ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Automatizace spolehlivostní analýzy ve vývoji vojenských letounů

Automation of Reliability Analysis in Military Aircraft Development

Bakalárska práca

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

Vedúci práce: doc. Ing. Andrej Lališ, Ph.D.
Ing. Karel Mündel

Tomáš Pivarči

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):

Tomáš Pivarči

Studijní program (obor/specializace) studenta:

bakalářský – TUL – Technologie údržby letadel

Název tématu (česky): **Automatizace spolehlivostní analýzy ve vývoji vojenských letounů**

Název tématu (anglicky): Automation of Reliability Analysis in Military Aircraft Development

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je stanovení možností a postupu pro automatizované spolehlivostní analýzy v rámci vývoje a výroby vojenských letounů s pomocí metod FTA a FHA.
- Analyzujte metody hodnocení spolehlivosti FTA a FHA v letectví.
- Analyzujte dostupné řešení pro automatizaci spolehlivostních analýz.
- Vyberte a popište konkrétní systém vojenského letounu.
- Proveďte analýzu spolehlivosti s pomocí vybraného nástroje pro automatizaci spolehlivostních analýz.
- Dosažené výsledky ověřte a vyhodnoťte.

ČVUT FD

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.
Caset, J.-F. et al. Failure analysis and products in a model-based environment. IEEE Aerospace Conference, 2018.

Vedoucí bakalářské práce: **doc. Ing. Andrej Liš, Ph.D.**
Ing. Karel Mündel

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.

Tomáš Pivarči
jméno a podpis studenta

V Praze dne..... 7. října 2022

Abstrakt

V oblasti spoľahlivostných analýz je pomerne veľa limitácií. Medzi najvýznamnejšie patrí veľa času potrebného na ich vypracovanie a chýbajúca automatizácia spoľahlivostných analýz. Pri analýze Fault tree analysis (FTA) to znamená vytvoriť vlastný strom porúch pre zlyhanie každej funkcie. Po vytvorení stromov porúch nasleduje vyplnenie pravdepodobností elementárnych komponentov. Tento proces zaberie veľké množstvo času osobám vykonávajúcim analýzu. Riešením, ako tento čas skrátiť, je automatizácia priebežných procesov analýzy. Bola overovaná možnosť využitia automatizovanej metódy pomocou FTA/FMEA toolu pri tvorbe FTA analýz a automatizácie vkladania technickej dokumentácie do FTA/FMEA toolu. Pre konkrétnu modelovú situáciu boli použité podkladové údaje vojenského cvičného lietadla L-39 NG, ktoré boli poskytnuté od firmy Aero Vodochody AEROSPACE a.s. Na prácu bol využitý systém pozdĺžneho riadenia, pri ktorom sa rozmýšľa o zaradení jednotky PCA (Pitch Control Actuator), ktorá znižuje sily v riadení pilota. Podľa získaných podkladov bola vytvorená zjednodušená schéma pozdĺžneho riadenia so zapojením jednotky PCA. Porovnaním dostupných softvérov sa zistilo, že optimálnym softvérovým riešením pre túto prácu bude využitie FTA/FMEA toolu. Ďalej môžeme potvrdiť na vzorke 27 stromov porúch, že tento softvér generuje stromy porúch totožne ako pri manuálnom spracovaní FTA analýzy. Postupy s využitím modelu v jazyku UML (Unified Modeling Language) a následnom exporte dát pomocou jazyka OWL (Ontology Web Language) do FTA/FMEA toolu dávajú reálnu možnosť vytvorenia plne automatizovaného softvéru na vytváranie FTA analýz.

Kľúčové slová: automatizácia vkladania dát, fault tree analysis, L-39 NG, spoľahlivostná analýza

Abstract

There are quite a lot of limitations in area of reliability analysis. Among the most important are the long time needed to prepare them and the lack of automation of reliability analyses. For Fault tree analysis (FTA), this means creating a specific fault tree for the failure of each function. The creation of the fault trees is followed by filling the probabilities of the elementary components. This process takes a large amount of the time of the persons completing the analysis. The solution to reduce this time is to automate the ongoing analysis processes. The possibility of using an automated method using the FTA/FMEA tool in the creation of FTA analyses and automating the input of technical documentation into the FTA/FMEA tool was verified. For a specific model situation, the important data of a military L-39 NG trainer aircraft provided by Aero Vodochody AEROSPACE a.s. were used. The longitudinal control system was used for the work, for which the inclusion of a PCA (Pitch Control Actuator) unit was considered, which reduces the forces in the pilot's control. According to the obtained data, a simplified scheme of longitudinal control with the inclusion of the PCA unit was created. By comparing the available software, it was found that the optimal software solution for this work would be the use of FTA/FMEA tool. We can further confirm on a sample of 27 fault trees that this software generates fault trees identically to the manual processing of the FTA analysis. Procedures using the model in UML (Unified Modeling Language) language and then exporting the data using OWL (Ontology Web Language) language to FTA/FMEA tool give a realistic possibility of creating fully automated software for creating FTA analyses.

Keywords: data entry automation, fault tree analysis, L-39 NG, reliability analysis

Poďakovanie

Ďakujem školiteľom mojej bakalárskej práce doc. Ing. Andrejovi Lališovi Ph.D. a Ing. Karlovi Mündelovi za odborné vedenie, metodickú pomoc a cenné rady, ktoré mi poskytli pri jej vypracovávaní. Moje poďakovanie patrí Mgr. Milanovi Pšeničkovi z oddelenia analýz firmy Aero Vodochody AEROSPACE a.s. za pomoc pri vytváraní analýz a technické podklady, použité pri vytváraní bakalárskej práce. Zároveň ďakujem pracovníkom Ústavu letecké dopravy, Fakulty dopravní, České vysoké učení technické v Praze za možnosť vypracovať túto bakalársku prácu. V neposlednom rade patrí poďakovanie mojej rodine za podporu a pomoc počas celého štúdia.

Čestné prehlásenie

Prehlasujem, že bakalársku prácu s názvom Automatizace spolehlivostní analýzy ve vývoji vojenských letounů som vypracoval samostatne a uviedol k tomu úplný zoznam citácií použitých prameňov, ktoré uvádzam v zozname priloženom k bakalárskej práci.

Nemám závažný dôvod proti použitiu tohoto školského diela v zmysle §60 Zákona č.121/2000 Sb., o autorskom práve a právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon).

V Prahe dňa 7. augusta 2023 ……...

Podpis

Obsah

Zoznam obrázkov

Zoznam skratiek

AVA	Aero Vodochody AEROSPACE a.s.
ČVUT	České vysoké učení technické v Praze
EASA	European Union Aviation Safety Agency
ECU	Electrical Control Unit
ETA	Event Tree Analysis
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FDAU	Flight Data Acquisition Unit
FHA	Functional Hazard Assessment
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HOTAS	Hands On Throttle And Stick
LH	Letová Hodina
MAWA	Military Airworthiness Authorities
MBSE	Model-Based System Engineering
MFD	Multi Function Display
MO	Ministerstvo obrany
MTBF	Mean Time Between Failure
NG	New Generation
ODVL	Odbor dohľadu nad vojenským letectvom
OWL	Ontology Web Language
PCA	Pitch Control Actuator
PHA	Preliminary Hazard Analysis
RAC	Risk Assessment Coefficient
RCA	Roll Control Actuator
TP	Technické Podmienky
TZ	Technické Zadania
UML	Unified Modeling Language

Úvod

Pri vývoji lietadiel je veľmi dôležitý čas. Každý výrobca lietadiel, či už vojenských alebo civilných, sa vždy snaží o čo najefektívnejší a ak sa dá aj najrýchlejší postup pri vývoji nového lietadla. Jedným zo spôsobov, ako je možné tento čas skrátiť a vývoj zefektívniť, je automatizácia postupov počas vývoja. V súčasnosti sa využitie automatizácie pri vytváraní analýz javí ako nevyhnutný krok. Pri vytváraní analýz spoľahlivosti sa naskytuje mnoho postupov, ktoré by bolo možné automatizovať a vďaka čomu by bolo možné znížiť potrebný čas. Pri dnešných technológiách je naozaj nepredstaviteľné, aby vypracovávanie analýz prebiehalo úplne manuálne a preto sa na trhu objavujú prostriedky aspoň s čiastočnou automatizáciou. Do budúcna je cieľom vytvorenie a využitie plne automatizovaného softvéru, ktorý by pomohol zefektívniť procesy vytvárania spoľahlivostných analýz.

Cieľom práce je stanovenie možností a postupov pre automatizované spoľahlivostné analýzy v rámci vývoja a výroby vojenských lietadiel s pomocou metód FTA a FHA. Základným krokom je porovnanie a výber poloautomatizovaného softvéru do ktorého by bolo možné do budúcna zaradiť automatické vkladanie dát a technickej dokumentácie, vďaka čomu by vznikol plne automatizovaný softvér na vytváranie spoľahlivostných analýz. Následnou úlohou je navrhnutie inovatívneho riešenia postupov a možností zaradenia plne automatizovaného softvéru do firmy Aero Vodochody Aerospace a.s. Softvérové rozšírenie na automatizáciu vkladania technickej dokumentácie má obrovský význam a zaradenie tejto inovácie bude veľkým prínosom pre každú firmu, ktorá sa rozhodne pre jeho zaradenie.

Táto bakalárska práca vznikla v spolupráci s českým výrobcom vojenských lietadiel Aero Vodochody Aerospace a.s (AVA). AVA je jednou z firiem, ktoré nad zaradením automatizovaných softvérov rozmýšľajú a zároveň si uvedomujú prínosy zaradenia automatizácie do postupov pri vytváraní spoľahlivostných analýz.

1. Súčasný stav

V tejto kapitole sa zaoberám rozborom spoľahlivosti a bezpečnosti počas vývoja a prevádzky lietadiel, stručným popisom firmy Aero Vodochody, popisom vývoja moderného cvičného stíhacieho lietadla L-39 NG a presným popisom pozdĺžneho riadenia na lietadle L-39 NG so stanovením komponentov systému.

1.1 Vývoj lietadiel

Vývoj lietadiel je zložitý a vysoko regulovaný proces, ktorý zahŕňa niekoľko fáz, od počiatočného návrhu až po konečnú certifikáciu, začiatok výroby a následné nasadenie do prevádzky. Tu sú niektoré kroky, z ktorých pozostáva vývoj lietadiel:

Koncepčný návrh: Počiatočná fáza vývoja lietadla zahŕňa koncepčný návrh, kde dizajnéri a inžinieri vyvinú základnú predstavu o tom, ako bude lietadlo vyzerať a ako bude fungovať.

Predbežný návrh: Po dokončení koncepčného návrhu sa návrh lietadla presunie do fázy predbežného návrhu, kde sa vykonajú podrobnejšie konštrukčné práce na zdokonalenie tvaru, veľkosti a výkonnostných charakteristík lietadla.

Podrobný návrh: Fáza podrobného návrhu zahŕňa vytvorenie podrobných technických výkresov a špecifikácií lietadla. Táto fáza zahŕňa aj výber materiálov a komponentov, ktoré budú použité pri konštrukcii lietadla.

Testovanie a certifikácia: Po dokončení podrobného návrhu musí lietadlo prejsť rozsiahlym testovaním, aby sa zaistilo, že spĺňa prísne bezpečnostné a výkonnostné normy. To zahŕňa pozemné testovanie, letové testovanie a certifikáciu regulačnými orgánmi, ako je Federálny úrad pre letectvo (FAA) alebo Agentúra Európskej únie pre bezpečnosť letectva (EASA). V prípade vojenského sektoru a teda firmy Aero Vodochody je certifikačný orgán ODVL MO (Odbor dohľadu nad vojenským letectvom Ministerstva Obrany), ktorý je súčasťou Military Airworthiness Authorities (MAWA).

Výroba: Keď je dizajn lietadla certifikovaný, môže byť vyrobený v súlade so schváleným dizajnom. Výroba lietadiel zahŕňa zložité procesy a použitie pokročilých materiálov a technológií.

1.2 Bezpečnosť a spoľahlivosť v letectve

V dnešnej dobe je veľmi dôležité, aby väčšina vyrobených systémov alebo komponentov boli vytvorené s vysokou mierou spoľahlivosti. V prípade, že sa jedná o letectvo sú tieto požiadavky mnohonásobne vyššie a musí sa počítať s vysokou mierou bezpečnosti. Sú aj niektoré systémy alebo komponenty, ktoré majú nižšiu spoľahlivosť ale väčšinou bývajú viac-násobne zabezpečené, teda v prípade zlyhania sa spolieha na záložný komponent. Letecká doprava má oproti iným druhom dopravy mnohonásobne vyššie štandardy bezpečnosti a spoľahlivosti, vďaka čomu je právom vyhlásená za najbezpečnejší druh dopravy na svete.

Požiadavky na spoľahlivosť a bezpečnosť sa stávajú jednou z najdôležitejších súčastí technických požiadaviek kladených na letecké a celkovo všetky technické systémy. Je nepredstaviteľné, že by vývoj nového moderného systému nespĺňal vysoko kladené požiadavky na spoľahlivosť a bezpečnosť. Každý výrobca počas vývoja alebo počas výroby musí tieto požiadavky spĺňať. Bežnou praxou pri vývoji je, že musí byť splnená požadovaná úroveň bezpečnosti a spoľahlivosti ešte pred tým, ako začne výroba lietadla alebo jeho prototypu. Táto požiadavka vyplýva zo skúseností, že každá nevyhnutná zmena v konštrukcii systému sa behom predvýrobnej etapy realizuje podstatne jednoduchšie a s oveľa menšími nákladmi ako v neskorších etapách.

Cieľom týchto analýz je včasné objavenie rizík a poruchových stavov ktoré by mohli výrazne ovplyvniť bezpečnosť systému. Následne ich je nutné odstrániť alebo zmierniť, aby tieto riziká vyhovovali stanoveným štandardom. Analýza bezpečnosti a spoľahlivosti sa skladá z nasledujúcich činností: získavanie, skúmanie a usporiadanie informácii o danom systéme. Analýza musí byť vytvorená podľa presne stanovených postupov. [1]

1.3 Bezpečnostné a spoľahlivostné analýzy

Pri vytváraní analýz spoľahlivosti a bezpečnosti sa využívajú najčastejšie tieto metódy:

a) PHA - Preliminary Hazard Analysis (Induktívny postup)
b) FMEA - Failure Mode and Effect Analysis (Induktívny postup)
c) FMECA - Failure Mode, Effect and Criticality Analysis (Induktívny postup)
d) FTA - Fault Tree Analysis (Deduktívny postup)
e) ETA - Event Tree Analysis (Induktívny postup)
f) RBD - Reliability Block Diagram (Deduktívny postup)

V praxi sú využívané dva typy metodologických postupov pri vytváraní analýz spoľahlivosti a bezpečnosti, jedná sa o induktívny prístup a deduktívny prístup.

1.3.1 Induktívny prístup pri vykonávaní analýz

Tento typ prístupu vykonávania analýzy je založený na princípe postupu od základných, teda elementárnych problémov až k tým obecnejším. Prístup teda začína u zlyhaní základných komponentov systému a dostáva sa až ku koncovým zlyhaniam celého systému. Ako môže strata niektorej riadiacej funkcie lietadla ovplyvniť celý systém lietadla. [1]

FMEA

Účelom analýzy poruchových stavov a dôsledkov porúch (FMEA) je stanoviť, ako by mohli systémy alebo procesy zlyhať pri vykonávaní svojej funkcie, aby mohli byť identifikované všetky potrebné nápravné opatrenia. FMEA poskytuje systematickú metódu pre identifikáciu poruchových stavov spolu s ich dôsledkami pre systém alebo určitý proces, v oboch prípadoch lokálne ale aj globálne. Môže sa do nej zahrnúť identifikácia príčin poruchových stavov. Poruchovým stavom môže byť priradená priorita s cieľom podporiť rozhodnutie o nápravných opatreniach. FMEA sa používa v procese certifikácie alebo pri preukazovaní spoľahlivosti. U metódy FMEA sa využíva induktívny postup. [2]

FMECA

Pokiaľ sa do klasifikácie kritičnosti zahrňuje prinajmenšom kritičnosť následkov a často i iné ukazovatele významnosti, je táto analýza známa ako analýza porúch, dôsledkov a kritickosti porúch (FMECA). Jedná sa o rozšírenie metódy FMEA. Oproti analýze FMEA slúži táto analýza k stanoveniu kritičnosti dôsledkov daných poruchových stavov. Následne sa zoradia poruchové stavy podľa kritičnosti ich dôsledkov. Táto analýza by sa mala začať už v koncepčnej fáze pri návrhu dizajnu, keď sa požiadavky na systém a výkonové parametre ešte len vyvíjajú. Výsledný dizajn by mal by odrážať a zahŕňať výsledky a odporúčania analýzy. [2]

ETA

Analýza využíva induktívny postup, v ktorom postupujeme od základnej poruchy až po jej následky. ETA sa bežne používa v leteckom priemysle. Vykonáva sa s cieľom určiť dôsledky jednej poruchy pre celý systém. Využíva podobnú logiku a výpočty ako FTA, ale u ETA analýzy sa používa iný postup pri jej vypracovávaní. Samotný strom v ETA je vizuálnou reprezentáciou jednotlivých porúch s dopadom tejto poruchy na iné udalosti alebo na celý systém.

Pravdepodobnosť každého výsledku sa hodnotí na základe dostupných údajov a názoru odborníkov. Dôsledky sa hodnotia na základe ich závažnosti a dopadu na systém. [3]

PHA

Predbežná analýza nebezpečenstva (PHA) je metóda na hodnotenie potenciálneho nebezpečenstva, ktoré predstavuje systém pre personál alebo iných ľudí. Cieľom PHA je identifikovať potenciálne nebezpečenstvá, ktoré môžu vzniknúť v systéme a určiť závažnosť alebo kritičnosť potenciálnych nehôd či incidentov, ktoré by mohli vzniknúť. Analýza PHA by sa mala vykonať čo najskôr, ešte vo fáze vývoja systému. Toto by malo byť umožnené vďaka skorému vývoju konštrukčných bezpečnostných požiadaviek, čím sa ušetria neskoršie konštrukčné zmeny, ktoré by boli mnohonásobne drahšie. Prvým krokom v PHA je identifikácia potenciálne nebezpečných prvkov alebo komponentov v rámci celého systému. Tento proces často vychádza z technických skúseností a používaním mnohých kontrolných zoznamov, ktoré už boli vypracované. Druhým krokom v PHA je identifikácia tých udalostí, ktoré by mohli z nebezpečenstiev prejsť k potenciálnym nehodám. Potom sa posudzuje závažnosť týchto potenciálnych nehôd a či bude potrebné prijať preventívne opatrenia. [4]

1.3.2 Deduktívny prístup pri vykonávaní analýz

Je presným opakom induktívneho prístupu. Začíname z druhej strany, teda najprv analyzujeme zlyhania celkového systému a postupujeme analýzou jeho príčin a ako sa na tomto zlyhaní podieľali jednotlivé elementárne komponenty. Pre príklad, ak spadne lietadlo, aké komponenty museli zlyhať, aby k pádu došlo. [1]

FTA

Analýza FTA (Fault tree analysis) je analytická metóda využívaná pre posúdenie možných poruchových stavov zložitejších systémov. Je založená na vrcholovej udalosti, kde sa následne identifikujú možné poruchy vedúce k tejto vrcholovej udalosti. Cieľom tejto analýzy je nájdenie všetkých poruchových stavov, ktoré môžu viesť k vrcholovej udalosti a následne využitie týchto informácii pre vylepšenie systému a zníženie pravdepodobnosti výskytu poruchy v danom systéme. Jednotlivým elementárnym poruchovým stavom sa priradí pravdepodobnosť a následne sa dopočíta pravdepodobnosť poruchy vrcholovej funkcie. Podľa postupu vypracovávania môžeme vidieť že sa jedná o deduktívny postup. [5]

RBD

Blokový diagram spoľahlivosti sa využíva pri analýze zložitých systémov, kde je systém rozdelený do funkčných blokov. Tie sú navzájom prepojené šípkami, ktoré znázorňujú funkčnú cestu. RBD sa vytvára ako skupina blokov zapojených paralelne alebo do série. V prípade paralelného zapojenia môže zlyhať jeden z funkčných blokov a aj napriek tomu bude systém fungovať. Na rozdiel od sériového zapojenia, kde v prípade poruchy jedného bloku zlyhá celý systém. Každý blok v tomto diagrame vyjadruje komponent s určitou pravdepodobnosťou zlyhania. Pri výpočte RBD sa počíta s pravdepodobnosťami zlyhaní daných komponentov zapojených v diagrame. [6]

1.4 Aero Vodochody (AVA)

Spoločnosť Aero Vodochody celým názvom AERO Vodochody AEROSPACE a.s. sa v súčasnej dobe zameriava na výrobu a vývoj vojenských a civilných lietadiel. Momentálne sa zaoberá aj kooperáciou s celosvetovými leteckými výrobcami ako napríklad Airbus, Embraer alebo Leonardo. V súčasnosti vo firme pracuje okolo 1600 zamestnancov. [7]

História spoločnosti siaha až do roku 1919, kedy bolo v spoločnosti vytvorené prvé lietadlo, ktoré odštartovalo éru výroby lietadiel vo vtedajšom Československu. Do dnešného dňa sa v AVA vyrobilo približne 12 tisíc lietadiel. Medzi tie najznámejšie môžeme zaradiť vojenské lietadla mig-15, mig-19, no najmä, čo sa týka výroby cvičných lietadiel navrhnutých a vyrobených priamo vo firme Aero Vodochody, L-29 Delfín, L-39 Albatros a L-159 Alca, ktorých bolo spolu vyrobených okolo 3000 kusov. Lietadlo L-39 Albatros (Obrázok 1) je jedno z najúspešnejších cvičných lietadiel na svete a dokonca najrozšírenejšie, o čom svedčí aj fakt, že Albatros bol využívaný vo viac ako 35 krajinách svete a stále vo veľa z nich ešte lieta. Dokonca bol medzinárodne využívaný aj ako akrobatické lietadlo v akrobatických skupinách, napríklad v slovenskej akrobatickej skupine Biele Albatrosy a celosvetovo známej skupine BREITLING JET TEAM. Aero Vodochody poskytuje okrem leteckej výroby aj celý rad služieb na podporu svojich produktov. Tieto služby zahŕňajú školenia, údržbu, opravy a generálne opravy lietadiel a komponentov lietadiel. [7]

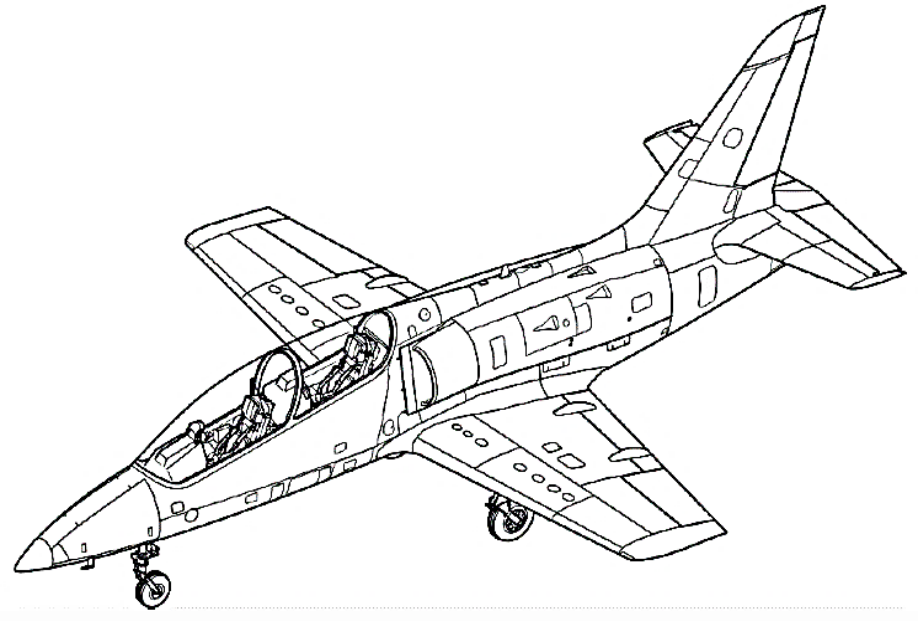
Obrázok 1 Čelný pohľad na L-39 Albatros [21]

Momentálne sa pracuje na sériovej výrobe najnovšieho lietadla L-39 NG, z ktorého je už jeden model výrobného čísla 7005 pre vojenské letectvo štátu Vietnam plne dokončený. Ďalej sa v firme pracuje na kooperáciách s inými spoločnosťami a subjektami. Kooperácia so spoločnosťou Embraer je založená na výrobe nástupných dverí, zadnej nákladovej rampy aj s celou zadnou časťou lietadla okolo nákladovej rampy a nábežných hrán krídla pre model vojenského transportného lietadla KC-390. Kooperácia so spoločnosťou Airbus je pre dopravné lietadlá rodiny C-Series A220 (verzie A220-100 a A220-300), kde sa vyrába pevná nábežná hrana krídla. Prebieha tu sériová výroba na plne industrializovanej výrobnej linke. Vývoj L-39 NG stále nekončí a momentálne je v pláne zaradenie jednotky posilňovania pozdĺžneho riadenia (Pitch Control Actuator), do budúcna sa taktiež uvažuje o zaradení plnohodnotného autopilota vyvíjaného a vyrábaného priamo vo firme Aero Vodochody. Spoločnosť je kľúčovým hráčom v českom leteckom priemysle a nadviazala partnerstvá s viacerými medzinárodnými leteckými spoločnosťami. Aero Vodochody sa zaviazalo k inováciám a investovala do výskumu a vývoja, aby zabezpečilo, že ich produkty zostanú na čele leteckej techniky. [7]

Obrázok 2 Moderné cvičné vojenské lietadlo L-39 NG [7]

1.5 Vývoj a výroba L-39 NG

L-39 NG (Obrázok 2) je modernizovaná verzia L-39 Albatros, obľúbeného prúdového cvičného lietadla, ktoré bolo prvýkrát predstavené v 70. rokoch minulého storočia. Lietadlo L-39 NG je moderné ľahké prúdové lietadlo schopné plniť rolu ľahkého stíhača. Je určené pre plnohodnotný výcvik pilotov moderných vzdušných síl ktorejkoľvek krajiny na svete. Lietadlo vychádza z úspešnej pôvodnej koncepcie L-39 Albatros s úplne novými technologickými vymoženosťami ako napríklad integrálne nádrže v krídlach, moderné prístrojové vybavenie ako multifunkčný displej (MFD) a head-up displej, lepší aerodynamický tvar a spoľahlivejšia pohonná jednotka s dlhšou životnosťou, aby mohol model L-39 NG úspešne konkurovať súčasným leteckým trendom a byť využitý ako cvičné lietadlo pre ktorékoľvek iné stíhacie lietadlo na svete. O pohon lietadla sa stará spoľahlivá pohonná jednotka FJ44-4M s elektrickým štartovaním a plne digitálnym riadením pomocou systému FADEC. Oproti svojmu predchodcovi vďaka integrálnym nádržiam unesie o 300 kg viac paliva a je schopné použiť prídavné palivové nádrže, ktoré zvýšia množstvo paliva o ďalších 500 kg. Užitočný náklad, ktorý môže niesť je až 1200 kg, čo je oproti L-39 Albatros, ktorý uniesol iba 250 kg mnohonásobné zlepšenie. Maximálny dostup až 11 500 metrov je na cvičné lietadlo viac ako úctyhodný. Vďaka využitiu kompozitných materiálov je nová L-39 NG ľahšia o 250 kg v porovnaní s modelom L-39 Albatros (Tabuľka 1). [7][8]



Obrázok 3 Technický nákres lietadla L-39 NG [9]

Vývoj L-39 NG sa začal v roku 2014 a prvý let prototypu lietadla sa uskutočnil v roku 2018. Od tej doby začala sériová výroba lietadla L-39 NG (obrázok 3). Momentálne je dokončené prvé lietadlo so sériovým číslom 7005 a lietadlo s číslom 7006 bude dokončené každú chvíľu. Prvými zákazníkmi, ku ktorým prvý model čísla 7005 poputuje, bude Vietnam, ďalšími sú Maďarsko a Česká republika.

Základné parametre lietadla L-39 NG

Tabuľka 1 Parametre L-39 NG [7]

Dĺžka:	11,7 m
Rozpätie:	9,4 m
Prázdna váha:	3250 kg
MTOW:	5600 kg
Maximálna rýchlosť:	900 km/h
Maximálny výkon:	16,87 kN
Maximálne preťaženie konštrukcie:	+8/-4 g
Stúpavosť:	23 m/s
Maximálna hmotnosť paliva:	1250 kg

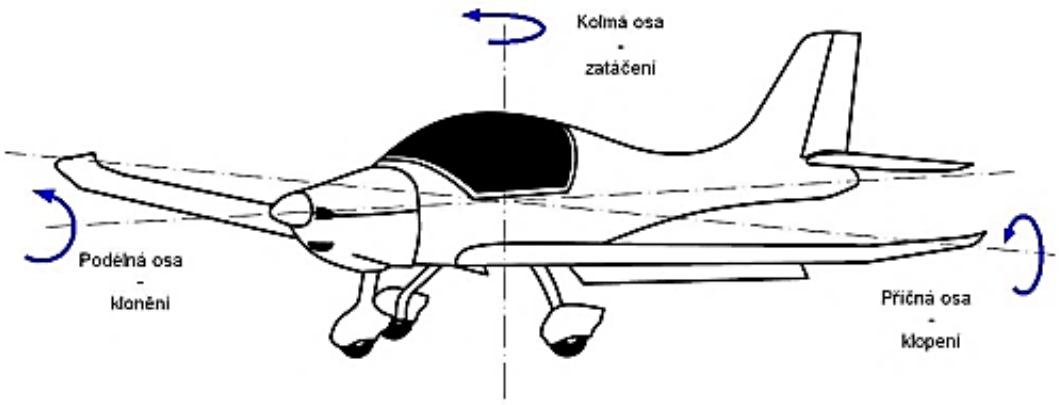
1.6 Ovládanie lietadla

Rozhodol som sa, že v tejto práci budem vypracovávať spoľahlivostnú analýzu na systéme pozdĺžneho riadenia. Pre túto mechanickú trasu je vo vývoji systém PCA, ktorý bude slúžiť na korigovanie síl na pilotovej páke. Pre tento systém s použitím PCA ešte analýzy FTA neexistujú a preto prácu na tomto systéme možno považovať za prínosnú aj pre firmu Aero Vodochody.

Ovládanie lietadla môžeme definovať ako systém jednotlivých ovládacích prvkov, ktoré umožňujú ovládanie lietadla za letu. Ovládacie prvky lietadla sa delia na primárne ovládacie prvky a vedľajšie ovládacie prvky. Primárne riadenie lietadla zaisťuje pohyb okolo troch hlavných osí lietadlového súradnicového systému (Obrázok 4), okolo pozdĺžnej, priečnej a kolmej osi. Medzi vedľajšie riadenie patrí napríklad trimovacia plôška, odľahčovacia plôška, vyvažovania plôška, vztlaková mechanizácia alebo aerodynamické brzdy.

Medzi primárne kormidlá patria 3 základné:

- Výškové kormidlo – zaisťuje klopenie (okolo priečnej osi)
- Smerové kormidlo – zaisťuje zatáčanie (okolo kolmej osi)
- Krídelka – zaisťujú klonenie (okolo pozdĺžnej osi)



Obrázok 4 Osi lietadlového súradnicového systému

1.6.1 Hlavné riadenie na lietadle

Pohyb okolo priečnej osi, v anglickom jazyku nazývanej „Pitch Control“, zabezpečuje výškové kormidlo. To vyvoláva momenty vzhľadom k ťažisku pozdĺž priečnej osi pomocou prírastku alebo úbytku vztlaku na vodorovných chvostových plochách. Vodorovná chvostová plocha môže byť v konfigurácii ako delená alebo nedelená. Delené znamená, že výškové kormidlo a horizontálny stabilizátor sú rozdelené, teda pohyb koná iba výškové kormidlo. Nedelené alebo plávajúce znamená, že výškové kormidlo a stabilizátor sú pevne spojené a teda konajú pohyb ako jedna veľká plocha.

Pohyb okolo kolmej osi, v anglickom jazyku „Yaw Control“, zabezpečuje smerové kormidlo uchytené na kýlovej ploche. Vzniknutá aerodynamická sila na smerovom kormidle vyvolá v ťažisku lietadla točivý moment. Smerové kormidlo je vždy delené a preto býva uchytené ku kýlovej ploche. Je dôležitým elementom riadenia pri lete s bočným vetrom alebo pri lete s nefunkčným motorom na jednej strane.

Pohyb okolo pozdĺžnej osi, v anglickom jazyku „Roll Control“, zabezpečujú krídelka na koncoch krídel. Ich opačné vychýlenie má za následok rozdielne vychýlenie profilu na pravom a ľavom krídle a tým pádom vznik aerodynamickej silovej dvojice, čo zapríčiní klonenie lietadla. Krídelká bývajú uchytené ku krídlu. Pri vysokých rýchlostiach je nutné obmedziť výchylky krídelok, aby sa zamedzilo vzniku príliš veľkých momentov, čomu napomáhajú diferencované výchylky. Krídelko, ktoré sa vychyľuje dole sa vychýli do polovičnej výchylky krídelka vychyľujúceho sa hore. Taktiež je možné využitie vnútorných krídelok.

1.6.2 Ovládacie prvky na lietadle L-39 NG

Obdobne ako na všetkých lietadlách, aj na lietadle L-39 NG, je zabezpečované hlavné riadenie pomocou troch kormidiel, umožňujúcich pohyb okolo troch hlavných osí lietadlovej súradnicovej sústavy. Všetky hlavné riadiace prvky sú ovládané ručne pomocou sústavy táhiel. Momentálne je RCA (Roll Control Actuator) zabudovaný iba v trase priečneho riadenia lietadla. RCA koriguje sily pôsobiace na pilotovej páke vznikajúce počas klonenia pri vysokých rýchlostiach alebo vysokých násobkoch. Ovládanie výškového kormidla a krídelok je zabezpečené pomocou dvoch riadiacich pák v prednej a zadnej kabíne (Obrázok 5). Ovládanie smerového kormidla je pomocou dvoch párov pedálov v prednej a zadnej kabíne. [9]

Obrázok 5 Znázornenie trás ovládania lietadla L-39 NG [10]

1.6.3 Pozdĺžne riadenie na L-39 NG

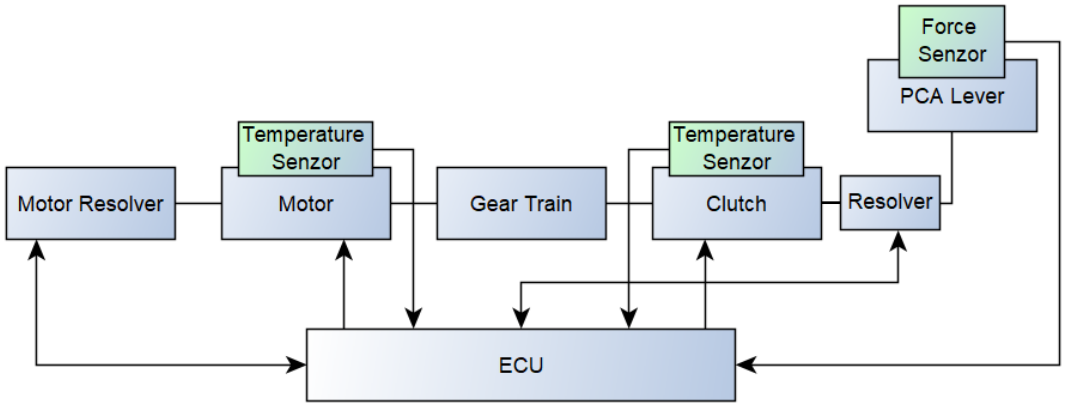
Ovládanie výškového kormidla sa nazýva pozdĺžne riadenie z dôvodu pohybu páky v pozdĺžnom smere. Jedná sa čisto o mechanickú trasu, tvorenú sústavou táhiel. Trasa začína v pilotnej kabíne kde sú napojené páky HOTAS – „Hands On Throttle And Stick“ oboch pilotov, následne sústavou táhiel až k výškovému kormidlu.

Momentálne sa vyvíja jednotka PCA (Pitch Control Actuator). Jedná sa o vytvorenie systému s paralelne zaradeným servopohonom PCA v trase pozdĺžneho riadenia umožňujúcu modifikovať výsledné pilotné sily v závislosti na vstupných parametroch. V budúcnosti sa uvažuje aj nadväznosť na podobné zariadenie v priečnom riadení s RCA (Roll Control Actuator), ktorý by mohol byť v ďalších fázach lietadla použitý do systému autopilota. [10]

1.6.4 Pitch Control Actuator (PCA)

Jedná sa o jednotku napojenú paralelne na trasu pozdĺžneho riadenia. Napojenie na trasu bude medzi 28 a 29 prepážkou lietadla (Obrázok 7). Na jednotku PCA je napojená páka PCA ktorá je napojená cez prepojovacie tiahlo napojené priamo na páku FCS, ktorá je súčasť trasy

pozdĺžneho riadenia. PCA sa skladá z ECU, elektrického motora, prevodovky a spojky (Obrázok 6). ECU (Electrical Control Unit) jednotka je elektrická jednotka slúžiaca na zber dát z externých zdrojov alebo senzorov, na výpočet požadovanej sily a riadenie procesov vo vnútri PCA. Jednotka PCA bude môcť pracovať v dvoch módoch MODE 1 a MODE 2. Pri MODE 2 bude mať jednotka ECU na starosti aj ovládanie trimovacej plôšky. [10]



Obrázok 6 Rozloženie komponentov jednotky PCA

1.6.4.1 PCA MODE 1

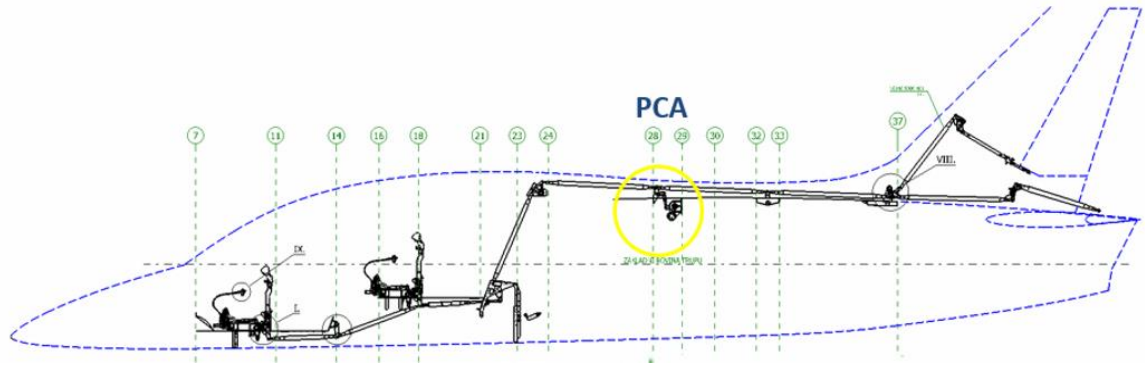
PCA odvodí cieľovú vstupnú silu načítaním výstupnej sily, pridá k nej korekciu faktora zaťaženia a škáluje tento výsledok proporcionálnou korekciou. Do ECU sú odosielané hodnoty výstupnej sily a sily na páke PCA. Taktiež sú do ECU odosielané dáta z externých zdrojov ADAHRS a LCR-100, ktoré dodávajú hodnotu faktoru zaťaženia. Potrebné dáta sú ďalej posielané do jednotky FDAU, kde sú spracované a následne odoslané na MFD oboch pilotov. [10]

- Výhody:
  - Jednoduchšie riešenie (aj oproti RCA)
  - Nezávislosť na mechanickom trime lietadla (pilot priamo ovláda polohu plôšky
- Nevýhody:
  - Pri výpadku PCA v manévre by mohlo prísť k značnému skoku v sile na páke
  - V tomto móde nie je možné implementovať auto pilotné systémy, ktoré by ako aktuátory použili PCA a RCA

1.6.4.2 PCA MODE 2

PCA odvodí cieľovú vstupnú silu načítaním vstupnej sily a škálovaním pomocou zosilnenia vzdušnej rýchlosti a pridaním korekcie faktora zaťaženia k výsledku. PCA na základe pozície páky voči umelo vytrimovanej pozícii odvodí základnú silu zo závislosti sila-výchylka, z ktorej ďalej dedukuje cieľovú hodnotu sily na páke riadenia pomocou znalosti rýchlosti letu a násobku lietadla. Na túto cieľovú hodnotu sily je riadený krútiaci moment PCA. Funkcia AUTO-TRIM pri dlhodobom účinku PCA v jednom zmysle pošle signál do motorčeka mechanického trimu a automaticky dolaďuje mechanický trim lietadla tak, aby uľahčoval PCA prácu. Do ECU sú odosielané hodnoty vstupnej sily a sily na páke PCA. Taktiež sú do ECU odosielané dáta z externých zdrojov ADAHRS a LCR-100, ktoré dodávajú hodnotu faktoru zaťaženia. Zo zdrojov ADAHRS a ADC-39 je dodávaná hodnota vzdušnej rýchlosti. Senzor aktuálnej hodnoty páky HOTAS slúži pre vychýlenie trimovacej plôšky. Následne sú dôležité dáta odoslané cez jednotku FDAU na MFD oboch pilotov. [10]

- Výhody:
  - Menší skok v sile na páke riadenia u pilota pri výpadku PCA v manévri vďaka AUTO-TRIMu
  - Možnosť budúceho vývoja nezávislého auto pilotného systému
- Nevýhody:
  - Zložitejší riadiaci zákon, ktorý bude vyžadovať dlhé ladenie
  - Nutnosť zlepšiť plynulosť a rýchlosť regulácie síl, aby AUTO-TRIM nebol v riadení znateľný



Obrázok 7 Plánované umiestnenie jednotky PCA medzi 28. a 29. prepážkou [10]

1.7 Limitácia súčasného stavu

V rámci procesu vytvárania analýzy musí inžinier spoľahlivosti zhromaždiť existujúce údaje o systéme, ako je zoznam komponentov, ich pridružené funkcie a rôzne diagramy zobrazujúce ich vzájomné pôsobenie. Tieto prvky sú zvyčajne definované a zdokumentované konštruktérmi a zhromaždenie všetkých požadovaných údajov sa môže stať neefektívnym a časovo náročným. V dôsledku toho sa výsledky analýzy môžu rýchlo odchýliť od návrhu počas vývoja a stať sa zastaranými. Pri modelovej analýze, kde sú tieto údaje k dispozícii v spoločnom úložisku a je implementovaná automatizácia zberu a spracovania údajov, vedú tieto inovácie k ušetreniu času a zefektívneniu práce osoby pracujúcej na danej analýze . [11]

Ako to už býva, aj v odvetví spoľahlivostných analýz sa nájdu určité limitácie, ktoré otvárajú otázky, ako danú metódu upraviť alebo pozmeniť. V odvetví spoľahlivostných analýz je týchto limitácii pomerne veľa, na čom sa podpísalo aj to, že pôvod niektorých metód siaha až do 60. rokov minulého storočia. Medzi najvýznamnejšie obmedzenia spoľahlivostných analýz patria obmedzené dáta, použitie predpokladov alebo odhadov, veľké množstvo času, chýbajúca automatizácia.

Obmedzené dáta

Pri vytváraní spoľahlivostných analýz sa spolieha na určité dáta alebo materiály popisujúce systém lietadla. V niektorých prípadoch, ako napríklad pri vývoji nového systému lietadla alebo nového lietadla, je k dispozícii iba obmedzené množstvo údajov a dát o danom systéme, čo môže sťažiť alebo ovplyvniť výslednú analýzu. V tomto bode je nutné, aby analýzu vypracoval dostatočne skúsený analytik, ktorý môže niektoré údaje odhadnúť z praxe, keď už na podobnom systéme pracoval. V prípade pravdepodobností nastáva podobný problém, kedy pri niektorých nových súčiastkach nie je daná pravdepodobnosť zlyhania tejto súčiastky. V tomto prípade sa často využíva spôsob, pri ktorom sa použijú prevádzkové dáta z podobného komponentu z iného lietadla. Tieto dáta použité z podobnej komponenty neurčujú presnú hodnotu súčiastky, ktorá sa v danom systéme využíva.

Použitie predpokladov alebo odhadov

Ako je spomenuté v predchádzajúcom bode, pri vytváraní analýz sa často používa odhad, aby sa vyplnili medzery v znalostiach alebo chýbajúcich dátach. Tento krok môže vykonávať iba poverená osoba, ktorá dokáže s určitou presnosťou chýbajúce údaje odhadnúť. Vďaka tejto limitácii sa do analýzy dostávajú určité nepresnosti, ktoré môžu ovplyvňovať výsledok analýzy.

Množstvo času

Vykonanie dôkladnej a presnej analýzy spoľahlivosti zaberie veľké množstvo času. Je potrebné dôkladné pochopenie systému, aby bolo možné určiť všetky funkcie a ich poruchové stavy. Ďalej je nutnosťou porozumenie interakcii daných funkcií a vykonanie analýzy, v prípade analýzy FTA to znamená vykonať vlastný strom porúch pre každú funkciu. Po vytvorení stromov porúch nasleduje vyplnenie pravdepodobností elementárnych komponentov. Tento proces zaberie veľké množstvo času osôb vykonávajúcich analýzu. Riešením, ako tento čas skrátiť je, že niektoré procesy pri vypracovávaní by bolo možné automatizovať, čomu sa budem venovať v ďalšom kroku.

Chýbajúca automatizácia

Pri vytváraní analýz spoľahlivosti sa naskytuje mnoho postupov, ktoré by bolo možné automatizovať. V súčasnej dobe a pri dnešných technológiách je naozaj nepredstaviteľné, aby vypracovávanie analýz prebiehalo celkovo manuálne, preto sa na trhu objavujú prostriedky aspoň s čiastočnou automatizáciou. Napríklad RAM Commander alebo FTA/FMEA tool sú softvéry, ktoré pracujú na poloautomatickej úrovni, čo znamená, že všetky dáta o systéme, jeho funkcie a poruchové stavy je nutné zadať manuálne. Samozrejme táto automatizácia ušetrí veľké množstvo času, no momentálne sa rieši otázka ako zautomatizovať zadávanie údajov a dát o systéme do softvéru, ktorý by z týchto dát dokázal automaticky vytvoriť analýzu spoľahlivosti.

Limitácie, ktoré budeme riešiť v tejto práci

V mojej bakalárskej práci sa budem zaoberať dvoma z hlavných problémov spomenutých v predchádzajúcom bode. Jedná sa o automatizáciu spoľahlivostných analýz a k tomu náležiace ušetrenie času. Budem pracovať s jedným s dostupných poloautomatizovaných softvérov pre vytváranie analýzy FTA. Následne sa pokúsim stanoviť možnosti a postupy využitia plno automatizovanej spoľahlivostnej analýzy. V tomto kroku stanovím, ako by bolo možné vkladať alebo načítať údaje o systéme do softvérového riešenia automaticky. Teda ako by bolo možné, aby softvér dokázal načítať alebo porozumieť technickú dokumentáciu a následne automaticky vygenerovať spoľahlivostnú analýzu FTA.

2. Metódy práce

Použité boli postupy vypracovania spoľahlivostných analýz FHA a FTA, použité softvérové riešenie vo firme Aero Vodochody, automatizovaný FTA/FMEA tool vytvorený na ČVUT, Fakulte dopravnej a Fakulte elektrotechnickej a následné porovnanie dostupných poloautomatizovaných softvérov.

2.1 Metódy pre analýzu spoľahlivosti

V tomto bode sa budeme zaoberať dvoma v praxi často používanými metódami pre analýzu spoľahlivosti, ktoré sa využívajú aj v AVA. Sú to analýzy FHA a FTA.

2.1.1 FHA – Functional Hazard Assessment

Úlohou FHA je identifikovať a posúdiť dôsledky na lietadlo alebo lietadlový systém, ktoré môžu vyplynúť z poruchových stavov funkcií systému. Ak je to potrebné, mali by sa vytvoriť postupy alebo nápravné opatrenia, ktoré môžu minimalizovať dôsledky týchto poruchových stavov. FHA slúži na prioritizáciu nebezpečných poruchových stavov, ktorých dôsledky by mohli mať katastrofálny dopad. Každý tento poruchový stav je nutné overiť určitou verifikačnou metódou (FTA alebo FMEA), ktorou sa vypočíta pravdepodobnosť, že tento poruchový stav nastane. Následne sa určí hodnota RAC (Risk Assessment Coefficient), ktorá je spojením kritičnosti daného poruchového stavu a pravdepodobnosti, že táto porucha nastane. Vďaka tejto hodnote RAC sa následne určí, do akej miery je tento poruchový stav nebezpečný. Ešte pred začatím vypracovania je veľmi dôležitý popis systému, vďaka čomu je jednoduchšie stanovenie všetkých funkcii systému a pochopenie interakcii v systéme. Táto metóda je kľúčová aj čo sa týka prezentácie výsledkov, keďže každý nebezpečný poruchový stav je dostatočne prioritizovaný.

Postup vypracovávania FHA analýzy

Prvým krokom pri vykonávaní FHA je definovanie systému alebo subsystému, ktorý chceme analyzovať. Môže sa jednať o celé lietadlo alebo akýkoľvek systém, ako napríklad pozdĺžne ovládanie lietadla alebo dodávka elektrickej energie. Druhým krokom pri vypracovávaní je identifikácia všetkých funkcii systému, ktoré môže daný systém vykonávať. Takže je potrebné dôkladné porozumenie všetkých funkcií systému aby sa na niektoré nezabudlo. Následným krokom je identifikácia poruchových stavov náležiacich ku všetkým funkciám, ktoré sme v kroku dva identifikovali. Je dôležité si zapamätať, že každá funkcia môže mať viac ako jeden

poruchový stav. Aby sa nezabudlo na žiadny z nich, je praktické a často aj v praxi používané rozdelenie si poruchových stavov na NEFUNGUJE/NEFUNGUJE DOSTATOČNE/FUNGUJE SAMOVOĽNE. Ďalším krokom po určení funkcií a poruchových stavoch je stanovenie dôsledkov ku každému poruchovému stavu. V tomto kroku je potrebné poznať aj interakcie rozličných funkcií, aby bolo jednoduchšie určiť, čo spôsobí zlyhanie jednej z nich na lietadlo ako celok. Väčšinou sa tu uvádza dôsledok na lietadlo ako celok, ale môže byť rozpísaný aj podrobnejšie. Posledným krokom je stanovenie kritičnosti a vypočítanie pravdepodobnosti pre každý poruchový stav. Kritičnosť je určená podľa tabuľky na určenie kritičnosti (Obrázok 8). Ako môžeme vidieť, najkritickejšie je číslo 1 a najmenej kritické je číslo 4.

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Obrázok 8 Tabuľka na určenie kritičnosti poruchového stavu [12]

Pravdepodobnosť, že daný poruchový stav nastane, je nutné vypočítať pomocou verifikačnej metódy. Najčastejšie sa na výpočet pravdepodobnosti využíva metóda FTA. Hodnota pravdepodobnosti sa premení na písmeno pre ďalšie použitie podľa tabuľky na obrázku. Najčastejšie vyskytujúcim sa poruchovým stavom sú priradené písmená od začiatku abecedy a najmenej vyskytujúcim sú priradené písmená E a D (Obrázok 9). [12]

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Obrázok 9 Tabuľka na stanovenie triedy pomocou pravdepodobnosti [12]

Po vypočítaní všetkých pravdepodobností pre každý poruchový stav sa pomocou tejto pravdepodobnosti a kritičnosti stanoví hodnota RAC. Hodnota RAC je spojenie úrovne pravdepodobnosti, ktorej sa priradí zodpovedajúce písmeno (od A do E) a kategórie kritičnosti vyjadrenej číslom (od 1 do 4). Následne sa podľa tabuľky Risk Assessment Matrix určí riziko daného poruchového stavu, ktorá sa delí na LOW/MEDIUM/SERIOUS/HIGH (Obrázok 10). [12]

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Obrázok 10 Tabuľka na stanovenie rizika poruchových stavov [12]

Podľa úrovne rizika je možné priradiť poruchovým stavom farbu od zelenej až po červenú. Vďaka tomu je jednoduchšie kritický poruchový stav objaviť a vykonať potrebné opatrenia, aby sa mu zabránilo. Farba z matice rizík (Obrázok 10) vyjadruje prijateľnosť daného rizika. Teda napríklad zelená farba vyjadruje, že s daným rizikom nemusíme robiť nič, pretože nepredstavuje takmer žiadne riziko. Naopak červená farba vyjadruje, že riziko je neprípustné a je nutné niečo zmeniť inak to nespĺňa štandardy.

Výstupom FHA analýzy je tabuľka, v ktorej sú vysvetlené všetky vopred použité postupy. Na obrázku je možné vidieť farebné označenie, ktoré zvýrazňuje riziko poruchového stavu (Obrázok 11).

Funkce		Popis a hodnocení důsledků poruchových stavů								Poznámky	
		Poruchový stav		Signalizácia	Fáze letu	Důsledky poruchového stavu na letoun/ posádku	Kritičnost	Pravděp.	RAC	Odkazy na podkladové materiály	Verif. metoda
ID	Popis	ID	Popis	áno/nie							
1	*Podélne riadenie L-39NG*	FC_1									
1.1.	Ovládanie výchylky výškového kormidla	FC_1.1	Výškové kormidlo nereaguje	x	2-7	Strata podélneho ovládania lietadla. Veľmi nebezpečný jav ktorý nie je signalizovaný. Pilot to zistí pocitovo pri pôsobení na HOTAS sa nič nestane. Pilot musí okamžite prerušiť let a pokúsiť sa pristáť.	1	1,23E-04	1D		8
1.1.	Ovládanie výchylky výškového kormidla	FC_1.2	Výškové kormidlo nereaguje dostatočne	x	2-7	Čiastočná strata podélneho ovládania lietadla. Lietadlo nie je schopné plných výchyliek. Pilot to zistí pocitovo pri pôsobení na HOTAS lietadlo nereaguje dostatočne. Pilot musí prerušiť let.	2	6,20E-06	2D		8
1.2.	Ovládanie výchylky výškového kormidla s pomocou PCA (MODE 1)	FC_1.3	Výškové kormidlo nie je možné ovládať pomocou PCA	áno	2-7	Podélne riadenie je bez posilovača riadenia. Pilot môže lietadlo stále ovládať manuálne ale je znížený komfort počas letu. Odpojenie PCA je signalizované na MFD a Master Table. Pilot môže pokračovať v lete pretože nie je priamo ohrozená bezpečnosť letu	4	3,12E-04	4D		8

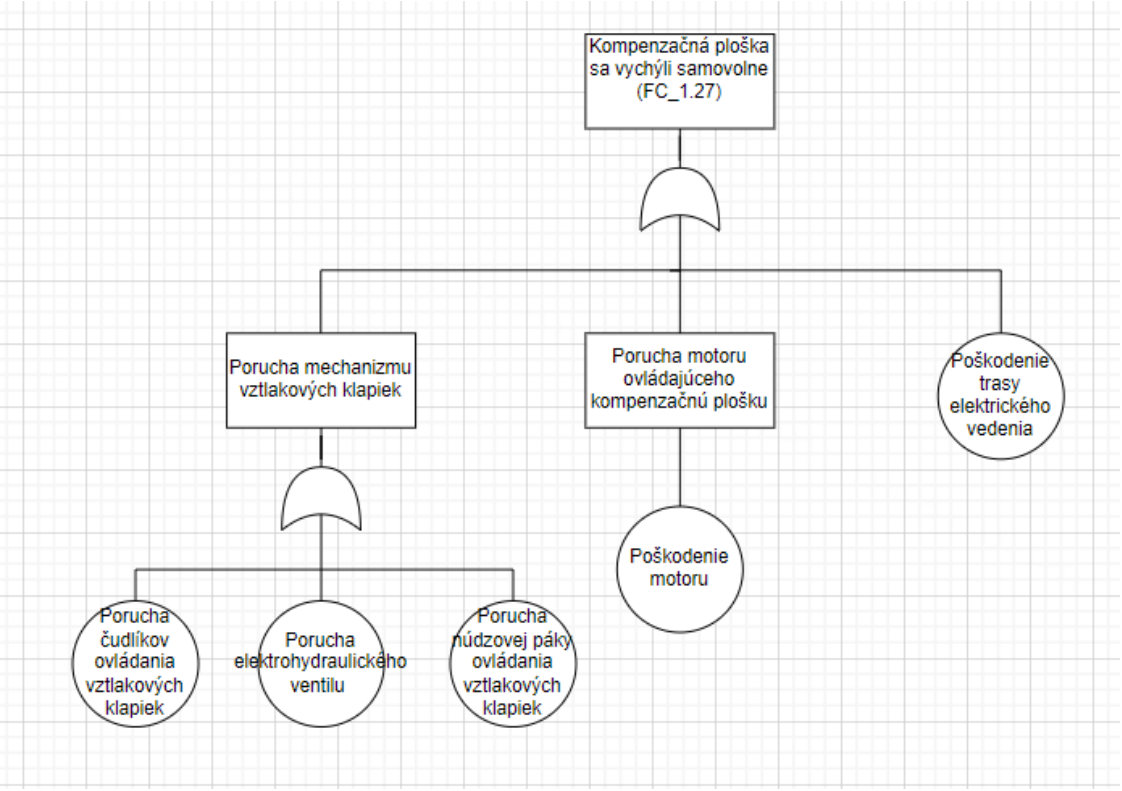
Obrázok 11 Tabuľka FHA analýzy s vyznačením miery rizika

2.1.2 FTA – Fault tree analysis

FTA, teda analýzu stromu porúch možno zjednodušene opísať ako analytickú techniku, pri ktorej dochádza k určeniu poruchových stavov daného systému. Poruchový stav je stav, ktorý je kritický z hľadiska bezpečnosti alebo spoľahlivosti alebo nie je kritický, ale spôsobí určité zlyhanie v systéme. Následne sa systém analyzuje v kontexte jeho použitia a prevádzky, aby sa našli všetky možnosti, pri ktorých by mohlo dôjsť k poruchovým stavom. Samotný strom porúch je grafickým modelom rôzne napojených kombinácii porúch, ktoré budú mať za následok výskyt poruchových stavov. Poruchy môžu byť udalosti spojené so zlyhaním komponentov, softvérovej chyby alebo akejkoľvek inej udalosti vedúcej k poruchovým stavom. Strom porúch teda zobrazuje logické nadväznosti základných udalostí, ktoré vedú k vrcholovej udalosti daného stromu. Treba si uvedomiť, že strom porúch nie je modelom všetkých možných zlyhaní systému. Strom porúch je prispôsobený danej vrcholovej udalosti, ktorej zodpovedajú určité zlyhania komponentov, teda zahŕňa len tie zlyhania, ktoré prispievajú k tejto vrcholovej udalosti. Analýza stromu porúch je príkladom deduktívneho postupu pri vytváraní analýz. Tento postup je založený na nájdení vrcholovej udalosti, kde sa následne identifikujú možné poruchy vedúce k tejto vrcholovej udalosti. Cieľom tejto analýzy je nájdenie všetkých zlyhaní elementárnych komponentov, ktoré môžu viesť k vrcholovej udalosti a následne využitie týchto informácii pre vylepšenie systému a zníženie pravdepodobnosti výskytu poruchy v danom systéme. [13][14]

Postup vypracovávania

Prvým krokom pri vykonávaní FTA analýzy je definovanie systému, na ktorom bude daná analýza vykonávaná. Môže to byť špecifický systém lietadla alebo celé lietadlo. Ďalším krokom je identifikácia vrcholových udalostí. Aby nastala táto udalosť, musí zlyhať viacero elementárnych systémov alebo komponentov. Jedná sa teda o vrchol daného stromu porúch. Po identifikácii vrcholových udalostí je potrebné identifikovať elementárne udalosti alebo zlyhania jednotlivých komponentov, ktoré v prípade zlyhania môžu viesť k zlyhaniu vrcholovej udalosti. Pomocou identifikovaných elementárnych udalostí vytvoríme strom porúch ukazujúci, ako by tieto systémy mohli zlyhať, aby spôsobili zlyhanie vrcholovej udalosti. Strom porúch je vizuálnou reprezentáciou logických vzťahov medzi elementárnymi udalosťami. Posledným krokom je vyhodnotenie pravdepodobnosti každej elementárnej udalosti. Tieto pravdepodobnosti je možné získať z prevádzkových dát určitých komponentov alebo znaleckých odhadov. Pravdepodobnosti zlyhania elementárnych komponentov sa využijú na výpočet celkovej pravdepodobnosti zlyhania vrcholovej funkcie. [13][14]



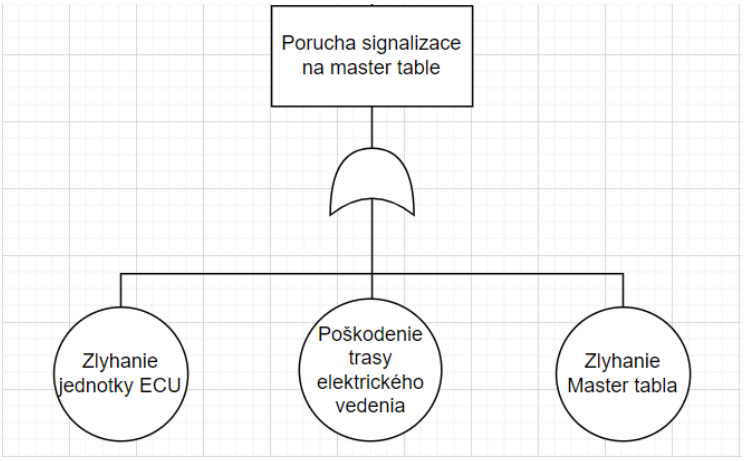
Obrázok 12 Strom porúch FTA analýzy vytvorený manuálne

Kruhové označenia sú použité na označenie zlyhania základného komponentu vopred definovaného systému (Obrázok 12). Následne sa tieto zlyhania spájajú logickým hradlom do obdĺžnika ktorý predstavuje názov poruchy určitej skupiny, do ktorej patria napojené komponenty. Najvyšší blok predstavuje vrcholovú udalosť, ktorá nastane v prípade, že budú splnené podmienky logiky analýzy FTA.

Logické hradlá

Poznáme dve základné logické hradlá využívané v stromoch porúch, a to logické hradlo AND a OR.

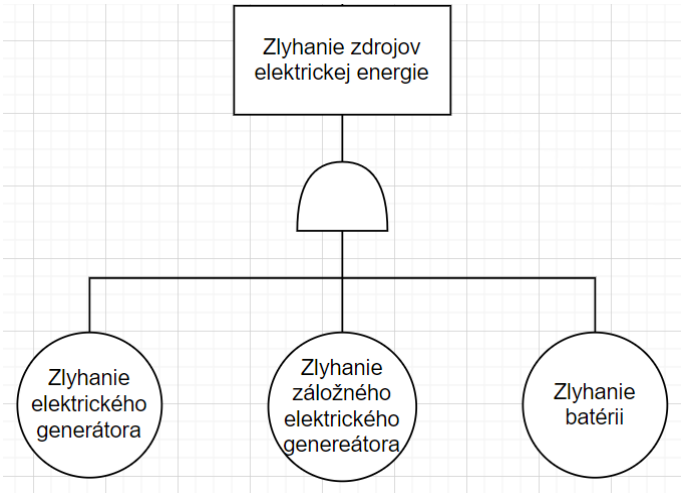
Logické hradlo OR sa používa na vyjadrenie toho, že výstupná udalosť nastane iba vtedy, ak nastane jedna alebo viac vstupných udalostí. Do logického hradla OR môže vstupovať ľubovoľný počet vstupných udalostí.



Obrázok 13 Spojenie elementárnych zlyhaní pomocou logického hradla OR

Na Obrázku 13 je zobrazená situácia možnej poruchy signalizácie. Porucha signalizácie nastane pri vzniku jednej alebo viac elementárnych porúch, ktoré do logického hradla OR vstupujú.

Logické hradlo AND sa používa na vyjadrenie toho, že výstupná udalosť nastane iba vtedy, ak nastanú všetky vstupujúce udalosti. Môže existovať ľubovoľný počet vstupných udalostí vstupujúcich na logické hradlo AND.



Obrázok 14 Spojenie elementárnych zlyhaní pomocou logického hradla AND

Pri zlyhaní zdrojov elektrickej energie (Obrázok 14) by museli zlyhať všetky vstupujúce elementárne udalosti. V prípade, že by nastala iba jedna alebo dve, sa stále nejedná o zlyhanie všetkých zdrojov a teda energia je stále do systému dodávaná. [13]

Výpočet pravdepodobnosti vrcholových funkcii

V analýze FTA sa logické hradlá ako OR a AND používajú na kombináciu pravdepodobnosti základných udalostí a slúžia k výpočtu pravdepodobnosti vrcholovej udalosti.

Rovnica (1) sa využíva pre výpočet pravdepodobnosti vrcholovej udalosti pri vstupe 2 základných udalostí do logického hradla OR.

$$P_v = 1 - (1 - P_{u1}) * (1 - P_{u2}) \qquad \text{(Rovnica 1)}$$

Kde P_v je pravdepodobnosť vrcholovej udalosti. P_{u1} a P_{u2} sú pravdepodobnosti udalostí vstupujúce do logického hradla OR.

Pravdepodobnosť výskytu vrcholovej udalosti pri použití logického hradla AND sa vypočíta vynásobením pravdepodobnosti každej základnej udalosti, ktorá musí nastať. Táto rovnica (2) nám ukazuje výpočet pravdepodobnosti vrcholovej udalosti pri vstupe 2 základných udalostí do logického hradla AND.

$$P_v = P_{u1} * P_{u2} \qquad \text{(Rovnica 2)}$$

Kde P_v je pravdepodobnosť vrcholovej udalosti. P_{u1} a P_{u2} sú pravdepodobnosti udalostí vstupujúce do logického hradla AND.

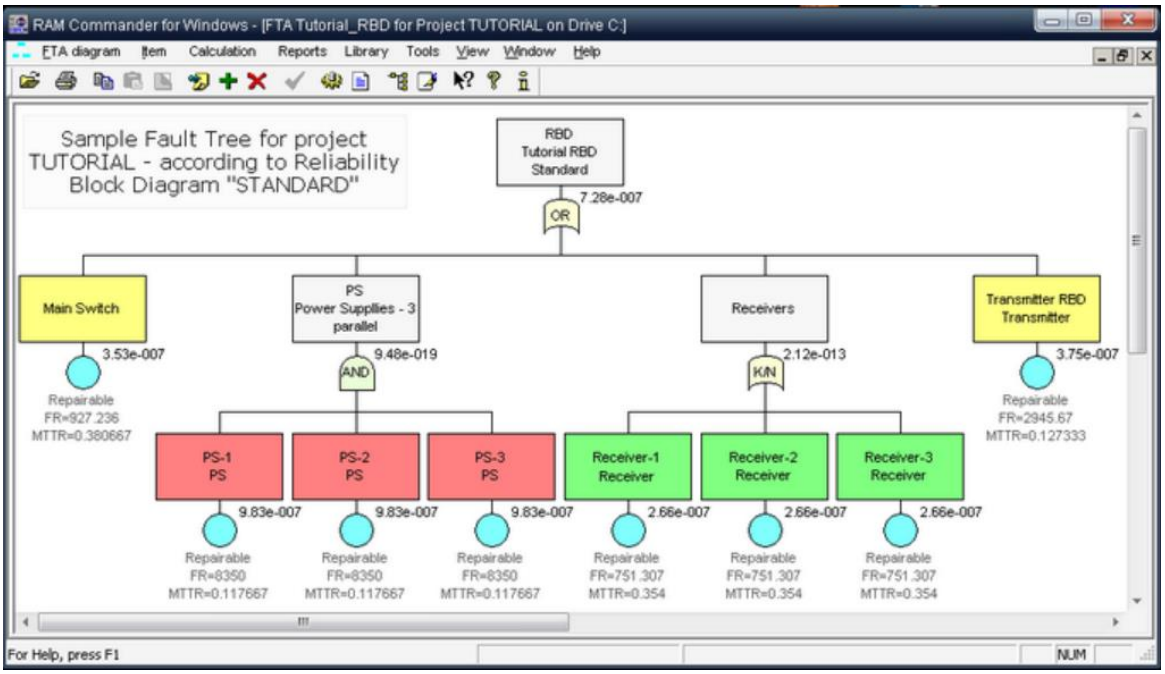
2.2 Poloautomatizované spoľahlivostné analýzy

V tomto bode popisujem súčasný softvér vo firme Aero Vodochody na vytváranie FTA analýz, následne popisujem poloautomatizované softvérové riešenie vyvinuté na Fakulte dopravnej a Fakulte elektrotechnickej, ČVUT a následne ostatné dostupné riešenia na automatizáciu spoľahlivostných analýz.

2.2.1 Softvérové riešenie využité vo firme Aero Vodochody

Vo firme Aero Vodochody sa využíva softvér RAM Commander[1] (Obrázok 15). RAM Commander je komplexný softvérový nástroj pre analýzu a predikciu spoľahlivosti, hodnotenie bezpečnosti a testovanie systémov. Pokrýva všetky súčasné štandardy a normy spoľahlivosti a prístupy k analýzam porúch. Všetky jeho nástroje sú integrované v jednom softvérovom balíku. RAM Commander je dôležitým nástrojom pre zabezpečenie spoľahlivosti sofistikovaných systémov. Pre vytváranie analýz FTA je potrebné všetky stromy porúch vymodelovať manuálne. Pre každú vrcholovú funkciu systému sa vytvorí jeden strom porúch. Následná vymoženosť spočíva v tom, že RAM Commander pracuje s databázou na výpočet pravdepodobností komponentov a je možné nastavenie presných parametrov, pri ktorých sa komponent využíva a v akých podmienkach bude prevádzkovaný, vďaka čomu je možné pracovať s oveľa presnejšími hodnotami pravdepodobností a celá analýza je vo výsledku oveľa presnejšia. V zozname komponentov daného systému, pre ktorý túto analýzu vykonávame, sa uložia pravdepodobnosti zlyhaní komponentov s vopred zadanými parametrami z databázy. Tieto hodnoty pravdepodobností sa automaticky importujú do stromov porúch, kde automaticky dopočítajú výslednú pravdepodobnosť zlyhania vrcholovej funkcie. [15]

[1] https://aldservice.com/Reliability-Products/fta.html



Obrázok 15 Ukážka stromu porúch analýzy FTA v softvéri RAM Commander [15]

2.2.2 Dostupné riešenia pre automatizáciu spoľahlivostných analýz

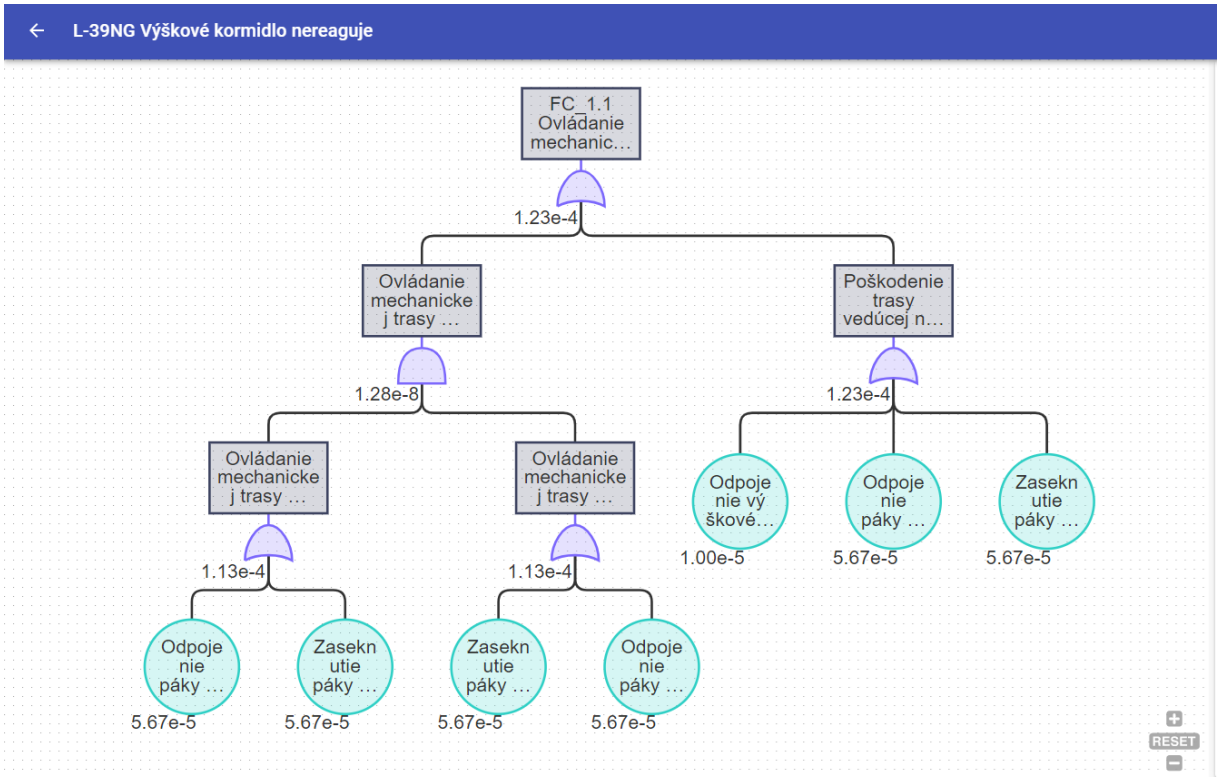
V tomto bode popíšem poloautomatizované softvérové riešenie FTA/FMEA tool a dostupné riešenia na automatizáciu spoľahlivostných analýz, ku ktorým som mal prístup a bola v nich uplatnená čiastočná automatizácia.

2.2.2.1 Poloautomatizované softvérové riešenie FTA/FMEA tool

Softvérové riešenie FTA/FMEA tool[2] je poloautomatizovaný softvér určený na vytváranie spoľahlivostných analýz. Bol vytvorený pod záštitou Ústavu leteckej dopravy, Fakulty dopravnej za pomoci Fakulty elektrotechnickej na automatizáciu spoľahlivostných analýz FTA a FMEA. Momentálne sa jedná o poloautomatizovaný softvér, ktorý na základe vložených dát o systéme automaticky vygeneruje stromy porúch (Obrázok 16) a z nich je následne možné vytvoriť FMEA analýzu. Po zadaní pravdepodobností zlyhaní elementárnych komponentov sa vypočíta pravdepodobnosť vrcholovej udalosti daného stromu porúch. FTA/FMEA tool prináša oproti úplne manuálnemu vytváraniu analýz niekoľko výhod. Jednou z nich je, že dokáže automaticky vypočítať pravdepodobnosť vrcholovej udalosti po zadaní pravdepodobností zlyhania elementárnych komponentov. Po zadaní všetkých dát o systéme do toolu vygeneruje

[2] https://kbss.felk.cvut.cz/fta-fmea-aero-vodochody/

stromy porúch, takže nie je nutné vytvárať všetky stromy porúch po jednom, ako to je pri plne manuálnom vytváraní. Momentálne sa jedná o poloautomatický softvér z dôvodu, že vkladanie dát do softvéru prebieha na manuálnej úrovni. To znamená, že v prvom kroku sa do FTA/FMEA toolu zadávajú komponenty systému, funkcie komponentov a systému, poruchové stavy a následne vzájomné napojenia medzi jednotlivými funkciami systému, takže ešte pred začatím analýzy musí personál vytvárajúci analýzu dôkladne porozumieť funkciám, poruchovým stavom a interakciám daného systému.



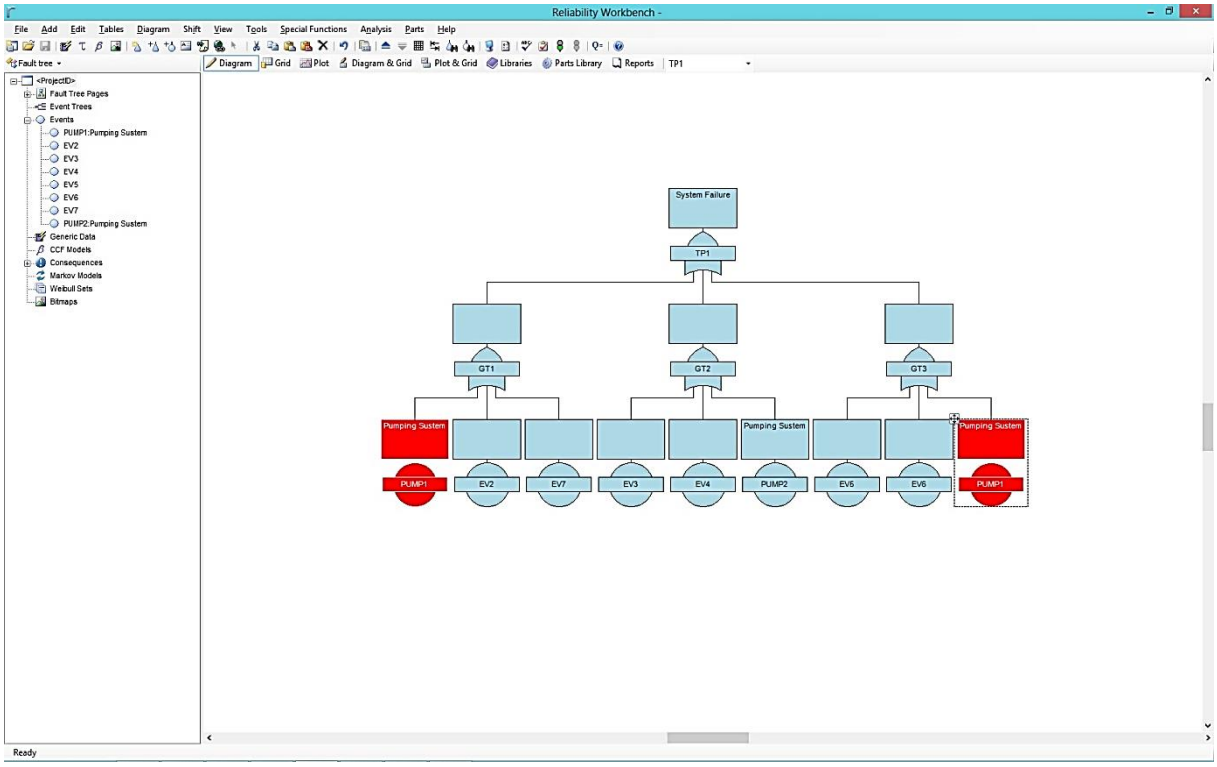
Obrázok 16 Ukážka stromu porúch analýzy FTA v softvéri FTA/FMEA tool

2.2.2.2 Poloautomatizované softvérové riešenie Isograph Reliability Workbench

Jedná sa o softvér od firmy Isograph, ktorý poskytuje čiastočnú automatizáciu pri vytváraní FTA analýzy. Využíva sa aj pri iných typoch analýz napríklad RBD alebo FMECA. Softvér Isograph[3] umožňuje vytváranie stromov porúch pomocou grafického rozhrania (Obrázok 17). Je možné si vybrať zo širokej škály symbolov a z databáz pre jednotlivé typy porúch a jednoducho ich pridávať a upravovať. Použitie databáz uľahčuje proces tvorby stromov

[3] https://www.isograph.com/software/reliability-workbench/fault-tree-analysis-software/

porúch. Softvér umožňuje importovať dáta z databáz alebo tabuliek. Tým sa umožňuje automatizované načítanie relevantných dát o komponentoch do FTA analýzy a ich použitie pri vytváraní stromov porúch. Je možné automatické počítanie pravdepodobností zlyhaní. Taktiež softvér dokáže odhadnúť pravdepodobnosť niektorých porúch, pomocou historických dát



Obrázok 17 Ukážka stromu porúch analýzy FTA v softvéri Isograph [16]

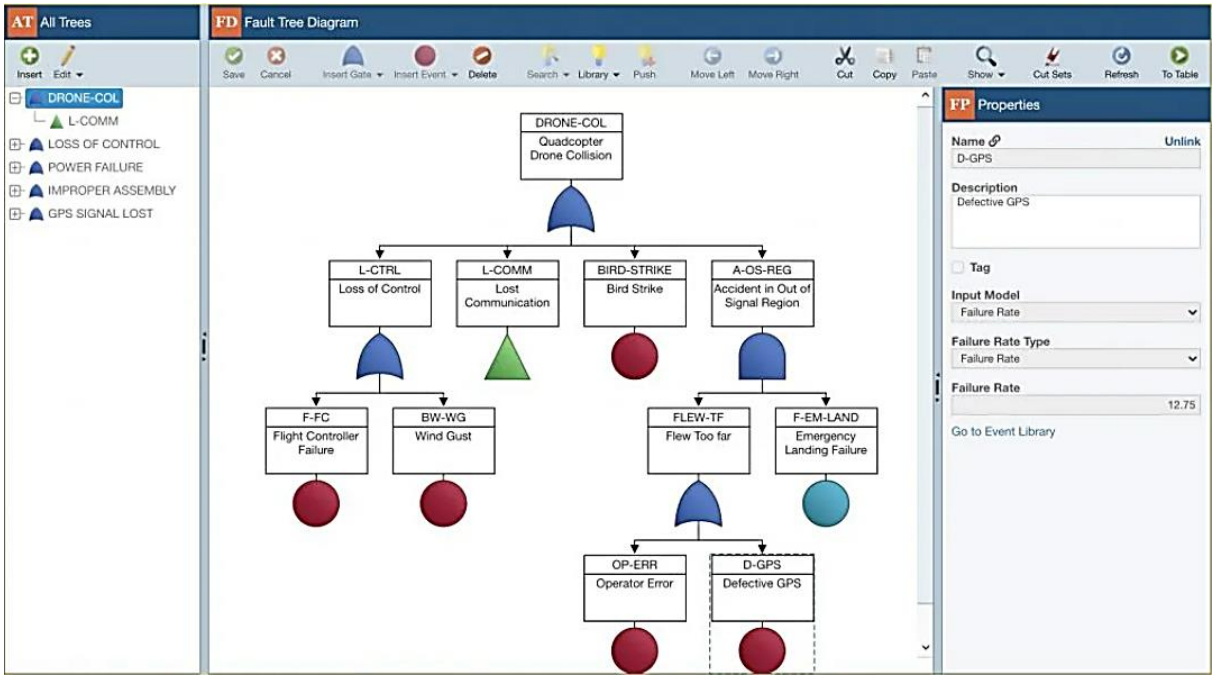
alebo pomocou výpočtov priamo zabudovaných v softvéri. Isograph poskytuje nástroje na analýzu a vyhodnotenie jednotlivých stromov porúch. Vypočíta celkovú pravdepodobnosť zlyhania systému, identifikuje kľúčové príčiny zlyhania a ich vplyv na spoľahlivosť. Tieto výsledky pomôžu lepšie porozumieť chybám a rizikám v systéme. Taktiež softvér umožňuje generovanie prehľadných a podrobných správ z FTA analýzy. Tieto správy obsahujú výsledky analýzy, grafy, tabuľky a ďalšie informácie. Výstupné správy je možné jednoducho exportovať do rôznych formátov, ako je PDF alebo Excel. [16]

2.2.2.3 Poloautomatizované softvérové riešenie Relyence

Softvér Relyence[4] od firmy Relyence Corporation je softvérové riešenie slúžiace na čiastočnú automatizáciu pri vytváraní FTA analýz. Poskytuje užívateľské rozhranie pri vytváraní analýz

[4] https://relyence.com/products/fault-tree/

a umožňuje jednoduchú manipuláciu a zmeny v tomto základnom rozhraní (Obrázok 18). V počiatočnom kroku je potrebné definovať a vytvoriť stromy porúch. Pri tvorbe stromov porúch musíme identifikovať jednotlivé poruchy a stanoviť ich vzťahy a hierarchiu v systéme. Po vytvorení stromu porúch nasleduje priradenie pravdepodobností zlyhania k jednotlivým poruchám. Softvér umožňuje zadávanie pravdepodobnosti zlyhania komponentov do tabuľky alebo databázy z ktorej následne tieto hodnoty importuje do stromov porúch. Relyence umožňuje použiť rôzne pravdepodobnostné modely, historické údaje alebo vlastné odhady na určenie pravdepodobností zlyhania. Po priradení pravdepodobností zlyhania vykoná Relyence automatický výpočet. Automaticky vypočíta pravdepodobnosť vrcholovej udalosti. Softvér poskytuje nástroje na vyhodnotenie vplyvu jednotlivých porúch na celkovú spoľahlivosť systému. Na základe pravdepodobností zlyhania a vzťahov medzi poruchami je možné identifikovať najkritickejšie poruchy. Relyence taktiež umožňuje generovanie prehľadných a podrobných správ z FTA analýzy. Tieto správy obsahujú informácie o pravdepodobnostiach zlyhania, vplyve jednotlivých porúch, grafy a tabuľky. [17]



Obrázok 18 Ukážka stromu porúch analýzy FTA v softvéri Relyence [17]

Prínosom softvéru Relyence je využitie databáz a výpočtových metód na určenie pravdepodobnosti zlyhania komponentov, výpočet pravdepodobnosti vrcholových udalostí, identifikácia najkritickejších komponentov a následné generovanie výstupných správ.

3. Aplikácia metód FHA a FTA na systéme pozdĺžneho riadenia L-39 NG

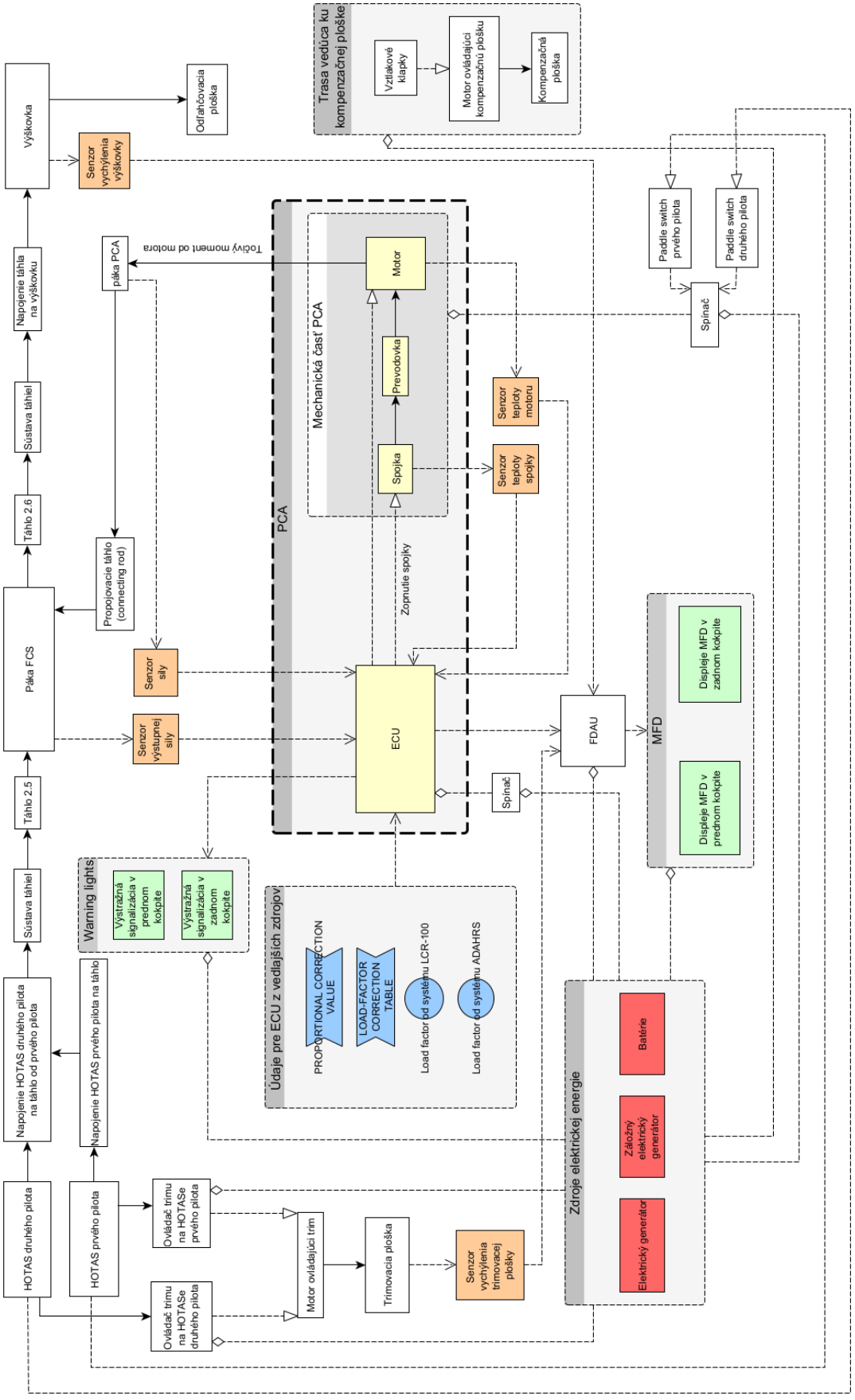
V tejto kapitole popisujem, ako som postupoval pri vytváraní spoľahlivostnej analýzy. Na stanovenie spoľahlivosti systému som si vybral dve metódy, ktoré spolu súvisia. Jedná sa o metódu FTA a FHA. Ako prvú predstavím schému pozdĺžneho riadenia lietadla L-39 NG, slúžiacu na porozumenie rozloženia a napojenia komponentov systému a porozumenie vzájomným interakciám medzi nimi. Následne ukážem vytvorenú analýzu FHA, do ktorej som vložil výsledky z FTA analýzy. Následne potvrdím alebo vyvrátim správnosť výstupov z FTA/FMEA toolu. Vstupné dáta sú prevažne dáta od firmy Aero Vodochody a pri niektorých je táto hodnota dopočítaná pomocou MTBF Calculator[5].

3.1 Schéma pozdĺžneho riadenia L-39 NG

Pre následnú spoľahlivostnú analýzu a porozumenie funkciám a interakciám komponentov v systéme pozdĺžneho riadenia som vypracoval zjednodušenú schému systému, ktorá znázorňuje jednotlivé komponenty systému a vzájomné prepojenie medzi nimi. Pracoval som v programe yEd Graph Editor[6]. Táto schéma mi pomáhala pri stanovení funkcii systému a vytváraní spoľahlivostných analýz. Schému som vypracoval za pomoci údajov o systéme, schém systému a technickej dokumentácie. Tieto podklady som získal od konštruktérov a od školiteľa z oddelenia analýz v AVA. Schéma znázorňuje mechanickú trasu pozdĺžneho riadenia na ktorú je napojená jednotka PCA, ktorá je stále vo vývoji. Jednotka PCA môže pracovať v dvoch módoch, v tejto kapitole odprezentujem a vysvetlím schému pre MODE 1. Na Obrázku 19 môžeme vidieť schému pozdĺžneho riadenia so všetkými dôležitými komponentami.

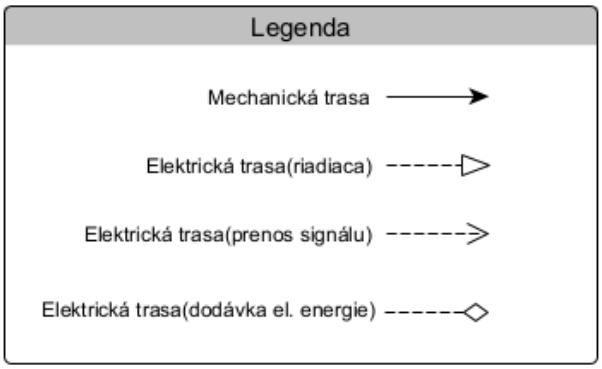
Úplne na vrchu je mechanická trasa, ktorá začína od páky HOTAS až po výškové kormidlo. Tieto bloky majú bielu farbu. Ďalej sa tu nachádzajú bloky so žltou farbou, sú súčasťou jednotky PCA. Všetky bloky, ktoré predstavujú senzory majú farbu oranžovú, tieto senzory odosielajú signál do jednotky ECU alebo FDAU. Ďalšou skupinou sú komponenty, ktoré slúžia na signalizáciu alebo zobrazovanie informácii, bloky týchto komponentov sú v zelenej farbe. Zdroje elektrickej energie sú označené červenou. Modré bloky obsahujú externé systémy dodávajúce hodnotu faktora zaťaženia do jednotky ECU na výpočet cieľovej sily. Modré bloky taktiež obsahujú tabuľky na korekciu pri výpočte cieľovej sily.

[5] https://aldservice.com/Free-MTBF-Calculator.html
[6] https://www.yworks.com/products/yed



Obrázok 19 Schéma pozdĺžneho riadenia L-39 NG

V tejto schéme môžeme vidieť ako sú na sebe jednotlivé komponenty napojené a aká je medzi nimi väzba. Na Obrázku 20 je vysvetlené, čo predstavuje dané spojenie medzi dvoma komponentmi. Prvá relácia vyjadruje, že sa jedná o čisto mechanické napojenie. Napríklad spojenie táhiel, toto spojenie predstavuje mechanickú väzbu medzi komponentami. Druhá relácia predstavuje elektrickú trasu, ktorá slúži na riadenie určitého procesu. Napríklad spojenie medzi ECU a spojkou, jednotka ECU odošle riadiaci signál na zopnutie spojky. Tretia relácia vyjadruje elektrickú trasu, ktorá slúži na prenos signálu. Senzor teploty nameria určitú hodnotu, ktorá je odoslaná do jednotky ECU, teda je prenášaná hodnota teploty. Poslednou reláciou je elektrická trasa slúžiaca na dodávku elektrickej energie. Táto trasa prenáša elektrickú energiu od zdrojov elektrickej energie ku komponentom, ktoré je využívajú.



Obrázok 20 Legenda k schéme pozdĺžneho riadenia

3.2 Výber poloautomatizovaného softvéru

Na vzorke troch poloautomatizovaných softvérov a jedného softvéru použitého vo firme AVA som ukázal ako vyzerá práca v každom z nich a aké výhody prinášajú. Všetky okrem FTA/FMEA toolu fungujú na logike mechanického modelovania stromov porúch v rozhraní jednotlivého softvéru. Automatizácia nastáva až pri počítaní pravdepodobností vrcholových udalostí, kedy konkrétny softvér importuje vopred zadané dáta z databázy a vypočíta pravdepodobnosť vrcholovej udalosti. V tomto kroku FTA/FMEA tool zaostáva a je nutné tieto pravdepodobnosti manuálne vkladať do každého stromu porúch. U týchto zvyšných softvérov navyše funguje kompatibilita s určitými databázami pre dohľadanie alebo dopočítanie pravdepodobnosti zlyhania komponentov, čo v FTA/FMEA toole chýba.

Po dôkladnej analýze všetkých zmienených softvérov a ich inováciách som prišiel k záveru, že pre moju prácu bude najvhodnejší práve FTA/FMEA tool. Hlavným dôvodom je, že softvér dokáže generovať stromy porúch, vďaka čomu má najlepšie predpoklady k doplneniu softvéru o softvérové rozšírenie na automatické vkladanie dát. Stačí vložiť potrebné dáta/údaje a následne tool vygeneruje stromy porúch. Táto inovácia nie je využitá ani v jednom zo skúmaných poloautomatizovaných softvérov a pre ďalšiu automatizáciu je nevyhnutná. Všetky softvéry okrem FTA/FMEA toolu plnia skôr funkciu zjednodušenia a urýchlenia práce pri vytváraní FTA analýzy. Z popisu je jasné, že sa nejedná o úplnú automatizáciu pri vytváraní analýz, ale iba o automatizáciu počítania pravdepodobností a následné generovanie výsledných správ. Vďaka tomuto porovnaniu sa javí použitie FTA/FMEA toolu ako najlepšie riešenie v prípade využitia v tejto práci.

3.3 FHA analýza pozdĺžneho riadenia L-39 NG

V tomto bode sa venujem analýze FHA, táto metóda je dôležitá pri vytváraní analýzy FTA. Analýza slúži na stanovenie funkcií vybraného systému a následné priradenie poruchových stavov priamo k týmto funkciám. Pri stanovení poruchových stavov som postupoval metódou, pri ktorej som každej funkcii, priradil poruchový stav NEFUNGUJE / NEFUNGUJE DOSTATOČNE / FUNGUJE SAMOVOĽNE. Následne tieto poruchové stavy slúžia ako vrcholové udalosti v analýze FTA. Pre každý poruchový stav som dopočítal pravdepodobnosť cez verifikačnú metódu FTA. Po dopočítaní som tieto pravdepodobnosti a kritičnosti posúdil podľa tabuľky Risk Assessment Matrix na vyhodnotenie hodnoty RAC. Zo všetkých 27 poruchových stavov, ktoré som riešil a počítal, vyšiel iba jeden v oranžovej farbe. To znamená, že by sa mal tento poruchový stav zvážiť a prehodnotiť jeho bezpečnosť v systéme. Ostatné poruchové stavy vyšli maximálne do žltej farby, ktorá nepredstavuje výrazné riziko.

Analýzu FHA som vypracovával do vzoru, v ktorom vytvárajú tieto analýzy v AVA. Na Obrázku 21 je možné vidieť zvýraznený poruchový stav, ktorý by mohol vážne ohroziť bezpečnosť letu. Jedná sa o poruchový stav „Výškové kormidlo nereaguje“. Tento stav by mohol byť spôsobený poruchou v mechanickej trase ovládania výškového kormidla. Tým, že sa jedná o čisto mechanickú trasu, tak každá porucha alebo zaseknutie na tejto trase môže znamenať nefunkčnosť ovládania výškového kormidla. Táto porucha nie je ani signalizovaná, ale pilot by to mal pocítiť na páke HOTAS. Keď bude pôsobiť v pozdĺžnom smere na páku, tak lietadlo nebude klopiť.

Funkce		Popis a hodnocení důsledků poruchových stavů								Poznámky	
		Poruchový stav		Signalizácia		Fáze letu	Důsledky poruchového stavu na letoun/ posádku	KritKonst	Pravděp.	RAC	Odkazy na podkladové materiály	Verif. metoda
ID	Popis	ID	Popis	áno/nie								
1	*Podélne riadenie L-39NG*	FC_1										
1.1.	Ovládanie výchylky výškového kormidla	FC_1.1	Výškové kormidlo nereaguje	x		2-7	Strata podélneho ovládania lietadla. Veľmi nebezpečný jav ktorý nie je signalizovaný. Pilot to zistí pocitovo pri pôsobení na HOTAS sa nič nestane. Pilot musí okamžite prerušiť let a pokúsiť sa pristáť.	1	1,23E-04	1D		8
1.1.	Ovládanie výchylky výškového kormidla	FC_1.2	Výškové kormidlo nereaguje dostatočne	x		2-7	Čiastočná strata podélneho ovládania lietadla. Lietadlo nie je schopné plných výchyliek. Pilot to zistí pocitovo pri pôsobení na HOTAS lietadlo nereaguje dostatočne. Pilot musí prerušiť let.	2	6,20E-06	2D		8
1.2.	Ovládanie výchylky výškového kormidla s pomocou PCA (MODE 1)	FC_1.3	Výškové kormidlo nie je možné ovládať pomocou PCA	áno		2-7	Podélne riadenie je bez posilovača riadenia. Pilot môže lietadlo stále ovládať manuálne ale je znížený komfort počas letu. Odpojenie PCA je signalizované na MFD a Master Table. Pilot môže pokračovať v lete pretože nie je priamo ohrozená bezpečnosť letu	4	3,12E-04	4D		8
1.2.	Ovládanie výchylky výškového kormidla s pomocou PCA (MODE 1)	FC_1.4	Výškové kormidlo nie je možné ovládať pomocou PCA	nie		2-7	Podélne riadenie je bez posilovača riadenia. Pilot môže lietadlo stále ovládať manuálne ale je znížený komfort počas letu. Odpojenie PCA nie je signalizované na MFD a ani na Master Table. Pilot to zistí pocitovo pretože musí vynaložiť viac sily.Pilot môže pokračovať v lete pretože nie je priamo ohrozená bezpečnosť letu.	3	3,12E-04	3D		8

Obrázok 21 Ukážka FHA analýzy zobrazujúca 4 z 27 poruchových stavov

3.4 Pravdepodobnosti zlyhania komponentov systému

V tomto bode pracujem s hodnotami, ktoré som následne využil na výpočet pravdepodobností vrcholových udalostí v analýze FTA. Zdroje týchto hodnôt sú od dodávateľov komponentov do AVA, prevádzkových dát L-159 ALCA, odhadov AVA alebo z programu MTBF Calculator. Tabuľku s priradenými hodnotami MTBF nie je možné zverejniť v práci, z dôvodu citlivosti údajov. V prvom rade som vytvoril zoznam najvýznamnejších súčiastok systému pozdĺžneho riadenia, ku každému som priradil poruchu a následne hodnotu MTBF. Hodnota MTBF je skratka pre strednú dobu medzi poruchami po anglicky „Mean Time Between Failure“. Vyjadruje priemerný čas za ktorý nastane porucha. V tejto tabuľke je MTBF vyjadrená v letových hodinách (LH). Táto hodnota je využívaná ako ukazateľ v oblasti spoľahlivosti a využívaná predovšetkým v leteckom priemysle. Vyššia hodnota MTBF značí, že je komponent spoľahlivejší a tým pádom menej poruchovejší. Hodnota MTBF sa vypočíta pomocou rovnice (3). [18]

$$MTBF = \frac{t_P}{n_p} \quad [LH] \qquad \text{(Rovnica 3)}$$

Veličina t_P je prevádzkový čas daného komponentu, zadáva sa väčšinou v letových hodinách (LH). Veličina n_p vyjadruje množstvo porúch počas času prevádzky, jedná sa o bezrozmernú veličinu. Výsledná hodnota MTBF má jednotku LH.

Pri výpočte MTBF sa výsledky výrazne líšili. Medzi niektorými komponentami až viacnásobne. U niektorých komponentov táto hodnota nedosahuje ani hodnotu 10 000 letových hodín.

Je možné skonštatovať, že každý z komponentov s nízkou hodnotou MTBF je vždy buď zálohovaný iným systémom alebo jeho poruchový stav neohrozuje priamo bezpečnosť letu. Elektrický generátor je zálohovaný záložným elektrickým generátorom a ešte aj batériami. Externé systémy, ako sú ADAHRS, LCR-100 a ADC-39 slúžiace na dodávanie hodnôt rýchlosti a faktoru zaťaženia do jednotky ECU, sú vždy zdvojené. Pri zlyhaní obidvoch by sa odpojilo PCA a lietadlo by bolo možné ovládať manuálne. Pri zlyhaní Master tabla zabezpečujúceho Master Caution by boli všetky potrebné signalizácie zobrazené na displeji MFD. Motor trimovacej a kompenzačnej plôšky síce nie je zálohovaný, ale v prípade straty funkcie trimovania alebo kompenzácie síl od vztlakovej mechanizácie by pilot mal síce viacej

práce s riadením lietadla, ale nejednalo by sa o stav priamo ohrozujúci bezpečnosť letu. Každopádne by bolo potrebné zamyslieť sa nad spoľahlivosťou motoru trimovacej a kompenzačnej plôšky, pretože jeho hodnota MTBF je veľmi nízka.

Následne sa hodnota MTBF prepočíta na pravdepodobnosť zlyhania vybraného komponentu. Tento výpočet je dôležitý pre zadávanie pravdepodobností do stromov porúch FTA analýzy. Pravdepodobnosť zlyhania sa z hodnoty MTBF prepočíta nasledovne pomocou rovnice (4).

$$P = \frac{1}{MTBF} \qquad \text{(Rovnica 4)}$$

Veličina P je pravdepodobnosť zlyhania komponentu a hodnota $MTBF$ je zadaná vo forme času, väčšinou vo forme letových hodín (LH).

Tieto vypočítané hodnoty sa priamo zadávajú do stromov porúch FTA analýzy, aby sa vypočítali pravdepodobnosti vrcholových udalostí analýzy FTA.

3.5 FTA analýza pozdĺžneho riadenia L-39 NG

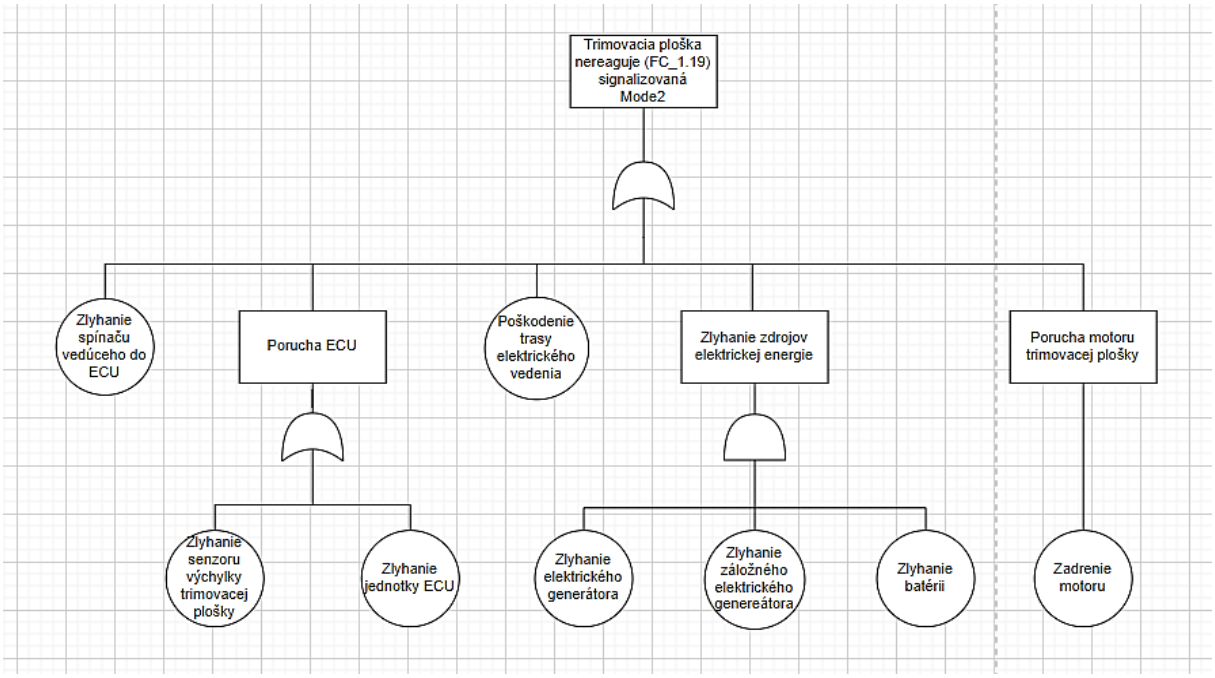
Po určení všetkých poruchových stavov v analýze FHA bolo možné pustiť sa do analýzy FTA. Poruchových stavov, ktoré vyplynuli z FHA analýzy bolo 27. Pre každý poruchový stav, bolo potrebné vytvoriť strom porúch. Po dôkladnom porovnaní dostupných softvérových riešení bolo mojou úlohou vytvorenie FTA analýzy za pomoci automatizovanej metódy cez FTA/FMEA tool. Keďže FTA/FMEA tool generuje stromy porúch automaticky po zadaní vstupných parametrov a je v prototypovej verzii, rozhodol som sa overiť tieto výstupy pomocou manuálne vypracovanej FTA analýzy. Keďže sa stále jedná o prototyp, počas práce bolo niekedy nutné riešiť jeho nestabilné chovanie, ale s týmto správaním je nutné počítať. Analýzy som vytvoril v programe DRAW.io[7], v ktorom je možné tieto analýzy modelovať a zároveň je bezplatný. Analýzu FTA som vypracoval pre celý systém pozdĺžneho riadenia lietadla. Po vytvorení všetkých stromov porúch môžeme začať vytvárať FTA analýzu automatizovaným softvérom FTA/FMEA toolom. Po vygenerovaní stromov porúch bolo možné skontrolovať správnosť výstupu pomocou manuálne vytvoreného stromu prislúchajúcemu tomu vygenerovanému. Je jasné, že každý program má iné rozhranie, takže nie vždy to vyzeralo identicky. Po vygenerovaní a porovnaní všetkých 27 stromov porúch som prišiel k záveru, že FTA/FMEA tool generuje stromy naozaj správne a pre väčšinu pokusov boli tieto stromy identické. Akurát môže nastať problém, ak pri zadávaní informácii o systéme do softvéru dôjde k chybe zo strany užívateľa. Vtedy môže prísť k chybne vygenerovanému stromu porúch a ak nemáme na porovnanie strom porúch FTA analýzy vytvorený manuálne, je možné túto chybu prehliadnuť.

Po porovnaní výstupov z dvoch odlišných zdrojov vytvárania FTA analýz, je možné využiť vopred vypočítané hodnoty pravdepodobností zlyhania komponentov. Tieto hodnoty nám poslúžia na výpočet vrcholových udalostí, ktoré predstavujú ekvivalent poruchovým stavom určených pomocou FHA analýzy, vďaka ktorej je možné následne určiť úroveň spoľahlivosti systému.

Z dôvodu veľkého množstva poruchových stavov ukážem v tejto kapitole na porovnanie iba jeden z nich, ukážku 5 z 27 poruchových stromov vytvorených v FTA/FMEA toole, ktoré sú totožné s tými manuálne vytvorenými, prikladám v Prílohe 1. Na Obrázku 22 je možné vidieť analýzu FTA pre poruchový stav „Trimovacia plôška nereaguje“. Tento strom porúch nám ukazuje, že aby nastala vrcholová udalosť stačí aby zlyhala jedná z vetví, takže je vrcholová udalosť závislá na každom z uvedených systémov. Či už by sa jednalo o zlyhanie spínaču pre

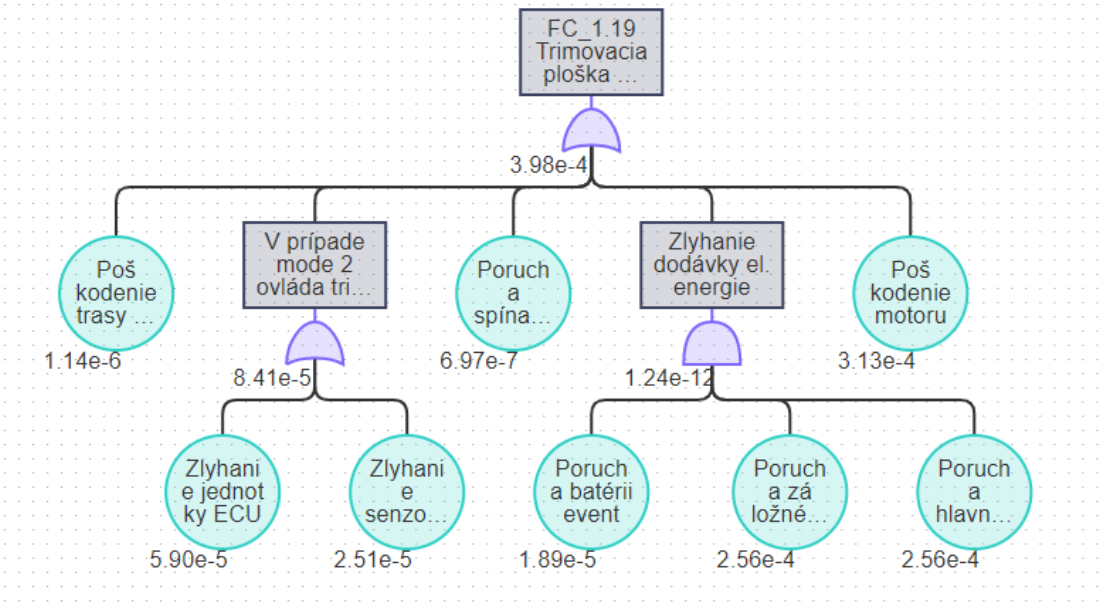
[7] https://app.diagrams.net/

jednotku ECU, jednotku ECU, trasu elektrického vedenia, zdroja elektrickej energie alebo poruchy motoru trimovacej plôšky, vždy by to malo za následok zlyhanie vrcholovej funkcie. Naopak pri zdrojoch elektrickej energie môžeme vidieť, že aby nastala udalosť zlyhanie zdrojov elektrickej energie musí zlyhať každý z jej komponentov, inak sa táto vetva neberie ako poruchová.



Obrázok 22 Strom porúch FTA analýzy vytvorený manuálne

Na Obrázku 23 môžeme vidieť vygenerovaný strom pre tú istú vrcholovú funkciu ako na Obrázku 22. Jediný rozdiel je, že na obrázku nie je možné prečítať názvy porúch a poruchových stavov. Je možné vidieť, že daný poruchový stav už má dopočítanú hodnotu pravdepodobnosti vrcholovej udalosti, ktorá sa zadá do FHA analýzy. Môžeme teda skonštatovať, že FTA/FMEA tool generuje stromy porúch správne, čo sme dokázali aj na vzorke 27 stromov porúch. Ukážku 5 z 27 poruchových stromov vygenerovaných v FTA/FMEA toole prikladám v Prílohe 1.



Obrázok 23 Strom porúch FTA analýzy vygenerovaný pomocou FTA/FMEA toolu

Na Obrázku 23 môžeme vidieť vyplnené pravdepodobnosti zlyhaní elementárnych komponentov a následne vypočítanú hodnotu pravdepodobnosti vrcholovej udalosti FC_1.19. Tieto čísla vyjadrujú pravdepodobnosť zlyhania daného komponentu.

4. Návrh možností a postupov automatického vkladania dát

Vďaka tejto práci sa potvrdilo, že je na automatizáciu možné využiť FTA/FMEA tool. Vyplýva to z porovnania FTA analýz, vytvorených manuálnym spôsobom a automatizovaným spôsobom pomocou FTA/FMEA toolu. Pre porovnanie sme mali 27 vzoriek poruchových stromov FTA analýzy. Môžeme povedať, že tieto poruchové stromy boli identické a teda vygenerované poruchové stromy z FTA/FMEA toolu splnili očakávania. Vďaka tomuto zisteniu je možné rozmýšľať nad pridaním automatizácie vkladania dát priamo do FTA/FMEA toolu, čím by sa stala z FTA/FMEA toolu plne automatizovaná metóda na vypracovávanie FTA analýz.

Čas potrebný pre vytvorenie FTA analýzy pomocou FTA/FMEA toolu sa skoro vyrovná s časom potrebným pri súčasných postupoch vypracovávania analýz FTA vo firme AVA. Tento fakt som overil pri vypracovávaní FTA analýzy pomocou manuálnej metódy a následnom vypracovaní FTA analýzy s pomocou FTA/FMEA toolu. Vypracovanie všetkých stromov porúch vytvorených manuálne mi zabralo zhruba 50 hodín, čo je niečo viac ako vyplnenie všetkých údajov do FTA/FMEA toolu pre vygenerovanie stromov porúch, ktoré mi zabralo okolo 45 hodín. Následné počítanie výsledných pravdepodobností je v prípade FTA/FMEA toolu automatické, po zadaní všetkých pravdepodobností zlyhaní elementárnych komponentov. V prípade manuálneho postupu je nutné všetky výpočty prevádzať ručne. Zautomatizovaním tohoto kroku sa ušetrí veľmi veľké množstvo času a predíde sa možnej chybe pri počítaní. Treba ale spomenúť, že túto automatizáciu má aj softvér využívaný vo firme AVA, presnejšie RAM Commander, ktorý som ja ale nemal k dispozícii. Výhodou softvéru RAM Commander využívaného vo firme Aero Vodochody je, že umožňuje vytvoriť databázu všetkých komponentov systému, kde sa zadávajú pravdepodobnosti a následne sú automaticky importované do stromov porúch. Táto vymoženosť sa v FTA/FMEA toole nevyskytuje a je nutné tieto pravdepodobnosti zadávať do každého stromu porúch zvlášť. Kvôli tomu, že sa v FTA/FMEA toole nenachádza databáza všetkých komponentov, tak sa čas potrebný na vytvorenie celkovej analýzy v softvéri RAM Commander a v softvéri FTA/FMEA toole približne vyrovná. Vďaka tomuto zisteniu a porovnaniu týchto postupov vyplýva, že vo firme AVA by bolo potrebné skôr zaradiť plnoautomatizovanú metódu na vytváranie FTA analýz, aby sa ušetrilo väčšie množstvo času a zmena postupov analytikov mala väčší a opodstatnený význam.

Základnou predstavou firmy Aero Vodochody, kvôli ktorej bola táto bakalárska práca vypracovaná je, aby dokázal vybraný softvér automaticky čítať Technické zadania (TZ) a Technické podmienky (TP) a aby dokázal porozumieť funkciám daného systému, interakciám medzi nimi a aby bolo možné po načítaní týchto údajov automaticky vygenerovať stromy porúch FTA analýzy. Toto riešenie si vyžiadala postupná zmena súčasných trendov vo svete a zavádzanie automatizácie do všetkých druhov analýz, aby sa ušetril čas a v najlepšom prípade znížilo množstvo ľudí, ktorý na danej analýze budú pracovať. V prípade, že by sa používal FTA/FMEA tool do ktorého by sme chceli zaviesť túto automatizáciu, bude nutné zaviesť niektoré zmeny. Dôležitou úlohou je vytvorenie univerzálnych Technických podmienok (TP) a Technických zadaní (TZ), aby tool dokázal týmto dokumentom porozumieť.

Súčasná technická dokumentácia je súbor viacerých dokumentov a technických nákresov daného lietadla alebo systému, v ktorej je popísaná funkcia systému. Aby bolo možné previesť technickú dokumentáciu do určitého softvéru, bolo by potrebné previesť funkcie systému a jeho komponenty do jedného z modelovacích jazykov. V tomto modelovacom jazyku by bolo možné tieto komponenty a ich funkcie namodelovať ako model celého systému, vďaka čomu by bolo možné tieto údaje o systéme previesť do vybraného softvéru.

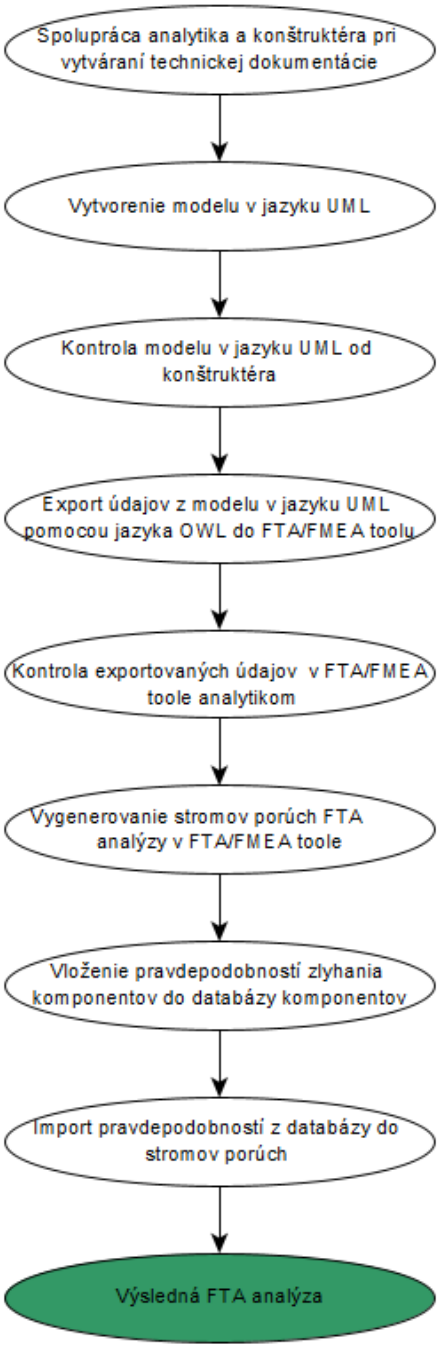
Na tento krok by sa mohol použiť napríklad unifikovaný jazyk UML (Unified Modeling Language) [19]. Tento unifikovaný jazyk slúži pre vizuálne modelovanie vybraného systému. UML pomáha k prehľadnému zobrazeniu štruktúry systému a vyjadreniu jeho funkcii. Týmto spôsobom by bolo možné previesť celý systém do logického modelu, ktorý by dokázal pochopiť či už konštruktér, ktorý daný systém vymyslel ale aj programátor, ktorý bude vytvárať rozšírenie na automatizáciu vkladania dát.

Aby bolo možné technickú dokumentáciu automatizovať, je nutné zaviesť model celého lietadla alebo systému namodelovaného v unifikovanom jazyku UML, ktorý by bol súčasťou technickej dokumentácie. Po vytvorení modelu systému v jazyku UML by bolo potrebné tieto údaje z modelu previesť priamo do softvéru, ktorý bude ďalej s týmito údajmi pracovať. V tomto kroku sa pracuje s MBSE (Model-Based System Engineering), kedy je možné technické dokumenty nahradiť modelom, napríklad v jazyku UML, v ktorom sa vyskytujú všetky dôležité informácie využiteľné pre spoľahlivostné analýzy. Na krok prenosu údajov z modelu v jazyku UML do softvéru by bolo možné využiť jeden zo softvérov pracujúcich s OWL (Ontology Web Language) [20]. Jazyk OWL poskytuje možnosť exportovania údajov o systéme z modelu v jazyku UML do vybraného softvéru. Vďaka prevedeniu modelu do jazyku OWL by bolo možné tieto údaje o systéme vložiť priamo do FTA/FMEA toolu.

Zároveň by bolo potrebné analytikov z oddelenia analýz preškoliť, aby sa špecializovali na vytváranie modelov lietadiel a systémov v jazyku UML v spolupráci s konštruktérom. Vďaka tejto zmene v oddelení analýz by vznikla priamo technická dokumentácia obohatená o model v jazyku UML a súčasne by analytik spolupracujúci s konštruktérom dôkladne porozumel danému systému. Takže analytici pracujúci s týmto toolom by boli oveľa viac spojení s konštruktérmi a chápali funkciám celého systému. V prípade určitých nejasností ohľadne modelu v jazyku UML by mohol analytik kontrolovať tento model priamo s konštruktérom. Tento krok je zrozumiteľnejší ako vytváranie modelov lietadla v jazyku UML priamo od konštruktérov, hlavne z dôvodu, že by sa musela zaviesť kompletná zmena spôsobov, ako by mali vyzerať technické schémy a nákresy v technickej dokumentácii. Ďalej by nebolo možné všetky informácie o systéme vložiť do modelu v jazyku UML. Súčasne by bolo žiadané zaviesť univerzálnu verziu technickej dokumentácie, kde by sa používalo rovnaké písmo, jazyk a logika vypracovávania, aby bola technická dokumentácia v jednotnom formáte. Konštruktéri budú vytvárať upravenú technickú dokumentáciu v jednotnom formáte a budú spolupracovať s analytikmi. Táto technická dokumentácia obohatená o model v jazyku UML a následnom prevedení pomocou jazyku OWL, by mala tvoriť dostatočný základ pre automatizáciu vkladania dát o systéme do FTA/FMEA toolu. Aby táto automatizácia mala zmysel muselo by sa zaviesť, aby každý dodávateľ komponentov alebo leteckých systémov do firmy AVA začal využívať už spomínanú univerzálnu verziu technickej dokumentácie, ktorá bude doplnená o model v unifikovanom jazyku UML. Model bude vytvorený v dodávateľskej firme analytikom, ktorý by spolupracoval s konštruktérom pri vytváraní technickej dokumentácie. Vďaka zavedeniu vytvárania modelov v jazyku UML v dodávateľských firmách by sa ušetril čas analytikov v AVA tým, že by nemuseli dodatočne vytvárať model v jazyku UML na systém pri ktorom nespolupracovali s konštruktérom.

Aby sa jednalo o plnú automatizáciu spoľahlivostnej analýzy, bolo by nutné zaviesť databázu komponentov využitých v systéme lietadla. Do tejto databázy komponentov by sa vkladali pravdepodobnosti zlyhaní všetkých komponentov a tým pádom by sa tieto pravdepodobnosti automaticky importovali do stromov porúch. Taktiež by bolo možné túto úpravu ešte vylepšiť pridaním databázy pre výpočet MTBF priamo do FTA/FMEA toolu, vďaka čomu by bolo oveľa jednoduchšie nájsť pravdepodobnosti zlyhania daného komponentu priamo v toole. Keďže táto databáza na výpočet MTBF umožňuje zadať presné podmienky využitia daného komponentu a nastaviť aj prostredie v ktorom sa využíva, vďaka čomu sa jedná o veľmi presnú metódu na určenie pravdepodobnosti zlyhania komponentu v špecifických podmienkach. Týmto krokom by sa uľahčilo zadávanie pravdepodobností do každého stromu porúch zvlášť

a následne po vygenerovaní stromov porúch by sa automaticky dopočítala pravdepodobnosť vrcholových udalostí každého stromu porúch.



Obrázok 24 Návrh postupov automatizovanej FTA analýzy vo firme AVA

Na Obrázku 24 navrhujem postupy ako by bolo možné zaviesť automatizáciu vkladania údajov o systéme do FTA/FMEA toolu. Tento postup by mohlo byť možné priamo aplikovať vo firme Aero Vodochody.

V prípade, že by kontrola konštruktéra nebola uspokojivá, bude potrebné model v jazyku ešte raz prediskutovať s konštruktérom, ktorý môže vydať odporúčanie na zmenu alebo pridanie určitého elementu. Ak by nastala nezhoda exportovaných údajov do FTA/FMEA toolu, bude potrebné aby analytik zistil, prečo sa tak stalo a doplnil chýbajúcu alebo zmenil nepravdivú informáciu. Následne po oprave môže analýza pokračovať podľa stanovených krokov (Obrázok 24).

5. Diskusia

Použitý softvér FTA/FMEA tool generuje stromy porúch automaticky po zadaní vstupných parametrov. S ohľadom na fakt, že sa jedná o prototyp boli výstupy, stromy porúch, porovnávané s výstupmi manuálne vypracovanej FTA analýzy. Potvrdila sa vysoká zhoda výstupov automatického a konvenčného postupu vytvárania FTA analýzy. FTA/FMEA tool je perspektívnym nástrojom na plnú automatizáciu FTA analýzy. Čiastočnú nestabilitu softvéru je potrebné doladiť, aby fungoval bez problémov. Po odstránení menších problémov sa FTA/FMEA tool stane plne funkčným softvérom s budúcou víziou pre plne automatizované vypracovávanie FTA analýz. Porovnaním automatizovaného postupu s manuálnym postupom spoľahlivostných analýz bol splnený jeden z cieľov práce.

Uplatnenie FTA/FMEA toolu v súčasnom stave prináša určité ušetrenie času pri vytváraní FTA analýzy. Čas potrebný pre spracovanie analýzy nemá však výrazný efekt, v prospech toolu, v porovnaní s manuálnym postupom. S využitím dát od spoločnosti AVA bolo vypracovanie všetkých stromov porúch vytvorených manuálne o málo časovo dlhšie, ako vyplnenie všetkých údajov do FTA/FMEA toolu pre vygenerovanie stromov porúch. Počítanie výsledných pravdepodobností je v prípade FTA/FMEA toolu automatické po zadaní všetkých pravdepodobností zlyhaní elementárnych komponentov. V prípade manuálneho postupu je nutné všetky výpočty prevádzať ručne. Zautomatizovaním tohoto kroku sa ušetrí čas niekoľkonásobne. Treba ale spomenúť, že túto automatizáciu má aj softvér využívaný vo firme AVA presnejšie RAM Commander, ktorý som ja ale nemal k dispozícii. S ohľadom na skutočnosť, že v FTA/FMEA toole nie je databáza všetkých komponentov, tak sa čas, potrebný na vytvorenie celkovej analýzy v softvéri RAM Commander približne vyrovná času vytvárania analýzy v softvéri FTA/FMEA tool. Pre AVA je odporučené uplatnenie plnoautomatizovanej metódy na vytváranie FTA analýz.

Predovšetkým, aby vybraný softvér dokázal automaticky porozumieť Technickým zadaniam (TZ) a Technickým podmienkam (TP), musí porozumieť funkciám daného systému a interakciám medzi nimi. Na automatizáciu zberu technickej dokumentácie je potrebné vytvoriť model lietadla v jazyku UML. Softvér vytvorený na báze OWL (Ontology Web Language) dokáže exportovať dáta z modelu v jazyku UML do požadovaného softvéru. Je teda nutné zaviesť model celého lietadla alebo systému namodelovaného v unifikovanom jazyku UML ako súčasť technickej dokumentácie. Model lietadla v unifikovanom jazyku UML v sebe má všetky dôležité informácie ako sú interakcie medzi komponentami a funkcie. Návrh

automatizovaného systému je náročný na prípravu a spracovanie podkladových dát, ale v konečnom dôsledku prináša efekt v úspore času. Zaradenie automatizácie spoľahlivostných analýz vo vývoji vojenských lietadiel je nevyhnutný krok v rozvoji spoľahlivostných analýz. Rozhodne prispeje k zvýšeniu efektívnosti práce konštruktérov a analytikov.

Ciele práce boli splnené, stanovili sa postupy pre automatizovanú spoľahlivostnú analýzu v rámci vývoja a výroby vojenských lietadiel s pomocou metód FTA a FHA, porovnala sa automatizovaná spoľahlivostná analýza s manuálnou spoľahlivostnou analýzou, navrhlo sa využitie modelu v jazyku UML prevedené pomocou softvéru pracujúceho pomocou jazyku OWL do softvéru FTA/FMEA toolu. Potvrdila sa myšlienka, že automatizované spoľahlivostné analýzy v rámci vývoja a výroby vojenských lietadiel sú efektívny nástroj pri vývoji nielen vojenských lietadiel.

6. Záver

Medzi obmedzenia spoľahlivostných analýz vo vývoji vojenských lietadiel patria častokrát neúplné dáta, použitie predpokladov alebo odhadov, veľká časová záťaž a nedostatočná automatizácia. S čiastočnou automatizáciou pracujú viaceré systémy, jedným z nich je poloautomatický FTA/FMEA tool, ktorý vygeneruje stromy porúch FTA analýzy a vypočíta pravdepodobnosť zlyhania vrcholových udalostí. FTA/FMEA tool, s ohľadom na jeho menšiu stabilitu, bol porovnávaný s výstupmi manuálne vypracovanej FTA analýzy. Potvrdila sa vysoká zhoda výstupov automatického a manuálneho vypracovania spoľahlivostnej analýzy. FTA/FMEA tool je perspektívnym nástrojom na automatizáciu spoľahlivostnej analýzy. Ďalšou výhodou uplatnenia FTA/FMEA toolu je možnosť ušetrenia času pri tvorbe spoľahlivostnej analýzy. Čas potrebný na vytvorenie stromov porúch nemá výrazný efekt v prospech FTA/FMEA toolu v porovnaní s manuálnou prípravou. Na podklade dát od spoločnosti AVA bola vypracovaná FTA analýza manuálnou metódou a následne FTA analýza pomocou FTA/FMEA toolu. Vytvorenie všetkých stromov porúch manuálne trvalo len o niečo dlhšie (50 hodín), ako vyplnenie všetkých údajov do FTA/FMEA toolu (45 hodín). Následne FTA/FMEA tool po zadaní pravdepodobností zlyhania komponentov automaticky vypočíta pravdepodobnosť vrcholových udalostí. Zautomatizovaním tohoto kroku sa ušetrí čas niekoľkonásobne. Treba ale spomenúť, že túto automatizáciu má aj softvér využívaný vo firme AVA, presnejšie RAM Commander, ktorý som ja ale nemal k dispozícii. S ohľadom na skutočnosť, že v FTA/FMEA toole nie je databáza všetkých komponentov, tak sa čas, potrebný na vytvorenie celkovej analýzy v softvéri RAM Commander a v softvéri FTA/FMEA tool približne vyrovná. Pre AVA je odporučené uplatnenie plnoautomatizovanej metódy na vytváranie FTA analýz. Na automatizáciu zberu dát do FTA/FMEA toolu je potrebné vytvoriť model v jazyku UML a následne pomocou softvéru pracujúceho s jazykom OWL tieto údaje exportovať do FTA/FMEA toolu. Automatizácia spoľahlivostných analýz vo vývoji vojenských lietadiel je nevyhnutný krok k zvýšeniu ich efektivity.

Víziou do budúcnosti je prepojenie navrhnutých postupov a ich zaradenie do praxe vo firme Aero Vodochody. Výber softvéru pracujúceho s jazykom OWL bude otázkou pokračovania vo výskume po tejto práci, kde bude potrebné vybrať a odskúšať, ktorý softvér bude na export dát z modelu v unifikovanom jazyku, ako je napríklad jazyk UML, do FTA/FMEA toolu najlepší. Po vyriešení tohto problému bude možné tieto znalosti a postupy prepojiť a vytvoriť softvér s automatizovaným vkladaním údajov.

7. Zoznam použitej literatúry

[1] VINTR, Zdeněk. *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*. Praha: Česká společnost pro jakost, 2009. ISBN ISBN978-80-02-02156-8.

[2] *ČSN EN IEC 60812 ed. 2 (010675): Analýza způsobů a důsledků poruch (FMEA a FMECA)*. 2019.

[3] *Rozdiely medzi analýzami ETA a FTA: Allison Lynch* [online]. [cit. 2023-07-15]. Dostupné z: https://www.edrawsoft.com/difference-faulttree-eventtree.html

[4] *Accelerated Quality and Reliability Solutions: BASIC CONCEPTS OF SAFETY RISK ASSESSMENT*. Lev M. Klyatis and Eugene L. Klyatis, 2006, pages 413-469. ISBN 978-0-08-044924-1.

[5] *ČSN EN 61025 (010676): Analýza stromu poruchových stavů (FTA)*. 2007.

[6] *Reliability block diagram: James Kovacevic* [online]. 2017 [cit. 2023-07-15]. Dostupné z: https://hpreliability.com/understanding-reliability-block-diagrams/

[7] *Aero Vodochody* [online]. 2023 [cit. 2023-07-11]. Dostupné z: https://www.aero.cz/l-39ng/

[8] *L-39 NG* [online]. 2020 [cit. 2023-07-11]. Dostupné z: https://www.armadninoviny.cz/letoun-l-39ng-otevrel-letovou-obalku.html

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

[10] *Technical Requirements: TZL39001-20-EN-X Pitch Control Actuator for the L-39NG Aircraft*. AERO Vodochody AEROSPACE a.s., Sheets: 36.

[11] CASTET, Jean-Francois, Magdy BAREH, Jeffery NUNES, Shira OKON, Larry GARNER, Emmy CHACKO a Michel IZYGON. Failure analysis and products in a model-based environment. *2018 IEEE Aerospace Conference*. IEEE, 2018, 1-13. ISBN 978-1-5386-2014-4. Dostupné z: doi:10.1109/AERO.2018.8396736

[12] *MIL-STD-882E*. DEPARTMENT OF DEFENSE USA, máj 2012. Dostupné také z: https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf

[13] RUIJTERS, Enno a Mariëlle STOELINGA. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review* [online]. 2015, **15-16**, 29-62 [cit. 2023-07-11]. ISSN 15740137. Dostupné z: doi:10.1016/j.cosrev.2015.03.001

[14] VESELY, Dr. William. NASA. *Fault tree handbook with Aerospace applications*. Washington. DC, August 2002. Dostupné také z: http://www.mwftr.com/CS2/Fault%20Tree%20Handbook_NASA.pdf

[15] *RAM Commander* [online]. ALD Software [cit. 2023-07-11]. Dostupné z: https://www.aldsoftware.com/download/ramc/UserManual/html/index.html?welcome_to_ram_commander.htm

[16] *Fault Tree: Isograph* [online]. In: . [cit. 2023-07-21]. Dostupné z: https://www.isograph.com/blog/faulttree-friday-2/

[17] *Ukážka FTA: Relyence* [online]. In: . [cit. 2023-07-21]. Dostupné z: https://relyence.com/products/fault-tree/risk-analysis/

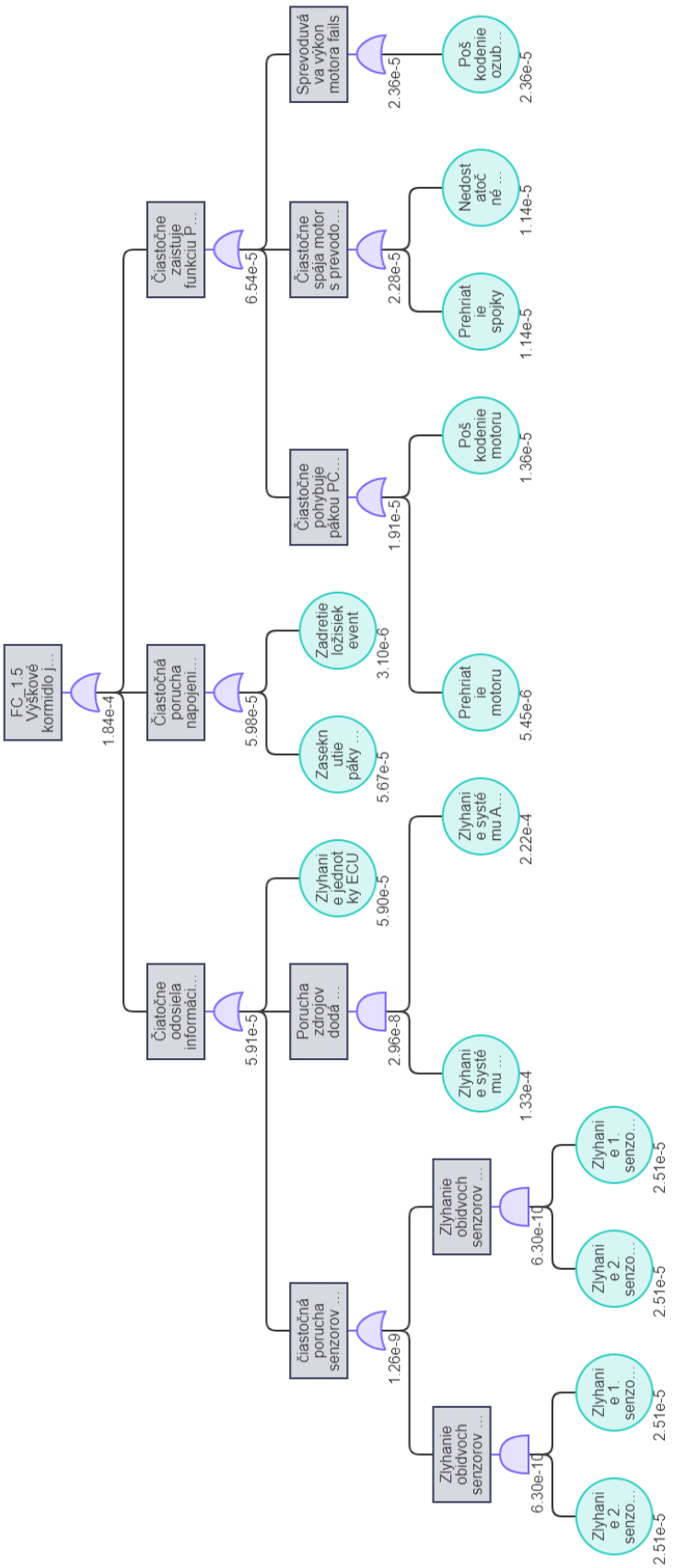
[18] TORELL, Wendy. *Střední doba mezi poruchami: vysvětlení a standardy* [online]. [cit. 2023-07-13]. Dostupné z: http://gabben.wbs.cz/mtbf1.pdf

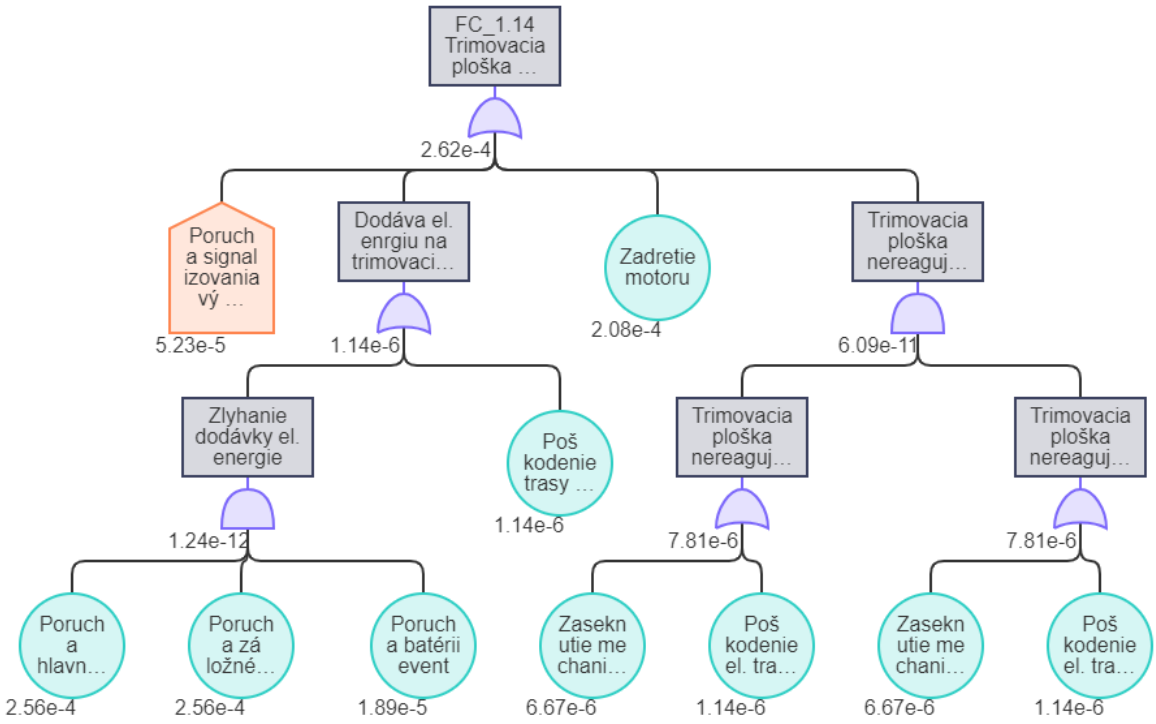
[19] Russ Miles a Kim Hamilton. *Learning UML 2.0*. Unified Modeling Language, O'Reilly Media, April 2006. ISBN 9780596009823.

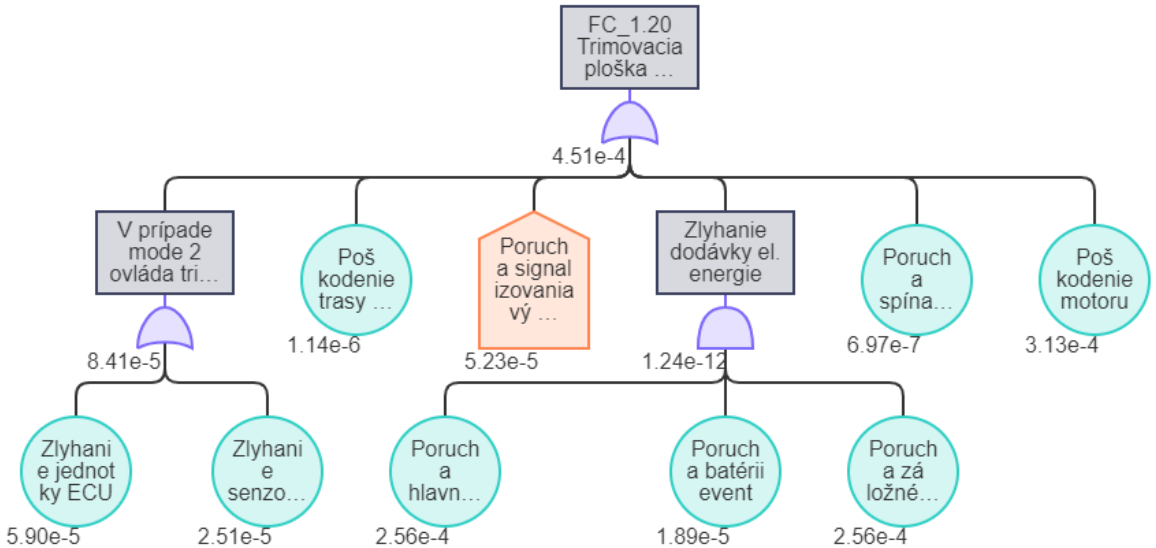
[20] Antoniou, G., van Harmelen, F. *Web Ontology Language: OWL. In: Staab, S., Studer, R. (eds) Handbook on Ontologies. International Handbooks on Information Systems*. Springer, Berlin, Heidelberg., 2004. ISBN 978-3-540-24750-0. Dostupné z: doi:https://doi.org/10.1007/978-3-540-24750-0_4

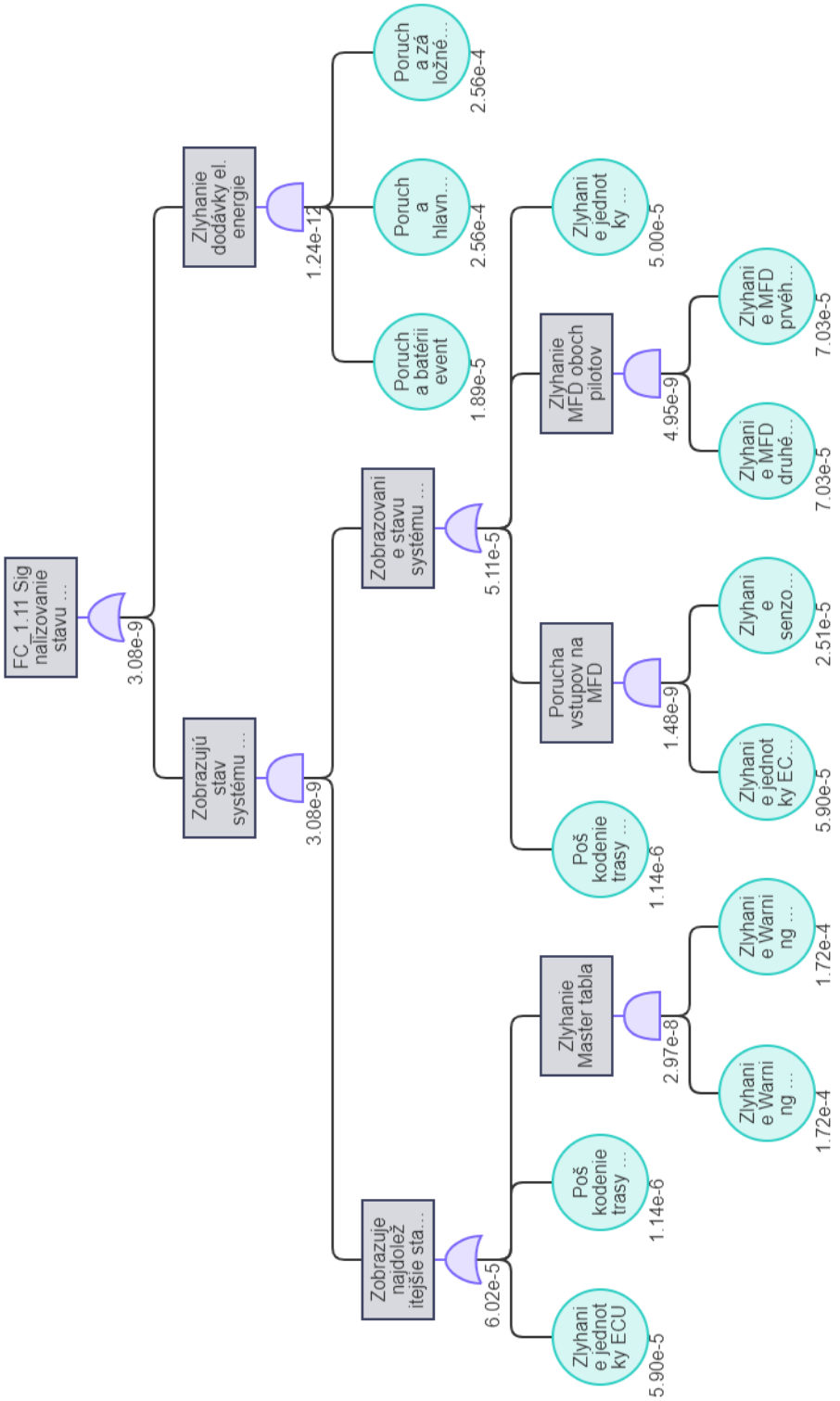
[21] FERRIERE, Richard. *Schéma L-39 Albatros* [online]. [cit. 2023-07-13]. Dostupné z: https://www.the-blueprints.com/blueprints/modernplanes/modern-aa-an/46766/view/aero_l-39_albatros/

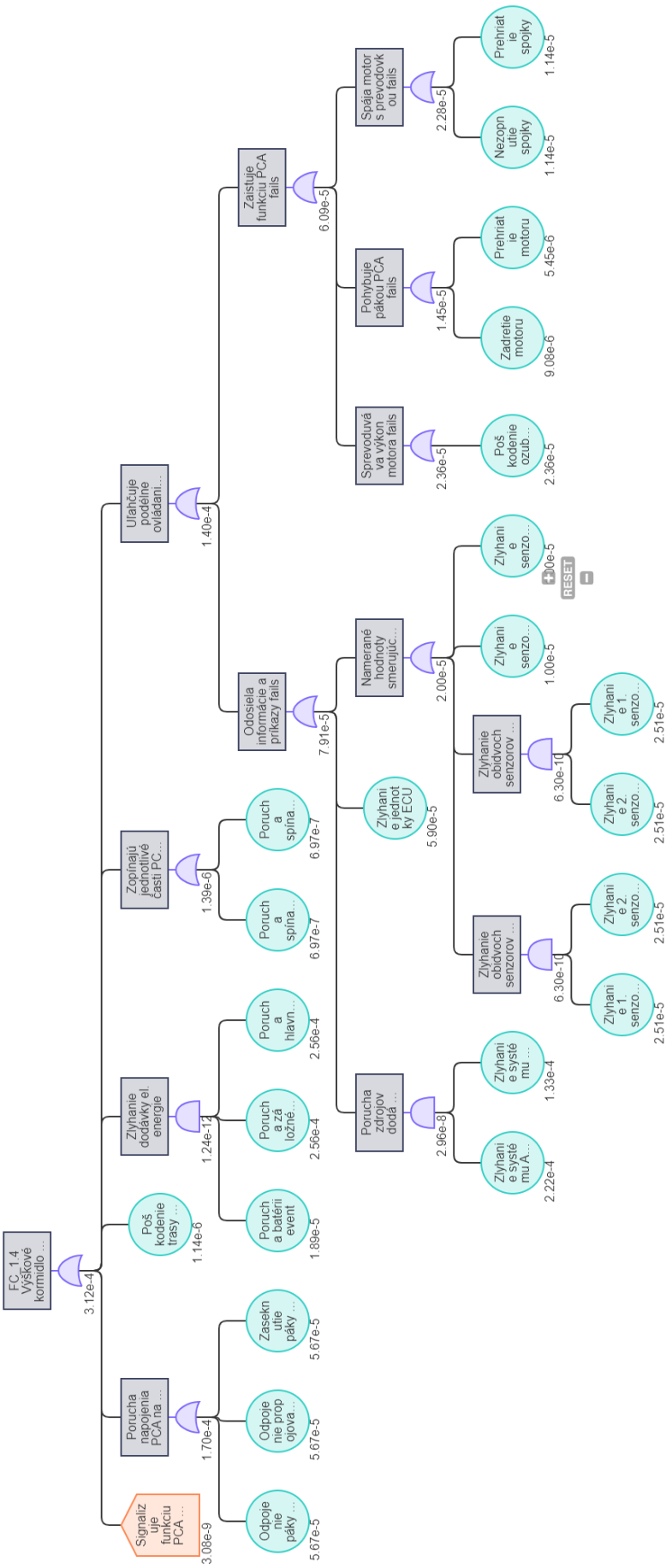
8. Príloha 1


FC_1.5 Výškové kormidlo j...
1.84e-4
Čiatočne odosiela informáci...
5.91e-5
Čiastočná porucha napojeni...
5.98e-5
Čiastočne zaistuje funkciu P...
6.54e-5
Porucha zdrojov dodá ...
2.96e-8
Zlyhanie jednotky ECU
5.90e-5
Zasekn utie páky ...
5.67e-5
Zadretie ložisiek event
3.10e-6
Čiastočne ponybuje pákou PC...
1.91e-5
Čiastočne spája motor s prevodo...
2.28e-5
Sprevoduvá va výkon motora fails
2.36e-5
Zlyhani e systé mu ...
1.33e-4
Zlyhani e systé mu A...
2.22e-4
Prehriat ie motoru
5.45e-6
Poš kodenie motoru
1.36e-5
Prehriat ie spojky
1.14e-5
Nedost atoč né ...
1.14e-5
Poš kodenie ozub...
2.36e-5
čiastočná porucha senzorov ...
1.26e-9
Zlyhanie obidvoch senzorov ...
6.30e-10
Zlyhanie obidvoch senzorov ...
6.30e-10
Zlyhani e 1. senzo...
2.51e-5
Zlyhani e 2. senzo...
2.51e-5
Zlyhani e 1. senzo...
2.51e-5
Zlyhani e 2. senzo...
2.51e-5


FC_1.14 Trimovacia ploška ...
2.62e-4
Poruch a signal izovania vý ...
5.23e-5
Dodáva el. enrgiu na trimovaci...
1.14e-6
Zadretie motoru
2.08e-4
Trimovacia ploška nereaguj...
6.09e-11
Zlyhanie dodávky el. energie
1.24e-12
Poš kodenie trasy ...
1.14e-6
Trimovacia ploška nereaguj...
7.81e-6
Trimovacia ploška nereaguj...
7.81e-6
Poruch a hlavn...
2.56e-4
Poruch a zá ložné...
2.56e-4
Poruch a batérii event
1.89e-5
Zasekn utie me chani...
6.67e-6
Poš kodenie el. tra...
1.14e-6
Zasekn utie me chani...
6.67e-6
Poš kodenie el. tra...
1.14e-6


FC_1.20 Trimovacia ploška ...
4.51e-4
V prípade mode 2 ovláda tri...
8.41e-5
Poš kodenie trasy ...
1.14e-6
Poruch a signal izovania vý ...
5.23e-5
Zlyhanie dodávky el. energie
1.24e-12
Poruch a spína...
6.97e-7
Poš kodenie motoru
3.13e-4
Zlyhani e jednot ky ECU
5.90e-5
Zlyhani e senzo...
2.51e-5
Poruch a hlavn...
2.56e-4
Poruch a batérii event
1.89e-5
Poruch a zá ložné...
2.56e-4


FC_1.11 Sig nalizovanie stavu ...
3.08e-9
Zlyhanie dodávky el. energie
1.24e-12
Poruch a zá ložné...
2.56e-4
Poruch a hlavn...
2.56e-4
Poruch a batérii event
1.89e-5
Zobrazujú stav systému ...
3.08e-9
Zobrazovani e stavu systému ...
5.11e-5
Zlyhani e jednot ky ...
5.00e-5
Zlyhanie MFD oboch pilotov
4.95e-9
Zlyhani e MFD prvéh...
7.03e-5
Zlyhani e MFD druhé...
7.03e-5
Porucha vstupov na MFD
1.48e-9
Zlyhani e senzo...
2.51e-5
Zlyhani e jednot ky EC...
5.90e-5
Poš. kodenie trasy ...
1.14e-6
Zobrazuje najdoležitejšie sta...
6.02e-5
Zlyhanie Master tábla
2.97e-8
Zlyhani e Warni ng ...
1.72e-4
Zlyhani e Warni ng ...
1.72e-4
Poš kodenie trasy ...
1.14e-6
Zlyhani e jednot ky ECU
5.90e-5


FC 1.4 Výškové kormidlo ...
3.12e-4
Signalizuje funkciu PCA ...
3.08e-9
Odpojenie páky ...
5.67e-5
Porucha napojenia PCA na ...
1.70e-4
Odpojenie prop ojova...
5.67e-5
Zasekn utie páky ...
5.67e-5
Poš kodenie trasy ...
1.14e-6
Zlyhanie dodávky el. energie
1.24e-12
Poruch a batérii event
1.89e-5
Poruch a zá ložně...
2.56e-4
Poruch a hlavn...
2.56e-4
Zopínajú jednotlivé časti PC...
1.39e-6
Poruch a spína...
6.97e-7
Poruch a spína...
6.97e-7
Uľahčuje podelne ovládani...
1.40e-4
Odosiela informácie a príkazy fails
7.91e-5
Porucha zdrojov dodá ...
2.96e-8
Zlyhani e systé mu A...
2.22e-4
Zlyhani e systé mu ...
1.33e-4
Zlyhani e jednot ky ECU
5.90e-5
Namerané hodnoty smerujúc...
2.00e-5
Zlyhanie obidvoch senzorov ...
6.30e-10
Zlyhani e 1. senzo...
2.51e-5
Zlyhani e 2. senzo...
2.51e-5
Zlyhanie obidvoch senzorov ...
6.30e-10
Zlyhani e 2. senzo...
2.51e-5
Zlyhani e 1. senzo...
2.51e-5
Zlyhani e senzo...
1.00e-5
Zlyhani e senzo...
1.00e-5
RESET
Zaistuje funkciu PCA fails
6.09e-5
Spája motor s prevodovk ou fails
2.28e-5
Prehriat ie spojky
1.14e-5
Nezopn utie spojky
1.14e-5
Pohybuje pákou PCA fails
1.45e-5
Prehriat ie motoru
5.45e-6
Zadretie motoru
9.08e-6
Sprevoduvá va výkon motora fails
2.36e-5
Poš kodenie ozub...
2.36e-5