ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Ústav letecké dopravy

Spolehlivostní analýza ve vývoji turbovrtulových motorů založená na STAMP

Reliability Analysis in Turboprop Engine Development based on STAMP

Bakalářská práce

Studijní program: Bakalářský

Studijní obor: TUL – Technologie údržby letadel

Vedoucí práce: Ing. Oldřich Štumbauer

Ing. Kateřina Stuchlíková

Martin Tisoň

Praha

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):

Martin Tisoň

Studijní program (obor/specializace) studenta:

bakalářský – TUL – Technologie údržby letadel

Název tématu (česky): **Spolehlivostní analýza ve vývoji turbovrtulových motorů založená na STAMP**

Název tématu (anglicky): Reliability Analysis in Turboprop Engine Development based on STAMP

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je ověřit možnost využití spolehlivostních analýz v rámci vývoje a výroby turbovrtulových motorů pomocí modelu bezpečnosti STAMP.
- Analyzujte metody hodnocení spolehlivosti v letectví.
- Analyzujte systémový model bezpečnosti STAMP.
- Vyberte a popište konkrétní systém leteckého turbovrtulového motoru.
- Proveďte analýzu spolehlivosti s pomocí modelu STAMP.
- 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: Leveson, Nancy. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
A. Birolini. Reliability Engineering. Theory and Practice. Springer, 2017.

Vedoucí bakalářské práce: **Ing. Oldřich Štumbauer**
Ing. Kateřina Stuchlíková

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

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

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

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

Potvrzuji převzetí zadání bakalářské práce.

Martin Tisoň
jméno a podpis studenta

V Praze dne ..... 7. října 2022

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Spolehlivostní analýza ve vývoji turbovrtulových motorů založená na STAMP vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské práci.

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

Tato Bakalářská práce s názvem "Spolehlivostní analýza ve vývoji turbovrtulových motorů založená na STAMP" byla zpracována s použitím důvěrných informací a se souhlasem společnosti GE Aviation Czech s.r.o., IČ: 27928845, se sídlem Beranových 65, 199 02, Praha 9, zapsané v obchodním rejstříku vedeném Městským soudem v Praze pod spisovou značkou C127155.

V Praze, dne 14. července 2023 .....

Martin Tisoň

Poděkování

Mé poděkování patří vedoucímu práce Ing. Oldřichu Štumbauerovi za jeho vstřícný přístup, cenné rady a odborné vedení při psaní této práce. Společnosti GE Aviation Czech za možnost, vypracovat tuto práci s daty o motorech, svým kolegům za sdílení informací, ochotu pomoci s danou problematikou. Také bych rád poděkoval své rodině a blízkým za podporu během celého studia a psaní této práce.

Abstrakt

Tato bakalářská práce se zaměřuje na ověření možnosti využití spolehlivostních analýz v rámci vývoje a výroby turbovrtulových motorů pomocí modelu bezpečnosti STAMP.

Nejprve je proveden přehled o firmě GE Aviation a jejich práce, dále je navázáno na popis současných metod spolehlivostních analýz v leteckém průmyslu. Následuje představení modelu STAMP a analýzy založené na modelu. Na konci této části je popsán turbovrtulový motor, jeho princip a regulátor vrtule s jeho jednotlivými komponenty.

V další části práce je použita metoda STPA na regulátoru vrtule v rámci vývoje a výroby turbovrtulového motoru. Jsou identifikovány jednotlivé komponenty a analyzovány jejich interakce a závislosti. Na základě této analýzy jsou navržena a doporučena konkrétní opatření pro zlepšení bezpečnosti a spolehlivosti regulátoru vrtule.

V závěru práce jsou shrnuty dosažené výsledky a zhodnocen přínos modelu STAMP pro současné spolehlivostní analýzy regulátoru vrtule vývoje a výroby turbovrtulových motorů. Jsou diskutovány možnosti dalšího rozvoje a aplikace tohoto modelu v praxi, se zaměřením na konkrétní vylepšení regulátorů vrtule.

Klíčová slova: Regulátor vrtule, Systém Theoretic Accident Model and Process, System-Theoretic Process Analysis, Turbovrtulový motor

Abstract

This bachelor thesis focuses on the verification of the possibility of using reliability analyses in the development and production of turboprop engines using the STAMP safety model.

First, an overview of GE Aviation and their work, followed by a description of current reliability analysis methods in the aerospace industry. This is followed by an introduction to the STAMP model and the analysis based on the model. At the end of this section, the turboprop engine, its principle and the propeller controller with its various components are described.

In the next part of thesis, the STPA method is applied to the propeller controller in the context of turboprop engine development and production. The individual components are identified and their interactions and dependencies are analyzed. Based on this analysis, specific measures are proposed and recommended to improve the safety and reliability of the propeller governor.

The thesis concludes by summarizing the results obtained and evaluating the contribution of the STAMP model to the current reliability analysis of propeller governor development and turboprop engine manufacturing. The possibilities of further development and application of this model in practice are discussed, with a focus on specific improvements of propeller controllers.

Keywords: Propeller governor, System-Theoretic Accident Model and Process, System-Theoretic Process Analysis, Turboprop engine

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

CAST	Causal Analysis based on STAMP	Analýza příčin, která je založená na STAMP
ECL	Engine Control Lever	Páka řízení motoru
EHO	Electro – Hydraulic Actuator	Elektro – hydraulický aktuátor
FCU	Fuel Control Unit	Palivová řídící jednotka
FMEA	Failure Mode and Effect Analysis	Metoda analýzy a odstranění chyb
FTA	Fault Tree Analysis	Analýza stromu příčin
GE	General Electric	General Electric
GEAC	General Electric Czech	General Electric Czech
PCL	Propeller Control Lever	Páka řízení vrtule
RPN	Risk Priority Number	Číslo prioritního rizika
SC	Scenarios	Scénáře
SHP	Shaft horsepower	Výkon na hřídeli
STAMP	System-Theoretic Accident Model and Processes	Systémově – teoretický model nehod a procesů
STPA	System-Theoretic Process Analysis	Systémově – teoretická analýza procesů
UCA	Unsafe Control Action	Nebezpečné řídící akce

Úvod

Turbovrtulové motory představují klíčový prvek v leteckém průmyslu malých dopravních letadel, zajišťující pohyb a spolehlivost letadel ve velké škále letových podmínek. Součástí těchto motorů je regulátor vrtule, který má za úkol řídit otáčky a náklon listů vrtule, což ovlivňuje tah motoru a tím i letové parametry. Bezpečnost a spolehlivost regulátoru vrtule jsou tedy klíčovými faktory pro zajištění bezpečného letu.

Tato bakalářská práce se soustředí na zkoumání možnosti využití metody STPA v procesu vývoje turbovrtulových motorů ve společnosti GE Aviation Czech (GEAC). Metoda STPA představuje moderní přístup k analýze bezpečnosti, který se zaměřuje na identifikaci systémových selhání a jejich interakcí, s cílem odhalit potenciální rizika a navrhnout odpovídající bezpečnostní opatření.

V rámci práce byla poskytnuta data z aktuálně využívané analýzy FTA (Fault Tree Analysis), která se zabývá identifikací jednotlivých selhání a jejich příčin. Cílem porovnání výsledků STPA s daty z FTA, je zhodnotit, zda metoda STPA poskytuje větší a komplexnější pohled na bezpečnostní aspekty regulátoru vrtule v porovnání s FTA. Dále bude zohledněno, zda STPA může doplnit či rozšířit stávající analýzy a přinést nový pohled na bezpečnostní rizika.

Cílem práce je přinést nový přístup k analýze bezpečnosti a spolehlivosti v rámci vývoje turbovrtulových motorů, který může být pro společnost GEAC cenným nástrojem pro identifikaci kritických bezpečnostních aspektů a navržení efektivních opatření. Výsledky této práce mohou vést ke zlepšení bezpečnosti a spolehlivosti regulátoru vrtule a tím i celkového provozu turbovrtulových motorů ve společnosti. Práce je zaměřena na možnost využití spolehlivostních analýz v rámci vývoje turbovrtulových motorů pomocí metody STPA. Analyzujeme, jaký přínos a doplnění může přinést STPA ve srovnání s tradiční analýzou FTA a zda je STPA dostatečně komplexní a srovnatelná s FTA.

1. Výrobce leteckých motorů GE Aviation

1.1 Historie General Electric

Americký vynálezce Thomas Alva Edison je držitelem 1093 patentů, vytvořil fonograf, filmovou kameru, fluoroskop, diktafon a proslulou elektrickou žárovku. Byl to úspěšný obchodník, který v roce 1878 založil Edison Electric Light Company. O jedenáct let později byla Edison Electric Light Company spojena se všemi jeho dalšími podniky a vytvořila Edison General Electric Company. General Electric Company byla vytvořena v roce 1892 jako výsledek fúze mezi Edison General Electric Company a Thompson-Houston Electric Company (GE). Koncem 20. století byla General Electric díky rychlému růstu společnosti výrobcem prakticky všech zařízení na výrobu a spotřebu elektřiny používaných při elektrifikaci Spojených států. [1]

General Electric se postupem času stala globálním konglomerátem a v roce 2012 ji Forbes Global 2000 zařadil jako čtvrtou největší společnost na světě. GE Aviation je v současnosti jedním z deseti provozních segmentů společnosti.

Je předním světovým dodavatelem proudových, turbohřídelových a turbovrtulových motorů pro civilní a vojenské draky je GE Aviation. Všechny typy letadel, od širokotupého Boeingu 787 až po malá letadla jako Thrush 510G, jsou poháněny motory GE. Kromě toho společnost vytváří integrované systémy pro výrobce letadel, díly pro výrobce motorů, avioniku, elektrickou energii a mechanické systémy letadel, kromě toho nabízí služby, jako je podpora produktů, služby údržby, materiálové služby, digitální služby a analýza dat, komponenty opravy a údržba, opravy a generální opravy a údržba součástí. [2]

1.2 Walter Engines

Historie společnosti Walter Aircraft Engines sahá až do roku 1911, kdy Josef Walter založil společnost na výrobu motocyklů, motorových tříkolek a automobilů. Na počátku 20. let 20. století začala společnost v reakci na rostoucí letecký průmysl také navrhovat, vyvíjet a opravovat letecké motory. Jejím prvním vyvinutým motorem byl vzduchem chlazený pístový motor. Věhlas motorů Walter se velmi rychle rozšířil do zahraničí a do roku 1936 poháněly letecké motory Walter letadla letectva třinácti zemí. Poslední léta existence společnosti Walter jsou spojena s turbovrtulovým motorem M601 určeným pro použití v letadlech Let L-410. Motor M601 byl bezpochyby jedním z úspěšných motorů společnosti s celkovým počtem 17 milionů letových hodin. V červenci 2008 koupila

společnost Walter Aircraft Engines. GE Aviation, která pokračuje ve výrobě derivátů motorů řady M601 tzv. H-Series. [3]

1.3 General Electric Aviation Czech

Rok 2008 byl pro GE Aviation významný. V prvních měsících tohoto roku byla založena organizace zaměřená na trh obchodního a všeobecného letectví General Electric Aviation Czech. V témže roce GEAC získala některá aktiva společnosti Walter Aircraft Engines a zahájila vývoj a výrobu turbovrtulových leteckých motorů v České republice. V důsledku této akvizice vznikla společnost GEAC, která přepracovala konstrukci motoru M601 a uvedla na trh nový turbovrtulový motor s označením H80 a úspěšně vstoupila do leteckého segmentu malých turbovrtulových letadel pro menší dopravu. Ve srovnání s motorem Walter M601 je motor H80 vybaven novým kompresorem, lopatkami, blisky a statory, což vedlo ke zvýšení výkonu o 3 %, vyšší účinnosti o 8 % z hlediska měrného množství paliva a nižší náklady na údržbu o více než 15 %. Hřídel motoru H80 dosahuje výkonu až 800 koňských sil.

V roce 2011 byl motor H80 certifikován Evropskou agenturou pro bezpečnost letectví (EASA). Tento certifikace otevřela trh Evropské unie pro řadu H80 a motor H80 byl namontován do letadel Thrush 510G a L410. V roce 2012 byl motor také certifikován Federálním úřadem pro letectví. V návaznosti na úspěch motoru H80, motory H75 a H85 byly vyvinuty odvozené od motoru H80 s drobnými odlišnostmi ve výkonu na hřídeli. [4] [5]

V roce 2015 si společnost Textron vybrala turbovrtulový motor Catalyst, motor s čistou konstrukcí od společnosti GE pro pohon svého zcela nového letounu Cessna Denali. V současné době více než 400 inženýrů GE v České republice, Polsku, Itálii a Německu navrhuje a testuje hardware pro Catalyst, jehož plné testování motoru mělo začalo koncem roku 2021. Certifikace Catalystu pro uvedení do provozu se očekává v dalších letech.

Nový motor Catalyst s výkonem 1 240 SHP je první položkou v nové rodině turbovrtulových motorů GE zaměřených na letadla pro business a všeobecné letectví v rozsahu 1 000 - 1 600 SHP. [5]

1.4 Motory řady Hxx a M601x

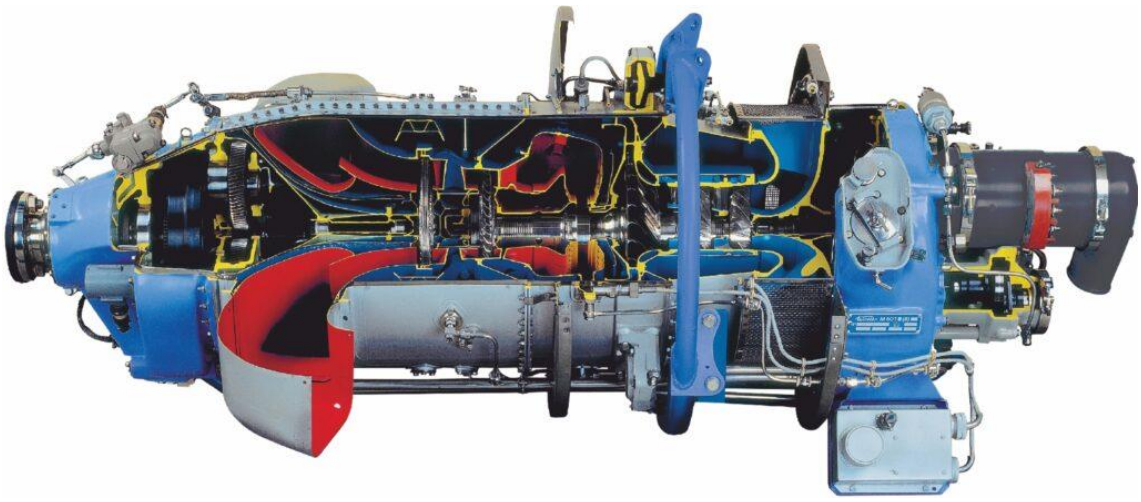
1.4.1 Motory řady M601x

Walter M601 je československý turbovrtulový letecký motor vyvinutý v 60. letech 20. století společností Motorlet, později známou jako Walter. Tento motor byl prvním turbovrtulovým motorem této společnosti a našel široké uplatnění v lehkých transportních, užitkových, zemědělských a vojenských cvičných letounech.

Vývoj motoru M601 začal v roce 1960 a první funkční prototyp byl otestován v roce 1964. První kompletní motor byl spuštěn v roce 1967, ale kvůli technickým problémům musel být první sériově vyráběný letoun L-410A vybaven dovozem kanadských motorů PT6A-27.

Sériová výroba verze M601A byla zahájena až v roce 1975. V průběhu 80. let byly vyvinuty zdokonalené verze motoru pro různé varianty letounů, včetně zemědělského letounu Zlín Z-37 Čmelák a polských letounů PZL-106 Kruk a PZL-130 Orlik. Motor M601 také nahradil pístové motory ve starších letounech po celém světě.

Díky své spolehlivosti a certifikacím získaným podle mezinárodních standardů se motor M601 stal oblíbenou volbou pro modernizaci letadel a byl vyvážen do mnoha zemí, včetně USA. [16]



Obrázek 1: Motor Walter M601 [18]

1.4.2 Motory řady Hxx

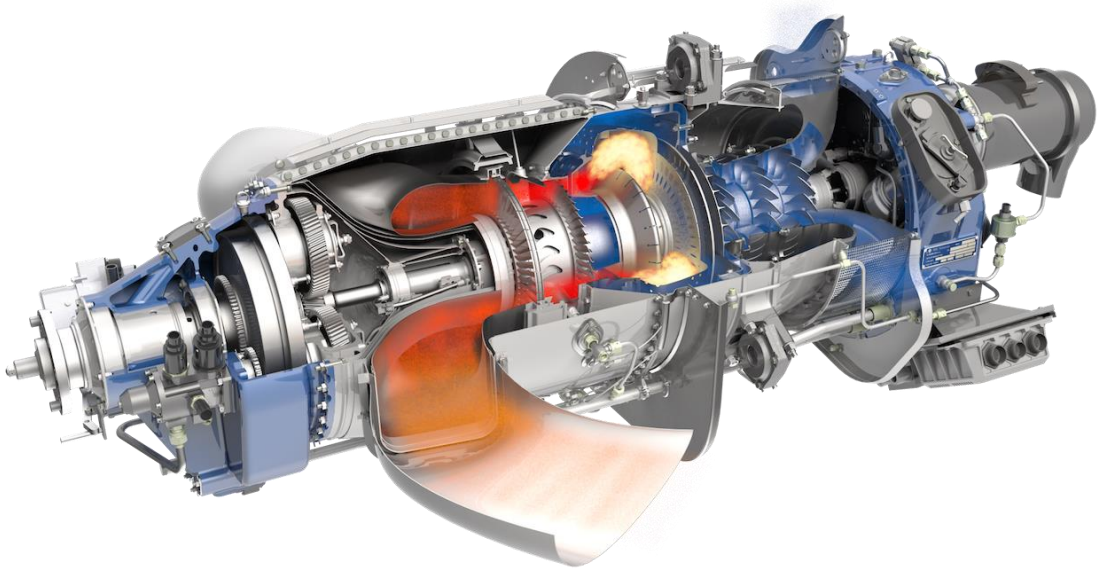
Série motorů H, vyvinutá společností GE Aviation Czech, představuje skupinu výkonných turbovrtulových motorů, které slouží různým účelům v leteckém průmyslu. Tyto motory se vyznačují širokým spektrem výkonů a parametrů, které umožňují jejich použití ve

všech typech letadel, od komerčních a soukromých letadel až po zemědělské stroje a akrobatické cvičné letouny.

Díky své flexibilitě a vysoké spolehlivosti jsou motory série H vhodné pro různé letectví související úkoly. Mohou být nasazeny pro zvládání seskoků padákem, poskytování zdravotnické pomoci nebo přepravu nákladu. Navíc se osvědčují v extrémních podmínkách, jako jsou horké pouště, vysoké hory a odlehlé ostrovy, kde je vyžadována připravenost k nasazení a bezpečný provoz.

Motorová řada H disponuje dvouhřídelovou konstrukcí s protiproudem a volnou turbínou. Je vybavena axiálním kompresorem a kompresorovou turbínou s pokročilou 3D geometrií. Tento design umožňuje efektivní přenos energie a výkonu na vrtuli letadla. Kromě toho je palivo přiváděno do spalovací komory pomocí prstencového systému, který usnadňuje údržbu a eliminuje potřebu pravidelné kontroly trysek paliva.

Díky svým vlastnostem a schopnostem je motorová řada H široce využívána v leteckém průmyslu. Jeho výkon, spolehlivost a přizpůsobivost ho činí ideální volbou pro různé typy letadel a aplikací, ať už jde o přepravu osob nebo nákladu, provádění zemědělských prací nebo cvičení akrobatických manévrů. Je to spolehlivý a výkonný motor, který je schopen plnit náročné úkoly v různých prostředích a podmínkách. [15]



Obrázek 2: Motor H80 [19]

2. Spolehlivost

Spolehlivosti je klíčovým faktorem při vývoji, návrhu, výrobě, provozu a údržbě všech systémů letadlových motorů. Předpovídání spolehlivosti v raných fázích vývoje návrhu poskytuje podporu pro požadavky na spolehlivost a pomáhá předvídat potenciální degradaci komponent během jejich životnosti. Výsledkem analýzy spolehlivosti může být vylepšení návrhu systému, zabránění nadměrného navrhování s cílem snížit zbytečné náklady, zvýšení povědomí o kritických komponentách a celkové zvýšení spolehlivosti a bezpečnosti eliminací určitých způsobů selhání nebo přijetím opatření k jejich zmírnění.

Spolehlivost je starý koncept, který podstoupil složitý historický vývoj. Její interpretace se liší v závislosti na kontextu a může znamenat různé věci pro různé lidi. Nicméně v systémovém inženýrství je nejčastější definicí spolehlivosti to, že spolehlivost komponentu nebo systému je pravděpodobnost, že komponent nebo systém bude plnit svou zamýšlenou funkci za určitých provozních a environmentálních podmínek po určité období. [9]

2.1 Metody pro analýzy spolehlivosti

2.1.1 FMEA

Failure Mode and Effect Analysis (FMEA) je systémová metoda používaná k identifikaci možných selhání a jejich následků v produktu nebo procesu. Tato metoda se používá v mnoha průmyslových odvětvích, včetně leteckého průmyslu.

FMEA se postupuje od jednotlivých komponent směrem k jejich možným selháním a následným důsledkům. Tento postup umožňuje identifikovat kritické aspekty systému, na které je třeba se zaměřit a provést preventivní kroky pro minimalizaci potenciálních problémů a nedostatků v konstrukci nebo provozu. Cílem FMEA je zvýšit spolehlivost, bezpečnost a kvalitu systému a zabránit nežádoucím událostem, které by mohly mít negativní dopad na uživatele nebo prostředí.

FMEA se skládá z několika kroků. Prvním krokem je identifikace potenciálních selhání. Tyto chyby mohou být způsobeny řadou faktorů, včetně materiálů, konstrukce, výrobních procesů. Dalším krokem je určení pravděpodobnosti výskytu těchto chyb.

Následujícím krokem je určení dopadu selhání na produkt nebo proces. Tyto dopady se mohou lišit v závislosti na konkrétním průmyslovém odvětví, ale mohou zahrnovat finanční ztráty, ztráty na kvalitě, nebezpečí pro bezpečnost a narušení plánu.

Poté se identifikují možnosti pro prevenci nebo detekci selhání. Prevence zahrnuje úpravy designu nebo výrobního procesu, aby se minimalizovala pravděpodobnost vzniku

chyb. Detekce zahrnuje testování, kontrolu kvality nebo monitoring procesů, aby se zajistilo, že selhání nebudou mít dopad.

V rámci FMEA je k posouzení rizika spojeného s jednotlivými možnými selháními často používána metoda RPN (Risk Priority Number). Toto číslo je výsledkem součinu pravděpodobnosti selhání, závažnosti následků a možnosti odhalení selhání. Čím vyšší hodnota RPN, tím vyšší je riziko daného selhání a tím důležitější je přijmout opatření pro minimalizaci rizika. Přesto mohou některé FMEA metody zahrnovat i jiné způsoby vyhodnocení rizika spojeného se selháním, jako je kvantitativní hodnocení nebo jiná kritéria závažnosti.

FMEA se v leteckém průmyslu používá k identifikaci a minimalizaci rizik spojených s letadly a souvisejícími procesy. Jedním z hlavních cílů je minimalizovat riziko nehod nebo poruch letadel, což má klíčový význam pro bezpečnost pasažérů a posádky.

FMEA se používá během vývoje a výroby letadel, ale také během údržby a oprav. Výsledky FMEA jsou také důležité pro povinné auditní procesy a certifikaci letadel. [14]

2.1.2 FTA

FTA je metoda analýzy, která se používá k identifikaci a hodnocení rizik v technických systémech. Tento nástroj umožňuje modelovat, jak se různé události a chyby mohou vzájemně ovlivňovat a vést k nežádoucím důsledkům. FTA tedy slouží k identifikaci zdrojů nebezpečí, analýze rizik a návrhu opatření pro minimalizaci těchto rizik.

FTA se skládá z několika úrovní. Nejvyšší úroveň obsahuje hlavní nežádoucí událost, které je nutné zabránit. Pod touto úrovní se nachází tzv. události nižší úrovně, které mohou vést ke vzniku hlavní události. Tyto události jsou propojeny logickými prvky, nejčastěji AND a OR. Například, pro vznik požáru v budově může být zapotřebí buď poruchy elektrického systému OR poruchy topného systému AND hořlavých materiálů v budově.

FTA může být aplikována na různé systémy a procesy, včetně technických zařízení, programování, logistických operací a dalších oblastí. FTA je obzvláště užitečná při návrhu nových systémů nebo při identifikaci problémů s existujícími systémy.

FTA lze použít v kombinaci s dalšími metodami, jako je například FMEA (Failure Mode and Effects Analysis). FMEA se zaměřuje na identifikaci možných způsobů selhání jednotlivých součástek systému a následného hodnocení důsledků těchto selhání. Použití FMEA v kombinaci s FTA může pomoci získat komplexnější pohled na celkové riziko. [17]

3. Bezpečnost

3.1 Model STAMP

STAMP (System-Theoretic Accident Model and Processes) je nový model příčin nehod, který vychází ze systémové teorie a poskytuje teoretický základ pro STPA (System-Theoretic Process Analysis), to je preventivní metoda analýzy, která analyzuje možné příčiny nehod během vývoje a provozu. Tento model se zaměřuje na dynamický problém řízení bezpečnosti a neomezuje se pouze na prevenci selhání, ale zahrnuje složitější procesy a interakce mezi komponenty systému.

V STAMP jsou zahrnuty i příčinné faktory, jako jsou lidé, organizace, software a bezpečnostní kultura, což umožňuje aplikovat tento model na jakýkoli emergentní jev v systému, včetně kybernetické bezpečnosti.

Výhodou používání STAMP je to, že funguje na velmi složitých systémech, neboť se zaměřuje na řízení bezpečnosti z vrchu dolů. Tento model také umožňuje vytváření výkonnějších nástrojů, jako je analýza nehod, nazvaná CAST.

Je důležité poznamenat, že STAMP je model. Alternativou k současným analýzám jsou analýzy STPA a CAST, které jsou založené na modelu STAMP. STAMP rozšiřuje předpoklady selhání o složitější procesy a interakce mezi komponenty, což umožňuje modelovat větší škálu příčin a dává lepší představu o tom, jakým způsobem se systémy mohou chovat nebezpečně. Tento nový přístup nabízí nový pohled na bezpečnost a nové možnosti pro analýzu a řízení rizik v různých oblastech. [13]

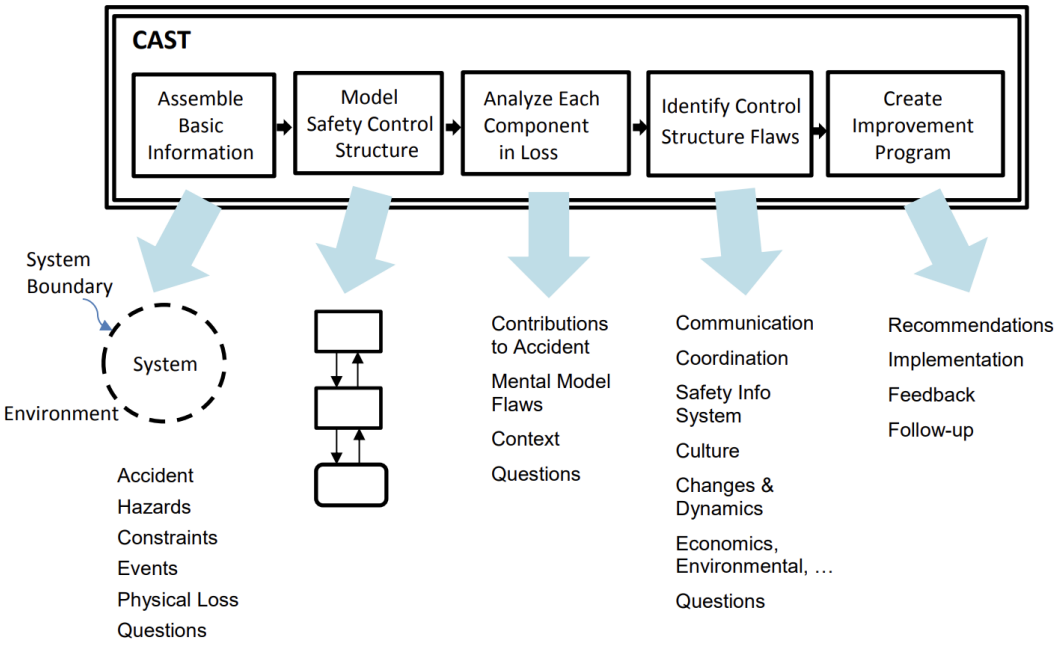
Umožňuje vytváření výkonnějších nástrojů, jako jsou STPA, CAST, identifikace a řízení proaktivních indikátorů bezpečnosti zvyšujícího se rizika a organizace řízení rizik. Protože se STAMP vztahuje na jakýkoli emergentní jev, lze STPA použít pro jakékoli vlastnosti systému.

3.2 Analýzy založené na modelu STAMP

3.2.1 CAST

CAST je analytická metoda, která se zabývá zkoumáním nehod a incidentů, které se již staly v minulosti. Tato metoda se zaměřuje na důkladný rozbor již existujícího systému a hledání příčin nehod a chyb, které vedly k nim nebo je provázely. CAST analyzuje konkrétní scénář, který vedl ke zjištěné nehodě, a identifikuje chyby pouze v tomto scénáři. Cílem analýzy je místo typického hledání selhání zaměřit se na to, proč systémy a struktury, které měly zabránit událostem, nebyly úspěšné. Doporučení se zaměřují na posílení těchto preventivních (kontrolních) struktur na základě poznatků z vyšetřování. [11]

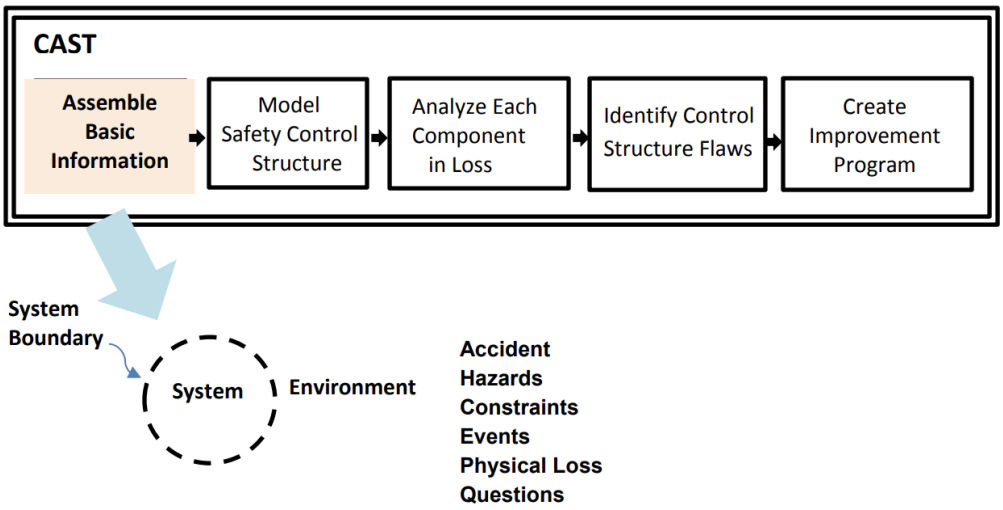
Analýza má pět kroků, které jsou popsány níže.



Obrázek 3: Obecný pohled na tvoření CAST analýzy [11]

1) Shromáždění základních informací

První krok analýzy CAST je shromáždění základních informací pro provedení analýzy. To zahrnuje vymezení dotčeného systému a hranice analýzy, popis ztráty a nebezpečného stavu, který k ní vedl, identifikaci bezpečnostních omezení na úrovni systému, která jsou nutná k zabránění nebezpečí, popis toho, co se stalo, bez závěrů nebo obviňování, a analýzu fyzické ztráty z hlediska fyzického vybavení a ovládacích prvků, požadavků na konstrukci, aby se zabránilo danému ohrožení, fyzických ovládacích prvků zahrnutých do konstrukce, aby se zabránilo tomuto typu nehody, poruch a nebezpečných interakcí vedoucích k ohrožení, chybějících nebo nedostatečných ovládacích prvků, které mohly nehodě zabránit, a všech faktorů, které ovlivnily události. [11]



Obrázek 4: První krok CAST analýzy [11]

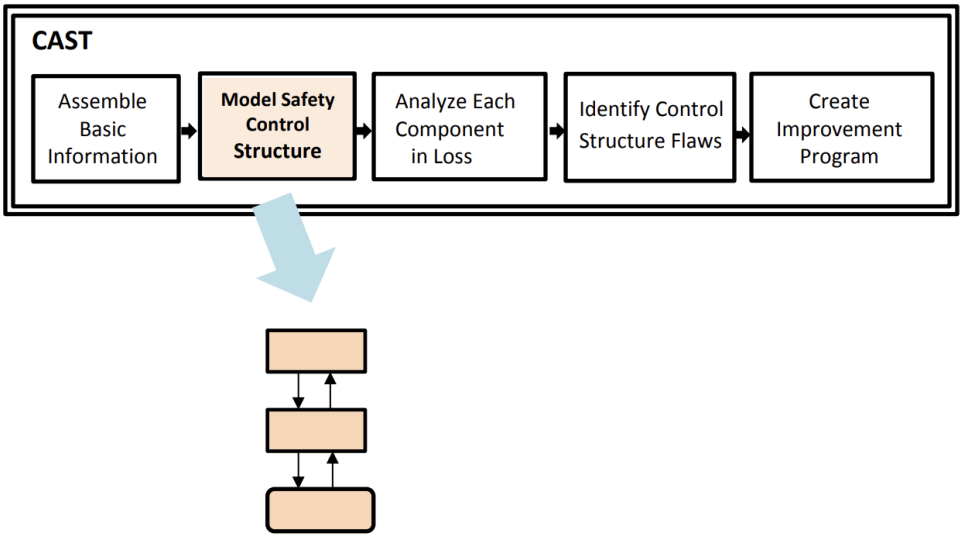
2) Modelování bezpečnostního řízení pro daný typ nebezpečí

V rámci CAST analýzy je krok "Modelování bezpečnostního řídícího systému" zásadní pro porozumění struktuře a fungování systému a identifikaci omezení a nedostatků. V tomto kroku se provádí detailní modelování informací o bezpečnostním řídícím systému. Cílem je získat komplexní přehled o tom, jak jednotlivé komponenty systému interagují a jakým způsobem jsou řízeny.

Modelování bezpečnostního řídícího systému zahrnuje popis jednotlivých komponent, jako jsou zařízení, ovládací prvky, procedury, lidské interakce atd., a jejich vzájemné vztahy. Pomocí různých metod a technik, jako je například bloková schémata, příčinné diagramy nebo podobné nástroje, se vytváří model systému. Tento model poskytuje ucelený pohled na bezpečnostní řídící strukturu

a pomáhá identifikovat slabá místa a nedostatky, které byly přítomny během ztráty.

Důkladné modelování umožňuje analytikům lépe porozumět, jak jednotlivé komponenty spolupracují a jak mohou být ovlivněny různými faktory. Modelování také umožňuje identifikovat, jakým způsobem byly kontrolní mechanismy používány nebo jak mohly selhat v rámci daného incidentu. [11]



Obrázek 5: Druhý krok CAST analýzy [11]

3) Analýza jednotlivých komponent při ztrátě

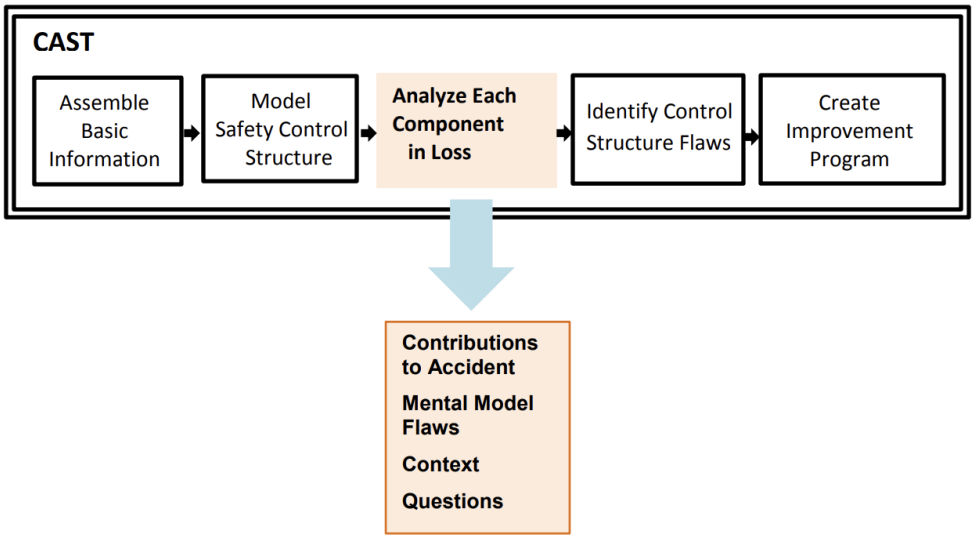
V rámci CAST analýzy je analýza jednotlivých komponent, které byly přítomny při ztrátě, klíčovým krokem pro porozumění jejich role a příspěvku ke vzniku nebezpečí. Tento krok se zaměřuje na podrobnou analýzu jednotlivých částí systému s cílem identifikovat, jak každá komponenta přispěla k vzniku ztráty a jak mohla selhat.

Během analýzy se zkoumají různé aspekty jednotlivých komponent, jako jsou fyzická zařízení, ovládací prvky, procedury, lidské faktory atd. Cílem je získat hlubší porozumění jejich fungování a zjistit, jak mohou být spojeny s nebezpečným stavem.

Analýza jednotlivých komponent zahrnuje identifikaci případných nedostatků, poruch a nebezpečných interakcí, které se týkaly dané komponenty. Cílem je odhalit slabá místa, chyby v návrhu, selhání nebo nevhodné interakce, které přispěly k nebezpečné situaci.

Důkladná analýza každé komponenty také zahrnuje hodnocení fyzických kontrolních mechanismů, které byly součástí dané komponenty. Posuzuje se, zda

tyto kontroly byly dostatečné a účinné při prevenci daného typu nehody. Pokud se identifikují nedostatky nebo chyby v těchto kontrolních mechanismech, jsou zaznamenány a berou se v úvahu při formulaci doporučení na zlepšení. [11]



Obrázek 6: Třetí krok CAST analýzy [11]

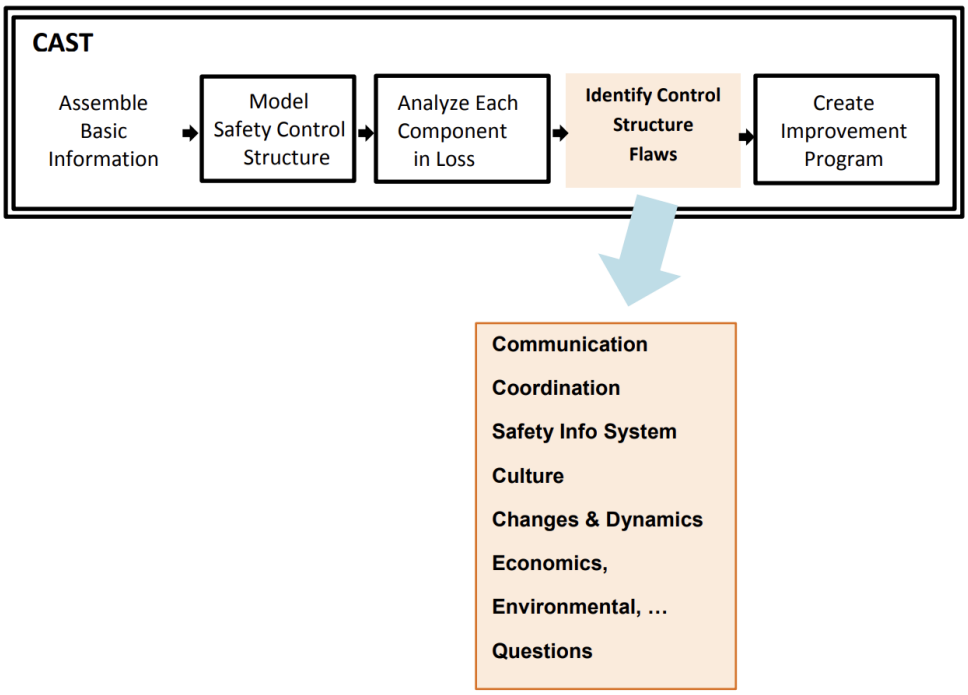
4) Identifikace nedostatků řídící struktury

Ve čtvrtém kroku CAST analýzy se zaměřujeme na identifikaci nedostatků v řídící struktuře. Cílem je zjistit, jaké nedostatky a chyby v rámci systému přispěly k vzniku ztráty a jak byla řídící struktura nedostatečná při zabránění nebezpečným stavům.

Během tohoto kroku se analyzují různé aspekty řídící struktury, včetně postupů, politik, komunikačních kanálů, zodpovědnosti a pravidel. Cílem je identifikovat nedostatky a chyby, které mohou vést ke snížení účinnosti řídících mechanismů a ochraně proti nebezpečím.

Analýza nedostatků řídící struktury se zaměřuje na identifikaci systémových nedostatků, které mohou zahrnovat nedostatečné řízení rizik, nedostatečné monitorování a hodnocení, nedostatečnou komunikaci, nedostatečné školení a podobně. Cílem je odhalit nedostatky, které byly přítomny v rámci systému a které měly vliv na vznik nebezpečných stavů.

Identifikované nedostatky v řídící struktuře jsou důležité pro pochopení, jak byla preventivní opatření nedostatečná a jakým způsobem mohly selhat. Tyto informace jsou klíčové pro formulaci návrhů na zlepšení a posílení řídící struktury. [11]



Obrázek 7: Čtvrtý krok CAST analýzy [11]

5) Vytvoření programu zlepšení

Posledním krokem v rámci CAST analýzy je vytvoření programu zlepšení. Cílem tohoto kroku je formulovat konkrétní opatření a doporučení, která mají za úkol posílit preventivní mechanismy a zlepšit ochranu před nebezpečími, aby se podobné události v budoucnosti minimalizovaly.

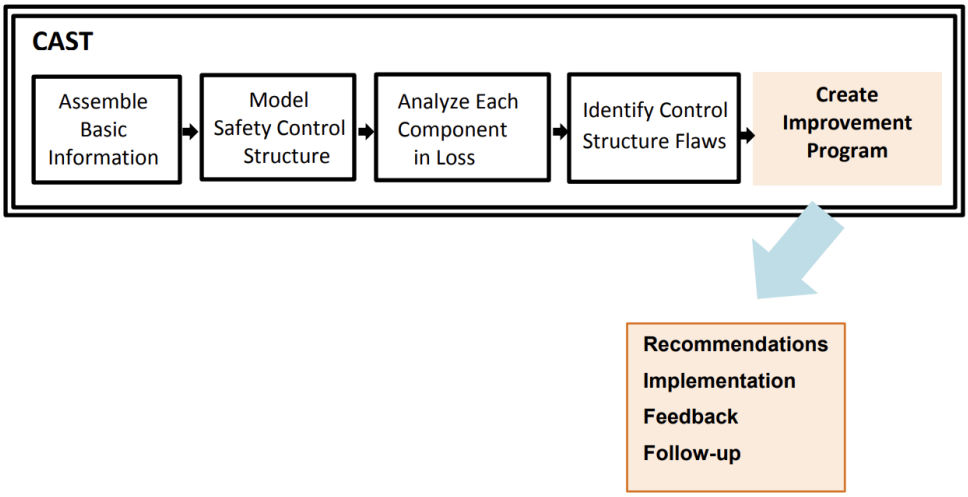
Program zlepšení vychází z identifikovaných nedostatků a chyb v řídící struktuře a dalších analýzách provedených v rámci CAST. Zahrnuje specifické kroky, které mají být podniknuty, a doporučení, která mají být implementována.

Při tvorbě programu zlepšení se zohledňují příčiny a faktory, které vedly k vzniku ztráty, a zaměřuje se na posílení ochranných opatření a prevenci podobných událostí v budoucnosti. Doporučení se mohou týkat různých aspektů, včetně změn v postupech, zlepšení komunikace, aktualizace politik, zvýšení úrovně školení, posílení monitorování a hodnocení a dalších.

Důležitým aspektem programu zlepšení je jeho realizace a monitorování. Implementace doporučení vyžaduje spolupráci a angažovanost relevantních

zainteresovaných stran. Pravidelné hodnocení a monitorování programu zlepšení jsou klíčové pro zajištění, že přijatá opatření jsou účinná a odpovídají cílům zlepšení.

Cílem programu zlepšení je posílit bezpečnostní řídící strukturu a minimalizovat riziko podobných incidentů v budoucnosti. Tímto způsobem se CAST analýza zaměřuje na vytvoření udržitelných opatření a systémových změn, které přispějí k vytvoření bezpečnějšího pracovního prostředí a ochraně lidského života. [11]



Obrázek 8: Pátý krok CAST analýzy [11]

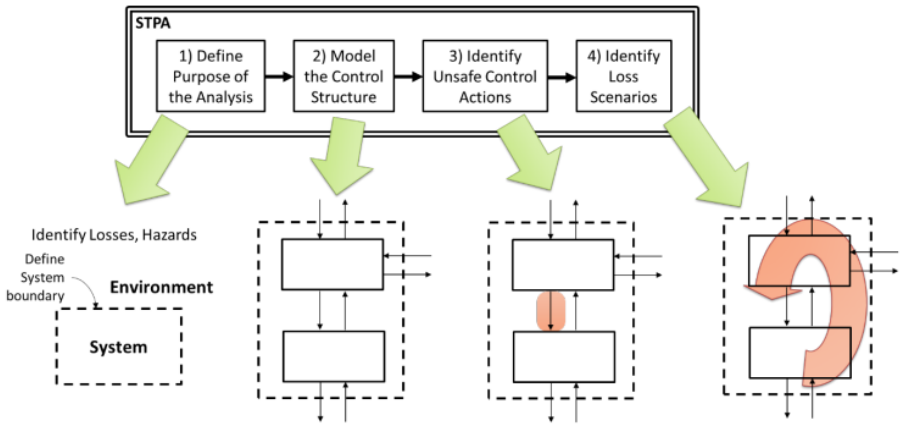
3.2.2 STPA

System-Theoretic Process Analysis (STPA) je preventivní metoda analýzy, která analyzuje možné příčiny nehod během vývoje a provozu, aby mohly být nebezpečí eliminována nebo řízena. STPA nám umožňuje analyzovat velmi složité systémy. "Neznámé neznámé", které byly dříve nalezeny pouze během provozu, lze identifikovat již v rané fázi vývoje a buď eliminovat, nebo minimalizovat jejich vliv. Jsou zahrnuty jak zamýšlené, tak i nezamýšlené funkce. Zamýšlené funkce jsou ty, které jsou navrženy a plánovány jako součást systému, zatímco nezamýšlené funkce se objevují nebo vznikají jako neplánované důsledky interakcí mezi různými částmi systému. STPA zahrnuje v analýze jak softwarové, tak lidské operátory, což zajišťuje, že analýza nebezpečí zahrnuje všechny potenciální příčinné faktory pro ztráty. STPA poskytuje dokumentaci funkcionality systému, která je často chybějící nebo obtížně k nalezení u velkých a složitých systémů. [12] [13]

STPA je důkladná a pečlivá top-down technika systémového inženýrství, která má schopnost identifikovat potenciální nedostatky v návrhu. STPA se zaměřuje na

identifikaci potenciálních nedostatků v návrhu systému s vysokou úrovní detailnosti a analýzy. Tato technika se snaží odhalit jak zjevné, tak i skryté nedostatky a nepředvídatelná rizika. STPA poskytuje systematický a strukturovaný postup pro identifikaci a analýzu těchto nedostatků, což umožňuje navrhnout a implementovat opatření pro jejich odstranění a minimalizaci. Přísnost STPA je důležitá pro dosažení vyšší úrovně bezpečnosti a prevenci potenciálních nebezpečí v systémech.

STPA se skládá ze čtyř fází analýzy (viz obrázek 9), které musí být provedeny. Po dokončení všech fází jsou vytvořeny výsledky v podobě seznamu nebezpečných řídících akcí s kontextem a scénáři vedoucími k nebezpečím. Nebezpečím musí být předcházeno, protože mohou vést ke ztrátě. STPA odhaluje nízkoúrovňová a vysokoúrovňová nebezpečí systému a potenciální ztráty, provádí průzkum funkčnosti systému, identifikuje řídící a jejich řídící akce a navrhuje požadavky a omezení systému. Nízkoúrovňová nebezpečí se vztahují ke konkrétním aspektům systému, jako jsou fyzické komponenty, software, procedury a lidské faktory. Jsou to nebezpečí, která jsou přímo pozorovatelná nebo měřitelná a mají okamžitý vliv na bezpečnost nebo mohou vést ke ztrátám. Vysokoúrovňová nebezpečí se týkají širších systémových aspektů a interakcí mezi různými částmi systému. Jsou to komplexní nebezpečí, která mohou mít nepřímý nebo dlouhodobý vliv na bezpečnost. Vysokoúrovňová nebezpečí se často týkají organizačních faktorů, politik, procesů rozhodování, komunikačních kanálů a dalších systémových vlastností. Například nedostatečný dohled nad vývojem systému, nedostatečná komunikace mezi týmy STPA používá model řídicí struktury bezpečnosti systému pro identifikaci potenciálních nebezpečných řídících akcí. [13]

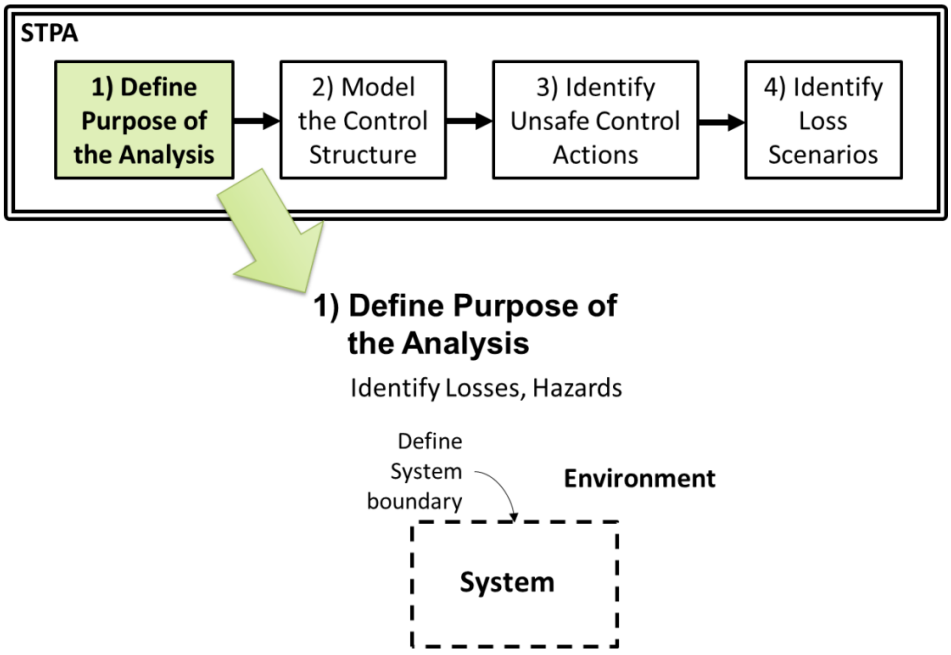


Obrázek 9: Obecný pohled na postup STPA analýzy [13]

Čtyři kroky pro provedení metody STPA jsou následující:

1) **Definovat účel analýzy**

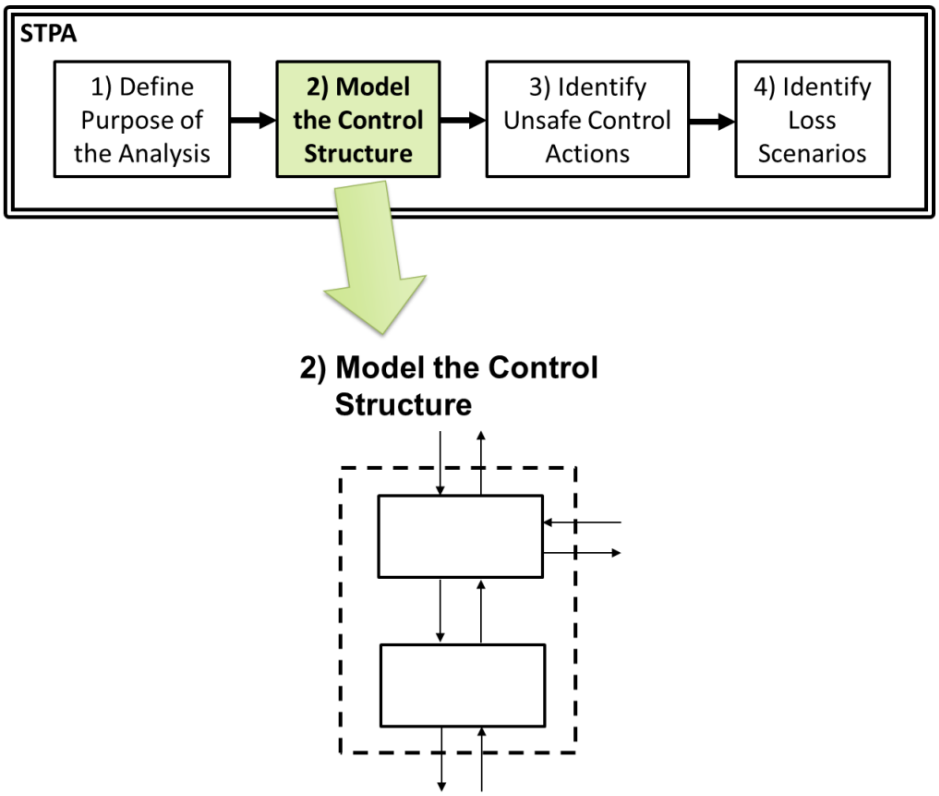
Cílem analýzy nebezpečí je předcházet různým ztrátám (např. úrazům, škodám na majetku, znečištění životního prostředí, ztrátě výkonu). Dalším krokem metody STPA je identifikace ztrát na úrovních systému. Systémové nebezpečí je definováno jako stav systému nebo soubor podmínek, které spolu s určitým souborem nejhorších podmínek prostředí povedou ke ztrátě. Hranice systému je stanovena (obvykle zahrnuje pouze procesy, které jsou pod naší kontrolou). Pro každé systémové nebezpečí musí být stanoveny bezpečnostní omezení. Systémové omezení určuje podmínky nebo chování systému, které je nutné splnit, aby se předešlo nebezpečí.



Obrázek 10: První krok STPA analýzy [13]

2) Model řídící struktury

Druhým krokem je modelování hierarchické řídící struktury. Model řídící struktury je funkční systémový model složený zpětnovazebních řídících smyček.

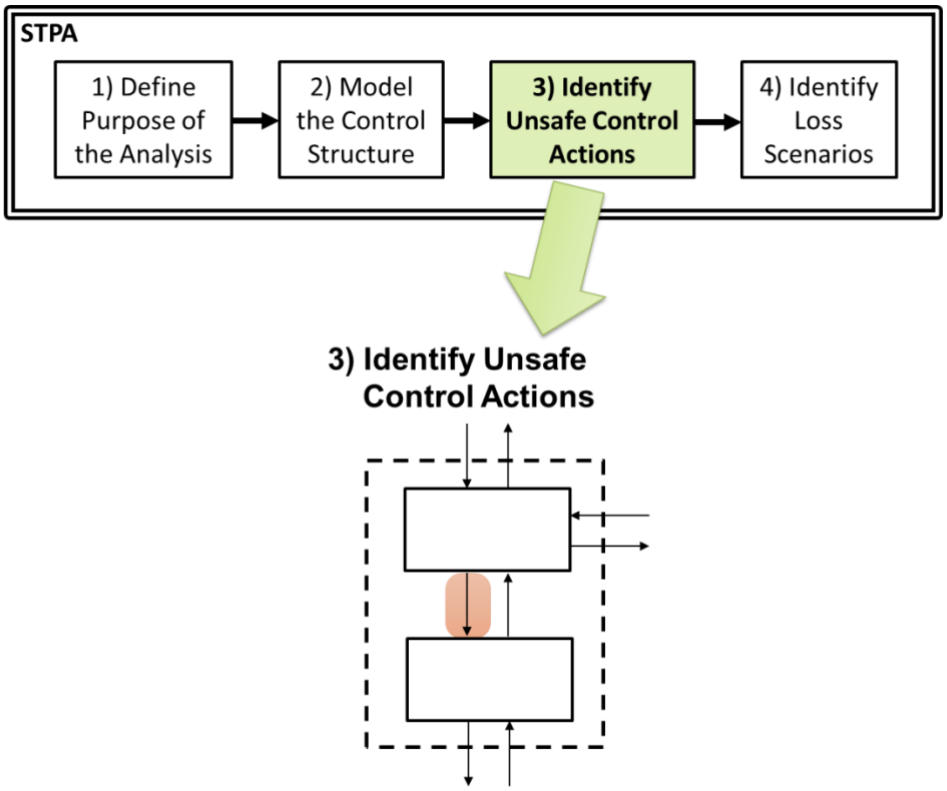


Obrázek 11: Druhý krok STPA analýzy [13]

Model řídící struktury prosazuje omezení chování celého systému. Řídící prvky poskytují řídící akce pro ovládání nějakého procesu a pro prosazování omezení na ovládaném procesu. Řídící algoritmus představuje rozhodovací proces řídícího, který určuje řídící akce k poskytnutí. Řídící také mají procesní modely, které představují vnitřní přesvědčení řídícího používané k rozhodování. Procesní modely mohou být aktualizovány zpětnou vazbou použitou k pozorování řízeného procesu. Systémy obvykle mají několik překrývajících se a vzájemně působících řídících smyček. Tyto smyčky jsou modelovány, což vytváří hierarchickou řídící strukturu. V některých případech stačí nakreslit diagram řídící struktury se všemi definovanými prvky, aby byly zjevné dříve neobjevené nedostatky. Řídící struktura zdůrazňuje funkční vztahy a funkční interakce, což je velmi užitečné pro identifikaci problémů, jako jsou konstrukční chyby.

3) Identifikace nebezpečných řídících akcí

Dalším krokem po dokončení modelu s řídící strukturou je hledání nebezpečných řídících akcí, které v konkrétním kontextu vedou k nebezpečí.



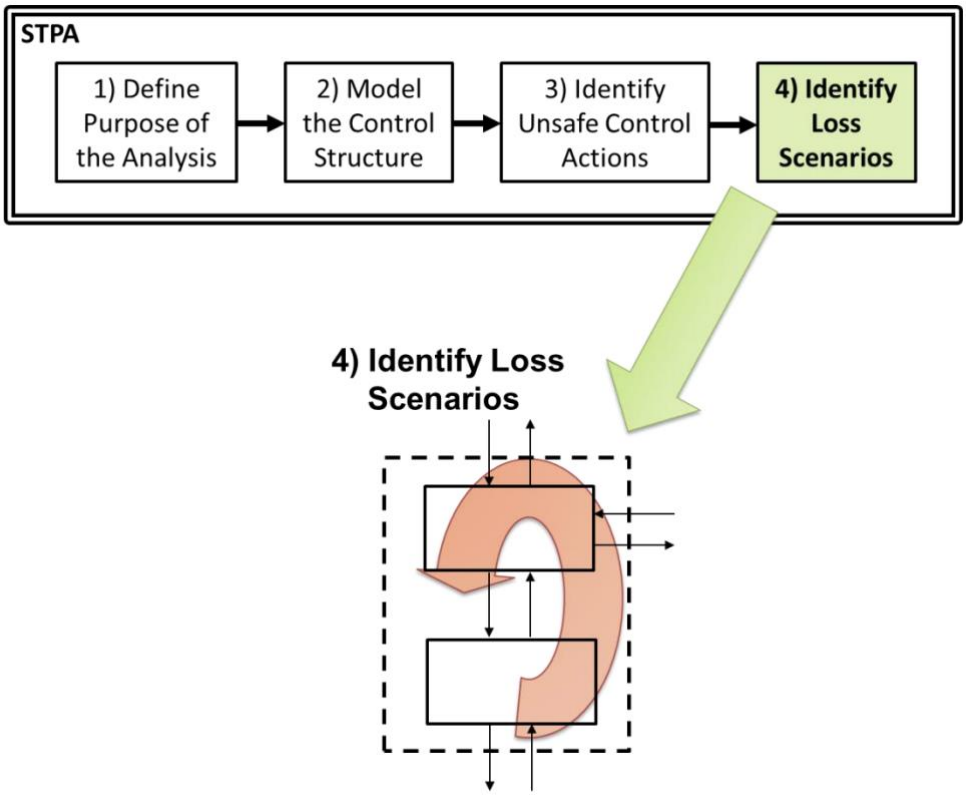
Obrázek 12: Třetí krok STPA analýzy [13]

Řídící akce mohou být nebezpečné buď tehdy, když jsou poskytnuty, ale ve špatném kontextu, nebo když řídící akce není vůbec poskytnuta. Pro zajištění zpětného sledování musí být každá nebezpečná řídící akce propojena s nebezpečím. Podle STPA existují čtyři typy nebezpečných řídících akcí:

- Neposkytnutí řídící akce vede k nebezpečí;
- Poskytnutí řídící akce vede k nebezpečí;
- Poskytnutí řídící akce příliš brzy, příliš pozdě nebo v nesprávném pořadí;
- Řídící akce se používá příliš dlouho nebo je příliš brzy zastavena.

4) Identifikace ztrátových scénářů

Posledním krokem je nalezení příčinných faktorů, které vedou k nebezpečným kontrolním akcím.



Obrázek 13: Čtvrtý krok STPA analýzy [13]

Ztrátové scénáře jsou způsob, jak nebezpečné řídící akce vznikají. Zahájení scénáře ztráty vychází z nedostatků v obecné řídící smyčce. Může se jednat o nevhodný procesní model, nebezpečný řídící vstup, nevhodný řídící algoritmus řídícího, problémy na řídící cestě, neefektivní řízený proces, nedostatečnou zpětnou vazbu nebo nesprávné informace získané ze senzorů. Zpětná vazba má rozhodující vliv na řídícího, neboť je klíčovým vstupem pro generování nových kontrolních akcí. Scénáře s řídícími akcemi, které jsou odeslány, ale nesprávně provedeny nebo vůbec nejsou provedeny, mohou být způsobeny zpožděním v komunikaci, chybovostí přenosu, ztracenou komunikací a dalšími problémy. [11]

4. Turbovrtulový motor

Turbovrtulové motory jsou přizpůsobené pro pohon vrtulí a nabízejí výrazné výhody oproti jednoproudovým a dvouproudovým motorům v oblasti nižších rychlostí letu. Tyto motory jsou velmi efektivní v krátkých přeletech, protože spotřebují méně paliva na kilometr a letadla s turbovrtulovým motorem potřebují kratší dráhu pro vzlet a přistání. Některé příklady letadel poháněných turbovrtulovými motory jsou Let L-410, Alenia ATR 42 a Pilatus PC-12.

K výrobě energie se v turbovrtulových motorech využívají stejné principy jako v proudových motorech, včetně kompresoru, spalovací komory a turbíny v plynovém generátoru. Hlavním rozdílem je, že turbovrtulové motory mají další turbíny, hnací hřídel a redukční převodovku pro pohon vrtule. [6]

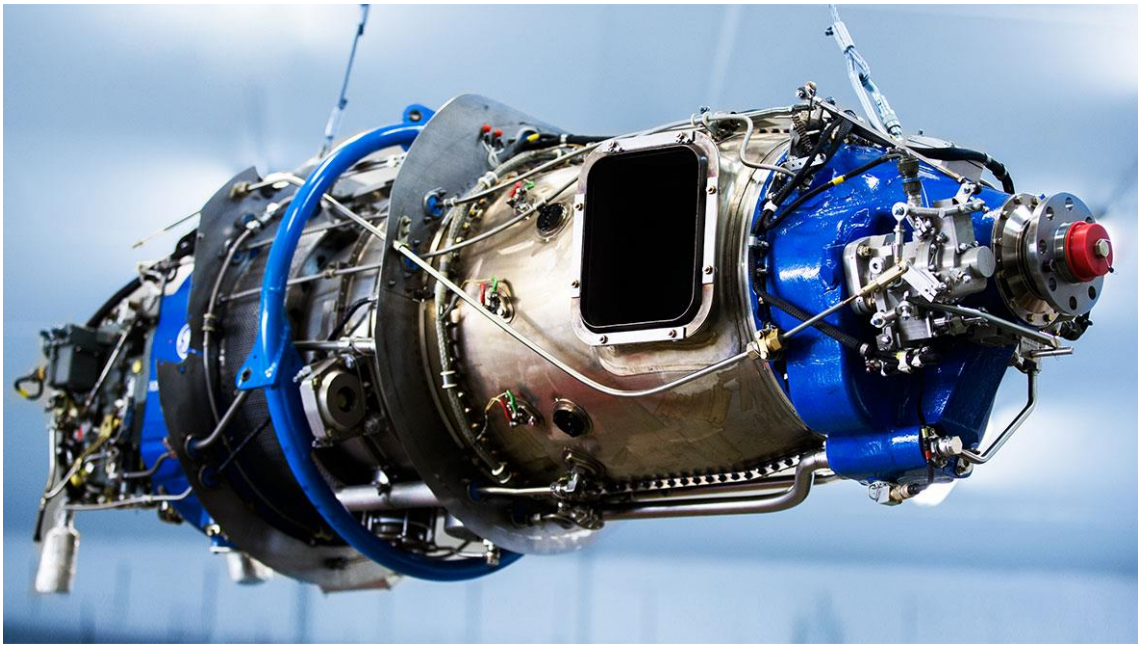
4.1 Princip fungování

Turbovrtulové motory jsou velmi podobné proudovým motorům, ale odlišují se způsobem, jakým vytvářejí tah. U proudového motoru ve výstupní trysce za turbínou je vysoký tlak a tepelná energie, jež sem proudí, se zde mění na energii kinetickou. Tím vzniká tah motoru, zatímco u turbovrtulových motorů se tato energie přeměňuje na rotační energii vrtule, která vede k proudění vzduchu skrz lopatky a tím se vytváří tah. Vzduch vstupuje do motoru atmosférickým vstupním hrdlem a prochází kompresorem, který zvyšuje jeho tlak. Kompresor může být radiální nebo axiální a u turbovrtulových motorů se často používá kombinace obou. Stlačený vzduch se poté dostává do spalovací komory, kde se smísí s palivem a dojde k zážehu. Výsledný plamen způsobuje vznik cirkulace a víření plamenů, což umožňuje dokonalé spálení paliva a zvýšení teploty. Zbytek vzduchu vstupuje v sekundární oblasti, čímž dochází k ochlazení rozpáleného vzduchu až o polovinu. Žhavý vzduch dál putuje do trysky, kam prochází skrz takzvané turbíny. Turbína je, stejně jako kompresor, lopatkové ústrojí, které ale naopak přeměňuje energii spalin na rotační energii. Zatímco u běžných proudových motorů se této energie získává jen nezbytné množství pro funkci kompresorů a pohon některých přístrojů letadla, tak v případě turbovrtulových motorů se usiluje o přeměnu veškeré tlakové energie. Důvodem pro to je možnost přenést tuto rotační energii až do vrtule na čele motoru, která pak způsobuje tah. Plyny tak po průchodu jednou nebo více turbínami (v závislosti na konstrukci motoru) vycházejí ven z motoru skrz trysku, avšak již nemají významné množství energie a neprojevují se výrazně na pohánění letounu. Turbína přenáší točivý moment na výstupní hřídel, na kterou je přes převodové ústrojí napojena vrtule. Vrtule je lopatkový stroj tvořený rotorem a alespoň dvěma vrtulovými listy rovnoměrně rozmístěnými po obvodu. Podobně jako u křídel letadla obtékání vzduchu přes listy vrtule

způsobuje rozdílné hodnoty tlaků nad a pod listem, což vede ke vzniku vztlakové a odporové aerodynamické síly. [10]

5. Regulátor vrtule (Propeller Governor)

Regulátor vrtule je zařízení, které umožňuje pilotovi ovládat otáčky vrtule letadla. Úkolem regulátoru vrtule je optimalizovat výkon motoru a vrtule tak, aby se dosáhlo maximální efektivity a výkonu. Regulátor vrtule umožňuje pilotovi manuální ovládání otáček vrtule nebo automatické ovládání, které se přizpůsobuje různým podmínkám letu, jako je například rychlost letu, nadmořská výška a teplota okolního vzduchu.



Obrázek 14: Motor H80 a zobrazený regulátor vrtule [19]

Regulátor vrtule funguje tím, že ovládá úhel náběhu vrtule, což ovlivňuje množství vzduchu, který protéká vrtulí. Pokud pilot potřebuje větší výkon, zvýší úhel náběhu a tím i množství vzduchu, který proteče vrtulí. Naopak pokud pilot potřebuje menší výkon, sníží úhel náběhu a tím i množství vzduchu, který se dostane do motoru. [8]

Regulátor vrtule je důležitým prvkem letadla, který umožňuje pilotovi přizpůsobit výkon motoru a vrtule různým podmínkám letu. To zajišťuje bezpečný a efektivní let. Existují i další režimy, které jsou popsány u komponent a jednotlivých interakcí. Jedná se o režimy zapraporování vrtule a BETA režim.

5.1 Zapraporování vrtule

Zapraporování vrtule je proces, který může být prováděn za letu při vypnutí motoru. Dvoumotorové letouny jsou obvykle vybaveny systémem pro zapraporování, který

zahrnuje elektrohydraulický ovladač a praporovací čerpadlo. Tento systém může být aktivován manuálně z kabiny letounu nebo automaticky.

V manuálním režimu pilot stiskne tlačítko v kabině, čímž spustí praporovací čerpadlo a přepne elektrohydraulický ovladač. Ovladač propojí regulační obvod, čímž se olej z čerpadla přivádí přímo k vrtuli a nastavují se listy na praporový úhel. Tento proces je signalizován kontrolní žárovkou v kabině. Po restartu motoru a nastavení volnoběhu se vrtule vrátí zpět do normálního režimu.

V automatickém režimu postupuje pilot stejným způsobem jako při manuálním zapraporování, s tím rozdílem, že zapnutí praporovacího čerpadla probíhá automaticky na základě vyhodnocování kroutícího momentu vrtule. Automatický systém obvykle funguje v určitém rozsahu ovládací páky motoru a jeho činnost je signalizována kontrolkou v kabině. Tento režim lze také vypnout.

Nouzové zapraporování se používá, pokud praporovací čerpadlo nefunguje nebo není k dispozici. Pilot provede nouzové zapraporování posunutím ovládací páky vrtule do polohy pro praporování. Listy vrtule jsou posunuty do praporového úhlu působením momentu od závaží vrtule nebo tlakem oleje. Přechod vrtule do praporového režimu trvá v nouzovém případě asi třikrát déle než při manuálním nebo automatickém zapraporování. [20]

5.2 BETA režim

Beta řízení vrtule se používá k ovládání tahu vrtule při pojíždění na zemi a také pro dosažení záporného tahu po přistání letounu. Tento systém umožňuje pilotovi nastavit vrtuli do libovolné polohy mezi minimálním letovým úhlem a maximálním reverzním tahem, a to při stále zachování odpovídajícího výkonu motoru. [20]

5.3 Jednotlivé komponenty regulátoru vrtule

A/C Feather Pump

U turbovrtulového motoru se čerpadlo pro překlopení listů obvykle označuje jako "Feathering Pump" a slouží k zapraporování vrtule.

Funkce čerpadla pro zapraporování listů spočívá v dodávání oleje do hydraulických válců umístěných u každého listu vrtule. Tento tlak působí na mechanismus listů, který umožňuje jejich překlopení do správné polohy pro zapraporování.

Při nouzové situaci, například v případě selhání motoru nebo potřeby rychlého zastavení motoru, pilot aktivuje čerpadlo pro zapraporování listů. To dodá hydraulický tlak do válců, které rychle překlopí listy vrtule do polohy, která minimalizuje jejich aerodynamický odpor. Tím se snižuje brzdící efekt vrtule a umožňuje letounu pokračovat v letu se sníženým odporem.

Electro-Hydraulic Actuator

Jeho hlavní funkcí je ovládání polohy vrtulových listů, což umožňuje regulaci tahu a výkonu motoru. EHO kombinuje elektrický pohon s hydraulickým mechanismem pro přesné a rychlé ovládání listů vrtule.

Elektro-hydraulický aktuátor je typicky umístěn v blízkosti vrtulového mechanismu a je připojen k vrtulovým listům pomocí hydraulických válců. Aktuátor přijímá signály a řídící signály z řídícího systému letadla nebo pilotního panelu, které určují požadovanou polohu listů vrtule.

Po obdržení řídícího signálu aktuátor využívá elektrický pohon k ovládání hydraulických ventilů, které ovládají přítok hydraulického oleje do válců. Tím se mění délka válců a poloha vrtulových listů se upravuje.

To umožňuje pilotovi nebo řídícímu systému letadla regulovat tahu motoru, optimalizovat spotřebu paliva, řídit rychlost letadla nebo možnost zapraporování vrtule.

Engine Control Lever (ECL)

Jeho hlavní funkcí je umožnit pilotovi ovládat výkon a rychlost motoru, včetně nastavení režimů letu, brzdného tahu.

ECL je obvykle umístěn na pilotním panelu nebo v ovládací kabině a je připojen k regulátoru vrtule a dalším ovládacím mechanismům motoru. Pilot nebo řídící systém může posunout ECL do různých poloh, což ovlivňuje množství paliva dodávaného do motoru a tím i jeho výkon.

Pohyb ECL reguluje tahu motoru. Při posunutí ECL do předních poloh se zvyšuje dodávané palivo a tím i tah motoru. Naopak, posunutí ECL do zadních poloh snižuje dodávané palivo a snižuje tah motoru. Při správném ovládání ECL může pilot nebo řídící systém optimalizovat výkon motoru v různých fázích letu a letových režimech.

BETA Lever

BETA Lever je ovládací prvek umístěný na motoru turbovrtulového motoru. Jeho hlavní funkcí je ovládat BETA Valve, které je součástí regulátoru vrtule přímo na motoru. BETA Lever je ovládán pomocí Engine Control Leveru v kabině letadla.

Engine Control Lever (ECL) umožňuje pilotovi nebo obsluze ovládat pohyb BETA Leveru. Posunutím ECL se přenáší pohyb na BETA Lever na motoru, který pak upravuje polohu BETA Valve. Tím je regulován úhel náběhu vrtulových listů a ovlivňuje se brzdný efekt a regulace tahu vrtule.

Když je BETA Lever ve vypnuté poloze, BETA Valve je uzavřeno a vrtulové listy jsou nastaveny na normální letový úhel náběhu. Posunutím BETA Lever pomocí ECL do BETA režimu se otevírá BETA Valve a umožňuje se změna úhlu náběhu vrtulových listů, což vytváří brzdný efekt nebo reguluje tah letadla.

Pressure Relief Valve

Funkce Pressure Relief Valve spočívá v udržování optimálního tlaku oleje v systému. Pokud se tlak v olejovém systému příliš zvýší, Pressure Relief Valve se otevře a umožní vypuštění nadbytečného tlaku. Tím se zajišťuje bezpečnost a ochrana ostatních komponent regulátoru vrtule a motoru před příliš vysokým tlakem, který by mohl způsobit jejich poškození.

Pressure Relief Valve je navržen tak, aby uvolňoval tlak pouze při překročení bezpečného limitu. Když tlak v systému klesne na přijatelnou hodnotu, ventil se opět uzavře a zabraňuje úniku oleje. Tím se udržuje stabilita a správná funkce olejového systému a regulátoru vrtule.

Pressure Relief Valve obvykle nemá žádné zpětné vazby nebo nepodává žádné údaje jiným komponentám regulátoru vrtule. Jeho úlohou je pouze monitorovat a udržovat stanovený tlak v systému. Pokud je tlak v systému příliš vysoký, ventil odlehčení tlaku se otevře a umožní únik hydraulického média, čímž snižuje tlak na bezpečnou úroveň.

Pitch Lock Valve

Funkce Pitch Lock Valve spočívá v udržování stabilní polohy vrtulových listů ve vybraném úhlu náběhu. Když je Pitch Lock Valve aktivován, zajišťuje, že vrtulové listy zůstanou v dané poloze, čímž se udržuje konstantní úhel náběhu. To je důležité zejména při určitých

fázích letu, jako je start, vzlet, stoupání, klesání nebo přistání. Pitch Lock Valve se ovládá pomocí hydraulického aktuátoru a je integrován do regulátoru vrtule.

A/C Pitch Lock System

A/C Pitch Lock System je součástí regulátoru vrtule u turbovrtulového motoru, která slouží k uzamčení polohy vrtulových listů v určitých režimech.

Systém aktivuje na základě letových parametrů a nastavení regulátoru vrtule. Například při dosažení určité rychlosti nebo nadmořské výšky, nebo při konkrétní fázi letu, může systém automaticky zapnout A/C Pitch Lock a udržovat konstantní úhel náklonu listů vrtule.

Jakmile je systém aktivován, Pitch Lock Valve se otevře nebo uzavře podle požadovaného úhlu náklonu listů vrtule. Tímto způsobem je zajištěno, že listy vrtule zůstanou v požadované poloze a nebudou se pohybovat nekontrolovaně.

Control Valve

Funkce Control Valve spočívá v regulaci množství a směru průtoku oleje, který ovlivňuje polohu a pohyb vrtulových listů. Control Valve přijímá signály a instrukce ze systému řízení a na základě nich upravuje průtok oleje do jednotlivých aktuátorů, které ovládají pohyb vrtulových listů.

Přesná kontrola průtoku oleje pomocí Control Valve je důležitá pro správnou regulaci úhlu náběhu vrtulových listů a tím i pro generování optimálního tahu a výkonu motoru. Control Valve umožňuje pilotovi nebo řídícímu systému letadla přesné nastavení a přizpůsobení polohy vrtulových listů v závislosti na potřebách letu a různých režimech provozu.

Oil Inlet

Komponenta, která slouží k dodávání oleje do regulátoru vrtule u turbovrtulového motoru. Olej v systému regulátoru vrtule slouží k ovládání a změnám polohy listů vrtule. Olej je dodáván do regulátoru vrtule pomocí olejového vstupu a je dále řízen a distribuován pomocí různých komponent, jako je například čerpadlo, ventily a aktuátory.

Hlavní funkcí oleje v systému regulátoru vrtule je umožnit plynulou a přesnou změnu úhlu náběhu listů vrtule. Úhel náběhu listů vrtule ovlivňuje tah a brzdění letadla.

Olej je důležitý pro pohyb a uzamčení aktuátorů, které ovládají polohu listů vrtule. Správný průtok a tlak oleje je zásadní pro správnou a přesnou regulaci úhlu náběhu listů vrtule. Nedostatečný průtok nebo příliš vysoký tlak oleje mohou mít negativní dopad na správnou funkci a výkon regulátoru vrtule.

Gear Pump

Funkce Gear Pump spočívá v dodávání potřebného množství oleje do různých částí regulátoru vrtule. Pohybuje se pomocí ozubených kol, která vytvářejí tlak a poháněji olej skrz systém. Gear Pump je obvykle poháněn samotným motorem nebo pomocí jiného pohonného mechanismu, jako je hydraulický nebo elektrický motor.

Gear Pump zajišťuje dodávku oleje do důležitých částí regulátoru vrtule, jako je Pitch Lock Valve, BETA Valve nebo EHA (Electro-Hydraulic Actuator). Správný průtok a tlak oleje jsou klíčové pro správnou funkci těchto komponent a pro přesné ovládání polohy vrtulových listů.

One Way Valve

Tento ventil je navržen tak, aby umožňoval průtok oleje pouze v jednom směru. To znamená, že umožňuje plynulý a kontrolovaný průtok oleje v jednom směru, zatímco zabraňuje zpětnému toku oleje.

One Way Valve je obvykle vyroben z kvalitních materiálů, které jsou odolné vůči oleji a vyšším teplotám. Jeho konstrukce zahrnuje jednosměrnou klapku nebo membránu, která se otevírá a uzavírá v souladu s požadovaným směrem průtoku oleje.

Selection Valve

Hlavní funkcí Selection Valve je dodávat hydraulický olej do elektro-hydraulického aktuátoru, který je zodpovědný za ovládání pohybu a nastavení polohy listů vrtule. Tento ventil přijímá olej ze dvou hlavních zdrojů – Control Valve a Governor, a také z BETA Valve, pokud je aktivován BETA režim.

V běžném režimu letu, Selection Valve přepíná a řídí průtok oleje z Control Valve a Governoru. Tyto komponenty slouží k regulaci tlaku a průtoku oleje, aby bylo dosaženo správného nastavení polohy listů vrtule v souladu s požadavky letu.

V případě aktivace BETA režimu, Selection Valve přepíná proudění oleje z BETA Valve, který umožňuje regulaci úhlu náběhu vrtule pro brzdění nebo zpětný tah. Tímto

způsobem Selection Valve zajišťuje správný průtok oleje z BETA Valve do elektro-hydraulického aktuátoru, což umožňuje přesné ovládání a nastavení úhlu náběhu listů vrtule v BETA režimu.

Propeller Control Lever

Páka pro ovládání vrtule, součástí systému regulátoru vrtule u turbovrtulového motoru. Je umístěna v kokpitu letadla a slouží k ovládání nastavení otáček a polohy vrtule.

Propeller Control Lever může ovlivnit nastavení letového úhlu náběhu vrtulových listů. Tímto ovládáním pilot může měnit účinnost vrtule a přizpůsobit ji požadovaným letovým podmínkám.

Governor

Následující komponenty jsem zahrnul jako komplet a nazval Governor, který je zobrazený i v modelu. Jedná o sadu komponent, které ovládají normální režim letu.

- **Control Valve**: Funkce Control Valve spočívá v regulaci množství a směru průtoku oleje, který ovlivňuje polohu a pohyb vrtulových listů. Control Valve přijímá signály a instrukce ze systému řízení a na základě nich upravuje průtok oleje do jednotlivých aktuátorů, které ovládají pohyb vrtulových listů.
- **Flyweight Governor**: (regulátor s rotačními závažími) je součástí regulátoru vrtule, který slouží k udržování konstantní otáček vrtule. Jeho funkce spočívá v regulaci úhlu náběhu listů vrtule na základě otáček motoru a naměřených hodnot. Regulátor obsahuje rotační závaží, která jsou umístěna na rotační hlavě. Tyto závaží reagují na odstředivou sílu vyvolanou otáčkami motoru a pohybují pilotním ventilem, který ovládá tok oleje do mechanismu změny úhlu náběhu listů vrtule. Tím se dosahuje rovnováhy mezi sílami a udržuje se konstantní otáčky vrtule.
- **Speeder Spring**: (regulační pružina) jeho funkce spočívá v poskytování protitlaku proti působení rotačních závaží (flyweights) v regulátoru. Speeder spring je pružina, která je nastavitelná a vyvíjí sílu, která se snaží vyrovnat sílu rotačních závaží. Tato síla se přenáší na pilotní ventil, který ovládá tok oleje do mechanismu změny úhlu náběhu listů vrtule.
- **Pilot Valve**: Jeho hlavní funkcí je ovládat tok oleje do mechanismu změny úhlu náběhu listů vrtule na základě působení rotačních závaží (flyweights) a dalších signálů. Pilot Valve je umístěn v hřídeli pohonu a je poháněn rotačními závažími.

Pohyb rotačních závaží vyvolává otevření a uzavření kontrolních otvorů, které regulují přítok a odtok oleje do a z mechanismu vrtulových listů.

Tyto komponenty spolupracují prostřednictvím hydraulického systému, aby umožnily přesné a dynamické řízení vrtule v souladu s požadavky letu. Control Valve přijímá signály od flyweight governoru, Pilot Valve a dalších senzorů a na základě těchto signálů upravuje průtok oleje a nastavuje požadovaný úhel náběhu listů vrtule. Tím se ovlivňuje tah, rychlost a další charakteristiky letadla.

BETA Valve

BETA Valve je klíčovou komponentou v regulátoru vrtule u turbovrtulového motoru. Jeho hlavní funkcí je umožnit ovládání úhlu náběhu lopatek vrtule v tzv. BETA režimech.

BETA režimy se využívají brzdění na zemi nebo při provádění zpětného tahu. BETA Valve umožňuje regulovat úhel náběhu lopatek vrtule tak, aby se zvýšil odpor vůči vzduchu a vytvořil opačný tah, což přispívá k zpomalení letadla.

BETA Valve je ovládán pomocí BETA Leveru, který může být ovládán pilotem nebo řídicím systémem letadla. Pohyb BETA Leveru ovlivňuje otevření a uzavření BETA Valve, což dále upravuje úhel náběhu lopatek vrtule.

Při otevřeném BETA Valve se vzduch vedený mezi listy vrtule zvýší odpor vůči vzduchu a vytváří se tak negativní tah nebo brzdný efekt. Toto se využívá při přistání a brzdění na zemi, kdy je žádoucí snížit rychlost letadla.

Drain

Hlavní funkcí výpustí je umožnit efektivní odvádění odpadního oleje z regulátoru vrtule. Olej se může hromadit v různých částech systému, a pokud není správně vypouštěn, může způsobit poruchy nebo omezení výkonu vrtulového systému.

Výpustě jsou obvykle vybaveny odpovídajícími ventily nebo ventilovými systémy, které umožňují otevření a uzavření při potřebě vypuštění oleje.

Pro lepší přehled zde byli popsány všechny komponenty. Nejedná se jen o celkový popis komponent, ale i jejich funkce a další zjednodušený popis interakcí s dalšími komponenty. Informace od jednotlivých komponent byly z interních zdrojů GE a veřejně dostupných manuálů a příruček od Avia Propeller. [20] [21] [22]

6. Metodika – analýza STPA

Cílem této práce je navrhnout sadu bezpečnostních doporučení pro regulátor vrtule na turbovrtulovém motoru, a dané výsledky porovnat se současně využívanými metodami ve společnosti GEAC.

Praktická část se věnuje analýze STPA na regulátor vrtule. V práci jsou analyzovány jednotlivé interakce komponent mezi sebou a interakce mezi komponentami a lidským faktorem. Poté proběhne vytvoření strukturovaného modelu, kde jsou zobrazeny jednotlivé interakce, které budou v dalším kroku analyzovány a následně vybrány jednotlivé nebezpečné řídící akce. V posledním kroku budou vytvořeny ztrátové scénáře.

Při analýze regulátoru vrtule pomocí metody STPA budou identifikovány klíčové řídící akce, které mají vliv na jeho bezpečné fungování. STPA zkoumá, jak mohou chyby v řídících akcích vést k nebezpečným stavům, a navrhuje opatření k jejich prevenci a minimalizaci.

Při aplikaci metody STPA na regulátor vrtule je také důležité zohlednit specifické požadavky, omezení letadla a jeho provozu. Metoda STPA umožňuje komplexní analýzu včetně interakcí mezi komponenty regulátoru vrtule a dalšími systémy letadla, jako je řídicí systém motoru, avionika a posádka.

Metoda STPA nám představuje nový přístup a pohled k analýze regulátoru vrtule, který umožňuje identifikovat klíčová bezpečnostní rizika a poskytuje komplexní pohled na interakce mezi technickými a lidskými faktory. Ve srovnání se současnými metodami FMEA a FTA může metoda STPA přinést nový pohled na bezpečnost vrtulového systému, a tak přispět k dalšímu zlepšování bezpečnosti letadel a jednotlivých komponent.

6.1 První krok STPA

Prvním krokem v analýze STPA pro regulátor vrtule je stanovení účelu analýzy, identifikace ztrát a analýza hazardů spojených s regulátorem vrtule. Tento krok je klíčový pro pochopení rizik a potenciálních problémů spojených s provozem regulátoru vrtule. [13]

A. IDENTIFIKACE ZTRÁT

- L-1 Ztráty na životech či zranění
- L-2 Ztráty nebo poškození na motoru a regulátoru vrtule
- L-3 Ztráty nebo poškození na předmětech mimo letecký motor
- L-4 Ztráta účelu (přeprava)
- L-5 Ztráta zákaznické spokojenosti
- L-6 Ekologické ztráty – životní prostředí

B. IDENTIFIKACE SYSTÉMOVÝCH NEBEZPEČÍ

- H-1 Chybné nebo neúplné ovládání otáček
- H-2 Nemožnost nastavení úhlu
- H-3 Pilotova chyba – lidský faktor
- H-4 Chybné zapraporování vrtule nebo nemožnost zapraporování vrtule
- H-5 Nemožnost aktivování BETA režimu
- H-6 Selhání komponentů

C. IDENTIFIKACE OMEZENÍ

- SC-1 Regulátor vrtule musí vždy fungovat ve všech režimech letu [H-4, H-5]
- SC-2 Nastavení vrtule musí vždy možné ovládat [H-1, H-2]
- SC-3 Pilot musí být řádně vyškolen a provést úkony správně [H-3]
- SC-4 Všechny komponenty musí fungovat po celou dobu provozu [H-6]

Cílem tohoto prvního kroku STPA analýzy regulátoru vrtule je získat celkový přehled o rizicích a potenciálních problémech spojených s provozem regulátoru vrtule. Tímto způsobem lze lépe porozumět bezpečnostním požadavkům a navrhnout opatření k minimalizaci rizik a zlepšení bezpečnosti vrtulového systému.

6.2 Druhý krok STPA

Druhým krokem STPA je modelování řídící struktury. Tato struktura je vytvořena především pro přehlednost systému a skládá se z řídících prvků, kterým jsou přiřazeny řídící akce a následně zpětná vazba. Pro vytvoření této struktury je potřeba znát celý systém. [13]

Všechny komponenty jsou přebrány z dat FTA analýzy, která poskytla společnost GEAC. Jsou zachovány původní anglické názvy, aby nedošlo k nedorozumění v českých překladech.

Dále v rámci kroku 2 analýzy STPA je rozebrání, jak mezi sebou jednotlivé komponenty fungují a jaké mají mezi sebou interakce viz tabulka 1.

Tabulka 1 – Interakce mezi komponenty

Komponenty	Interakce mezi komponenty
A/C Feather Pump – EHO	A/C Feather Pump, jeho hlavní funkcí je poskytovat potřebný tlak pro pohyb vrtulových listů do polohy zavěšení (feathering). EHO je odpovědný za přesné ovládání polohy vrtulových listů v regulátoru vrtule. Interakce mezi A/C Feather Pump a EHO je realizována pomocí dodávky oleje do EHO. Díky této interakci může pilot nebo systém ovládání letadla rychle a spolehlivě provádět zavěšení vrtulových listů v případě potřeby.

ECL – BETA Lever	Nastavení Engine Control Leveru ovlivňuje dodávku paliva do motoru a také ovládání BETA režimu. Pohyb Engine Control Leveru ovlivňuje pohyb BETA Leveru a tím ovlivňuje otevření nebo uzavření BETA Valve. Tímto způsobem pilot může měnit úhel náběhu vrtulových listů do režimu revers a přizpůsobovat výkon a chování letadla různým letovým situacím.
A/C Feather Pump – Pressure relief valve	A/C Feather Pump je čerpadlo určené k zapraporování listů vrtule. Pressure Relief Valve je ventil, který je umístěn v systému olejového tlaku a slouží k uvolňování nadbytečného tlaku. Interakce mezi A/C Feather Pump a Pressure Relief Valve spočívá v tom, že A/C Feather Pump generuje tlak oleje potřebný pro zapraporování listů vrtule a tento tlak je regulován a udržován na správné úrovni právě díky fungování Pressure Relief Valve.
A/C Pitch Lock systém – Pitch Lock Valve	Pitch Lock Valve reaguje na signály a příkazy z A/C Pitch Lock systému a uzamkne polohu vrtulových listů, aby se zabránilo jejich nežádoucímu pohybu. Pitch Lock Valve udržuje polohu vrtulových listů stabilní a pevnou, což je důležité zejména při přistání a během letu v kritických fázích. Tímto způsobem interakce mezi A/C Pitch Lock systémem a Pitch Lock Valve zajišťuje správné uzamčení polohy

	vrtulových listů a poskytuje stabilitu a řízení vrtule v různých letových režimech.
ECL – Pilot Valve	ECL je páka nebo ovládací mechanismus umístěný v kokpitu letadla, který slouží k nastavení motoru. Jeho hlavní funkcí je umožnit pilotovi regulovat výkon motoru, včetně nastavení rychlosti motoru (RPM), přechodu mezi různými režimy letu a aktivaci specifických funkcí, jako je reverzní tah (BETA režim). Interakce mezi ECL a Pilot Valve spočívá v přenosu pohybu a ovládacích signálů z ECL na Pilot Valve. Pohyb ECL je přenášen na mechanický mechanismus, který ovládá otevření, uzavření nebo regulaci Pilot Valve. Tím se ovlivňuje tok oleje do dalších částí regulátoru vrtule a následně se mění poloha vrtulových listů.
Oil Inlet – Gear Pump	Oil Inlet poskytuje přívod oleje do Gear Pump. Gear Pump pak vytváří tlak a přečerpává olej dál do systému. Tímto způsobem se zajistí neustálý tok oleje a dostatečný tlak pro správnou funkci komponent systému regulátoru vrtule. Správná interakce mezi Oil Inlet a Gear Pump je důležitá pro zajištění dostatečného přívodu oleje a správného fungování celého systému.
PCL – GOVERNOR	PCL ovládá pozici regulátoru a tím ovlivňuje nastavení úhlu listů vrtule. Správné nastavení PCL je důležité pro

	dosažení optimálních výkonových charakteristik a bezpečnou provozu turbovrtulového motoru.
BETA Valve – Selection Valve	Interakce mezi BETA Valve a Selection Valve spočívá v tom, že do Selection Valve proudí olej z BETA Valve při aktivaci BETA režimu. Tím se umožňuje ovládání a nastavení úhlu náběhu vrtulových listů v BETA režimu.
BETA Valve – Drain	Interakce mezi BETA Valve a výpustí spočívá v tom, že výpusť umožňuje odpouštění tlaku z BETA Valve a vrtulových listů po ukončení použití BETA režimu. Tím se zajišťuje bezpečné a plynulé přecházení mezi různými režimy regulace vrtulových listů.
One Way Valve – BETA Valve	Interakce mezi One Way Valve a BETA Valve spočívá v tom, že One Way Valve zajišťuje správný směr průtoku oleje mezi těmito ventily. To umožňuje BETA Valve přijímat olej ze správného zdroje a regulovat jeho průtok do vrtulových listů v BETA režimu.
One Way Valve – EHO	Interakce mezi One Way Valve a EHO spočívá v tom, že One Way Valve reguluje průtok oleje do EHO. To umožňuje, aby EHO dostával správný objem oleje a mohl pohybovat se a nastavit polohu vrtulových listů v souladu s požadovaným úhlem náběhu.
Pitch Lock Valve – BETA Valve	Interakce mezi Pitch Lock Valve a BETA Valve je důležitá pro správné fungování vrtulového systému. Pitch Lock Valve

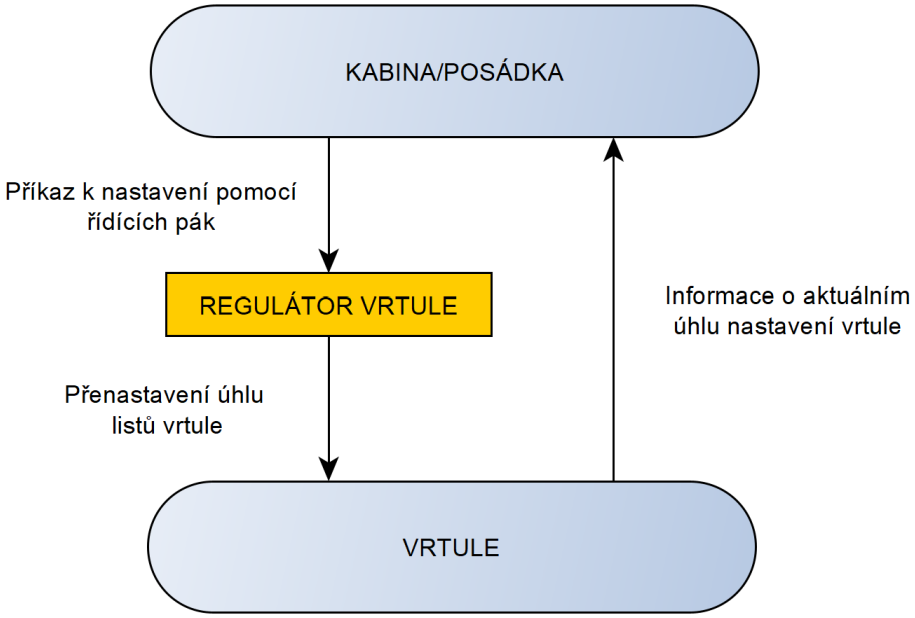
	zajišťuje, že vrtulové listy zůstanou uzamčené v předepsaných režimech, což je důležité pro stabilitu a bezpečnost letu. BETA Valve pak ovládá přítok oleje do EHO a ten ovládá nastavení vrtulových listů v BETA režimech.
EHO – Listy Vrtule	EHO je odpovědný za pohyb a nastavení polohy vrtulových listů v souladu s požadovaným úhlem náběhu. Je aktivován signálem z letového systému a převádí tento signál na pohyb, který ovlivňuje polohu listů vrtule. Interakce mezi EHO a listy vrtule spočívá v tom, že EHO pohybuje listy vrtule do požadované polohy. Při přijímání signálu se EHO a ovládá listy vrtule na požadovanou polohu.
Selection Valve – EHO	Pohybem Selection Valve do polohy pro regulaci rychlosti vrtule je vytvořen průtok oleje z Control Valve/BETA Valve do EHO, který ovládá polohu vrtulových listů. Tím se mění úhel náběhu listů vrtule.
Control Valve – Drain	Interakce mezi Control Valve a výpustí spočívá v tom, že Control Valve ovládá otevírání a uzavírání výpusti v souladu s požadovaným tlakem a průtokem oleje. Při potřebě snížení tlaku nebo odtoku oleje může Control Valve otevřít výpusť.
Pressure Relief Valve – Control Valve	V interakci mezi Pressure Relief Valve a Control Valve dochází k tomu, že Control Valve monitoruje tlak v systému a v případě nadměrného tlaku otevře

	Pressure Relief Valve, aby umožnil odtok oleje a snížení tlaku zpět na bezpečnou hodnotu.
Gear Pump – Control Valve	Gear Pump je čerpadlo, které přivádí olej do regulátoru vrtule. Jeho hlavní funkcí je zajistit dostatečný tlak a průtok oleje, který je potřebný pro pohyb a nastavení vrtulových listů. Interakce mezi Gear Pump a Control Valve spočívá v tom, že Gear Pump dodává olej pod tlakem do Control Valve.
BETA Valve – BETA Lever	BETA Lever je ovládán mechanicky pohybem Engine Control Lever. Pohybem Engine Control Leveru se přenáší pohyb na BETA Lever, který poté nastavuje polohu BETA Ventilu. BETA Ventil reguluje průtok oleje do aktuátoru.
Control Valve – Selection Valve	Selection Valve je ventil, který je zodpovědný za směrování průtoku oleje mezi různými komponentami regulátoru vrtule. Interakce mezi Control Valve a Selection Valve spočívá v tom, že Control Valve řídí množství oleje a tlak dodávaného do Selection Valve.
Control Valve – Pitch Lock Valve	Control Valve reguluje průtok oleje do vrtulových listů a umožňuje jejich plynulou změnu úhlu náběhu. Pitch Lock Valve je ventil, který je zodpovědný za uzamčení polohy vrtulových listů v určitých režimech letu.

	Jeho úlohou je zajištění stabilní polohy vrtulových listů při určitých provozních podmínkách. Interakce mezi Control Valve a Pitch Lock Valve spočívá v tom, že Control Valve řídí množství oleje a tlak dodávaného do Pitch Lock Valve, který následně uzamkne polohu vrtulových listů v souladu s požadovaným režimem letu
Control Valve – One Way Valve	Interakce mezi Control Valve a One Way Valve spočívá v tom, že Control Valve reguluje průtok oleje do vrtulových listů a zároveň zajišťuje, že tento olej proudí pouze jedním směrem pomocí One Way Valve. Tím se zajišťuje, že olej proudí správným směrem a nedochází k nežádoucímu zpětnému toku oleje.

Informace od jednotlivých komponent a interakcí jsou z interních zdrojů GE a veřejně dostupných manuálů a příruček od Avia Propeller. [20] [21] [22]

Jako poslední část tohoto kroku byl vytvořen model řídící struktury. Níže je vložen obecný model k popsání interakcí mezi stranami, které jsou zahrnuty v tomto modelu. Viz obrázek 15.



Obrázek 15: Obecný model řídící struktury regulátoru vrtule

Celé schéma s jednotlivými komponenty je v příloze 1.

6.3 Třetí krok STPA

Třetím krokem je zhodnocení všech řídících akcí a zjištění jaké nebezpečné akce mohou nastat. UCA (Unsafe control action – nebezpečné řídící akce) se odvozuje podle čtyř důvodů, kterými jsou:

- neprovedení vede k nebezpečí (Not providing causes hazard),
- provedení vede k nebezpečí (Providing causes hazard),
- příliš brzy, příliš pozdě, v nesprávném pořadí (Too early, too late, out of order),
- zastaveno příliš brzy, aplikováno příliš dlouho (Stopped too soon, applied too long). [13]

Při tvoření nebezpečných řídicích akcí bere tato práce v úvahu všechny čtyři typy UCA.

V některých případech se nedají všechny typy UCA použít. Pro příklad je k vidění část UCA v tabulce 2. Kompletní tabulka je v příloze 2.

Tabulka 2: Nebezpečné řídící akce

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Nastavení polohy vrtulových listů	UCA-26: Nedojde k akci EHA na ovládání polohy listů vrtule v předepsaných situacích [H-2, H-5, H-6]	UCA-27: Neoprávněné akci EHO na ovládání polohy listů vrtule. [H-2, H-5, H-6]	UCA-47: EHO přenastaví úhlu listů vrtule příliš brzy nebo příliš pozdě. [H-2, H-5, H-6]	N/A

6.4 Čtvrtý krok STPA

Posledním krokem STPA analýzy je vysvětlení, co vede k situaci a kdy dochází k nebezpečnému řízení. Toto vysvětlení je popsáno pomocí scénářů a jejich bezpečnostním omezením. Scénáře, které vedou k nebezpečnému řízení, odkazují buď na nebezpečné chování řídícího prvku nebo nedostatečnou zpětnou vazbu, případně jsou způsobeny neadekvátním řízením nadřazeného prvku. Bezpečnostní omezení předcházejí vzniku scénářům, které můžou vést ke vzniku nebezpečným řízením. [13]

V analýze bylo identifikováno 47 scénářů. Všechny scénáře i s bezpečnostními omezeními jsou v příloze 3. Níže v tabulce 3 zobrazen příklad pro UCA-26 a UCA-27.

Tabulka 3: Ztrátové scénáře

UCA	SCENARIO	CONSTRAINSTS
UCA-26: Nedojde k akci EHA na ovládání polohy listů vrtule v předepsaných situacích [H-2, H-5, H-6]	SC26.1: EHO selže a nedojde k provedení požadované akce na ovládání polohy listů vrtule v předepsaných situacích, například při změně letového režimu.	SC26.1C: EHO musí fungovat v každé fázi letu a nastavit požadovaný úhel na listech vrtule.
UCA-27: Neoprávněné akci EHA na ovládání polohy listů vrtule. [H-2, H-5, H-6]	SC27.1: Neoprávněná akce jako špatná manipulace při ovládání polohy listů vrtule SC27.2: Dojde k neoprávněné akci při poruše EHO, a nastaví polohu listů vrtule jinak, než bylo požadováno.	SC27.1C: Posádka musí vždy správně zacházet s ovládáním polohy listů vrtule. SC27.2C: EHO musí vždy správně nastavit úhel listů vrtule do požadované polohy.

7. Výstup STPA Analýzy – Bezpečnostní doporučení

Během práce na všech 4 krocích na STPA analýze, bylo vytvořeno celkem 47 scénářů a na ně doporučené bezpečností omezení. Vyplynuly z toho podmínky a doporučení pro správné fungování na daném systému regulátoru vrtule.

Na základě provedené analýzy regulátoru vrtule byla vypracována sada bezpečnostních doporučení, která se zaměřují na jednotlivé scénáře. Tyto doporučení jsou navržena s cílem minimalizovat rizika nežádoucích událostí a zajistit bezpečný provoz letounu.

Jednotlivé sady jsou rozděleny na oblasti pro lepší popis a rozdělení bezpečnostních doporučení. První oblastí je kabina/posádka, další oblastí je regulátor vrtule, kde jsou zahrnuty všechny komponenty regulátoru vrtule, dle strukturovaného modelu. V poslední oblasti se nachází oblast vrtule a nastavení, do této oblasti jsou zahrnuty EHO a listy vrtule.

7.1 Kabina a posádka

Do této části jsou zahrnuty všechny scénáře, které se týkají akcí, které vytvořila posádka nebo měla původ v kabině letounu a mělo to dosah na další komponenty v systému regulátoru vrtule. Popis bezpečnostních doporučení v tabulce 4.

Tabulka 4: Bezpečnostní doporučení oblast kabina/posádka

Bezpečnostní doporučení	Odkaz na scénáře
1) Posádka musí být řádně vyškolena a má výcvik na daný typ letadla.	SC1.1, SC2.1, SC3.1, SC3.2, SC4.2, SC5.1, SC5.2, SC6.1, SC12.1, SC12.2, SC15.1, SC16.1
2) Jasné a srozumitelné instrukce, příručky pro ovládání systémů, motoru a letadla.	SC1.1, SC2.1, SC3.1, SC5.2, SC6.1, SC10.1, SC11.1, SC46.3
3) Správné nastavení a kalibrace všech ovládacích pák.	SC1.2, SC4.1, SC9.1, SC10.1, SC12.2, SC46.1, SC46.2
4) Pravidelné kontroly a testování komponent.	SC1.2, SC1.3, SC4.1, SC10.1, SC11.1, SC15.2, SC46.1, SC46.2
5) Implementace pojistek nebo bezpečnostních mechanismů	SC5.1, SC8.2, SC8.3, SC9.1, SC12.1, SC12.2

7.2 Regulátor vrtule

V této části jsou zahrnuty scénáře, které se týkají všech komponent, které jsou součástí regulátoru vrtule. Popis bezpečnostních doporučení v tabulce 5.

Tabulka 5: Bezpečnostní doporučení oblast regulátor vrtule

Bezpečnostní doporučení	Odkaz na scénáře
1) Implementace monitorovaní tlaků, mezi komponenty	SC14.1, SC14.2, SC28.2, SC31.1, SC39.2, SC40.1, SC42.1, SC44.2
2) Pravidelná inspekce, údržba a testování pro zajištění správného fungovaní	SC13.1, SC13.2, SC13.3, SC17.1, SC18.1, SC18.2, SC19.1, SC20.1, SC20.2, SC21.1, SC22.2, SC24.1, SC28.1, SC28.2, SC29.2, SC30.1, SC31.1, SC33.1, SC34.1, SC35.1, SC35.2, SC37.1, SC38.1, SC39.1, SC40.1, SC41.1, SC42.1, SC44.1
3) Instalace filtrů nebo záchytných zařízení pro proudění oleje	SC13.3, SC17.2, SC18.2, SC21.1, SC29.2, SC30.2, SC33.1, SC39.2
4) Implementace zálohových systémů, omezovačů průtoku, nebo monitorovacích systémů pro případnou detekci poruch	SC14.1, SC14.2, SC19.1, SC21.2, SC22.1, SC23.1, SC24.1, SC25.1, SC29.1, SC31.1, SC34.1, SC35.1, SC36.1, SC36.2, SC41.1, SC42.1, SC43.1, SC44.1, SC45.1
5) Správné nastavení a kalibrace komponentů	SC24.1, SC25.1, SC36.1, SC36.2, SC37.1, SC43.1, SC45.1

7.3 Vrtule a nastavení

Do této části jsou zahrnuty ty scénáře, které se týkají konečného ovládání, které jsou mimo úroveň regulátoru vrtule. Je to EHO a přímo listy vrtule, které jsou jím ovládány. Popis bezpečnostních doporučení v tabulce 6.

Tabulka 6: Bezpečnostní doporučení oblast vrtule a nastavení

Bezpečnostní doporučení	Odkaz na scénáře
1) Správné nastavení a kalibrace EHO	SC47.1
2) Pravidelná inspekce, údržba a testování pro zajištění správného fungovaní	SC26.1
3) Implementace zálohových systémů, monitorovacích systémů pro případnou detekci poruch	SC26.1, SC27.2
4) Posádka je řádně vyškolena a má výcvik na daný typ letadla.	SC27.1

8. Porovnání analýz

V tomto kroku jsou podrobně rozebrány a porovnány metody a výsledky analýzy STPA a FTA. Zahrnuje popis a srovnání těchto metod z hlediska podobnosti, dostatečnosti, výhod a omezení. Dále je zkoumáno, zda je metoda STPA dostačující pro použití při vývoji turbovrtulových motorů.

8.1 Porovnání metod STPA a FTA

STPA (Systems-Theoretic Process Analysis) a FTA (Fault Tree Analysis) jsou dvě různé metody s rozdílnými přístupy používané k analýze bezpečnosti v rámci vývoje leteckých systémů. Každá z těchto metod má své specifické vlastnosti a přínosy pro identifikaci a minimalizaci bezpečnostních rizik.

STPA je novější metoda, která poskytuje systémový a komplexní pohled na bezpečnostní rizika. STPA se zaměřuje na interakce mezi jednotlivými částmi systému a analyzuje nejen technické selhání, ale také sociální a organizační faktory. Tato metoda se snaží odhalit všechna potenciální selhání, která mohou vyplývat z chyb v návrhu, provozních postupů nebo lidského jednání.

Výhody metody STPA spočívají v její schopnosti odhalit nová a nečekaná rizika, která by jinak mohla zůstat skryta pomocí tradičních analytických metod, jako je například FTA. Díky svému holistickému přístupu nabízí komplexní pohled na bezpečnost, což umožňuje lépe porozumět interakcím mezi jednotlivými částmi systému a identifikovat potenciální selhání zahrnující technické, organizační a lidské aspekty. STPA klade důraz na časné zásahy a preventivní opatření umožňuje minimalizaci rizik již v raných fázích vývoje nebo provozu, což přispívá k vyšší spolehlivosti, bezpečnost a snižování nákladů v rámci vývoje a výroby.

Nevýhodou STPA je, že je časově náročnější, vyžaduje více úsilí a zdrojů než metoda FTA, se kterou je STPA v této práci porovnávána. Vyžaduje detailní znalost systému a proces analýzy STPA. Zahrnutí sociálních a organizačních faktorů může být subjektivní a náročné na vyhodnocení.

Na druhé straně FTA je tradiční metoda používaná v oblasti analýzy spolehlivosti. Tato metoda se zaměřuje na identifikaci možných chyb nebo poruch v systému a jejich důsledků. FTA vytváří stromovou strukturu (fault tree), která vizualizuje vzájemné vztahy mezi událostmi a podmínkami, které vedou k nehodě nebo poruše systému a poskytuje kvantifikaci pravděpodobností, ale může se stát omezenou v identifikaci nových nebezpečí. Analýza FTA začíná od nežádoucího stavu nebo události a následně identifikuje postupně všechny možné příčiny tohoto stavu a jejich kombinace směrem ke

zdrojům a základním příčinám, což umožňuje identifikovat klíčové faktory vedoucí k problému. Cílem FTA je identifikovat kritické události a faktory, které mohou vést k těmto událostem a kvantitativní hodnocení, poté navrhnout opatření pro minimalizaci rizika.

8.2 Popis výstupu analýzy FTA

Pro účely srovnání a získání komplexnějšího pohledu na bezpečnost byla společností GEAC poskytnuta data z existující analýzy FTA (Fault Tree Analysis) pro regulátor vrtule. FTA analýza zahrnuje posouzení kritických případů (Hazardous Effects Assessment) a posouzení závažných případů (Major Effects Assessment). Analýza, ze které čerpám je uvedena jako příloha 4: Interní data poskytnutá firmou GEAC.

V části posouzení kritických případů existuje jen jeden případ, a to je:

- Výrazný tah v opačném směru, než jaký nařídil pilot. (Significant thrust in the opposite direction to that commanded by the pilot)

Jedná se o kritický případ, který musí být zařazen jako kritický dle předpisu CS-E 510 [7]

V druhé části posouzení závažných případů existuje celkem šest případů, jsou to následující případy:

- Nemožnost nastavení zapraporování vrtule (Impossibility to feather the propeller).
- Nemožnost nastavit úhel vrtule na povel (Inability to set propeller pitch when commanded)
- Výrazná změna úhlu vrtule bez příkazu (Significant uncommanded change to propeller pitch)
- Výrazné nekontrolovatelné kolísání tahu/výkonu (Significant uncontrollable thrust/power oscillation)
- Nepřikázaný úhel vrtule menší než minimální letový úhel nastavení (Uncommanded propeller pitch smaller than minimum flight pitch)
- Generování tahu většího, než je maximální jmenovitý tah (Generation of thrust greater than maximum rated thrust)

Pro každý jednotlivý případ byl stanoven cíl analýzy. Cílem prokázat je, že žádná pravděpodobná porucha nebo nesprávná činnost nezpůsobí nebezpečný nebo závažný případ.

Následně byla provedena analýza selhání v daném kontextu, která zahrnovala identifikaci technických komponent regulátoru vrtule a jejich potenciální chyby nebo nedostatečnou funkčnost.

Pro hodnocení pravděpodobnosti těchto selhání byla využita metoda Fault Tree, která byla rozšířena o zahrnutí bezpečnostních prvků, servisních informací a relevantních dat z provozu motorů M601 a H80.

Výstupem této analýzy je strom příčin selhání a kvantifikované pravděpodobnosti jednotlivých větví stromu, které slouží k hodnocení rizika a prioritizaci opatření.

8.3 Porovnání výsledků

Pokud porovnáme výsledky STPA analýzy se zjištěními výsledky z analýzy FTA, lze pozorovat, že obě analýzy poskytují různý pohled na bezpečnost a spolehlivost regulátoru vrtule.

Výstup STPA je soubor bezpečnostních doporučení, které jsou rozděleny na 3 oblasti, pro které jsou vytvořena bezpečnostní doporučen. Jsou to oblasti kabina/posádka, regulátor vrtule a jako poslední vrtule a její nastavení.

FTA se soustředí na systematické vyhodnocení existujících nebezpečných a závažných případů a jako výstup produkuje strom příčin selhání a kvalitativní výsledky možných kombinací selhaní spolu s kvantifikací pravděpodobností těchto selhání.

Prvním porovnáním a rozdílem v analýzách je popis ztrát a nebezpečí. V STPA u kroku 1 je uvedeno celkem 6 možných ztrát, jsou to například ztráty na životech, majetku, ztráta účelu či ekologické ztráty. Ztráty v FTA analýze nejsou přímo řešeny. Možné porovnání vzniká u definování rizik a nebezpečí. Níže je provedeno srovnání rizik mezi analýzami.

Z STPA analýzy pro *Chybné nebo neúplné ovládáni otáček* najdeme podobnost s 3 riziky u FTA analýzy, je to jedno kritické riziko *Výrazný tah v opačném směru, než jaký nařídil pilot. A dvě závažná rizika generováni tahu většího, než je maximální jmenovitý tah* a *výrazné nekontrolovatelné kolísaní tahu/výkonu*. V tomto případě se jedná o problematiku s tahem motoru. Výsledek hodnocení rizik mezi STPA a FTA je, že vypracovaná STPA analýza je pojata v hodnocení rizik obecněji než FTA, která má konkrétněji zaměřená rizika.

Další riziko z STPA, které má podobné alternativy u FTA analýzy je *nemožnost nastaveni úhlu náběhu*. Zde má FTA analýza podobnost u 3 případů. Jsou to případy *nemožnost nastavit úhel vrtule na povel, výrazná změna úhlu vrtule bez příkazu a nepřikázaný úhel*

vrtule menší než minimální letový úhel nastavení. Zde podobně jako v předchozím hodnocení rizik, je STPA analýza pojata obecněji a FTA má konkrétněji zaměřená rizika.

Jedno riziko vyplynulo stejné z obou analýz, tím rizikem je nemožnost zapraporování vrtule.

U STPA analýzy byli navíc přidány 3 rizika, která v FTA analýze chybí. Jedná se o *lidsky faktor – chyba pilota*, který je u FTA analýzy i v dalších krocích kompletně postrádán, *nemožnost aktivováni BETA režimu* a *selháni komponentu*, tyto dvě rizika by šla zakomponovat i do předešlých rizik STPA.

Dalším rozdílem mezi analýzami je postup, liší se v následujících bodech. U FTA se pokračuje stanovením příčin selhání, a vytvoření modelu stromu poruch. U metody jsou využita kvalitativní data, tj. příčiny selháni. Na tyto příčiny selhání komponent je následně vyprodukována kvantifikace pravděpodobností. Pro tu jsou využita data z provozu, kde se počítá s konkrétními čísly poruch a selhání jednotlivých komponent. Zatímco u STPA následuje krok 2, to je vytvoření modelu řídicích struktur, který slouží k vytvoření všech interakci v systému, poté proběhne identifikace nebezpečných řídících akcí v kroku 3. Dále jsou na tyto nebezpečné řídicí akce, v kroku 4, vytvořeny ztrátové scénáře.

Pro konkrétní srovnání a předvedení rozdílů v postupu je zvoleno stejně hodnocené riziko, tím je nemožnost zapraporovaní vrtule. Jsou zde porovnány scénáře STPA analýzy z kroku 4 a příčiny selhání z FTA analýzy.

Z STPA analýzy jsou převzaty interakce a nebezpečné řídicí akce *mezi A/C Feather Pump – EHO a EHO – Listy vrtule*, dostupné v tabulce příloze 2. Na tyto zvolené interakce mezi *A/C Feather Pump – EHO a EHO – List vrtule* jsou v kroku 4 vypracovány scénáře, viz. tabulka 7.

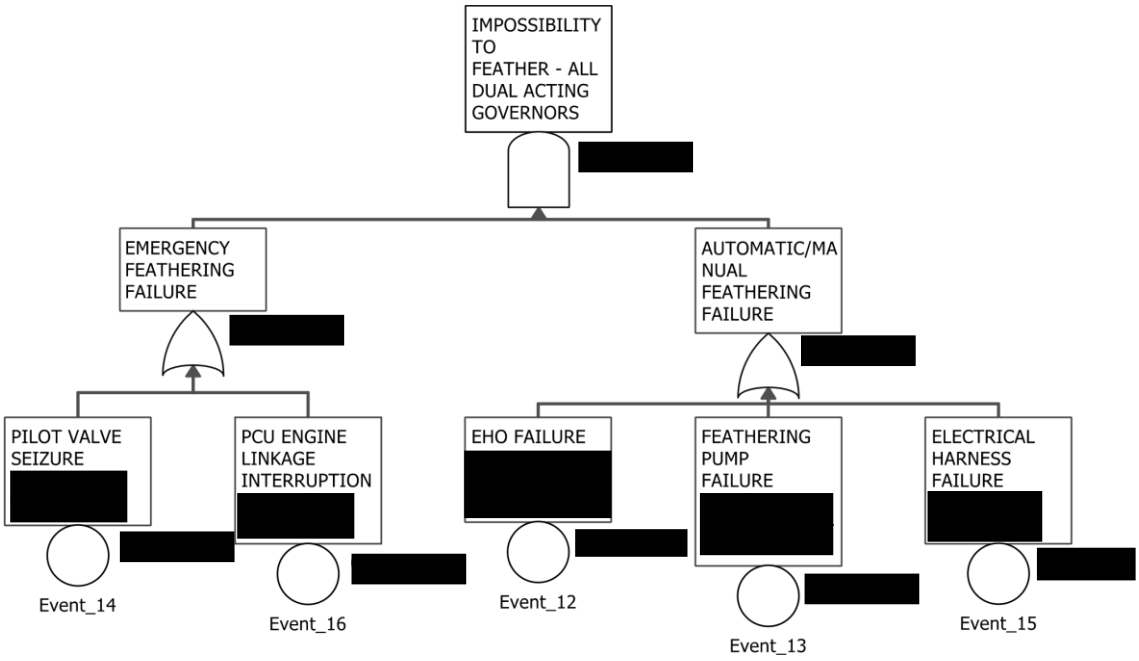
Tabulka 7: Scénáře pro interakci mezi A/C Feather Pump – EHO a EHO – Listy Vrtule

UCA	SCENARIO	CONSTRAINSTS
UCA-1: A/C Feather Pump nedodá potřebný tlak oleje pro zapraporování vrtule [H-2, H-4]	SC1.1: Neprovedení správného nastavení Propeller Control Leveru do polohy pro spuštění praporování. SC1.2: Elektro-hydraulický aktuátor nenastaví požadovaný úhel listů vrtule, protože je poškozen.	SC1.1C: Nutnost správného a úplného pohybu Propeller Control Leveru do polohy pro spuštění praporování. SC1.2C: Správné fungování elektro-hydraulického aktuátoru, který umožňuje pohyb listů pro spuštění praporování.

	SC1.3: A/C Feather Pump je poškozen nebo selhal.	SC1.3C: A/C Feather Pump musí vždy správně fungovat.
UCA-2: Nesprávné zapnutí A/C Feather Pump pro zapraporování vrtule [H-2, H-3]	SC2.1: Pilot provede chybné postupy při zapínání čerpadla pro zapraporování vrtule.	SC2.1C: Pilot provede vždy správné zapnutí čerpadla pro zapraporování vrtule.
UCA-3: A/C Feather Pump spustí nebo zastaví praporování listů příliš brzy, příliš pozdě [H-2, H-3]	SC3.1: Pilot spustí praporování listů příliš pozdě, když už by mělo být aktivováno. To může způsobit ztrátu příležitosti pro efektivní brzdění nebo reverzní tah. SC3.2: Pilot spustí praporování listů příliš brzy. Může dojít k narušení stability letadla a ztráty tahu.	SC3.1C: Pilot vždy provede spuštění praporování listů vrtule, včas a ve správný moment.
UCA-46: Dodávka oleje z A/C Feather Pump trvá příliš dlouho nebo nebyla ukončena. [H-4]	SC46.1: Zahájení dodávky oleje trvá příliš dlouho, může to vést ke zpoždění při přenastavení úhlu listů vrtule. To může ovlivnit výkon letadla, zejména při změnách rychlosti a přistávání. SC46.2: Neukončená dodávka oleje může znamenat nedostatečnou hydraulickou sílu pro přenastavení úhlu listů vrtule, což může ovlivnit kontrolu nad letadlem a jeho ovladatelnost.	SC46.1C: Dodávka oleje musí trvat stanovenou dobu požadovanou pro přenastavení vrtule.
UCA-26: Nedojde k akci EHA na ovládání polohy listů vrtule v předepsaných situacích [H-2, H-5, H-6]	SC26.1: EHO selže a nedojde k provedení požadované akce na ovládání polohy listů vrtule v předepsaných situacích, například při změně letového režimu.	SC26.1C: EHO musí fungovat v každé fázi letu a nastavit požadovaný úhel na listech vrtule.
UCA-27: Neoprávněné akci EHA na ovládání polohy listů vrtule. [H-2, H-5, H-6]	SC27.1: Neoprávněná akce jako špatná manipulace při ovládání polohy listů vrtule může vést k nebezpečným situacím SC27.2: Dojde k neoprávněné	SC27.1C: Posádka musí vždy správně zacházet s ovládáním polohy listů vrtule. SC27.2C: EHO musí vždy správně nastavit úhel listů

	akci při poruše EHO, a nastaví polohu listů vrtule jinak, než bylo požadováno.	vrtule do požadované polohy.
UCA-47: EHO přenastaví úhlu listů vrtule příliš brzy nebo příliš pozdě. [H-2, H-5, H-6]	SC47.1: Úhel listů vrtule je přenastaven příliš brzy, před dosažením požadovaných letových podmínek nebo provozních parametrů. Toto může vést k neefektivnímu využití motoru a neoptimálním letovým vlastnostem. SC47.2: Úhel listů vrtule je přenastaven příliš pozdě, což znamená, že nedochází k dostatečnému využití motoru nebo se neplní požadované letové parametry. To může mít negativní dopad na výkon letadla a spotřebu paliva.	SC47.1C: Zajištění správného načasování a synchronizace přenastavení úhlu listů vrtule s požadavky letových podmínek a provozních parametrů.

Oproti tomu z FTA analýzy rizika pro nemožnost zapraporování vrtule, jsou převzaty příčiny selhání. Dostupné v příloze číslo 4. Pro porovnání je níže strom příčin převzatý z FTA analýzy, jedná se o riziko pro *nemožnost zapraporování vrtule*: [21]



Obrázek 16: Strom příčin pro nemožnost zapraporování vrtule

Příčiny selháni následující:

Selhání EHO (EHO Failure), *Selhání A/C Feather Pump* (Feather Pump failure), *Selhaní elektriky* (Electrical harness failure), *Zadřeni pilotního ventilu PCU* (PCU Pilot Valve Seizure), *Přerušení spojeni mezi PCU a motorem* (PCU-Engine linkage interruption).

Níže jsou popsány rozdíly mezi jednotlivými analýzami, jedná se o porovnání scénářů, které nám představují možné nebezpečí či ztráty s příčinami selhání z FTA analýzy.

Zde se analýzy shodují v osmi scénářích. Jedná se o selhání jednotlivých technických komponent. Jsou to následující scénáře: SC1.2, SC1.3, SC46.1, SC46.2, SC26.1, SC27.2, SC47.1, SC47.2. Jedná se o selhání komponent Feather Pump nebo EHO, oba tyto komponenty jsou zahrnuty ve scénáři STPA i příčinách selhání FTA.

Naopak se neshodují scénáře SC2.1, SC3.1, SC3.2, SC27.1. Zde je prokázána výhoda STPA, kde pracuje a zahrnuje i lidský faktor jako je například chyba posádky. To u FTA nenajdeme v žádném případě, jelikož FTA pracuje jen s technickými prvky.

Na druhé straně u FTA je několik případů, které STPA analýza neidentifikovala. Jedná se o následují příčiny selhání: *Selhání elektriky, Zadření pilotního ventilu PCU, Přerušení spojení mezi PCU a motorem*. Důvodem je nezahrnutí elektrické části do analýzy STPA. Do STPA analýzy byly zahrnuty jen olejové a mechanické vazby v rámci regulátoru vrtule a oblast kabiny/posádky. Důvod nezahrnutí je nastavení jiných hranic STPA analýzy.

U následujících závažných rizik a jednoho kritického z FTA analýzy: *Výrazně nekontrolovatelné kolísaní tahu/výkonu*, *Generovaní tahu většího, než je maximální jmenovitý tah*, *Výrazný tah v opačném směru, než jaký nařídil pilot*, je v rámci analýzy pracováno i s FCU, který v STPA analýze zahrnut není, a proto toto riziko není porovnáváno. STPA analýza byla zvolena jen na regulátor vrtule, tudíž měla omezení a nebyla pojata široce jako FTA analýza.

U dalších FTA rizik jako jsou *nemožnost nastavit úhel vrtule na povel*, *výrazná změna úhlu vrtule bez příkazu*, jsou příčiny selháni velmi podobné jako u rizika *nemožnosti zapraporování vrtule*. Jedná se stejná selhaní technických komponent jako je selháni EHO, selhaní A/C Feather Pump, selhaní elektriky, zadření pilotního ventilu PCU nebo přerušeni spojení mezi PC a motorem. Navíc se zde nachází zadření PCU Control Valve. U STPA rizika nemožnost nastaveni úhlu, které je nastaveno vice obecně, oproti těmto dvou rizikům FTA, je k dispozici více scénářů, jelikož pracuje i s lidským faktorem. Jedná se například o scénář SC16.2 nesprávné použití PCL během letu, zde je jasné pochybení pilota.

U rizika *Výrazný tah v opačném směru, než jaký nařídil pilot. (Significant thrust in the opposite direction to that commanded by the pilot)*, který je brán jako kritické riziko, nebylo dále více popsáno, protože pracuje i s FCU, který není zahrnut v STPA analýze.

Další rozdíl je v zaměření. Zatímco obě analýzy se zaměřují na bezpečnost a spolehlivost regulátor vrtule, STPA analýza se také může zaměřovat na identifikaci nedostatků a problémů v řídicích strukturách a procesech, kde je zahrnut i lidsky faktor, což může vést ke komplexnějšímu pochopeni systému. FTA je v tomto směru limitována, jelikož zahrnuje jen technické prvky a jejich příčiny selhání.

Hlavní rozdílem těchto dvou analýz je forma výstupu a zahrnutí lidského činitele. Výstup STPA analýzy je prezentován ve formě doporučených bezpečnostních doporučení, která cílí na konkrétní scénáře. Naopak, FTA analýza poskytuje příčiny selhání, a na tyto příčiny vypracované kvantifikované pravděpodobnosti jednotlivých větví stromu, což pomáhá hodnotit rizika a prioritu jednotlivých selhání. A druhým je nezahrnutí lidského faktoru v rámci analýzy FTA, zatímco STPA analýza s ním pracuje a hodnotí procesy ním spojené.

Celkově lze konstatovat, že obě analýzy mají své přednosti a poskytují důležité informace o bezpečnosti a spolehlivosti regulátoru vrtule. Použití obou metod společně může poskytnout komplexnější pohled na bezpečnostní aspekty daného systému a pomoci identifikovat klíčová rizika a možná selhání, což umožní přijmout efektivnější bezpečnostní opatření.

9. Diskuse

Tato bakalářská práce se zabývá ověřením možnosti využití metody STPA (Systems-Theoretic Process Analysis) ve vývoji turbovrtulových motorů. Cílem bylo prozkoumat, zda STPA analýza může přinést užitečné informace pro zlepšení bezpečnosti a spolehlivosti regulátoru vrtule v leteckých turbovrtulových motorech. Pro dosažení tohoto cíle byla poskytnuta současná data firmou GEAC pro porovnání a zjištění nedostatků a rozdílů mezi metodami.

Nedílnou součástí bakalářské práce bylo vypracování STPA analýzy. Analýza STPA nám poskytla širší a komplexnější pohled na bezpečnost a spolehlivost regulátoru vrtule ve srovnání s metodou FTA. STPA se zaměřuje na identifikaci nových a nečekaných rizik, která byla přehlédnuta při tradiční analýze FTA. Díky celostnímu přístupu STPA zahrnuje technické, organizační a lidské aspekty a umožňuje lépe porozumět interakcím mezi jednotlivými částmi systému.

STPA analýza prokázala svou schopnost identifikovat ztrátové scénáře a omezení pro nebezpečné řídící akce a navrhnout odpovídající preventivní bezpečnostní doporučení a opatření. Díky holistickému přístupu umožňuje STPA analyzovat nejen technické aspekty, ale také organizaci a lidské faktory, což poskytuje komplexní a úplný pohled na bezpečnost tohoto systému. Jako výstup je navrhnuta sada bezpečnostních doporučení.

Výstup STPA analýzy je poté porovnán se současnou profesionálně vypracovanou analýzou FTA. Výstupy analýz jsou si v něčem podobné, pokrývají se, nicméně byli nalezeny i nedostatky a rozdíly mezi jednotlivými analýzami.

Prvním rozdílem je zaměření analýz – STPA může identifikovat nedostatky a problémy v řídících strukturách a procesech, což umožní komplexnější pochopení systému. Jelikož byla STPA analýza zaměřena specificky na regulátor vrtule, byli do při tvorbě analýzy zahrnuty jak komponenty, tak i lidský faktor.

Obě analýzy identifikovaly rizika spojená s regulátorem vrtule, v několika případech se lišila. Rizika spojená z pohledu STPA analýzy jsou více obecné a některá nezahrnují FCU, proto nebylo možné všechny případy porovnat. Rizika FTA jsou více konkrétní, jsou zaměřené na možné kritické a závažné případy, které by mohli nastat při provozu regulátoru vrtule. Tato zjištění poukazují na nedostatky obou analýz a ukazuje, že použití obou metod společně může poskytnout komplexnější a vyváženější pohled na hodnocení rizik v systému regulátoru vrtule. U STPA by bylo možné rozdělit do hierarchických úrovní, kde by bylo možné zaměřit se i na konkrétnější rizika. Další omezením je subjektivní názor, ten může ovlivnit jak a jakým způsobem jsou rizika identifikována.

Dále byl rozebrán další postup u jednotlivých analýz, a to u stejného případu nemožnost zapraporování vrtule. Po nastavení rizik se pokračuje rozdílnými postupy, ale ve výsledku je vidět porovnaní scénářů z STPA analýzy s příčinami selhání z FTA analýzy. Výsledky tohoto porovnaní se shodovali v selhaní jednotlivých komponent, ale obě analýzy měli i některé příčiny a scénáře rozdílné. U FTA scénářů byli navíc zahrnuta i elektrika, ta u STPA zahrnuta není. Důvodem je nezahrnutí elektrické části a FCU do analýzy STPA. Na druhé straně u STPA vyplynula výhoda zahrnutí i lidského faktoru, kde se objevili ztrátové scénáře pro pochybení nebo nedostatečné kvalifikace pilota. Zde byla nalezena limitace zaměření na regulátor vrtule, jelikož u STPA není zahrnuto a pracováno s FCU, ani elektrickou částí. Pokud by bylo FCU a elektrika zahrnuta, je možné, že by STPA analýza pokryla všechny možné příčiny selhání, a mohla nahradit nebo doplnit kvalitativní část FTA.

Největší rozdílem jednotlivých analýz je forma výstupu. STPA prezentuje doporučená bezpečnostní doporučení a opatření pro konkrétní scénáře, zatímco FTA poskytuje kvalitativní data ve formě příčin selhání a kvantifikované pravděpodobnosti jednotlivých větví stromu, což pomáhá hodnotit rizika a prioritu jednotlivých selhání. STPA neposkytuje kvantifikovaná data, tudíž v tomto směru nemůže nahradit současnou FTA analýzu. Na druhou stranu výstup STPA, čímž jsou bezpečnostní doporučení, kde je zahrnut právě chybějící lidský faktor, může doplnit současnou FTA analýzu pro posílení bezpečnosti a minimalizaci rizik.

Dosažené výsledky této bakalářské práce mají klíčový význam pro naplnění stanovených cílů. Ověření možnosti využití STPA analýzy ve vývoji turbovrtulových motorů poskytuje nové poznatky o bezpečnosti a spolehlivosti regulátoru vrtule. Analýza metod hodnocení spolehlivosti v letectví, zkoumání systémového modelu bezpečnosti STAMP a aplikace STPA analýzy na regulátor vrtule umožnily identifikovat klíčová rizika a navrhnout efektivní bezpečnostní opatření. Výsledky pomáhají lépe porozumět potenciálním nedostatkům v systému a procesech a přispívají k celkovému zvýšení bezpečnosti letounů s turbovrtulovými motory.

Vzhledem k tomu, že bezpečnostní analýzy jsou dynamickým procesem, mohou se objevovat nová rizika a problémy, které vyžadují další zkoumání a analýzu. Další kroky a příležitosti pro další výzkum mohou zahrnovat rozšíření analýzy na další komponenty motoru, posouzení vlivu lidského faktoru a provádění pravidelných revizí a aktualizací výstupních doporučení pro neustálé zlepšování bezpečnosti a spolehlivosti regulátoru vrtule.

Jak STPA, tak FTA analýzy mohou být citlivé na předpoklady, které jsou založeny na odborných znalostech a zkušenostech analytiků. Nesprávné nebo nepřesné předpoklady mohou vést k nepřesnostem a zkresleným výsledkům analýz.

Obě analýzy mají své omezení v komplexnosti, kterou mohou zachytit. STPA je schopná identifikovat systémové problémy a interakce, ale nemusí podrobně analyzovat jednotlivé technické aspekty. Naopak, FTA analýza může být omezena pouze na identifikaci selhání a následků bez zohlednění lidských faktorů a organizace.

Důležitým aspektem je zapojení odborníků z různých oborů. Spolupráce mezi techniky, inženýry a provozním personálem umožní získat holistický pohled na bezpečnost regulátoru vrtule. Tento multidisciplinární přístup umožní identifikovat komplexní rizika a navrhnout účinná preventivní opatření.

Zhodnocení účinnosti doporučení je nezbytné pro zlepšení analýz a revize opatření. Průběžné monitorování implementovaných bezpečnostních doporučení umožní ověřit jejich účinnost a případně upravit postupy pro dosažení lepších výsledků.

Zohlednění lidského faktoru je dalším důležitým hlediskem. Výzkum zaměřený na lidské faktory a jejich dopad na bezpečnost může pomoci identifikovat a řešit potenciální rizika spojená s lidským chováním a rozhodováním. Přizpůsobení analýz a preventivních opatření lidským faktorům může zvýšit celkovou bezpečnost a spolehlivost regulátoru vrtule.

Další vývoj metodik STPA a FTA nabízí široké možnosti pro zlepšení a rozšíření jejich použití v analýze bezpečnosti a spolehlivosti. Integrace obou metod dohromady umožní komplexnější analýzu rizik a pravděpodobností selhání. Automatizace analýzy přispěje k efektivnějšímu a rychlejšímu zpracování dat, zatímco rozšíření aplikace těchto metod do jiných odvětví poskytne užitečné poznatky a zvýší bezpečnost širokého spektra aplikací. Dále je důležité zapojení uživatelů a odborné veřejnosti do procesu analýzy, což umožní získat zpětnou vazbu a identifikovat potenciální rizika. Celkově lze očekávat, že neustálý vývoj nových metod a zaměření na lidský faktor přinesou pokrok v analýze bezpečnosti a spolehlivosti systémů.

Zjištění a doporučení z této práce mají široké možnosti aplikace v praxi. Navržená bezpečnostní omezení a opatření mohou být přímo aplikována v procesu vývoje turbovrtulových motorů a mohou přispět k zvýšení bezpečnosti a spolehlivosti těchto zařízení. Výstupy STPA analýzy mohou také sloužit jako základ pro revize současných bezpečnostních standardů a směrnic v oblasti leteckého průmyslu. Dále mohou být využity pro školení posádky a techniků, aby byli lépe informováni o potenciálních rizicích a jak jim předcházet.

Závěr

Cílem této práce bylo ověřit možnost využití spolehlivostních analýz v rámci vývoje a výroby turbovrtulových motorů pomocí modelu bezpečnosti STAMP. Pro dosažení tohoto cíle bylo použito analytické metody STPA založené na bezpečnostním modelu STAMP.

Nejprve bylo potřeba seznámit se s problematikou bezpečnostních a spolehlivostních metod užívaných v letectví. Poté seznámit se s danou komponentou turbovrtulového motoru, čím byl regulátor vrtule. Bylo zapotřebí seznámit se s jeho fungováním a jednotlivými komponenty pro dostatečnou znalost k vytvoření STPA analýzy.

Pro dosažení cíle jsem vytvořil STPA analýzu pro regulátor vrtule, jejímž výstupem je soubor bezpečnostních doporučení a výsledky poté srovnat se současně užívanou FTA analýzou.

Na základě provedené analýzy lze konstatovat, že STPA je užitečným nástrojem pro analýzu bezpečnosti systému regulátoru vrtule v rámci vývoje leteckých motorů. STPA analýza nám poskytla nový pohled pro identifikaci nových a nečekaných rizik, včetně zahrnutí lidského faktoru, který u FTA analýzy kompletně chybí. STPA se zaměřuje na prevenci problémů a identifikaci nedostatků v systému již v rané fázi vývoje a provozu. Pomocí STPA je možné identifikovat potenciální hazardy a nebezpečí, analyzovat interakce mezi komponenty a strukturami systému a navrhnout opatření pro zlepšení bezpečnosti a spolehlivosti ve vývoji turbovrtulových motorů.

Ve srovnání se současnou FTA analýzou, která se zaměřuje na prediktivní analýzu příčin selhání, má STPA několik výhod. Jedním z hlavních rozdílů je výstupní forma obou analýz. Zatímco FTA poskytuje kvalitativní výsledky a kvantitativní pravděpodobnosti selhání příčin a kvantitativní hodnocení rizika, STPA se zaměřuje na poskytování bezpečnostních doporučení. STPA umožňuje navrhnout a implementovat opatření pro zlepšení bezpečnosti na základě identifikovaných nedostatků a rizik se zahrnutím lidského faktoru.

Dalším rozdílem mezi STPA a FTA je jejich přístup k analýze. Zatímco FTA se soustředí na identifikaci konkrétních selhávajících komponent a konstruuje stromovou strukturu zobrazující kombinace těchto selhání vedoucí k nežádoucím událostem, STPA se zaměřuje na systémový pohled. STPA analyzuje interakce mezi různými komponenty a strukturami systému, což umožňuje lépe porozumět celkovému fungování systému a identifikovat potenciální nedostatky a rizika.

Je však důležité si uvědomit, že STPA nemůže zcela nahradit současnou FTA analýzu, protože FTA poskytuje kvantitativní hodnocení rizika a konkrétní čísla, která jsou důležitá

pro hodnocení bezpečnosti a navrhování konkrétních opatření. STPA nám kvantitativní část v této analýze neposkytuje, protože jako výstup byl zvolen soubor bezpečnostních doporučení, tudíž v tomto směru nemůže FTA nahradit. STPA je spíše zaměřena na odhalení potencionálních rizik a nebezpečí, prevenci problémů a posilování bezpečnostních opatření již v rané fázi vývoje.

Vzhledem k rozdílům ve výstupech a přístupu obou analýz je vhodné kombinovat STPA se současnou FTA analýzou pro dosažení komplexnější a efektivnější analýzy bezpečnosti systému regulátoru vrtule v rámci vývoje leteckých motorů. Kombinací obou metod je možné získat jak kvantitativní hodnocení rizika, tak i bezpečnostní doporučení, s ohledem na lidský faktor, která posilují preventivní opatření a minimalizují rizika spojená s regulátorem vrtule.

Je doporučeno zvážit začlenění STPA do analytického procesu při vývoji leteckých motorů, aby bylo možné využít jeho přínosů a posílit bezpečnostní opatření. Přestože STPA a FTA mají odlišný přístup a zaměření, jejich kombinace může přinést komplexní a vyváženou analýzu bezpečnosti a minimalizovat rizika spojená s regulátorem vrtule v rámci vývoje leteckých motorů.

Seznam použité literatury

1. General Electric Company – Company History. Read about how all the great companies came about! | Browse the list! [online]. Dostupné z: https://www.company-histories.com/General-Electric-Company-Company-History.html
2. Aviation History | GE Aerospace | GE Aerospace. Home | GE Aerospace | GE Aerospace [online]. Copyright © 2022 General Electric [cit. 28.11.2022]. Dostupné z: https://www.geaerospace.com/company/aviation-history
3. Walter Engines [online]. [cit. 2023-07-17]. Dostupné z: https://cs.wikipedia.org/wiki/Walter_(podnik)
4. General Aviaton Czech [online]. [cit. 2023-07-21]. Dostupné z: https://cs.wikipedia.org/wiki/GE_Aviation_Czech
5. GE and Czech Republic finalize investment agreement to build new turboprop headquarters to support Advanced Turboprop development program | GE Aerospace. Home | GE Aerospace | GE Aerospace [online]. Copyright © 2022 General Electric [cit. 30.11.2022]. Dostupné z: https://www.geaerospace.com/press-release/business-general-aviation/ge-and-czech-republic-finalize-investment-agreement-build
6. Turboprop Engine | SKYbrary Aviation Safety. SKYbrary Aviation Safety [online]. Copyright © SKYbrary Aviation Safety, 2021 [cit. 22.02.2023]. Dostupné z: https://www.skybrary.aero/articles/turboprop-engine
7. CSE 510 Safety Analysis. In: . EASA. Dostupné také z: https://www.easa.europa.eu/sites/default/files/dfu/agency-measures-docs-certification-specifications-CS-E-CS-E_Amendment-2.pdf
8. MOIR, Ian Moir a Allan SEABRIDGE. Aircraft Systems: Mechanical, Electrical, and Avionics Subsystems Integration. 2011. ISBN 978-1-119-96520-6.
9. PROF. ING. RUDOLF HOLUB, CSC. Spolehlivost letadlové techniky [online]. [cit. 2023-07-21]. Dostupné z: http://www.fsiforum.cz/upload/soubory/databaze-predmetu/QDS/QDS-skripta-SpolehlivostLetadloveTechniky.pdf. VUT.
10. ROLLS-ROYCE: The jet engine. 5. vydání. Derby, Velká Británie: The Technical Publications Department Rolls-Royce PLT, 1996. 292 s. ISBN 0902121 235
11. LEVESON, Nancy G., CAST Handbook [online]. [cit. 17.6.2021] Dostupné z: http://sunnyday.mit.edu/CAST-Handbook.pdf
12. Intro to Systems Theoretic Process Analysis (STPA) [online]. Dr. John Thomas [cit. 2023-07-17]. Dostupné z: http://psas.scripts.mit.edu/home/wp-

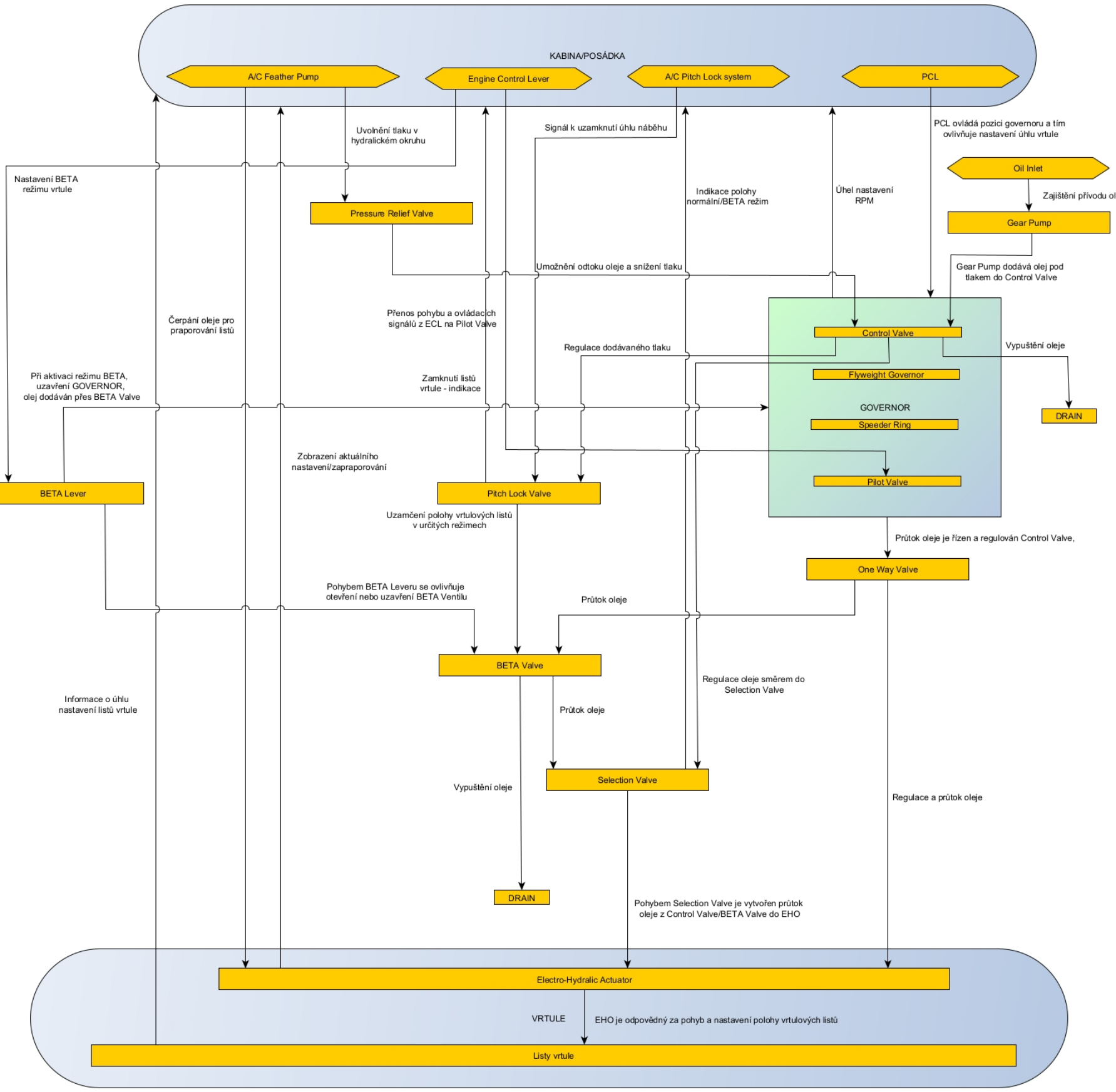
content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf

13. LEVESON, Nancy G. A John P. THOMAS, STPA Handbook [online]. [cit. 17.6.2021] Dostupné z: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
14. Failure Mode and Effect Analysis (FMEA) for Aerospace and Defense [online]. [cit. 2023-07-21]. Dostupné z: https://www.dsiintl.com/wp-content/uploads/2017/04/SAE20ARP5580.pdf
15. H-Series Turboprop engine family I [online]. [cit. 09.07.2023] Dostupné z: https://www.geaerospace.com/sites/default/files/GE-Aerospace-Hseries-datasheet.pdf
16. Walter Engine M601. Wikipedia.org [online]. [cit. 2023-07-09]. Dostupné z: https://cs.wikipedia.org/wiki/Walter_M601
17. Fault Tree Handbook. In: . Washington, D.C., 1981. [online]. [cit. 2023-07-09]. Dostupné také z: http://www.nrc.gov/docs/ML1007/ML100780465.pdf
18. Motor Walter M601 [online]. [cit. 2023-07-14]. Dostupné z: https://www.muzeum-kunovice.cz/walter-m601-b-8/
19. Motory [online]. [cit. 09.07.2023]. Dostupné z: https://www.geaviation.cz/motory
20. Manuál regulátor vrtule Avia Propeller [online]. In: . [cit. 2023-07-17]. Dostupné z: http://pdf.aviapropeller.cz/manuals/E-1500.pdf
21. GE Aviation Czech. Interní zdroj. Praha : GE Aviation Czech, 2023.
22. OPERATION AND INSTALLATION MANUAL [online]. [cit. 2023-07-17]. Dostupné z: http://pdf.aviapropeller.cz/manuals/E-1707.pdf

Seznam příloh

Příloha 1

Model řídící struktury


KABINA/POSÁDKA
A/C Feather Pump
Engine Control Lever
A/C Pitch Lock system
PCL
Uvolnění tlaku v hydralickém okruhu
Signál k uzamknutí úhlu náběhu
PCL ovládá pozici governoru a tím ovlivňuje nastavení úhlu vrtule
Oil Inlet
Zajištění přívodu oleje
Gear Pump
Gear Pump dodává olej pod tlakem do Control Valve
Nastavení BETA režimu vrtule
Pressure Relief Valve
Indikace polohy normální/BETA režim
Úhel nastavení RPM
Umožnění odtoku oleje a snížení tlaku
Čerpání oleje pro praporování listů
Přenos pohybu a ovládacích signálů z ECL na Pilot Valve
Control Valve
Regulace dodávaného tlaku
Vypuštění oleje
Flyweight Governor
Při aktivaci režimu BETA, uzavření GOVERNOR, olej dodáván přes BETA Valve
Zamknutí listů vrtule - indikace
GOVERNOR
Speeder Ring
DRAIN
Zobrazení aktuálního nastavení/zapraporování
Pilot Valve
BETA Lever
Pitch Lock Valve
Uzamčení polohy vrtulových listů v určitých režimech
Průtok oleje je řízen a regulován Control Valve,
One Way Valve
Pohybem BETA Leveru se ovlivňuje otevření nebo uzavření BETA Ventilu
Průtok oleje
BETA Valve
Regulace oleje směrem do Selection Valve
Informace o úhlu nastavení listů vrtule
Průtok oleje
Selection Valve
Vypuštění oleje
Regulace a průtok oleje
DRAIN
Pohybem Selection Valve je vytvořen průtok oleje z Control Valve/BETA Valve do EHO
Electro-Hydralic Actuator
VRTULE
EHO je odpovědný za pohyb a nastavení polohy vrtulových listů
Listy vrtule

Příloha 2

Nebezpečné řídící akce

Interaction	Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
A/C Feather Pump – EHO	Dodávka, spuštění, zastavení nebo změna intenzity čerpání oleje pro praporování listů.	UCA-1: A/C Feather Pump nedodá potřebný tlak oleje pro zapraporování vrtule. [H-2, H-4]	UCA-2: Nesprávné zapnutí A/C Feather Pump pro zapraporování vrtule. [H-2, H-3]	UCA-3: A/C Feather Pump spustí nebo zastaví praporování listů příliš brzy, příliš pozdě. [H-2, H-3]	UCA-46: Dodávka oleje z A/C Feather Pump trvá příliš dlouho nebo nebyla ukončena. [H-4]
ECL – BETA Lever	Nastavení ECL na režim BETA/Revers. Pohyb Engine Control Leveru ovlivňuje pohyb BETA Leveru.	UCA-4: Neprovedení posunu Engine Control Leveru do režimu BETA při přistání. [H-1, H-3, H-5, H-6]	UCA-5 Nepřiměřené nebo nevhodné použití Engine Control Lever. [H-1, H-5, H-3]	UCA-6: Nastavení ECL na BETA režim příliš brzy. [H-1, H-3, H-5]	N/A
A/C Feather Pump – Pressure relief valve	A/C Feather Pump generuje tlak oleje potřebný pro zapraporování listů vrtule, uvolnění nadbytečného tlaku díky Pressure Relief Valve.	UCA-7: Pressure Relief Valve neuvolní nadbytečný tlak v systému. [H-6]	N/A	UCA-8: Předčasné uvolnění tlaku v systému pomocí Pressure Relief Valve. [H-3, H-6]	N/A
A/C Pitch Lock system - Pitch Lock Valve	Pitch Lock Valve reaguje na signály a příkazy z A/C Pitch Lock systému a uzamkne polohu vrtulových listů, aby se zabránilo jejich	UCA-9: Nedojde k aktivaci Pitch Lock Valve po obdržení signálu/příkazu nebo nedojde k odeslání signálu z A/C Pitch Lock Systém. [H-2, H-6]	UCA-10: Nevhodné nebo chybné poslání signálu z A/C Pitch Lock System na zamknutí úhlu náběhu vrtule. [H-2, H-6]	UCA-11: Aktivace zamknutí úhlu nastavení vrtule příliš brzy před přistáním. [H-2, H-6]	N/A

	nežádoucímu pohybu.				
ECL – Pilot Valve	Pohyb ECL je přenášen na mechanický mechanismus, který ovládá Pilot Valve. Tím se ovlivňuje tok oleje do dalších částí regulátoru vrtule.	N/A	UCA-12: Pohyb na proveden Engine Control Leveru nekontrolovaně nebo neadekvátně. [H-1, H-3]	N/A	N/A
Oil Inlet - Gear Pump	Zajištění dostatečného přívodu oleje a správného fungování celého systému.	UCA-13: Nedochází k dodávce oleje z olejového vstupu do čerpadla. [H-6]	UCA-14: Dodávka oleje z olejového vstupu do čerpadla prováděna nevhodným způsobem – příliš velký tlak/průtok. [H-6]	N/A	N/A
PCL – GOVERNOR	PCL ovládá pozici governoru a tím ovlivňuje nastavení otáček motoru.	UCA-15: Nedojde k žádnému pohybu PCL a není provedena žádná akce. [H-3, H-2, H-6]	UCA-16: Nesprávná manipulace s PCL při nastavování úhlu nastavení listů vrtule. [H-2, H-3]	N/A	N/A
BETA Valve – Selection Valve	Do Selection Valve proudí olej z BETA Valve při aktivaci BETA režimu.	UCA-17: Z BETA Valve nedochází k žádnému proudění oleje do Selection Valve. [H-5, H-6]	N/A	N/A	N/A
BETA Valve – Drain	Odpouštění tlaku z BETA Valve.	UCA-18: Nedojde k vypuštění oleje z BETA Valve. [H-6]	UCA-19: Dojde k neoprávněnému vypuštění oleje z BETA Valve. [H-6]	N/A	N/A

One Way Valve – BETA Valve	One Way Valve zajišťuje správný směr průtoku oleje mezi těmito ventily.	UCA-20: Nedostatečný průtok oleje z One Way Valve do BETA Valve. [H-6]	UCA-21: Nesprávný průtok oleje nebo příliš vysoký tlak z One Way Valve do BETA Valve. [H-6]	N/A	N/A
One Way Valve – EHO	One Way Valve reguluje průtok oleje do EHO.	UCA-22: Nedojde k otevření/uzavření ventilu pro cestu oleje One Way Valve do EHO. [H-2, H-6]	UCA-23: Nežádoucímu otevření One Way Valve. [H-2, H-6]	N/A	N/A
Pitch Lock Valve – BETA Valve	Pitch Lock Valve zajišťuje, že vrtulové listy zůstanou uzamčené v předepsaných režimech.	UCA-24: Neuzamčení polohy vrtulových listů v předepsaných režimech. [H-5, H-6]	UCA-25: Uzamčení polohy vrtulových listů v nevhodných nebo nebezpečných režimech. [H-5, H-6]	N/A	N/A
EHO – Listy Vrtule	Nastavení polohy vrtulových listů.	UCA-26: Nedojde k akci EHA na ovládání polohy listů vrtule v předepsaných situacích. [H-2, H-5, H-6]	UCA-27: Neoprávněné akci EHA na ovládání polohy listů vrtule. [H-2, H-5, H-6]	UCA-47: EHO přenastaví úhlu listů vrtule příliš brzy nebo příliš pozdě. [H-2, H-5, H-6]	N/A
Selection Valve – EHO	Pohybem Selection Valve je vytvořen průtok oleje z Control Valve/BETA Valve do EHO.	UCA-28: Pokud Selection Valve selže, nedojde k přívodu hydraulického tlaku do elektro-hydraulického aktuátoru. [H-2, H-5, H-6]	UCA-29: Dojde k nesprávnému ovládání Selection Valve a nesprávnému přívodu hydraulického tlaku do aktuátoru. [H-2, H-5, H-6]	N/A	N/A
Control Valve – Drain	Vypuštění oleje.	UCA-30: Nedojde k vypuštění oleje z Control Valve. [H-6]	UCA-31: Dojde k neoprávněnému vypuštění oleje z Control Valve. [H-6]	N/A	N/A

Pressure Relief Valve – Control Valve	Umožnění odtoku oleje a snížení tlaku.	UCA-33: Nedojde k otevření Pressure Relief Valve a snížení tlaku na řízené cestě. [H-6]	UCA-34: Dojde k nežádoucímu otevření Pressure Relief Valve bez příslušného důvodu. [H-6]	N/A	N/A
Gear Pump – Control Valve	Gear Pump dodává olej pod tlakem do Control Valve.	UCA-35: Nedojde k čerpání oleje ze strany Gear Pump. [H-6]	UCA-36: Gear Pump nepřiměřeně nebo příliš silně čerpá olej. [H-6]	N/A	N/A
BETA Valve – BETA Lever	Pohybem BETA Leveru se ovlivňuje otevření nebo uzavření BETA Ventilu.	UCA-37: Nedojde k žádnému pohybu BETA Leveru a BETA Valve zůstává ve své aktuální poloze. [H-3, H-5, H-6]	UCA-38: BETA Lever nevhodně posunut nebo nevykonává pohyb na BETA Valve. [H-3, H-5]	N/A	N/A
Control Valve – Selection Valve	Regulace průtoku oleje do vrtulových listů.	UCA-39: Nedodání správného tlaku nebo průtoku z Control Valve do Selection Valve. [H-6]	UCA-40: Control Valve ovládá/tlak průtok oleje neúměrně nebo nevhodně. [H-6]	N/A	UCA-41: Control Valve předčasně zastaví dodávku oleje. [H-2, H-6]
Control Valve – Pitch Lock Valve	Regulace průtoku oleje do vrtulových listů.	UCA-42: Nedodání správného tlaku nebo průtoku z Control Valve do Pitch Lock Valve. [H-6]	UCA-43: Control Valve ovládá/tlak průtok oleje neúměrně nebo nevhodně. [H-6]	N/A	N/A
Control Valve – One Way Valve	Regulace průtoku oleje do vrtulových listů.	UCA-44: Nedodání správného tlaku nebo průtoku ze Control Valve do One Way Valve. [H-6]	UCA-45: Control Valve ovládá/tlak průtok oleje neúměrně nebo nevhodně. [H-6]	N/A	N/A

Příloha 3

Scénáře

UCA	SCENARIO	CONSTRAINSTS
UCA-1: A/C Feather Pump nedodá potřebný tlak oleje pro zapraporování vrtule. [H-2, H-4]	SC1.1: Neprovedení správného nastavení Propeller Control Leveru do polohy pro spuštění praporování. SC1.2: Elektro-hydraulický aktuátor nenastaví požadovaný úhel listů vrtule. SC1.3: A/C Feather Pump je poškozen nebo selhal.	SC1.1C: Nutnost správného a úplného pohybu Propeller Control Leveru do polohy pro spuštění praporování. SC1.2C: Správné fungování elektro-hydraulického aktuátoru, který umožňuje pohyb listů pro spuštění praporování. SC1.3C: A/C Feather Pump musí vždy správně fungovat.
UCA-2: Nesprávné zapnutí A/C Feather Pump pro zapraporování vrtule. [H-2, H-3]	SC2.1: Pilot provede chybné postupy při zapínání čerpadla pro zapraporování vrtule.	SC2.1C: Pilot provede vždy správné zapnutí čerpadla pro zapraporování vrtule.
UCA-3: A/C Feather Pump spustí nebo zastaví praporování listů příliš brzy, příliš pozdě. [H-2, H-3]	SC3.1: Pilot spustí praporování listů příliš pozdě, když už by mělo být aktivováno. To může způsobit ztrátu příležitosti pro efektivní brzdění nebo reverzní tah. SC3.2: Pilot spustí praporování listů příliš brzy. Může dojít k narušení stability letadla a ztráty tahu.	SC3.1C: Pilot vždy provede spuštění praporování listů vrtule, včas a ve správný moment.
UCA-4: Neprovedení posunu Engine Control Leveru do polohy BETA režimu při přistání. [H-1, H-3, H-5, H-6]	SC4.1: Dojde k mechanické poruše ECL, což zabraňuje správnému posunu Engine Control Leveru do režimu BETA. SC4.2: Pilot neprovede manipulaci s ECL, tedy posun do režimu BETA.	SC4.1C: ECL musí být vždy v provozu a letuschopném stavu pro ovládání letadla. SC4.2C: Pilot musí vždy správně manipulovat s pákou ECL, pro ovládání všech režimů letu.
UCA-5 Nepřiměřené nebo nevhodné použití Engine Control Lever. [H-1, H-5, H-3]	SC5.1: Pilot provede nepřiměřené použití ECL během fáze přistání, například nepřiměřené posunutí do polohy Revers nebo jiného nevhodného režimu. SC5.2: Pilot provede nevhodné použití ECL během fáze vzletu, například	SC5.1C: Pilot vždy správně použije ECL během různých fází letu, včetně omezení pro použití polohy Revers nebo jiných režimů.

	nepřiměřené posunutí do polohy Revers nebo jiného nevhodného režimu.	
UCA-6: Nastavení ECL na BETA režim příliš brzy. [H-1, H-3, H-5]	SC6.1: Pilot aktivuje BETA režim příliš brzy během fáze přistání, kdy ještě není vhodné nebo bezpečné používat BETA režim.	SC6.1C: Pilot musí vždy správně manipulovat s ECL a nastavení BETA režimu během vzletu a přistání, včetně omezení pro příliš brzkou aktivaci.
UCA-7: Pressure Relief Valve neuvolní nadbytečný tlak v systému. [H-6]	SC7.1: Ventil pro uvolňování tlaku nefunguje správně nebo se zablokuje, čímž znemožňuje účinné snižování tlaku v systému.	SC7.1C: Ventil pro uvolňování tlaku musí vždy fungovat, aby uvolnil nadbytečný tlak v systému.
UCA-8: Předčasné uvolnění tlaku v systému pomocí Pressure Relief Valve. [H-3, H-6]	SC8.1: Ventil určený k uvolňování tlaku je uzavřen/otevřen příliš brzy. To může vést k zablokování tlaku v systému a omezení pohybu listů.	SC8.1C Správné a přesné nastavení a funkčnost ventilu pro uvolňování tlaku je zásadní pro účinné a spolehlivé uvolňování tlaku v systému.
UCA-9: Nedojde k aktivaci Pitch Lock Valve po obdržení signálu/příkazu nebo nedojde k odeslání signálu z A/C Pitch Lock Systém. [H-2, H-6]	SC9.1: Poškození nebo selhání Pitch Lock Valve. SC9.2: A/C Pitch Lock z důvodu selhání nebo poškození nedokáže poslat požadovaný signál pro zamknutí nastavení úhlu nastavení listů. To znamená, že po provedení změny úhlu nastavení listů není zajištěno jeho správné a stabilní zamknutí.	SC9.1C: Pitch Lock Valve musí fungovat a být schopný uzamkout nastavení listů vrtule během všech fází letu. SC9.2C: A/C Pitch Lock System musí fungovat a být schopný poslat signál pro uzamčení nastavení listů vrtule během všech fází letu.
UCA-10: Nevhodné nebo chybné poslání signálu z A/C Pitch Lock System na zamknutí úhlu náběhu vrtule. [H-2, H-6]	SC10.1: A/C Pitch Lock System pošle chybný signál pro zamknutí úhlu náběhu vrtule v jiném než požadovaném úhlu.	SC10.1C: A/C Pitch Lock Systém vždy pošle správný signál pro nastavení a zamknutí úhlu náběhu vrtule na požadovanou hodnotu.
UCA-11: Aktivace zamknutí úhlu nastavení vrtule příliš brzy nebo příliš pozdě před přistáním. [H-2, H-6]	SC11.1: Předčasné aktivování zamknutí úhlu nastavení vrtule před přistáním. Vrtule je zamčena na pevný úhel příliš brzy před přistáním, možné prodloužení délky přistání.	SC11.1C: Včasné aktivování a zamknutí úhlu nastavení listů vrtule pro bezpečné přistání.

	SC11.2: Příliš pozdní aktivace zamknutí úhlu nastavení vrtule před přistáním. Vrtule není zamčena na požadovaný úhel včas před přistáním.	
UCA-12: Pohyb na Engine Control Leveru proveden nekontrolovaně nebo neadekvátně. [H-1, H-3]	SC12.1: Pilot nekontrolovaně posune Engine Control Lever dopředu. Dochází k vyššímu výkonu a možnému přehřátí motoru nebo přetížení letadla. SC12.2: Neadekvátní pohyb Engine Control Leveru dozadu. Dochází k poklesu tahu motoru a ovlivní letové vlastnosti letadla.	SC12.1C: Pilot vždy musí správně a kontrolovaně manipulovat s ECL.
UCA-13: Nedochází k dodávce oleje z olejového vstupu do čerpadla. [H-6]	SC13.1: Dojde k poruše nebo uzavření olejového vstupu do regulátoru vrtule. Nedostatečný nebo žádný přísun oleje do čerpadla. SC13.2: Gear Pump v systému čerpání oleje je nesprávně fungující nebo porušená. SC13.3: Dojde k blokádě v cestě oleje mezi olejovým vstupem a čerpadlem, například kvůli mechanické překážce nebo ucpanému filtru.	SC13.1C: Olejový vstup musí být vždy funkční a dodávat dostatečný přísun oleje. SC13.2C: Gear Pump musí vždy správně fungovat a čerpat požadované množství oleje. SC13.3C: Cesta mezi Oil Inlet a Gear Pump musí být vždy průchozí pro zajištění dostatečného průtoku oleje.
UCA-14: Dodávka oleje z olejového vstupu do čerpadla prováděna nevhodným způsobem – příliš velký tlak/průtok. [H-6]	SC14.1: Příliš vysoký tlak oleje při dodávce z olejového vstupu do čerpadla. SC14.2: Nedostatečné množství oleje při dodávce z olejového vstupu do čerpadla.	SC14.1C: Nutno vždy dodržovat maximální limity tlaku/průtoku oleje. SC14.2C: Nutno dodržovat minimální a požadované množství oleje při dodávce z olejového vstupu do čerpadla.
UCA-15: Nedojde k žádnému pohybu PCL a není provedena žádná akce. [H-3, H-2, H-6]	SC15.1: Pilot nemanipuluje s PCL. SC15.2: Dojde k mechanické poruše Propeller control lever (PCL), která brání jeho pohybu.	SC15.1C: Pilot musí správně manipulovat s PCL za všech okolností. SC15.2C: PCL musí být funkční za každé fáze letu,

		pro kompletní ovládání nastavení listů vrtule.
UCA-16: Nesprávná manipulace s PCL při nastavování úhlu nastavení listů vrtule. [H-2, H-3]	SC16.2: Nesprávné použití PCL během letu.	SC16.1C: Pilot musí vždy správně manipulovat s PCL ve všech fázích letu.
UCA-17: Z BETA Valve nedochází k žádnému proudění oleje do Selection Valve. [H-5, H-6]	SC17.1: Mechanická porucha Beta Valve nebo Selection Valve – Ventily se neotevřou ani neuzavřou kvůli fyzickému poškození, zaseknutí nebo selhání mechanismu. SC17.2: Blokování průtoku oleje do Selection Valve cizí látkou, například nečistotami nebo zablokovaným filtrem.	SC17.1C: Beta Valve a Selection Valve musí vždy správně fungovat. SC17.2C: Cesta mezi Selection Valve a BETA Valve musí být vždy průchozí, a bez závad, aby došlo k požadované dodávce oleje pro nastavení vrtule.
UCA-18: Nedojde k vypuštění oleje z BETA Valve. [H-6]	SC18.1: Odtokový ventil je mechanicky poškozený nebo nefunkční SC18.2: Cesta, kterou by měl olej proudit mezi BETA Valve a výpustí je blokovaná nečistotami, zbytky oleje nebo mechanickou překážkou.	SC18.1C: Odtokový ventil musí být vždy funkční a schopný odpustit nepotřebný olej. SC18.2C: Zajištění volné cesty mezi BETA Valve a výpustí pro odtok oleje. Použití vhodných filtrů a ochranných prvků na cestě oleje mezi Control Valve a výpustí, které minimalizují riziko blokády.
UCA-19: Dojde k neoprávněnému vypuštění oleje z BETA Valve. [H-6]	SC19.1: Dojde k poruše ovládacího mechanismu BETA Valve, který nekontrolovatelně otevírá nebo uzavírá vypouštěcí ventil.	SC19.1C: BETA Valve musí být funkční po celou dobu pro správné fungovaní a vždy nutno správně regulovat odpuštění oleje.
UCA-20: Nedostatečný průtok oleje z One Way Valve do BETA Valve. [H-6]	SC20.1: Dojde k mechanické poruše BETA Valve, která omezuje průtok oleje z One Way Valve. SC20.2: Dojde k mechanické poruše One Way Valve, která způsobuje omezený průtok oleje do BETA Valve.	SC20.1C: One Way Valve a BETA Valve musí být funkční po celou dobu užívání, a být schopen dodávat požadované množství a tlak oleje.

UCA-21: Nesprávný průtok oleje nebo příliš vysoký tlak z One Way Valve do BETA Valve. [H-6]	SC21.1: Dojde k nesprávnému průtoku oleje mezi One Way Valve a BETA Valve, například kvůli úniku nebo blokádě v cestě oleje. SC21.2: Dojde k zvýšenému tlaku oleje mezi One Way Valve a BETA Valve, například kvůli selhání regulace tlaku.	SC21.1C: Průtok musí být konstantní a regulovaný po celou dobu. SC21.2C: Regulace tlaku musí fungovat po celou dobou provozu motoru.
UCA-22: Nedojde k otevření/uzavření ventilu pro cestu oleje One Way Valve do EHO. [H-2, H-6]	SC22.1: Při pokusu o otevření One Way Valve nedojde k žádnému pohybu, například kvůli mechanické poruše ventilu nebo blokádě v cestě oleje. SC22.2: Při pokusu o uzavření One Way Valve nedojde k žádnému pohybu, například kvůli selhání ventilu nebo neúčinnému mechanismu uzavírání.	SC22.1C: One Way Valve musí být funkční po celou dobu, a to při otevírání i zavírání pro správnou regulaci průtoku a tlaku oleje.
UCA-23: Nežádoucímu otevření One Way Valve. [H-2, H-6]	SC23.1: Nežádoucí otevření One Way Valve způsobí nekontrolovaný průtok oleje do EHO, což může vést k nesprávnému nastavení listů vrtule a ovlivnit výkon a bezpečnost letadla.	SC23.1C: One Way Valve musí vždy správně fungovat a regulovat správný průtok do EHO.
UCA-24: Neuzamčení polohy vrtulových listů v předepsaných režimech. [H-5, H-6]	SC24.1: Pitch Lock Valve selže při uzamčení polohy vrtulových listů v předepsaných režimech, což znamená, že listy nejsou správně zajištěny a mohou se pohybovat nekontrolovaně.	SC24.1C: Zajištění spolehlivosti a odolnosti Pitch Lock Valve vůči selháním. Komponenta musí fungovat správně a uzamknout listy vrtule na signál.
UCA-25: Uzamčení polohy vrtulových listů v nevhodných nebo nebezpečných režimech. [H-5, H-6]	SC25.1: Nesprávné uzamčení polohy vrtulových listů v nevhodných nebo nebezpečných režimech může vést k omezení výkonu letadla, narušení letových vlastností nebo dokonce ke ztrátě kontroly nad letadlem.	SC25.1C: Zajištění správného provozu a kalibrace Pitch Lock Valve a BETA Valve.

UCA-26: Nedojde k akci EHA na ovládání polohy listů vrtule v předepsaných situacích. [H-2, H-5, H-6]	SC26.1: EHO selže a nedojde k provedení požadované akce na ovládání polohy listů vrtule v předepsaných situacích, například při změně letového režimu.	SC26.1C: EHO musí fungovat v každé fázi letu a nastavit požadovaný úhel na listech vrtule.
UCA-27: Neoprávněná akce EHO na ovládání polohy listů vrtule. [H-2, H-5, H-6]	SC27.1: Neoprávněná akce jako špatná manipulace při ovládání polohy listů vrtule může vést k nebezpečným situacím SC27.2: Dojde k neoprávněné akci při poruše EHO, a nastaví polohu listů vrtule jinak, než bylo požadováno.	SC27.1C: Posádka musí vždy správně zacházet s ovládáním polohy listů vrtule. SC27.2C: EHO musí vždy správně nastavit úhel listů vrtule do požadované polohy.
UCA-28: Pokud Selection Valve selže, nedojde k přívodu hydraulického tlaku do elektro-hydraulického aktuátoru. [H-2, H-5, H-6]	SC28.1: Při pokusu o ovládání Selection Valve nedojde ke správnému pohybu ventilu nebo nedojde k jeho otevření/uzavření. SC28.2: Nedojde k dostatečnému přívodu oleje do elektro-hydraulického aktuátoru, který je odpovědný za ovládání polohy vrtulových listů.	SC28.1C: Zajištění správného a fungování Selection Valve. Musí fungovat a dodávat olej pro požadované nastavení úhlu listů vrtule. SC28.2C: Selection Valve musí vždy zajistit dostatečný a nepřetržitého přívodu oleje do elektro-hydraulického aktuátoru.
UCA-29: Dojde k nesprávnému ovládání Selection Valve a nesprávnému přívodu hydraulického tlaku do aktuátoru. [H-2, H-5, H-6]	SC29.1: Při pokusu o ovládání Selection Valve dochází k chybě ve volbě požadované polohy ventilu nebo nevhodnému ovládacímu pohybu. SC29.2: Při pokusu o přívod hydraulického tlaku do aktuátoru dochází k problému s hydraulickým systémem, například úniku oleje, poruše trubek nebo nefunkčnosti čerpadla.	SC29.1C: Selection Valve musí vždy správně volit polohu ventilu dle požadavků na nastavení vrtule. SC29.2C: Cesta mezi Selection Valve a EHO musí být vždy průchozí, a bez závad, aby došlo k požadované dodávce oleje pro nastavení vrtule. Použití vhodných filtrů a ochranných prvků na cestě oleje mezi Control Valve a výpustí, které minimalizují riziko blokády.
UCA-30: Nedojde k vypuštění oleje z Control Valve. [H-6]	SC30.1: Odtokový ventil je mechanicky poškozený nebo	SC30.1C: Odtokový ventil musí být vždy funkční a

	nefunkční. SC30.2: Cesta, kterou by měl olej proudit mezi Control Valve a výpustí je blokovaná například nečistotami, zbytky oleje nebo mechanickou překážkou.	schopný odpustit nepotřebný olej. SC30.2C: Zajištění volné cesty mezi Control Valve a výpustí pro odtok oleje. Použití vhodných filtrů a ochranných prvků na cestě oleje mezi Control Valve a výpustí, které minimalizují riziko blokády.
UCA-31: Dojde k neoprávněnému vypuštění oleje z Control Valve. [H-6]	SC31.1: Dojde k poruše ovládacího mechanismu Control Valve, který nekontrolovatelně otevírá nebo uzavírá ventil.	SC31.1C: Control Valve musí být funkční po celou dobu pro správné fungovaní přenastavení listů vrtule.
UCA-33: Nedojde k otevření Pressure Relief Valve a snížení tlaku na řízené cestě. [H-6]	SC33.1: Pressure Relief Valve se neotevře z důvodu mechanické poruchy, například zablokování ventilem nebo porušení jeho těsnosti.	SC33.1C: Pressure Relief Valve musí vždy fungovat a zajistit možné odpuštění nadbytečného tlaku oleje.
UCA-34: Dojde k nežádoucímu otevření Pressure Relief Valve bez příslušného důvodu. [H-6]	SC34.1: Dojde k mechanické poruše Pressure Relief Valve, která způsobuje nežádoucí otevření ventilu bez příslušného důvodu. SC34.2: Dojde k chybě při regulaci tlaku v systému, což vede k nežádoucímu otevření Pressure Relief Valve.	SC34.1C: Pressure Relief Valve musí vždy fungovat a zajistit možné odpuštění nadbytečného tlaku oleje nebo nedošlo k nechtěnému úniku oleje. SC34.2C: Regulace tlaku v systému musí být prováděna přesně a spolehlivě, aby se zabránilo nežádoucímu otevření ventilu.
UCA-35: Nedojde k čerpání oleje ze strany Gear Pump. [H-6]	SC35.1: Gear Pump selže nebo nedokáže čerpat olej ze své strany, což zabraňuje přenosu oleje do Control Valve.	SC35.1C: Gear Pump musí fungovat a být schopný dodávat požadované množství a tlak oleje do systému regulátoru.
UCA-36: Gear Pump nepřiměřeně nebo příliš silně čerpá olej. [H-6]	SC36.1: Gear Pump čerpá olej nepřiměřenou rychlostí nebo množstvím, které přesahuje požadavky a kapacitu Control Valve. SC36.2: Gear Pump čerpá olej s příliš vysokým tlakem,	SC36.1C: Gear Pump musí vždy čerpat olej dle požadavků Control Valve. SC36.2C: Control musí vždy správně regulovat a dávat požadavky pro čerpání oleje z Gear Pump.

	který přesahuje odolnost a kapacitu Control Valve.	
UCA-37: Nedojde k žádnému pohybu BETA Leveru a BETA Valve zůstává ve své aktuální poloze. [H-3, H-5, H-6]	SC37.1: BETA Lever je zablokován nebo uvízl v jedné poloze, což brání jeho pohybu.	SC37.1C: BETA Leveru musí mít volný pohyb pro správnou funkcionalitu a ovládání BETA Valve.
UCA-38: BETA Lever nevhodně posunut nebo nevykonává pohyb na BETA Valve. [H-3, H-5]	SC38.1: BETA Lever je porušen nebo nefunkční, a proto BETA Valve zůstává ve své aktuální poloze, ačkoli je požadován pohyb	SC38.1C: BETA Lever musí vždy zajistit správný pohyb a funkcionalitu, jako je pohyb na BETA Valve.
UCA-39: Nedodání správného tlaku nebo průtoku z Control Valve do Selection Valve. [H-6]	SC39.1: Selhání Control Valve při dodávání tlaku do Selection Valve. SC39.2: Dojde k blokádě v cestě tlaku mezi Control Valve a Selection Valve, například kvůli mechanické překážce nebo ucpanému potrubí.	SC39.1C: Zajištění správného fungování Control Valve pro zajištění dodání tlaku. SC39.2C: Zajištění volné cesty mezi Control Valve a Selection Valve pro průtok oleje.
UCA-40: Control Valve ovládá/tlak průtok oleje neúměrně nebo nevhodně. [H-6]	SC40.1: Dojde k nesprávnému ovládání průtoku oleje ze strany Control Valve, například příliš velkým nebo malým průtokem v závislosti na požadavcích letu.	SC40.1C: Control Valve musí správně regulovat a ovládat tlak oleje, aby zajistil přesný a odpovídající průtok oleje do Selection Valve.
UCA-41: Control Valve předčasně zastaví dodávku oleje. [H-2, H-6]	SC41.1: Dojde k předčasnému zastavení dodávky tlaku ze strany Control Valve před dosažením požadovaného stavu nebo nastavení Selection Valve.	SC41.1C: Control Valve musí dodávat tlak po celou dobu než dojde k požadovanému stavu nastavení. SC41.2C: Selection Valve musí správně fungovat a dodávat tlak dále do EHO.
UCA-42: Nedodání správného tlaku nebo průtoku z Control Valve do Pitch Lock Valve. [H-6]	SC42.1: Dojde k nedodání správného tlaku ze Control Valve do Pitch Lock Valve, například kvůli poruše čerpacího systému nebo selhání regulace tlaku.	SC42.1C: Zajistit správné nastavení a regulaci tlaku ze strany Control Valve do Pitch Lock Valve.
UCA-43: Control Valve ovládá/tlak průtok oleje	SC43.1: Control Valve dodává příliš vysoký tlak oleje do Pitch Lock Valve, který překračuje bezpečné limity a	SC43.1C: Control Valve musí správně regulovat a ovládat tlak oleje, aby zajistil přesný

neúměrně nebo nevhodně. [H-6]	může narušit jeho správnou funkci a ovlivnit uzamčení polohy vrtulových listů.	a odpovídající průtok oleje do Pitch Lock Valve.
UCA-44: Nedodání správného tlaku nebo průtoku ze Control Valve do One Way Valve. [H-6]	SC44.1: Mechanická blokáda v cestě mezi Control Valve a One Way Valve, která brání průtoku oleje. SC44.2: Dojde k poruše Control Valve, která ovládá průtok oleje mezi Control Valve a One Way Valve.	SC44.1C: Cesta mezi Control Valve a One Way Valve musí být vždy průchozí pro dostatečný průtok oleje. SC44.2C: Control Valve musí správně fungovat a regulovat množství průtoku oleje po celou dobu.
UCA-45: Control Valve ovládá/tlak průtok oleje neúměrně nebo nevhodně. [H-6]	SC45.1: Control Valve nesprávně ovládá průtok oleje přes One Way Valve, například způsobuje příliš vysoký nebo příliš nízký průtok.	SC45.1C: Control Valve musí správně regulovat a ovládat tlak oleje, aby zajistil přesný a odpovídající průtok oleje přes One Way Valve.
UCA-46: Dodávka oleje z A/C Feather Pump trvá příliš dlouho nebo nebyla ukončena. [H-4]	SC46.1: Zahájení dodávky oleje trvá příliš dlouho, může to vést ke zpoždění při přenastavení úhlu listů vrtule. To může ovlivnit výkon letadla, zejména při změnách rychlosti a přistávání. SC46.2: Neukončená dodávka oleje může znamenat nedostatečnou hydraulickou sílu pro přenastavení úhlu listů vrtule, což může ovlivnit kontrolu nad letadlem a jeho ovladatelnost.	SC46.1C: Dodávka oleje musí trvat stanovenou dobu požadovanou pro přenastavení vrtule.
UCA-47: EHO přenastaví úhlu listů vrtule příliš brzy nebo příliš pozdě. [H-2, H-5, H-6]	SC47.1: Úhel listů vrtule je přenastaven příliš brzy, před dosažením požadovaných letových podmínek nebo provozních parametrů. Toto může vést k neefektivnímu využití motoru a neoptimálním letovým vlastnostem. SC47.2: Úhel listů vrtule je přenastaven příliš pozdě, což znamená, že nedochází k	SC47.1C: Zajištění správného načasování a synchronizace přenastavení úhlu listů vrtule s požadavky letových podmínek a provozních parametrů.

	dostatečnému využití motoru nebo se neplní požadované letové parametry. To může mít negativní dopad na výkon letadla a spotřebu paliva.	

Příloha 4

Interní data poskytnutá firmou General Electric Aviation Czech

INTERNÍ DATA POSKYTNUTÁ FIRMOU GENERAL ELECTRIC AVIATION CZECH

INTERNAL DATA PROVIDED BY GENERAL ELECTRIC AVIATION CZECH REPUBLIC

6 HAZARDOUS EFFECTS ASSESSMENT

6.1 SIGNIFICANT THRUST IN THE OPPOSITE DIRECTION TO THAT COMMANDED BY THE PILOT

6.1.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001, H80-200-002, H85-200-BC04 engine built configurations cause a "Significant thrust in the opposite direction to that commanded by the pilot" failure with a probability of occurrence in excess of that defined as Extremely Remote (ref. CS-E 510 (g)(2)(iii) and AMC E 510 (d)(i)).

6.1.2 Failure Definition

As specified in the AMC E 510, the CS-E 510 (g)(2)(iii) concerns Engine Failures resulting in significant thrust in the opposite direction to that commanded by the pilot can, depending on the flight phase, result in a hazardous condition relating to aircraft controllability.

6.1.3 Analysis Assumptions

An analysis has been made to identify engine failures that can cause significant thrust in the opposite direction to that commanded by the pilot. Each identified failure mode and contributing failure/condition was studied to determine if there are any likely situations that can cause this hazardous engine effect.

Possible contributing failures are summarized into the 2 failure modes:

1. Unintentional high forward thrust when reverse thrust is commanded (on ground)
2. Unintended movement of the propeller blades below the established minimum in flight low pitch position

6.1.4 Failure Modes

6.1.4.1 Unintended movement of the Propeller blades below the established minimum in-flight low-pitch position

The operation below the minimum flight pitch position is possible in the Beta mode. This mode is controlled by the Power control lever set below the idle regime during ground operation. Dual acting system provides safeguards preventing from failure condition occurrence. Beta mode is inactive during all flight modes except taxing and reverse mode.

BETA Valve is the element used for setting of minimal flight angle (Figure 1). BETA valve is mechanically connected with BETA lever and BETA carbon block, which is inserted into rotating propeller BETA ring. Axial movement of rotating BETA ring from Pick up angle to Minimal flight angle position is transferred through BETA carbon block and BETA lever to BETA valve.

Minimal flight pitch is established via Linear backward movement of BETA Valve blocks and supply of oil to propeller dome when BETA ring achieves position which corresponds to minimal flight pitch. The unintentional movement below this minimum flight pitch position is possible

only in case of failure of the Beta feedback system. In this situation, the beta valve doesn't prevent the propeller blades from movement below minimum flight angle up to full reverse, independently of the Power lever position (Figure 1).

The maintenance actions on the propeller governors to prevent Hazardous Engine effect are defined in the EMM and overview is listed in the Table 1.

Engine effect	Maintained device	Maintenance action interval	Source
Unintended movement of the Propeller blades below the established minimum in- flight low-pitch position	Propeller governors (P-W2X-3, P-W2X-4)	During installation, field replacement, troubleshooting or during Overhaul	

Table 1: Maintenance actions being carried out for preventing the occurrence of Hazardous Engine Effects

The propeller system consists of the pitch lock system (at engine and aircraft level) which provides prevention from unintentional movement of the propeller below minimal flight angle.

In case of the Beta feedback system failure, the propeller blades unintentional movement below the minimum blade angle can occur. Further movement of the BETA ring to the position that corresponds to the minimum in-flight low pitch electrically closes the BETA switch. This enables the pitch lock system that blocks oil supply through the BETA valve to the propeller dome and stops movement of the propeller blades below the minimum in-flight low pitch position.

The test switch (as a part of aircraft system), which is included in the pitch lock system, is used for the pitch lock system testing. Test of the pitch lock system is performed during unfeathering phase. When flipping the switch to "test" position, pitch lock system is enabled, it blocks oil supply to propeller dome and stops movement of the propeller blades to finer pitch (pass/fail criteria). As indicated in the Table 2, this check of the Pitch Lock system is carried on before every flight in accordance with the Aircraft Operation Manual.

Engine Failure mode	Object of the pre-flight verification	Verification interval	Source
Unintended movement of the Propeller blades below the established minimum in- flight low-pitch position	Pitch Lock solenoid valve	Before every flight	Aircraft Operation Manual

Table 2: Verification of the satisfactory functioning of safety or other devices at pre-flight

In the event of BETA valve hard seizure at the position when oil is supplied into propeller dome, the propeller blades are moving towards the negative pitch position. When BETA ring moves to the position below minimum flight pitch (established as minimum in-flight low pitch position), the Pitch Lock Valve is enabled and further movement of the propeller blades to the negative pitch is prevented.

When one way valve is contaminated by the impurities present in the oil. Due to contamination of one way valve, the pressurized oil is directly supplied to the propeller fine pitch cavity and the Pitch Lock Valve functioning is inhibited (Figure 1).

Both contributing failures must occur at the same time to achieve the uncommanded oil supply in the propeller dome fine pitch cavity. In the event of BETA valve hard seizure at the same time when one way valve is contaminated and thus provide direct supply of the pressurized oil to the propeller dome fine pitch cavity, the Pitch Lock Valve function is inhibited, and the propeller blades move towards the negative pitch position.

The top level Contributing Failures/Conditions related to the unintended movement of the Propeller blades below the established minimum in-flight low-pitch position were defined (see Table 3). The Safeguards and Design Considerations designed to reduce the likelihood of these undesired events, are presented in the Hazard Analysis table (Table 3).

Failure Mode	Contributing Failures/Conditions	Safeguards and Design Considerations
Unintended movement of the Propeller blades below the established minimum in-flight low-pitch position	Beta Feedback System Failure	[redacted]
	Pitch Lock System Failure on engine level	[redacted]
	Hard seizure of BETA valve in open position	[redacted]
	One way valve jam in open position due to oil contamination	[redacted]

Table 3: Unintended movement of the Propeller blades below the established minimum in-flight low-pitch position failure hazard analysis

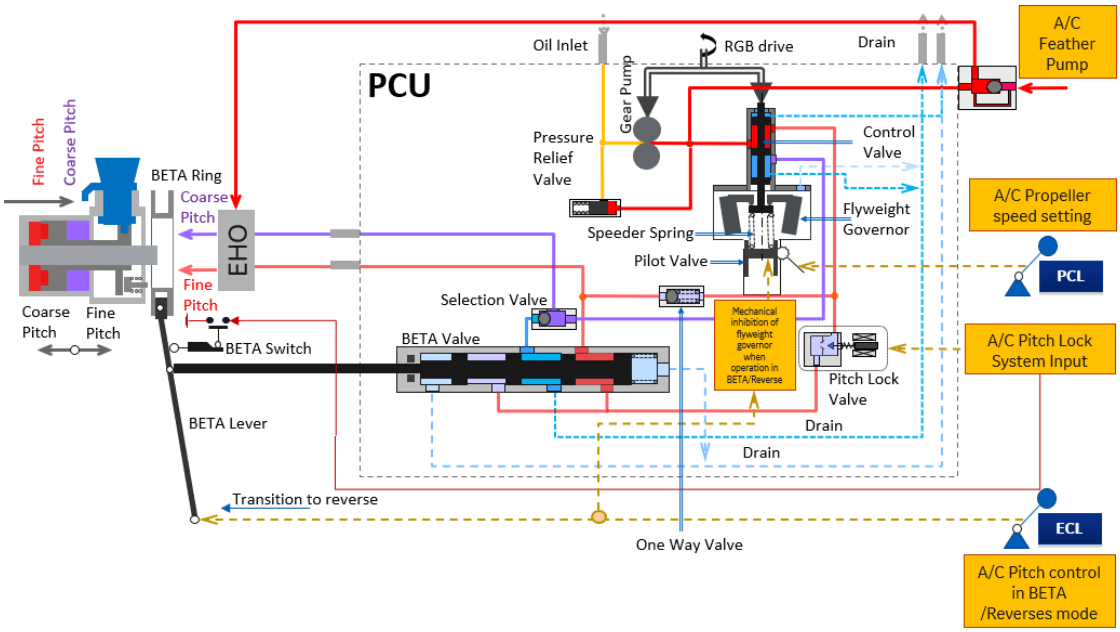


Figure 1: Propeller Control Unit (Propeller Governor)

6.1.4.2 Unintentional high forward thrust when reverse thrust is commanded

Following contributing failures/conditions for the "Unintentional high forward thrust when reverse thrust is commanded" failure mode were evaluated:

1. Unintentional forward thrust
2. Unable to reduce fuel flow to ground idle

For the purposes of this FTA the worst case scenario is assumed. If propeller is in the reverse mode and the "Unintentional forward thrust" occurs, the pilot has only a limited time to react when the propeller blades start to move from reverse mode towards the coarse pitch. To prevent the unintentional high forward thrust, the FCU primary circuit is used to reduce the fuel flow to ground idle or the FCU back-up lever is used to cut-off the fuel flow to the engine. Due to the limited reaction time, it is assumed that the pilot has the either option. Therefore, "OR" gate is used at the inability to reduce fuel flow in the appropriate FTA.

The Contributing Failures/Conditions related to the unintentional high forward thrust when reverse thrust is commanded (see Table 4) were defined. The Safeguards and Design Considerations designed to reduce the likelihood of this undesired events, are presented in the Hazard Analysis table (Table 4).

Failure Mode	Contributing Failures/Conditions	Safeguards and Design Considerations
Unintentional high forward thrust when reverse thrust is commanded	Unintentional forward thrust	[redacted]
	Unable to reduce fuel flow to ground idle	[redacted]

Table 4: High forward thrust when reverse thrust is commanded on ground failure hazard analysis

6.1.5 Analysis results

This analysis demonstrates that "Unintended movement of the Propeller blades below the established minimum in-flight low-pitch position" failure is controlled to a safe level through:

- The maintenance actions defined in the Engine Maintenance Manual
- The pre-flight pitch lock system test, which is done on the airframe level according to the Aircraft Operation Manual
- The safeguards and considerations of the Propeller Governor design

In case of all other subsystems, LRUs and the contributing failures/conditions, the top event failure is controlled to a safe level through safeguards and considerations that have been applied to the design.

The probability of the hazardous failure "Significant thrust in the opposite direction to that commanded by the pilot" was evaluated using the Fault Tree Analysis method expanded to the subsystems, local failure effects and contributing events

Conclusion

The analysis presents that the inherent design features, design considerations and safeguards (pursuant the engine maintenance on the H80-200-001/002 & H85-200-BC04 engine built configurations prevent from the occurrence of the defined failure modes.

Based on the Hxx/M601 service experience and supplier data, the calculated probability of occurrence of each failure mode is less than that defined as Extremely Remote [redacted]

- Unintended movement of the propeller blades below the established minimum in-flight low-pitch position [redacted]
- Unintentional high forward thrust when reverse thrust is commanded (on ground) [redacted]

The conclusion is that the single failures of propeller control system components do not result in "Significant thrust in the opposite direction" and probability of occurrence is Extremely Remote. Calculated probability of the top event failure is [redacted]

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
15	One way valve sticks open	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
19	Beta valve hard seizure in open position	[redacted]	[redacted]	[redacted]	
29	Beta Carbon failure	[redacted]	[redacted]	[redacted]	Based on Supplier analysis

Table 5: Significant thrust in the opposite direction to that commanded by the pilot contributing failures – failure rates substantiation

Unintentional high forward thrust when reverse thrust is commanded (on ground)					
9	FCU Condition Cam seizure	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
20	Total loss of pressurized oil to propeller governor	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
22	Mechanical inhibition of flyweight governor	[redacted]	[redacted]	[redacted]	
23	Speeder spring failure	[redacted]	[redacted]	[redacted]	
25	Uncommanded activation of Pitch Lock Valve	[redacted]	[redacted]	[redacted]	
26	Uncommanded activation of Electrohydraulic actuator	[redacted]	[redacted]	[redacted]	

Table 6: Subdiagram HI_FWD_TH_REV - Contributing failures/conditions – failure rates substantiation

Pitch Lock System Failure on Engine Level					
11	Beta switch failure. Not engaged when propeller blades moves below minimum flight pitch	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience
12	Harness failure due to fire	[redacted]	[redacted]	[redacted]	
14	Single stage Pitch Lock solenoid failure	[redacted]	[redacted]	[redacted]	
Beta Feedback System Failure					
16	Unsecured/disconnected rod due to maintenance error	[redacted]	[redacted]	[redacted]	Based on maintenance error estimation (GE experience)
17	Linkage disconnection	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience

4	Beta valve binding in open position	[redacted]	[redacted]	[redacted]	
27	Beta valve hard seizure in open position	[redacted]	[redacted]	[redacted]	
18	Substantial vibration caused by rotor unbalance	[redacted]	[redacted]	[redacted]	Engineering judgment based on Hxx/M601 experience. Undeveloped event because information is unavailable
5	Push/pull lever failed to provide correct interface	[redacted]	[redacted]	[redacted]	Based on Supplier data

Table 7: Subdiagram UN_MOV_MFP - Contributing failures/conditions – failure rates substantiation

FCU Emergency Circuit Control Failure					
6	Emergency circuit control mechanism failure	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
2	Emergency control valve jamming	[redacted]	[redacted]	[redacted]	
1	Emergency control valve gear damage	[redacted]	[redacted]	[redacted]	

Table 8: Subdiagram 1_5 - Contributing failures/conditions – failure rates substantiation

7 MAJOR EFFECTS ASSESSMENT

7.1 IMPOSSIBILITY TO FEATHER THE PROPELLER

7.1.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will cause an impossibility to feather the propeller at a rate in excess of that defined as Remote.

7.1.2 Failure Definition

Impossibility to feather the propeller occurs when feathering functions of Propeller Control Units P-W2X-3/P-W2X-4 and EHO LUN 7880.01-8 (with External Feathering Pump) are inoperative (Figure 1).

7.1.3 Failure Modes

7.1.3.1 PCU Pilot Valve seizure

Propeller Governor Pilot valve seizure due to contamination leads to inability to move the pilot valve (through inability to control the tension of the speeder spring) into the position that corresponds to the feather condition (Figure 1).

7.1.3.2 PCU and engine connection interruption

To feather the propeller, the PG control valve shall be moved. To do this, the speeder spring must be fully uploaded (Figure 1). This is done by movement of pilot valve to upward position by means of PG engine linkage. In the event of linkage interruption, the PCL in the cockpit does not control the tension of the speeder spring anymore.

7.1.3.3 EHO failure (Feathering through Feathering Pump + EHO)

In normal function, when EHA/EHO is energized it bypasses PG and oil from the AGB is directly provided to propeller dome by feathering pump. In case of EHA/EHO malfunction, the PG is not bypassed (Figure 1).

7.1.3.4 Feathering pump failure

In case of feathering pump gear failure, the feathering pump is unable to provide pressurized oil to the propeller dome and propeller cannot be feathered (Figure 1).

7.1.3.5 Electrical harness failure (Feathering through Feathering Pump + EHO)

When integrity of harness is lost, the power supply to the EHO/EHA is interrupted and it cannot be energized, thus cannot bypass the PG and feather the propeller.

7.1.4 Probability Assessment

Propeller feathering can be accomplished by either one of the two independent feathering systems (Emergency feathering via PG & Automatic/Manual feathering via aircraft feathering system) and the complete impossibility to feather occurs only if these systems are both in the specific failed condition.

The probability of the failure “Impossibility to feather the propeller” was evaluated using the Fault Tree Analysis method (Figure 2) expanded to the subsystems described above, based mainly on the safeguards incorporated in the design of the H80 engine and on the H80 & M601 service experience. The probability of occurrence of the failure “Impossibility to feather the propeller” is less than that defined as Remote.

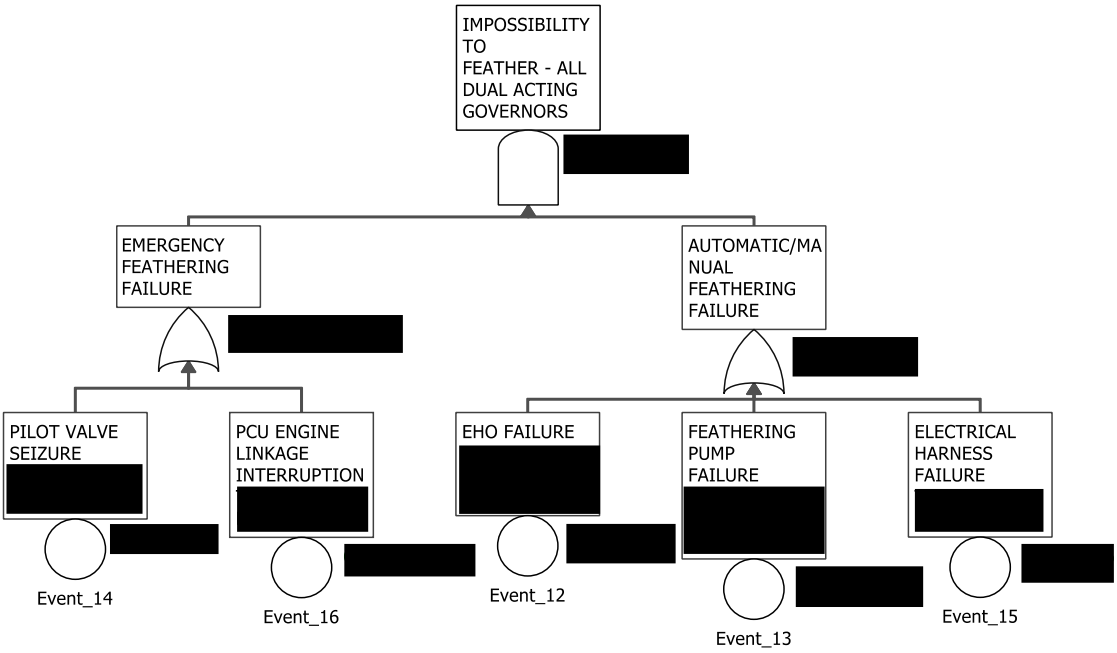


Figure 2: An impossibility to feather the propeller - H80-200-001/002 & H85-200-BC04 FAULT TREE ANALYSIS

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
Automatic/Manual Feathering Failure					
12	EHO failure				Based on M601/Hxx accumulated data and field experience & Based on Supplier data
13	Feathering pump failure				
15	Electrical harness failure				
Emergency Feathering Failure					
14	Pilot valve seizure				Based on M601/Hxx accumulated data and field experience & Based on Supplier data
16	PCU-ENGINE linkage interruption				Based on M601/Hxx accumulated data and field experience

Table 9: "An impossibility to feather the propeller" contributing failures/conditions - failure rates substantiation

7.2 INABILITY TO SET PROPELLER PITCH WHEN COMMANDED

7.2.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will cause an inability to set the propeller pitch when commanded at a rate in excess of that defined as Remote.

7.2.2 Failure Definition

Inability to set propeller pitch when commanded is either a result of oil contamination, which will cause clogging of the PG valves that will prevent their satisfactory function or an effect of the loss of linkage/feedback between the engine and the PG.

7.2.3 Failure Modes

7.2.3.1 PCU Control valve seizure (Inability to change propeller pitch)

Propeller governor Control valve seizure due to oil contamination leads to inability to distribute the oil in and out the propeller dome, therefore the propeller pitch is not changed when it is commanded by the PCL (Figure 1).

7.2.3.2 Interrupted connection between PCU and engine (Inability to change propeller speed)

On the constant speed propellers, the propeller speed is controlled by the propeller pitch. In the event of PG-engine linkage separation, the PCL in the cockpit does not control the tension of the speeder spring anymore. Therefore, the propeller speed (pitch) will not change when it is commanded (Figure 1).

7.2.3.3 Seizure of the Pilot Valve (Inability to change propeller speed)

Propeller governor Pilot valve seizure due to contamination leads to inability to set the pilot valve to the position, which corresponds to the required propeller speed (pitch) (Figure 1).

7.2.4 Probability Assessment

The probability of the failure “Inability to set the propeller pitch when commanded” was evaluated using the Fault Tree Analysis method (Figure 3) expanded to the subsystem described above, based mainly on the safeguards incorporated in the design of the H80 engine and on the H80 & M601 service experience. The probability of occurrence of the failure “Inability to set the propeller pitch when commanded” is less than that defined as Remote.

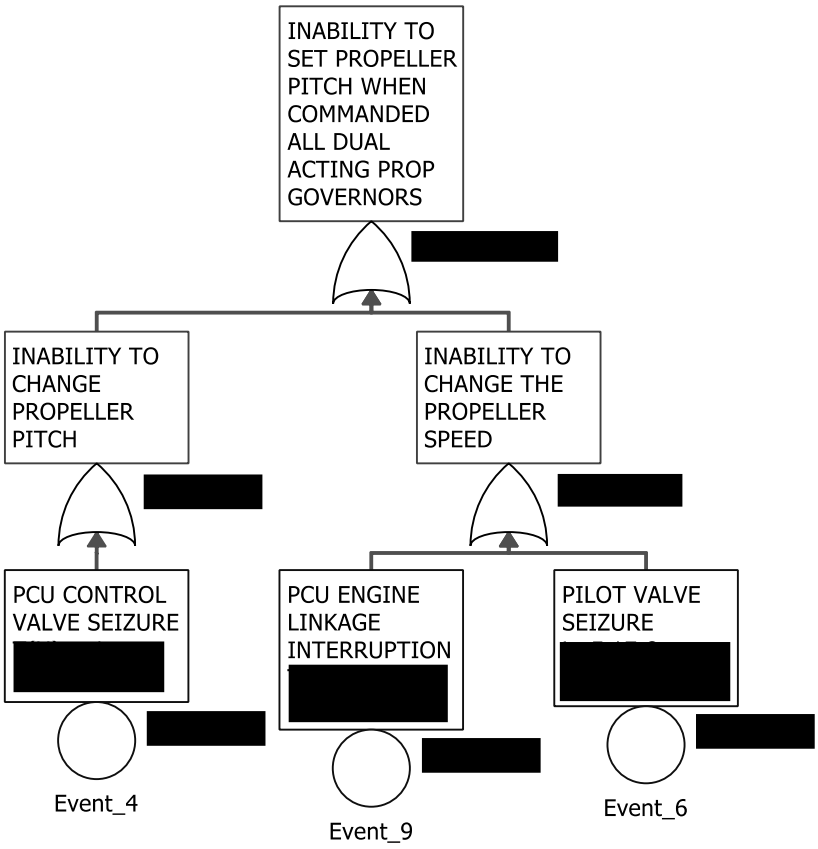


Figure 3: An inability to set the propeller pitch when commanded - H80-200-001/002 & H85-200-BC04 FAULT TREE ANALYSIS

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
Inability to Change Propeller Pitch					
4	PCU Control valve seizure	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
Inability to Change Propeller Speed					
6	Pilot valve seizure	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
9	PCU-ENGINE linkage interruption	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience

Table 10: "An inability to set the propeller pitch when commanded" contributing failures/conditions - failure rates substantiation

7.3 SIGNIFICANT UNCOMMANDED CHANGE TO PROPELLER PITCH

7.3.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will cause a significant uncommanded change to propeller pitch at a rate in excess of that defined as Remote.

7.3.2 Failure Definition

Significant uncommanded change to propeller pitch demonstrate itself as an uncommanded unfeathering and arises when PG failures (PG-engine lever disconnection and pilot valve seizure) are bounded together with the malfunction of the aircraft feathering system. The complete inability to feather the propeller, which results in uncommanded unfeathering, develops only if both of the feathering systems are in the specific failed condition.

7.3.3 Failure Modes

7.3.3.1 PCU Pilot Valve seizure

Propeller governor Pilot valve seizure due to contamination leads to inability to move the pilot valve (through inability to control the tension of the speeder spring) into the position that corresponds to the feather condition (Figure 1).

7.3.3.2 PCU and engine connection interruption

In case that the PG-engine lever is disconnected, the flyweight governor speeder spring is no longer fully loaded, but it is relaxed.

7.3.3.3 EHO failure (Aircraft feathering system)

In normal function, when EHA/EHO is energized, the PG is bypassed and oil from the AGB is directly provided to propeller dome by feathering pump. In case of EHA/EHO malfunction, the feathering function is fully on the PG feathering system. The aircraft feathering pump (system) is inactive (Figure 1).

7.3.3.4 Feathering pump failure (Aircraft feathering system)

In case of the aircraft feathering pump gear failure, the feathering pump is unable to provide pressurized oil to the propeller dome and propeller cannot be feathered (Figure 1).

7.3.3.5 Electrical harness failure (Aircraft feathering system)

When integrity of harness is lost, the power supply to the EHO/EHA is interrupted and it cannot be energized, hence cannot bypass the PG. The aircraft feathering pump is inactive.

7.3.4 Probability Assessment

Propeller feathering can be accomplished by either one of the two independent unfeathering/feathering systems (Emergency feathering via PG & Automatic/Manual feathering via aircraft feathering system) and the uncommanded unfeathering occurs only if these systems are both in the specific failed condition.

The probability of the failure "Significant uncommanded change to propeller pitch" was evaluated using the Fault Tree Analysis method (Figure 4) expanded to the component level as described above, based on the H80 & M601 service experience. The probability of occurrence of the failure "Significant uncommanded change to propeller pitch" is less than that defined as Remote.

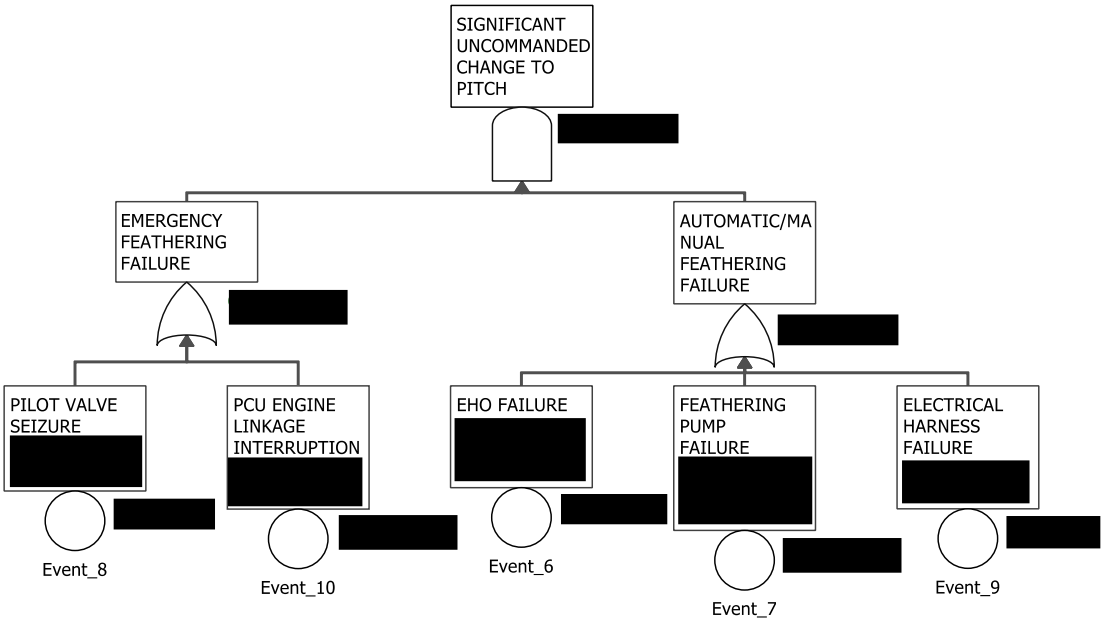


Figure 4: A significant uncommanded change to propeller pitch - H80-200-001/002 & H85-200-BC04 FAULT TREE ANALYSIS

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
PG feathering/unfeathering system					
8	Pilot Valve seizure				Based on M601/Hxx accumulated data and field experience & Based on Supplier data
10	PCU-Engine linkage interruption				Based on M601/Hxx accumulated data and field experience & Based on Supplier data
Automatic/manual aircraft feathering system					
6	EHO failure				Based on M601/Hxx accumulated data and field experience
7	Feathering pump failure				

9	Electrical harness failure	[redacted]	[redacted]	[redacted]	

Table 11: "A significant uncommanded change to propeller pitch" contributing failures/conditions - failure rates substantiation

7.4 SIGNIFICANT UNCONTROLLABLE THRUST/POWER OSCILLATION (AN UNCONTROLLABLE TORQUE OR SPEED FLUCTUATION)

7.4.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will cause a significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation) at a rate in excess of that defined as Remote.

7.4.2 Failure Definition

A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation) occurs either as a result of the FCU main and emergency circuits failures or as a consequence of inefficient damping of the propeller system that leads to the propeller speed fluctuation.

7.4.3 Failure Modes

Description and analysis of failure modes "Power instability due to the FCU main circuit failure" and "FCU emergency control circuit failure" are defined in the H80 Engine FMEA/FMES.

7.4.3.1 PCU control valve hysteresis (due to contamination)

Contamination between control valve and spline shaft could cause higher friction (Figure 1). To overcome the higher friction the higher axial force is required. Higher axial force corresponds to higher centrifugal force, therefore flyweight governor speed. The sudden increase of speed results in excessive hysteresis leading to propeller speed fluctuation, significantly increasing the system speed unsensitivity from ±5 RPM to >>5 RPM.

7.4.3.2 Excessive propeller shaft bearing leakages

An excessive oil leakage through the bearing on the propeller shaft cause insufficient dynamic dampening of the propeller system that leads to the propeller speed oscillation.

7.4.3.3 PCU pressure relief valve fracture

The fracture of pressure relief valve coil spring (reduction of spring stiffness) results in spring compression factor „K" reduction. This failure is followed by the drop of control pressure (downstream the gear pump), which still remains higher then governing pressure (downstream the control valve) (Figure 1). The drop of control pressure causes the reduction of oil flux through the PG to propeller dome as more of the oil is bypassed through the pressure relief valve. The oil flux reduction develops the propeller speed oscillation (due to insufficient system damping).

7.4.4 Probability Assessment

The probability of the failure "A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation)" was evaluated using the Fault Tree Analysis method (Figure 5 & Figure 6) expanded to the subsystems described above, based mainly on the safeguards incorporated in the design of the H80 engine and based on the H80 & M601 service experience. The probability of occurrence of the failure "A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation)" is less than that defined as Remote.

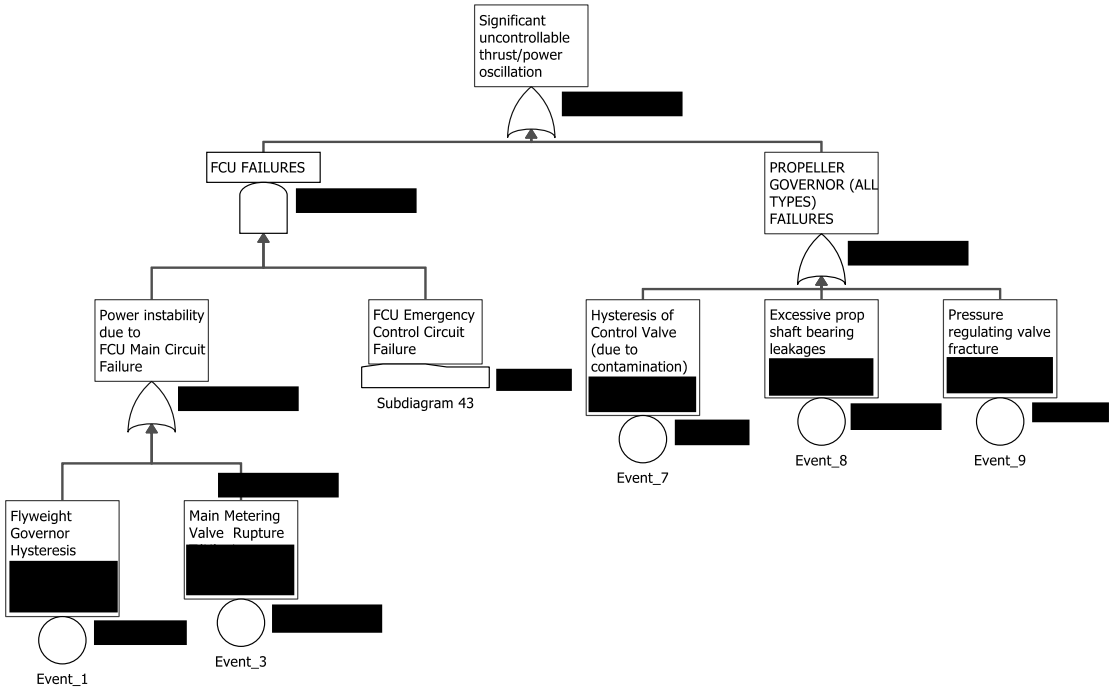


Figure 5: A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation) - H80-200-001/002 & H85-200-BC04 FAULT TREE ANALYSIS

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
Power Instability due to FCU Main Circuit Failure					
1	Flyweight Governor Hysteresis	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data
3	Main Metering Valve Rupture	[redacted]	[redacted]	[redacted]	
Propeller Governor Failures					
7	Hysteresis of control valve (due to contamination)	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience
8	Excessive propeller shaft bearing leakages	[redacted]	[redacted]	[redacted]	

9	Pressure relief valve fracture	[redacted]	[redacted]	[redacted]	Based on M601/Hxx accumulated data and field experience & Based on Supplier data **Chyba! Nenalezen zdroj odkazů.**

Table 12: "A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation)" contributing failures/conditions - failure rates substantiation

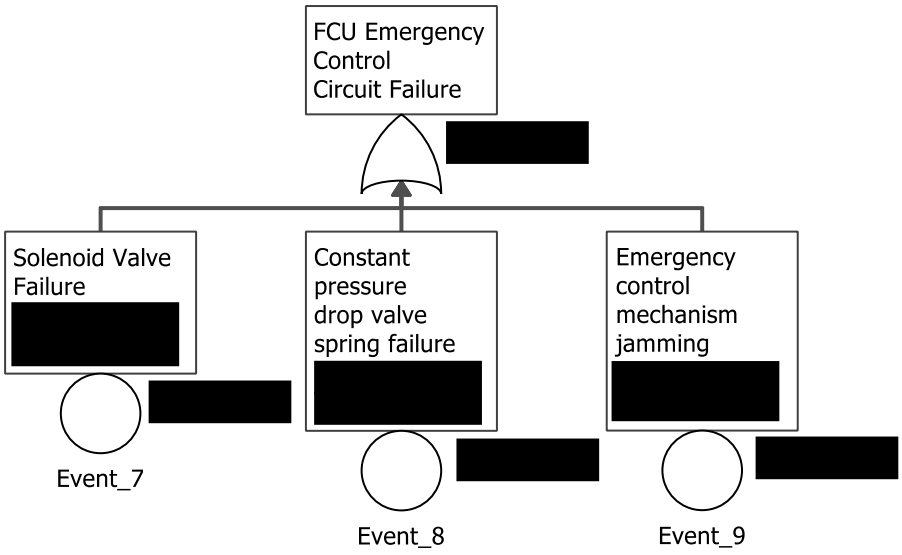


Figure 6: Subdiagram 43 - A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation) - H80-200-001/002 & H85-200-BC04 FTA

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
7	Solenoid valve failure	[redacted]	[redacted]	[redacted]	[redacted]
8	Constant pressure drop valve spring failure	[redacted]	[redacted]	[redacted]	
9	Emergency control mechanism jamming	[redacted]	[redacted]	[redacted]	

Table 13: Subdiagram 43: " A significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation)" contributing failures/conditions – failure rates substantiation

7.5 UNCOMMANDED PROPELLER PITCH SMALLER THAN MINIMUM FLIGHT PITCH

7.5.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will

cause an uncommanded propeller pitch smaller than minimum flight pitch at a rate in excess of that defined as Remote.

7.5.2 Failure Definition

The failure “Uncommanded propeller pitch smaller than minimum flight pitch” occurs as a result of unintended movement of the propeller blades below established minimum flight pitch as an effect of the Beta feedback system failure bounded together with the failure of the Pitch Lock system.

7.5.3 Failure Assessment

The safety analysis of the Major Failure Effect “Uncommanded propeller pitch smaller than minimum flight pitch” was performed in the frame, and as a part, of the Hazardous engine failure “Significant thrust in the opposite direction to that commanded by the pilot” ref. Section 6.1.

The engine control system is designed to operate in predefined pitch values. The pitch lock system engagement point is set by the airframer to a minimum in-flight low pitch position where the continued safe flight and landing is maintained. There are no provisions or design features in the engine control system to stop the propeller blades (that are below the pitch lock engagement position) on the different pitch position than that, which corresponds to the full reverse.

Propeller flat pitch position is not considered. The propeller control system works in pre-set pitch positions (i.e. feathered position, constant propeller RPM position, pitch lock enable position and full reverse position). There is no pre-set position for the propeller flat pitch (the propeller pitch is approximately 0° with respect to plane of rotation).

For that reason, any failure or combination of failures in engine control system result in a condition where the propeller pitch is locked at pitch lock enable position or at full reverse pitch position. As given in the Hazardous engine failure “Significant thrust in the opposite direction to that commanded by the pilot”, ref. Section 6.1. When Beta feedback system is in a failed state, the propeller blades further movement below minimum flight pitch position is stopped by the Pitch Lock system engagement. If the pitch lock system fails to operate, the propeller blades move to full reverse position.

7.6 GENERATION OF THRUST GREATER THAN MAXIMUM RATED THRUST

7.6.1 Objective

The objective of this analysis is to show that no probable malfunction, single or multiple failure, or improper operation of the H80-200-001/002, H85-200-BC04 engine built configurations will cause a generation of thrust greater than maximum rated thrust at a rate in excess of that defined as Remote.

7.6.2 Failure Definition

The thrust bigger than the maximum rated thrust is generated in the event of FCU main circuit failure of the Flyweight Speed Governor.

7.6.3 Failure Modes

For the purposes of this FTA the worst case scenario is assumed i.e. in the transition time between the flyweight speed governor failure and the pilot intervention, the gas generator will be over-speeded and rated torque (thrust) is exceeded. Nevertheless, this Major engine failure effect can be prevented by the movement of the ECL lever to the idle position or by switching of the engine to the emergency back-up mode.

The occurrence of this Major engine failure effect is conditioned by the position of the Engine Control Lever (ECL). The ECL must be in a position that corresponds to the gas generator speed above 80% of maximum rated speed.

7.6.3.1 FCU Flyweight Speed Governor failure

The collapse of the double row ball bearing on the FCU flyweight speed governor results in the partial or, in worst case scenario, complete loss of feedback between the engine and the FCU. The primary control law (gas generator RPM = constant) is override by the secondary control law (i.e., fuel schedule), so the FCU maximum fuel delivery that corresponds to the FCU control lever (ECL). As a consequence, the gas generator is in overspeed condition and rated torque is exceeded (rated thrust is exceeded).

7.6.4 Probability Assessment

The probability of the failure “Generation of thrust greater than maximum rated thrust” was evaluated using the Fault Tree Analysis method (Figure 7) expanded to the LRU detail, based on the H80 & M601 service experience. The probability of occurrence of the failure “Generation of thrust greater than maximum rated thrust” is less than that defined as Remote.

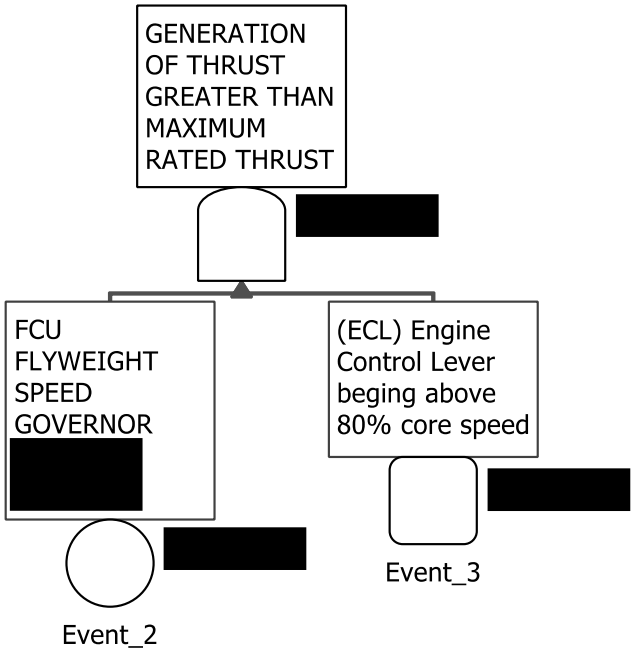


Figure 7: Generation of thrust greater than maximum rated thrust - H80-200-001/002 & H85-200-BC04 FAULT TREE ANALYSIS

Event No.	Description	λ	T(H)	Pf	Failure rate and exposure rate substantiation
2	FCU flyweight speed governor failure	[redacted]	[redacted]	[redacted]	[redacted]
3	(ECL) Engine Control Lever being above 80% of Ng speed	[redacted]	[redacted]	[redacted]	[redacted]

Table 14: "Generation of thrust greater than maximum rated thrust" contributing failures/conditions - failure rates substantiation

7.7 CONCLUSION – MAJOR EFFECTS ANALYSIS RESULTS

Based on the safeguards incorporated in the design of the H80-200-001/002 & H85-200-BC04 engine built configurations and based on the H80 & M601 service experience, the probability of occurrence of the major effects is less than that defined as Remote (1.00E-05).

No probable malfunction, nor any probable single or multiple failures, nor any probable improper operation of the engine will cause the engine probability of failure for major effects to be in excess of that defined as Remote.

The safety analysis of the major effects, caused or contributed by the engine control system was performed in with the following results:

No.	Engine level effect description	Severity Classification	Probability of occurrence per flight hour	Threshold
3	Impossibility to feather the propeller	Major	[redacted]	1.00E-05
4	Inability to set propeller pitch when commanded		[redacted]	
5	Significant uncommanded change to propeller pitch		[redacted]	
6	Significant uncontrollable thrust/power oscillation (An uncontrollable torque or speed fluctuation)		[redacted]	
7	Uncommanded propeller pitch smaller than minimum flight pitch		[redacted]	
8	Generation of thrust greater than maximum rated thrust		[redacted]	

Table 15: Summary of Major Effects on engine

Příloha 5

Validace výsledků bakalářské práce

Validace výsledků bakalářské práce

Na základě prostudování bakalářské práce pana Tisoně s názvem *Spolehlivostní analýza ve vývoji turbovrtulových motorů založená na STAMP* prohlašuji, že výsledky jsou validní a použitelné. Závěry práce je možné využít na vylepšení procesů spolehlivosti v konkrétní organizaci.

Ing. Zuzana Sekerešová, Ph.D.

Flight Safety Leader & Consulting Engineer

V Praze 27. 7. 2023