ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní
Ústav letecké dopravy

Bezpečnostní analýza ve vývoji vojenských letounů založená na STAMP

Safety Analysis in Military Aircraft Development based on STAMP

Bakalářská práce

Studijní program: B3710 - Technika a technologie v dopravě a spojích 3
Studijní obor: 3708R033 - Technologie údržby letadel

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

Autor práce: **Guanbao Gao**

Praha 2023

Fakulta dopravní
České vysoké učení technické v Praze

K621.....Ústav letecké dopravy

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Guanbao Gao

Studijní program (obor/specializace) studenta:

bakalářský – TUL – Technologie údržby letadel

Název tématu (česky): **Bezpečnostní analýza ve vývoji vojenských letounů založená na STAMP**

Název tématu (anglicky): Safety Analysis in Military Aircraft Development based on STAMP

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je provedení bezpečnostní analýzy v rámci vývoje a výroby vojenských letounů s pomocí modelu bezpečnosti STAMP a stanovení vstupů pro zajištění potřebné spolehlivosti hodnocené techniky.
- Analyzujte metody hodnocení bezpečnosti a spolehlivosti v letectví
- Analyzujte systémový model bezpečnosti STAMP
- Vyberte a popište konkrétní systém vojenského letounu
- Proveďte analýzu bezpečnosti s pomocí modelu STAMP a stanovte vstupy pro zajištění potřebné spolehlivosti
- Dosažené výsledky ověřte a vyhodnoťte

Rozsah grafických prací: dle pokynů vedoucího závěrečné práce

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

Seznam odborné literatury: Birolini, A. Reliability Engineering. Theory and Practice. Springer, 2017.
Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N., Thomas, J. STPA Handook, 2018.

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

Datum zadání bakalářské práce: **7. října 2022**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

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

L. S.

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

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

Potvrzuji převzetí zadání bakalářské práce.

Guanbao Gao
jméno a podpis studenta

V Praze dne 7. října 2022

Abstrakt:

S rostoucí komplexitou systému se zvyšuje i riziko vzniku nečekaných poruch vedoucí k nebezpečí. Aby byl nový systém dostatečně bezpečný, dělají se na něj bezpečnostní a spolehlivostní analýzy, které ověří bezpečnost nově navrhnutého systému. Na dnešní moderní systémy, které se vyznačují vysokou komplexitou, už mnohdy nemusí stačit tradiční analytické metody, jež bývají nepřehledné při analyzování komplexních systémů, nedokáží se adaptovat na dnešní technologie a nekladou tak velký důraz na lidský faktor. Z toho důvodu se v mé práci zaměřuji na relativně novou analytickou metodu STPA, která má za cíl eliminovat tyto limitace tradičních analytických metod a přispět k vyšší bezpečnosti moderních systémů. Tuto metodu využiji k analyzování systému podélného řízení a posilovače letounu Aero L-39 NG, což je lehký bojový letoun, co se nedávno začal sériově vyrábět ve Vodochodech. Ke konci se chci zaměřit na přínosy a limitace, které může integrace metody STPA do organizací přinést, a zdali se její integrace může ve Vodochodech vyplatit.

Klíčová slova:

bezpečnost, bezpečnostní analýza, L-39 NG, nebezpečí, spolehlivost, System-Theoretic Process Analysis

Abstract:

As the complexity of the system increases, so does the risk of unexpected malfunctions leading to danger. In order for the new system to be sufficiently safe, safety and reliability analyzes are made on it, which will verify the safety of the newly designed system. Traditional analytical methods may no longer be sufficient for today's modern systems, which are characterized by high complexity, as they tend to be confusing when analyzing complex systems, cannot adapt to today's technologies and do not place much emphasis on the human factors. For that reason, in my work I focus on the relatively new analytical method STPA, which aims to eliminate these limitations of traditional analytical methods and contribute to higher security of modern systems. I will use this method to analyze the pitch control system and pitch control actuator of the Aero L-39 NG, which is a light combat aircraft that has recently started to be serially produced in Aero Vodochody. Towards the end, I want to focus on the benefits and limitations that the integration of the STPA method can bring into organizations, and whether its integration can pay off in Aero Vodochody.

Keywords:

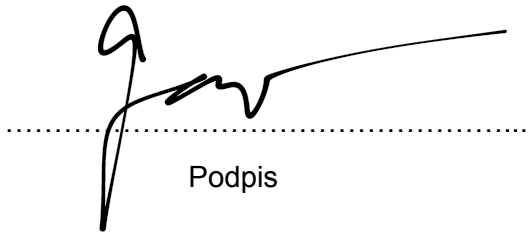
hazard, L-39 NG, reliability, safety, safety analysis, System-Theoretic Process Analysis

Čestné prohlášení

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

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

Praze dne 1.8.2023



Podpis

Poděkování

Na tomto místě bych chtěl poděkovat všem, kteří mi pomáhali s vypracováním mé bakalářské práce tím, že mi poskytovali podklady, naučili mnoho teoretických i praktických věcí, dělali revize práce, dávali své podněty a podobně. Chtěl bych obzvláště poděkovat mým vedoucím práce, konkrétně panu docentovi Andrejovi Lališovi a panu inženýrovi Oldřichovi Stummbauerovi. V neposlední řadě bych chtěl vyjádřit obrovský vděk zaměstnancům společnosti Aero Vodochody, speciálně panu magistrovi Milanovi Pšeničkovi a paní inženýrce Michaele Fukalové, za veškerou podporu a spolupráci při mé roční stáži ve Vodochodech.

Obsah

Seznam zkratek a pojmů

Zkratka	Anglicky	Česky
B2B	Business To Business	Obchodování mezi společnostmi
CA	Control Action	Řídící akce
CC	Controller Constrain	Požadavek a omezení na řídící člen
CFC	Controller and Feedback Constrain	Požadavek a omezení na řídící člen a zpětnou vazbu
CPC	Controller and Path Constrain	Požadavek a omezení na řídící člen a trasu řídící akce
EASA	European Union Aviation Safety Agency	Agentura Evropské Unie pro bezpečnost letectví
ECU	Electronic Control Unit	Elektrická řídící jednotka
FAA	Federal Aviation Administration	Federální letecká správa v USA
FHA	Functional Hazard Analysis	Funkční analýza nebezpečí
FMEA	Failure Modes and Effects Analysis	Analýza možného výskytu a vlivu poruch
FMS	Flight Management System	Systém na správu letových informací
FTA	Fault Tree Analysis	Stromová analýza poruch
H	Hazard	Nebezpečí
HOTAS	Hands On Throttle-And-Stick	Koncept, kdy na řídící páce jsou tlačítka, aby piloti při jejich ovládání nemuseli dávat ruce pryč od řídící páky
MCAS	Maneuvering Characteristics Augmentation System	Systém pro augmentaci letových charakteristik (zabraňuje přetažení)
MFD	Main Flight Display	Primární letový displej
MTOW	Maximum Take-Off Weight	Maximální vzletová hmotnost
NG	Next Generation	Další genrace
ODVL	Department of Supervision over Military Aviation	Odbor dohledu nad vojenským letectvím
PCA	Pitch Control Actuator	Posilovač pro vychylování výškových kormidel
RBD	Reliability Block Diagram	Blokový diagram pro analyzování spolehlivosti
SC	System Constrain	Omezení a požadavek na systém
STAMP	System-Theoretic Accident Model and Processes	Nehodový model a procesy založené na systémové teorii
STPA	System-Theoretic Process Analysis	Procesová analýza založená na systémové teorii
UCA	Unsafe Control Action	Nebezpečná řídící akce
ÚCL	Civil Aviation Authority	Úřad pro civilní letectví

Úvod

Bezpečnost je nepochybně jedním z nejdůležitějších pilířů leteckého průmyslu. Vývoj letadla představuje časově i finančně náročný proces, který vyžaduje vysokou pozornost na bezpečnost v každém stádiu vývoje. S čím dál novějšími a sofistikovanějšími technologiemi nabírá bezpečnost v letectví zcela nový rozměr, neboť i nový systém, jehož účelem je nehodě zabránit, může sám nehodu způsobit. Kvůli rostoucí komplexitě nových letadel musíme najít nový způsob vyhodnocování bezpečnosti, který se dokáže adaptovat na dnešní komplexní systémy a technologie.

Hlavním cílem mé bakalářské práce je provést bezpečností analýzu pomocí metody zvané STPA (System-Theoretic Process Analysis), a to v rámci vývoje a výroby vojenských letounů. Metoda STPA je založena na tzv. systémové teorii, která byla vynalezena po druhé světové válce, kdy systémy začínaly nabírat na složitosti a tradiční analytické metody už nemusely na nové systémy stačit. Tuto analýzu poté využiji k tomu, abych stanovil vstupy pro zajištění potřebné bezpečnosti a spolehlivosti daného systému. V mé práci se budu také snažit najít, jaké výhody (a případně i nevýhody) představuje metoda STPA oproti tradičním metodám, jako jsou FTA (Fault Tree Analysis) a FMEA (Failure Modes and Effects Analysis).

V úvodu práce se budu věnovat procesu vývoje letadel, kdy už je potřeba postupně odhalovat nebezpečí a rizika spojené s provozem systému, a poté odhalím problémy, které mohou při analyzování bezpečnosti vyvíjeného systému nastat. Všechny tyto činnosti by nám měly pomoci navrhnout a vyrobit systém, který bude dostatečně bezpečný a dokáže splnit bezpečnostní požadavky úřadu při certifikačním procesu.

Druhá část práce je věnována samotné metodice, kde budou popsány tradiční analytické metody (FTA, FMEA a FHA) a relativně nová metoda STPA. U metody STPA bude také popsán postup pro vytváření STPA analýzy. Dále zde bude popsán systém, který je předmětem mé analýzy v praktické části, a tím je systém podélného řízení s posilovačem (zvaný jako PCA – Pitch Control Actuator), který se aktuálně vyvíjí ve Vodochodech pro nově vyvinutý letoun Aero L-39 NG.

V poslední kapitole se budu snažit ukázat, jaké přínosy (a případně i rizika) může metoda STPA představovat, a zdali se zakomponování této nové analytické metody do organizací může vyplatit.

1. Současný stav

Následující kapitoly jsou věnovány procesu vývoje letadel a limitacím, se kterými se aktuálně můžeme setkat.

1.1. Vývoj letadel

Vývoj každého letadla představuje zdlouhavý a složitý proces, který může trvat měsíce i roky, v závislosti na komplexnosti letadla (pro zajímavost, vývoj letounu A380 trval zhruba 11 let). Během tohoto procesu je nutná spolupráce mnoha týmů, kteří se na vývoji podílejí přímo i nepřímo. Jsou to například týmy zaměřující se na návrhy konstrukce a systémů, dimenzování, bezpečnost a spolehlivost, certifikace, B2B, testování atd.

Součástí vývoje letadla je nepochybně vytváření kompromisů, neboť letadla musí být dostatečně pevná, musí unést požadovaný náklad a zároveň musí být co nejlehčí, aby byla ekonomická (nízká spotřeba, nízké nároky na údržbu apod.). Kvůli tomu je nutné provádět zátěžové testy, které ověří, že konstrukce letounu splňuje požadavky na pevnost, tuhost, stabilitu a aeroelasticitu.

Obr. 1.1: Testování modelu letounu L-39 NG v aerodynamickém tunelu

Z důvodu vysoké komplexnosti dnešních letadlových systémů je nutné ověřovat bezpečnost a spolehlivost těchto systémů pomocí analýz, které nám pomohou předpovědět, jaké poruchy mohou během provozu nastat a případně jaké následky mohou tyto poruchy mít. Tyto analýzy se tvoří průběžně s aerodynamickými a zátěžovými testy, které nám spolu pomohou ověřit, zdali je systém dostatečně bezpečný. Každý výrobce využívá různé metody analýz (např.

společnost Boeing využívá metody FTA a FMEA). Metodám analyzování se budu podrobněji věnovat ve druhé části své bakalářské práce.

1.2. Aero Vodochody – vývoj L-39 NG

Aero Vodochody Aerospace a.s. je česká společnost zaměřující se na výrobu letadel a letadlových celků. Společnost sídlí v okrese Praha-Východ vedle Odolené Vody, kde se také nacházejí všechna její pracoviště a montážní haly. Přímo vedle jejího areálu leží letiště Vodochody, které slouží výhradně firemním účelům společnosti Aero Vodochody.

Společnost byla založena roku 1919 a zaměřovala se na výrobu menších letadel. Do roku 1953 probíhala výroba v Praze na Vysočanech a v Karlíně, poté se výroba přestěhovala do Odolené Vody, kde probíhá dodnes. Do roku 2006 bylo Aero Vodochody státním podnikem; poté bylo do roku 2021 vlastněno konsorciem Penta Investments. V současné době je vlastníkem maďarská státní firma HSC Aerojet Zrt.

Obr. 1.2: Pohled na areál Aero Vodochody z ptačí perspektivy

Mezi její nejznámější letadla patří například letouny L-39 Albatros, L-29 Delfín nebo L-159 Alca, což byly podzvukové cvičné letouny, určené primárně pro vojenské účely. Dnes společnost pracuje na několika projektech a zakázek, jako jsou:

- výroba náběžných hran křídel pro letoun Airbus A220,
- výroba dveří a nájezdové rampy pro vojenské transportní letouny Embraer KC-390,
- sériová výroba letounu Aero L-39 NG v různých zákaznických variantách
- vývoj nových modifikací určených pro letoun Aero L-39 NG.

AERO L-39 NG

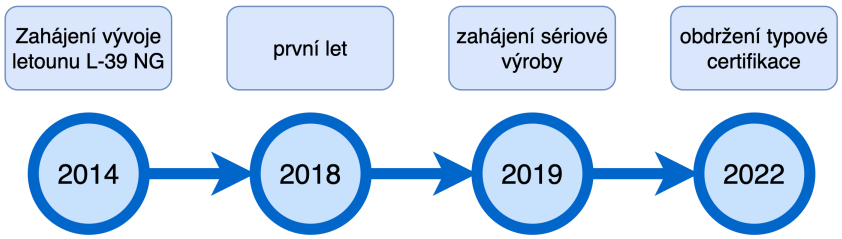
Aero L-39 NG (Next Generation) je podzvukový proudový letoun, který byl nově vyvinut společností Aero Vodochody Aerospace. Jeho koncepce vychází z jeho úspěšného předchůdce L-39 Albatros, který se vyráběl mezi lety 1971 a 1999 a dodnes jich stále létá několik stovek kusů po světě. Nová verze získala mnoho vylepšení, jako jsou kompozitní části konstrukce, integrální nádrž (ve Vodochodech přezdívané jako “mokré křídlo”), moderní avionika nebo nový motor od firmy Williams International.

Tab. 1.2: Technické specifikace letounu L-39 NG

posádka	2 piloti	maximální rychlost	780 km/h
prázdná hmotnost	3,2 tun	dostup	10 670 m
MTOW	5,65 tun	dolet	1 900 km
rozměry (š x d x v)	(9,37 x 11,83 x 4,87) m	dolet s přídavnými nádrži	2 500 km

Kromě výcviku vojenských pilotů je letoun primárně určen také pro lehké bitevní, hlídkové nebo průzkumové úkoly. V roce 2018 se uskutečnil jeho první let a v roce 2019 začala sériová výroba. Letoun získal typovou certifikaci až v roce 2022. Dodnes probíhá vývoj jeho nových systémů, mezi které patří například autopilot nebo posilovač podélného řízení, jenž je předmětem mé bezpečnostní analýzy.

Obr. 1.3: Prototyp letounu L-39 NG



Obr. 1.4: Harmonogram vývojové fáze letounu L-39 NG

Navzdory velké konkurenci od jiných výrobců obdrželo Aero objednávky na více než 60 kusů letounu L-39 NG. Mezi jejími hlavními kupci patří například Vietnam (12 kusů), Maďarsko (12 kusů), americká výcviková organizace RSW Aviation (12 kusů), portugalská společnost SkyTech (10 kusů), Ghana (6 kusů) a Senegal (4 kusy). Ačkoliv technické specifikace letounu výrazně zaostávají za její konkurencí, je jeho relativně velký úspěch postaven na jeho úspěšném předchůdci Albatrosovi a přívětivé ceně. Mezi jeho hlavními konkurenty patří například:

- Itálie: M-346 Master (má mnohem lepší letové vlastnosti, avšak je 2-3 krát dražší),
- Jižní Korea: KAI T-50 Golden Eagle (nadzvukový, MTOW přes 10 tun, avšak je 2-3 krát dražší),
- USA/Švédsko: Boeing–Saab T-7 Red Hawk (nadzvukový, pokročilejší, avšak stále ve vývoji a je zhruba dvakrát dražší).

1.3. Přehled vědecké literatury

Vědeckou literaturu jsem čerpal ze stránky scopus.com, což je široká databáze odborné literatury pokrývající široké spektrum oborů. Z této stránky jsem se snažil nalézt texty, ve kterých se implementovala analytická metoda STPA na konkrétní systémy a porovnávala metoda STPA s tradičními analytickými metodami, jako je FTA, FMEA nebo FHA, což jsou dnes nejpoužívanější tradiční metody analýz. Níže jsou uvedeny práce, které jsem nalezl na Scopusu a měl jsem k nim přístup:

1) Improved Systemic Hazard Analysis Integrating With Systems Engineering Approach for Vehicle Autonomous Emergency Braking System [7]
    - práce se zaměřuje na aplikování metody STPA na komplexní systém (konkrétně systém nouzového brždění autonomních vozidel)
    - porovnává metodu STPA s tradičními metodami (FTA, FMEA)
2) The Safety Analysis of Multiple Method Fusion on Reactor Scram Subsystem [8]
    - práce se zaměřuje na aplikování metody STPA na komplexní systém (konkrétně systém pro ochranu jaderného reaktoru)
    - podrobněji rozebírá rozdíly v metodách STPA, FTA a FMEA
    - popisuje limitace tradičních metod (FTA, FMEA)
3) System-Theoretic Process Analysis for reliability assessment: Aircraft's wheel braking system case study [9]

- práce porovnává vytváření spolehlivostní analýzy metodami STPA a FMEA
- popisuje limitace aplikace metody STPA na spolehlivostní analýzy (nutno nezaměňovat s bezpečnostními analýzami)

Dalšími články, které se zabývají stejnými nebo podobnými problémy jsou:

4) System Theoretic Process Analysis for a Vehicle SAE Level four [10]
5) Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site [11]
6) A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software [12]

Posledním dokumentem, o kterém stojí za to se zmínit, je STPA Handbook [6]. Jeho autory jsou Nancy Leveson a John Thomas a ve spolupráci s odborníky z celého světa zpracovali kompletní příručku pro vytváření STPA analýz. Kromě toho obsahuje také informace týkající se zakomponování metodiky STPA do vývojových procesů systémů a integrace do velkých organizačních struktur. Právě svou praktickou část bakalářské práce, což je vytvoření STPA analýzy na konkrétní systém vojenského letounu, jsem většinou vypracovával podle postupů uvedených v této příručce.

1.4. Limitace současného stavu

KOMPLEXNÍ SYSTÉMY

Dnešní letadla se vyznačují svou vysokou komplexností a obsahují mnoho pokročilých technologií, které mají za úkol zvyšovat efektivitu a bezpečnost. Každý nový systém, jehož účelem je zabránit nehodě, může také paradoxně nehodu způsobit. Příkladem může být systém MCAS u letounů Boeing 737 MAX generace, kdy tento systém měl zabránit pádu letounu při přetažení tím, že klopil letoun dolu. Chybná aktivace tohoto systému způsobila pád dvou letounů B737 MAX (v Etiopii a Indonésii).

Čím novější letouny, tím bývají jeho systémy složitější a sofistikovanější. Dokazuje to například relativně nový a velmi sofistikovaný dopravní letoun Boeing 787 Dreamliner, který z důvodu vysokého počtu elektrických systémů musí mít čtyři palubní akumulátory. Pro porovnání, jeho starší, a zároveň i větší předchůdce Boeing 777 má “pouze” dva palubní akumulátory.

Abychom dokázali provést dostatečnou bezpečnostní analýzu na systémy letounu, musíme mít metody analyzování, které se dokáží přizpůsobit i komplexním systémům. Na to už mnohdy nemusí stačit ani tradiční metody analyzování (například metody FTA nebo FMEA), neboť tyto metody často nezahrnují lidský faktor a při analyzování komplexnějších systémů se stávají analýzy nepřehlednými a neúplnými (u komplexních systémů mohou být některé typy problémů těžce predikovatelné).

KVANTITATIVNÍ METODY ANALÝZ

Každé nově navrhnuté letadlo musí projít určitým certifikačním procesem závisejícím na jeho typu. Tyto certifikace pro civilní letadla zajišťují úřady, jako jsou EASA (pro oblast EU), FAA (pro Spojené státy americké) nebo ÚCL (pro ČR). V případě vojenských letadel je certifikace

zpravidla zajišťována ministerstvem obrany daného státu, jako je to u letounu Aero L-39 NG, kdy certifikaci zajišťoval ODVL (Odbor dohledu nad vojenským letectvím).

V dnešní době certifikace nových letadel zahrnuje kontroly pomocí kvalitativních i kvantitativních metod analýz. Kvantitativní analýzy mají za účel dokázat pravděpodobnost, že daný systém neselže (neboli spolehlivost). Pro úřady to bývá nejjednodušší způsob kontroly, neboť jim stačí zkontrolovat, zdali je daná pravděpodobnost v povolených mezích. Na první pohled se to může zdát být jako velmi efektivní metoda, avšak problém nastává u úplně nových nebo složitějších systémů.

Kvantitativní metody analýz vysoce spoléhají na dostupnost a přesnost hodnot – i malá nepřesnost nebo nedostupnost hodnoty jedné komponenty může způsobit velkou nejistotu v koncovém výsledku. To může způsobit, že skutečná spolehlivost se bude výrazně lišit od předpokladu a při budoucím vývoji daného systému nebo letadla se bude pracovat s chybnými pravděpodobnostními hodnotami.

ŘEŠENÍ

Existuje relativně nová analytická metoda, která narozdíl od tradičních analytických metod bere v potaz lidský faktor, je přehledná i při analyzování komplexních systému, zahrnuje selhávání i více komponent a umí zakomponovat i nehmotné předměty, jako je software nebo dokonce i organizační struktury firem. Tato metoda se nazývá STPA (System-Theoretic Process Analysis) a níže v kapitole č. 2.2 je podrobně popsána.

Hned ze začátku je nutné počítat s určitými limitacemi, které metoda STPA může představovat. Níže jsou popsány limitace, které jsou zmíněny ve výše uvedených odborných literaturách:

- nedostatečný formalismus [7] (metoda STPA má relativně benevolentní strukturu, tudíž každá STPA analýza od jiných analytiků může mít úplně jinou strukturu a formát),
- metoda STPA je primárně určená pro vytváření bezpečnostních analýz než spolehlivostních [9] a
- nemusí se vyplatit při analyzování systémů hardwarového charakteru, neboť metoda FTA má větší procentuální pokrytí hardwarových systémů než STPA [8] (metoda FTA má 100% pokrytí, zatímco STPA “pouze” 90%).

Tab. 1.2: Pokrytí analytických metod v jednotlivých oblastech

Analysis of the category / Analysis method	hardware	software	The system interaction and communication
FMEA	80%	85%	80%
FTA	100%	65%	75%
STPA	90%	90%	100%

2. Metodika analyzování

Tato část bakalářské práce je věnována metodám analýz, které se využívají při vývoji systémů pro analyzování bezpečnosti a spolehlivosti. Mezi nejpopulárnější metody analýz v leteckém průmyslu patří například FHA, FTA, FMEA, RBD (Reliability Block Diagram) a nebo STPA. Těmto metodám se budu níže věnovat podrobněji, obzvláště metodě STPA.

Cílem mé bakalářské práce je provést bezpečností analýzu na konkrétní systém pomocí metody STPA, a to v rámci vývoje vojenských letounů. Předmětem mé analýzy je posilovač řízení, zvaný jako PCA (Pitch Control Actuator), který je též níže podrobněji popsán.

2.1. Metody

2.1.1. FTA

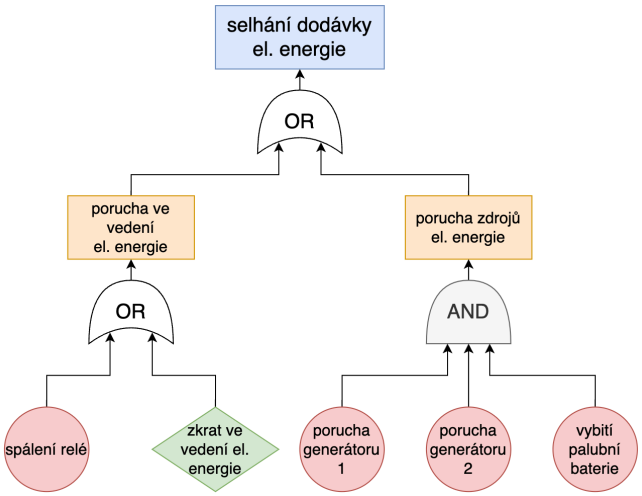
Metoda FTA (Fault Tree Analysis) [1] je grafická, kvantitativní i kvalitativní metoda analýz, pomocí které se snažíme najít příčiny vzniku různých nehod. FTA metoda byla vyvinuta telekomunikační společností Bell v roce 1962, kdy tuto metodu aplikovali pro analýzu balistických střel armády USA. Později tuto metodu převzala společnost Boeing a dodnes ji využívají při analyzování svých produktů.

Analýzu sestavujeme pomocí logických obvodů Booleovy algebry [5], kdy pro každý poruchový stav, jenž se může přihodit, se snažíme dojít až k individuálním komponentám, které mohou v případě selhání způsobit daný poruchový stav. Tento přístup nazýváme jako “top-down” přístup, neboť na vrchu je poruchový stav a na spodu jsou jednotlivé komponenty. Metoda FTA bývá většinou kombinována s metodou FMEA (Failure Mode and Effects Analysis), která je níže podrobněji popsána.

Logické obvody Booleovy algebry sestávají z následujících symbolů:

- logické členy, neboli hradla (angl. logic gates),
- symboly reprezentující události, stavy, selhání apod.

Níže je příklad jednoduchého FTA logického obvodu, neboli “stromu”:



Obr. 2.1: příklad jednoduchého FTA “stromu”

2.1.2. FMEA

Metoda FMEA (Failure Modes and Effects Analysis) [3] je kvalitativní metodou analyzování, která se snaží systematicky analyzovat každou komponentu v systému a předvídat, jaké poruchové stavy mohou vzniknout vlivem poruchy daného komponentu. Narozdíl od metody FTA využívá FMEA “bottom-up” přístup, neboť začíná u jednotlivých komponent a končí u nehodových událostí.

FMEA analýza se vytváří pomocí tabulky, ve které systematicky zaznamenáváme jednotlivé informace o komponentech. Níže je příklad, jak taková FMEA tabulka může vypadat (z důvodu velikost tabulky byla tabulka rozdělena na dva řádky):

Tab. 2.1: příklad FMEA tabulky (část 1/2)

referenční číslo	komponenta	potenciální porucha	kontext	příčina potenciální poruchy	lokální následky poruchy
1.1.1	spojka posilovače řízení	spojka se neodpojí	při poruše posilovače	zadrhnutí mechanismu spojky	poničení mechanismu spojky

Tab. 2.2: příklad FMEA tabulky (část 2/2)

systémové následky poruchy	pravděpodobnost vzniku poruchy	závažnost poruchy	pravděpodobnost detekce poruchy	riziko	požadavek na komponentu nebo systém
pilot musí působit proti silám vyvolaným posilovačem	2 (velmi nízká)	3 (střední)	3 (vysoká): pilot si všimne poruchy poté, co začne ovládat výšková kormidla	nízké	spojka musí být pravidelně kontrolována na zadrhávání

Jak už jsem zmínil výše, metoda FMEA je velmi často využívána v kombinaci s metodou FTA. Důvodem jsou jejich rozdílné přístupy, kdy FTA využívá “top-down” přístup, zatímco FMEA využívá “bottom-up” přístup. Kromě toho mají tyto obě metody další odlišnosti, které jsou shrnuty v jednoduché tabulce tab. 2.3 [2]:

Tab. 2.3: porovnání metod FTA a FMEA

FTA	FMEA
“top-down” přístup	“bottom-up” přístup
kvantitativní i kvalitativní metoda	kvalitativní metoda
analyzuje systém jako celek	analyzuje pouze individuální komponenty
počítá i s více než jednou poruchou	počítá pouze s poruchou jednoho komponentu
uvažuje i vnější podmínky	neuvažuje vnější podmínky

2.1.3. FHA

Další metodou analyzování, která je hojně využívána v leteckém průmyslu, je metoda FHA (Functional Hazard Analysis) [4]. S tvorbou FHA analýzy se začíná zpravidla už v počátečních fázích vývoje, kdy nemusí být známy všechny funkce systému.

Jejím hlavním cílem je zjistit následující:

- které funkce nesmí v systému chybět pro uskutečnění dané akce,
- poruchy, které mohou v provozu nastat,
- následky a riziko těchto poruch a
- bezpečností kritéria pro zajištění dostatečné bezpečnosti.

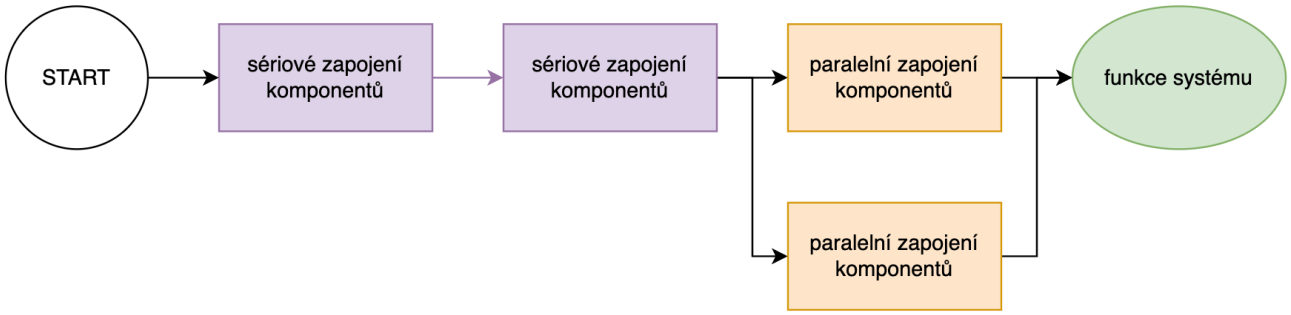
Analýza se vytváří v tabulce, jež může připomínat tabulku z FMEA analýzy, avšak narozdíl od ní využívá metoda FHA “top-down” přístup. Tato tabulka může vypadat takto:

Tab. 2.4: příklad jednoduché FHA tabulky

funkce		poruchový stav			krit.	pravděp.
ref. číslo	popis funkce	ref. číslo	popis poruchového stavu	důsledky poruchového stavu		
1.1	vychylování trimovací plošky	F-1.1.1	trimovací ploška se nevychyluje	posádka nebude moci trimovat	2	2
		F-1.1.2	trimovací ploška se vychyluje na opačnou stranu	trimovací ploška bude posádce “přitěžovat”	3	1
		F-1.1.3	trimovací ploška se zasekne ve vychýlené poloze	trimovací ploška bude klopit letounem v jednom směru	3	2

2.1.4. RBD

RBD (Reliability Block Diagram) je grafická metoda pro počítání spolehlivost systému. Základem je soubor bloků představující jednotlivé komponenty, které jsou v diagramu sériově nebo paralelně propojeny, vedoucí ke konečné funkci systému. U každého RBD diagramu se pak snažíme vypočítat pravděpodobnost úspěšného vykonání koncové funkce.



Obr. 2.2: Zapojení komponentů sériově a paralelně

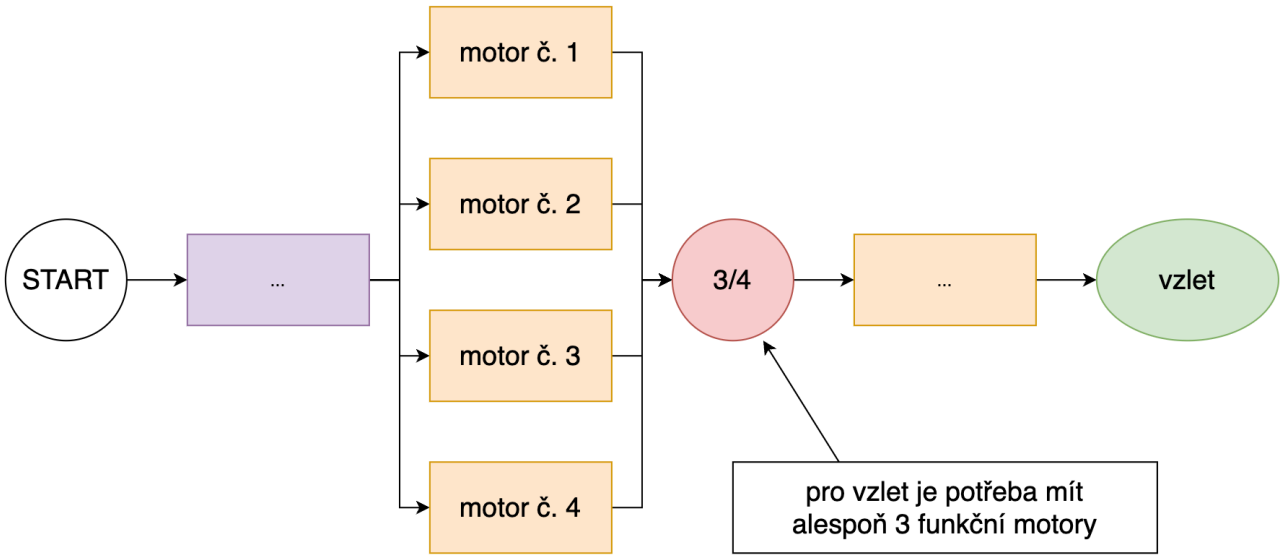
Díky metodě RBD je velmi snadné najít oblasti, na které je potřeba se zaměřit z důvodu nízké spolehlivosti. Využívají se k tomu následující pravidla:

- čím více komponentů je v sériovém zapojení, tím spolehlivost systému klesá,
- čím více komponentů je v paralelním zapojení, tím spolehlivost systému roste,
- pro zvýšení spolehlivosti v sériovém zapojení je nejefektivnější zvýšit spolehlivost komponentu s nejnižší spolehlivostí,
- pro zvýšení spolehlivosti v paralelním zapojení je nejefektivnější zvýšit spolehlivost komponentu s nejvyšší spolehlivostí.

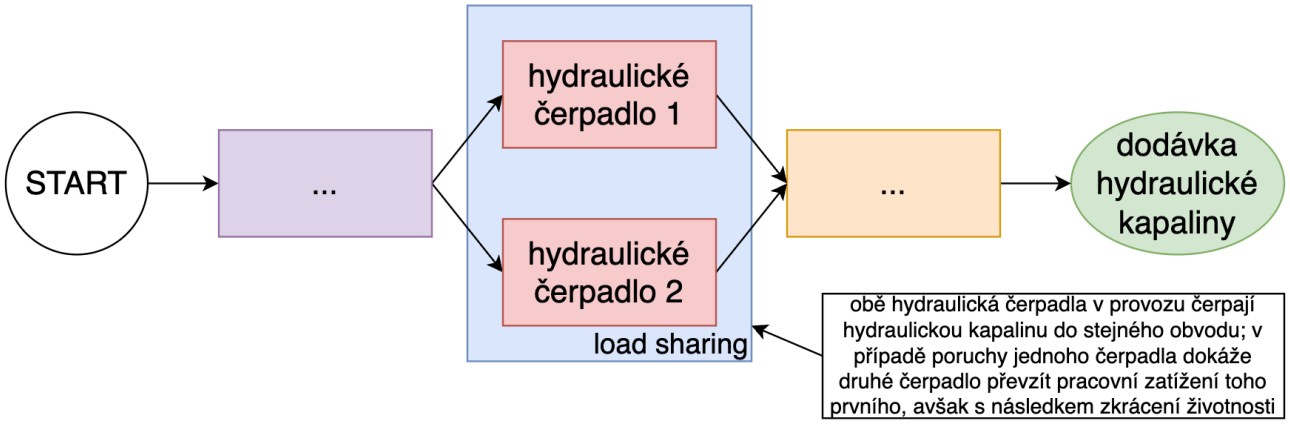
Kromě kombinací sériového a paralelního zapojení bloků lze komponenty zapojit i pomocí jiných konfigurací:

- *k* z *n* paralelní konfigurace (k-out-of-n),
- tzv. “load-sharing” konfigurace,
- konfigurace se záložním blokem…

Výhodou metody RBD je kromě jeho dobré přizpůsobitelnosti ke komplexním systémům také to, že jej lze propojit s ostatními metodami analýz, jako třeba s metodou FTA (pomocí aplikace De Morganových teorémů) nebo dokonce i STPA, která je popsána podrobně v následující kapitole.



Obr. 2.3: Příklad zapojení “k-out-of-n” konfigurace



Obr. 2.4: Příklad zapojení tzv. “load-sharing” konfigurace

2.2. Systémový přístup – metoda STPA/STAMP

STAMP (System-Theoretic Accident Model and Processes) [6] je relativně nový model pro vytváření modelu systémů a je založena na tzv. systémové teorii. Systémová teorie je nový přístup k nahlížení na systémy, který se vytvořil po druhé světové válce, kdy systémy začaly být čím dál komplexnější a konvenční metody jako jsou FTA a FMEA přestaly stačit. Narozdíl od konvenčních metod nahlíží systémová teorie na systémy jako celek, zatímco konvenční metody rozdělovaly komplexnější systémy na menší části a analyzovaly systémy po jednotlivých částech. Je obecně známé tvrzení: “Celek je více než jen součet všech jeho částí.” To platí obzvláště u komplexních systémů, neboť při rozdělování systému na menší části je velmi jednoduché přehlédnout interakce mezi komponentami z odlišných částí.

Oproti konvenčním metodám má model STAMP také další výhody, jako jsou např.:

- model STAMP funguje i na velmi komplexních systémech,
- zahrnuje také lidský faktor, software, organizační struktury a další,

- propojenost s účinnými metodami analyzování, jako je STPA.

STPA (System-Theoretic Process Analysis) je velmi účinná, proaktivní metoda analyzování bezpečnosti, která je založena na modelu STAMP. Její využití najdeme nejenom u letadel, ale například i v řízení letového provozu, kosmonautice, vojenské obraně, železnici, automobilech, rafinérském průmyslu a v neposlední řadě i farmaceutickém průmyslu. Každá STPA analýza se skládá ze čtyř hlavních kroků, které postupně odhalují možné rizikové scénáře, které mohou nastat během provozu. Na konci analýzy se vytvoří seznam požadavků a omezení, který později poslouží jako "checklist" při dalším plánování. Díky tomu dokážeme předvídat, jak se bude systém pravděpodobně v provozu chovat. Postup vytváření STPA analýzy je podrobněji popsán níže.

2.2.1. Krok 1: Definujte účel analýzy

Definování účelu analýzy bývá prvním krokem každé analýzy, kdy se snažíme dopředu identifikovat ztráty, kterým chceme zabránit.

Tento krok se skládá ze 4 částí, které budou níže podrobněji popsány:

- identifikace ztrát,
- identifikace systémových nebezpečí,
- identifikace systémových omezení a
- rozbor nebezpečí (volitelný krok).

2.2.1.1. Identifikace ztrát

Nejprve je nutné si identifikovat ztráty, u kterých nechceme, aby během provozu nastaly. Ztráta představuje něco, co má pro účastníky zúčastněných v provozu systému určitou hodnotu. Účastníci mohou být například posádka, letecká společnost, ale i výrobce.

Ztráty mohou být například:

- ztráta lidského života,
- ztráta zákaznické spokojenosti,
- ztráty na životním prostředí,
- ztráta reputace,
- ztráta účelu (letového plánu)
- ztráty nebo poškození letounu a další…

Postup pro identifikace ztrát:

1. identifikuje účastníky (posádka, letecká společnost, výrobce…)
2. identifikuje hodnoty a účely těchto účastníků (udržování letadlové flotily, poskytovat dopravu, vyrábět a navrhovat systémy…)
3. přeměňte tyto hodnoty a účely do ztrát (např. ztráta letadla, ztráta letového plánu, ztráta reputace…)

Je nutné míti na paměti, že tento krok se vztahuje k systému jako celku, nikoliv však individuálním komponentám (šrouby, lidský faktor, brzdné destičky…).

2.2.1.2. Identifikace systémových nebezpečí (hazards)

Nebezpečí je definováno jako stav nebo podmínky, které mohou v nejhorším případě vést ke ztrátě. Při identifikaci systémových nebezpečí musíme mít na paměti, že u nebezpečí nemůžeme zahrnovat faktory, které nemůžeme ovlivnit (vítr, blesk…). Dále musíme zůstat pouze na úrovni systému, nikoliv až na úrověň komponent. Takže když budeme chtít vytvořit nebezpečí, kdy se trimovací ploška bude vychylovat v opačném, než požadovaném směru, nesmíme zmínit už ze začátku přímo poruchu elektromotoru (aktuátoru) trimovací plošky. Tímto můžeme v příštích krocích snadno přehlédnout ostatní příčiny, které způsobí vychýlení trimovací plošky v opačném směru.

Uvažujme, že máme systém podélného řízení letounu. Mezi faktory, které mohou vést k deformaci táhel podélného řízení mohou být silný poryv nebo poddimenzovaná táhla podélného řízení. Následkem toho je nevychylování výškových kormidel v požadované úrovni (nebezpečí), což může vést ke ztrátě letového plánu (ztráta). Jako konstruktéři není v našich silách, abychom ovlivnili rychlost nebo sílu poryvu, avšak můžeme ovlivnit tuhost a pevnost táhel podélného řízení tím, že táhla mírně naddimenzujeme, čemuž pak můžeme předejít nebezpečí.

Mezi dalšími příklady systémových nebezpečí mohou být např.:

- systém podélného řízení vychyluje výšková kormidla bez vstupu od posádky,
- letadlo nedodržuje bezpečný odstup od ostatních letadel.

Každé nebezpečí musí mít přímo odkaz na ztráty, které mohou nastat v případě nastání toho nebezpečí.

2.2.1.3. Vymezení systémových omezení

Z našeho pohledu můžeme definovat omezení jako požadavky, které musí systém splňovat, abychom předešli nebezpečí (a tím předešli i ztrátám). Jakmile identifikujeme systémová nebezpečí, můžeme pak jednoduše vytvořit seznam omezení, jež náš systém musí splňovat.

Pro vytvoření systémových omezení (System Constrains) stačí jednoduše převrátit smysl vět v systémových nebezpečí. Příklady jsou znázorněny níže:

Tab. 2.5: Tvoření systémových omezení

	Systém	**Činnost**	**Kontext**
Nebezpečí H-1	Systém podélného řízení	vychyluje výšková kormidla	bez vstupu od posádky.
Systémové omezení SC-1	Systém podélného řízení	nesmí vychylovat výšková kormidla	bez vstupu od posádky.
Nebezpečí H-2	Systém podélného řízení	nevychyluje výšková kormidla	v požadované úrovni.
Systémové omezení SC-2	Systém podélného řízení	musí vychylovat výšková kormidla	v požadované úrovni.

Není však nutností, aby jedno systémové omezení (SC) sedělo jen na jeden systémový nebezpečí (H), a to samé obráceně. Každé systémové omezení (SC) může vést i k více systémových nebezpečí (H) a každé systémové nebezpečí (H) může obsahovat více systémových omezení (SC).

V pozdějších krocích analýzy vytvoříme a identifikujeme scénáře (a příčiny), které vedou k nedodržení systémových omezení (SC), a tudíž i ke ztrátám.

2.2.1.4. Rozbor nebezpečí

Jakmile si vytvoříme seznam systémových nebezpečí, můžeme je pak rozebrat do tzv. sub-hazards. Ačkoliv je tento krok volitelný, tak nám pomůže v následujících krocích analýzy, obzvláště u velmi komplexních systémů. Příklad rozboru nebezpečí je uveden v následující tabulce.

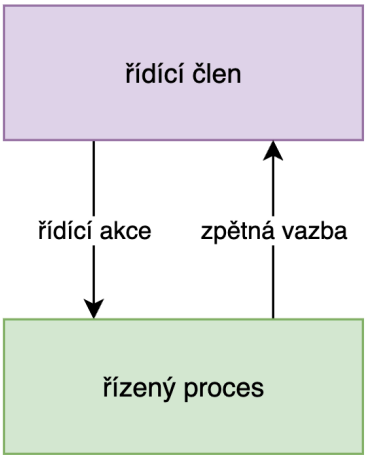
Tab. 2.6: Příklad rozboru nebezpečí

H-1	Letadlo nedodržuje bezpečný odstup od ostatních letadel.
H-1.1	Motory letadla produkují asymetrický tah, způsobující nerovnou trajektorii letadla.
H-1.2	Brzdy nebo spoilery letadla poskytují nedostatečné brždění.
H-1.3	Křidélka neposkytují dostatečné zatáčení letadla.
H-1.4	Výšková kormidla neposkytují dostatečné klopení letadla.
H-1.5	a další…

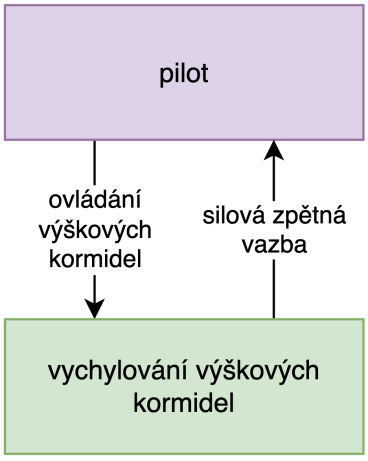
2.2.2. Krok 2: Vytvořte STAMP model

Ve druhém kroku STPA analýzy se vytváří model, který bude znázorňovat hierarchickou řídící strukturu systému. Tento krok je extrémně důležitý a vyžaduje velkou přesnost, neboť následující kroky jsou postaveny na tomto diagramu a veškeré pozdější úpravy v diagramu způsobí nutnost úprav i v dalších krocích.

Každá řídící struktura obsahuje tzv. smyčky, které sestávají z řídících akcí a zpětných vazeb. Na následujících obrázcích je znázorněno jednoduché schéma řídící smyčky:



Obr. 2.5: řídící smyčka



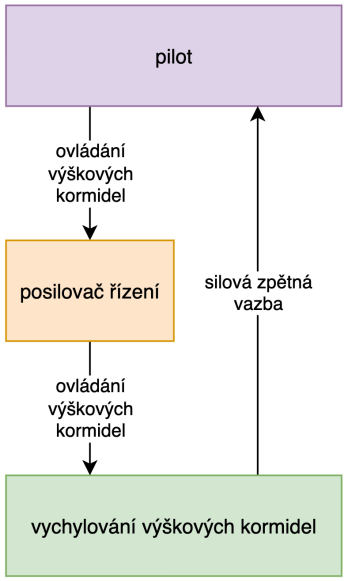
Obr. 2.6: příklad řídící smyčky

Během provozu mohou nastat problémy v jakékoliv části smyčky - ať už u pilota, nebo i ve zpětné vazbě. Zde je pár příkladů, jaké problémy mohou nastat v jednotlivé části smyčky:

- **pilot**: zaneprázdnění, lidský faktor, chybné proškolení, chybná interpretace…
- **řídící akce**: zaseknutí řídící páky, odpojení nebo deformace táhel…
- **vychylování výškových kormidel**: zakročení posilovače řízení výškových kormidel…
- **zpětná vazba**: deformace táhel…

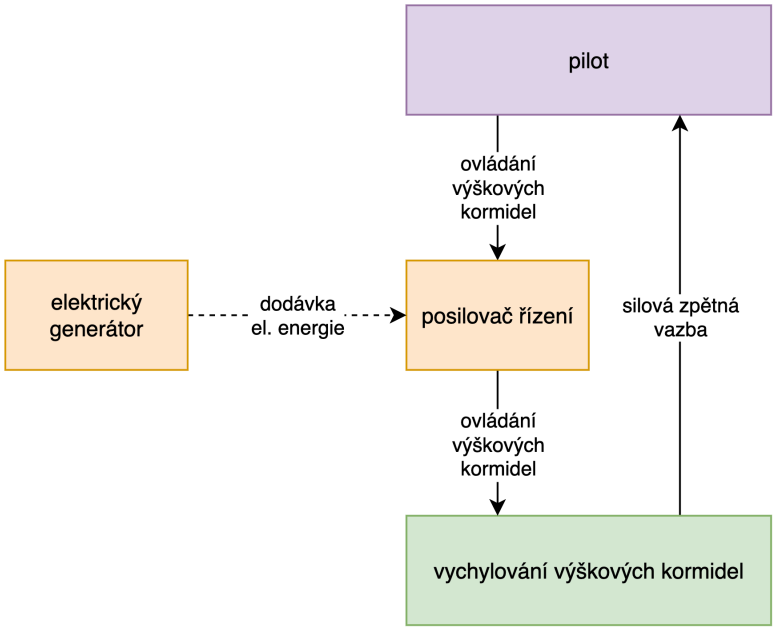
Problémů může nastat opravdu mnoho a STPA metodika nám pomáhá systematicky tyto problémy odhalit a najít způsob, abychom předešli ztrátám.

Řídící akce mohou obsahovat i mnoho dalších subsystémů, které jsou potřebné k uskutečnění daného řízeného procesu. Zpravidla to bývají aktuátory (výkonové členy), ale mohou to také být ovládací členy nebo i mechanické vedení k ovládanému členu (táhla, vedení el. energie…). Následující diagram znázorňuje příklad zakomponování aktuátoru do trasy řídící akce.



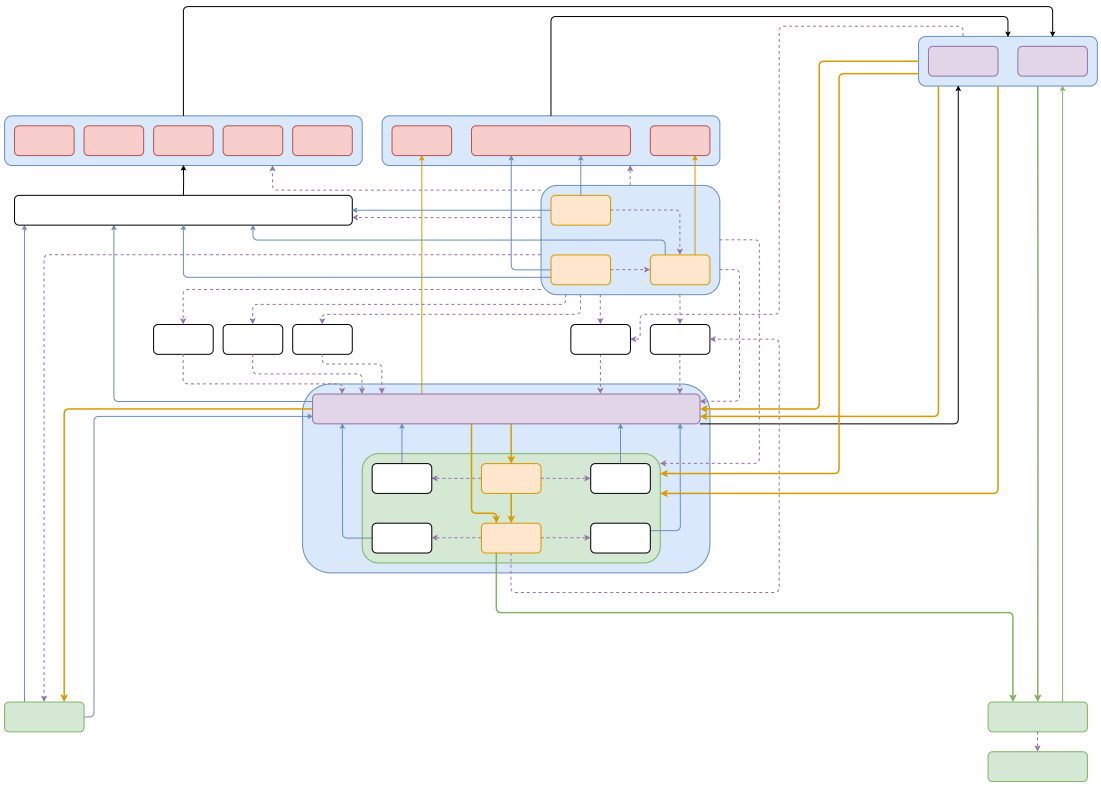
Obr. 2.7: zakomponování aktuátoru do trasy řídící akce

V systémech se mohou rovněž vyskytovat vstupy (tzv. inputs), které nelze identifikovat jako řídící akce a ani zpětné vazby. Nejčastěji to bývají např. dodávka el. energie, dodávka hydraulické kapaliny, datové přenosy mezi řídícími jednotkami apod.



Obr. 2.8: zakomponování vstupu do diagramu

Je samozřejmé, že u komplexních systémů se diagramy nebudou skládat jen z takto jednoduché smyčky. Čím komplexnější systém, tím více smyček bude diagram obsahovat, a to samé platí i pro řídící členy, řídící akce, řízené procesy, zpětné vazby, aktuátory a v neposlední řadě i vstupy (inputs). Při detailnějším rozpracování lehce složitějšího systému může diagram vypadat i takto:



Obr. 2.9: příklad složitějšího STPA diagramu

Vertikální členění hierarchického diagramu má jeden velký význam, a to, že nám indikuje autoritu řídících členů v systému. Tento vertikální systém ukazuje členy s nejvyšší autoritou, které jsou až na vrchu, a ty s nejnižší autoritou, které jsou položeny nejníže v diagramu. Každý člen má určitou autoritu nad členy, které jsou položeny pod ním, a každý člen pod jiným řídícím členem je opět subjektem jeho řízení. Můžeme říci, že veškeré šipky směřující dolu jsou řídící akce, a šipky směřující nahoru jsou zpětné vazby (nebudeme-li zahrnovat vstupy). Tyto konvence nám usnadňují práci s komplexními systémy a zviditelňují jednotlivé řídící smyčky.

2.2.2.1. Rady a poznámky při vytváření STPA diagramu

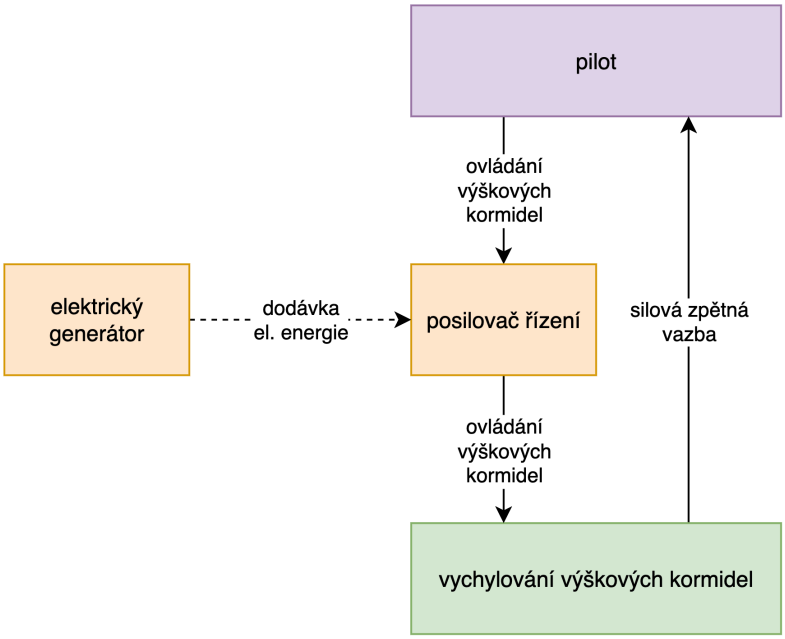
Tato hierarchická řídící struktura je funkční model, nikoliv však fyzické schéma (např. potrubí, el. vedení, táhla…). V STPA diagramu jsou zobrazeny jednotlivé informace, které se posílají mezi jednotlivými komponentami a tyto vazby/informace nemusí být přímo znázornitelné ve fyzických schématech. Příkladem může být komunikace mezi posádkou nebo softwarové procesy – tyto vazby existují, avšak nelze je zobrazit ve fyzickém schématu.

V případě analyzování komplexního systému je dobré, aby se na začátku vytváření diagramu nezacházelo příliš do detailů. STPA je analytická metoda, která se často využívá ještě ve fázích, kdy tyto podrobné detaily v systémech nemusí být známé. Při vytváření diagramu můžeme ze začátku zjednodušit model například takto:

- místo toho, abychom zobrazovali tři piloty, tak stačí je sloučit do jednoho bloku jako posádku
- veškeré indikace posádce lze sloučit jako jeden blok (např. MFD, FMS, Master Warning Tablo…)

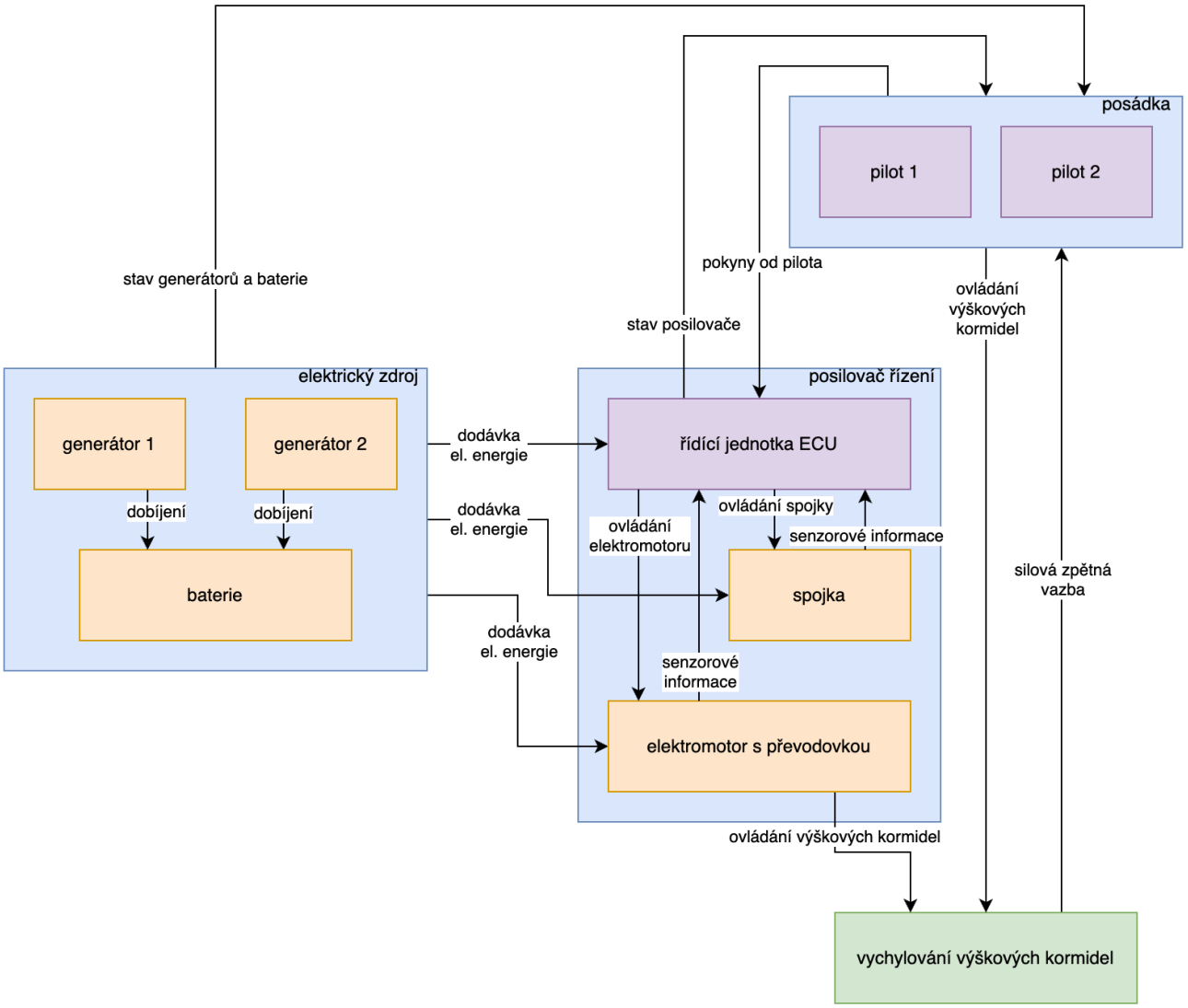
Až budeme mít ve zjednodušeném diagramu celý systém, můžeme pak postupně po jednotlivých komponentech zacházet do čím dál menších detailů.

Níže je znázorněn příklad pro postupné vytváření STPA diagramu:



Obr. 2.10: vytváření STPA diagramu v počáteční fázi

Nejprve je nutné si stanovit pozice jednotlivých komponentů v hierarchické struktuře a jejich vzájemné interakce. Poté můžeme postupně odhalovat detaily těchto komponentů a přidávat další toky informací. Po těchto krocích pak může diagram vypadat takto:



Obr. 2.11: vytváření STPA diagramu v pokročilejší fázi

2.2.3. Krok 3: Identifikujte UCA (Unsafe Control Actions)

UCA (Unsafe Control Actions) jsou nebezpečné řídící akce, které v nejhorším případě mohou vést k nebezpečí. Jejich identifikace se provádí pomocí systematických postupů STPA analýzy a slouží pak jako podklad pro vytváření scénářů v následujícím 4. kroku.

Tento krok přímo navazuje na již vytvořený STPA diagram, ze kterého se vyberou všechny řídící akce a následně se tyto řídící akce přetransformují do UCA podle jejich způsobu vzniku.

UCA může vzniknout čtyřmi následujícími způsoby:

1. aplikování řídící akce vede k nebezpečí,
2. neaplikování řídící akce vede k nebezpečí,
3. řídící akce je uskutečněna příliš brzy nebo příliš pozdě a
4. řídící akce je aplikována příliš dlouho nebo je ukončena příliš brzo.

Jednotlivé způsoby vzniku UCA mohou být pro přehlednost uspořádány do tabulky:

Tab. 2.7: Příklad identifikace UCA

Řídící akce (Control Action)	Aplikování vede k nebezpečí	Neaplikování vede k nebezpečí	Příliš brzo či pozdě, mimo provoz	Zastaveno příliš brzo nebo příliš dlouho aplikováno
[CA-1]: ovládání výškových kormidel	[UCA-1.1]: Posádka ovládá výšková kormidla v jiné, než požadované úrovni nebo směru. [H-1]	[UCA-1.2]: Posádka neovládá výšková kormidla v požadovaném směru. [H-1]	[UCA-1.3]: Posádka začala ovládat výšková kormidla v požadovaném směru příliš pozdě. [H-1]	[UCA-1.4]: Posádka přestala ovládat výšková kormidla v požadovaném směru příliš brzy. [H-1]

Čtvrtý (poslední) způsob vzniku UCA platí pouze pro kontinuální řídící akce, nikoliv diskrétní. V případě diskrétních řídících akcí stačí nechat poslední sloupec volný, jako v následujícím příkladu:

Tab. 2.8: Příklad identifikace diskrétních UCA

Řídící akce (Control Action)	Aplikování vede k nebezpečí	Neaplikování vede k nebezpečí	Příliš brzo či pozdě, mimo provoz	Zastaveno příliš brzo nebo příliš dlouho aplikováno
[CA-8]: rozepnutí/sepnutí mechanického obvodu	[UCA-8.1]: Jednotka ECU sepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	[UCA-8.2]: Jednotka ECU neodepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	[UCA-8.3]: Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA. [H-1]	N/A

Každé UCA musí obsahovat tyto následující položky:

Tab. 2.9: Položky UCA

Řídící člen	Typ UCA	Řídící akce	Kontext	Odkaz na nebezpečí
Posádka	ovládá	výšková kormidla	v jiné, než požadované úrovni nebo směru.	[H-1]
Posádka	neovládá	výšková kormidla	v požadované úrovni nebo směru.	[H-1]
Posádka	začala ovládat příliš pozdě	výšková kormidla	v požadované úrovni nebo směru.	[H-1]
Posádka	přestala ovládat příliš brzy	výšková kormidla	v požadované úrovni nebo směru.	[H-1]

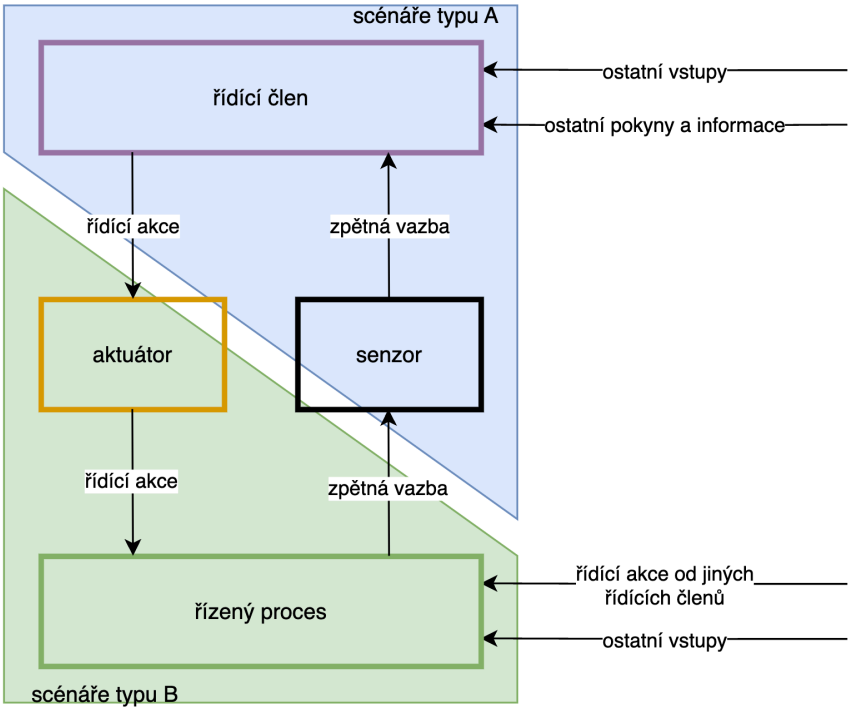
Je extrémně důležité, aby každé UCA obsahovalo přesně definovaný kontext, při kterém je řídící akce považována za nebezpečnou. V případě výškových kormidel je požadované, aby se výšková kormidla vychylovala nahoru pro stoupání letounu a dolu pro klesání. Tato akce může být nebezpečná v případě, že jsou tato výšková kormidla vychýlena v opačném směru, což je právě ten kontext, který musí každé UCA obsahovat.

Do kontextu lze zařadit například také: vnější meteorologické podmínky, stav řídícího člena, předchozí vykonané řídící akce řídícího člena, pozice analyzovaného systému vůči vnějšímu prostředí, směr vykonání řídící akce atd.

2.2.4. Krok 4: Identifikujte ztrátové scénáře

Jakmile identifikujeme UCA, je na řadě vytváření ztrátových scénářů pro každé UCA. Ztrátové scénáře popisují soubor faktorů, které mohou vést k UCA, čímž mohou dále vést k nebezpečím. Podle těchto scénářů pak vytváříme ve finálním kroku seznam vstupů (seznam požadavků a omezení).

Scénáře dělíme na scénáře typu A a typu B. Oba typy scénářů se snaží identifikovat faktory vedoucí k UCA, avšak scénáře typu A se zaměřují na řídící člen a zpětnou vazbu, zatímco scénáře typu B se zaměřují na cestu řídící akce a samotný řízený proces. Pro přehlednost je níže graficky znázorněno zaměření scénářů typu A a B:



Obr. 2.12: grafické odlišení scénářů typu A a B

2.2.4.1. Scénáře typu A

V první části scénářů se snažíme zjistit, co může vést k tomu, že řídící člen vykoná danou řídící akci špatně, nebo ji vůbec nevykoná. Obecně to může být způsobeno následujícími příčinami:

- Chyby zahrnující řídící člen
- Neadekvátní řídící algoritmus
- Nebezpečný vstup od jiného řídícího členu
- Neadekvátní procesní model

Každý scénář musí být očíslovaný a obsahovat, na které UCA se odkazuje.

CHYBY ZAHRNUJÍCÍ ŘÍDÍCÍ ČLEN

Tyto scénáře se zaměřují na příčiny, které se vztahují na stav řídícího člena. Mohou to být například fyzické poruchy řídícího člena, ale také i ztráta dodávky elektrické energie, hydraulické kapaliny apod. Níže je několik scénářů, které se zaměřují na chyby zahrnující řídící člen:

Tab. 2.10: Příklady scénářů (chyby zahrnující řídící člen)

Scénář 1.2.1 pro UCA-1.2 Chyby zahrnující řídící člen	Posádka nevychyluje výšková kormidla v požadovaném směru z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 3.1.1 pro UCA-3.1 Chyby zahrnující řídící člen	Posádka zapnula přívod el. energie pro posilovač při jeho poruše z důvodu nechtěné manipulace.

Scénář 5.4.1 pro UCA-5.4 Chyby zahrnující řídící člen	Posádka přestala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš brzy, neboť z ergonomických důvodů už nedokázala nadále prstem udržet spínač v dané poloze.
Scénář 9.5.1 pro UCA-9.5 Chyby zahrnující řídící člen	Posilovač přestal ovládat výšková kormidla příliš brzy v kritické fázi letu, jelikož se porouchala řídící jednotka (zkrat v obvodu, přehřátí…).

NEADEKVÁTNÍ ŘÍDÍCÍ ALGORITMUS

Nebezpečná řídící akce může být rovněž způsobena neadekvátním řídícím algoritmem. Chyby v řídícím algoritmu mohou způsobovat například:

- chybné naprogramování nebo nakonfigurování řídícího člena,
- stav řídícího člena po předešlých vstupech a výstupech (řídící člen se může chybně domnívat, že řídící akce byla správně vykonána),
- tzv. “decision making” (u lidského faktoru),
- proškolení a zkušenosti,
- chybná implementace řídící akce,
- degradace nebo zaostalost (řídící algoritmus je zastaralý)…

Pro identifikaci těchto scénářů je nutné začít s UCA a zjistit, jakým způsobem může chybný řídící algoritmus způsobit toto UCA.

Tab. 2.11: Příklady scénářů (neadekvátní řídící algoritmus)

Scénář 6.3.1 pro UCA-6.3 Neadekvátní řídící algoritmus	Posádka ovládá trimovací spínač při vypnuté nebo nefunkční řídící jednotce, z důvodu nedostatečného proškolení posádky.
Scénář 7.1.1 pro UCA-7.1 Neadekvátní řídící algoritmus	Řídící jednotka ovládá trimovací plošku v opačném, než požadovaném, směru z důvodu chybného naprogramování (např. chybná proporční korekce vstupních údajů).

NEBEZPEČNÝ VSTUP OD JINÉHO ŘÍDÍCÍHO ČLENU (CONTROLLER)

Tento případ scénářů se vztahuje pouze pro řídící členy, již dostávají pokyny od jiných řídících členů. Příkladem může být komunikace mezi řídícím letového provozu a pilotem, kdy pilot dostává instrukce od řídícího letového provozu. Ačkoliv pilot instrukci splní a vykoná správně svou řídící akci, stále se může jednat o UCA, neboť pilot může obdržet chybnou instrukci, která může způsobit nebezpečí.

NEADEKVÁTNÍ PROCESNÍ MODEL

Procesní modely reprezentují vnitřní domněnky řídícího člena, které ovlivňují, jak řídící člen vykonává danou řídící akci. V případě, že vnitřní domněnka řídícího člena není v souladu se skutečností, může pak řídící člen vykonat UCA. Tento nesoulad může být způsoben následujícími příčinami:

- Řídící člen získá chybnou zpětnou vazbu (informaci),
- řídící člen získá správnou zpětnou vazbu, ale špatně si ji interpretuje nebo ji ignoruje,

- řídící člen nezíská zpětnou vazbu ve chvíli, kdy ji potřebuje (opožděně nebo nikdy),
- potřebná zpětná vazba neexistuje.

Jakmile identifikujeme všechny chybné domněnky řídícího člena, které mohou vést k UCA, je na čase najít jejich příčinu. Jestliže řídící člen neobdrží zpětnou vazbu, může to být z následujících důvodů:

- zpětná vazba je odeslána senzory, avšak nedorazila k řídícímu členovi,
- zpětná vazba je obdržena senzory, avšak senzory tuto informaci nepřeposlaly dále,
- zpětná vazba není obdržena senzory, tudíž ji nemohly přeposlat dále,
- zpětná vazba v řídící struktuře neexistuje.

Může se také stát, že řídící člen může obdržet chybnou zpětnou vazbu. To může být ve zpětné vazbě způsobeno například chybnými datovými převody, ztrátou komunikace, zpoždění v komunikaci apod. V tomto případě může jít o následující situace:

- senzory přeposlaly zpětnou vazbu správně, avšak k řídícímu členovi dorazila chybně,
- senzory chybně přeposlaly zpětnou vazbu,
- senzory nejsou navrženy pro přeposílání určitého typu zpětné vazby.

V tabulce tab. 2.12 jsou příklady, jak by zahrnutí procesních modelů v analýze mohlo vypadat:

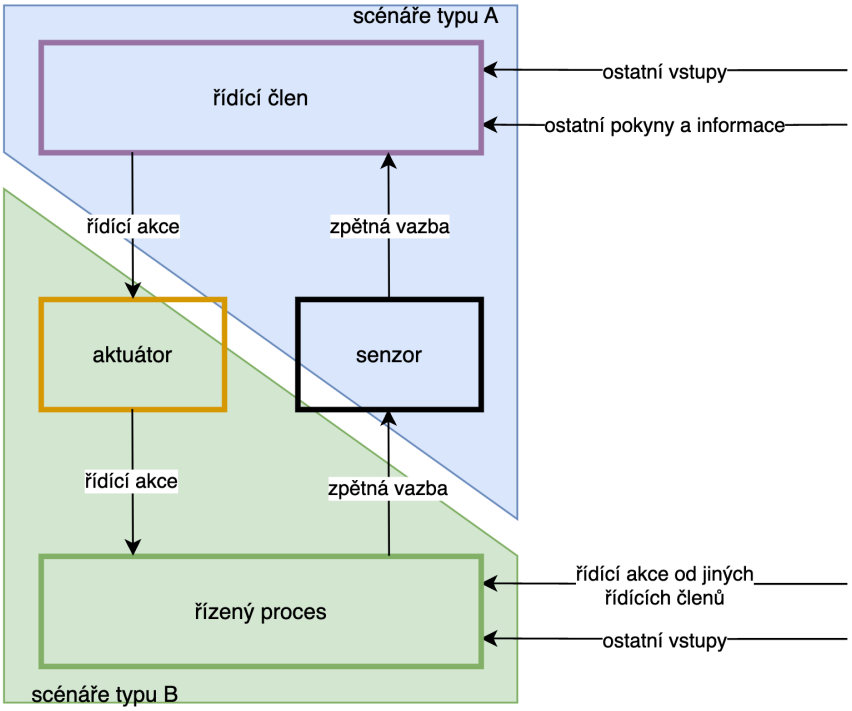
Tab. 2.12: Příklady scénářů (neadekvátní procesní model)

Scénář 1.1.3 pro UCA-1.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Posádka vychyluje výšková kormidla v jiné, než požadované, úrovni, neboť dostává neadekvátní silovou zpětnou vazbu v řízení.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že v systému není žádná porucha.
Co mohlo toto způsobit	- praskl pružinový posilovač - posilovač v každém směru dodává jiný výkon - páky v cestě podélného řízení mají chybný převod
Scénář 1.3.2 pro UCA-1.3 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka vychýlila výšková kormidla v požadovaném směru příliš pozdě, neboť si posádka příliš pozdě všimla, že výšková kormidla nikdo neovládá.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že výšková kormidla ovládá druhý pilot.
Co mohlo toto způsobit	- špatná komunikace mezi posádkou - zaneprázdnění posádky - nejednoznačně rozdělené role (pilot flying/monitoring)
Scénář 2.1.3 pro UCA-2.1 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka nevypnula přívod el. energie do posilovače při jeho poruše, neboť nedostala indikaci o jeho poruše.

Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že posilovač je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - řídící jednotka posilovače je špatně nakonfigurovaná, z toho důvodu neodeslala informace o jeho poruše
Scénář 7.1.3 pro UCA-7.1 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Řídící jednotka ovládá trimovací plošku v opačném, než požadovaném, směru, jelikož řídící jednotka nepřepnula směr ovládání trimovací plošky poté, co se výšková kormidla vychýlila na opačnou stranu.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla jsou stále vychýlena v původním směru.
Co mohlo toto způsobit	- zamrznutí řídící jednotky - řídící jednotka je zahlcena vstupními údaji a nezvládá včas zpracovávat nápor dat

2.2.4.2. Scénáře typu B

Tato část scénářů je zaměřena na cestu vykonání řídící akce a ostatní faktory, které mohou ovlivnit řízený proces.



Obr. 2.13: grafické odlišení scénářů typu A a B

CESTA VYKONÁNÍ ŘÍDÍCÍ AKCE (CONTROL PATH)

Cesta vykonání řídící akce nám pomáhá přenášet řídící akce od řídícího člena až k řízenému procesu. Tato cesta může zahrnovat například jeden nebo i více aktuátorů, elektrické vedení, komunikace mezi satelity a další.

Obecně scénáře zahrnující cestu vykonání řídící akce se mohou dělit do následujících kategorií:

- řídící akce nebyla vykonána:
  - řídící akce byla vykonána řídícím členem, avšak nebyla obdržena aktuátorem,
  - řídící akce byla obdržena aktuátorem, avšak aktuátor nereaguje,
  - aktuátor reaguje adekvátně, avšak řízený proces neobdržel řídící akci.
- řídící akce byla chybně vykonána:
  - řídící akce byla vykonána řídícím členem, avšak chybně obdržena aktuátorem,
  - řídící akce byla obdržena aktuátorem, avšak aktuátor reaguje neadekvátně,
  - aktuátor reaguje adekvátně, avšak u řízeného procesu je řídící akce aplikována neadekvátně,
  - aktuátor reaguje navzdory tomu, že žádná řídící akce nebyla vykonána.

Tyto scénáře mohou zahrnovat příčiny, jako jsou: ztráta komunikace, prodlevy v komunikaci, porucha aktuátoru, ztráta dodávky energie do aktuátoru, protikladné vstupy, nebo degradace aktuátoru. Níže je zobrazeno více příkladů, které mohou nastat v cestě vykonání řídící akce.

Tab. 2.13: Příklady scénářů (cesta vykonání řídící akce)

Řídící akce byla chybně vykonána: **Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru.**	
Scénář 1.1	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu trvalé deformace táhel.
Řídící akce nebyla vykonána: **Výšková kormidla nebyla vychylována v požadovaném směru.**	
Scénář 1.4	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru, jelikož došlo k rozpojení mechanické cesty podélného řízení.
Řídící akce byla chybně vykonána: **Trimovací ploška byla vychylována v jiném, než požadovaném směru.**	
Scénář 5.1	Trimovací ploška byla vychylována v jiném, než požadovaném směru, jelikož je aktuátor trimovací plošky opačně propojen k trimovacímu spínači.
Řídící akce nebyla vykonána: **Trimovací ploška není vychylována při velkých silách v řízení.**	
Scénář 5.4	Trimovací ploška není vychylována při velkých silách v řízení z důvodu mechanické poruchy aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: **Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy.**	

Scénář 5.6	Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy, neboť během ovládání trimovací plošky došlo k přerušení dodávky el. energie do aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: Trimovací ploška se vychyluje, i když nebyla vychýlena výšková kormidla.	
Scénář 7.2	Trimovací ploška se vychyluje, i když nebyla vychýlena výšková kormidla z důvodu samovolné aktivace aktuátoru trimovací plošky.
Scénář 7.4	Trimovací ploška se nevychyluje v požadovaném směru při velkých silách v řízení z důvodu přerušení dodávky el. energie do aktuátoru trimovací plošky.

FAKTORY OVLIVŇUJÍCÍ ŘÍZENÝ PROCES

I v případě, že je řídící akce úspěšně aplikována na řízený proces, stále je zde možnost, že se řízený proces neuskuteční nebo uskuteční chybně. Tyto scénáře vztahující se na faktory ovlivňující řízený proces mohou být často způsobeny nevhodnými nebo chybějícími vstupy (inputs), jako je třeba nízký tlak v hydraulické soustavě, špatné počasí, chybějící dodávka el. energie, zpožděná reakce řízeného procesu, protikladné pokyny od jiných řídících členů a další.

Tyto scénáře mohou zahrnovat následující situace:

- řízený proces se neuskutečnil:
  - řízená akce byla aplikována řídícím členem a aktuátory, avšak řízený proces nereaguje
- řízený proces se uskutečnil chybně:
  - řízená akce byla aplikována řídícím členem a aktuátory, avšak řízený proces reaguje chybně
  - řízená akce nebyla aplikována řídícím členem nebo aktuátory, avšak řízený proces reaguje, jako kdyby byla aplikována

Tab. 2.14: Příklady scénářů (faktory ovlivňující řízený proces)

Řídící akce byla chybně vykonána: Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru.	
Scénář 1.2	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu zakročení posilovače řízení.
Řídící akce byla chybně vykonána: Trimovací ploška je vychýlena příliš dlouho i poté, co se přestala vychylovat výšková kormidla.	
Scénář 7.10	Trimovací ploška je vychýlena příliš dlouho i poté, co se přestala vychylovat výšková kormidla z důvodu zaseknutí mechanismu trimovací plošky (např. vlivem uvolnění součástky, vniknutí cizích předmětů…).

2.2.5. Finální krok: Identifikujte požadavky a omezení

Jakmile dokončíme všechny čtyři základní kroky STPA analýzy, je na čase vytvořit seznam požadavků a omezení. Tento seznam může později sloužit jako tzv. “checklist” pro další fáze vývoje systému, jako třeba při tvoření letových manuálů, školení personálu apod.

Tyto požadavky a omezení se musí vytvářet ke každému kroku STPA analýzy (kromě druhého kroku). Níže je zobrazen postup pro tvoření požadavků a omezení pro jednotlivé kroky.

KROK 1

Požadavky a omezení vztahující se k systémovým nebezpečím jsme již v prvním kroku udělali, jako je to u tabulky tab. 2.5 v kapitole 2.2.1.

KROK 3

Ve třetím kroku se musí požadavky a omezení vztahovat k jednotlivým UCA. Stačí jednoduše obrátit jejich význam, jako níže v tabulce:

Během toho se rovněž může stát, že více než jedno UCA se nám bude vztahovat jen k jednomu požadavku nebo omezení, a někdy také se k jednomu UCA musí vytvořit více požadavků a omezení.

Tab. 2.15: Příklady identifikace požadavků a omezení (krok 3)

UCA-1.4	Posádka přestala ovládat výšková kormidla v požadovaném směru příliš brzy. [H-1]
CC-1.2	Posádka nesmí přestat ovládat výšková kormidla příliš brzy. [UCA-1.4]
UCA-6.1	Posádka ovládá trimovací spínač v opačném, než požadovaném, směru. [H-1.1; H-1.2]
CC-6.1	Posádka musí ovládat trimovací spínač v požadovaném směru. [UCA-6.1]
UCA-7.2	Řídící jednotka vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla. [H-1; H-1.2; H-2]
CC-7.2	Řídící jednotka nesmí vychylovat trimovací plošku, nejsou-li vychýlena výšková kormidla. [UCA-7.2]

KROK 4

U čtvrtého kroku se požadavky a omezení vztahují k jednotlivým scénářům. U jednotlivých scénářů je potřeba vytvořit takové požadavky a omezení, abychom minimalizovali vznik daného scénáře. I zde se může stát, že k jednomu požadavku nebo omezení se bude vztahovat více scénářů, a také k jednomu scénáři bude náležet více požadavků a omezení.

Zde je obecný postup pro tvoření požadavků a omezení podle scénářů:

Tab. 2.16: Příklad scénáře pro identifikace požadavků a omezení (krok 4)

Scénář 1.1.2 pro UCA-1.1 Neadekvátní řídící algoritmus	Posádka vychyluje výšková kormidla v jiné, než požadované, úrovni z důvodu nedohodnutého zakročení druhého pilota do řízení.

Pro výše uvedený scénář může požadavek nebo omezení vypadat takto:

Tab. 2.17: Příklad identifikovaného požadavku nebo omezení (krok 4)

Požadavky a omezení CFC-1.1	Druhý pilot nesmí zasahovat řídícímu pilotovi do řízení. [Scénář 1.1.2]

Níže jsou další příklady, jak může tvoření požadavků a omezení ze scénářů vypadat:

Tab. 2.18: Příklady identifikace požadavků a omezení (krok 4)

Scénář 6.3.1 pro UCA-6.3 Neadekvátní řídící algoritmus	Posádka ovládá trimovací spínač při vypnuté nebo nefunkční ECU jednotce, z důvodu nedostatečného proškolení posádky.
Požadavky a omezení CFC-5.5	Posádka musí být poučena, že při nefunkční nebo vypnuté řídící jednotce není možné nadále ovládat trimovací plošku. [Scénář 6.3.1]
Scénář 1.5	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu zakročení posilovače řízení.
CPC-1.3	Jednotka PCA nesmí začít působit proti silám vyvolaných posádkou. [Scénář 1.5; 1.7]

Někdy se může stát, že u jednoho scénáře potřebujeme vytvořit více požadavků a omezení, jako u níže zmíněného scénáře, u kterého nám vznikly rovnou dva.

Tab. 2.19: Příklad identifikace více požadavků a omezení z jednoho scénáře

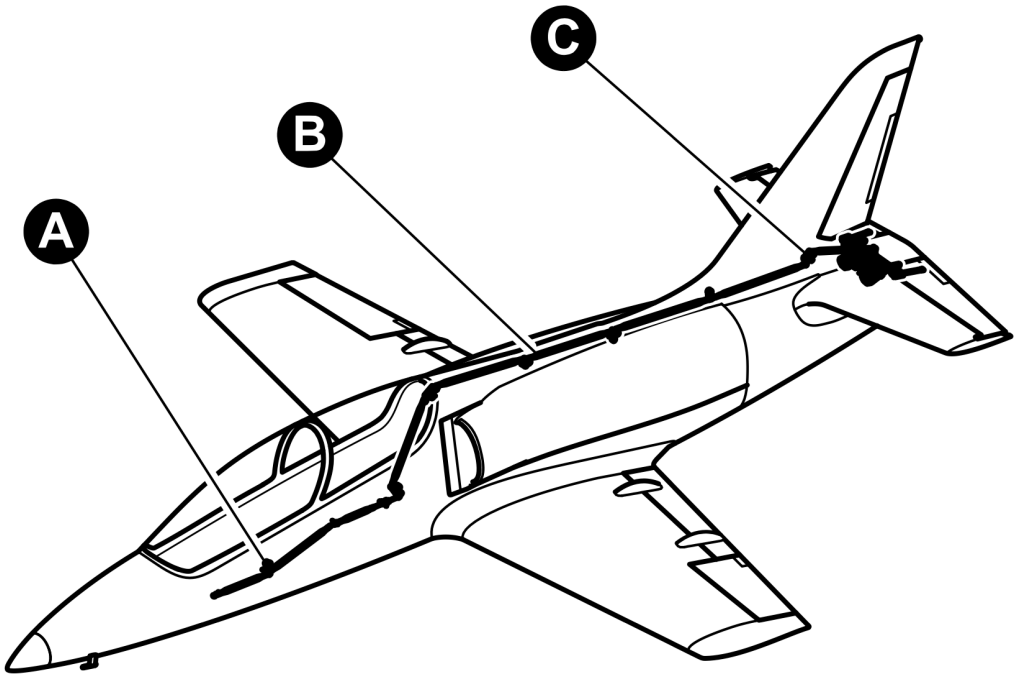
Scénář 3.1.2 pro UCA-3.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Posádka na zemi zapnula přívod el. energie do posilovače při jeho poruše, jelikož nedostala indikaci o jeho nefunkčnosti po sepnutí el. obvodu.
Doměnka řídícího členu, která vede k UCA	Posádka se domnívá, že jednotka PCA je funkční.
Co mohlo toto způsobit	- řídící jednotka je špatně nakonfigurovaná, z toho důvodu neodeslala informace o jeho poruše - posádka neotestovala funkčnosti žárovek pro master tabla
Požadavky a omezení CFC-3.1	Posádka musí ještě před zapnutím přívodu el. energie do posilovače otestovat funkčnost žárovek na Master Tablu. [Scénář 3.1.2]
Požadavky a omezení CFC-2.3	Jednotka ECU musí být nastavená na správné provozní hodnoty, aby v případě poruchy jednotky PCA dokázala detekovat vadu a bezprostředně o ní informovat posádku. [Scénář 2.1.3; 2.2.3; 3.1.2; 3.2.3; 3.3.3; 4.2.3; 4.3.3; 7.4.1; 8.1.1; 8.2.2; 9.1.2]

2.3. Popis systému podélného řízení

Vodorovné ocasní plochy letounu L-39 NG jsou děleného typu s výškovými kormidly na odtokových hranách stabilizačních ploch. Jedná se o nepřímé mechanické řízení, kdy do táhlového vedení je vložen silový člen, v našem případě označován jako PCA (Pitch Control Actuator).

Výšková kormidla zajišťují podélné řízení, jsou vychýlitelná v obou směrech do libovolné polohy a ovládají se pomocí dvou HOTAS (Hands On Throttle And Stick) pák, jež jsou mechanicky propojené soustavou táhel a pák. Maximální výchylky kormidel jsou 30° v horním směru a 20° v dolním směru.

Na obr. 2.14 je znázorněno zjednodušené schéma trasy podélného řízení letounu, kde sekce A vede pod prostorem pilotních kabin, sekce B v oblasti nad pohonnou jednotkou a sekce C u ocasních ploch.



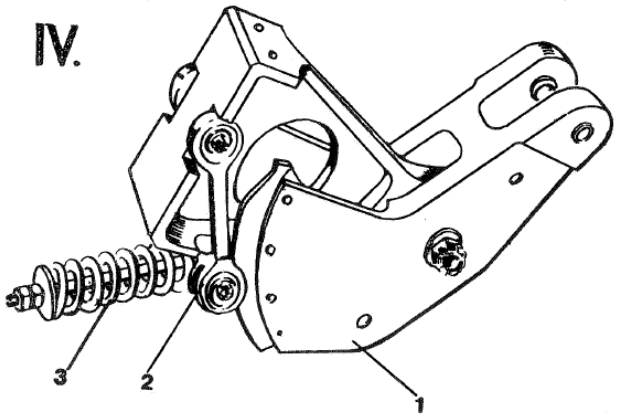
Obr. 2.14: zjednodušené schéma trasy podélného řízení letounu L-39 NG

2.3.1. Trasa podélného řízení

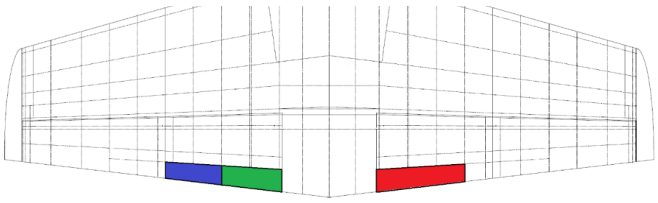
Trasa podélného řízení začíná v prostorách pilotní kabiny, kde piloti ručně ovládají HOTAS páky, které jsou kloubním spojením uchycené k táhlům. Při přitlačení nebo přitažení HOTAS páky dojde k přenosu pohybu z řídící páky na táhla pomocí pákového mechanismu. Páky (angl. bellcrank) po celé trase zajišťují propojení táhel a jejich upevnění k trupovým přepážkám.

Trasa je vedena nejprve v prostoru pod pilotní kabinou. V místě za pilotní kabinou a před vstupním ústrojím motoru přechází systém táhel a pák do prostoru nad motorem, kudy pak vede dále až k oblasti pod kýlovou plochou. Zde je táhlo podélného řízení napojené na páku, která kromě toho, že je mechanicky propojená k výškovým kormidlům pomocí čepů, tak také obsahuje závaží a pružinový posilovač s vačkovým mechanismem. Vychýlení tohoto pákového spoje způsobí přímo pohyb výškového kormidla v horním nebo dolním směru.

Pružinový posilovač se sám aktivuje výchylkách vyšších než cca ±13° a částečně pomáhá odstraňovat aerodynamické síly působící do systému řízení při vyšších rychlostech nebo násobcích. Kromě toho udržuje výškové kormidlo v horizontální poloze pomocí napnuté pružiny, a ta se při vychýlení kormidel napíná.



Obr. 2.15: pružinový posilovač se závažím



Obr. 2.16: rozložení odlehčovací plošky (zeleně), vyvažovací plošky (červeně) a kompenzační plošky vztlakových klapek (modře)

Za levým komidlem se nachází odlehčovací ploška, která se vychyluje v závislosti na výchylce výškového kormidla. Je jedním z prostředků, jež snižují síly působící pilotům do řídících pák. Tato ploška je přímo mechanicky propojena táhlem k horizontálnímu stabilizátoru tak, aby při výchylce kormidla nahoru šla odlehčovací ploška dolu a nahoru při výchylce kormidla dolu.

Kromě odlehčovací plošky se za levým kormidlem nachází také kompenzační ploška vztlakových klapek, která však nespadá do systému podélného řízení letounu. Jejím hlavním účelem je kompenzovat klopivý moment vztlakových klapek a pomáhat udržovat nos letounu nahoře, aby mohl pilot efektivně provést podrovnání (angl. flare) při přistání.

2.3.2. Pitch Control Actuator

Při letu ve vyšších rychlostech nebo při vyšším násobku dochází k růstu aerodynamických sil působících do systému podélného řízení. Kromě rychlosti a násobku se mohou na přírůstku sil významně podílet i krajní centráže, kdy oproti ostatním polohám citelně zvyšují sílu do řízení.

Jedním ze způsobů pro překonávání sil v řízení je zasazení posilovače “paralelně” do systému řízení. U letounu L-39 NG je tento posilovač nazýván jako Pitch Control Actuator. Jednotka PCA se primárně skládá z elektromotoru, převodovky, spojky, vestavěného počítače a výstupní hřídeli. V jednotce jsou dále nainstalované senzory na teplotu a tlak, které měří sílu vyvolanou pilotem na řídící páky. Údaje z těchto senzorů jsou zasílány do vestavěného počítače ECU.

ECU, neboli Electronic Control Unit, vyhodnocuje přijaté informace a podle nich ovládá hlavně elektromotor a spojku. Elektromotor roztáčí hřídel s převodovkou, která mění otáčky na výstupní hřídeli. Na té je pak upevněna páka servopohonu a je táhlem propojena k systému podélného řízení.

2.3.3. Režimy jednotky PCA

V současné chvíli je jednotka PCA stále ve vývoji a není ještě jasné, v jakém režimu bude jednotka PCA fungovat. Nabízí se zatím dva režimy (mode 1 a mode 2), avšak do ostrého provozu se musí zvolit pouze jeden režim. Zvolení obou režimů (tj. že piloti budou moci přepínat mezi režimem 1 a režimem 2) by nejenom ztížilo vývoj a výrobu jednotky PCA, ale také by výrazně zkomplikovalo její testování a certifikaci.

Oba režimy se liší hlavně naprogramováním řídící jednotky ECU a uspořádáním silových senzorů. Ostatní mechanické komponenty, jako jsou spojka, elektromotor, převodovka apod. jsou v obou režimech stejné.

Dalším rozdílem je řízení trimovací plošky, což je podrobněji rozepsáno níže u jednotlivých režimů. Trimovací ploška pomáhá efektivněji odstraňovat aerodynamické síly v řízení než odlehčovací ploška a narozdíl od výškových kormidel je vychylována elektromotorem (aktuátorem), nikoliv však táhly.

2.3.3.1. Režim 1 (mode 1)

V režimu 1 získává řídící jednotka ECU vstupní údaje od dvou silových senzorů. Silový senzor 1 měří příspěvek síly, který vznikne působením jednotky PCA, a silový senzor 2 měří sílu, která vznikne na výstupním táhle působením od pilota. Dále získává jednotka ECU vstupní údaje o násobku letu a pomocí tohoto údaje vytváří korekci pro výpočet síly, již bude generovat elektromotor.

V tomto režimu je trimovací ploška ovládána posádkou nezávisle na jednotce PCA (tj. trasa ovládání trimovací plošky nezahrnuje jednotku PCA). Posádka ovládá trimovací plošku pomocí spínače na HOTAS páce, jenž přímo vysílá signály do elektromotoru (aktuátoru) trimovací plošky.

Tudíž v případě poruchy nebo vypnutí jednotky ECU nehrozí, že posádka ztratí možnost ovládání trimovací plošky.

Hlavní výhodou režimu 1 (oproti režimu 2) je jeho jednoduchost. Díky tomu je systém méně nákladný na výrobu a certifikaci, což nejenom zjednoduší celý proces vývoje a výroby, ale také zvýší jeho bezpečnost.

2.3.3.2. Režim 2 (mode 2)

Režim 2 se od režimu 1 liší svou výraznou komplexností a propojeností s ostatními systémy. Řídící jednotka ECU získává vstupní údaje taktéž od dvou silových senzorů, avšak silové senzory měří odlišné údaje. Silový senzor 1 měří sílu, která vznikne působením od pilota na řídící páce, a silový senzor 2 měří výchylku výstupní páky, neboli výchylku výškových kormidel. Kromě násobku letu získává jednotka ECU také vstupní údaje o rychlosti letu. Pomocí těchto dvou údajů jednotka ECU vytváří korekce pro výpočet síly, kterou bude generovat elektromotor.

V režimu 2 je trimovací ploška rovněž vychylována pomocí elektromotoru (aktuátoru) trimovací plošky, avšak celý proces jejího řízení je řízen jednotkou ECU, nikoliv však posádkou, jak je tomu v režimu 1. Pokud posádka vychýlí trimovací spínač na HOTAS páce, jednotka ECU nezačne ihned vychylovat trimovací plošku. Místo toho nechá zvýšit sílu, kterou bude generovat elektromotor, a to pouze po omezenou dobu. Jestliže posádka i po uplynutí této omezené doby stále ovládá trimovací spínač ve stejném směru, jednotka ECU vyšle signál k vychýlení trimovací plošky. Díky tomu dochází k nižšímu opotřebení trimovací plošky, což opět pomáhá snížit náklady na její údržbu.

Narozdíl od režimu 1 má režim 2 jeden velký přínos pro budoucí vývoj letounu L-39 NG, a tím je vývoj autopilota. Díky jejímu propojení s ostatními systémy lze do jednotky PCA (v režimu 2) doprogramovat autopilota, což v současné chvíli letoun L-39 NG nenabízí.

Její propojenost s ostatními systémy nese však jedno velké riziko. V případě poruchy nebo vypnutí jednotky ECU posádka nemá možnost nadále ovládat trimovací plošku, neboť celý proces vychylování trimovací plošky řídí jednotka ECU.

2.4. Stanovení vstupů pro zajištění potřebné spolehlivosti

Metoda STPA je pouze kvalitativní, nikoliv kvantitativní, analytickou metodou. To je jedním z důvodů, proč při certifikaci letadel a letadlových celků nelze využít pouze STPA analýzu. STPA analýzu, která analyzuje bezpečnost systému, musí vždy doplňovat jiné analytické metody, které analyzují spolehlivost systému, aby se tyto různé analýzy navzájem doplňovaly a byly úřadem uznány za vhodné.

Bezpečnost a spolehlivost jsou dva kritické aspekty, které se vzájemně doplňují. U bezpečnosti se snažíme, aby nedošlo k určitým nebezpečím a tím i ke ztrátám, což mohou být například nehody, škody na majetku, zranění, znečištění životního prostředí a další. Za to spolehlivost je vyjádřena procentuální hodnotou, jež značí pravděpodobnost, že u daného systému nebo komponenty nenastane poruchový stav. V závislosti na typu a závažnosti selhání má každá

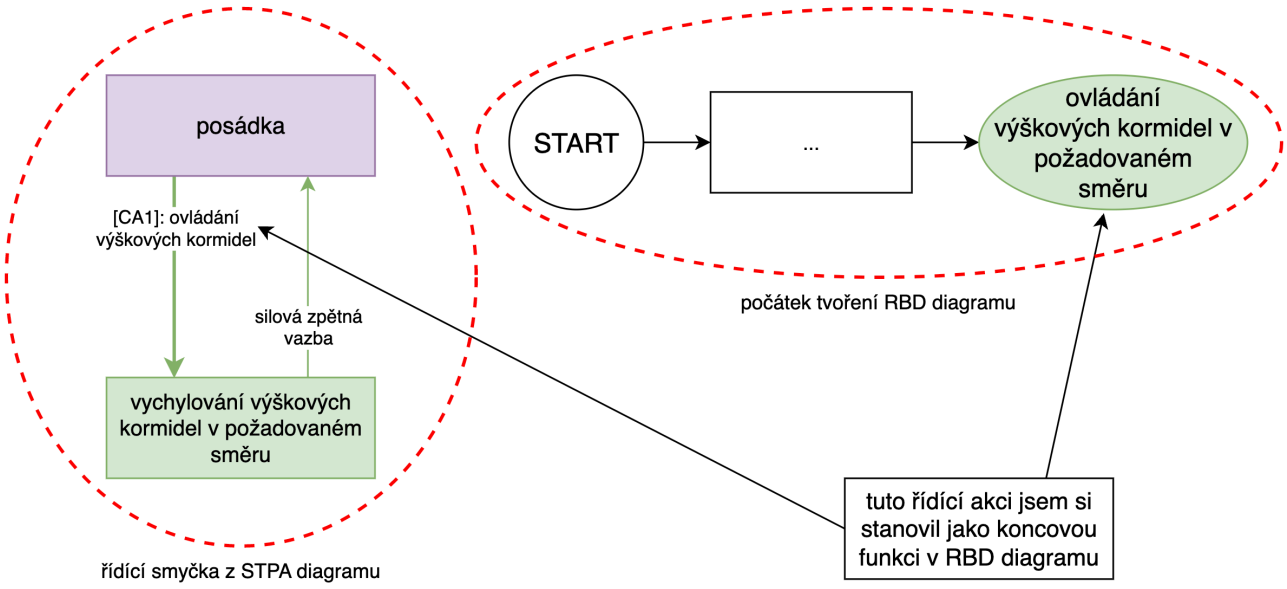
funkce z pohledu spolehlivosti rozdílné přípustné rozmezí pro určení pravděpodobnosti poruch. Pro určení, jakou přípustnou pravděpodobnost selhání můžeme na danou funkci aplikovat, využíváme právě bezpečnostní analýzy, což v mém případě byla STPA analýza. Díky propojenosti všech scénářů (4. krok) s nebezpečími (1. krok) se dá snadno a přesně určit závažnost dané poruchy, což například u metody FTA nemusí být případem. Zde může nastat situace, kdy komponenta, jejíž porucha může způsobit vážnější následky, bude mít tolerantnější rozmezí pravděpodobnosti poruchy než jiná komponenta, jejíž porucha bude mít mírnější následky.

Jedním z cílů mé bakalářské práce je stanovit vstupy pro zajištění potřebné spolehlivosti hodnocené techniky, v tomto případě posilovače řízení, neboli jednotky PCA. Pomocí analytické metody STPA jsem stanovil vstupy pro zajištění potřebné bezpečnosti systému, avšak pro vypočítání procentuální hodnoty spolehlivosti jsem již musel využít metodu RBD, již jsem popsal výše v kapitole 2.1.4.

2.4.1. Postup tvoření RBD

Níže jsem stručně popsal postup, jak jsem podle STPA diagramu z mé STPA analýzy vytvořil RBD diagramy:

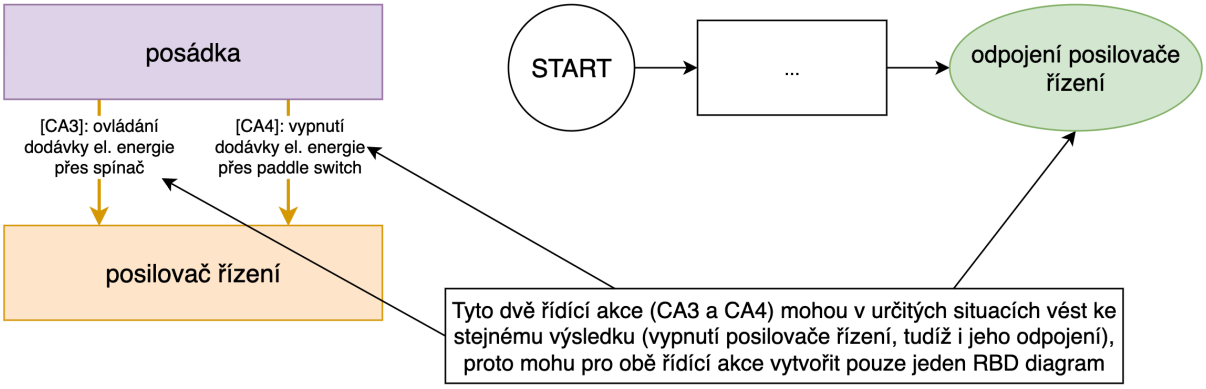
1) Určím si, pro jaké koncové funkce systému budu vytvářet RBD diagramy:
   a) Každou řídící akci nebo vstupy (inputs) z STPA diagramu si nejprve stanovím jako koncovou funkci. Na obrázku Obr. 2.17 je znázorněno, jak z řídící akce jsem si vytvořil koncovou funkci v RBD diagramu.



Obr. 2.17: Postup stanovení koncové funkce v RBD diagramu

   b) Zkontroluji si, zdali nejdou koncové funkce některých řídících akcí sloučit. Jedná se o řídící akce, které mohou vést ke stejnému výsledku. Na obr. 2.18 jsem uvedl zjednodušený příklad, kde řídící akce CA3 ovládá dodávku el. energie přes spínač

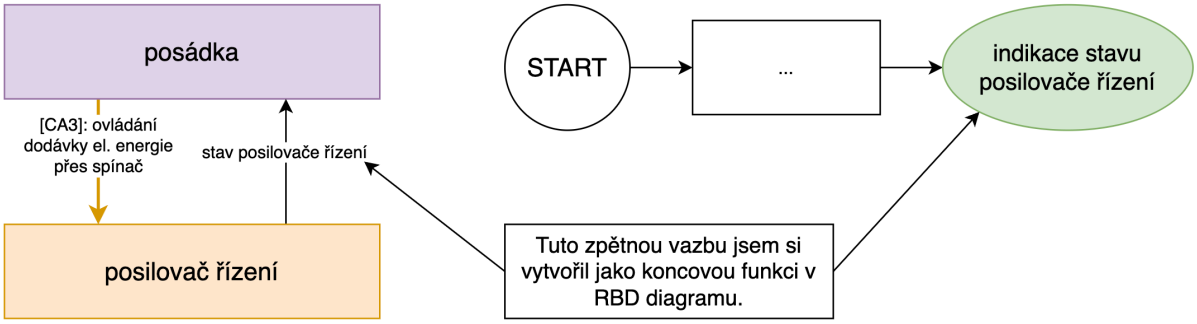
(může dodávku zapnout i vypnout) a řídící akce CA4 pouze vypíná dodávku přes paddle switch.



Obr. 2.18: Příklad sloučení funkcí dvou řídících akcí

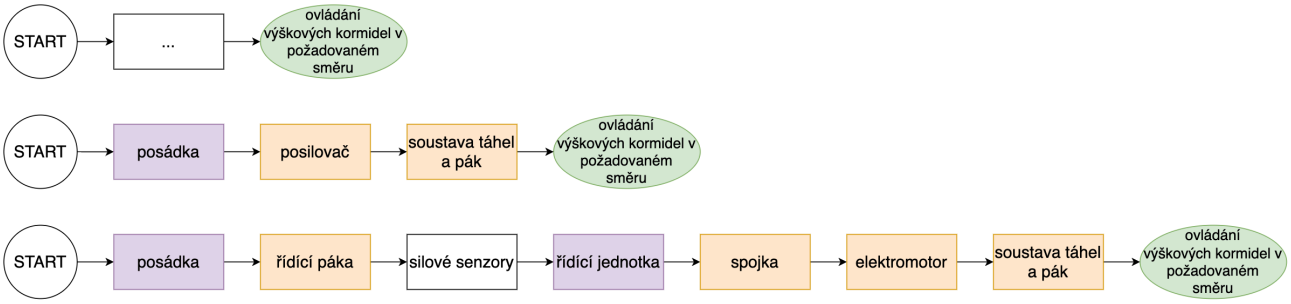
c) Zkontroluji si, jestli z jedné řídící akce nelze vytvořit více koncových funkcí. Například řídící akce CA3 (ovládání dodávky el. energie přes spínač) ve výše uvedeným obrázku obr. 2.18 může vést k vykonání dvou rozdílných koncových funkcí, a to zapnutí dodávky el. energie do posilovače (při nastartování systému) a jeho vypnutí (při poruše posilovače).

d) Nesmíme zapomenout, že i indikace stavu nějaké komponenty je nezbytnou koncovou funkcí. Aby pilot mohl bezpečně ovládat výšková kormidla pomocí posilovače řízení, musí mít správnou zpětnou vazbu, která ho informuje o případné poruše posilovače.



Obr. 2.19: Příklad indikace jako koncové funkce v RBD

2) Do diagramu budu postupně přidávat jednotlivé komponenty, které jsou obsaženy v cestě dané řídící akce. Mohou to být například mechanické vazby (táhla, lanka), mechanismy, elektrická vedení, aktuátory nebo řídící jednotky – prostě vše, co je obsaženo v dané trase.



Obr. 2.20: Příklad postupného zakomponování jednotlivých komponentů do RBD diagramu

3. Výsledky a diskuze

CÍL PRÁCE A KONTEXT

Hlavním cílem mé bakalářské práce je provést bezpečností analýzu pomocí metody zvané STPA, a to v rámci vývoje a výroby vojenských letounů. Tuto metodu jsem chtěl poté porovnat s tradičními metodami, jako je FTA, FMEA nebo FHA. Praktická část bakalářské práce sestává z bezpečnostní analýzy, jež byla vytvořena metodou STPA. Předmětem mé analýzy byl systém podélného řízení s posilovačem (zvaný jako PCA – Pitch Control Actuator), který se aktuálně vyvíjí ve Vodochodech pro nově vyvinutý letoun Aero L-39 NG. Pomocí této analýzy jsem chtěl zjistit, jaké přínosy může metoda STPA přinést a zdali se její implementace ve výrobních organizacích může vyplatit.

VÝSLEDKY BEZPEČNOSTNÍ ANALÝZY

Praktická část mé bakalářské práce obsahuje STPA analýzu, jejíž výstupem je seznam požadavků a omezení na analyzovaný systém, což je systém podélného řízení s posilovačem letounu Aero L-39 NG. Příklady těchto požadavků a omezení jsou uvedeny v kapitole 2.2.5. “Finální krok: Identifikujte požadavky a omezení”, kde je uveden i jejich postup tvoření.

Požadavky a omezení z STPA analýzy se tvoří celkem ve třech úrovních:

- úroveň systému (z 1. kroku),
- úroveň řídící smyčky (ze 3. kroku) a
- úroveň jednotlivých komponent v řídící smyčce (ze 4. kroku).

Nejdůležitější jsou výstupy z úrovně jednotlivých komponent (ze 4. kroku), neboť výstupy z úrovně systému a řídící smyčky jsou relativně obecné. Níže jsem uvedl několik příkladů, u kterých si osobně myslím, že mohou mít přínos pro vývoj systému.

Tab. 3.1: Výstup z analýzy (CFC-1.3)

CFC-1.3	Posádka musí vědět, jak kompenzovat chybějící síly od pružinového posilovače, dojde-li k jeho prasknutí. [Scénář 1.1.3]

Mechanický pružinový posilovač, který se nachází v oblasti ocasních ploch, pomáhá držet výškové kormidlo v úrovni (aby vlivem gravitace nešlo kormidlo dolu) a při velkých výchylkách pomáhá pilotům překonávat velké síly v řízení. V případě, že dojde k prasknutí jeho pružiny, dojde k tomu, že se výšková kormidla nemusí vrátit do své neutrální polohy (mohou být lehce vychýlena). Z toho důvodu by posádka měla vědět, zdali k této události došlo, a případně jak ovládat výšková kormidla tak, aby nedošlo k dalším ztrátám.

Tab. 3.2: Výstup z analýzy (CFC-1.8)

CFC-1.8	Posádka musí být ihned informována, dojde-li k (nechtěnému) vypnutí dodávky el. energie do jednotky PCA. [Scénář 1.3.3; 9.5.3]

Při ztrátě nebo vypnutí dodávky elektrické energie může dojít k tomu, že se z komponenty (v tomto případě posilovače, neboli jednotky PCA) nevyšle elektrický signál, který má signalizovat její stav. To může zapříčinit, že posádka nebude na tuto skutečnost upozorněna a nemusí tuto poruchu čekat. V případě, že si této poruchy posádka všimne až když začne v kritické fázi letu ovládat výšková kormidla a posilovač, může být už pozdě. Tento stejný princip je aplikován i v níže uvedené tabulce Tab. 3.3.

Tab. 3.3: Výstup z analýzy (CFC-2.2)

CFC-2.2	Posádka musí být informována bezprostředně poté, co došlo ke ztrátě dodávky el. energie na Master Tabla. [Scénář 2.1.3; 2.2.3; 3.2.3; 4.2.3; 4.3.3]

Tab. 3.4: Výstup z analýzy (CFC-3.2)

CFC-3.2	Dojde-li k výpadku el. energie, musí si posádka zkontrolovat funkčnost žárovek na Master Tablu, neboť výpadek dodávky el. energie do určité komponenty nemusí znamenat poruchu celého el. systému. [Scénář 3.3.3]

Výpadek dodávky elektrické energie do určité komponenty (např. MFD) nemusí nutně znamenat poruchu celého elektrického systému. Z toho důvodu je dobré si zkontrolovat, zdali fungují žárovky na Master Tablu; v případě, že fungují a není indikována porucha generátorů, baterie nebo posilovače řízení (jednotky PCA), může posádka nadále ovládat výšková kormidla se zapnutou jednotkou PCA. Nebudou-li nadále svítit kontrolky na Master Tablu, může za tím být porucha celého el. systému nebo těchto kontrolek. V tomto případě je pak vhodné odpojit jednotku PCA od systému podélného řízení.

Tab. 3.5: Výstup z analýzy (CFC-5.4)

CFC-5.4	Trimovací spínač musí být dostatečně ergonomicky navržen, aby posádka dokázala udržet trimovací spínač ve vychýlené poloze dostatečně dlouho. [Scénář 5.4.1]

I tento poměrně triviální požadavek (CFC-5.4) může mít velký vliv na chování letounu a jeho bezpečnost v kritických fázích letu. Bude-li trimovací spínač na HOTAS páce z ergonomického hlediska špatně navržen, může nastat situace, kdy pilot v kritických chvílích dostane křeč do rukou a nebude nadále schopen ovládat výšková kormidla svou dominantní rukou. Z dlouhodobého hlediska může hrozit pilotům karpální tunel.

Tab. 3.6: Výstup z analýzy (CFC-5.5)

CFC-5.5	Posádka musí být poučena, že při nefunkční nebo vypnuté ECU jednotce není možné nadále ovládat trimovací plošku. [Scénář 6.3.1]

V režimu 2 jednotky PCA je trimovací ploška na výškovým kormidle ovládána automaticky pomocí řídící jednotky zvané ECU (Electronic Control Unit), která mimo jiné ovládá i posilovač řízení (jednotku PCA). V případě, že nastane porucha v jednotce PCA, může posádka vypnout přívod el. energie do řídící jednotky ECU, což způsobí, že trimovací plošku už nebude ovládat žádný systém, včetně posádky. Z toho důvodu je důležité, aby posádka po vypnutí řídící jednotky ECU nadále neovládala trimovací spínač, a místo toho se soustředila na vyvozování větší síly při vychylování výškových kormidel.

Tab. 3.7: Výstup z analýzy (CFC-7.13)

CFC-7.13	Jednotka ECU nesmí přerušit ovládání trimovací plošky poté, co posádka stiskla Paddle switch.

Požadavek CFC-7.13 se rovněž týká pouze režimu 2 jednotky PCA, kdy trimovací ploška je ovládána automaticky pomocí řídící jednotky ECU. Na HOTAS páce se nachází tzv. Paddle switch, který má za úkol odpojení posilovače od systému podélného řízení. To se využívá hlavně při poruše v posilovači, nebo když posádka chce ovládat výšková kormidla vlastní silou. Aby posádka i poté mohla nadále ovládat trimovací plošku, nesmí se řídící jednotka ECU odpojit od aktuátoru trimovací plošky, což je vyjádřeno ve výše uvedeném požadavku CFC-7.13.

Tab. 3.8: Výstup z analýzy (CPC-4.1)

CPC-4.1	Aktuátor trimovací plošky musí být spojen se správnou polaritou k el. obvodu. [Scénář 5.1; 7.1]

Na první pohled velmi triviální požadavek (CPC-4.1), avšak v provozu je to kritický parametr. Propojení aktuátoru s opačnou polaritou může posádce výrazně znepříjemnit řízení a při kritických manévrech vést i k nebezpečím.

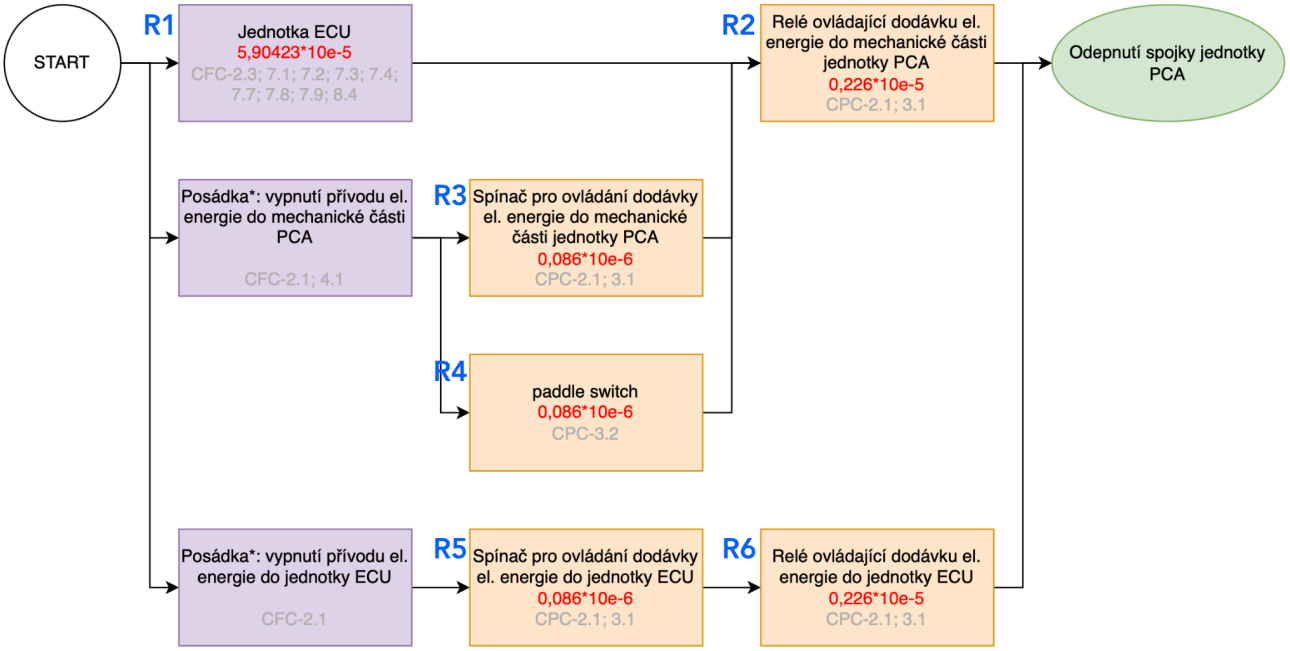
Po vypracování této analýzy mohu z vlastních zkušeností říci, že je metoda STPA opravdu velmi účinná metoda, která narozdíl od tradičních metod, jako jsou FTA nebo FMEA, dokáže zahrnovat i lidský faktor. Lidský faktor je nezbytná věc, kterou návrháři systému nesmí nikdy opomenout, neboť v nebezpečných situací může hrát zásadní roli.

Pokud mám z vlastních zkušeností porovnat metodu STPA s metodami FTA, FMEA a FHA, tak kromě situací zahrnující lidský faktor jsem nenašel jiné situace, které by tradiční analytické metody nedokázaly najít oproti metodě STPA. A to i navzdory tomu, že se o metodě STPA tvrdí, že dokáže předpovědět více situací než tradiční metody. Hlavním důvodem bude fakt, že mnou analyzovaný systém je spíše hardwarového charakteru než softwarového (procentuální pokrytí jednotlivých metod je zobrazeno v tab. 1.2. v kapitole 1.4).

VÝSLEDKY SPOLEHLIVOSTNÍ ANALÝZY

Součástí praktické části mé bakalářské práce jsou i RBD diagramy, které mají za cíl analyzovat spolehlivost systému, neboť metoda STPA je určena primárně pro analyzování bezpečnosti systému, nikoliv spolehlivost. Tyto RBD diagramy jsem popsal v kapitole 2.1.4 a její postup je popsán v kapitole 2.4.1.

Celkem jsem vytvořil šest RBD diagramů, kdy pro každý diagram jsem vypočítal i výslednou pravděpodobnost[1]. Pro představu jsem níže uvedl jeden z mých RBD diagramů, kde je zobrazen i obecný postup výpočtu. Díky jednoduchosti těchto diagramů stačilo vypočítat pravděpodobnosti pomocí jednoduchých vzorců pro sériové a paralelní zapojení.



Obr. 3.1: Příklad RBD diagramu (diagram 6)

Tab. 3.9: Postup výpočtu výsledné spolehlivosti (diagram 6)

veličina	vzorec výpočtu	výsledek	pozn.
R34	1-P3*P4	0,999999999999993	hodnota P značí pravděpodobnost výskytu poruchy (P = 1 - R)
R134	1-[(1-R34)*P1]	1	spolehlivost R134 se limitně blíží k hodnotě 1, proto Excel jej zobrazuje jako hodnotu 1
R1234	R134*R2	0,99999774	
R56	R5*R6	0,999997654000194	
R123456	1-[(1-R56)*(1-R1234)]	0,999999999994698	

Tab. 3.10: Výsledná spolehlivost a pravděpodobnost poruchy (diagram 6)

	Spolehlivost:	Pravděpodobnost poruchy
Odpojení spojky jednotky PCA	0,999999999994698	5,302E-12

[1] Pro jednoduchost jsem při počítání pravděpodobností nebral lidský činitel v potaz.

LIMITACE A VÝZVY

Navzdory svým velkým přednostem, které jsem popisoval výše, přináší metoda STPA i určité limitace, se kterými je nutno při její implementaci počítat. Níže jsem uvedl její limitace (tyto limitace vychází z mých vlastních zkušeností, nikoliv odborné literatury, jak je tomu v kapitole 1.4).

Každá STPA analýza může obsahovat rozdílné výstupy, i když se bude jednat o ten samý systém, neboť tyto výstupy subjektivitě posuzuje analytik. Kromě toho vysoce spoléhá i na jeho znalosti systému a jeho zkušenosti s touto metodou, což všechno výrazně ovlivní výslednou kvalitu analýzy.

Další výzvou, se kterou se organizace mohou setkat, je její složitá integrace. Větší organizace, jako jsou Boeing, Airbus, Embraer a nebo i Aero Vodochody, zpravidla mívají týmy zaměřující se na bezpečnost a spolehlivost, které úzce spolupracují s ostatními odděleními. Narozdíl od jiných metod využívá metoda STPA jiné formáty dat a informací, proto její implementace vyžaduje přesnou koordinaci mezi jednotlivými týmy.

V neposlední řadě je nutno počítat s tím, že i když je metoda STPA přesnější a detailnější, tak se kromě toho vyznačuje i svou časovou náročností a vysokou pracností, obzvláště u čtvrtého kroku (scénáře). To vyžaduje vysokou koncentraci analytika, což tvoří metodu STPA jako jednu z nejnáročnějších a nejpracnějších analytických metod.

POROVNÁNÍ VÝSLEDKŮ S VĚDECKOU LITERATUROU

Ve všech výše zmíněných vědeckých literaturách se autoři snaží aplikovat analytickou metodu STPA na určitý systém a popisují její přednosti před tradičními analytickými metodami. Většina z nich dokázala tyto přednosti v analýze najít, což jsem bohužel u mé analýzy nedokázal, neboť tito autoři prováděli analýzu na komplexní systémy, kde hrál software v systému velkou roli, jako jsou brzdící systém autonomních vozidel nebo jaderné reaktory, zatímco má analýza byla provedena na systém spíše hardwarového charakteru.

INTEGRACE METODY STPA V AERO VODOCHODY

V současné době se v Aeru využívají stále tradiční analytické metody, konkrétně FTA, FMEA, FHA a podobně. Touto STPA analýzou na systém podélného řízení a jednotku PCA jsem se snažil zjistit, jaké přínosy (případně limitace) může implementace metody STPA v Aeru přinést a případně zdali se může vyplatit.

Pro posouzení, zdali se vyplatí integrace metody STPA do organizace, jako je Aero Vodochody, je potřeba vyhodnotit, jaké přínosy a limitace může toto rozhodnutí přinést. Jak už jsem psal výše, má STPA analýza nenalezla žádné jiné situace, které by tradiční metoda FTA nedokázala najít (nezahrnuji-li lidský faktor), neboť mnou analyzovaný systém je spíše hardwarového charakteru. Výsledky mé STPA analýzy byly tudíž téměř stejné jako výsledky FTA analýzy, kterou měli ve Vodochodech také zpracovanou. Dále její integrace vyžaduje přesnou koordinaci mezi jednotlivými týmy a změny v organizační struktuře, a to všechno vyžaduje spoustu času, což může v současné době představovat velký problém z následujících důvodů:

- nedostatek zaměstnanců v daných odděleních,

- relativně vysoká vytíženost současných zaměstnanců nedovoluje tento časově náročný proces uskutečnit a
- neochota současných zaměstnanců přistupovat k takto velkým změnám v organizaci.

Když vezmeme ještě v potaz, že drtivá většina systémů vyvíjených ve Vodochodech jsou spíše hardwarového charakteru, vyjde nám, že implementace metody STPA se v současné chvíli ve Vodochodech skutečně nevyplatí.

NÁVRHY PRO BUDOUCÍ VÝVOJ

Jak už jsem psal, metoda STPA posuzuje systém pouze z kvalitativního pohledu, nikoliv kvantitativního. To výrazně ztěžuje práci analytikům při procesu certifikace, neboť úřad může požadovat dodatečné analýzy, které posoudí systém i z kvantitativní stránky.

Jednou z možností je zkombinovat STPA analýzu s RBD diagramy, které posuzují systém z kvantitativního pohledu a mohou se využít pro analyzování systémové spolehlivosti (metoda STPA je primárně určena pro analyzování systémové bezpečnosti, nikoliv spolehlivosti). Postup, jak jsem podle své STPA analýzy vytvořil RBD diagramy je uveden v kapitole 2.4.1. V současné době neexistuje žádná příručka, pomocí které by se daly vytvářet RBD diagramy podle STPA analýz, z toho důvodu může můj popisovaný postup obsahovat určité limitace.

Vytvořením univerzální příručky pro vytváření RBD diagramů podle STPA analýzy by mohlo vyřešit tuto Achillovu patu metody STPA. Tím, že se standardizuje zkombinování metody STPA s RBD diagramy, můžeme využívat tyto dvě analytické metody k certifikaci letadel a letadlových celků, aniž bychom potřebovali další analýzy. Tím by se mohl výrazně zjednodušit a zrychlit proces analyzování, díky čemuž se zkrátí i doba certifikace.

Dle mého osobního názoru se metoda STPA a RBD diagramy vzájemně doplňují, což jsem se snažil zobrazit do níže uvedené tabulky tab. 3.11:

Tab. 3.11: Pokrytí analytických metod v různých oblastech

	STPA	RBD	FTA & FMEA
Lidský faktor	🟢	🟠	🟠
Kvantitativní	🔴	🟢	🟢
Kvalitativní	🟢	🔴	🟢
Software	🟢	🟠	🟠
Hardware	🟢	🟢	🟢
Legenda:	🟢 velmi dobré pokrytí	🟠 omezené pokrytí	🔴 špatné pokrytí

Závěr

Hlavním cílem mé bakalářské práce bylo provést bezpečností analýzu metodou STPA v rámci vývoje a výroby vojenských letounů a stanovit vstupy pro zajištění potřebné spolehlivosti. Tato analýza byla provedena na systém letounu Aero L-39 NG, konkrétně systém podélného řízení a posilovač, neboli jednotku PCA. Z mé STPA analýzy jsem poté identifikoval bezpečnostní požadavky a pro stanovení vstupů pro zajištění potřebné spolehlivosti jsem využil metodu RBD, kterou jsem hned navázal na mou STPA analýzu.

STPA je relativně nová analytická metoda, která má částečně nebo úplně eliminovat limitace tradičních analytických metod, jako jsou FTA, FMEA nebo FHA. Těmito limitacemi jsou například neúplné zahrnutí lidského faktoru, nepřehlednost analýz u komplexních systémů, neuvažování selhání více komponentů nebo i špatná přizpůsobitelnost současným technologiím. Má samotná STPA analýza se skládala ze čtyř hlavních kroků, ze kterých jsem pak odvozoval finální požadavky a omezení na systém. Tyto požadavky a omezení na systém slouží pak jako kontrolní seznam (checklist) pro další oddělení podílející se na vývoji jednotky PCA.

Pomocí této analýzy jsem dokázal osobně poznat přínosy metody STPA, neboť o metodě STPA se hodně píše, že dokáže vyřešit mnoho limitací tradičních analytických metod, o kterých jsem psal již výše. Kromě toho mi pomohla zjistit, jestli se její implementace ve Vodochodech může vyplatit, což se nakonec ukázalo, že se nevyplatí. Navzdory jejím přednostem nemusí mít pro firmu takový přínos, jelikož i její implementace může představovat značné komplikace pro jednotlivá oddělení.

Ačkoliv se o metodě STPA tvrdí, že dokáže předpovědět více situací než tradiční metody, tak má analýza nedokázala identifikovat více požadavků než tradiční metoda FTA (nepočítám-li situace zahrnující lidský faktor). Je to způsobeno hlavně tím, že mnou analyzovaný systém je spíše hardwarového charakteru než softwarového. To je jedním z důvodů, proč se dle mého názoru implementace metody STPA ve společnosti Aero Vodochody Aerospace nevyplatí, neboť drtivá většina systémů vyvíjených ve Vodochodech jsou hlavně hardwarového, než softwarového, charakteru. V neposlední řadě představuje implementace metody STPA časově náročný proces, který může znamenat dodatečné náklady pro společnost.

Jednou z největších limitací pro metodu STPA je její pracnost a časová náročnost. Jak jsem psal výše, metoda STPA vyžaduje vysokou koncentraci analytika v jednotlivých krocích, což ji činí jako jednu z nejnáročnějších a nejpracnějších analytických metod. Kromě toho metoda STPA posuzuje bezpečnost systému pouze z kvalitativního, nikoliv kvantitativního pohledu, z toho důvodu je pro proces certifikace nutno zkombinovat metodu STPA ještě s další metodou, která ještě posoudí i spolehlivost systému z kvantitativního pohledu. V mém případě jsem ji propojil s metodou RBD, což může být jedním z řešení této problematiky. V kapitole 2.4.1 jsem se pokusil o vytvoření krátkého manuálu pro tvoření RBD diagramů podle STPA analýzy, avšak kvůli nedostatku času jsem už nestihl udělat podrobnější průzkum na tuto problematiku, která by pomohla vyřešit tuto Achillovu patu metody STPA. Tím, že se standardizuje zkombinování metody

STPA s RBD diagramy, můžeme využívat tyto dvě analytické metody k certifikaci letadel a letadlových celků, aniž bychom potřebovali další analýzy, neboť jak jsem psal v předešlé kapitole, metody STPA a RBD se vzájemně doplňují. Tím by se mohl výrazně zjednodušit a zrychlit proces analyzování, díky čemuž se zkrátí i doba certifikace.

Seznam použité literatury

[1] HESSING, Ted. Fault Tree Analysis. Sigma Study Guide [online]. [cit. 2023-06-30]. Dostupné z: https://sixsigmastudyguide.com/fault-tree-analysis/#

[2] INFRASPEAK TEAM. FTA vs FMEA: What Are The Differences?. Infraspeak: Infraspeak Blog [online]. 23.10.2020 [cit. 2023-06-30]. Dostupné z: https://blog.infraspeak.com/fta-vs-fmea/

[3] Přispěvatelé Wikipedie, FMEA [online], Wikipedie: Otevřená encyklopedie, c2022, Datum poslední revize 20. 05. 2022, 09:30 UTC, [citováno 3. 07. 2023] <https://cs.wikipedia.org/w/index.php?title=FMEA&oldid=21295315>

[4] KRITZINGER, Duane. Functional Hazard Analysis. Science Direct [online]. 2017 [cit. 2023-07-03]. Dostupné z: https://www.sciencedirect.com/topics/engineering/functional-hazard-analysis#:~:text=The%20FHA%20looks%20at%20what,2.&text=The%20FMEA%20looks%20at%20what,system%20fails%20in%20various%20ways.

[5] FA MENDELU. Specific Methods of Quality Control: Fault tree analysis (FTA). Inovace studijních programů AF MENDELU směrem k internacionalizaci studia [online]. Brno: Mendelova Univerzita v Brně, 4.7.2023 [cit. 2023-07-03]. Dostupné z: https://web2.mendelu.cz/af_291_projekty2/vseo/print.php?page=7425&typ=html

[6] LEVESON, Nancy G. a John P. THOMAS. STPA Handbook [online]. Massachusetts, USA, 2018 [cit. 2023-07-06]. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Massachusets Institute of Technology.

[7] DUAN, Jianyu. Improved Systemic Hazard Analysis Integrating With Systems Engineering Approach for Vehicle Autonomous Emergency Braking System [online]. Peking, ČLR, 2022 [cit. 2023-07-06]. ISSN 23329017. Dostupné z: https://asmedigitalcollection.asme.org/risk/article/8/3/031101/1114604/Improved-Systemic-Hazard-Analysis-Integrating-With. Výzkumný článek. School of Transportation Science and Engineering, Beihang University, Beijing 100191, China.

[8] LIU, Hua, Zhaohui LIU, Xiaohua YANG, Shiyu YAN a Zhi CHEN. The Safety Analysis of Multiple Method Fusion on Reactor Scram Subsystem [online]. Heng Yang, ČLR, 2018 [cit. 2023-07-06]. ISBN 978-079185149-4. Dostupné z: https://asmedigitalcollection.asme.org/ICONE/proceedings/ICONE26/51494/V06BT08A059/272841. Vědecký článek. University of South China, Heng Yang.

[9] CHOPART, Max a Andrej LALIŠ. System-Theoretic Process Analysis for reliability assessment: Aircraft's wheel braking system case study [online]. Praha, 2022 [cit. 2023-07-06]. ISBN 23521457. Výzkumný článek. Fakulta dopravní, České Vysoké Učení Technické v Praze.

[10] KÖLLN, Greta, Michael KLICKER, Tobias SCHMIDT a Stephan SCHMIDT. System Theoretic Process Analysis for a Vehicle SAE Level four [online]. Mnichov a Magdeburg, SRN, 2020 [cit. 2023-07-21]. ISBN 978-981148593-0. Dostupné z: http://rpsonline.com.sg/proceedings/9789811485930/html/5700.xml. Výzkumný článek. Otto von Guericke University Magdeburg, Institute for Mobile Systems; BMW Group.

[11] BAUMGART, Stephan, Froberg JOAKIM a Punnekkat SASIKUMAR. Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site [online]. Vasteras, Švédsko, 2018 [cit. 2023-07-21]. ISBN 978-153864446-1. Dostupné z: https://ieeexplore.ieee.org/document/8544433. Výzkumný článek. School of Innovation, Malardalen University, Design and Engineering, Vasteras, Sweden; Research Institutes of Sweden, RISE ICT/SICS, Vasteras, Sweden.

[12] ASIM, Abdulkhaleq a Stefan WAGNER. A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software [online]. Stuttgart, Německo, 2015 [cit. 2023-07-21]. ISBN 978-145033350-4. Dostupné z: https://dl.acm.org/doi/10.1145/2745802.2745817. Výzkumný článek. Institute of Software Technology, University of Stuttgart, Universitätsstraße 38, Stuttgart, 70569, Germany.

Seznam použitých obrázků, tabulek a příloh

Seznam použitých obrázků

Seznam použitých tabulek

Přílohy

Příloha 1: STPA analýza na podélné řízení a jednotku PCA

Krok 1: Definujte účel analýzy

A) IDENTIFIKACE ZTRÁT

L-1: Ztráty na životech či zranění
L-2: Ztráty nebo poškození na letadle a systému podélného řízení
L-3: Ztráty nebo poškození na předmětech mimo letoun
L-4: Ztráta účelu (letového plánu)
L-5: Ztráta zákaznické spokojenosti
L-6: Ztráty na životním prostředí a jeho ničení
L-7: Ztráta reputace výrobce

B) IDENTIFIKACE SYSTÉMOVÝCH HAZARDŮ

H-1: Systém podélného řízení nevychyluje výšková kormidla v požadované úrovni. [L-1-7]
H-2: Systém podélného řízení nebo PCA vychylují výšková kormidla bez vstupu pilota. [L-1-7]

C) IDENTIFIKACE SYSTÉMOVÝCH OMEZENÍ

H-1: Systém podélného řízení nevychyluje výšková kormidla v požadovaném směru.
SC-1: Systém podélného řízení musí vychylovat výšková kormidla v požadovaném směru.
H-2: Systém podélného řízení nebo PCA vychylují výšková kormidla bez vstupu pilota.
SC-2: Systém podélného řízení nebo PCA nesmí vychylovat výšková kormidla bez vstupu pilota.

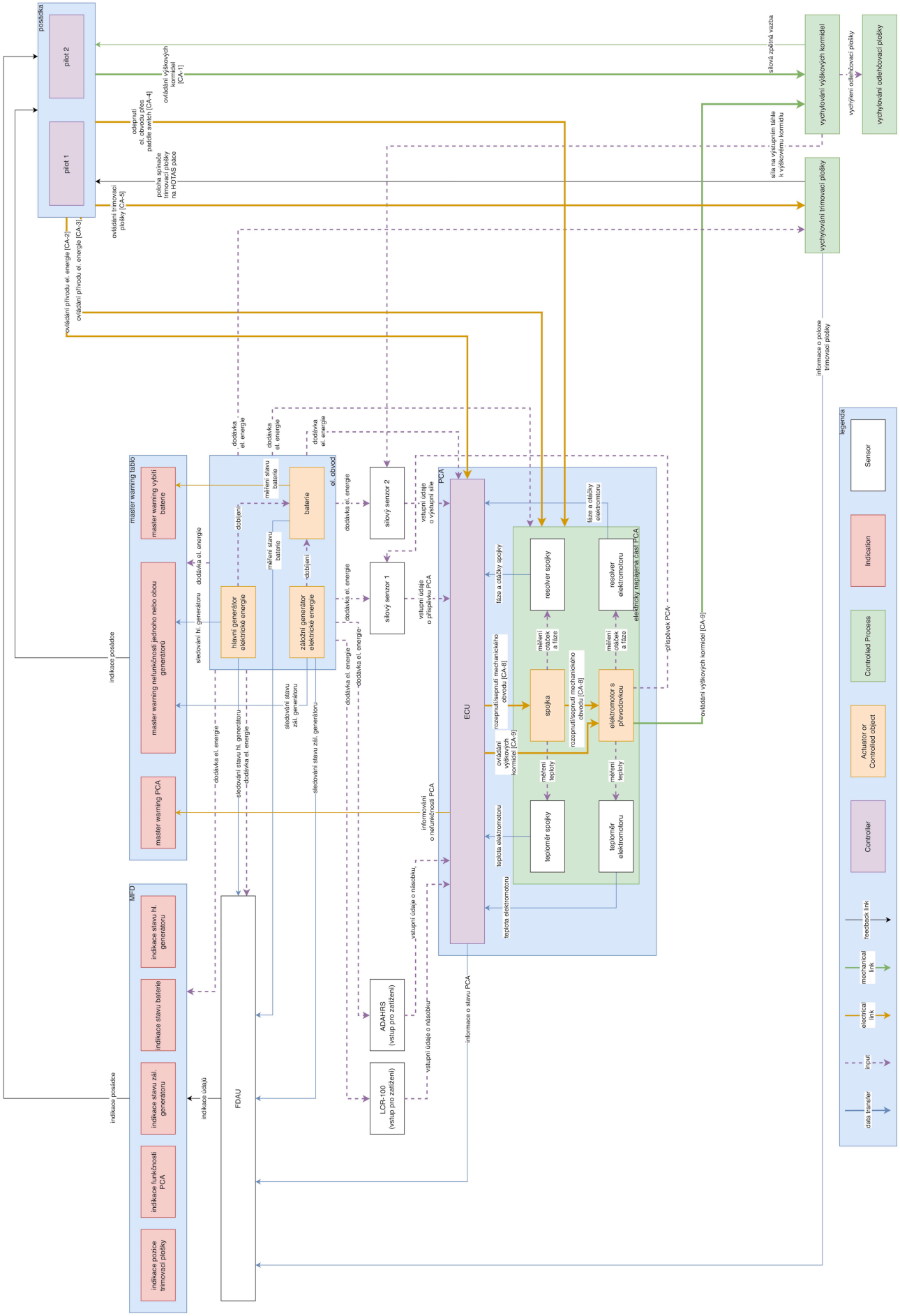
D) ROZBOR HAZARDŮ (VOLITELNÉ)

H-1: Systém podélného řízení nebo PCA nevychyluje ve správném okamžiku výšková kormidla v požadované úrovni.
H-1.1: Jednotka PCA klade odpor vůči pilotovým vstupům.
H-1.2: Trimovací ploška se vychyluje v opačném směru.
H-2: Systém podélného řízení nebo PCA vychylují výšková kormidla bez vstupu pilota.
H-2.1: Systém podélného řízení nebo PCA nekontrolovatelně kmitají s výškovými kormidly.

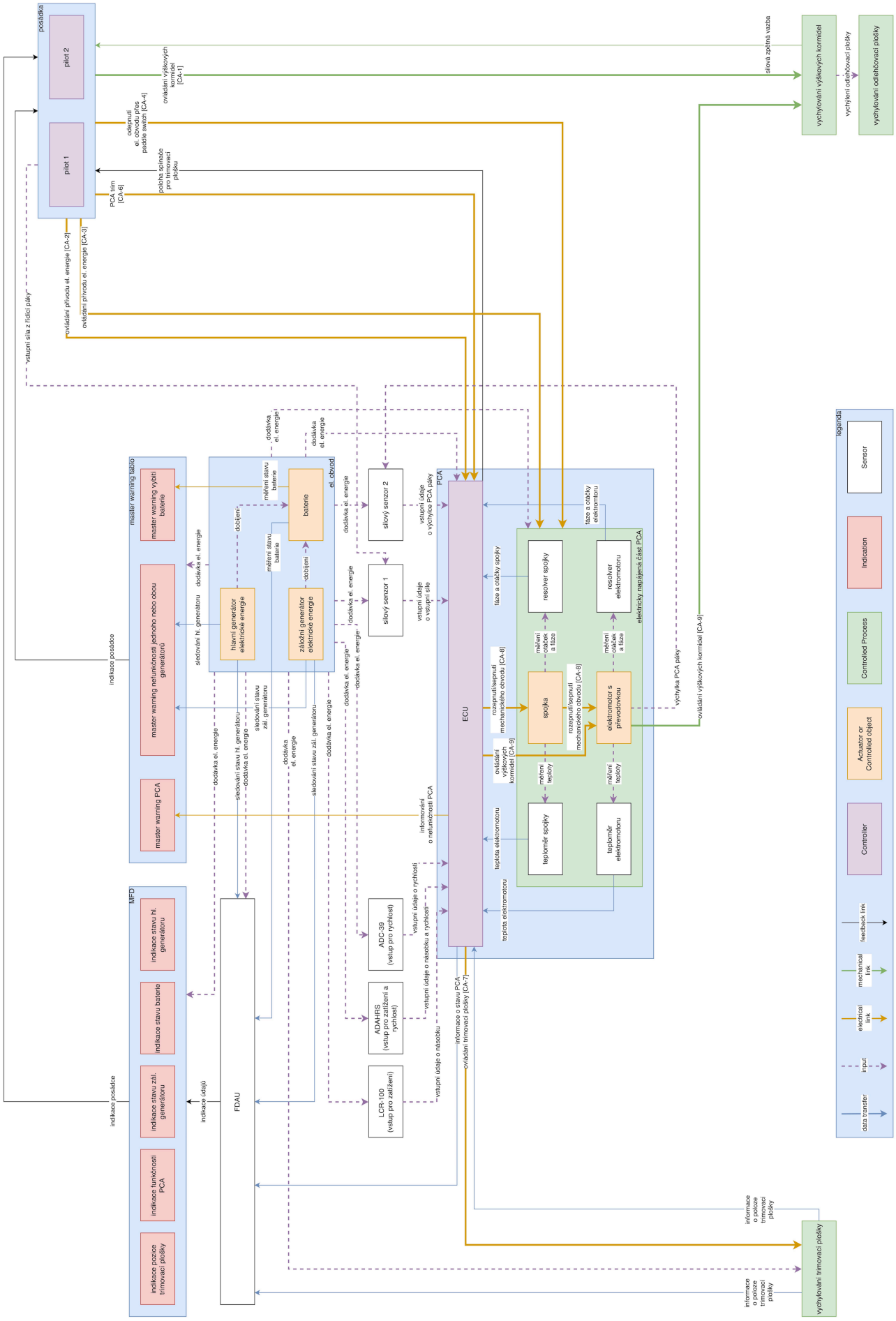
Vážnost:

Katastrofická
Kritická
Mezní
Zanedbatelná

Krok 2: Vytvoření modelu (režim 1)



Krok 2: Vytvoření modelu (režim 2)



Krok 3: Identifikace UCA (Unsafe Control Actions)

UCA se skládá z následujících pěti částí:

<zdroj>	<typ>	<control action>	<kontext>	<odkaz na hazardy>
Systém	aplikuje	brždění	při vzletu.	[H-x.x]

Control Action	Aplikování vede k hazardu	Neaplikování vede k hazardu	Příliš brzo či pozdě, mimo provoz	Zastaveno příliš brzo nebo příliš dlouho aplikováno
[CA-1]: ovládání výškových kormidel	[UCA-1.1]: Posádka ovládá výšková kormidla v jiné, než požadované úrovni nebo směru. [H-1]	[UCA-1.2]: Posádka neovládá výšková kormidla v požadovaném směru. [H-1]	[UCA-1.3]: Posádka začala ovládat výšková kormidla v požadovaném směru příliš pozdě. [H-1]	[UCA-1.4]: Posádka přestala ovládat výšková kormidla v požadovaném směru příliš brzy. [H-1]
[CA-2]: ovládání přívodu el. energie (pro ECU)	N/A	[UCA-2.1]: Posádka nevypnula přívod el. energie do jednotky ECU při poruše jednotky PCA. [H-1; H-2]	[UCA-2.2]: Posádka vypnula přívod el. energie do jednotky ECU příliš pozdě při poruše jednotky PCA. [H-1; H-2]	N/A
[CA-3]: ovládání přívodu el. energie (pro mechanickou část PCA)	[UCA-3.1]: Posádka zapnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA. [H-1; H-2]	[UCA-3.2]: Posádka nevypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA (při poruše paddle switche). [H-1; H-2]	[UCA-3.3]: Posádka vypnula přívod el. energie pro mechanickou část PCA příliš pozdě při poruše jednotky PCA. [H-1; H-2]	N/A
[CA-4]: sepnutí/odepnutí el. obvodu přes paddle switch	[UCA-4.1]: Posádka odepnula el. obvod mechanické části PCA při funkční jednotce PCA v kritické fázi letu. [H-1]	[UCA-4.2]: Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA. [H-1.1; H-2]	[UCA-4.3]: Posádka odepnula el. obvod mechanické části PCA příliš pozdě při poruše jednotky PCA. [H-1.1; H-2]	N/A
[CA-5]: ovládání trimovací plošky (Mode 1)	[UCA-5.1]: Posádka ovládá trimovací plošku v jiném, než požadovaném směru. [H-1]	[UCA-5.2]: Posádka neovládá trimovací plošku při velkých silách v řízení. [H-1.1]	[UCA-5.3]: Posádka začala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš pozdě. [H-1.1]	[UCA-5.4]: Posádka přestala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš brzy. [H-1.1]

Přílohy

Control Action	Aplikování vede k hazardu	Neaplikování vede k hazardu	Příliš brzo či pozdě, mimo provoz	Zastaveno příliš brzo nebo příliš dlouho aplikováno
[CA-6]: PCA trim (Mode 2)	[UCA-6.1]: Posádka ovládá trimovací spínač v opačném, než požadovaném, směru. [H-1.1; H-1.2]	N/A	N/A	[UCA-6.2]: Posádka ovládá trimovací spínač příliš dlouho i poté, co přestala vychylovat výšková kormidla. [H-2]
	[UCA-6.3]: Posádka ovládá trimovací spínač při vypnuté nebo nefunkční ECU jednotce. [H-1]			
[CA-7]: ovládání trimovací plošky (Mode 2)	[UCA-7.1]: Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru. [H-1; H-1.2; H-2; H-2.1]	[UCA-7.3]: Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení po delší dobu. [H-2.1]	[UCA-7.4]: Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení. [H-2.1]	[UCA-7.5]: Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení. [H-2.1]
	[UCA-7.2]: Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla. [H-1; H-1.2; H-2]			[UCA-7.6]: Jednotka ECU vychyluje trimovací plošku příliš dlouho i poté, co se přestala vychylovat výšková kormidla. [H-1; H-2]
[CA-8]: rozepnutí/sepnutí mechanického obvodu	[UCA-8.1]: Jednotka ECU sepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	[UCA-8.2]: Jednotka ECU neodepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	[UCA-8.3]: Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA. [H-1]	N/A
[CA-9]: ovládání výškových kormidel	[UCA-9.1]: Jednotka ECU ovládá výšková kormidla v opačném, než požadovaném, směru nebo příliš pomalu. [H-1]	[UCA-9.3]: Jednotka ECU neovládá výšková kormidla při sepnuté spojce. [H-1; H-1.1]	[UCA-9.4]: Jednotka ECU začala ovládat výšková kormidla příliš pozdě v kritické fázi letu. [H-1; H-1.1]	[UCA-9.5]: Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu. [H-1]
	[UCA-9.2]: Jednotka ECU vychyluje výšková kormidla bez vstupu od posádky. [H-2]			

Krok 4: Identifikace ztrátových scénářů

A) IDENTIFIKACE SCÉNÁŘŮ VEDOUCÍCH K UCA (UNSAFE CONTROL ACTION):

Jsou zde obecně 4 důvody, které mohou vést k UCA:

- Chyby zahrnující řídící člen (Controller, pouze pro fyzické řídící členy)
- Neadekvátní řídící algoritmus
- Nebezpečný vstup od jiného řídícího členu (Controller)
- Neadekvátní procesový model
  - Řídící člen získá chybnou zpětnou vazbu (informaci)
  - Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje
  - Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)
  - Potřebná zpětná vazba neexistuje

[UCA-1.1]: Posádka vychyluje výšková kormidla v jiné, než požadované úrovni nebo směru. [H-1]	
Scénář 1.1.1 pro UCA-1.1 Chyby zahrnující řídící člen	Posádka vychyluje výšková kormidla v jiné, než požadované, úrovni z důvodu zaneprázdnění, rozptýlení…
Scénář 1.1.2 pro UCA-1.1 Neadekvátní řídící algoritmus	Posádka vychyluje výšková kormidla v jiné, než požadované, úrovni z důvodu nedohodnutého zakročení druhého pilota do řízení.
Scénář 1.1.3 pro UCA-1.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Posádka vychyluje výšková kormidla v jiné, než požadované, úrovni, neboť dostává neadekvátní silovou zpětnou vazbu v řízení.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že v systému není žádná porucha.
Co mohlo toto způsobit	- praskl pružinový posilovač - jednotka PCA v každém směru dodává jiný výkon - páky v cestě podélného řízení mají špatný převod
[UCA-1.2]: Posádka nevychyluje výšková kormidla v požadovaném směru. [H-1]	
Scénář 1.2.1 pro UCA-1.2 Chyby zahrnující řídící člen	Posádka nevychyluje výšková kormidla v požadovaném směru z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 1.2.2 pro UCA-1.2 Neadekvátní řídící algoritmus	Posádka nevychyluje výšková kormidla v požadovaném směru, jelikož je posádka v domění, že druhý pilot ta výšková kormidla ovládá.
[UCA-1.3]: Posádka vychýlila výšková kormidla v požadovaném směru příliš pozdě. [H-1]	
Scénář 1.3.1 pro UCA-1.3 Chyby zahrnující řídící člen	Posádka vychýlila výšková kormidla v požadovaném směru příliš pozdě z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…

Scénář 1.3.2 pro UCA-1.3 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka vychýlila výšková kormidla v požadovaném směru příliš pozdě, neboť si posádka příliš pozdě všimla, že výšková kormidla nikdo neovládá.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že výšková kormidla ovládá druhý pilot.
Co mohlo toto způsobit	- špatná komunikace mezi posádkou - zaneprázdnění posádky - nejednoznačně rozdělené role (pilot flying/monitoring)
Scénář 1.3.3 pro UCA-1.3 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka vychýlila výšková kormidla v požadovaném směru příliš pozdě, neboť nedostala indikaci o nefunkčnosti jednotky PCA a musela působit proti silám vyvolané jednotkou PCA.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že v systému není žádná porucha.
Co mohlo toto způsobit	- selhání elektrického obvodu (generátory, baterie), kdy nemohl dodávat el. energii indikačním zařízením a jednotce PCA - přívod el. energie k jednotce PCA nebyl zapnut nebo byl vypnut (např. nechtěnou manipulací pilota…)
[UCA-1.4]: Posádka přestala ovládat výšková kormidla v požadovaném směru příliš brzy. [H-1]	
Scénář 1.4.1 pro UCA-1.4 Chyby zahrnující řídící člen	Posádka přestala ovládat výšková kormidla v požadovaném směru příliš brzy z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 1.4.2 pro UCA-1.4 Neadekvátní řídící algoritmus	Posádka přestali ovládat výšková kormidla v požadovaném směru příliš brzy, neboť se špatně domnívá, že kontrolu převzal druhý pilot.

[UCA-2.1]: Posádka nevypnula přívod el. energie do jednotky ECU při poruše jednotky PCA. [H-1; H-2]	
Scénář 2.1.1 pro UCA-2.1 Chyby zahrnující řídící člen	Posádka nevypnula přívod el. energie do jednotky ECU při poruše jednotky PCA z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 2.1.2 pro UCA-2.1 Neadekvátní řídící algoritmus	Posádka nevypnula přívod el. energie do jednotky ECU při poruše jednotky PCA, neboť se domnívá, že tuto akci provedl druhý pilot.
Scénář 2.1.3 pro UCA-2.1 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka nevypnula přívod el. energie do jednotky ECU při poruše jednotky PCA, neboť nedostala indikaci o poruše jednotky PCA.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA
[UCA-2.2]: Posádka vypnula přívod el. energie do jednotky ECU příliš pozdě při poruše jednotky PCA. [H-1; H-2]	
Scénář 2.2.1 pro UCA-2.2 Chyby zahrnující řídící člen	Posádka vypnula přívod el. energie do jednotky ECU při poruše jednotky PCA příliš pozdě z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 2.2.2 pro UCA-2.2 Neadekvátní řídící algoritmus	Posádka vypnula přívod el. energie do jednotky ECU při poruše jednotky PCA příliš pozdě, neboť očekávali, že akci provede druhý pilot.
Scénář 2.2.3 pro UCA-2.2 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka vypnula přívod el. energie do jednotky ECU při poruše jednotky PCA příliš pozdě, neboť pilotům nedošla indikace poruchy jednotky PCA. Nestandartní chování jednotky PCA zjistila posádka až po vychylování výškových kormidel.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA

[UCA-3.1]: Posádka zapnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA. [H-1; H-2]	
Scénář 3.1.1 pro UCA-3.1 Chyby zahrnující řídící člen	Posádka zapnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA z důvodu nechtěné manipulace.
Scénář 3.1.2 pro UCA-3.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Posádka na zemi zapnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA, jelikož nedostala indikaci o nefunkčnosti jednotky PCA po sepnutí el. obvodu jednotky ECU.
Doměnka řídícího členu, která vede k UCA	Posádka se domnívá, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA - posádka neotestovala funkčnosti žárovek pro master tabla
[UCA-3.2]: Posádka nevypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA. [H-1; H-2]	
Scénář 3.2.1 pro UCA-3.2 Chyby zahrnující řídící člen	Posádka nevypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 3.2.2 pro UCA-3.2 Neadekvátní řídící algoritmus	Posádka nevypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA, neboť se domnívá, že tuto akci provedl druhý pilot.
Scénář 3.2.3 pro UCA-2.1 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka nevypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA, neboť nedostala indikaci o poruše jednotky PCA.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA
[UCA-3.3]: Posádka vypnula přívod el. energie pro mechanickou část PCA příliš pozdě při poruše jednotky PCA. [H-1; H-2]	
Scénář 3.3.1 pro UCA-3.3 Chyby zahrnující řídící člen	Posádka vypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA příliš pozdě z důvodu zaneprázdnění, rozptýlení, nepřítomnosti…
Scénář 3.3.2 pro UCA-3.3 Neadekvátní řídící algoritmus	Posádka vypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA příliš pozdě, neboť očekávali, že akci provede druhý pilot (ať už přes spínač nebo paddle switch).

Scénář 3.3.3 pro UCA-3.3 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka vypnula přívod el. energie pro mechanickou část PCA při poruše jednotky PCA příliš pozdě, neboť pilotům nedošla indikace poruchy jednotky PCA. Nestandartní chování jednotky PCA zjistila posádka až po vychylování výškových kormidel.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA

[UCA-4.1]: Posádka odepnula el. obvod mechanické části PCA při funkční jednotce PCA v kritické fázi letu. [H-1]	
Scénář 4.1.1 pro UCA-4.1 Chyby zahrnující řídící člen	Posádka nechtěně odepnula el. obvod mechanické části PCA při funkční jednotce PCA v kritické fázi letu, neboť pilot špatně uchopil řídící páku.
Scénář 4.1.2 pro UCA-4.1 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Posádka odepnula el. obvod mechanické části PCA při funkční jednotce PCA v kritické fázi letu, neboť rozsvícení sousedních kontrolek na Master Tablu si pilot interpretoval jako poruchu jednotky PCA.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že v jednotce PCA je porucha.
Co mohlo toto způsobit	- pilot se nepodíval důkladně na Master Tablo, neboť je v kritické fázi letu - akustický signál varování obou indikací na Master Tablu je stejný (pilot si mohl splést akustické varování)
[UCA-4.2]: Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA. [H-1.1; H-2]	
Scénář 4.2.1 pro UCA-4.2 Chyby zahrnující řídící člen	Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA z důvodu zaneprázdnění, rozptýlení, nepřítomnosti...
Scénář 4.2.2 pro UCA-4.2 Neadekvátní řídící algoritmus	Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA, neboť se domnívá, že akci již provedl druhý pilot.
Scénář 4.2.3 pro UCA-4.2 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA, neboť nedostala indikaci o poruše jednotky PCA.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA
Scénář 4.2.4 pro UCA-4.2 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Posádka neodepnula el. obvod mechanické části PCA při poruše jednotky PCA, neboť rozsvícení varování poruchy jednotky PCA na Master Tablu si pilot interpretoval jako rozsvícení sousedních kontrolek.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- pilot se nepodíval důkladně na Master Tablo - akustický signál varování obou indikací na Master Tablu je stejný (pilot si mohl splést akustické varování)

[UCA-4.3]: Posádka odepnula el. obvod mechanické části PCA příliš pozdě při poruše jednotky PCA. [H-1.1; H-2]	
Scénář 4.3.1 pro UCA-1.3 Chyby zahrnující řídící člen	Posádka odepnula el. obvod mechanické části PCA příliš pozdě při poruše jednotky PCA z důvodu zaneprázdnění, rozptýlení, nepřítomnosti...
Scénář 4.3.2 pro UCA-1.3 Neadekvátní řídící algoritmus	Posádka odepnula el. obvod mechanické části PCA příliš pozdě při poruše jednotky PCA, neboť očekávali, že akci provede druhý pilot.
Scénář 4.3.3 pro UCA-1.3 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Posádka odepnula el. obvod mechanické části PCA příliš pozdě při poruše jednotky PCA, neboť pilotům nedošla indikace poruchy jednotky PCA. Nestandartní chování jednotky PCA zjistila posádka až po vychylování výškových kormidel.
Doměnka řídícího členu, která vede k UCA	Posádka je v domění, že jednotka PCA je funkční.
Co mohlo toto způsobit	- elektrický obvod nedodává el. energii na master tabla a MFD, tudíž posádka nezískala zpětnou vazbu - jednotka ECU je špatně nakonfigurovaná, z toho důvodu neodeslala informace o poruše jednotky PCA

[UCA-5.1]: Posádka ovládá trimovací plošku v jiném, než požadovaném směru. [H-1]	
Scénář 5.1.1 pro UCA-5.1 Neadekvátní řídící algoritmus	Posádka ovládá trimovací plošku v jiném, než požadovaném směru z důvodu špatného proškolení nebo zvyku z jiného letounu.
Scénář 5.1.2 pro UCA-5.1 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Posádka ovládá trimovací plošku v jiném, než požadovaném směru, neboť se pilotovi zasekne trimovací spínač na řídící páce a pilot si toho nevšimne.
Doměnka řídícího členu, která vede k UCA	Posádka se domnívá, že trimovací spínač se vrátil do své původní polohy.
Co mohlo toto způsobit	- posádka si nezkontrolovala, zdali se trimovací knoflík vrátil do své neutrální polohy
[UCA-5.2]: Posádka neovládá trimovací plošku při velkých silách v řízení. [H-1.1]	
Scénář 5.2.1 pro UCA-5.2 Chyby zahrnující řídící člen	Posádka neovládá trimovací plošku při velkých silách v řízení, neboť je v domění, že trimovací ploška je ovládána automaticky.
[UCA-5.3]: Posádka začala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš pozdě. [H-1.1]	
Scénář 5.3.1 pro UCA-5.3 Chyby zahrnující řídící člen	Posádka začala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš pozdě, neboť si pilot neuvědomil včas, že trimovací ploška není ovládána automaticky.
[UCA-5.4]: Posádka přestala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš brzy. [H-1.1]	
Scénář 5.4.1 pro UCA-5.4 Chyby zahrnující řídící člen	Posádka přestala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš brzy, neboť z ergonomických důvodů už nedokázala nadále prstem udržet spínač v dané poloze.
Scénář 5.4.2 pro UCA-5.4 Neadekvátní řídící algoritmus	Posádka přestala ovládat trimovací plošku v požadovaném směru při velkých silách v řízení příliš brzy, neboť pilot ovládající řídící páku se špatně domnívá, že kontrolu nad trimovacím spínačem převzal druhý pilot.

[UCA-6.1]: Posádka ovládá trimovací spínač v opačném, než požadovaném, směru. [H-1.1; H-1.2]	
Scénář 6.1.1 pro UCA-6.1 Neadekvátní řídící algoritmus	Posádka ovládá trimovací spínač v opačném, než požadovaném, směru, z důvodu nedostatečného proškolení posádky.
[UCA-6.2]: Posádka ovládá trimovací spínač příliš dlouho i poté, co přestala vychylovat výšková kormidla. [H-2]	
Scénář 6.2.1 pro UCA-6.2 Chyby zahrnující řídící člen	Posádka ovládá trimovací spínač příliš dlouho i poté, co přestala vychylovat výšková kormidla, neboť posádka pod velkým časovým nátlakem zapomněla, že stále ovládá trimovací spínač.
Scénář 6.2.2 pro UCA-6.2 Řídící člen získá chybnou zpětnou vazbu (informaci)	Posádka ovládá trimovací spínač příliš dlouho i poté, co přestala vychylovat výšková kormidla, jelikož je řídící páka stále vychýlena.
Doměnka řídícího členu, která vede k UCA	Posádka se domnívá, že jsou výšková kormidla stále vychýlena.
Co mohlo toto způsobit	- došlo k mechanické deformaci na určitých částech trasy podélného řízení
[UCA-6.3]: Posádka ovládá trimovací spínač při vypnuté nebo nefunkční ECU jednotce. [H-1]	
Scénář 6.3.1 pro UCA-6.3 Neadekvátní řídící algoritmus	Posádka ovládá trimovací spínač při vypnuté nebo nefunkční ECU jednotce, z důvodu nedostatečného proškolení posádky.

[UCA-7.1]: Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru. [H-1; H-1.2; H-2; H-2.1]	
Scénář 7.1.1 pro UCA-7.1 Neadekvátní řídící algoritmus	Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru z důvodu chybného naprogramování (např. chybná proporční korekce vstupních údajů).
Scénář 7.1.2 pro UCA-7.1 Neadekvátní řídící algoritmus	Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru, neboť nedokázala rozpoznat chybný vstupní údaj z jednoho ze senzorů.
Scénář 7.1.3 pro UCA-7.1 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru, jelikož jednotka ECU nepřepnula směr ovládání trimovací plošky poté, co se výšková kormidla vychýlila na opačnou stranu.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla jsou stále vychýlena v původním směru.
Co mohlo toto způsobit	- zamrznutí jednotky ECU - jednotka ECU je zahlcena vstupními údaji a nezvládá včas zpracovávat nápor dat - jednotka ECU se přehřívá
Scénář 7.1.4 pro UCA-7.1 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru, jelikož jednotka ECU nepřepnula směr ovládání trimovací plošky poté, co se výšková kormidla vychýlila na opačnou stranu.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla jsou stále vychýlena v původním směru.
Co mohlo toto způsobit	- zamrznutí silového senzoru 1 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o vstupní síle) - zamrznutí silového senzoru 2 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o výchylce PCA páky)
[UCA-7.2]: Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla. [H-1; H-1.2; H-2]	
Scénář 7.2.1 pro UCA-7.2 Chyby zahrnující řídící člen	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla z důvodu chybného naprogramování (např. chybná proporční korekce vstupních údajů).
Scénář 7.2.2 pro UCA-7.2 Neadekvátní řídící algoritmus	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla, neboť nedokázala rozpoznat chybný vstupní údaj z jednoho ze senzorů.
Scénář 7.2.3 pro UCA-7.2 Řídící člen získá správnou zpětnou vazbu (informaci), ale špatně si ji interpretuje nebo ji ignoruje	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla, jelikož si vstupní údaje o vyšším násobku vlivem vlétnutí do poryvu interpretuje jako vychylování výškových kormidel.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že je letoun zatížen vyšším násobkem z důvodu vychýlení výškových kormidel.
Co mohlo toto způsobit	- chybná proporční korekce vstupních údajů ze senzorů 1 nebo 2

Scénář 7.2.4 pro UCA-7.2 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla, jelikož jednotka ECU nevrátila trimovací plošku do neutrální polohy poté, co posádka přestala vychylovat výšková kormidla.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla jsou stále vychýlena v původním směru.
Co mohlo toto způsobit	- zamrznutí silového senzoru 1 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o vstupní síle) - zamrznutí silového senzoru 2 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o výchylce PCA páky)
Scénář 7.2.5 pro UCA-7.2 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla, jelikož dostává chybné vstupní údaje ze senzorů 1 nebo 2.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla byla vychýlena.
Co mohlo toto způsobit	- senzory nebyly správně zkalibrovány - deformace táhel způsobily špatné snímání síly na senzorech 1 a 2
Scénář 7.2.6 pro UCA-7.2 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU vychyluje trimovací plošku, i když nebyla vychýlena výšková kormidla, jelikož dostává chybnou zpětnou vazbu od servomotoru trimovací plošky.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že trimovací ploška nebyla vychýlena.
Co mohlo toto způsobit	- servomotor trimovací plošky nebyl správně zkalibrován - ačkoliv je výstupní táhlo servomotoru v neutrální poloze, tak deformací táhla u servomotoru trimovací plošky došlo k vychýlení trimovací plošky
[UCA-7.3]: Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení. [H-2.1]	
Scénář 7.3.1 pro UCA-7.3 Chyby zahrnující řídící člen	Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení, jelikož jednotka ECU je špatně nakonfigurovaná.
Scénář 7.3.2 pro UCA-7.3 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení, jelikož dostává chybnou zpětnou vazbu od servomotoru trimovací plošky.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že trimovací ploška je vychýlena.
Co mohlo toto způsobit	- servomotor trimovací plošky nebyl správně zkalibrován - ačkoliv je výstupní táhlo servomotoru v neutrální poloze, tak deformací táhla u servomotoru trimovací plošky došlo k vychýlení trimovací plošky

Scénář 7.3.3 pro UCA-7.3 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení, jelikož jednotka ECU nezískává pravdivé vstupní údaje ze silových senzorů 1 a 2
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla nebyla vychýlena.
Co mohlo toto způsobit	- senzory nebyly správně zkalibrovány - deformace táhel způsobily špatné snímání síly na senzorech 1 a 2
Scénář 7.3.4 pro UCA-7.3 Neadekvátní řídící algoritmus	Jednotka ECU nevychyluje trimovací plošku v požadovaném směru při velkých silách v řízení, jelikož stisknutí Paddle switche způsobilo přerušení ovládání trimovací plošky.
[UCA-7.4]: Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení. [H-2.1]	
Scénář 7.4.1 pro UCA-7.4 Chyby zahrnující řídící člen	Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení z důvodu chybného naprogramování (jednotka ECU vychyluje trimovací plošku až při mnohem vyšším násobku nebo rychlosti, než by mělo).
Scénář 7.4.2 pro UCA-7.4 Neadekvátní řídící algoritmus	Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení, jelikož jednotka ECU nezvládala včas zpracovávat velký nápor dat.
Scénář 7.4.3 pro UCA-7.4 Neadekvátní řídící algoritmus	Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení, jelikož jednotka ECU nedokázala včas identifikovat chybný vstupní údaj.
Scénář 7.4.4 pro UCA-7.4 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU začala vychylovat trimovací plošku příliš pozdě při větších silách v řízení, jelikož obdržela příliš pozdě vstupní údaje o násobku a rychlosti od senzorů.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je dočasně v domění, že letoun nedosáhl vysokého násobku/rychlosti, nebo že výšková kormidla nejsou vychýlena.
Co mohlo toto způsobit	- zamrznutí silového senzoru 1 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o vstupní síle) - zamrznutí silového senzoru 2 nebo selhání jeho dodávky el. energie (senzor neodesílá údaje o výchylce PCA páky) - zamrznutí jednotky dodávající vstupní údaje o rychlosti nebo násobku
[UCA-7.5]: Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení. [H-2.1]	
Scénář 7.5.1 pro UCA-7.5 Chyby zahrnující řídící člen	Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení, jelikož přestala v danou chvíli fungovat (např. vlivem vystavení extrémním podmínkám, selháním dodávky el. energie…)

Scénář 7.5.2 pro UCA-7.5 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení, neboť přestala dostávat zpětnou vazbu o poloze trimovací plošky.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU nezná polohu trimovací plošky.
Co mohlo toto způsobit	- servomotor trimovací plošky přestal odesílat zpětnou vazbu (selhání el. obvodu) - trasa zpětné vazby od servomotoru k jednotce ECU je poškozena (vlivem vystavení extrémním teplotám, vibrací motoru, vlhkosti…)
Scénář 7.5.3 pro UCA-7.5 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení, neboť začala dostávat chybné vstupní údaje o násobku a rychlosti.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že letoun již není zatížen vysokými násobky nebo rychlostí.
Co mohlo toto způsobit	- senzory pro snímání rychlosti a násobku nebyly správně zkalibrovány - došlo k nedetekované poruše systému měření rychlosti nebo násobku (námraza, nečistoty…)
Scénář 7.5.4 pro UCA-7.5 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU přestala vychylovat trimovací plošku příliš brzy při větších silách v řízení, neboť přestala dostávat zpětnou vazbu o poloze výškových kormidel.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU nezná polohu výškových kormidel.
Co mohlo toto způsobit	- selhání dodávky el. energie silovým senzorům 1 a 2 - došlo k poruše trasy mezi silovými senzory a jednotkou ECU (vlivem vystavení extrémním teplotám, vibrací motoru, vlhkosti…) - došlo k mechanickému rozpojení trasy napojení jednotky PCA do systému podélného řízení (např. zlomení propojovacího táhla, uvolnění páky…)
[UCA-7.6]: Jednotka ECU vychyluje trimovací plošku příliš dlouho i poté, co se přestala vychylovat výšková kormidla. [H-1; H-2]	
Scénář 7.6.1 pro UCA-7.5 Chyby zahrnující řídící člen	Jednotka ECU vychyluje trimovací plošku příliš dlouho i poté, co se přestala vychylovat výšková kormidla, jelikož nestíhá zpracovávat velký nápor dat.
Scénář 7.6.2 pro UCA-7.5 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU vychyluje trimovací plošku příliš dlouho i poté, co se přestala vychylovat výšková kormidla, jelikož dostává chybné vstupní údaje od silových senzorů.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že výšková kormidla jsou stále vychýlena v původním směru.

Co mohlo toto způsobit	- došlo k poruše trasy mezi silovými senzory a jednotkou ECU (vlivem vystavení extrémním teplotám, vibrací motoru, vlhkosti…) - senzory nebyly správně zkalibrovány - deformace táhel způsobily špatné snímání síly na senzorech 1 a 2

[UCA-8.1]: Jednotka ECU sepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	
Scénář 8.1.1 pro UCA-8.1 Neadekvátní řídící algoritmus	Jednotka ECU sepne obvod při poruše jednotky PCA, neboť byla jednotka ECU špatně nakonfigurovaná (špatně nastavené rozsahy normálních hodnot), tudíž nedetekuje žádnou poruchu v jednotce PCA.
Scénář 8.1.2 pro UCA-8.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU sepne obvod při poruše jednotky PCA, neboť dostávala chybné údaje o teplotách, otáčkách a fázích.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že jednotka PCA je plně funkční.
Co mohlo toto způsobit	- teploměry či resolvery v jednotce PCA nebyly správně zkalibrovány, z toho důvodu odesílaly chybné údaje - teploměry vlivem extrémních venkovních teplot zkreslovaly odeslané údaje o teplotě - resolvery vlivem velkých vibrací z motoru zkreslovaly odeslané údaje o otáčkách a fázích
[UCA-8.2]: Jednotka ECU neodepne obvod při poruše jednotky PCA. [H-1; H-1.1; H-2; H-2.2]	
Scénář 8.2.1 pro UCA-8.2 Neadekvátní řídící algoritmus	Jednotka ECU neodepne obvod při poruše jednotky PCA, neboť nezvládala zpracovávat velký nápor dat.
Scénář 8.2.2 pro UCA-8.2 Neadekvátní řídící algoritmus	Jednotka ECU neodepne obvod při poruše jednotky PCA, neboť byla jednotka ECU špatně nakonfigurovaná (špatně nastavené rozsahy normálních hodnot), tudíž nedetekuje žádnou poruchu v jednotce PCA.
Scénář 8.2.3 pro UCA-8.2 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU neodepne obvod při poruše jednotky PCA, neboť nedetekuje žádnou poruchu v jednotce PCA.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že jednotka PCA je plně funkční.
Co mohlo toto způsobit	- teploměry či resolvery v jednotce PCA nebyly správně zkalibrovány, z toho důvodu odesílaly chybné údaje - teploměry vlivem extrémních venkovních teplot zkreslovaly odeslané údaje o teplotě - resolvery vlivem velkých vibrací z motoru zkreslovaly odeslané údaje o otáčkách a fázích
[UCA-8.3]: Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA. [H-1]	
Scénář 8.3.1 pro UCA-8.3 Neadekvátní řídící algoritmus	Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA, neboť jednotka ECU nedokázala včas ověřit funkčnost spojky a elektromotoru (vnitřní proces ověřování v jednotce ECU je příliš dlouhý).

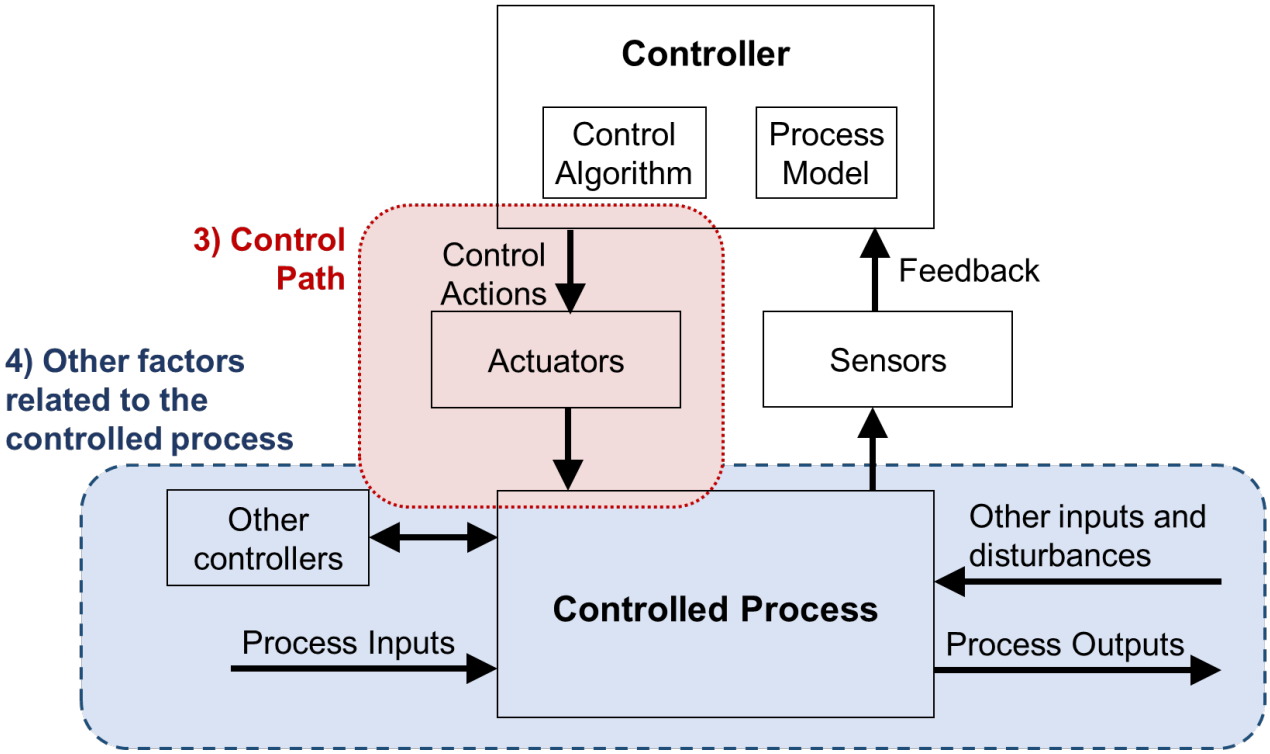
Scénář 8.3.2 pro UCA-8.3 Nebezpečný vstup od jiného řídícího členu (Controller)	Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA z důvodu pozdní dodávky el. energie do jednotky ECU.
Scénář 8.3.3 pro UCA-8.3 Neadekvátní řídící algoritmus	Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA, neboť nezvládala včas zpracovávat velký nápor dat.
Scénář 8.3.4 pro UCA-8.3 Nebezpečný vstup od jiného řídícího členu (Controller)	Jednotka ECU sepne obvod příliš pozdě v kritické fázi letu při funkční jednotce PCA, neboť posádka zapnula přívod el. energie do jednotky PCA příliš pozdě.

[UCA-9.1]: Jednotka ECU ovládá výšková kormidla v opačném, než požadovaném, směru nebo příliš pomalu. [H-1]	
Scénář 9.1.1 pro UCA-9.1 Chyby zahrnující řídící člen	Jednotka ECU ovládá výšková kormidla v opačném směru nebo příliš pomalu, neboť nezvládá včas zpracovávat vstupní údaje ze silových senzorů.
Scénář 9.1.2 pro UCA-9.1 Neadekvátní řídící algoritmus	Jednotka ECU ovládá výšková kormidla v opačném směru nebo příliš pomalu, jelikož je chybně nakonfigurovaná.
Scénář 9.1.3 pro UCA-9.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU ovládá výšková kormidla v opačném směru nebo příliš pomalu, neboť získává chybnou zpětnou vazbu od resolverů elektromotoru a spojky.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že získává správnou zpětnou vazbu od resolverů elektromotoru a spojky.
Co mohlo toto způsobit	- resolvery nebyly správně zkalibrovány - mechanické poškození resolverů způsobilo zkreslení odeslaných údajů - resolvery měří špatně otáčky a fáze z důvodu silných vibrací motoru
Scénář 9.1.4 pro UCA-9.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU ovládá výšková kormidla v opačném směru nebo příliš pomalu, neboť získává chybné vstupní údaje od silových senzorů.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že získává správné vstupní údaje od silových senzorů.
Co mohlo toto způsobit	- silové senzory nebyly správně zkalibrovány - silové senzory byly mechanicky poškozeny - silové senzory snímají špatně sílu z důvodu deformace táhel či pák - silové senzory nebo jednotka PCA nejsou správně upevněny
Scénář 9.1.5 pro UCA-9.1 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU ovládá výšková kormidla v opačném směru nebo příliš pomalu, jelikož jednotka ECU nezískává pravdivé údaje o rychlosti a násobku.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že letoun nedosáhl vysoké rychlosti nebo násobku.
Co mohlo toto způsobit	- jednotka ECU získává chybné vstupní údaje - jednotka ECU špatně rozpoznala špatný vstupní údaj, tudíž zahodila pravdivý vstupní údaj a pracovala se špatným vstupním údajem
[UCA-9.2]: Jednotka ECU vychyluje výšková kormidla bez vstupu od posádky. [H-2]	
Scénář 9.2.1 pro UCA-9.2 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU vychyluje výšková kormidla bez vstupu od posádky, neboť získává chybné údaje ze silových senzorů.

Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že získává správné vstupní údaje od silových senzorů.
Co mohlo toto způsobit	- silové senzory nebyly správně zkalibrovány - silové senzory byly mechanicky poškozeny - silové senzory snímají špatně sílu z důvodu deformace táhel či pák - silové senzory nebo jednotka PCA nejsou správně upevněny
[UCA-9.3]: Jednotka ECU neovládá výšková kormidla při sepnuté spojce. [H-1; H-1.1]	
Scénář 9.3.1 pro UCA-9.3 Chyby zahrnující řídící člen	Jednotka ECU neovládá výšková kormidla při sepnuté spojce, neboť nezvládá včas zpracovávat vstupní údaje ze silových senzorů.
Scénář 9.3.2 pro UCA-9.3 Neadekvátní řídící algoritmus	Jednotka ECU neovládá výšková kormidla při sepnuté spojce, neboť je dodávka el. energie do jednotky ECU vypnuta, zatímco dodávka el. energie do mechanické části PCA je zapnuta (spojka se neodepnula po vypnutí přívodu el. energie do jednotky ECU).
Scénář 9.3.3 pro UCA-9.3 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU neovládá výšková kormidla při sepnuté spojce, jelikož získává chybné vstupní údaje ze silových senzorů.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že získává správné vstupní údaje ze silových senzorů.
Co mohlo toto způsobit	- zmrazení silových senzorů vlivem mechanického poškození nebo vystavení extrémním teplotám
Scénář 9.3.4 pro UCA-9.3 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU neovládá výšková kormidla při sepnuté spojce, neboť získává chybnou zpětnou vazbu o stavu spojky.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že je spojka odepnutá.
Co mohlo toto způsobit	- spojka je mechanicky zaseknutá - resolver spojky je zaseknutý - resolver spojky je odpojen od dodávky el. energie, zatímco spojka je připojena k dodávce el. energie
[UCA-9.4]: Jednotka ECU začala ovládat výšková kormidla příliš pozdě v kritické fázi letu. [H-1; H-1.1]	
Scénář 9.4.1 pro UCA-9.4 Neadekvátní řídící algoritmus	Jednotka ECU začala ovládat výšková kormidla příliš pozdě v kritické fázi letu, neboť nezpracovává včas vstupní údaje ze silových senzorů.
Scénář 9.4.2 pro UCA-9.4 Nebezpečný vstup od jiného řídícího členu (Controller)	Jednotka ECU začala ovládat výšková kormidla příliš pozdě v kritické fázi letu, jelikož posádka ovládá trimovací spínač na opačnou stranu. (pro mód 2)
Scénář 9.4.3 pro UCA-9.4 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU začala ovládat výšková kormidla příliš pozdě v kritické fázi letu, neboť dostává příliš pozdě vstupní údaje ze silových senzorů

Doměnka řídícího členu, která vede k UCA	Jednotka ECU je v domění, že získává vstupní údaje ze silových senzorů včas.
Co mohlo toto způsobit	- nestabilní dodávka el. energie do silových senzorů - zmrazení silových senzorů vlivem mechanického poškození nebo vystavení extrémním teplotám - silové senzory byly mechanicky poškozeny
[UCA-9.5]: Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu. [H-1]	
Scénář 9.5.1 pro UCA-9.5 Chyby zahrnující řídící člen	Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu, jelikož jednotka ECU se porouchala (zkrat v obvodu, přehřátí…)
Scénář 9.5.2 pro UCA-9.5 Nebezpečný vstup od jiného řídícího členu (Controller)	Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu, jelikož odbržela informaci, že se spojka nebo elektromotor začaly přehřívat.
Scénář 9.5.3 pro UCA-9.5 Řídící člen získá chybnou zpětnou vazbu (informaci)	Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu, jelikož byla dodávka el. energie do jednotky PCA přerušena (zkrat v el. obvodu, posádka nechtěně stiskla paddle switch nebo spínače).
Scénář 9.5.4 pro UCA-9.5 Řídící člen nezíská zpětnou vazbu (informaci) ve chvíli, kdy ji potřebuje (opožděně nebo nikdy)	Jednotka ECU přestala ovládat výšková kormidla příliš brzy v kritické fázi letu, neboť přestala dostávat vstupní údaje od silových senzorů.
Doměnka řídícího členu, která vede k UCA	Jednotka ECU neví, že výšková kormidla jsou stále vychýlena.
Co mohlo toto způsobit	- zmrazení silových senzorů vlivem mechanického poškození nebo vystavení extrémním teplotám - silové senzory byly mechanicky poškozeny - selhání dodávky el. energie silovým senzorům 1 a 2

B) IDENTIFIKACE SCÉNÁŘŮ, U KTERÝCH JSOU CA (CONTROL ACTIONS) NESPRÁVNĚ PROVEDENY NEBO NEJSOU VŮBEC:



Scénáře zahrnující řídící cestu mohou obecně zahrnovat:

- řídící akce nebyla vykonána
  - řídící člen vykonal řídící akci, avšak tato akce nebyla obdržena aktuátorem
  - řídící akce byla obdržena aktuátorem, avšak aktuátor na ni nereaguje
  - akuátor reaguje, přestože řídící akce nebyla řídícím členem vykonána
- řídící akce byla chybně vykonána
  - řídící akce byla správně vykonána řídícím členem, ale aktuátor obdržel chybnou řídící akci
  - řídící akce byla správně vykonána řídícím členem, avšak aktuátor reaguje neadekvátně
  - aktuátor reaguje adekvátně, avšak řídící akce je chybně aplikována v řízeném procesu
  - řídící akce nebyla vykonána řídícím členem, avšak aktuátor se chová, jako by byl vykonán

Přílohy

[CA-1]: ovládání výškových kormidel	
Řídící akce byla chybně vykonána: Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru.	
Scénář 1.1	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu trvalé deformace táhel.
Scénář 1.2	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu zakročení jednotky PCA.
Scénář 1.3	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu prasklého pružinového posilovače.
Řídící akce nebyla vykonána: Výšková kormidla nebyla vychylována v požadovaném směru.	
Scénář 1.4	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru, jelikož došlo k rozpojení mechanické cesty podélného řízení.
Scénář 1.5	Výšková kormidla byla vychylována v jiné, než požadované úrovni nebo směru z důvodu zakročení jednotky PCA.
Řídící akce byla chybně vykonána: Výšková kormidla se přestala vychylovávat v požadovaném směru příliš brzy.	
Scénář 1.6	Výšková kormidla se přestala vychylovávat v požadovaném směru příliš brzy, jelikož během toho došlo k rozpojení mechanické trasy podélného řízení.
Scénář 1.7	Výšková kormidla se přestala vychylovávat v požadovaném směru příliš brzy z důvodu zakročení jednotky PCA.
[CA-2]: ovládání přívodu el. energie (pro ECU)	
Řídící akce nebyla vykonána: Dodávka el. energie do jednotky ECU nebyla přerušena při poruše jednotky PCA.	
Scénář 2.1	Dodávka el. energie do jednotky ECU nebyla přerušena při poruše jednotky PCA z důvodu poruchy spínače, který ovládá dodávku el. energie do jednotky ECU.
[CA-3]: ovládání přívodu el. energie (pro mechanickou část PCA)	
Řídící akce byla chybně vykonána: Dodávka el. energie pro mechanickou část PCA se zapnula při poruše jednotky PCA.	
Scénář 3.1	Dodávka el. energie pro mechanickou část PCA se zapnula při poruše jednotky PCA z důvodu poruchy spínáčů v el. obvodu.
Řídící akce nebyla vykonána: Dodávka el. energie pro mechanickou část PCA nebyla přerušena při poruše jednotky PCA.	
Scénář 3.2	Dodávka el. energie pro mechanickou část PCA nebyla přerušena při poruše jednotky PCA z důvodu poruchy spínačů v el. obvodu.

Přílohy

[CA-4]: sepnutí/odepnutí el. obvodu přes paddle switch	
Řídící akce byla chybně vykonána: El. obvod mechanické části PCA se odepnul při funkční jednotce PCA v kritické fázi letu.	
Scénář 4.1	El. obvod mechanické části PCA se odepnul při funkční jednotce PCA v kritické fázi letu, z důvodu poruchy spínače, který ovládá dodávku el. energie do mechanické části jednotky PCA.
Řídící akce nebyla vykonána: El. obvod mechanické části PCA se neodepnul při poruše jednotky PCA.	
Scénář 4.2	El. obvod mechanické části PCA se neodepnul při poruše jednotky PCA z důvodu poruchy paddle switche.
[CA-5]: ovládání trimovací plošky	
Řídící akce byla chybně vykonána: Trimovací ploška byla vychylována v jiném, než požadovaném směru.	
Scénář 5.1	Trimovací ploška byla vychylována v jiném, než požadovaném směru, jelikož je aktuátor trimovací plošky opačně propojen k trimovacímu spínači.
Řídící akce nebyla vykonána: Trimovací ploška není vychylována při velkých silách v řízení.	
Scénář 5.2	Trimovací ploška není vychylována při velkých silách v řízení, neboť došlo k rozpojení el. obvodu mezi spínačem a aktuátorem trimovací plošky.
Scénář 5.3	Trimovací ploška není vychylována při velkých silách v řízení z důvodu zaseknutí spínače trimovací plošky.
Scénář 5.4	Trimovací ploška není vychylována při velkých silách v řízení z důvodu mechanické poruchy aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: Trimovací ploška se začala vychylovat v požadovaném směru při velkých silách v řízení příliš pozdě.	
Scénář 5.5	Trimovací ploška se začala vychylovat v požadovaném směru při velkých silách v řízení příliš pozdě z důvodu pozdní reakce aktuátoru trimovací plošky na přijatý signál.
Řídící akce byla chybně vykonána: Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy.	
Scénář 5.6	Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy, neboť během ovládání trimovací plošky došlo k přerušení dodávky el. energie do aktuátoru trimovací plošky.
Scénář 5.7	Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy, neboť během ovládání trimovací plošky došlo k mechanické poruše aktuátoru trimovací plošky.

Scénář 5.8	Trimovací ploška se přestala vychylovat v požadovaném směru při velkých silách v řízení příliš brzy, neboť během ovládání trimovací plošky došlo k zaseknutí spínače trimovací plošky.
[CA-6]: PCA trim	
Řídící akce byla chybně vykonána: Trimovací ploška je ovládána v opačném, než požadovaném, směru.	
Scénář 6.1	Trimovací ploška je ovládána v opačném, než požadovaném, směru, neboť byl trimovací spínač opačně propojen k el. obvodu.
[CA-7]: ovládání trimovací plošky	
Řídící akce byla chybně vykonána: Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru.	
Scénář 7.1	Jednotka ECU ovládá trimovací plošku v opačném, než požadovaném, směru, neboť je aktuátor trimovací plošky opačně propojen.
Řídící akce byla chybně vykonána: Trimovací ploška se vychyluje, i když nebyla vychýlena výšková kormidla.	
Scénář 7.2	Trimovací ploška se vychyluje, i když nebyla vychýlena výšková kormidla z důvodu samovolné aktivace aktuátoru trimovací plošky.
Řídící akce nebyla vykonána: Trimovací ploška se nevychyluje v požadovaném směru při velkých silách v řízení.	
Scénář 7.3	Trimovací ploška se nevychyluje v požadovaném směru při velkých silách v řízení z důvodu poruchy nebo zaseknutí aktuátoru trimovací plošky.
Scénář 7.4	Trimovací ploška se nevychyluje v požadovaném směru při velkých silách v řízení z důvodu přerušení dodávky el. energie do aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: Trimovací ploška se začala vychylovat příliš pozdě při větších silách v řízení.	
Scénář 7.5	Trimovací ploška se začala vychylovat příliš pozdě při větších silách v řízení z důvodu pozdní reakce aktuátoru trimovací plošky na přijatý signál.
Scénář 7.6	Trimovací ploška se začala vychylovat příliš pozdě při větších silách v řízení z důvodu pozdní dodávky el. energie do aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: Trimovací ploška se přestala vychylovat příliš brzy při větších silách v řízení.	
Scénář 7.7	Trimovací ploška se přestala vychylovat příliš brzy při větších silách v řízení, z důvodu mechanického poškození aktuátoru trimovací plošky vzniklé vlivem působení vnějších aerodynamických a setrvačných sil.
Scénář 7.8	Trimovací ploška se přestala vychylovat příliš brzy při větších silách v řízení z důvodu přerušení dodávky el. energie.

Scénář 7.9	Trimovací ploška se přestala vychylovat příliš brzy při větších silách v řízení, neboť došlo k překročení teploty elektromotoru v aktuátoru trimovací plošky.
Řídící akce byla chybně vykonána: Trimovací ploška je vychýlena příliš dlouho i poté, co se přestala vychylovat výšková kormidla.	
Scénář 7.10	Trimovací ploška je vychýlena příliš dlouho i poté, co se přestala vychylovat výšková kormidla z důvodu zaseknutí mechanismu aktuátoru nebo trimovací plošky (např. vlivem uvolnění součástky, vniknutí cizích předmětů…).
[CA-8]: rozepnutí/sepnutí mechanického obvodu	
Řídící akce byla chybně vykonána: Mechanická část PCA se sepne při poruše jednotky PCA.	
Scénář 8.1	Mechanická část PCA se sepne při poruše jednotky PCA z důvodu špatně nastavené spojky (spojka reaguje opačně na signály od jednotky ECU)
Řídící akce nebyla vykonána: Mechanická část PCA se neodepne při poruše jednotky PCA.	
Scénář 8.2	Mechanická část PCA se neodepne při poruše jednotky PCA z důvodu zaseknuté spojky.
Scénář 8.3	Mechanická část PCA se neodepne při poruše jednotky PCA z důvodu poruchy přijímače signálu spojky.
Řídící akce byla chybně vykonána: Mechanická část PCA se sepne příliš pozdě v kritické fázi letu při funkční jednotce PCA.	
Scénář 8.4	Mechanická část PCA se sepne příliš pozdě v kritické fázi letu při funkční jednotce PCA, neboť el. energie dorazí do spojky příliš pozdě (problém s el. obvodem spojky).
Scénář 8.5	Mechanická část PCA se sepne příliš pozdě v kritické fázi letu při funkční jednotce PCA z důvodu zadření mechanismu spojky.
[CA-9]: ovládání výškových kormidel	
Řídící akce byla chybně vykonána: Výšková kormidla jsou vychýlena v opačném, než požadovaném, směru nebo příliš pomalu.	
Scénář 9.1	Výšková kormidla jsou vychýlena v opačném, než požadovaném, směru, neboť elektromotor se otáčí v opačném, než požadovaném, směru (elektromotor má nastavenou opačnou polarizaci).
Scénář 9.2	Výšková kormidla jsou vychýlena příliš pomalu z důvodu zadrhnutí mechanismu elektromotoru či spojky.
Scénář 9.3	Výšková kormidla jsou vychýlena příliš pomalu z důvodu časové degradaci mechanismu elektromotoru.
Scénář 9.4	Výšková kormidla jsou vychýlena v opačném, než požadovaném, směru, neboť převodovka je po údržbě špatně namontovaná.

Řídící akce byla chybně vykonána: Výšková kormidla jsou vychýlena bez vstupu od posádky.	
Scénář 9.5	Výšková kormidla jsou vychýlena bez vstupu od posádky z důvodu poruchy spínačů, které ovlivňují dodávku el. energie do elektromotoru.
Řídící akce nebyla vykonána: Výšková kormidla nejsou vychýlena při sepnuté spojce.	
Scénář 9.6	Výšková kormidla nejsou vychýlena při sepnuté spojce z důvodu přehřátí elektromotoru.
Scénář 9.7	Výšková kormidla nejsou vychýlena při sepnuté spojce z důvodu zaseknutí mechanismu elektromotoru nebo převodovky.
Scénář 9.8	Výšková kormidla nejsou vychýlena při sepnuté spojce, neboť el. obvod elektromtoru je poškozen (např. vlivem extrémních podmínek, přehřátím komponent, zkratem vlivem vibrací z motoru…).
Scénář 9.9	Výšková kormidla nejsou vychýlena při sepnuté spojce, neboť došlo k uvolnění táhla od páky v cestě podélného řízení.
Řídící akce byla chybně vykonána: Výšková kormidla jsou vychýlena příliš pozdě v kritické fázi letu.	
Scénář 9.10	Výšková kormidla jsou vychýlena příliš pozdě v kritické fázi letu z důvodu velké časové prodlevy elektromotoru (elektromotor nereaguje okamžitě na přijímaný el. proud)
Řídící akce byla chybně vykonána: Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu.	
Scénář 9.11	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu přehřátí elektromotoru.
Scénář 9.12	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu samovolného odpojení spojky.
Scénář 9.13	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu uvolnění ozubeného kola z převodovky.
Scénář 9.14	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu uvolnění táhla z páky v cestě podélného řízení.
Scénář 9.15	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu deformace výstupní hřídele elektromotoru.
Scénář 9.16	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu spálení spínačů ovládající přívod el. energie k elektromotoru vlivem zkratu.
Scénář 9.17	Výšková kormidla se přestala vychylovat příliš brzy v kritické fázi letu z důvodu přerušení dodávky el. energie do jednotky PCA.

Finální krok: Identifikujte požadavky a omezení

Systémové požadavky a omezení (z 1. kroku)	
SC-1	Systém podélného řízení musí vychylovat výšková kormidla v požadovaném směru.
SC-2	Systém podélného řízení nebo PCA nesmí vychylovat výšková kormidla bez vstupu pilota
Požadavky a omezení na řídící členy (ze 3. kroku)	
CC-1.1	Posádka musí včas vychylovat výšková kormidla v požadovaném směru a do požadované úrovně. [UCA-1.1; UCA-1.2; UCA-1.3]
CC-1.2	Posádka nesmí přestat ovládat výšková kormidla příliš brzy. [UCA-1.4]
CC-2.1	Posádka musí včas vypnout přívod el. energie do jednotky ECU při poruše jednotky PCA. [UCA-2.1; 2.2]
CC-3.1	Posádka nesmí zapnout přívod el. energie do mechanické části jednotky PCA při poruše jednotky PCA. [UCA-3.1]
CC-3.2	Posádka musí včas spínačem vypnout přívod el. energie do mechanické části PCA při poruše jednotky PCA (nebude-li fungovat paddle switch) [UCA-3.2; UCA-3.3]
CC-4.1	Posádka nesmí vypnout přívod el. energie do mechanické části PCA přes paddle switch v kritické fázi letu, je-li jednotka PCA funkční. [UCA-4.1]
CC-4.2	Posádka musí včas vypnout přívod el. energie do mechanické části PCA přes paddle switch, vyskytne-li se v ní porucha. [UCA-4.2; UCA-4.3]
CC-5.1	Posádka musí včas začít ovládat trimovací plošku v požadovaném směru při velkých silách v řízení. [UCA-5.1; UCA-5.2; UCA-5.3]
CC-5.2	Posádka nesmí přestat ovládat trimovací plošku v požadovaném směru při velkých silách v řízení. [UCA-5.4]
CC-6.1	Posádka musí ovládat trimovací spínač v požadovaném směru. [UCA-6.1]
CC-6.2	Posádka nesmí ovládat trimovací spínač i poté, co přestala vychylovat výšková kormidla. [UCA-6.2]
CC-6.3	Posádka nesmí nadále ovládat trimovací spínač při nefunkční nebo vypnuté ECU jednotce. [UCA-6.3]
CC-7.1	Jednotka ECU musí včas ovládat trimovací plošku v požadovaném směru. [UCA-7.1; UCA-7.4]
CC-7.2	Jednotka ECU nesmí vychylovat trimovací plošku, nejsou-li vychýlena výšková kormidla. [UCA-7.2]
CC-7.3	Jednotka ECU musí vychylovat trimovací plošku, jsou-li v řízení velké síly po delší dobu. [UCA-7.3]
CC-7.4	Jednotka ECU nesmí přestat vychylovat trimovací plošku, jsou-li v řízení stále velké síly a jsou vychýlena výšková kormidla. [UCA-7.5]
CC-7.5	Jednotka ECU musí přestat vychylovat trimovací plošku hned poté, co se přestaly vychylovat výšková kormidla. [UCA-7.6]
CC-8.1	Jednotka ECU nesmí sepnout spojku při poruše jednotky PCA. [UCA-8.1]
CC-8.2	Jednotka ECU musí odepnout spojku hned poté, co se v jednotce PCA vyskytne porucha. [UCA-8.2]

CC-8.3	Jednotka ECU musí včas sepnout spojku, není-li v jednotce PCA žádná porucha. [UCA-8.3]
CC-9.1	Jednotka ECU musí včas vychylovat výšková kormidla v požadovaném směru. [UCA-9.1; UCA-9.4]
CC-9.2	Jednotka ECU nesmí vychylovat výšková kormidla bez vstupu od posádky. [UCA-9.2]
CC-9.3	Jednotka ECU musí ovládat výšková kormidla, je-li sepnutá spojka. [UCA-9.3]
CC-9.4	Jednotka ECU nesmí přestat vychylovat výšková kormidla, dokud neobdrží pokyn od posádky. [UCA-9.5]
Požadavky a omezení na jednotlivé systémové komponenty (ze 4. kroku)	
CFC-1.1	Druhý pilot nesmí zasahovat řídícímu pilotovi do řízení. [Scénář 1.1.2]
CFC-1.2	Posádka musí být informována v případě prasknutí pružinového posilovače. [Scénář 1.1.3]
CFC-1.3	Posádka musí vědět, jak kompenzovat chybějící síly od pružinového posilovače, dojde-li k jeho prasknutí. [Scénář 1.1.3]
CFC-1.4	Jednotka PCA musí v obou směrech dodávat stejný výkon. [Scénář 1.1.3]
CFC-1.5	Posádka nikdy nesmí nechat řídící páky bez kontroly. [Scénář 1.2.2; 1.4.2; 5.4.2]
CFC-1.6	Posádka musí vždy oboustranně komunikovat a potvrzovat, když se předává řízení. [Scénář 1.2.2; 1.3.2; 1.4.2; 5.4.2]
CFC-1.7	Nefunkčnost el. obvodu musí být vždy indikována posádce, a to i při poruše el. obvodu. [Scénář 1.3.3; 2.2.3; 3.2.3; 4.2.3; 4.3.3]
CFC-1.8	Posádka musí být ihned informována, dojde-li k (nechtěnému) vypnutí dodávky el. energie do jednotky PCA. [Scénář 1.3.3; 9.5.3]
CFC-2.1	Posádka si musí určit, kdo vypne dodávku elektrické energie do jednotky PCA, a to bezprostředně po obdržení indikace poruchy jednotky PCA. [Scénář 2.1.2; 3.2.2; 3.3.2; 4.2.2; 4.3.2]
CFC-2.2	Posádka musí být informována bezprostředně poté, co došlo ke ztrátě dodávky el. energie na Master Tabla. [Scénář 2.1.3; 2.2.3; 3.2.3; 4.2.3; 4.3.3]
CFC-2.3	Jednotka ECU musí být nastavená na správné provozní hodnoty, aby v případě poruchy jednotky PCA dokázala detekovat vadu a bezprostředně o ní informovat posádku. [Scénář 2.1.3; 2.2.3; 3.1.2; 3.2.3; 3.3.3; 4.2.3; 4.3.3; 7.4.1; 8.1.1; 8.2.2; 9.1.2]
CFC-3.1	Posádka musí ještě před zapnutím přívodu el. energie do mechanické části jednotky PCA otestovat funkčnost žárovek na Master Tablu. [Scénář 3.1.2]

CFC-3.2	Dojde-li k výpadku el. energie, musí si posádka zkontrolovat funkčnost žárovek na Master Tablu, neboť výpadek dodávky el. energie do určité komponenty nemusí znamenat poruchu celého el. systému. [Scénář 3.3.3]
CFC-4.1	Posádce musí být vysvětleno, jak správně uchopit řídící páku (aby nedošlo k nechtěnému stisknutí paddle switche). [Scénář 4.1.1; 9.5.3]
CFC-4.2	Kontrolky na Master Tablu musí být při rozesvícení dostatečně odlišitelné, a to i za zhoršených podmínek (např. při silných turbulencích, silných vibracích motoru…). [Scénář 4.1.2; 4.2.4]
CFC-5.1	Posádka musí být řádně proškolena, aby nevychylovala trimovací plošku v opačném, než požadovaném, směru. [Scénář 5.1.1; 6.1.1; 9.4.2]
CFC-5.2	Posádka si musí po každém ovládání trimovací plošky zkontrolovat, zdali se jí nezaseknul trimovací spínač v nežádoucí poloze. [Scénář 5.1.2; 6.2.1]
CFC-5.3	Posádka musí být poučena, že trimovací ploška není ovládána automaticky, ale pouze manuálně. [Scénář 5.2.1; 5.3.1]
CFC-5.4	Trimovací spínač musí být dostatečně ergonomicky navržen, aby posádka dokázala udržet trimovací spínač ve vychýlené poloze dostatečně dlouho. [Scénář 5.4.1]
CFC-5.5	Posádka musí být poučena, že při nefunkční nebo vypnuté ECU jednotce není možné nadále ovládat trimovací plošku. [Scénář 6.3.1]
CFC-7.1	Jednotka ECU musí umět včas rozpoznat chybný nebo chybějící vstupní údaj ze silových senzorů. [Scénář 7.1.2; 7.1.4; 7.2.2; 7.4.3]
CFC-7.2	Jednotka ECU musí umět detekovat případné zamrznutí jednotky ECU a silových senzorů. [Scénář 7.1.3; 7.1.4; 9.3.3; 9.4.3; 9.5.4]
CFC-7.3	Jednotka ECU musí být dostatečně výkonná, aby zvládala včas zpracovávat i mnohonásobně větší nápor vstupních provozních dat. [Scénář 7.1.3; 7.4.2; 7.6.1; 8.2.1; 8.3.3; 9.1.1; 9.3.1; 9.4.1]
CFC-7.4	Jednotka ECU musí vrátit trimovací plošku do neutrální polohy poté, co zjistí, že silové senzory zamrzly nebo zasílají chybné vstupní údaje. [Scénář 7.2.4]
CFC-7.5	Silové senzory musí být pravidelně kontrolovány a zkalibrovány, přičemž se musí zkontrolovat i stav táhel, zdali nedošlo k jejich deformaci. [Scénář 7.2.5; 7.3.3; 7.6.2; 9.1.4; 9.2.1]
CFC-7.6	Servomotor trimovací plošky musí být pravidelně kontrolován a zkalibrován, přičemž se musí zkontrolovat i stav táhla trimovací plošky, zdali nedošlo k jeho deformaci. [Scénář 7.2.6]

CFC-7.7	Jednotka ECU musí umět včas rozpoznat chybný nebo chybějící vstupní údaj z jednotek dodávajících vstupní údaje o rychlosti a násobku. [Scénář 7.1.2; 7.1.4; 7.2.2; 7.4.3; 7.5.3; 9.1.5]
CFC-7.8	Jednotka ECU musí umět včas rozpoznat chybný nebo chybějící zpětný signál od servomotoru trimovací plošky. [Scénář 7.5.2]
CFC-7.9	Jednotka ECU musí vrátit trimovací plošku do neutrální polohy poté, co zjistí, že servomotor trimovací plošky zamrznul nebo zasílá chybný zpětný signál. [Scénář 7.5.2]
CFC-7.10	Kabely vedoucí zpětný signál od servomotoru trimovací plošky k jednotce ECU musí vydržet extrémní podmínky vzniklé vlivem nestandartní činnosti pohonné jednotky. [Scénář 7.5.2]
CFC-7.11	Kabely vedoucí vstupní údaje ze silových senzorů k jednotce ECU musí vydržet extrémní podmínky vzniklé vlivem nestandartní činnosti pohonné jednotky. [Scénář 7.5.4; 7.6.2; 9.4.3]
CFC-7.12	Propojovací táhlo jednotky PCA musí vydržet extrémní podmínky vzniklé kombinací nestandartní činnosti pohonné jednotky a vysokého násobku. [Scénář 7.5.4]
CFC-7.13	Jednotka ECU nesmí přerušit ovládání trimovací plošky poté, co posádka stiskla Paddle switch.
CFC-8.1	Teploměry a resolvery musí být pravidelně zkalibrovány, aby odesílaly správné údaje jednotce ECU. [Scénář 8.1.2; 8.2.3; 9.1.3]
CFC-8.2	Odeslání údajů od resolverů do jednotky ECU nesmí být ovlivněno případnými vysokými vibracemi pohonné jednotky (zvýšené vibrace pohonné jednotky nesmí zkreslovat odeslané údaje). [Scénář 8.1.2; 8.2.3; 9.1.3]
CFC-8.3	Odesílání údajů od teploměrů do jednotky ECU nesmí být ovlivněno případnými zvýšenými teplotami od pohonné jednotky (zvýšená teplota pohonné jednotky nesmí zkreslovat odeslané údaje. [Scénář 8.1.2; 8.2.3]
CFC-8.4	Jednotka ECU musí po zapnutí být schopna včas ověřit funkčnost mechanické části PCA (proces vnitřního ověřování nesmí zabrat více než TBD) [Scénář 8.3.1]
CFC-9.1	Jednotka PCA a její součásti se nesmí uvolňovat vlivem zvýšeních vibrací od pohonné jednotky. [Scénář 9.1.4; 9.2.1]
CFC-9.2	Spojka jednotky PCA se musí odepnout bezprostředně poté, co byl vypnut přívod el. energie do jednotky ECU. [Scénář 9.3.2]
CFC-9.3	Jednotka ECU musí umět detekovat případné zaseknutí spojky nebo jeho resolveru [Scénář 9.3.4]

CFC-9.4	Při ztrátě dodávky el. energie do resolverů se bezprostředně musí odepnout spojka. [Scénář 9.3.4]
CFC-9.5	Spojka a elektromotor jednotky PCA se nesmí při intenzivnějším používání přehřívat. [Scénář 9.5.2]
Požadavky a omezení na trasu řídící akce (ze 4. kroku)	
CPC-1.1	Pružinový posilovač musí být pravidelně kontrolován a testován, aby nedošlo k jeho prasknutí během kritické fáze letu. [Scénář 1.3]
CPC-1.2	Mechanická cesta podélného řízení musí být pravidelně kontrolována, aby nedošlo k jejímu rozpojení během letu. [Scénář 1.4; 1.6; 9.9; 9.14]
CPC-1.3	Jednotka PCA nesmí začít působit proti silám vyvolané posádkou. [Scénář 1.5; 1.7]
CPC-2.1	Spínač ovládající dodávku el. energie do jednotky PCA musí být zdvojen nebo pravidelně kontrolován, aby se spolehlivě přerušila dodávka el. energie do jednotky PCA při poruše jednotky PCA (např. vlivem degradace může spínač přestat fungovat). [Scénář 2.1; 3.1; 3.2]
CPC-3.1	Spínače ovládající dodávku el. energie do jednotky PCA musí být pravidelně kontrolovány, aby nepřerušili dodávku el. energie při funkční jednotce PCA v kritické fázi letu (např. vlivem degradace může spínač přestat fungovat). [Scénář 4.1; 9.16]
CPC-3.2	Paddle switche musí být pravidelně kontrolovány, aby se zajistila jejich funkčnost. [Scénář 4.2]
CPC-4.1	Aktuátor trimovací plošky musí být spojen se správnou polaritou k el. obvodu. [Scénář 5.1; 7.1]
CPC-4.2	El. obvod vedoucí k aktuátoru trimovací plošky se nesmí během letu rozpojit. [Scénář 5.2; 5.6]
CPC-4.3	Spínače ovládající dodávku el. energie do aktuátoru trimovací plošky se nesmí zasekávat (např. vlivem degradace). [Scénář 5.3; 5.8]
CPC-4.4	Aktuátor trimovací plošky musí být pravidelně kontrolován, aby se předešlo její mechanické poruše nebo zaseknutí (např. cizími předměty). [Scénář 5.4; 5.7; 7.3; 7.10]
CPC-4.5	Aktuátor trimovací plošky musí reagovat na přijatý signál okamžitě bez výrazných prodlev. [Scénář 5.5; 7.5]
CPC-5.1	Trimovací spínač na řídící páce musí být propojen se správnou polaritou k el. obvodu. [Scénář 6.1]

CPC-6.1	Aktuátor trimovací plošky nesmí začít samovolně pracovat bez vstupu od jednotky ECU. [Scénář 7.2]
CPC-6.2	Aktuátor trimovací plošky musí vydržet i větší zatížení vzniklé aerodynamickými a setrvačnými silami, aniž by se přehřívala. [Scénář 7.7; 7.9]
CPC-7.1	Spojka a elektromotor jednotky PCA musí být připojena k el. obvodu se správnou polaritou. [Scénář 8.1; 9.1; 9.4]
CPC-7.2	Funkčnost spojky a elektromotoru musí být pravidelně kontrolována, aby se předešlo mechanické poruše nebo zaseknutí (např. cizími předměty nebo zadření). [Scénář 8.2; 8.3; 8.5; 9.2; 9.3; 9.7; 9.13]
CPC-8.1	Elektromotor jednotky PCA nesmí začít samovolně pracovat bez vstupu od jednotky ECU. [Scénář 9.5]
CPC-8.2	Jednotka PCA musí vydržet i větší zatížení vzniklé aerodynamickými a setrvačnými silami, aniž by se přehřívala. [Scénář 9.6; 9.11; 9.15]
CPC-8.3	Jednotka PCA musí vydržet extrémní podmínky vzniklé nestandartním chodem motoru (silné vibrace nesmí způsobit odření kabelů). [Scénář 9.6; 9.11; 9.16]
CPC-8.4	Elektromotor a spojka jednotky PCA musí okamžitě reagovat na přijatý el. signál bez výrazných prodlev. [Scénář 9.10]
CPC-8.5	Spojka jednotky PCA se nesmí samovolně odpojovat. [Scénář 9.12]

Příloha 2: RBD diagramy