčinu nebezpečí. Taktéž je nezbytné vyhnutí se nadměrným detailům. Nebezpečí se musí týkat pouze takových faktorů, které mohou být nějakým způsobem řízeny. (Například nebezpečí související s počasím se nepovažuje za systémové.) Během identifikování nebezpečí je zapotřebí jej definovat přesně bez použití termínů, jako jsou „nebezpečné“ či „náhodné“. [18]

Zpravidla se v systému identifikuje maximálně 7–10 systémových nebezpečí, avšak pokud je prováděná analýza rozsáhlá a systémová nebezpečí je potřeba detailněji identifikovat, lze si vytvořit tzv. **dílčí systémová nebezpečí,** která více zpřesňují danou

situaci a zpřehledňují analýzu. V takovém případě by se v navržené architektuře pouze přidal sloupec s názvem „dílčí systémová nebezpečí", kdy by poměr byl *1 : n*, tedy na jedno systémové nebezpečí by připadalo více dílčích.

Ztráty

Určení potenciálních ztrát je stěžejní pro organizaci z důvodu *ujasnění si priorit*. Ztráta může být hmotná – ztráta lidských životů – či nehmotná – ztráta důvěry zákazníka. V případě CAST analýzy se definují takové ztráty, kterými už utrpěla nějaká ze zúčastněných stran. V případě STPA analýzy se definují potenciální ztráty, kterými by organizace, či zúčastněné strany, nerada utrpěla.

Na rozdíl od systémového nebezpečí se v případě definování ztrát lze ohlížet i na faktory, které nemohou být řízeny. [18] Během definování ztrát může vyplynout i více ztrát náležící k jednomu nebezpečí, neboť poměr mezi ztrátami a nebezpečími je *n : n*, tzn. že k jednomu systémovému nebezpečí může připadat více ztrát a na jednu ztrátu může připadat více systémových nebezpečí.

Bezpečnostní omezení

Po dodržení všech principů definování systémového nebezpečí a ztrát je potřeba se zamyslet nad bezpečnostními omezeními, která jsou *potřebná k předcházení nehodám.* Model STAMP pracuje s omezeními jako předcházení nebezpečí, díky čemuž se následně předejde i ztrátám. Pokud jsou tedy některá z bezpečnostních omezení porušena, může to vést spolu s dalšími faktory k incidentu či nehodě. Proto je potřeba si je definovat hned v začátcích, aby se znala všechna omezení připadající na nebezpečí.

Poměr systémového nebezpečí a bezpečnostního omezení je *n : n*, to znamená, že na jedno nebezpečí může připadat více omezení k předcházení nehodě a na jedno omezení se může vztahovat více nebezpečí.

Řízený proces a jeho atributy

Při aplikaci CAST analýzy na nehodu bylo nejdříve zapotřebí definovat, *co* se vlastně stalo, než se analyzovalo, *proč* se to stalo. Stejný způsob lze využít i prediktivně v navržené architektuře registru. K tomu je nutné porozumět **řízeným procesům**. K zabránění vzniku potenciálního nebezpečí se musí nalézt nedostatečné řízení. Toho lze docílit identifikací řízeného procesu a analýzy všech aspektů hrající roli v regulační smyčce. Zprvu se

definuje řízený proces a co v procesu probíhá za interakce, poté se pohled upře na to, jakým způsobem by v řízení mohly vzniknout nedostatky.

Řízené procesy jsou ovládány **řídicím prvkem** pomocí **řídící akce**, což jsou další nezbytné atributy v registru. Řídicí prvek jistými mechanismy řídí a kontroluje chování procesu pomocí udržování bezpečnostních omezení, následně dostává **zpětnou vazbu**, která poskytuje informace o skutečném stavu řízeného procesu. Pokud je zpětná vazba nedostatečná či nesprávná, může způsobit nedostatečné řízení.

Pokud řídicí prvek nedostatečně vynucuje bezpečnostní omezení, může dojít k nehodě či incidentu. Řízený proces může být řízen více řídicími prvky, z toho vyplývá, že k procesu může vést i více řídicích akcí a zpětných vazeb.

Každý řídicí prvek má jednu či více **odpovědností** či přidělené povinnosti, které souvisí s vynucováním bezpečnostních omezení a jsou plněny pomocí řízení aktuálního stavu řízeného procesu. V registru jsou vypsány takové odpovědnosti, které jsou pouze relevantní k řízenému procesu, nikoliv všechny odpovědnosti náležící danému prvku.

Systémové nebezpečí je se všemi výše zmíněnými atributy v poměru *1 : n*, tedy na 1 nebezpečí může připadat více řízených procesů, prvků a vazeb.

Kauzální scénář

Jak vychází z CAST analýzy, nebezpečné řídicí akce způsobily velmi často neuspokojivě provedený proces údržby, který měl za následek několik nebezpečných událostí. Proto se musí zacílit právě na tyto nebezpečné řídicí akce, které následně mohou způsobit kauzální scénáře. Jelikož kauzálních scénářů mohou být až desítky, takové velké množství dat by v registru nebezpečí a rizik nebylo přehledné pro uživatele. Proto je zavedena Tabulka 12, která je následně níže popsána.

Riziko

Hodnocení rizika dle ICAO matice rizik se určovala předpokládaná pravděpodobnost a závažnost následků nebezpečí. V případě systémového nebezpečí počítá zcela odlišným způsobem. Popis hodnocení rizika dle systémového přístupu vyžaduje rozsáhlejší popis kroků, a proto jsou výpočty a snížení rizika zaneseny v samostatné Tabulka 13 a popsány v samostatné kapitole níže. Metodika, ze které se vychází je již popsána v teoretické části.

Datum zápisu do registru

Posledním atributem v registru je „datum zápisu do registru“. Aby registr rizik byl vůbec účinný, musí být pravidelně aktualizovaný. Nebezpečí se mohou časem měnit; některá mohou zanikat vzhledem k rychlosti rozvoje dnešní doby související s technologickým vývojem. Tím vznikají nová nebezpečí, která musí být brána v potaz. Při každé aktualizaci systémového nebezpečí či souvisejících atributů je zapotřebí aktualizovat taktéž i datum.

9.2 Kauzální scénáře

Jelikož jsou kauzální scénáře způsobeny nebezpečnými řídicími akcemi a případnými kontextuálními faktory, je v tomto návrhu cíleno na všechny jednotlivé řídicí akce. Ty se musí detailně zanalyzovat a zvážit, co všechno by mohlo způsobit nedostatečné řízení, které následně může vést k nehodám a ztrátám. Takových scénářů může být pak přirozeně až desítky. Příklady kauzálních scénářů jsou vypsány v Tabulka 12)

V případě STPA analýzy se to nazývá *nebezpečná řídicí akce (UCA – „Unsafe Control Action“), což je taková řídicí akce, která v konkrétním kontextu a prostředí nejhoršího případu vede k nebezpečí.* [18] Existují 4 způsoby, jak může řídicí akce potenciálně vést k nebezpečí:

1. Neposkytnutí žádné řídicí akce
2. Řídicí akce je provedena nevhodným způsobem vedoucí k nebezpečí
3. Řídicí akce je provedena příliš pozdě, brzo, nebo ve špatném pořadí
4. Řídicí akce trvá moc dlouho, nebo byla zastavena příliš brzy. [18]

Během identifikování UCA se musí specifikovat kontext, jakým se řídicí akce stává nebezpečnou pro systém a jaké skutečné stavy, podmínky či okolní vjemy mohly narušit řídicí akci.

CAST analýza se zase zaměřuje na vady v procesním modelu a zvažují se kontextuální faktory. Zde se popisuje, *jak prvky přispěly* k nehodě pomocí nebezpečné řídicí akce. Z toho plynou otázky, *proč se to tak stalo.* Tento aspekt je velice důležitý v této tabulce, jelikož po zodpovězení těchto otázek vyplyne série odůvodnění – v tabulce zapsané jako **možné důvody**, které ovlivnily či co mohly ovlivnit nebezpečnou řídicí akci. Tyto možné důvody jsou pak klíčoví pro práci s rizikem, konkrétně jeho zmírnění a zavádění nápravných opatření.

Kauzální scénář (UCA)				
ID	**ID s. nebezpečí**	**Řídící akce**	**Kauzální scénář (UCA)**	**Možný důvod**
UCA 1	H1	Instalace motoru do letounu	Pracovníci MRO nesprávně nakonfigurují motor a potrubí	Pracovníci MRO nemají informace, jak správně konfiguraci provést
				Pracovníci MRO neměli správné předpisy a postupy
				Pracovníci MRO nemají správné nástroje
UCA 2	H2	Kontroluje stav paliva	Stav paliva není vůbec zkontrolován	Pilot neví, jak ho má zkontrolovat
				Pilot neví, kdy ho má zkontrolovat
UCA 3	H2	Kontroluje stav paliva	Stav paliva je zkontrolován, ale moc pozdě	Pilot neví, kdy ho má zkontrolovat
				Pilot byl zaměstnán jinými důležitějšími procesy
UCA 4	H2	Vydá varování při úniku paliva	ADIRU nevydá varování o úniku paliva	Senzory detekce špatně snímají
UCA 5	H2	Vydá varování při úniku paliva	ADIRU vydá varování o úniku paliva, ale pozdě	ADIRU špatně vyhodnotí vstupní data
UCA 6	H2	Vydá varování při úniku paliva	ADIRU vydá falešné varování	Senzory detekce špatně snímají
UCA 7	H2	Plánování přesného množství paliva na daný let	Oddělení plánování letů naplánuje méně paliva, než je potřeba	Špatná kalkulace
				Finanční tíseň ze strany managementu (při nadbytečném množství letoun spaluje více paliva)
UCA 8	H2	Pilot manipuluje s přečerpáním paliva v případě potřeby	Pilot nevhodně přečerpá palivo dle instrukcí z manuálu	Pilot nemá dostačující vstupní informace k provedenému úkonu

Tabulka 12 – Kauzální scénáře (UCA)

V případě STPA na jedno systémové nebezpečí připadá minimálně 1 až spíše série několika UCA a zároveň na jedno UCA připadá více systémových nebezpečí. V případě CAST analýzy se pracuje s jedním systémovým nebezpečím, na které připadá několik kauzálních scénářů, avšak ne naopak. Tabulka 12 kauzálních scénářů je však navržena tak, že lze pracovat s oběma analýzami.

Tabulka se odkazuje na **řídicí akce** z Tabulka 11 registru nebezpečí a rizik. Ke každému systémovému nebezpečí – kterému je přiděleno **ID systémové nebezpečí** – náleží příslušná řídicí akce. Následně se identifikuje kauzální scénář, který je způsoben nebezpečnou řídicí akcí. Ke každému kauzálnímu scénáři je přiděleno ID, které je pak zapisováno jako **UCA 1, UCA 2**, atd. pro lepší přehled v tabulce.

Tabulka je doplněna jak o reálné kauzální scénáře vycházející z CAST analýzy, tak i kauzální scénáře, které by vznikly v případě STPA analýzy při práci s nebezpečnou řídicí akcí. Například UCA 1 a UCA 7–8 jsou reálné scénáře vycházející z analýzy CAST aplikované na nehodu letu 236, kdežto UCA 2–6 jsou pouze názorné příklady kauzálních scénářů v případě, že by se pracovalo s analýzou STPA.

9.3 Hodnocení rizika dle systémového přístupu

Riziko se hodnotí dle metodiky vyvinuté na MIT univerzitě, která je založená na systémovým přístupu. V Tabulka 13, kde jsou zaneseny hodnoty pro hodnocení rizika, se odkazuje na jednotlivé **kauzální scénáře** z Tabulka 12, se kterými se následně pracuje.

V tabulce hodnocení rizika je každé riziko přiřazené k jednomu kauzálnímu scénáři, to znamená, že poměr je *1 : 1*. Každý kauzální scénář má své **ID UCA** a ohodnocen závažností **PMS** („Pre-Mitigation Severity"), tedy hodnotou závažnosti připadající na riziko před zavedeným způsobem zmírnění. Pokud je PMS předem neznámo, zvolí se ta nejhorší možná závažnost, která je hodnotou 1. Jelikož jsou tabulky provázané přes kauzální scénáře, navazuje se na možné důvody z Tabulka 12, které jsou základem pro **zmírnění rizika** (RM – „Risk Mitigation").

Zavedených způsobů, jak zmírnit riziko, může být několik, naopak systémový přístup pracuje s kombinací takových způsobů. Čím více zavedených způsobů zmírnění rizika, tím více se úroveň rizika snižuje. Ke každému způsobu zmírnění rizika připadá identifikační číslo **ID RM, úroveň snížení rizika** a hodnocení **MES** („Mitigation Effectivness Score"), tedy hodnota síly potenciálních způsobů zmírnění rizika. V případě více hodnot MES následuje

výpočet hodnoty **CMES** („Combined Mitigation Efectivness Score“), která je kombinací všech MES pro daný kauzální scénář. V případě, že je navržen pouze jeden způsob zmírnění, hodnota CMES je úměrná hodnotě MES.

Po získání hodnoty CMES určující výslednou účinnost zmírnění rizika je zapotřebí ještě získat hodnotu **CPMS** („Combined Post Mitigation Severity“), která určuje závažnost rizika po aplikaci všech způsobů zmírnění rizika. K tomu je zapotřebí nejdříve určit hodnotu **PPMS** („Post-Potential Mitigation Severity“), která znázorňuje potenciální dopad změny závažnosti každého jednotlivého zmírnění. Ta se určuje podle toho, jakou má schopnost snížit původní hodnotu PMS. Kombinací všech PPMS hodnot je výsledná hodnota CPMS. V případě, že existuje pouze jedna hodnota PPMS na jeden kauzální scénář, výsledná hodnota CPMS je úměrná této hodnotě.

Výsledné riziko se určí na základě hodnot CMES a CPMS, které přísluší náležitým hodnotám z matice hodnocení rizik dle systémového přístupu.

V tabulce jsou vybrány takové kauzální scénáře, které jsou názornými příklady pro pochopení hodnocení rizika. V případě UCA 1 a UCA 3 se nabízí zavést více prostředků zmírnění rizika, což je nejefektivnějším způsobem, jak snížit riziko kauzálního scénáře, a proto je výsledné riziko eliminováno. V případě UCA 7 se nabízí zmírnění rizika pouze jedním způsobem, který má nízkou hodnotu MES, proto riziko není zcela eliminováno.

Hodnocení rizika										
ID UCA	Kauzální scénář (UCA)	PMS	ID RM	Doporučené snížení rizika	Úroveň snížení rizika	MES	CMES	PPMS	CPMS	Riziko
UCA 1	Pracovníci MRO nesprávně nakonfigurují motor a potrubí	1	RM01	Dodání příruček a manuálů	Redukce vlivem návrhu systému	3	ELIMIN. (F)	4	4	Eliminováno
			RM02	Dodání správných nástrojů	Redukce vlivem návrhu systému	3		4		
			RM03	Dodání správných postupů včetně zaškolení	Redukce vlivem návrhu systému	3		4		
			RM04	Zavedení školení a instruktáže	Školení a instruktáž	1		2		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
UCA 3	Stav paliva je zkontrolován, ale moc pozdě	1	RM07	Nainstalovat systém připomenutí kontroly stavu paliva po určitých úsecích letu do avioniky	Redukce vlivem návrhu systému	3	ELIMIN. (F)	4	3	Eliminováno
		1	RM08	Zavést školení a instruktáž	Školení a instruktáž	1		2		
UCA 4	ADIRU nevydá varování o úniku paliva	1	RM09	Zavést duplicitní systém detekce úniku paliva do avioniky	Eliminováno	X	ELIMIN. (F)	4	4	Eliminováno
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
UCA 7	Oddělení plánování letů naplánuje méně paliva, než je potřeba	1	RM13	Úprava programu plánování letů za účelem zlepšení přesnosti výpočtů paliva pro takovéto kritické scénáře	Redukce vlivem návrhu systému	3	MÍRNÉ (C)	4	4	Nízké

Tabulka 13 – Hodnocené riziko dle systémového přístupu

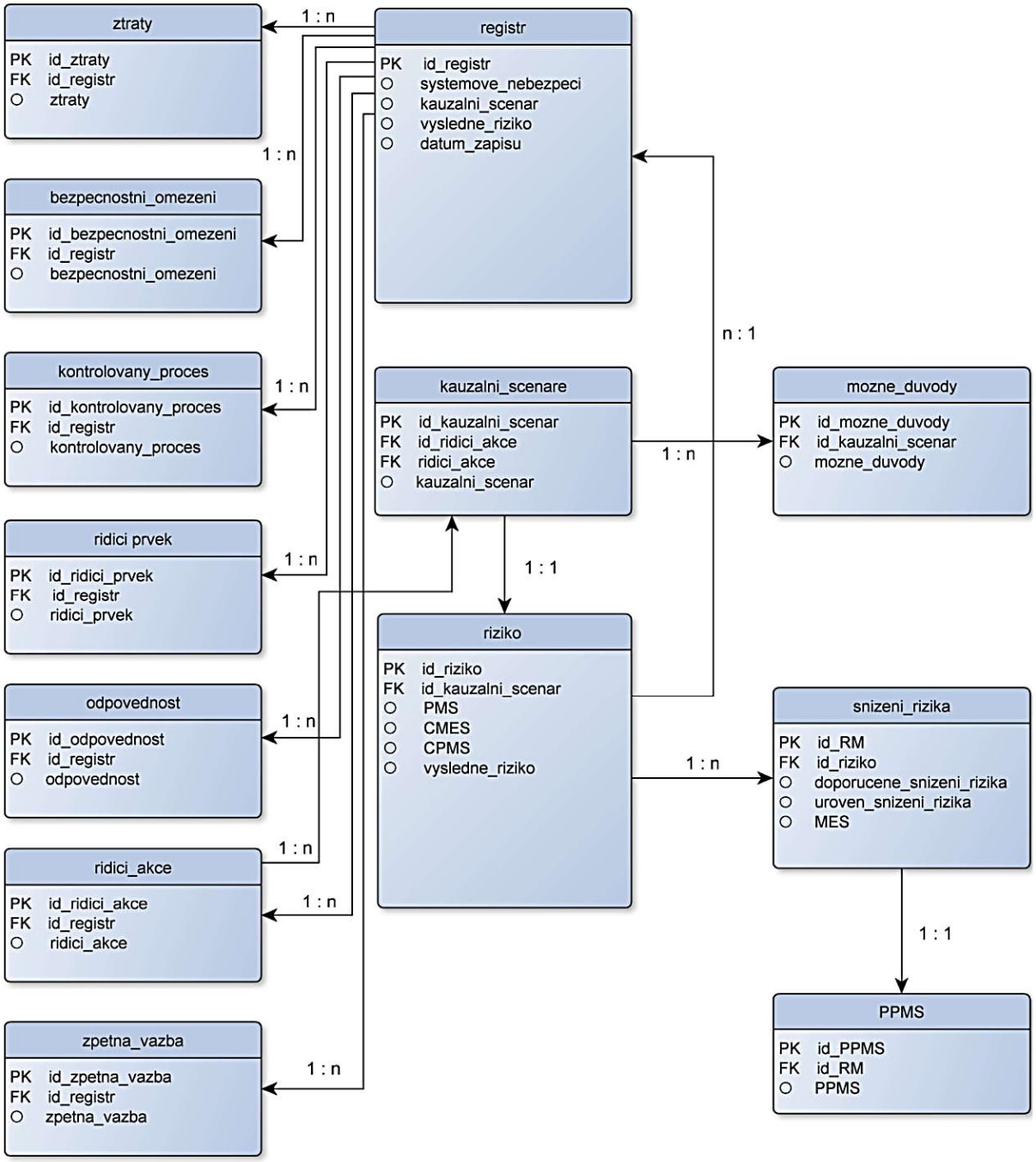
10. Aplikační návrh

Vzhledem k velkému množství dat je zapotřebí zajistit jejich vhodné uložení. K tomu je vytvořen databázový relační model, kde vznikají další tabulky provázané relačními vazbami cestou cizích klíčů. Databázový relační model zpřehlední a umožní využití uložených dat v praxi.

Diagram návrhu celkové databáze je znázorněn na Obrázek 7. Základem každé databáze jsou **entity**, které představují jednotlivé tabulky, dále to jsou **atributy** spadající pod entity a **vztahy** mezi jednotlivými entitami. Databáze jsou vzájemně propojeny vztahy a navzájem se na sebe odkazují; to je zajištěno pomocí identifikačních čísel ID. Pro každou entitu je vytvořen primární klíč (*PK* – Primary key), pokud se databáze odkazuje na jinou entitu, je tak zajištěno cizím klíčem (*FK* – Foreign key). Ostatní atributy označeny bodem jsou bez vztahových relací. Navržený relační model databáze je jeden ze způsobů, jak uložit data, se kterými se v tomto návrhu pracuje. Vzhledem k tomu, že diagram návrhu relačního databázového modelu není určen k výsledné reprezentaci, je zapotřebí tato data čitelněji prezentovat. Proto všechny navržené tabulky, které jsou již výše znázorněny, jsou ukázkou jako jednou z možností výsledné grafické reprezentace dat, kterou uvidí uživatel.

V praxi je aplikační návrh a jeho realizace mnohem složitější, je nutné užití mnoha filtrů a kategorizace výstupních dat. Zjednodušeným příkladem může být třídění produktů v rozsáhlejším internetovém obchodě, kde se uplatňují stejné principy při práci s daty. I v této reprezentaci se uvažuje forma rozevíracích seznamů, kdy položka zvolená v jednom seznamu ovlivní obsah výpisu dalšího seznamu.

V případě, že výsledná reprezentace dat je v tištěné verzi, tabulky či části v tabulce by se odkazovaly na jiné za účelem přiřazení souvisejících (nebo odpovídajících) dat.



Obrázek 7 – Diagram návrhu databázového relačního modelu

Výše navržený relační model vychází primárně z tabulky **registru.** Vzhledem k tomu, že v registru na jedno systémové nebezpečí může připadat *n* dalších atributů, všechny tyto položky musí být navrženy jako samostatné tabulky, které jsou propojeny pomocí klíčů.

Tabulka **kauzálních scénářů** se odkazuje na tabulku **řídící akce,** jelikož tento atribut je klíčový pro navrženou tabulku. Na jeden kauzální scénář připadá *n* možných důvodů, proto jsou kauzální scénáře navrženy v samostatné tabulce.

Tabulka **hodnocení rizika** je provázaná s tabulkou kauzálních scénářů, jelikož jedno hodnocené riziko připadá na jeden kauzální scénář. Jelikož způsobů, jak snížit riziko, je více, data jsou uložena v samostatné tabulce, na kterou se odkazuje výpočet PPMS.

Registr nebezpečí a rizik se následně odkazuje na tabulku hodnocení rizika, kde je provázán přes kauzální scénáře a hodnocení rizika.

11. Validace navrženého řešení

Validace práce byla prodiskutována na základě prostudování diplomové práce odborníkem z praxe, který má dlouholeté zkušenosti s provozní bezpečností jako *Safety Inspector ve společnosti Letiště Praha* a bývalý pracovník oddělení *Infra Engineering Co-op Safety and Reliability ve společnosti GE Aviation*.

V rámci validace byly shledány následující nedostatky:

1. **Vyjmenovaná nebezpečí nejsou kompletní**

V případě přístupu, kde se pracuje s kauzalitou, se generují desítky různých nebezpečí, která jsou kategorizovány, avšak v systémovým přístupu jich mnoho na systém nepřipadá.

Paní profesorka Nancy G. Leveson, autorka modelu STAMP, která vydala příručky „STPA Handbook" a „CAST Handbook", uvažuje počet systémových nebezpečí pouze 7 – 10 na celý systém, tedy na celý systém, kde probíhá více procesů, se jich mnoho nevztahuje. V případě potřeby bližší specifikace jednotlivých systémových nebezpečí lze definovat sérii dílčích systémových nebezpečí spadající pod jedno systémové nebezpečí.

Autorka také vydala publikaci „Increasing Learning from Accidents, A Systems Approach illustrated by the UPS Flight 1354 CFIT Accident", kde popisuje nehodu letu 1354 UPS, kdy identifikuje pouze jedno systémové nebezpečí na celou nehodz a tím je „CFIT".

2. **Návrh postrádá komplexní či systematický pohled**

Návrh architektury je navržen tak, že obsahuje všechny důležité výstupy vycházející z analýzy CAST. Architektura registru je navržena pro následné použití bezpečnostních dat vycházející jak z CAST analýzy, tak z analýzy STPA. V architektuře se začíná identifikací systémového nebezpečí a dat z řídící struktury, následuje výčet kauzálních scénářů, kde se hledají systémové faktory přispívající k nehodě. Po nalezení těchto faktorů lze následně snížit potenciální riziko. Z výše zmíněných důvodů je návrh vhodný pro komplexní systémy.

Data jsou následně uložena pomocí databáze, kde jsou jednotlivé tabulky propojeny přes cizí klíče, čímž celý návrh získává systematičnost a lze využít i v praxi.

3. Hodnocení rizik není jednoznačně pochopitelné

Hodnocení rizika je detailněji popsáno v teoretické části, na kterou je odkazováno z části praktické. V případě hodnocení rizika se postupovalo dle metodiky vyvinuté taktéž na MIT, která je založená na modelu STAMP, tudíž to není metodika nově navržená.

4. Rizika jsou hodnocena velmi mírně

Hodnocení rizika vychází z metodiky již výše zmíněné. Autorka této metodiky zavádí takové způsoby opatření a pracuje s jejich kombinacemi, aby se riziko snížilo. Pokud výsledná hodnota vyjde vysoká, znamená to, že se zavedly nevhodné či málo účinné způsoby snížení rizika, což by následně mohlo vést ke ztrátám, kterými by organizace utrpěla.

Diskuze

Tato práce nabízí ucelený pohled na problematiku systémové bezpečnosti zaměřenou primárně na oblast údržby letadel, ale také s přesahem do jiných odvětví letectví. Výše uvedený postup k řešení práce byl založen na předložení teoretických informací týkajících se systémového přístupu k bezpečnosti, což bylo podpořeno praktickou aplikací těchto informací a znalostí na příklady z reálného provozu, ať už v podobě CAST analýzy nehody letu 236, nebo návrhu registru nebezpečí a rizik pro využití v reálném provozu organizací MRO. Lze se domnívat, že tento předložený výzkum nabízí nové unikátní poznatky využitelné pro další výzkum v dynamickém prostředí odvětví bezpečnosti v civilním letectví. Jak lze vidět, organizace MRO jsou jedním z pilířů civilního letectví, a bezpečnost při údržbě letadel tvoří nedílnou součást jejich provozu, jenž indikuje důležitost přínosů této diplomové práce.

Nehoda společnosti Air Transat detailně popsána v kapitolách 7 a 8 reprezentuje datový vzorek pro další řešení práce a pro následnou validaci návrhu registru v kapitole 9 a 10. Aplikace CAST analýzy na tuto nehodu jednoznačně přinesla zajímavé otázky k jednotlivým řídícím prvkům, jenž měli na průběh letu zásadní vliv. Míra hloubky provedení této analýzy, ať už v podobě rozlišovací úrovně při modelování řídící struktury systému, nebo v podobě analýzy odpovědností každého řídícího prvku v systému byla zvolena s ohledem na potřeby této práce. Lze se domnívat, že při detailnějším rozboru řídící struktury systému, by bylo možné získat relevantnější závěry. Tak detailní analýza by ale vyžadovala znalost konkrétní řídící struktury v společnosti Air Transat, detailní znalost vazeb mezi prvky v systému, jenž rozhodně nejsou veřejné informace, a tudíž je nešlo použít.

Předložený návrh registru nebezpečí a rizik nabízí perspektivní a flexibilní řešení pro systém řízení provozní bezpečnosti v organizaci MRO. Architektura registru byla koncipována v souladu s moderním řešením bezpečnosti založeným na systémovém přístupu, jenž představuje jeden z hlavních rozdílů mezi již existujícími registry a zdejším návrhem. Registr byl navržen tak, aby byl schopen pojmout veškerá data vycházející z modelu STAMP. Dále aby vynikl svým UI – User Interface, které závisí na konkrétní grafické implementaci registru v organizaci, nicméně předložené tabulky v kapitole 10 nabízí jeden z možných grafických výstupů. V neposlední řadě registr disponuje zajímavým

řešením uchovávání dat jako databázový relační model, podporující přehlednost a integritu dat.

Jak lze vidět v kapitole 10, validace návrhu registru proběhla v podobě počátečního načítání dat vycházejících z nehody společnosti Air Transat. Jak lze vidět v tabulce 11, 12, 13, i menší množství dat poskytuje relevantní závěry přímo použitelné v organizaci MRO, a nabízí relevantní způsob hodnocení rizika a nebezpečí v souladu se systémovým přístupem. Je tedy jasné, že při kontinuální práci s registrem, výstupních dat bude mnohem více, a to vše při zachování přehlednosti a UI. Tímto lze návrh registru prokázat jako úspěšný.

Závěr

Cílem této práce bylo vytvoření návrhu architektury registru nebezpečí a rizik založeném na bezpečnostním modelu STAMP v MRO organizacích, který má obsahovat data o řídící struktuře, nebezpečí, rizika a nápravná opatření. K tomu bylo zapotřebí porozumět procesům týkající se provozní bezpečnosti v organizacích a jejich následnou práci s rizikem.

Z analýzy současného stavu bylo zjištěno, že metodika současně vedených registrů posuzuje rizika a nápravná opatření bez jakéhokoliv dalšího kontextu, a proto tyto registry nemusí být vhodné na hodnocení nebezpečí a rizik, která se vyskytují v dnešních komplexních socio-technických systémech. K registrům a práci s rizikem je zapotřebí navrhnout takovou architekturu, která tyto aspekty bude zohledňovat z pohledu systémové úrovně.

K návrhu architektury registru systémovým přístupem, bylo zapotřebí analyzovat model STAMP a jeho dvě metodiky. Tato práce se soustředí především na analýzu CAST, se kterou se pracuje v praktické části, ale vzhledem k tomu, že tyto dvě metodiky se na sebe velmi často vzájemně odkazují v příručkách od paní profesorky Nancy G. Leveson, ve výsledném návrhu se pracovalo s oběma metodikami.

Metoda CAST, která slouží především retroaktivně, byla použita v praktické části, kdy bylo zapotřebí získat vzorek bezpečnostních dat, se kterými se následně pracovalo v návrhu analýzy. K tomu bylo zapotřebí analyzovat proces spojený s údržbou, ze kterého lze čerpat vhodný vzorek dat, který pomůže jako vstup při návrhu nové architektury registru. Na základě toho byla vybrána nehoda, kterou byla způsobena vlivem údržby.

Vzhledem k velkému množství probíhajících procesů v údržbě by bylo velmi časově náročné je všechny analyzovat, načež tak rozsáhlá analýza není vyžadována pro účely této práce; proto byla zvolena právě tato letecká nehoda, kdy výstupem je dostatek bezpečnostních dat a není časově ani rozsahově náročná. Díky tomu se stala analýza srozumitelnou, kdy jednotlivé dílčí kroky na sebe plynule navazovaly.

Pro účely CAST analýzy byla zvolena nehoda letu 236 společnosti Air Transat, na které se z velké části podílela údržba letadla. K analýze byly nashromážděna relevantní data

z ověřených zdrojů a následně na nehodu byla aplikována analýza dle postupů z příručky *CAST Handbook*.

Pomocí analýzy CAST bylo odhaleno nedostatečné řízení na několika úrovních v řídící struktuře v systému. Způsobila to nedostatečná řídicí akce, kterou vzápětí následovala nedostatečná zpětná vazba. To vše zapříčinil především nedostatek informací a nedostatečný výcvik spolu s dalšími systémovými faktory, které přispěly k nehodě.

Při návrhu byly tyto výstupy zohledněny a následně implementovány do návrhu nové architektury registru, tudíž výsledná architektura je zacílena především na řídicí akce a zpětnou vazbu, které jsou základem předcházení vzniku kauzálních scénářů. Jádro současných registrů se stále uvažuje; tedy stále se pracuje s nebezpečími a rizikem, avšak nyní jsou posuzovány z pohledu systémového přístupu.

V návrhu architektury dále cílí na nebezpečné řídící akce a kontextuální systémové faktory, které náhledně mohou vést ke ztrátám. Během analýzy kauzálních scénářů se pokládají otázky, „proč" a co" k tomu mohlo vézt. Tím se získá série možných odůvodnění, které následně pomohou při zavádění nápravných opatření za účelem snížení rizika.

Riziko je hodnoceno dle metodiky vycházející z modelu STAMP, kdy se namísto pravděpodobnosti vzniku rizika uvažuje účinnost zmírňování rizika, se kterou se následně pracuje při hodnocení způsobů snížení rizika.

Vložením bezpečnostních dat získaných z analýzy CAST aplikovanou na nehodu letu 236 bylo ověřeno, že navržená architektura registru může být použita jako nástroj k řízení bezpečnostních rizik z pohledu systémového přístupu.

V poslední části celé práce byla navržena aplikační fáze a její realizace, která se následně implementuje v praxi. Jednou z možností bylo nabízeno uložení dat do databáze, kde jsou tabulky propojeny pomocí cizích klíčů. Databáze je popsána relačním modelem a je navržena způsobem, aby byla uživatelsky přehledná a jednoduše se s ní pracovalo. Tím se zajistí proaktivní přístup využití registru nebezpečí a rizik. Zohledněna je i výsledná reprezentace dat v tištěné formě.

Zdroje

[1] ICAO doc.9859, Safety Management Manual (SMM) Fourth Edition. Montreal, 2018. [cit. 2022-10-20]. ISBN 978-92-9249-214-4

[2] INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). Annex 19 – Safety Management. 2nd edition. Montreal, Quebec: International Civil Aviation Organization, 2016. ISBN 978-92-9249-965-5

[3] MINISTERSTVO DOPRAVY ČR. Předpis L19. Řízení bezpečnosti. 2013 [online]. [Cit. 2022-10-05]. Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-19/index.htm

[4] INTERNATION CIVIL AVIATION ORGANISATION (ICAO). Airworthiness Manual. 3rd edition. Montreal, Quebec: International Civil Aviation Organization, 2014. ISBN 978-92-9249-454-4

[5] ADREP Taxonomy [online]. In:. [cit. 2022-10-30]. Dostupné z: https://www.icao.int/safety/airnavigation/aig/pages/adrep-taxonomies.aspx

[6] The CAST/ICAO Common Taxonomy Team [online]. In: [cit. 2022-10-28]. Dostupné z: http://www.intlaviationstandards.org/apex/f?p=240:1

[7] ECCAIRS Implementation [online]. In: [cit. 2022-10-30]. Dostupné z: https://www.icao.int/sam/ssp/pages/eccairs_implementation.aspx

[8] NASA. Aviation Safety Reporting System [online]. [cit. 2022-10-20]. Dostupné z: https://asrs.arc.nasa.gov/

[9] ASN Aviation Safety Database [online]. In:. [cit. 2022-10-30]. Dostupné z: https://aviation-safety.net/database/

[10] AERO - MEDA Investigation process [online]. In: [cit. 2022-11-30]. Dostupné z: https://www.boeing.com/commercial/aeromagazine/articles/qtr_2_07/article_03_1.html

[11] Nařízení Komise (EU) č. 1321/2014. *Úřad pro civilní letectví* [online]. [cit. 2022-10-01]. Dostupné z: https://www.caa.cz/dokumenty/predpisy/zakladni-informace-k-narizenim-eu/zachovani-letove-zpusobilosti/narizeni-komise-eu-c-1321-2014/

[12] MINISTERSTVO DOPRAVY ČR. Předpis L15. O letecké informační službě. 2020 [online]. [Cit. 2022-10-05]. Dostupné z: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-15/data/print/L-15__cely.pdf

[13] Steven C. McNeely, Manager, Safety Management Systems, Jet Solutions, L.L.C, published by "Flight Safety Information February 12, 2010 No.034"

[14] SHORROCK, Steven, Jörg LEONHARDT, Tony LICU a Christoph PETERS. *Systems Thinking for Safety: Ten Principles A White Paper: Moving towards Safety-II* [online]. [cit. 2022-10-12]. Eurocontrol.

[15] LEVESON, Nancy G. CAST HANDBOOK: How to Learn More from Incidents and Accidents. [online]. 2019. [cit.2022-10-20] Available from: http://sunnyday.mit.edu/CAST-Handbook.pdf

[16] LEVESON, Nancy. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. [cit. 2022-10-03] ISBN 978-0-262-01662-9.

[17] GREGORIAN, Dro J. a Sam M. YOO. *A System-Theoretic Approach to Risk Analysis* [online]. 2021 [cit. 2022-11-25]. Master's thesis. MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Vedoucí práce Joan Rubin.

[18] LEVESON, Nancy G. a John P. THOMAS. STPA handbook [online]. [cit. 2022-07-04]. Dostupné z: https://psas.scripts.mit.edu/home/get__file.php?name=STPA__handbook.pdf

[19] T. Musil, H. Némethová, J. Jevčák, L. Choma, P. Petríček, J. Sabo, F. Balla, and V. Polishchuk. *Case Study of Metrojet Flight 9268 to Research the Risks Register* [online]. In: 2019 [cit. 2022-11-01]. Dostupné z: doi:10.1109/MOSATT48908.2019.8944092

[20] LIN, Xun Guo a Stephen DUFFIELD. *The development of the sector risk profiling methodology for Australian civil aviation activity and its application to the small aeroplane transport sector* [online]. In: . 2017 [cit. 2022-11-15].

[21] MALMQUIST, Shem, Nancy LEVESON, Gus LARARD, Jim PERRY a Darren STRAKER. *A Systems Approach illustrated by the UPS Flight 1354 CFIT Accident: Increasing Learning from Accidents* [online]. In: . s. 96 [cit. 2022-11-26]. Dostupné z: http://sunnyday.mit.edu/UPS-CAST-Final.pdf

[22] *Accident Investigation Final Report: All Engines-out Landing Due to Fuel Exhaustion* [online]. In: . Government of Portugal, Aviation Accidents Prevention and Investigation Department, 2004, s. 103 [cit. 2022-12-01]. Dostupné z: https://www.fss.aero/accident-reports/dvdfiles/PT/2001-08-24-PT.pdf