ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Využití bezpečnostní a spolehlivostní analýzy ve vývoji vojenských letounů

Utilization of Safety and Reliability Analysis in Military Aircraft Development

Bakalářská práce

Studijní program: Technika a technologie v dopravě a spojích
Studijní obor: Technologie údržby letadel

Vedoucí práce: doc. Ing. Andrej Lališ, Ph.D.
Ing. Oldřich Štumbauer

Václav Tichý

Praha 2023

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

K621.....Ústav letecké dopravy

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Václav Tichý

Studijní program (obor/specializace) studenta:

bakalářský – TUL – Technologie údržby letadel

Název tématu (česky): **Využití bezpečnostní a spolehlivostní analýzy ve vývoji vojenských letounů**

Název tématu (anglicky): Utilization of Safety and Reliability Analysis in Military Aircraft Development

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je identifikace možností využití výstupů bezpečnostních analýz na bázi systémového přístupu k bezpečnosti a kvantitativních spolehlivostních analýz v doméně vývoje a následného provozu vojenských letounů.
- Analyzujte kvantitativní metody hodnocení spolehlivosti v letectví.
- Analyzujte systémový model bezpečnosti STAMP a jeho metody.
- Srovnejte výstupy těchto typů analýz na zvoleném konkrétním systému letounu s ohledem na jejich další využitelnost.
- Navrhněte možnosti efektivního využití spolehlivostních a bezpečnostních analýz na bázi systémového přístupu k bezpečnosti ve vývoji a následném provozu zvoleného systému.
- Dosažené výsledky ověřte a vyhodnoťte.

Rozsah grafických prací: dle pokynů vedoucího závěrečné práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Birolini, A. Reliability Engineering. Theory and Practice. Springer, 2017.
Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.

Vedoucí bakalářské práce: **doc. Ing. Andrej Lališ, Ph.D.**
Ing. Oldřich Štumbauer

Datum zadání bakalářské práce: **7. října 2022**
(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 bakalářské práce: **7. srpna 2023**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

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

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

Potvrzuji převzetí zadání bakalářské práce.

Václav Tichý
jméno a podpis studenta

V Praze dne ..... 7. října 2022

Abstrakt

Tato bakalářská práce řeší identifikaci možností využití výstupů bezpečnostní analýzy na bázi systémového přístupu v porovnání s kvantitativní spolehlivostní analýzou. Součástí práce je srovnání jednotlivých přístupů s ohledem na jejich využitelnost v následném provozu. Práce je zaměřená na vývoj a provoz vojenských letounů, protože byla tvořena ve spolupráci s firmou Aero vodochody Aerospace. Porovnání přístupů jsem prováděl na palivovém systému nového letounu L-39NG. Na palivový systém jsem aplikoval tradiční metody FTA a FHA dle postupu, využívané firmou Aero Vodochody. Metoda *System Theory Process Analysis* (STPA) byla aplikována na modernizovaný letoun L-159 ALCA. Výsledky ukázaly, že využití STPA analýzy nekomplexních systémů není natolik přínosné a při současné potřebě aplikování tradičních metod by bylo neefektivní. Metoda STPA je vhodná a potřebná při analyzování komplexních systémů skládajících se ze složitých systémů v kombinaci s lidským faktorem. V případě těchto systémů je využití metody STPA pro zvýšení bezpečnosti či udržení stávající úrovně nevyhnutelné.

Klíčová slova: bezpečnost, L-39NG, spolehlivost, System Theory Process Analysis, palivový systém

Abstract

This bachelor thesis addresses the identification of the possibilities of using the outputs of safety analysis based on a systems approach in comparison with quantitative reliability analysis. The thesis includes a comparison of the different approaches with respect to their applicability in downstream operations. The work is focused on the development and operation of military aircraft, as it was created in cooperation with Aero vodochody Aerospace. The comparison of the approaches was performed on the fuel system of the new L-39NG aircraft. I applied the traditional FTA and FHA methods to the fuel system according to the procedure used by Aero Vodochody. The System Theory Process Analysis (STPA) method was applied to the upgraded L-159 ALCA aircraft. The results showed that the use of STPA analysis of non-complex systems is not so beneficial and would be ineffective with the current need to apply traditional methods. The STPA method is appropriate and necessary when analyzing complex systems consisting of complex systems in combination with human factors. In the case of such systems, the use of STPA is unavoidable to improve safety or maintain the current level.

Keywords: L-39NG, reliability, safety, System Theory Process Analysis, fuel system

Poděkování

Tímto bych rád poděkoval vedoucím mé bakalářské práce, panu Ing. Andreji Lališovi, Ph.D. a panu Ing. Oldřichovi Štumbauerovi za jejich odborné vedení a cenné rady během psaní práce a dále také panu Ing. Karlovi Mündelovi za jeho konzultace. Taktéž děkuji firmě Aero Vodochody Aerospace za poskytnutí stáže a potřebných podkladů. Zvláště bych chtěl poděkovat panu Mgr. Milanu Pšeničkovi za jeho ochotu sdílet své cenné zkušenosti a znalosti, které byly nezbytné pro dokončení mé práce. Nemenší dík patří mé rodině a přátelům, kteří mi poskytovali nepřetržitou podporu při psaní bakalářské práce a během celého studia.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou/diplomovou práci s názvem Název práce vypracoval/a samostatně a použil/a k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské/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 7. srpna 2023 ……...

Podpis

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

AC	Advisory Circular
AVA	Aero Vodochody Aerospace
CA	Control Action
EMACC	European Military Airworthiness Certification Criteria
ETA	Event Tree Analysis
FHA	Fault Hazard Analysis
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode Effect and Criticality Analysis
FTA	Fault Tree Analysis
MIL-STD	Military standard
MTBF	Mean Time Between Failures
NG	Next Generation
PHA	Preliminary Hazards Analysis
PSSA	Preliminary System Safety Assesment
RBD	Reliability Block Diagram
RPN	Risk Priority Number
SAE ARP	Society of Automotive Engineers Aerospace Recommended Practice
SSA	System Safety Assesment
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TAP	Total Assurance Plus

Úvod

Od prvního řízeného letu uplynulo přes 119 let. V současnosti se civilní letectví rozvíjí velkou rychlostí a systémy se za téměř 12 dekád enormně vyvinuly. Během vývoje docházelo k velkému množství nehod, jenž si vyžádaly mnoho lidských životů. Z tohoto důvodu bylo nutné vyvinout metody na posuzování bezpečnosti a spolehlivosti letadel. V současné době se stále využívají metody vyvinuté v druhé polovině 20. století. Tyto metody, které jsou označovány jako tradiční, byly koncipovány pro nesložité systémy, které mezi sebou neinteragují a jejichž rizika jsou identifikovatelná. V kontextu stálého vývoje systémů s implementovanou elektronikou, která je schopna za letovou posádku rozhodovat a vstupovat do řízení, již nemusí tradiční metody dostačovat. Na tyto systémy je vhodnější aplikovat metodu *System Theory Process Analysis* (STPA) založenou na teorii systémů.

Téma jsem si zvolil, protože jsem si chtěl osvojit bezpečnostní analýzy a vyzkoušet si jejich aplikaci na reálný systém letadla. Kromě seznámení se s bezpečnostními analýzami jsem se zabýval i certifikačním procesem a s ním spojenými normami a standardy. Kvůli stanovení využitelnosti výstupů během provozu jsem zkoumal, v jakých odděleních se dají využívat výstupy bezpečnostních a spolehlivostních analýz. V mé práci se zabývám odlišnostmi jednotlivých přístupů. Bakalářská práce vznikala ve spolupráci s firmou Aero Vodochody Aerospace. Kde jsem měl možnost aplikovat tradiční bezpečnostní analýzy na palivový systém letounu L-39NG.

Systém jsem analyzoval pomocí *Fault Hazzard Analysis* (FHA), kterou jsem využil pro identifikaci poruchových stavů. Na vybrané stavy jsem aplikoval metodu poruchových stromů sloužící k vypočítání pravděpodobnosti nastání jednotlivých poruchy. Mou analýzu jsem následně porovnával s vypracovanou metodou STPA na modernizovaný letoun L-159 ALCA.

Bakalářská práce má za cíl stanovit, zda a v jakých ohledech je přínosné využití moderní metody STPA při vývoji a v následném provozu vojenských letadel. V závěru jsem navrhl, v jakých případech by bylo vhodné aplikovat metodu STPA.

1 Vývoj a provoz letadel z pohledu bezpečnosti

Analýzy slouží k zajištění bezpečnosti a spolehlivosti výrobku a v neposlední řadě také ke snížení nákladů na vývoj a následný provoz. V dnešní době se pro fázi vývoje a ověření, zda letadla opravdu splňují certifikační předpisy, využívají kombinace kvalitativních a kvantitativních analýz. Certifikační požadavky jsou pro civilní letectví stanoveny v prováděcích předpisech dokumentů AC 23.1309 pro kategorii letadel CS-23 a AC 25.1309 pro velká letadla kategorie CS-25. Cílem analýz je odhalit všechna možná rizika a posoudit, které z nich by měla závažný dopad na ohrožení bezpečnosti. Následně je možné tato rizika eliminovat, snížit pravděpodobnost jejich výskytu, snížit závažnost jejich dopadu nebo zkombinovat zmíněné postupy. Kvalitativní analýzy se využívají k nalezení všech poruchových stavů a následně tvoří seznam všech nebezpečných situací, které je nutné prověřit. Kvantitativními analýzami se poté dopočítají pravděpodobnosti nastání těchto poruch. Analýzy můžeme dále dělit podle přístupu na induktivní a deduktivní. [1] [2]

1.1 Induktivní přístup

Indukce představuje uvažování od jednotlivých případů k obecnému závěru. Při posuzování systému indukcí hledáme určité poruchy či iniciační faktory a posuzujeme, jaký dopad budou mít na celý systém. Tento postup se nazývá induktivní analýza. V praxi například posuzujeme, jaký dopad bude mít porucha palivového čerpadla či prasknutí palivového potrubí na letoun. [3]

Metody, které využívají induktivní přístup jsou například:

- PHA – Preliminary Hazards Analysis
- FMEA – Failure Mode and Effect Analysis
- FMECA Failure mode Effect and Criticality Analysis
- FHA – Fault Hazard Analysis
- ETA – Event tree Analysis

1.2 Deduktivní přístup

Dedukce představuje uvažování od obecného ke konkrétnímu. Je tedy opakem induktivního přístupu. V deduktivním přístupu uvažujeme, že daný systém již selhal a snažíme se analyzovat veškeré možné příčiny selhání. Typickým příkladem deduktivní analýzy je

Fault Tree Analysis (FTA), která od vrcholové události zkoumá možné cesty, jak k tomuto selhání mohlo dojít. [3]

Zástupci deduktivních analýz jsou:

- FTA – Fault Tree Analysis
- RBD – Reliability Block Diagram

V praxi se zpravidla využívá kombinace deduktivního přístupu s induktivním, protože v jednom případě uvažujeme nad selhání systémů tzv. „*top down*" a v druhém opačným způsobem neboli „*bottom up*". Výhodou těchto rozdílných přístupů je kontrola správnosti a ověření, zda si analýzy odpovídají.

1.3 Vývojová fáze

Bezpečnostní a spolehlivostní analýzy neslouží pouze k certifikaci a prokázání bezpečnosti letadla, ale využívají se již během vývojové fáze při posouzení návrhu. Umožňují eliminovat případné bezpečnostní problémy již v raných fázích vývoje. Cílem analýz je identifikovat všechna možná nebezpečí či selhání a následně ohodnotit jejich riziko, které se posuzuje na základě závažnosti a pravděpodobnosti. Díky tomuto můžeme nebezpečí či selhání kategorizovat. Nebezpečí kriticky ohrožují let, musí být důkladně posouzeny. Pokud je pravděpodobnost výskytu tohoto rizika příliš vysoká, musí být provedeny opatření k nápravě. Cílem je dosáhnout takové bezpečnosti, aby riziko selhání systému bylo přípustné a aby byly kritické komponenty dostatečně zálohovány.

Při vývoji letounů výrobci nevyvíjí a nevyrábí veškeré komponenty, ale nakupují je od dodavatelů. Většinou dodávají pro každý výrobek jejich vlastní analýzu bezpečnosti a spolehlivosti. Pro kritické komponenty bývá využita předběžná analýza, vytvořená výrobcem letounu, stanovující požadavky na dodávané díly. Pro certifikaci letounu musí analytik využít data získaná od různých dodavatelů a zanalyzovat je nejprve na úrovni systému a poté i na úrovni letounu.

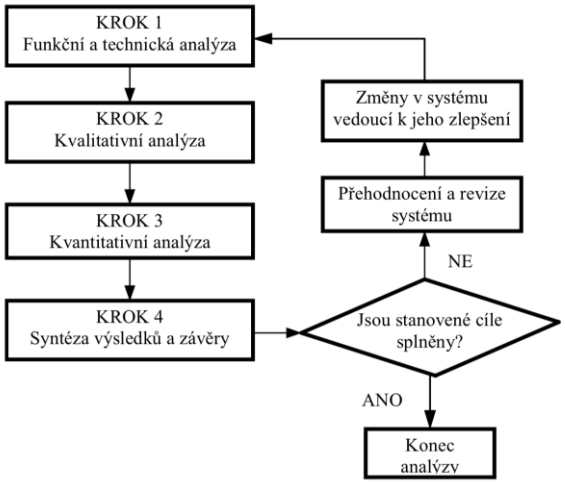
Po dokončení finální verze letounu, musí být tyto analýzy provedeny znovu, a to pro danou konfiguraci letounu. Závěrečná zpráva poté tvoří dokument, který se využívá pro certifikaci daného letadla.

Analýzy se během vývoje a provozu letadla dělí na:

1. Předběžná fáze vývoje – PSSA Preliminary System Safety Assessment
2. Analýza finální konfigurace letounu – SSA System Safety Assessment (Systémová úroveň
3. Analýza provozních dat

1.4 Předběžná fáze vývoje: [4]

Během vývojové fáze jakéhokoli výrobku, jehož selhání by mělo dopad na ohrožení zdraví, ztráty lidského života či poškození životního prostředí, je nutné prokázat jeho bezpečnost a spolehlivost stanovenou příslušnými standardy. K tomuto ověření se používají prediktivní analýzy, které se provádí ještě před dokončením návrhu systému či sestavením prvního prototypu. Jejich přínosem je snížení nákladů na vývoj a výrobu, protože v počáteční fázi je mnohem snadnější měnit konstrukční návrh. Naopak mohou sloužit při rozhodování mezi různými konstrukčními řešeními systémů. Zároveň tyto analýzy stanovují bezpečnostní a spolehlivostní požadavky na systém, a proto by bez nich nebylo ani možné navrhnout dostatečně bezpečný systém. Výstupy z této analýzy bývají také často využívány jako spolehlivostní požadavky výrobcům jednotlivých komponentů, kdy musí daný komponent vyrobit s požadovanou úrovní spolehlivosti. Postup posuzování je rozebraný níže na obr. 2.



Obrázek 1: Postup vývojové analýzy [4]

V každé z těchto analýz se nacházejí jisté nejasnosti či nedostatky, které jsou způsobeny především vnitřním a vnějším omezením. Konkrétně se může jednat o nejasnosti v konstrukčním návrhu systému, interferencí s jinými systémy, provozních podmínek či vliv lidského faktoru. Dalším ovlivňujícím faktorem je hloubka analýzy, která musí být definována

hned na začátku. Jedná se o rozhodnutí, zda bude analýza provedena na úrovni komponentů či o úroveň hlouběji, kde jsou uvažovány i části, ze kterých dané komponenty sestávají. Všechny tyto nejasnosti a nedostatky postupně vymizí s vývojem návrhu systému.

Postup předběžné analýzy:

1. Funkční a technický popis systému
2. Kvalitativní analýza
3. Kvantitativní analýza
4. Porovnání výstupů analýz

V prvním kroku se shromáždí veškerá data o systému včetně technických výkresů a všech dokumentů popisujících funkce tohoto systému. Analytik se musí podrobně seznámit se všemi funkcemi a interakcemi, protože počáteční pochopení systému je v dalších fázích klíčové. Dále se také musí nastavit hranice analyzovaného systému a hloubka analýzy.

Kvalitativní analýzy se využívají k nalezení všech poruchových stavů a následně tvoří seznam všech nebezpečných situacích, které je nutné prověřit. Přehled kvalitativních analýz, které lze využít: FHA, FMEA, FMECA

Kvantitativní analýzy slouží k určení pravděpodobností poruchových stavů. Tyto pravděpodobnosti v kombinaci se závažností stanovují celkovou kategorii nebezpečí daného poruchového stavu. Přehled kvalitativních analýz, které lze využít: FTA, RBD, Markovova metoda

V posledním kroku je nutné ověřit, zda si všechny analýzy odpovídají a zda byly splněny všechny bezpečnostní a spolehlivostní požadavky na systém. V případě, že by tomu tak nebylo, je nutné provést změny a celý postup provést znovu do té doby, dokud nebudou požadavky splněny.

1.5 Analýza finální konfigurace letounu

Po dokončení všech úprav konstrukčního návrhu musí být provedena finální analýza daného letounu. Většina leteckých výrobců prodává letouny v různých konfiguracích, a proto musí daná analýza odpovídat konkrétní konfiguraci prodávaného typu. Princip postupu těchto analýz je identický s vývojovou fází, jen s tím rozdílem, že jsou provedeny pro konkrétní systémy, a to již velmi detailně bez jakýchkoli nedostatků z vývojové fáze. Výstupem této analýzy je systémová analýza *System Safety Assessment* (SSA) tvořící souhrn

technických výkresů, popis funkcí systému, seznam poruchových stavů kategorizovaný podle výstupu z kvantitativních analýz. SSA analýza bývá prováděna zpravidla na systémové úrovni. Analýzy na systémové úrovni se následně spojují do *Functional Hazard Assessment* (FHA), která bývá vytvořena na úrovni letadla. FHA poté tvoří základní dokument pro certifikaci letadla.

Po dokončeném certifikačním procesu, analyzování bezpečnosti a spolehlivosti nekončí, ale přejde se z vývojových analýz k analýzám provozním, kde se sledují důležité provozní údaje jako počty letových hodin, poruchy, a bezporuchovost během celé doby životnosti letounu. U provozovatele se poté sleduje provozuschopnost pro ověření, zda bude schopen naplnit to co se od flotily letounů očekává. [5]

1.6 Analýza provozních dat

Pro provádění provozních spolehlivostních analýz je klíčové zajištění sběru dat z provozu. Kontrakty o poskytování provozních dat jsou zajištěny spolu s prodejem letounů. Sběr probíhá buď pomocí poruchových karet a následným zasíláním sledovaných parametrů nebo u moderních systémů jsou sbírány a zasílány data v reálném čase během provozu.

V případech, kdy nejsou k dispozici data z provozu lze využít:

- Zkoušky spolehlivosti
- Provozní data ze starších letounů vyráběných stejným výrobcem
- Provozní data z databáze letounů stejné kategorie a použití

Zkoušky spolehlivosti lze provádět i simulacemi. V případě, kdy výrobce disponuje modelem systému, je možné prokazovat jeho spolehlivost i tímto způsobem. Výhodou je ekonomičtější a bezpečné odzkoušení systému a zisk dat řádově vyšších, než jaké by bylo možné prokázat letovými zkouškami. Nevýhodou takové simulace mohou být nevhodně zvolená vstupní data, která vedou ke zkresleným výsledkům nebo složité simulování lidského chování či přírodních jevů. Limitujícím faktorem může být omezený rozsah zkoušky postavený na předpokladech o možných poruchách a provozních podmínkách a v neposlední řadě náklady na potřebné vybavení a model k simulaci komplexních systémů.

Pokud letecký výrobce již vyráběl letoun stejné kategorie lze využít pro počáteční návrh spolehlivostního programu i data z provozu starších letadel, protože ze statistického hlediska

si budou data odpovídat. Je ale vhodné tyto data aktualizovat a postupně nahradit daty získanými od provozovatelů nových letadel.

Využití těchto výstupů se dále využívá ve vývoji nových letounů nebo pro plánování údržby. Pro oddělení plánování jsou primárně důležité pravděpodobnosti poruch a střední doby mezi poruchami v anglické terminologii označovány jako „*Mean Time Between Failures*“ (MTBF).

Dále lze využít data stanovená ve standardech. V těchto standardech lze dohledat intenzity poruch pro danou kategorii letounů. V mé práci jsem využíval volně přístupný program MTBF-Calculator[1], který slouží k vyhledávání intenzity poruch v těchto a mnoha dalších standardech:

- BRITISH TELECOM HRD4
- MIL-HDBK-217E
- NPRD-95, NPRD-2011, NPRD-2016
- NSWC-98/LE1 Mechanics

Je nutné podotknout, že se v těchto databázích dají dohledat pouze elektrické či mechanické součástky nikoli celá zařízení. Pro stanovení hodnoty intenzity poruchy složitějšího zařízení je nutné sečíst intenzity všech součástek, ze kterých se zařízení skládá. Přístup zkoumající jednotlivé části celku odděleně se nazývá analytický rozklad, který je rozebrán v kapitole 5.1.

Výstupy provozních analýz slouží k vytvoření databáze spolehlivosti jak jednotlivých komponentů, tak i celého letadla. Největší výhodou pro provozovatele může být sledování provozní spolehlivosti, provozuschopnosti a dostupnosti jeho flotily. U výrobce se tyto data mohou promítnout jak do dalšího vývoje, modifikací, tak i do programu údržby, který je s provozní spolehlivostí úzce spjatý. V neposlední řadě se tyto data odráží v oddělení logistiky, které z těchto predikcí vychází a snaží se zajistit dostupnost komponentů, aby se co nejlépe optimalizovala údržba a minimalizovali se prostoje během oprav. [6]

[1] Dostupný z url: https://aldservice.com/Free-MTBF-Calculator.html

2 Aero Vodochody – vývoj L-39NG

V této kapitole jsem popsal průběh vývoje letounu L-39NG, normy a postupy využité během vývoje, certifikace a provozu. Součástí kapitoly je i popis letounu a palivového systému, na který jsem vypracoval analýzu dle využívaných postupů v Aero Vodochody Aerospace.

2.1 Popis letounu a základní technické parametry

Letoun L-39NG je moderní proudový letoun schopný plnit funkce lehkého bitevníku. Je určený pro komplexní výcvik bojových pilotů a přípravu na letouny 4. a 5. generace. Letouny 4. a 5. generace jsou pojmem pro vojenské letouny s pokročilou avionikou, komunikačními prostředky či vysokou manévrovatelností. Koncepce letounu vychází z předchozího modelu L-39 Albatros, která byla rozšířena o moderní avioniku, prvky ke snížení odporu a úsporný motor FJ44-4M. Motor je zároveň dodávaný s novým údržbovým systémem TAP blue, jehož výhodou je předvídatelnost nákladů na údržbu. Nový údržbový plán umožňuje platbu za letové hodiny s garancí provozních nákladů vztahujících se kromě plánované údržby i na údržbu neplánovanou. Letoun je vybaven výcvikovým systémem simulujícím pilotovi virtuální vzdušný souboj. Podle požadavků zákazníka lze letoun přizpůsobit do požadované konfigurace. Firma Aero Vodochody Aerospace nabízí kromě nového letounu také modernizaci předchozích modelů zastavěním nové moderní avioniky a motorů FJ44-4M. Základní technické parametry letounu jsou zobrazeny v tabulce 1. [7]

Obrázek 2 Letoun L-39NG [7]

Tabulka 1: Základní letové parametry [7]

Rozpětí křídel	9,38 m
Délka	11,70 m
Prázdná hmotnost	3 200 kg
Maximální vzletová hmotnost	5 600 - 5 800 kg
Maximální hmotnost paliva (interní)	1 250 kg
Maximální množství externích zásob	1640 kg
Maximální rychlost	780 km/h
Stoupavost	23 m/s
Maximální tah	16,87 kN
Maximální násobky	+8/-4 g

2.2 Vojenské a civilní normy využité pro certifikaci a vývoj L-39NG [5]

Firma Aero Vodochody Aerospace (AVA) se zabývá především výrobou vojenských letounů. Jejich vývoj a následná certifikace se proto řídí zejména vojenskými a některými civilními normami. Veškeré normy a dokumenty využité pro letoun L-39NG jsou rozebrány níže.

2.2.1 EMACC [8]

Certifikační proces se řídí základním dokumentem *European Military Airworthiness Certification Criteria* (EMACC), který stanovuje obecné postupy pro tvorbu bezpečnostních analýz a spolehlivostního programu. Pro certifikaci letadla je povaha tohoto dokumentu příliš obecná, proto EMACC schvaluje a uvádí další doporučené dokumenty, kde jsou uvedeny podrobnější informace. Těmito dokumenty jsou civilní a vojenské normy či jejich kombinace, které jsou rozebrány níže.

2.2.2 MIL-STD-882E [9]

Základní normou využívanou při certifikaci letounu L-39 NG byla vojenská norma MIL-STD-882E. V ní lze nalézt podrobný proces, jak posoudit bezpečnost systémů, identifikovat nebezpečí a kategorizovat je podle jejich pravděpodobnosti a závažnosti. Tyto kategorie zobrazuje obr. 4 níže. Dále zde nalezneme i metodiku jednotlivých analýz či postupy pro eliminaci nebezpečných stavů.

Matice hodnocení rizik / Risk Assessment Matrix				
Závažnost / Pravděpodobnost	Katastrofická (1) Catastrophic (1)	Kritická (2) Critical (2)	Závažná (3) Marginal (3)	Nezávažná (4) Negligible (4)
Četné (A) Frequent (A)	Vysoké High	Vysoké High	Závažné Serious	Střední Medium
Pravděpodobné (B) Probable (B)	Vysoké High	Vysoké High	Závažné Serious	Střední Medium
Občasné (C) Occasional (C)	Vysoké High	Závažné Serious	Střední Medium	Nízké Low
Málo pravděpodobné (D) Remote (D)	Závažné Serious	Střední Medium	Střední Medium	Nízké Low
Nepravděpodobné (E) Improbable (E)	Střední Medium	Střední Medium	Střední Medium	Nízké Low
Vyloučené (F) Eliminated (F)	Vyloučené Eliminated			

Obrázek 3: Matice hodnocení rizik (přeloženo z [9]) [2]

2.2.3 SAE ARP 4761 [10]

Tento dokument obsahuje civilní metodiku pro provádění analýz. A to jak z pohledu procesu, tak i metodiku konkrétních analýz jako jsou FTA, FMEA apod. Zaměřuje se především na posuzování bezpečnosti, identifikaci rizik a jejich následnou eliminaci či zmírnění dopadů.

Udává standardizovaný postup procesu posuzování, který rozděluje do třech fází, kterými jsou:

1. FHA – Functional Hazard Assessment
2. PSSA – Preliminary System Safety Assesment
3. SSA – System Safety Assesment

2.2.4 AC 23.1309 [1]

Dokument je provádějícím předpisem obsahujícím možné způsoby, jak prokázat splnění požadavků předepsaných v § 23.1309 pro kategorii letadel CS-23. Zabývá se

[2] Využil jsem matici hodnocení rizik přeloženou Aero Vodochody Aerospace z MIL-STD-882E.

hodnocením bezpečnosti a prováděním analýz konkrétně FHA. Nalezneme zde i další metody, které již nejsou popisované detailně. Dokument se pro stručnost jeho popisu v některých částech odkazuje na normu SAE ARP4761. Dle tohoto prováděcího předpisu je také možné kategorizovat jednotlivé poruchové stavy v závislosti na závažnosti dané poruchy. Dalším faktorem ovlivňujícím výši přípustného rizika je kategorie letounu.

2.3 Předběžná vývojová fáze

V raných fázích vývoje je nutné vypracovat předběžný bezpečnostní a spolehlivostní program, který obsahuje rámec práce v oblasti bezpečnosti a spolehlivosti. Konkrétně se jedná o popis využívaných norem, standardů či druhů analýz. Předběžný program poté musí být posouzen a schválen příslušným dozorujícím orgánem. Dalším krokem je vytvoření PFHA analýzy sloužící k nalezení všech možných poruchových stavů, které bude nutno prověřit. V počáteční vývojové fázi není konstrukční návrh zdaleka dokončen, a proto se u většiny systémů uvažuje o různých konstrukčních řešeních. Pomocí předběžné analýzy je poté možné provést rozhodnutí mezi jednotlivými řešeními či poukázat na nutnost řešení nového. Cílem analýz je eliminovat možné následky poruchových stavů či snížit pravděpodobnost jejich výskytu. Pro závěrečné kategorizování poruchových stavů a hodnocení jejich závažnosti se využívá kategorizace dle MIL-STD-882E viz tabulka 2. [5]

Tabulka 2: Kategorie závažnosti dle MIL-STD-882E (přeloženo z [9])

KATEGORIE ZÁVAŽNOSTI		
POPIS	**KATEGORIE**	**KRITÉRIA VÝSLEDKU NEHODY**
KATASTROFICKÁ	1	Mohlo by mít za následek jednu nebo více z následujících příčin: smrt, trvalou úplnou invaliditu, nevratný významný dopad na životní prostředí nebo peněžní ztrátu rovnající se nebo převyšující 10 milionů USD.
KRITICKÁ	2	Mohlo by mít za následek jednu nebo více z následujících příčin: trvalá částečná invalidita, zranění nebo nemoc z povolání, které mohou vést k hospitalizaci alespoň tří zaměstnanců, vratný významný dopad na životní prostředí nebo finanční ztráta rovnající se nebo převyšující 1 milion USD, ale nižší než 10 milionů USD.
ZÁVAŽNÁ	3	Může mít za následek jednu nebo více z následujících příčin: zranění nebo nemoc z povolání, které mají za následek jeden nebo více ztracených pracovních dnů, vratný středně závažný dopad na životní prostředí nebo finanční ztrátu rovnající se nebo převyšující 100 tisíc USD, ale nižší než 1 milion USD.
BEZVÝZNAMNÁ	4	Může mít za následek jednu nebo více z následujících příčin: úraz nebo nemoc z povolání, které nemají za následek ztrátu pracovního dne, minimální dopad na životní prostředí nebo finanční ztrátu nižší než 100 tisíc USD.

2.4 Finální vývojová fáze

Po dokončení finální konstrukční varianty musí být analýza provedena znovu. Analýza musí odpovídat přesné konstrukční konfiguraci. Pokud obsahuje zastavěný letecký celek, lišící se od základní konfigurace, musí být takovéto zařízení součástí analýz. Výstupem z finální analýzy je závěrečná zpráva tzv. SSA (*System Safety Assessment*), která shrnuje veškeré podstatné informace o jednotlivých systémech včetně stručného popisu a technických výkresů. SSA dále zahrnuje analýzy, kterými byl vytvořen seznam poruchových stavů a kterými byly stanoveny jejich pravděpodobnosti. Převážně se jedná o analýzy FTA či FMEA, FMECA. SSA sdružuje analýzy na úrovni systémů a pro prokázání bezpečnosti a spolehlivosti celého letounu musí být tyto jednotlivé analýzy na úrovni systémů seskupeny do letounové úrovně. K takovémuto seskupení se využívá analýza FHA, jež tvoří základní dokument prokazující bezpečnost a spolehlivost celého letounu. Veškeré dokumenty a zprávy vzniklé během vývoje nalezneme poté ve finálním programu bezpečnosti a spolehlivosti vycházejícím z předběžného programu. [5]

2.5 Certifikační fáze

Před samotnou certifikací je nutné stanovit tzv. certifikační bázi. Jedná se o soubor norem, kterými se během této fáze výrobce řídí. Je obsažena v dokumentu, který se nazývá plán vývoje a certifikace. Při certifikaci L-39NG byla hlavním dokumentem norma EMACC stanovující dílčí prováděcí předpisy pro splnění certifikačních požadavků. Těmito prováděcími předpisy byly MIL-STD a CS 23.1309. Plán vývoje obsahuje, kromě použitých norem, také metodiku využitou pro posuzování bezpečnosti a časový harmonogram. Harmonogram plánu vývoje letounu je podrobný časový plán, popisující fáze a aktivity vývoje letadla. Obsahuje etapy, cíle a časové termíny, důležité pro dokončení projektu vývoje letounu. Po schválení vytvořeného plánu vývoje a certifikace příslušným orgánem je vydán dokument, kterým je finální program bezpečnosti a spolehlivosti. Ten spojuje certifikační předpisy dané prováděcími předpisy a skutečné prokázané hodnoty získané během analýz z finální fáze vývoje. [5]

Hlavními dokumenty certifikační fáze jsou:

- Plán vývoje a certifikace
- Předběžný program bezpečnosti a spolehlivosti
- Finální program bezpečnosti a spolehlivosti
- Průkaz bezpečnosti a spolehlivosti

2.6 Provozní analýzy

Další fází, která nastává po certifikovaní, jsou analýzy dat sbíraných z provozu. Jedná se především o nálet letounů a o záznamy poruch. Sběr dat probíhá formou poruchových karet, do kterých se zaznamenávají informace o poruchách, opravách a údržbě během provozu letadla. Vyhodnocují se jednou ročně. Každá karta obsahuje podrobný popis poruchy, selhání komponentů, typu letounu a další popis situace, ve které porucha nastala. Do karet se zapisují i poruchy, za která nenese odpovědnost výrobce a musí se z analýzy vyfiltrovat. Příkladem takového poškození může být srážka s ptákem nebo například poruchy způsobené nedodržením předepsaných postupů. Hlavním výstupem z této analýzy jsou tzv. MTBF označující odhadovanou střední dobu do poruchy. Z vyfiltrovaných dat je poté možné určit MTBF pro jednotlivé agregáty, systémy či letouny.

Hlavní způsoby, jakými výrobci letadel využívají karty poruch, zahrnují:

Vlastní vývoj: Informace zaznamenané v kartách poruch letounů poskytují výrobcům cenné informace o slabých místech nebo nedostatcích jejich letadel. Tato data mohou být využita k identifikaci potenciálních problémů v konstrukci, které by mohly vést k poruchám. Na základě těchto poznatků mohou výrobci provádět změny v návrhu a vylepšovat své letouny, aby minimalizovali opakování poruch a zvýšili jejich spolehlivost. K odhalení nejrizikovějších agregátů se využívá Paretův diagram zobrazující systémy/agregáty s nejvyšším podílem poruch. U takovýchto systémů je nejvhodnější provádět konstrukční úpravy, protože budou mít největší dopad na zvýšení spolehlivosti.

Podpora údržby a logistiky: Karty poruch obsahují informace využitelné při predikování údržbových úkonů. Výrobci letadel mohou poskytovat doporučení a postupy na opravy na základě těchto záznamů, což usnadňuje provádění včasné a efektivní údržby. To pomáhá minimalizovat prostoje letadel, zlepšit jejich provozuschopnost a prodloužit jejich životnost. Zároveň je zde velice důležité propojení s oddělením logistiky, které musí zajistit dostatek náhradních dílů nutných k údržbě dle predikcí.

Plnění předpisů: Výrobci letadel jsou povinni splňovat příslušné letecké předpisy a normy. Sběr provozních dat nařizuje kromě výkladu organizace DOA i norma EMAR 21, jež je vojenskou verzí partu 21. [11] Karty poruch letounů slouží jako důkaz o tom, že letadlo bylo v souladu s předpisy opravováno a udržováno, a že byly provedeny veškeré potřebné kontroly. Shromažďování dat z provozu je tedy důležitým prvkem kontinuálního zlepšování a monitorování výkonu letadel výrobci letadel, což přispívá k bezpečnosti a spolehlivosti.

Reklamace: v případech, kdy provozovatelé reklamují nějakou závadu, je nutné posoudit, jak často se daná závada během provozu objevovala i u dalších provozovatelů, a zda je nutná náhrada či úprava konstrukčního řešení.

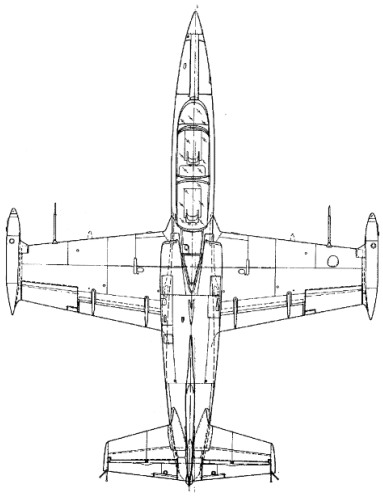
2.6.1 Palivový systém

Pro srovnání jsem si vybral palivový systém, protože je to jediný systém, na který byla vypracována analýza STPA [12]. Zároveň mi tento systém byl nabídnut firmou AVA.

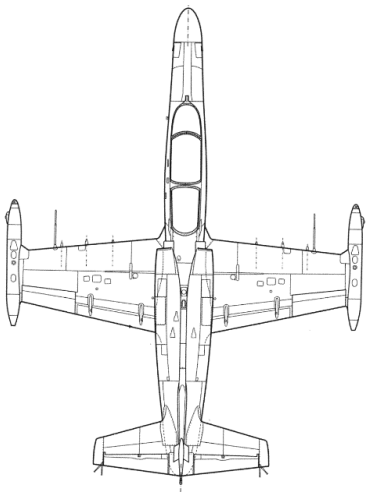
Palivový systém disponuje těmito funkcemi:

- Doprava paliva do palivové soustavy motoru
- Přečerpávání paliva z podvěsných a integrálních křídelních nádrží do trupové
- Tlakové plnění

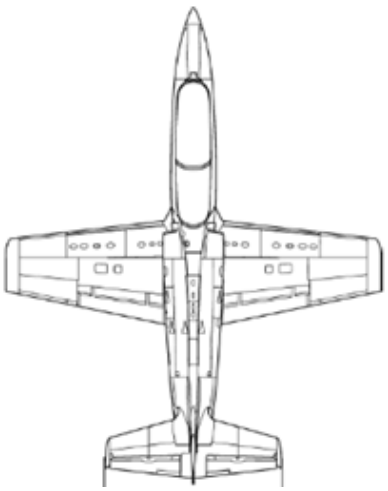
U letounu L-39NG byla provedena zásadní modernizace palivového systému. Oproti přechozím letounům zde byl zachován pouze jeden pár podvěsných nádrží a nově je zde využita technologie tzv. „mokrého křídla“, jež umožňuje zabudovat integrální nádrž přímo do konstrukce křídla. To zvyšuje jeho pevnost a zároveň snižuje aerodynamický odpor oproti koncepci s dvěma páry podvěsných nádrží. Nové je i zobrazení informací o palivovém systému, kdy analogové přístroje nahradilo zobrazení na digitálním multifunkčním displeji. Oproti předchozím modelům se zde již nenachází koncové křídelní nádrže, což také redukuje aerodynamický odpor (viz obr.4,5,6).



Obrázek 6 L-39 Albatros [18]

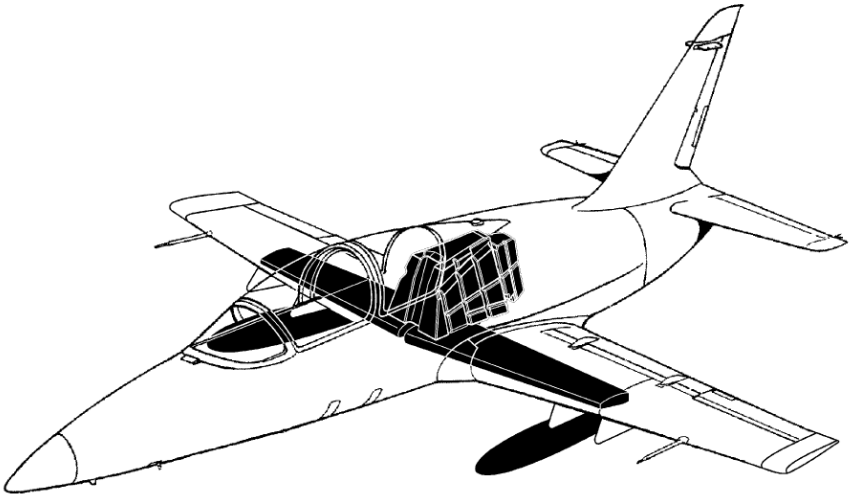


Obrázek 5 L-159 ALCA [19]



Obrázek 4 L-39 NG [13]

Letoun disponuje celkem 5 nádržemi – jedním párem podvěsných křídelních, jedním párem integrálních křídlových a trupovou integrální nádrží. Nádrž v trupu je rozdělena na nádrž a tzv. „*feeder*“, ze kterého je dopravováno palivo palivovým čerpadlem do motoru. Systém nádrží je nepřetlakovaný s výjimkou podvěsných nádrží. Letoun disponuje tlakovým plněním z jednoho přístupového bodu, odkud je dle požadavků plnění automaticky řízeno.



Obrázek 7 Lokace palivových nádrží [13]

Tabulka 3 Objemy palivových nádrží [13]

	Litry	US gal	kg	lbs
Trupové nádrže	740	195	599	1321
Křídelní nádrže	680	180	551	1215
Celkové interní množství paliva	1420	375	1150	2536
Celkové externí množství paliva	700	185	567	1250

3 Přehled vědecké literatury

V současnosti se tématem využitelnosti výstupů bezpečnostních a spolehlivostních analýz zabývají tyto otázky:

3.1 Řízení kvality s využitelností tradičních analýz [14]

Analýzy FHA, FMEA, FTA se využívají k nalezení kritických prvků systémů a následně se používají na kontrolu kvality výroby, montáže a skladování. V článku [14] se zaměřili na výzkum metody identifikace kritických a důležitých komponentů u civilních leteckých systémů. Jedná se o komponenty, které by v případě jejich selhání mohly mít dopad na ohrožení bezpečnosti. Identifikace kritických prvků vychází z tradičních metod typu FTA, FHA, FMEA.

Podle závislosti funkce na komponentu lze díly klasifikovat jako:

- **Kritické** – jsou takové díly, jejichž ztrátou by selhal systém
- **Důležité** – v případě ztráty by systém neselhal, ale již by neplnil plnohodnotnou funkci, která by se odrážela v provozních omezeních a zvyšovala by zátěž posádky
- **Běžné** – nemají vliv na bezpečnost letu

Metodou je nutné stanovit minimální počet kritických a důležitých dílů, u kterých by byla později kontrolována výroba, montáž a skladování. Zpřísněním kontroly kvality by měla být snížena pravděpodobnost závad. Taková kontrola dílů by byla velmi ekonomicky nákladné, a proto se zde nabízí výběr pouze kritických a důležitých komponent.

Postup

Základním vstupem je analýza FHA, která je schopna poruchové stavy kategorizovat. Následně z poruchových stavů vybereme pouze ty, které spadají do katastrofické či kritické kategorie. Poruchové stavy v FHA jsou rozšířeny o kvalitativní analýzu FTA. V těchto stromech je nutné dohledat kritické cesty obsahující 2-3 komponenty vedoucí ke katastrofické události. Pro kritické události se dohledávají cesty s 2 komponenty. Do analýzy se přidávají i komponenty, které jsou spojené s hlavními poruchovými stavy či s často se vyskytujícími díly ve zprávách z údržby.

Tabulka 4 Přehled analyzovaných položek (přeloženo z [14])

Kategorie	Analytické položky	Analýza obsahu
Funkční nebo výkonnostní ukazatele	Funkce systému	Analýza potenciálně ovlivněných funkcí systému na základě kritéria
	Funkce dílu	Analyzujte funkce, které má systém vykonávat, přiřazené k dílům podle funkcí systému
	Ukazatel výkonnosti	Stanovit ukazatele výkonnosti pro funkce prováděné dílem
Podmínky dopadu	Podmínky montáže	Faktory v procesu montáže, které mohou ovlivnit výkon nebo funkci součásti.
	Podmínky prostředí	Faktory, které mohou ovlivnit výkon nebo funkci dílů během skladování, přepravy a provozu
	Podmínky údržby	Faktory v procesu údržby, které mohou ovlivnit výkon nebo funkci dílů

Tradiční metody mohou být cenným vstupním materiálem pro řízení kontroly kvality. Tyto analýzy lze získat z certifikačních podkladů. Zaměření se na kontrolu kritických komponentů při výrobě, skladování i montáž má dopad na zvyšování bezpečnosti a spolehlivosti systémů.

3.2 Aplikace FMEA-FTA při plánování údržby zaměřené na spolehlivost [15]

Článek [15] pojednává o důležitosti spolehlivosti v průmyslových systémech. Popisuje potřebu efektivní analýzy způsobů selhání pro plánování a provoz spolehlivých systémů. Tato analýza je označována jako R*eliability Centered Maintenance* (RCM). Zaměřuje se na preventivní údržbu a vývoj spolehlivých systémů a komponentů. Existují dvě hlavní úlohy v rámci RCM. První je analýza způsobů selhání a jejich dopadů na výkon systému. Druhá je vyhodnocení vlivu plánovaných údržbových opatření na spolehlivost systému. K tomu se používají dva přístupy:

- analýza způsobů selhání a jejich účinků (FMEA)
- analýza poruchových stromů (FTA)

FMEA je kvalitativní přístup, který slouží k identifikaci potenciálně slabých míst systému. K jejich upřednostňování slouží ukazatel tzv. *Risk Priority Number* (RPN). Následně jsou navržena preventivní opatření, která mají snížit pravděpodobnost výskytu selhání.

FTA je kvalitativní deduktivní analýzou. V tomto případě by analýza měla sloužit ke identifikaci kritických komponent a určit pravděpodobnosti jejich selhání. Tuto informaci lze využít jako podklad pro rozhodnutí o tom, jaký druh údržby bude nejefektivnější pro minimalizaci rizika selhání a maximalizaci spolehlivosti systému. Více k FTA viz kapitola 5.3.

Oba tyto přístupy, FMEA a FTA, se často používají již pro analýzu spolehlivosti. Z tohoto důvodu je jejich využití výhodné, protože jsme schopni získat vstupy pro metodu RCM z certifikačních podkladů. [15]

4 Limitace současného stavu

Analyzování systémů je v praxi limitováno mnoha faktory. Nejzásadnější, které z mého pohledu omezují rozsah a hloubku analýz jsou zmíněny níže.

1. **Čas:** je největším omezujícím faktorem provádění bezpečnostních a spolehlivostních analýz. V případě, kdy je analytik časově omezen, musí využít co nejefektivnější cestu k ověření bezpečnosti a spolehlivosti, jinak by nemusel mít dostatek času na pokrytí všech možných hrozeb. Z tohoto důvodu je nutné správně zvolit využívané metody, protože časová náročnost jednotlivých přístupů se značně liší. V praxi se proto jednotlivé selhání funkcí kategorizují podle závažnosti pro detailnější posouzení nejkritičtějších selhání.
2. **Lidské zdroje**: při analýze může časové omezení ovlivnit i počet analytiků a jejich zkušenosti. V případě, že na dané analýze pracuje vyšší počet lidí, může být analýza nejen časově úspornější, ale je zde i menší pravděpodobnost přehlednutí některých rizik, a výsledek není natolik subjektivní.
3. **Prostředky:** poskytnutí financí také značně ovlivní průběh analýz. Nejen s ohledem na počet analytiků, časovou dotaci potřebné k podrobné analýze, ale také třeba na softwarové vybavení usnadňující analýzy či automatizaci některých postupů.
4. **Vhodné využití analýzy:** Současně využívané tradiční metody analýz vyvíjené pro nekomplexní systémy nemusí dostatečně popisovat dnes konstruované systémy, avšak moderní metody k tomu určené nelze využít pro certifikaci letounu. Z tohoto důvodu je nutné stanovit efektivní postup pro využití vhodných analýz pro vývoj a následný provoz.

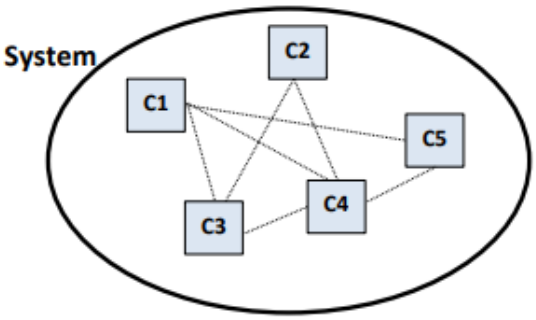
Z těchto důvodů je zřejmé, že časová limitace je významným faktorem ovlivňujícím rozsah, hloubku i úplnost prováděných analýz. Proto je důležité, aby výrobce poskytnul analytikům dostatečný čas i prostředky pro důkladné provedení analýz. V praxi je nutné navrhnout efektivní řešení pro využití analýz k certifikaci a jejich další využitelnost. Při zohlednění časové limitace je otázkou, zda je efektivní využít tradiční metody k ověření bezpečnosti a spolehlivosti, nebo zda by bylo přínosem do současných postupů zavést moderní metodu. Jedním z dalších omezení je reaktivita místo proaktivity. Mnoho bezpečnostních analýz se soustředí na předešlé incidenty nebo zjištěné hrozby, ale méně se zaměřují na proaktivní identifikaci potenciálních hrozeb. Toto je zpravidla také způsobeno časovým omezením a vytížeností analytiků, kteří musí splňovat úkoly spojené s certifikací, modernizacemi či odlišnými konstrukčními řešeními letounů.

5 Metodika

V následující kapitole popisuji jednotlivé přístupy, metody, schémata, které jsem ve své práci využil.

5.1 Analytický rozklad

Obecně můžeme systém analyzovat pomocí dvou přístupů. Prvním je tradiční analytický rozklad odpovídající induktivním a deduktivním analýzám. Tento přístup zkoumá jednotlivé prvky systému a dílčí výstupy poté spojuje v celek. Jedná se o tradiční přístup, kterým byly řešeny složité systémy. Takovýto systém byl poté rozložen na menší části, které byly zkoumány a analyzovány zvlášť. Následná syntéza výsledků umožnila pochopit chování složitých systémů. Tuto analýzu bylo možné aplikovat v případech, kdy bylo propojení jednotlivých komponentů přímé a zřejmé. Pro ilustraci slouží obr. 1 na kterém vidíme systém složený z komponent C1 až C5 a přímé vazby mezi prvky. Přístupem druhým je systémový přístup, který zkoumá systém vždy jako celek a nerozkládá jej na dílčí části viz kapitola 5.4.



Obrázek 8 Schéma vazeb mezi komponenty [16]

Pro využití analytického rozkladu je nutné splnit tyto podmínky:

1. Každý komponent pracuje nezávisle na ostatních
2. Chování komponentů se nezmění rozkladem systému
3. Komponenty podléhají přímým interakcím a zpětným vazbám
4. Komponenty lze analyzovat v kombinacích a posuzovat je složenou hodnotou.
5. Události poruch musejí být stochastické

V případě, že daný systém tyto podmínky splňuje, je možné tento přístup využít a posoudit ho pomocí tradičních spolehlivostních metod, které z tohoto přístupu vycházejí. Hodnocení spolehlivosti systému letadla je provedeno rozložením systému na jednotlivé komponenty. Matematickou kombinací pravděpodobností selhání je vypočtena výsledná pravděpodobnost selhání, jež udává spolehlivost celého systému. S rostoucí složitostí letadlových systémů a integrování softwaru do klíčových funkcí letadel není tato metoda dostačující pro nalezení všech možných nebezpečných stavů či příčin poruch. Události poruch musejí být stochastické, což software, stejně jako lidský faktor, nevykazuje, proto nemohou být součástí těchto analýz. Metodika analýz posuzující i tato chování je postavena na teorii systémů. [16]

5.2 FHA – Fault Hazard Analysis

Je induktivní kvalitativní analýza tvořící přehled funkcí systému a jejich poruchových stavů. Veškeré informace se vyplňují do tabulky. Názornou ukázku můžeme vidět v tabulce č. 7. Formát tabulky sestává z popisu funkce, kam se vyplní příslušná funkce spadající do daného systému. Pro snadnou orientaci v dokumentu je doplněn i kód poruchového stavu a jeho popis. Poruchové stavy se dělí na úplné selhání a částečné ztráty funkcí. V případech symetrických funkcí jako jsou vysouvání klapek či přečerpávání paliva z křídelních nádrží může být posuzován i asymetrický poruchový stav. Pro funkce zajišťované elektrickými systémy a řídícími jednotkami bývá zahrnut i stav samovolného spuštění. Přístup k analýze FHA ve firmě AVA rozšířil analýzu o odlišný dopad při ztrátě funkce, která je signalizovaná pilotovi a může na ni zareagovat. Při selhání funkcí mohou nastat tyto případy signalizace:

- Porucha je signalizována
- Došlo k částečné ztráta signalizace
- Porucha není signalizována

V praxi se do poruchových stromů přidává větev ztráty signalizace. Tabulka FHA dále člení poruchy dle fází letu, které se značí číslicemi 1-7 viz tabulka č. 5.

Tabulka 5: Rozdělení fází letu [10][3]

Fáze letu	
N	**Název fáze letu**
1	Pojíždění / Taxi
2	Vzlet / Take-off
3	Stoupání / Climb
4	Cestovní let / Cruise
5	Sestup / Descent
6	Přiblížení / Approach
7	Přistání / Landing

Následně v tabulce můžeme vidět popis důsledků, a to nejen s ohledem na letoun, ale i posádku. K ohodnocení kritičnosti[4] každého jednotlivého poruchového stavu se využívá kombinace kritičnosti a pravděpodobnosti získané kvalitativní analýzou. Kritičnost se dělí do 4 kategorií dle tabulky č. 6. Při rozhodování, do které kategorie poruchový stav spadá, se vychází z dokumentu MIL-STD-882E viz tabulka č. 2.v kapitole 2.3.

Tabulka 6: Kategorie kritičnosti [9]

Kategorie kritičnosti dle MIL- STD - 882E	
N	**Název kategorie kritičnosti**
1	Katastrofická / Catastrophic
2	Kritická / Critical
3	Závažná / Marginal
4	Nezávažná / Negligible

Pravděpodobnost lze následně dopočítat kvantitativními metodami. Dle výsledné hodnoty lze poruchy kategorizovat opět dle dokumentu MIL-STD-882E. Pro získání RAC tzv. „Risk Assessment Code“ je nutné zkombinovat kritičnost a pravděpodobnost daného poruchového stavu. RAC se poté skládá z číslice a písmene. Poslední částí jsou odkazy na podkladové materiály či verifikační metody využité k ověření a dopočítání pravděpodobností.

Tabulka 7: Vzorová šablona FHA

Funkce		**Popis a hodnocení důsledků poruchových stavů**							**Poznámky**	
		Poruchový stav		**Fáze letu**	**Důsledky poruchového stavu na letoun/ posádku**	**Kritičnost**	**Pravděp.**	**RAC**	**Odkazy na podkladové materiály**	**Verif. metoda**
ID	**Popis**	**ID**	**Popis**							
1	***Hydraulický systém***	**FC_1**	**Porucha hydraulického systému: viz níže**							
1.1.		FC_1.1.		1-7						

[3] Tabulky 5,6,7 byly převzaty z podkladů firmy AVA
[4] Termín kritičnost je využíván firmou AVA pro „*závažnost*“ používaný v jiné literatuře

5.3 FTA – Fault tree analysis

Tato tradiční metoda je využívaná k analýze systémových poruch a k zjištění jejich příčin. Jedná se o kvantitativní analýzu využívající pravděpodobnosti nastání jednotlivých základních či vnějších událostí. FTA využívá deduktivní přístup. Vrcholová porucha je způsobená základními událostmi, jejichž kombinace je reprezentována logickými hradly AND, OR. Přičemž logika hradla AND dané pravděpodobnosti sčítá a logika OR násobí. Logické hradlo AND se používá ve chvíli, kdy je selhání funkce zapříčiněno poruchou všech závislých prvků. Tento případ je využíván u funkcí, které jsou zálohovány více prvky. Opačně logické hradlo OR je využíváno, pokud selhání funkce způsobí jakýkoli závislý prvek. Přehled prvků využívaných v této práci je zobrazen a popsán v tabulce č. 8.

Postup analýzy:

1. **Identifikace hrozeb:** Identifikují se potenciální hrozby, kterými jsou poruchové stavy z FHA analýzy.
2. **Vytvoření poruchových stromů:** Poruchový strom, graficky reprezentuje vztahy mezi událostmi pomocí logických hradel.
3. **Kvantifikace pravděpodobností:** Jednotlivým událostem jsou následně přiřazeny pravděpodobnosti jejich nastání.
4. **Analýza stromu:** Stromy poruch jsou následně analyzovány, kvůli odhalení kritických míst či cest vedoucích k selhání systému.
5. **Návrh opatření:** Na základě analýzy jsou navržena opatření k minimalizaci rizik a zvýšení spolehlivosti systému

Tabulka 8: Přehled prvků poruchových stromů [3]

NÁZEV	SYMBOL	DEFINICE
Události		
Vrcholová událost		Může být vrcholovou událostí, či událostí mezilehlou, do níž vstupují události základní skrze logická hradla.
Základní událost		Základní příčina vzniku poruchy. Může symbolizovat jak selhání některého z komponentů, tak i možnou událost.
Vnější událost		Je externím zdrojem příčiny poruchy. Využívá se například při zahrnutí součásti, která je nepřímo závislá na daném systému, ale není jeho součástí.
Logická hradla		
OR		Je logickým hradlem symbolizující logický součin. Jakákoli událost, která do logického hradla OR vstupuje s pravděpodobnostní hodnotou 1 způsobí pravděpodobnostní hodnotu 1 na výstupu. Symbolizuje části systému, které nejsou zálohovány.
AND		Je logickým hradlem symbolizující logický součet. Události, které do logického hradla AND vstupují musí mít všechny pravděpodobnostní hodnotou 1, aby způsobily pravděpodobnostní hodnotu 1 na výstupu. Symbolizuje části systému, které jsou zálohovány.

5.4 Teorie systémů

Tato teorie vznikla po druhé světové válce v kontextu vývoje čím dál složitějších systémů, které se nedaly popsat pouhým analytickým rozkladem. Její využití je velmi široké od popsání biologických funkcí s nejasnými vazbami až po analýzy složitých systémů. V letectví byla poprvé využita v 50. a 60. letech dvacátého století k návrhu raketových systémů. V současnosti se k posuzování bezpečnosti začíná využívat systémový přístup. V případě, kdy chceme do analýzy zahrnout kromě hardwaru i software nebo například lidský faktor, musíme zvolit systémový přístup. Příkladem je moderní metoda STPA, která vychází z modelu bezpečnosti *System Theoretic Accident Model and Processes* (STAMP). [16] [17]

5.5 System theoretic process analysis STPA [16]

Je moderní kvalitativní metodou k analýze bezpečnosti, využívající se v letectví či jiných odvětvích k identifikaci rizik spojených s komplexními systémy. Analýza STPA je velmi složitou metodou, kterou by měl řešit tým odborníků z různých oblastí, s různými zkušenostmi. Rozmanitý tým poskytuje mnoho úhlů pohledu a zkušeností dle odbornosti.

Analýza sestává ze čtyřech základních kroků:

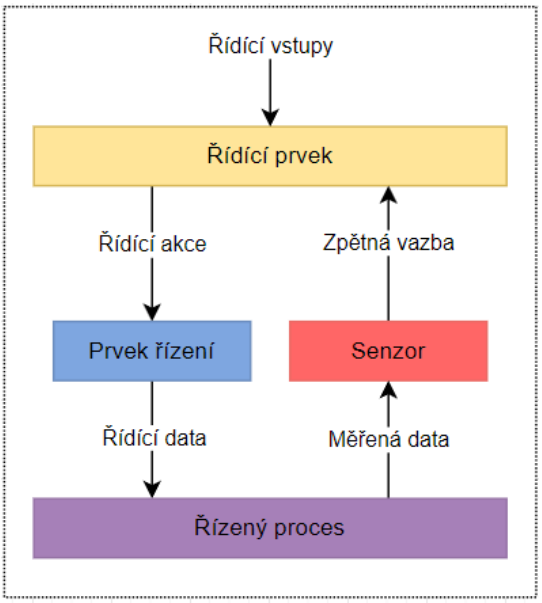
- Definujte účel analýzy
- Vytvořte model řídící struktury
- Identifikujte nebezpečné řídící akce
- Identifikujte ztrátové scénáře

Krok 1: Definování účelu analýzy je základním krokem u všech analýz. Nejprve je nutné vytvořit seznam ztrát v případě selhání. Tyto ztráty bývají globálními důsledky selháni jako je například ztráta lidského života, poškození životního prostředí či neuspokojení zákazníka. Dále se stanovují hranice analyzovaného systém. Zde je třeba uvážit, zda se bude analyzovat systém, letoun, či prostředí ve kterém se letoun pohybuje. Poslední částí je vytvoření nebezpečí, které jsou podobné ztrátám, avšak nejsou důsledkem globálním, ale lokálním. V praxi má každý hazard odkaz na jednu či více ztrát.

Krok 2: Vytvoření modelu struktury dle STAMP. Zobrazuje řídící strukturu mezi prvky řídícími a řízenými a jejich konkrétní příkazy a zpětné vazby. Model struktury STAMP je velmi účinný na popis systému s vysokou úrovní implementované elektroniky a výstižně zobrazuje řídící a zpětnovazební interakce v systému. Kromě daného systému se zde navíc vyskytují interakce s posádkou, což v následujících krocích analýzy STPA umožní rozšířit analýzu o možné pochybení či o nesprávné interakce v rozhraní člověk – stroj. Na obrázku č. 10. můžeme vidět palivový systém rozšířený o palivovou soustavu motoru a interakci s posádkou.

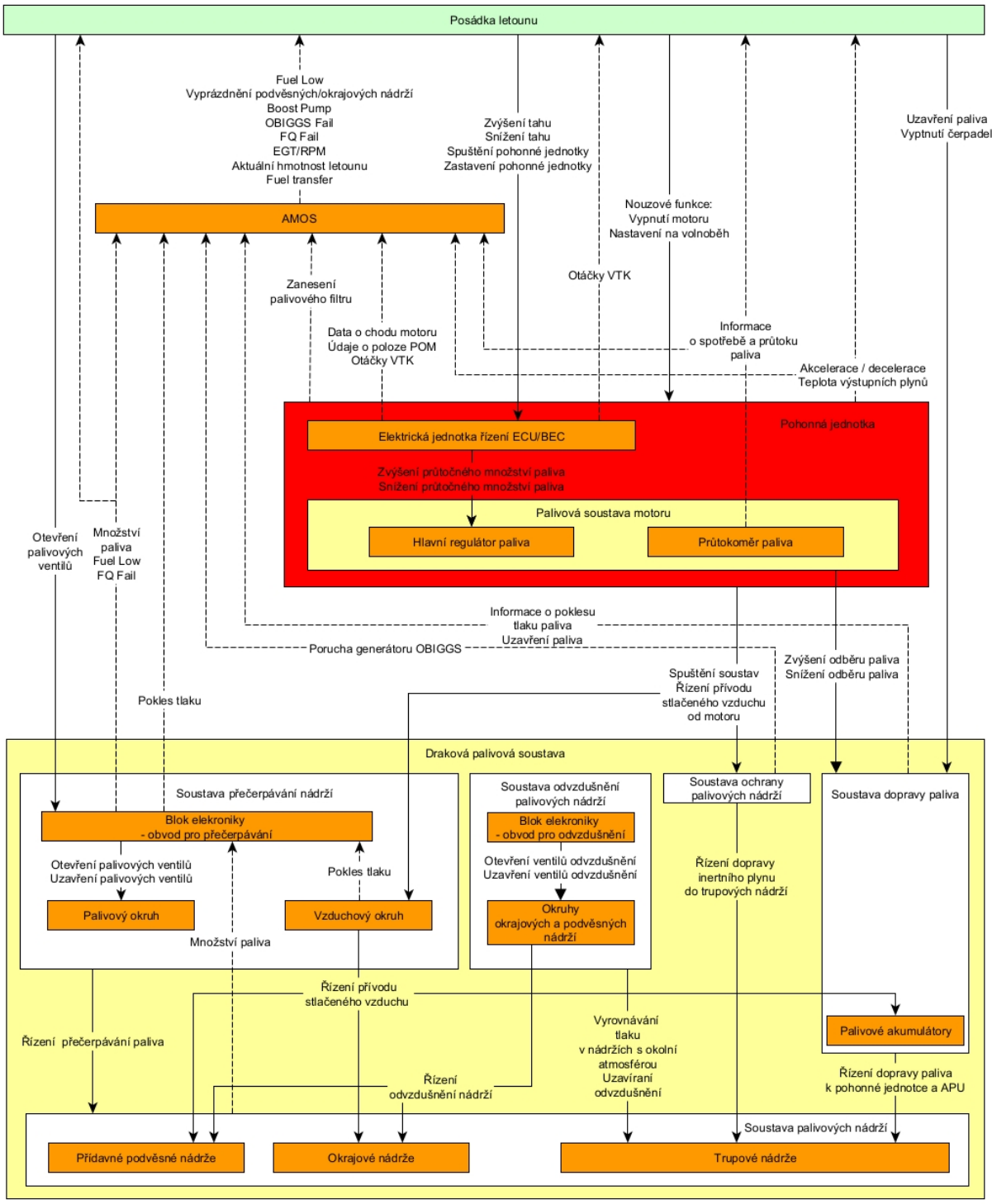
Model struktury STPA rozděluje komponenty systému do 4 kategorií dle jejich funkce.

- Controller – prvek rozhodující a vydávající řídící pokyny
- Actuator –prvek vykonávající svou funkci na základě přijatého signálu z „*controlleru*“
- Controlled process – proces řízený řídícím prvkem a sledovaný senzory
- Sensors – prvek kontrolující funkce systému a vysílající zpětnovazební interakce



Obrázek 9: Řídící smyčka STPA (upraveno a přeloženo z [16])

Následně jsou komponenty seřazeny tak, že řídící prvek („*controller*“) je umístěn nejvýše a signál od něj putuje směrem dolů přes prvky řízení („*actuator*“) vykonávající procesy. Senzory ověřují, zda a jak je daný řízený proces vykonáván. Zpravidla se systém v prvních fázích tvorby modelu zobrazuje co nejjednodušší. Komponenty jsou spojovány do společných bloků pro zjednodušení a nalezení základní struktury. Toho lze využít například ve fázích, kdy není jasné, z jakých komponentů se bude daný systém skládat. Takto lze popsat systémy bez konstrukčního návrhu, a i přesto vytvořit požadavky na systém. S pozdějším vývojem se do schématu přidávají další detaily a je možné zvětšit hloubku analýzy. V posledním kroku se při modelování systému doplňují řídící interakce a jejich zpětné vazby. Tyto řídící interakce tzv. *Control Actions* (CA) se dále analyzují z pohledu nebezpečného řízení a tvoří základ poruchových stavů.



Obrázek 10: Model struktury palivového systému [12]

Krok 3: Identifikace řídících akcí tzv. „*control actions*“ (CA), vedoucích k nebezpečím v kontextu kroku 1. Každá z těchto řídících akcí je posuzována dle následujících kategorií vzniku nebezpečných řídících akcí.

1. Neprovedení způsobí nebezpečí
2. Provedení způsobí nebezpečí
3. Příliš brzy, příliš pozdě, v nesprávném pořadí
4. Zastaveno příliš brzy, aplikováno příliš dlouho

V případě, že by nebezpečí mohlo nastat kterýmkoli způsobem, je každá z interakcí rozdělena na čtyři nebezpečné řídící akce. Důsledkem je mnohem detailnější popis nebezpečí způsobených zastavením či spuštěním funkcí v nesprávnou dobu. Popis UCA je detailnější s ohledem na interakce s jinými systémy, či řídícími členy (posádkou) s ohledem na tradiční metodu FHA. Příklad rozdělení řídící akce brždění můžeme názorně vidět v tabulce 9.

Tabulka 9: Identifikace nebezpečných řídících příkazů (přeloženo z [16])

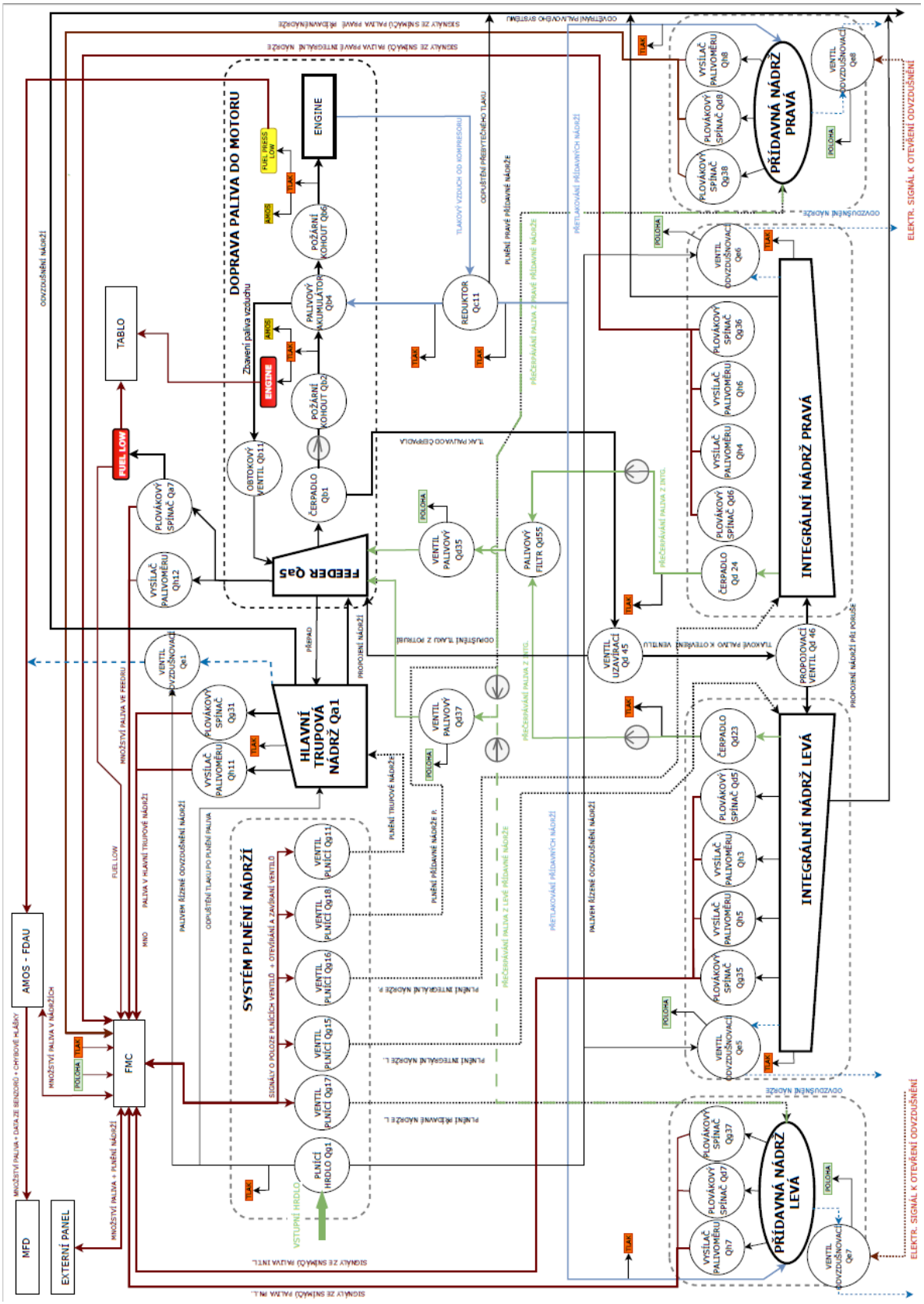
Kontrolní akce	Neposkytnutí funkce	Poskytnutí funkce	Příliš brzy, příliš pozdě, ve špatném pořadí	Zastaveno příliš brzy, aplikováno příliš dlouho
Brždění	UCA1: BSCU Autobrake neposkytuje činnost ovládání brzdy během přistávacího rolování, když je BSCU zajištěna [H-4.1]	UCA2: BSCU Autobrake zajišťuje ovládání brzdy během normálního vzletu [H-4.3, H-4.6]	UCA3: BSCU Autobrake poskytuje činnost ovládání brzdy příliš pozdě (>TBD sekund) po dotyku [H-4.1]	UCA4: BSCU Autobrake přestane poskytovat ovládání brzdy příliš brzy (před dosažením rychlosti pojíždění TBD), když letadlo přistane [H-4.1]

Krok 4: Čtvrtý krok identifikuje důvody, proč se v systému mohlo vyskytnout nebezpečné řízení. Tyto důvody se nazývají scénáře a jsou analogickým krokem k příčinám selhání ve stromech poruch. K těmto scénářům se poté definují tzv. „*constraints*“, sloužící jako požadavky na správnou funkci systémů.

5.6 Funkční schéma

Je určeno k seznámení analytika se systémem. Tento krok není vyžadován žádnou z norem, nicméně pochopení systému je zásadní pro budoucí analýzy, protože veškeré metody jsou velmi závislé na analytikovi a jeho zkušenostech s daným systémem. Slouží jako výchozí schéma, ve kterém jsou popsány vazby komponentů a jejich závislosti, proto je jeho vypracování pro budoucí analýzu stěžejní. Funkční schéma je zjednodušené schéma vycházející z technického výkresu systému rozšířeného o další potřebné či závislé systémy. Zobrazuje veškeré komponenty a jejich funkční propojení nikoliv řídící strukturu. Příklad funkčního schématu palivového systému můžeme vidět na obrázku 11.

Popis tvorby schématu: V prvním kroku se musí stanovit hranice systému. Je vhodné zpracovat seznam všech komponentů a jejich funkcí, který lze kromě využití ve funkčním schématu, využít v následující analýzách pro stanovení pravděpodobností selhání u konkrétních komponentů. Schéma se poté tvoří podle technického výkresu. Ten zpravidla neobsahuje elektrická schémata, která jsou potřebná pro následnou analýzu k prošetření dopadů ztráty el. zdrojů, čidel či jiných elektronických zařízení. Po vytvoření struktury se jednotlivé komponenty propojí funkcemi, které lze získat z technického popisu systému.



Obrázek 11: Funkční schéma palivového systému L-39NG

6 Porovnání analýz

Pro porovnání jednotlivých přístupů jsem si vybral palivový systém letounu L-39NG, pro který jsem vytvořil bezpečnostní analýzu tradičními metodami. Analýzu jsem vytvářel dle postupů, které se využívají ve firmě Aero Vodochody Aerospace a sestává z kombinace FHA a FTA analýz. Druhou srovnávanou metodou je analýza STPA, která byla využita k analyzování modernizovaného letounu L-159. Oba systémy se v jejich funkcích zásadně neliší a poruchové stavy, které jsou způsobené odlišností systémů jsem do srovnání nezahrnoval.

V prvním kroku jsem porovnal schémata využívaná oběma přístupy. Při analýze tradičními metodami se jedná o funkční schéma, u analýzy STPA je to poté model hierarchické zpětnovazebné struktury dle STAMP.

Následně jsem pro stanovení rozdílů výstupů jednotlivých metod vybral tři poruchové stavy.

- Soustava nedodává palivo do motoru
- Soustava nedodává palivo do motoru při letu na zádech
- Palivo není přečerpáváno z křídelních nádrží

Každý poruchový stav zahrnuje popis a rozdíly, které odhalila analýza STPA oproti analýzám tradičním. Za porovnáním jsou přiloženy výstupy jednotlivých přístupů ve formě tabulek a grafický výstup stromu poruch. V závěru jsou zobecněny rozdíly a výhody odlišných přístupů.

Analýza tradičními metodami obsahuje poruchy, které mohou vzniknout v cestě paliva přes jednotlivé komponenty. Díky tomuto se v analýze objevují některé poruchy jako jsou například porucha obtokového ventilu či požárních kohoutů. Toto není způsobené nedostatky analýzy STPA. Její přístup shledává problém bezpečnosti v selhání řízení systému nikoli ve fyzických poruchách. Rozdíl je zde i v hloubce analýzy a jejím zaměření. STPA byla využita k analýze modernizace systému, a proto je více zaměřená na modernizované prvky. V některých případech je vidět, že zobecněním systému ztrácíme značnou část informací, a tím i počet nalezených poruchových stavů, které by jinak STPA byla schopna odhalit. Součástí poruchových stromů bývají i průměrné hodnoty poškození, které během provozu nastávají jako jsou netěsnosti potrubí či jiné úniky.

6.1 Přístup jednotlivých schémat

Funkční schéma

Je v podstatě upravený technický výkres s doplněním funkcí a závislostí na elektrických či jiných závislých systémech, byť nepřímo. Schéma lze následně využít jako podklad pro jiné oddělení vývoje či jako doplňující schéma spolehlivostního programu či letové příručky. Pro provádění analýz tradičními metodami je toto výhodnější, protože je zde přehledně vidět, jaká komponenta mohla způsobit určitou poruchu. Pro tvorbu analýzy metodou FTA stačí zhodnotit, zda jsou poruchy přímo závislé na daných komponentech, nebo musí dojít k selhání více prvků. V případě elektrických interakcí jsou komponenty propojeny funkcemi či popisem toku dat. Na rozdíl od modelu STAMP se zobrazuje pouze systém a do schématu se již neimplementuje interakce s posádkou. Tímto je analýza ochuzena o lidský faktor, nicméně tradiční analýzy nebyly koncipované pro posuzování rozhraní člověk – stroj, a proto by jeho zahrnutí do funkčního schématu nebylo přínosem.

Model dle struktury STAMP

Jde o diametrálně odlišný druh schématu, než jsou například technické výkresy či funkční schéma, protože nezobrazuje fyzické propojení komponent. Pro pochopení a interpretaci některých funkcí daného systému není tento model vhodný, protože zobrazuje pouze řídící strukturu. Díky tomu je vhodný pro popis toho, jak je, který prvek systému řízen a zda jej ovládá posádka či je řízen elektronicky některou z řídících jednotek. Model nám může poskytnout i informaci, zda mají řízené procesy zpětné vazby a jejich funkce je tedy kontrolována. Pro popis a zobrazení toku dat elektrickou cestou je model vhodnější. Výhodou může být i možnost zobrazení hrubého návrhu v prvopočátcích vývoje, který lze s postupem nových konstrukčních řešení zdokonalovat.

Porovnání schémat

Schémata zobrazují systém velmi odlišně, a proto by tvorba obou schémat byla přínosná. Ze schématu dle STAMP lze vyčíst jaké jsou závislosti mezi jednotlivými řídícími smyčkami a jak mezi sebou systémy interagují. Technickou strukturu a fyzické propojení prvků by poté mohlo doplňovat funkční schéma, které by nemuselo obsahovat veškeré informace, ale pouze funkční propojení bez zahrnutí toku dat. Výsledkem by bylo přehlednější schéma závislosti funkcí. Popis řízení a zpětných vazeb by zobrazoval model STAMP, který je pro toto navržený a jeho výsledek je přehlednější.

6.2 Poruchový stav 1.

Popis poruchového stavu

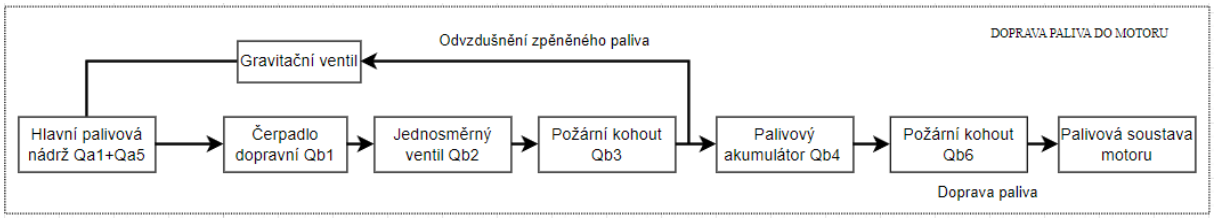
Poruchový stav č. 1 se zabývá přerušenou dodávkou paliva do palivové soustavy motoru. Palivo je dodáváno pomocí dopravního čerpadla, které zajišťuje přetlakovou dodávku paliva. Při jeho poruše je motorové palivové čerpadlo schopné nasát palivo přes obtokový ventil.

Analýza STPA: Tento poruchový stav odpovídá UCA-93 viz tabulka č. 11

Analýza metodou STPA objevila navíc tyto scénáře:

- Sc-93.4: Soustava přečerpávání paliva nedopraví palivo do trupových nádrží
- Sc-93.6: Posádka uzavře požární kohout

Analýza STPA rozšířila analýzu o nebezpečné chování posádky nevhodným uzavřením palivového kohoutu. Tímto scénářem vzniká požadavek pro konstruktéry systému, aby zajistili, že k takovémuto případu nedojde nevědomostí a že tato skutečnost bude součástí provozních postupů v letové příručce. Navíc je zde uveden i scénář Sc-93.4 popisující poruchu přečerpávání paliva do trupových nádrží. Tento stav je obsažen i v analýze tradičními metodami, avšak není součástí poruchového stavu přerušení dodávky paliva do palivové soustavy motoru. Na tomto příkladu je možné vidět přesah analýzy STPA do jiných funkcí či systémů, které by mohly ovlivnit funkci dodávky paliva do motoru.



Obrázek 12: Funkční schéma dopravy paliva do motoru

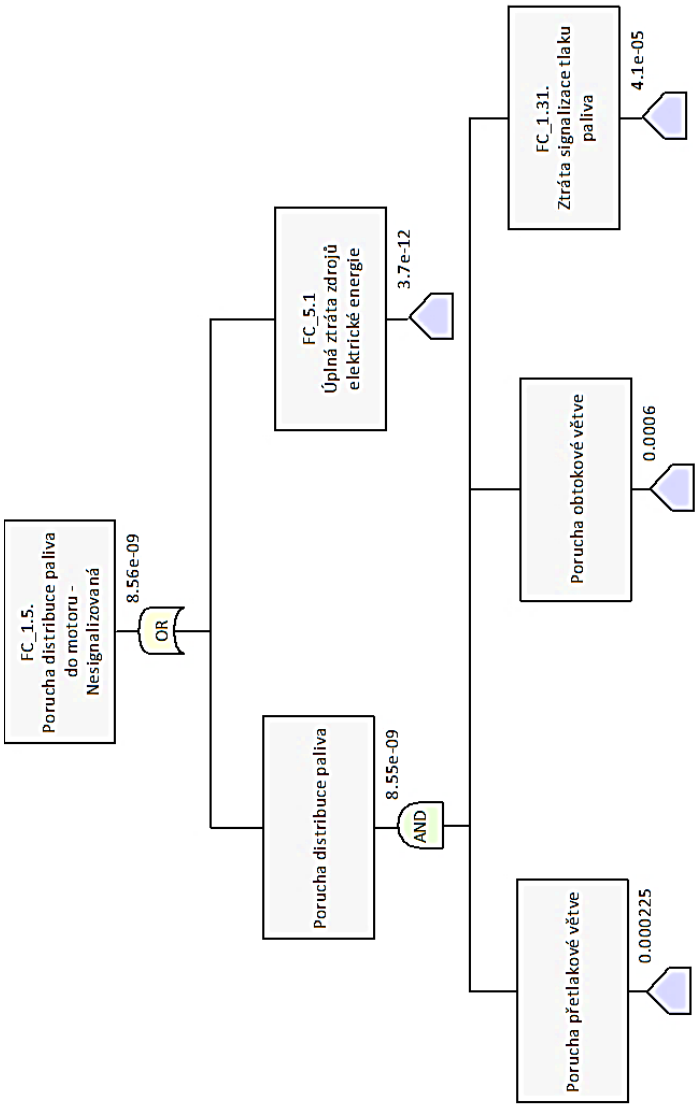
Funkce dodávky paliva (zobrazena na obr.12) je zajišťována dopravním čerpadlem, za kterým je umístěn jednosměrný ventil, požární kohouty, palivový akumulátor a tlaková čidla. Na tomto příkladu je vidět, že u funkcí, které nejsou natolik komplexní, není rozdíl výstupů z jednotlivých analýz významný. Výstup z analýzy tradičními metodami můžeme vidět v tabulce 10.

Tabulka 10: FHA Poruchový stav FC_1.6.

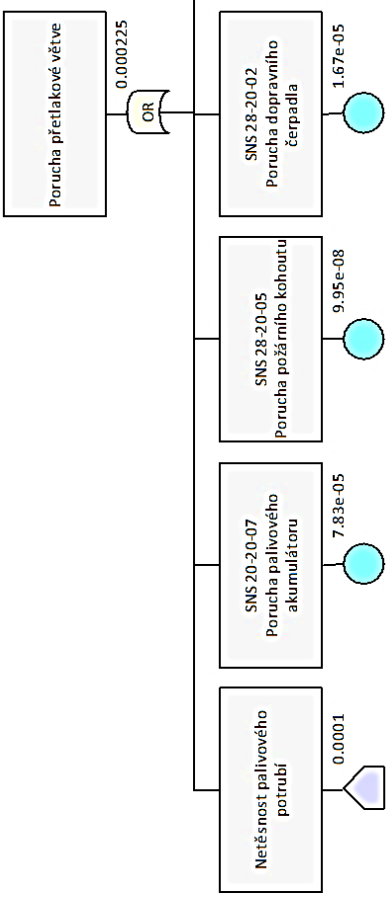
Funkce		Popis a hodnocení důsledků poruchových stavů							Poznámky	
		Poruchový stav		Fáze letu	Důsledky poruchového stavu na letoun/ posádku	Kritičnost	Pravděp.	RAC	Odkazy na podkladové materiály	Verif. metoda
ID	**Popis**	**ID**	**Popis**							
1	***Palivový systém***	**FC_1**	**Porucha palivového systému**							
1.1.	Distribuce paliva do motoru	FC_1.6.	Soustava nedodává palivo do motoru **NESIGNALIZOVÁNO**	2-7	Při přerušení dodávky paliva do motoru dojde k vysazení pohonné jednotky. Při nesignalizované poruše v systému dodávky paliva je velmi zvýšená zátěž posádky v ohledu na neočekávané vysazení pohonné jednotky.	1	$8{,}56^{-9}$	1E	FTA FC_1.5.	FTA

Tabulka 11: STPA: přehled scénářů a požadavků vyplívajících z UCA - 93

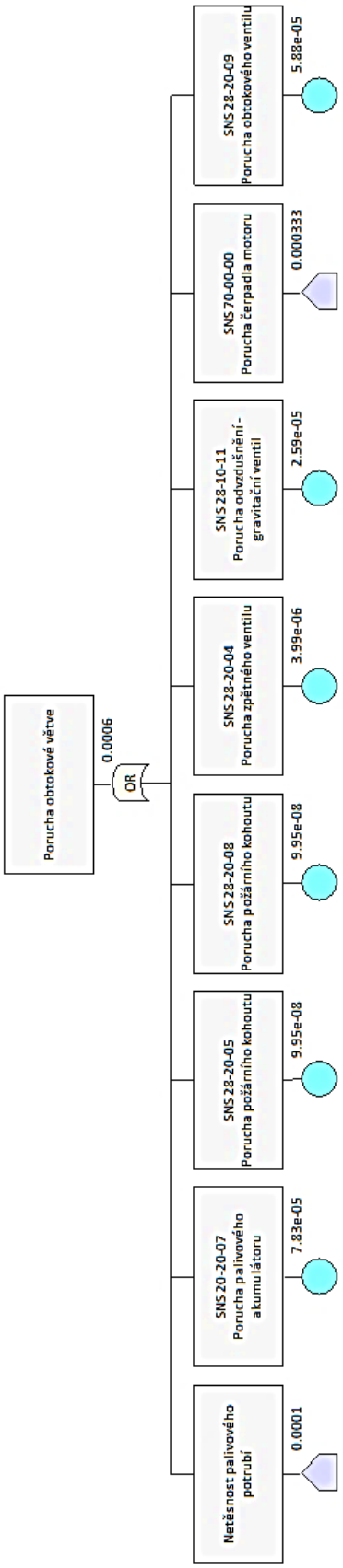
UCA	Scenario	Constraints
UCA-93: Nedodání paliva k odběru do palivové soustavy motoru [H-1, H-2, H-3, H-7]	Sc-93.1: Hlavní a záložní dopravní čerpadlo není schopno dopravit palivo z trupových nádrží;	Sc-93.1 C: Dopravní čerpadla musí plnit svou funkci;
	Sc-93.2: Záložní dopravní čerpadlo se nespustí po vysazení hlavního dopravního čerpadla;	Sc-93.2 C: Záložní dopravní čerpadlo se okamžitě spustí při výpadku hlavního dopravního čerpadla;
	Sc-93.3: Hlavní dopravní čerpadlo palivové soustavy motoru nedokáže palivo z dopravní větve odčerpat;	Sc-93.3 C: Hlavní palivové čerpadlo pohonné jednotky vždy odčerpá potřebné palivo;
	Sc-93.4: Soustava přečerpávání paliva nedopraví palivo do trupových nádrží;	Sc-93.4 C: Soustava přečerpávání paliva vždy dopraví potřební palivo do trupových nádrží;
	Sc-93.5: Soustava odvzdušnění nádrží nevyrovná tlak nad hladinou paliva v trupových nádržích;	Sc-93.5 C: Soustava odvzdušnění nádrží zabrání podtlaku či přetlaku v trupových nádržích
	Sc-93.6: Posádka uzavře požární kohout;	Sc-93.6 C: Posádka uzavře požární kohout pouze při vzniku požáru;
	Sc-93.7: Neotevření zpětných ventilů tlakem proudu paliva;	Sc-93.7 C: Zpětné ventily se vlivem provozního tlaku paliva otevřou;



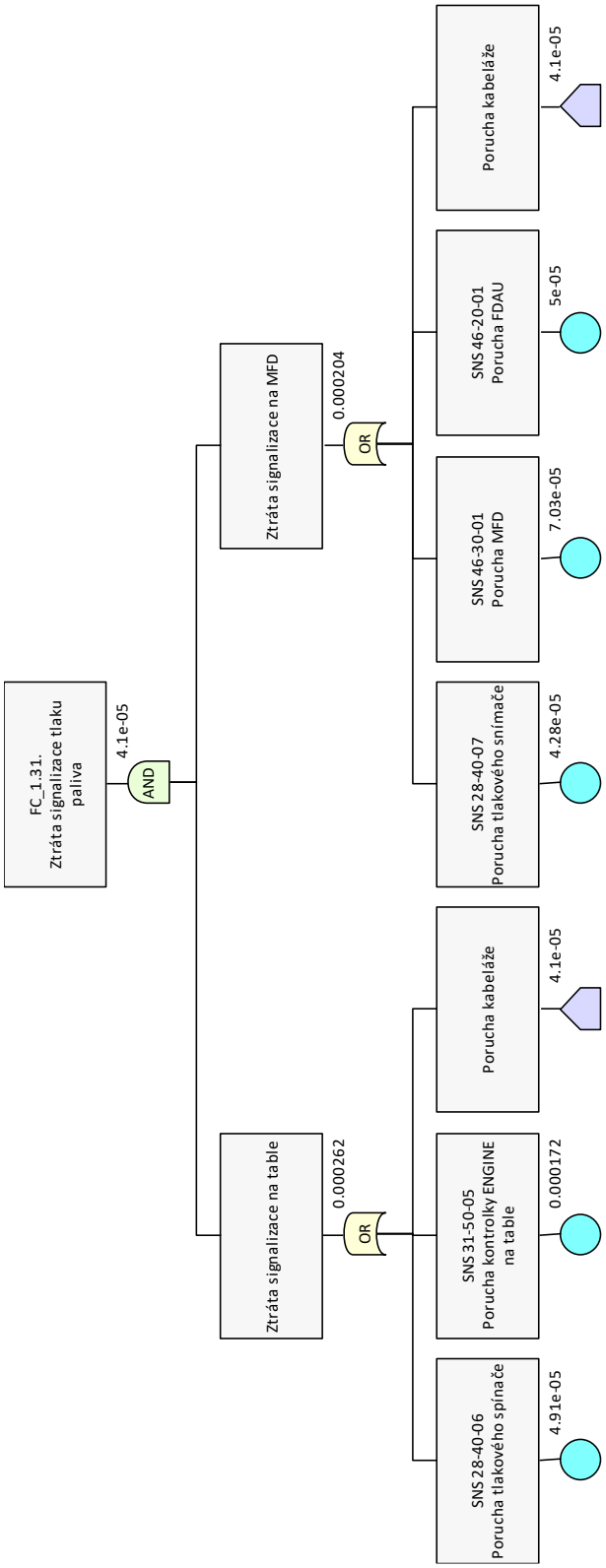
Obrázek 13 FTA – FC_1.5.



Obrázek 14 FTA – Porucha přetlakové větve



Obrázek 15 FTA – Porucha obtokové větve



Obrázek 16 FTA – Porucha signalizace paliva

6.3 Poruchový stav 2.

Popis poruchového stavu

Poruchový stav č. 2 se zabývá přerušenou dodávkou paliva do palivové soustavy motoru při letu na zádech či v náročnějších režimech. Konstrukce systému u letounu L-39 NG je koncipována pro let na zádech kratší než 20 sekund. Po tuto dobu je tlak paliva vytvářen palivovým akumulátorem, který je přetlakovaný vzduchem z motoru. Po provedeném manévru se musí letoun převést opět do běžného letu, aby se palivový akumulátor znovu natlakoval.

Analýza STPA: Tento poruchový stav odpovídá UCA-95 viz tabulka č. 13 .

Analýza metodou STPA objevila navíc tyto scénáře:

- Sc-95.3: Posádka provadí let se zápornými násobky nebo okolonulovými násobky příliš dlouho;
- Sc-95.4: Posádka nepřevede letoun do běžných letových podmínek na dostatečně dlouhou dobu;
- Sc-95.5: Palivové akumulátory byly vyčerpány dříve, než bylo nutné jejich použití vlivem vysokého tlaku přivedeného vzduchu;

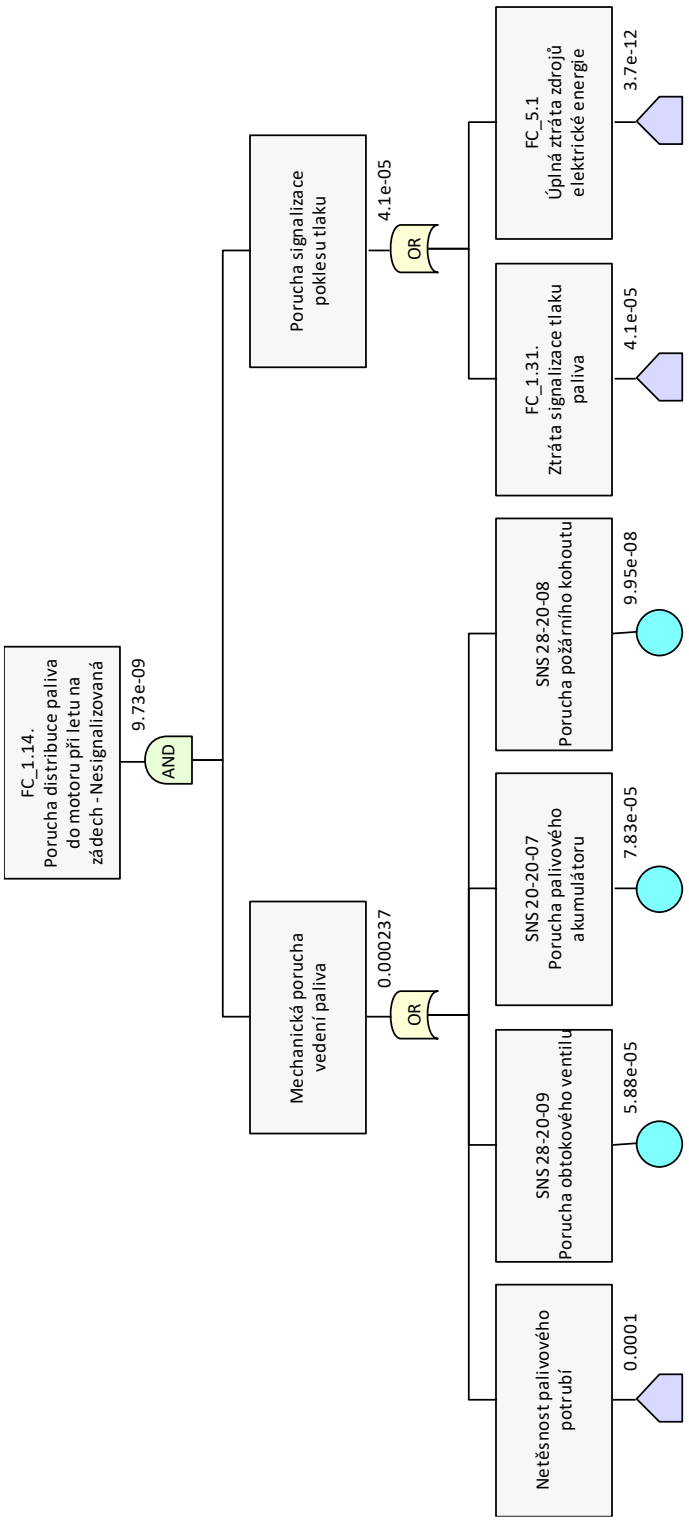
Díky přístupu využívaným v AVA je součástí FHA analýzy i vliv lidského činitele. Poruchové stavy, které jsou pilotovi signalizovány, jsou vnímany jako méně kritické kvůli možné reakci pilota na poruchu. Naopak nesignalizované případy jsou více kritické. Posuzování případů, kdy dojde k nesignalizované závadě, a přesto je jejich pravděpodobnost v limitech předepsaných norem, prokazuje vyšší bezpečnost systému. Implementací nesignalizovaných poruch se analýza odchyluje od standardů, ale značně rozšiřuje analýzu poruchových stavů, a tím zvyšuje bezpečnost provozu těchto systémů. V případě využití analýzy STPA místo FHA by byly již do kvalitativní analýzy zahrnuty tyto a další situace. Příklad rozšíření analýzy o nesignalizované poruchy odpovídá scénáři Sc-95.7. Scénář popisuje případ, kdy posádka neobdrží signál o ztrátě funkce hlavního dopravního čerpadla (kontrolka „BOOST PUMP“ na výstražném table, nápis „FUEL MAIN PUMP“ na MFD). Příčiny tohoto stavu odpovídají pravé větvi stromu poruch (FC_1.14.) ztráta signalizace. Výstup z analýzy tradičními metodami můžeme vidět v tabulce 12.

Tabulka 12: FHA poruchový stav FC_1.14.

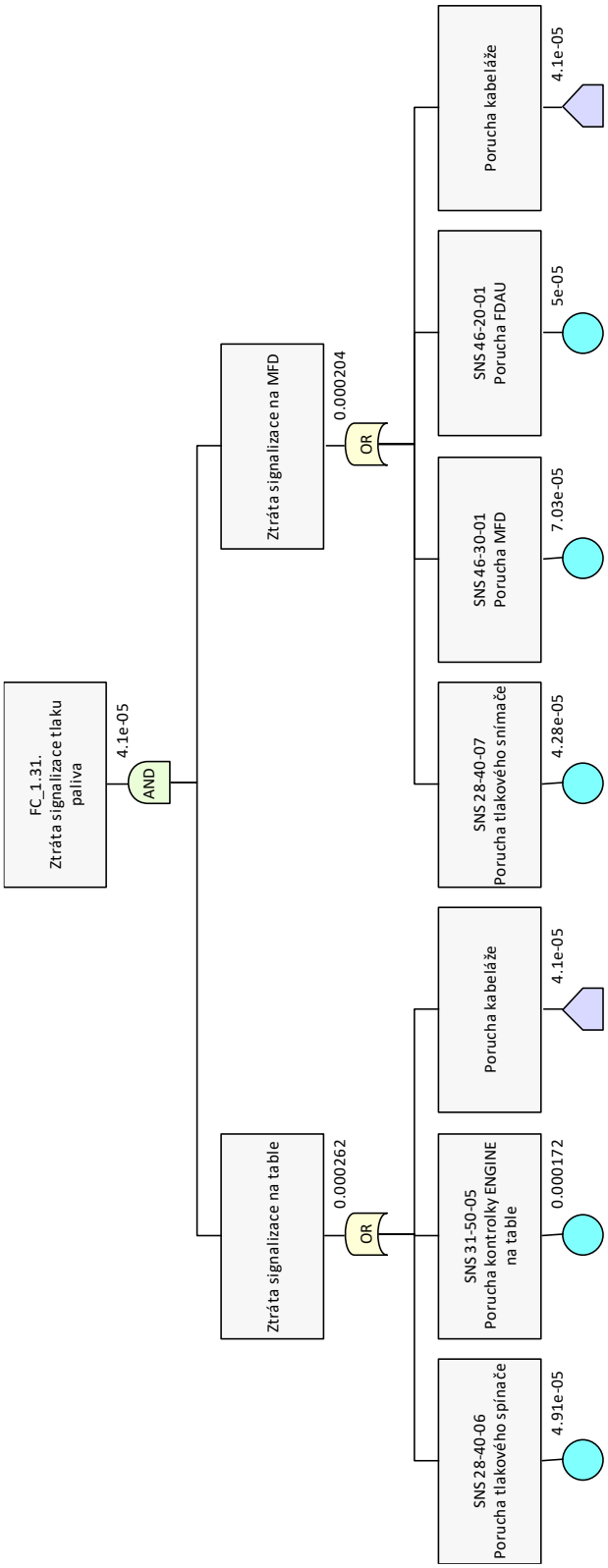
Funkce		Popis a hodnocení důsledků poruchových stavů							Poznámky	
		Poruchový stav		Fáze letu	Důsledky poruchového stavu na letoun/ posádku	Kritičnost	Pravděp.	RAC	Odkazy na podkladové materiály	Verif. metoda
ID	Popis	ID	Popis							
1	*Palivový systém*	FC_1	Porucha palivového systému							
1.2.	Distribuce paliva do motoru při letu na zádech	FC_1.14.	Soustava nedodává palivo do motoru při letu na zádech **NESIGNALIZOVÁNO**	4	Při poruše palivového akumulátoru není zajištěna přetlaková dodávka paliva při letových obratech. Při nesignalizované poruše tato situace zvyšuje zátěž posádky a ohrožuje bezpečnost letu z hlediska neočekávaného vysazení motoru v určitých fázích letu či letových obratech.	1	$9{,}73^{-09}$	1E	FTA FC_1.14.	FTA

Tabulka 13: STPA: přehled scénářů a požadavků vyplívajících z UCA-95

UCA	Scenario	Constraints
UCA-95: Nedopravení paliva při náročnějších režimech letu pomocí palivových akumulátorů [H-1, H-3, H-7]	Sc-95.1: Vzduchový okruh soustavy přečerpávání nádrží nedodá stlačený vzduch do palivových akumulátorů o potřebném tlaku;	Sc-95.1 C: Vzduchový okruh soustavy přečerpávání nádrží musí dodat stlačený vzduch do palivových akumulátorů o min. tlaku 35 kPa;
	Sc-95.2: Hlavní dopravní čerpadlo není ve funkci;	Sc-95.2 C: Hlavní dopravní čerpadlo se musí spustit k znovunaplnění akumulátoru palivem;
	Sc-95.3: Posádka provadí let se zápornými násobky nebo okolonulovými násobky příliš dlouho;	Sc-95.3 C: Posádka nebude uvádět letoun do záporných či okolonulových násobků déle než 20 sekund;
	Sc-95.4: Posádka nepřevede letoun do běžných letových podmínek na dostatečně dlouhou dobu;	Sc-95.4 C: Posádka musí počkat 15 sekund, než znovu uvede letoun do záporných či okolonulových násobků;
	Sc-95.5: Palivové akumulátory byly vyčerpány dříve, než bylo nutné jejich použití vlivem vysokého tlaku přivedeného vzduchu;	Sc-95.5 C: Vzduchový okruh soustavy přečerpávání nádrží nesmí přivést stlačený vzduch do palivových akumulátorů, jenž přesahuje 65 kPa;
	Sc-95.6: Snímač tlaku za hlavním čerpadlem nevyhodnotí pokles paliva;	Sc-95.6 C: Snímač tlaku vždy vyhodnotí pokles tlaku paliva za hlavním dopravním čerpadlem;
	Sc-95.7: Posádka neobdrží signál o ztrátě funkce hlavního dopravního čerpadla (kontrolka „BOOST PUMP“ na výstražném table, nápis „FUEL MAIN PUMP“ na MFD)	Sc-95.7 C: Posádka letounu vždy obdrží adekvátní signály o poklesu tlaku paliva za hlavním dopravním čerpadlem;



Obrázek 17 FTA – FC_1.14.



Obrázek 18 FTA – Ztráta signalizace tlaku paliva

6.4 Poruchový stav 3

Popis poruchového stavu

Tento stav nastává v případě přerušení přečerpávání paliva z křídelních/podvěsných nádrží do trupové odkud je palivo distribuováno do palivové soustavy motoru. Poruchou přečerpávání paliva se omezuje množství paliva pouze na trupové nádrže a tím se zkracuje dolet letounu. V případě, kdy tato skutečnost není indikována letové posádce, hrozí riziko vysazení motoru po vyčerpání paliva z trupových nádrží.

Analýza STPA: Tento poruchový stav odpovídá UCA-83 viz tabulka č. 15.

Analýza metodou STPA objevila navíc tyto scénáře:

- Sc-83.8: Posádka nevyhodnotí závadu řídící jednotky přečerpávání paliva (nápis „FQ FAIL“ na MFD, nápis „Err5“ na digitálním displeji palivoměru, analogová ručička palivoměru se přemístí na nulu) přemístěním přepínače „FUEL QTY“ do polohy „FAIL“
- Sc-83.7: Posádka nevyhodnotí minimální množství paliva v trupových nádržích (svítí kontrolka „FUEL LOW“ na levém výstražném table, ručička ukazatele palivoměru je v červeném poli) přemístěním přepínače „FUEL QTY“ do polohy „FAIL“

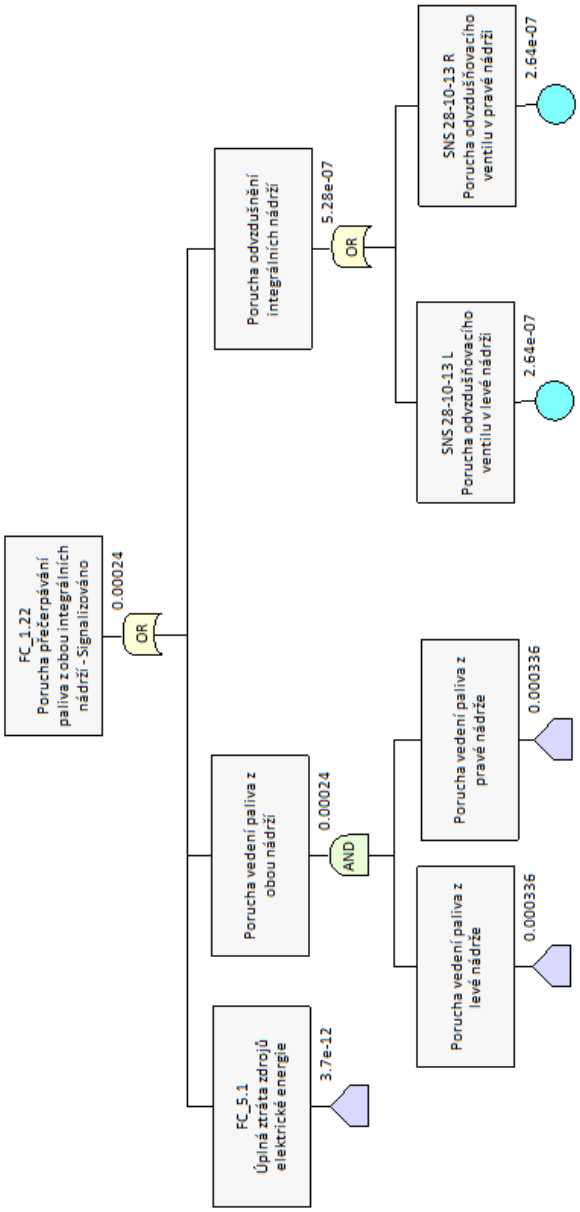
Jak můžeme vidět opět se jedná o rozšíření analýzy o pochybení letové posádky špatným vyhodnocením stavu paliva v trupových nádržích či špatné funkci řídící jednotky. Tradiční metody objevy stejné příčiny poruchových stavů vedoucích k přerušení přečerpávání paliva. Vyjímkou byly pouze případy spojené s pochybením posádky. Zahrnutí lidského faktoru je zde implementováno pouze v rozdělení poruchových stavů na signalizované a nesignalizované. Výstup z analýzy tradičními metodami můžeme vidět v tabulce 14.

Tabulka 14: FHA poruchový stav FC_1.22.

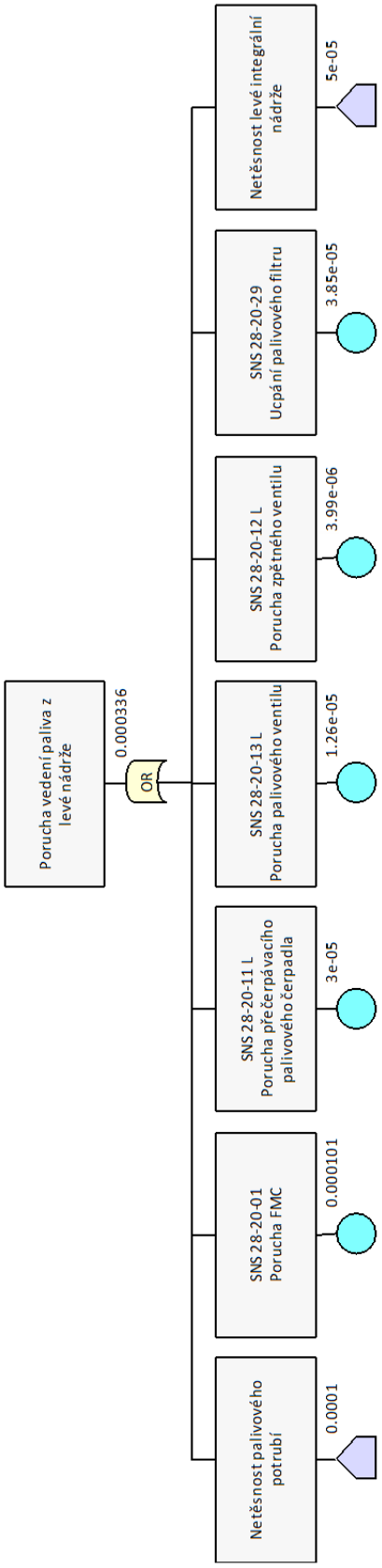
Funkce		Popis a hodnocení důsledků poruchových stavů							Poznámky	
		Poruchový stav		Fáze letu	Důsledky poruchového stavu na letoun/ posádku	Kritičnost	Pravděp.	RAC	Odkazy na podkladové materiály	Verif. metoda
ID	Popis	ID	Popis							
1	***Palivový systém***	**FC_1**	**Porucha palivového systému**							
1.4.	Přečerpávání paliva z integrálních nádrží	FC_1.22.	Palivo není přečerpáváno z obou nádrží **SIGNALIZOVÁNO FUEL TRANSFER FAIL**	1-7	Ztráta paliva z obou integrálních nádrží má za důsledek omezení množství paliva na podvěsné a trupové nádrže a tím i omezení doletu letounu.	4	$2,4^{-4}$	4D	FTA FC_1.22.	FTA

Tabulka 15: STPA: přehled scénářů a požadavků vyplívajících z UCA-83

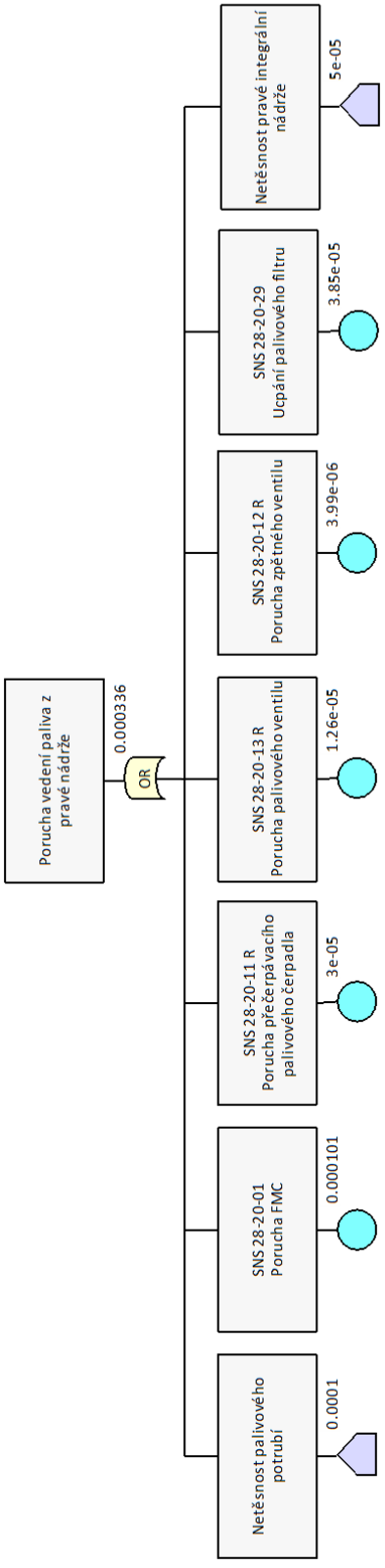
UCA	Scenario	Constraints
UCA-83: Nepřečerpání paliva mezi nádržemi za letu [H-1, H-2, H-3, H-5, H-7]	Sc-83.1: Nespuštění soustavy přečerpávání po ukončení spouštěcí sekvence motoru;	Sc-83.1 C: Pohonná jednotka začne napájet soustavu přečerpávání po ukončení její spouštěcí sekvence;
	Sc-83.2: Nepřivedení dostatečného tlaku odebraného vzduchu od motoru do soustavy přečerpávání;	Sc-83.2 C: Od motoru bude vždy přivedeno dostatečné množství stlačeního vzduchu do soustavy přečerpávání;
	Sc-83.3: Soustava odvzdušnění nádrží zrušila přetlak v křídelních nádržích;	Sc-83.3 C: Soustava odvzdušnění nádrží zruší přetlak pouze v stanovených případech;
	Sc-83.4: Vzduchový okruh soustavy přečerpávání nedostatečně distribuuje přiváděný tlak do křídelních nádrží;	Sc-83.4 C: Vzduchový okruh soustavy přečerpávání adekvátně distribuuje stlačený vzduch do křídelních nádrží;
	Sc-83.5: Blok elektroniky neotevře cestu skrz palivové ventily z křídelních do trupových palivových nádrží;	Sc-83.5 C: Blok elektroniky řídí otevíráním palivových ventilů stanovenou posloupnost přečerpávání;
	Sc-83.6: Tlak paliva nepřetlačí zpětné ventily palivového potrubí větve přečerpávání;	Sc-83.6 C: Zpětné palivové ventily jsou seřízeny, aby jimi palivo o provozním tlaku proteklo do trupových nádrží;
	Sc-83.7: Posádka nevyhodnotí minimální množství paliva v trupových nádržích (svítí kontrolka „FUEL LOW“ na levém výstražném table, ručička ukazatele palivoměru je v červeném poli) přemístěním přepínače „FUEL QTY“ do polohy „FAIL“;	Sc-83.7 C: Posádka vyhodnotí minimální množství paliva přestavením přepínače „FUEL QTY“ do polohy „FAIL“ / Posádka musí získat informaci o přerušeném přečerpávání dříve než obdrží příznaky o minimálním množství paliva;
	Sc-83.8: Posádka nevyhodnotí závadu řídící jednotky přečerpávání paliva (nápis „FQ FAIL“ na MFD, nápis „Err5“ na digitálním displeji palivoměru, analogová ručička palivoměru se přemístí na nulu) přemístěním přepínače „FUEL QTY“ do polohy „FAIL“;	Sc-83.8 C: Posádka vyhodnotí závadu řídící jednotky přečerpávání paliva přestavením přepínače „FUEL QTY“ do polohy „FAIL“;a



Obrázek 19 FTA – FC_1.22.



Obrázek 20 FTA – Porucha vedení paliva z levé nádrže



Obrázek 21 FTA – Porucha vedení paliva z pravé nádrže

6.5 Porovnání výstupů analýz

Tradiční přístup s přístupem dle modelu STAMP má velmi podobné rysy. V mnoha částech si analýzy odpovídají. V této části bych rád zhodnotil jednotlivé odlišnosti a zaměřil se na výhody, které z jednotlivých přístupů vyplývají.

Analýza STPA je schopna odhalit kromě poruchových stavů odhalených tradičními metodami i mnoho dalších. Dále je schopna poruchové stavy více členit, a to pro jakékoli fáze letu či podmínky před nebo po kterých se má funkce spustit/zastavit a není omezena jen na fáze (1-7) dané analýzou FHA viz kapitola 5.2. Dalším přínosem jsou *„constraints"* neboli omezení, které jsou negacemi scénářů poruch. Tento seznam je výstupem analýzy STPA a jeho využitelnost je přínosná v období vývoje komponentů. Především pokud je nutné vyvinout komponentu, u které neznáme jeho konstrukční návrh, můžeme pomocí STPA získat seznam požadavků na systém.

Analýza STPA je ochuzena o hodnocení závažnosti jednotlivých poruchových stavů. V takovémto seznamu poté nejsou vidět nejzávažnější poruchy, kterým by se měli analytici více věnovat. Jediné hodnocení závažnosti dopadů selhání je v rámci odkazů na nebezpečí. Poruchové stavy poté lze například upřednostnit podle nebezpečí s dopadem na ztrátu lidského života.

Dalším rozdílem je odlišnost mezi scénáři a poruchovými cestami ve stromu poruch. V FTA je možné modelovat celou cestu poruchy od příčiny až ke konečné funkci. V takovéto cestě můžeme zohlednit i poruchy hlavních a vedlejších větví sloužících pro zálohování funkcí. Oproti tomu je popis příčiny poruch u scénářů skládajících se z poruch více komponent velmi složitý. V tomto případě je grafické zobrazení vhodnější a srozumitelnější.

Analýza FHA poskytuje přehled všech funkcí, jimiž dané systémy disponují. Zatímco STPA vytváří přehled odpovědností, které jsou ve své podstatě funkcemi systému vztažené k tzv. „*process model*" jež jsou situacemi, kdy po systému vyžadujeme funkci. Zároveň vytváří přehled odpovědností spojených se zpětnými vazbami a poskytuje kontrolu, zda jsou tyto odpovědnosti ošetřeny kontrolujícími prvky. Využitelnost tohoto přehledu by mohla být výhodná pro oddělení konstrukce. Oproti tomu FHA poskytuje přehlednější seznam obecnějších funkcí, využitelný například pro letovou příručku. Nicméně oba seznamy by se dali využít téměř identicky, ale popis funkcí tradiční metodou není natolik podrobný.

7 Využitelnost výstupů z jednotlivých druhů analýz

V této kapitole jsem se pokusil shrnout přínosy jednotlivých analýz s ohledem na využitelnost jejich výstupů při vývoji a následném provozu. Využitelnost jsem stanovil jak pro kvalitativní FHA a STPA tak i pro kvantitativní analýzu FTA. Ke konci kapitoly jsem navrhl řešení pro zvýšení využitelnosti výstupů z analýzy STPA.

7.1 Fault Tree Analysis (FTA)

Výstupy ze stromu poruch lze využít v těchto oblastech:

Odhalení bezpečnostních rizik během vývojové fáze: Pomáhá nalézt kritická místa v návrhu systému, a tím odhalovat bezpečnostní rizika, a to již v raných fázích návrhu. Hlavním přínosem této metodiky je schopnost umožnit konstruktérům vyhodnotit a porovnat celkový vliv různých konstrukčních variant na bezpečnost během počátečního navrhování letadla. Je proto možné včasně upravovat konstrukční návrh, a tím snižovat náklady na pozdější modifikace.

Konstrukční požadavky: Strom poruch lze v období vývoje využít k návrhu požadavků pro výrobce komponentů. Pomocí stromu lze snadno modelovat závislosti funkcí systému a chybových hlášek využitelných pro tvorbu softwaru. Grafické zobrazení je přehledným podkladovým materiálem, který lze snadno překlopit do programovacího jazyka využívajícího podobných logických hradel „AND“ a „OR“

Plánování údržby: Z dat získaných z této analýzy lze predikovat střední doby do poruchy tzv. MTBF, které jsou zásadním faktorem v predikci údržbových či kontrolních činností. U nových letounů je toto pouze odhad, který je nutný během životnosti letounu upravovat o aktuální data z provozu. Při dostatečném množství dat je poté možné i prodlužovat údržbové intervaly, a tím snižovat náklady na provoz. V případě opakovaných poruch je poté možné využít poruchové stromy k nalezení a prověření možných příčin poruch. Výstup lze také použít jako vstup pro údržbovou strategii nazývanou údržba zaměřená na bezporuchovost neboli RCM více viz kapitola 3.2.

Školení: FTA může být velice přínosným grafickým podkladem pro tvorbu vzdělávacích materiálů k pochopení funkcí a závislostí ve složitých systémech. Pomocí stromu poruch je snadné zobrazit zálohování funkcí či příčiny poruch.

Odhalování příčin častých závad: Ve chvíli, kdy se u letounu opětovně objevuje stejná závada bez jasných příčin, je možné využít poruchové stromy k prošetření závislostí v systému.

Řízení kvality u kritických komponent: Využitelnost se nabízí i v odvětví řízení kvality. Pomocí stromu poruch lze nalézt minimální seznam kritických komponentů. Jedná se o komponenty s vysokou pravděpodobností selhání či o komponenty podílející se na funkcích bezprostředně ohrožujících bezpečnost letu. Zvýšení spolehlivosti provozu lze zajistit zvýšením požadavků a dohledu na jejich výrobu, skladování a montáž. Více viz kapitola 3.1.

7.2 Functional Hazard Analysis (FHA)

Výstupy z FHA lze využít v těchto oblastech:

PHA: Stanovení poruchových stavů na úrovni letounu během předběžných vývojových analýz je nedílnou součástí vývoje. Provádí se ve chvíli, kdy není dokončen konstrukční návrh. Výstupem je seznam poruchových stavů, které je nutné prověřit, a odhalení kritických míst, u kterých bude nutné eliminovat či alespoň snížit jejich pravděpodobnost či dopad na bezpečnost letu. Provedení PHA je nutnou podmínkou pro schválení předběžného plánu vývoje.

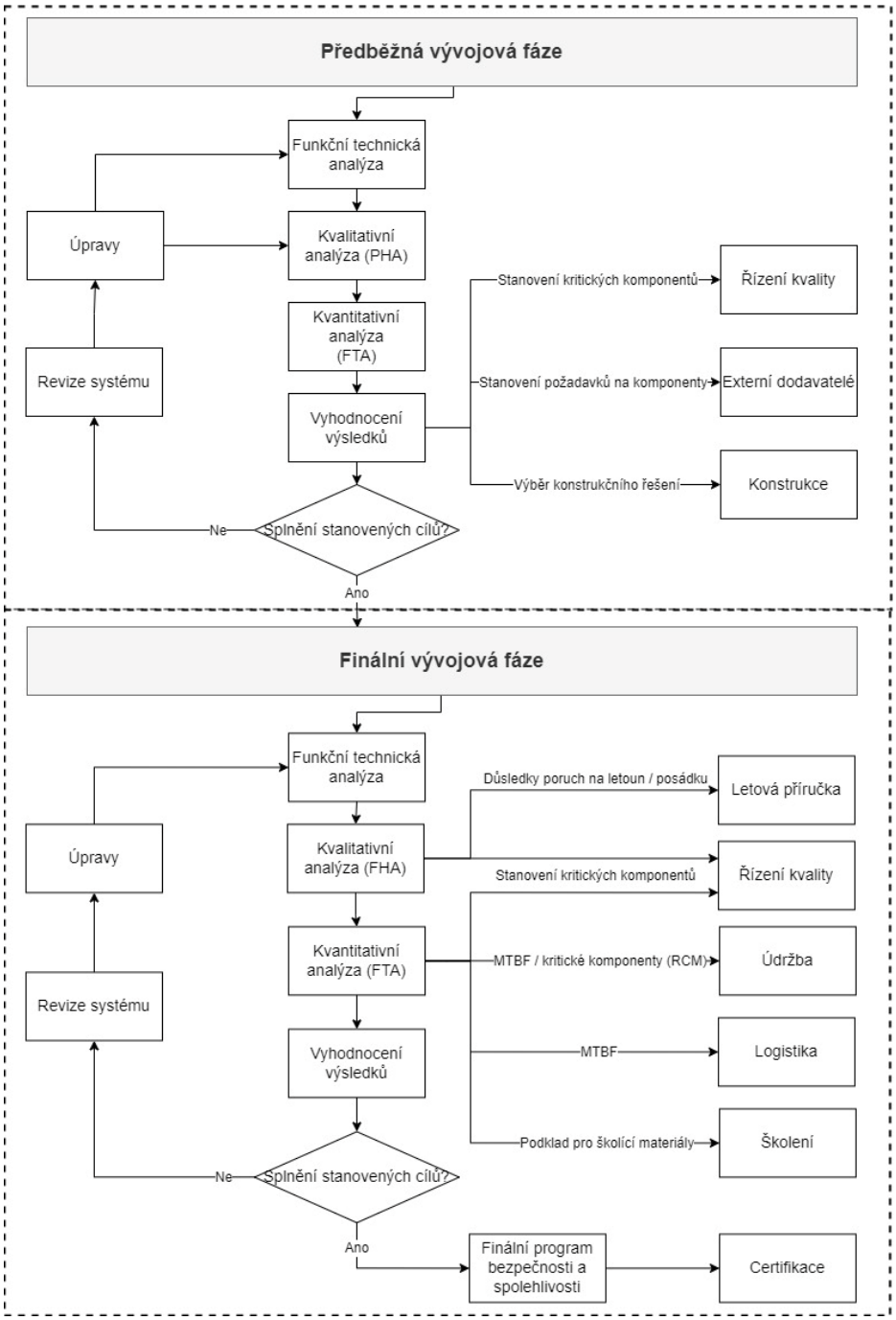
Požadavky na výrobce komponentů: Analýzu lze využít i pro stanovení základních požadavků na funkce a pravděpodobnosti jejich selhání. Výrobce poté musí prokázat vlastními analýzami, že splnil požadované nároky na dodávané komponenty.

Hodnocení a kategorizace bezpečnostních rizik: Součástí analýzy je kompletní přehled funkcí s příslušnými poruchovými stavy. Pravděpodobnost nastání každého stavu je poté ověřena kvantitativními metodami. Součástí výstupu je i ohodnocení závažnosti poruchových stavů, díky kterým je možné upřednostňovat ty, které mají nejvyšší dopad na bezpečnost či spolehlivost letounu.

Letová příručka: Každý poruchový stav obsahuje i popis důsledků na letoun/letovou posádku. Popisy důsledků lze později využít pro tvorbu letové příručky a pro vytváření provozních postupů. V porovnání s metodou STPA jsou u FHA důsledky popisovány mnohem podrobněji, proto je jejich využitelnost větší.

Certifikace: Tvoří základní certifikační dokument, ve kterém spojuje jednotlivé analýzy z SSA (systémová úroveň) do komplexnější letounové úrovně. Součástí dodávaných komponentů bývají dokončené analýzy, které musí analytik spojit právě do tohoto dokumentu.

Schématické zobrazení využití výstupů analýz FHA a FTA v jednotlivých fázích vývoje je zobrazeno na obrázku 22.



Obrázek 22 Schéma využitelnosti výstupů tradičních analýz

7.3 System Theoretic Process Analysis (STPA)

Výstupy z STPA lze využít v těchto oblastech:

Kvalitativní analýza: STPA je velmi komplexní metodou k nalezení poruchových stavů letounu. Její využití by v budoucnu mohlo nahradit dnes využívanou FHA analýzu. A to z důvodu podrobnějšího popisu poruchových stavů a odhalení skrytých rizik, které nemusí být zpočátku zřejmé. S rostoucí složitostí systémů a implementací elektroniky do kritických funkcí, tradiční metody k popisu a nalezení všech příčin poruch nestačí.

Požadavky na konstrukci: STPA popisuje velmi detailně požadavky na komponenty/systémy. Konkrétně se jedná o požadavky konstrukční, provozní, ergonomické, interakci stroj-posádka. Seznam omezení může sloužit jako doplňující seznam požadavků, které by měly být výrobcem ověřeny. Mohl by doplnit analýzu FHA obsahující kromě seznamu funkcí systému i o cílové pravděpodobnosti selhání funkcí/komponentů. Požadavky mohou být doplněny například i o poruchové stromy.

Seznam odpovědností: součástí analýzy je přehled odpovědností jednotlivých systémů spojených s druhem zpětné vazby. Využitelnost toho přehledu by mohla být přínosná pro oddělení konstrukce pro ověření bezpečnosti návrhu či letové příručky pro tvorbu letových postupů.

7.4 Návrh zvýšení využitelnosti STPA:

Pro větší využitelnost výstupu analýzy STPA, aby odhalila stejné poruchové stavy jako tradiční metody, je nutné popisovat systém velmi detailně a do hloubky. Schéma musí obsahovat veškeré komponenty a detailní popis jejich vzájemných interakcí. Každé zjednodušení schématu nebo hloubky analýzy má za důsledek ztrátu potřebných informací a neodhalení všech scénářů poruch. Příklad jsme mohli vidět u poruchového stavu č. 2.

Vhodným způsobem, jak zvýšit využitelnost výstupu analýzy STPA, by bylo rozdělení omezení neboli „*constraints*“. Rozdělení omezení by mělo za důsledek její větší využitelnost a předání požadavků na systém jednotlivým oddělením. Omezení by se daly rozdělit na požadavky pro: konstrukci, údržbu, provozní postupy, ergonomii a rozhraní člověk-stroj. Příklad, jak by takové rozdělení mohlo vypadat, je uveden v tabulce č. 16.

Tabulka 16 Návrh zvýšení využitelnosti rozšířením „constraints“ [12]

UCA	Scenario	Constraints
UCA-83: Nepřečerpání paliva mezi nádržemi za letu [H-1, H-2, H-3, H-5, H-7]	Sc-83.6: Tlak paliva nepřetlačí zpětné ventily palivového potrubí větve přečerpávání;	Sc-83.6.1 C: **KONSTRUKCE** Zpětné ventily se vlivem provozního tlaku paliva otevřou;
		Sc-83.6.2 C: **ÚDRŽBA** Zpětné palivové ventily jsou seřízeny, aby jimi palivo o provozním tlaku proteklo do trupových nádrží;
		Sc-83.6.3 C: **ROZHRANÍ ČLOVĚK-STROJ** Posádka vyhodnotí poruchu přečerpávání indikací na MFD;
		Sc-83.6.3 C: **PROVOZNÍ POSTUPY** Posádka přestaví přepínač přečerpávání na obtokovou větev[5];

Omezení by neměla přímo řešit danou problematiku, ale spíše tvořit kontrolní seznam požadavků, která jednotlivá oddělení ověří. Tímto se sníží počet možných scénářů, které by mohly být odděleními opomenuty.

[5] Tento požadavek je smyšlený pro názornou ukázku. Palivový systém letounu L-39NG takovouto funkcí nedisponuje.

8 Závěr

Moderní metoda STPA je oproti tradičním metodám mnohem komplexnější. Umožňuje popis a analýzu dnes konstruovaných systémů. Pro analýzu komplexních systémů, posuzující složité systémy v interakci s lidským faktorem, jakým je například autopilot, systém „*fly-by-wire*“ či jiné automatizované procesy tradiční metody, již nestačí. S budoucím vývojem letadel lze jen očekávat větší implementaci takto automatizovaných procesů. Bezpilotní letouny jsou příkladem komplexních systémů, které dokážou situace nejen vyhodnocovat, ale i řešit bez potřeby lidského zásahu. V těchto případech je využití metody STPA potřebné a k zvyšování či udržení stávající bezpečnosti doslova nevyhnutelné.

Z pohledu firmy Aero Vodochody by zavedení STPA k ověřování bezpečnosti a spolehlivosti letadel nebylo vhodnou metodou, a to z několika důvodů. V současné době, kdy STPA nelze využít k certifikaci, stále vzniká nárok na použití tradičních metod. Pro analýzu systémů, které nejsou natolik komplexní, jako je například palivový systém letounu L-39NG, který nedisponuje mnoha automatizovanými procesy, lze stále využít tradiční metody. V případě systémů s minimálními interakcemi, jejichž rizika jsou snadno identifikovatelná, mohou být jednodušší metody analýzy bezpečnosti dostačující. Na druhou stranu komplexní systémy, jako je například autopilot, zbraňové systémy, integrovaný systém bojového výcviku, STPA může být prohloubením analýzy bezpečnosti a přínosem při identifikaci skrytých rizik a jejich hlubších příčin. U nekomplexních systémů, které je možné popsat pomocí tradičních metod, není přínos STPA znatelný a její použití může působit nepřiměřeně. Analýza STPA detailním rozborem sice objeví minimálně stejné poruchové stavy jako tradiční přístup, ale ty, které objeví navíc nejsou pro bezpečnost zásadní. Jejím přínosem je detailnější popsání a rozdělení poruchových stavů, avšak přidaná hodnota se mi jeví nedostatečná. Tvorba analýzy je časově náročnější a při současné potřebě vypracování FHA a FTA analýz by byl celkový proces posuzování bezpečnosti a spolehlivosti neefektivní. STPA analýza oproti tradičnímu přístupu nepřináší vhodné výstupy, které by byly využitelné v jiných odděleních firmy. Analýzy FHA a FTA poskytují potřebné vstupy i jiným oddělením, které jsou nutné například k predikci údržby, zajišťování dostatku dílů z pohledu logistického oddělení či poskytnutí přehledu poruch oddělení letové příručky tvořící provozní postupy. Analýza STPA by se ale i přes tyto nevýhody mohla využívat například jako doplňující k tradičním metodám pro systémy využívající automatizované procesy. Dále by bylo její využití vhodné pro nově vyvíjené komponenty, u kterých nejsou jasně stanoveny požadavky ani konstrukční návrh. Zároveň by bylo možné analýzu využít k posouzení příčin selhání v rozhraní posádka - stroj. V současné chvíli by zavedení metody STPA na některý z uvedených případů mohlo být pro firmu, i přes zmíněné

nevýhody přínosné. Konkrétně, pokud bude v budoucnu firma Aero Vodochody Aerospace uvažovat o vývoji a implementaci například autopilota, systému „*fly-by-wire*“ či jiných automatizovaných procesů. V tomto případě by se v dnešní době měli zabývat i moderní metodou STPA, protože její využitelnost bude mít v takovéto oblasti obrovský přínos. Zároveň zavedení nové metody již v době, kdy její využitelnost není stěžejní, by analytikům umožnilo se s metodou důkladně seznámit a získat potřebné zkušenosti. Později by metodu mohli začít využívat v případech, kdy budou do letounů implementovány komplexní systémy.

STPA metoda je natolik komplexní, že je schopna posuzovat systém jako celek. Zahrnuje jak materiálové inženýrství, mechanickou konstrukci systémů, rozhraní s posádkou, popis automatizovaných procesů usnadňující ovládání systému, ergonomii a v neposlední řadě mezisystémové interakce, které by při využití tradičních metod nemusely být zřejmé. Tyto interakce mohou v automatizovaných procesech způsobit nežádoucí situace, které by mohly způsobit incident či leteckou havárii i bez nastání jakékoli poruchy. Pro civilní letectví, kde je brán velký důraz na bezpečnost a spolehlivost, je STPA metodou, která v budoucnu pravděpodobně nahradí stávající metody. Již v dnešní době je metoda STPA využívána společnostmi jako jsou *Boeing*, *Embraer* nebo například *Lockheed Martin*. Účel letadel ve vojenském sektoru a nároky na jejich bezpečnost a spolehlivost jsou značně odlišné od civilního letectví. Pro letouny spadající do kategorie podzvukových letounů zaměřených na výcvik, kde jsou požadavky kladeny na jiné cíle, využití metody STPA z mého pohledu zatím smysl nemá.

V návaznosti na mou bakalářskou práci by bylo možné zhodnotit rozdíly tradičních a moderních metod při posuzování komplexních systémů. Zároveň by bylo vhodné vytvořit postup pro využití metody STPA pro vývoj a certifikaci s doplněním kvantitativní části například v podobě Reliability block diagram (RBD), a následně stanovit postup využití tradičních metod pro nekomplexní systémy a STPA v kombinaci s RBD pro komplexní systémy

9 Seznam použité literatury

[1] FAA. *System Safety Analysis and Assessment for Part 23 Airplanes: AC 23.1309-1E*. 2011, 56 s. Dostupné také z: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_23_1309-1E.pdf

[2] FAA. *System Design and Analysis: 25.1309-1A*. 1988, 19 s. Dostupné také z: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25_1309-1A.pdf

[3] VESELY, W.E., F.F. GOLDBERG, N. H. ROBERTS a D. F. HAASL. *Fault Tree Handbook (NUREG-0492): U.S. Nuclear Regulatory Commission*. Washington, 1981. Dostupné také z: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

[4] *Analýzy spolehlivosti a bezpečnosti v praxi, (aneb, Jak přesvědčit zákazníka, že požadavky na spolehlivost a bezpečnost výrobku budou splněny): materiály z 35. setkání odborné skupiny pro spolehlivost : Brno, červen 2009*. Brno: Česká společnost pro jakost, 2009. ISBN 978-80-02-02156-8.

[5] *Měření, diagnostika, spolehlivost palubních soustav letadel: sborník příspěvků z 20. mezinárodní vědecké konference*. První. Brno: Univerzita obrany, 2022. ISBN 978-80-7582-472-1.

[6] NOVÁK, Ing. JOSEF. *METODY ANALÝZY SPOLEHLIVOSTNÍCH DAT Z PROVOZU A ZKOUŠEK LETADEL*. BRNO, 2011. TÉZE DOKTORSKÉ PRÁCE. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce Doc. Ing. KAREL TŘETINA, CSc.

[7] Letouny: L-39NG. In: *AERO Vodochody AEROSPACE* [online]. [cit. 2023-03-29]. Dostupné z: https://www.aero.cz/cz/letouny/programy/l-39ng/

[8] EUROPEAN DEFENCE AGENCY. *European Military Airworthiness Certification Criteria (EMACC)*. 2018, 662 s. 3.0. Dostupné také z: https://eda.europa.eu/docs/default-source/documents/emacc-hdbk-edition-3-0-(1-feb-2018)---endorsed-for-release.pdf

[9] *MIL-STD-882E: SYSTEM SAFETY*. DEPARTMENT OF DEFENSE STANDARD PRACTICE, 2012.

[10] *SAE ARP 4761: Guidelines for Development of Civil Aircraft and Systems*. United States: SAE International, 1996.

[11] EUROPEAN DEFENCE AGENCY. *EMAR 21: CERTIFICATION OF MILITARY AIRCRAFT AND RELATED PRODUCTS, PARTS AND APPLIANCES, AND DESIGN AND PRODUCTION ORGANISATIONS*. 2.0. Brusel, 2021. Dostupné také z: https://eda.europa.eu/docs/default-source/documents/emar-21-edition-2-0-(approved)-30-march-2021.pdf

[12] KUPČÍK, Václav. *Hodnocení bezpečnosti modernizace systémů letounu L-159 ALCA*. Praha, 2022. Diplomová práce. ČVUT. Vedoucí práce Doc. Ing. Andrej Lališ, Ph.D.

[13] *FLIGHT MANUAL L-39NG AIRCRAFT: ATM 1T-L39NG-1*. AERO Vodochody AEROSPACE a.s., 2022.

[14] ZHE, Dong. Research on the Identification Method of the Critical&Important Parts and its characteristics of Civil Aircraft Systems. In: *MEMAT 2022*. Guilin, China, 2022, s. 1-4. ISBN 978-1-5090-0249-8.

[15] AFEFY, Islam a M. HELAL. APPLICATION OF FMEA-FTA IN RELIABILITY-CENTERED MAINTENANCE PLANNING. *The International Conference on Applied Mechanics and Mechanical Engineering*. 2012, **15**, 1-11. Dostupné z: doi:10.21608/amme.2012.37083

[16] G. LEVESON, NANCY a JOHN P. THOMAS. *STPA handbook*. March, 2018. Dostupné také z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Handbook. MIT.

[17] LEVESON, Nancy. *Engineering a Safer World: Systems Thinking Applied to Safety* [online]. MIT Press, 2012 [cit. 2022-10-21].

[18] Aero L-39 Albatros Blueprint. In: *Blueprints: Blueprints for 3D modeling* [online]. [cit. 2023-08-06]. Dostupné z: https://drawingdatabase.com/aero-l-39-albatros/

[19] *Aero L-159 Alca Blueprint* [online]. In: . [cit. 2023-08-06]. Dostupné z: https://drawingdatabase.com/aero-l-159-alca/