VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

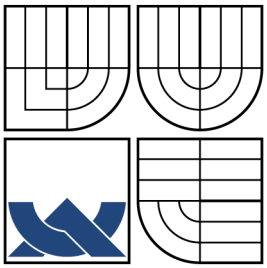
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

VÝBĚR VHODNÉ SBĚRNICE PRO DISTRIBUOVANÝ FLY-BY-WIRE SYSTÉM

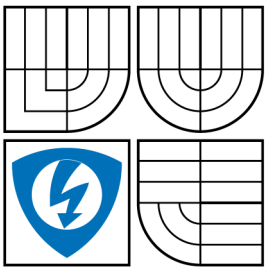
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE MARCEL FUNDERÁK
AUTHOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

VÝBĚR VHODNÉ SBĚRNICE PRO DISTRIBUOVANÝ FLY-BY-WIRE SYSTÉM

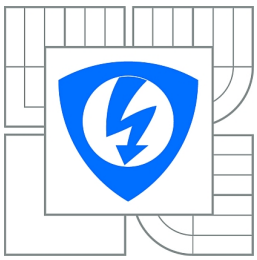
SELECTION OF AIRPLANE DATA BUS FOR DISTRIBUTED FLY-BY-WIRE SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — MARCEL FUNDERÁK
AUTHOR

VEDOUCÍ PRÁCE — ING. RADIM ČÍŽ, PH.D.
SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Marcel Funderák	***ID:***	78448
Ročník:	2	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Výběr vhodné sběrnice pro Distribuovaný Fly-by-Wire systém

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je vybrat vhodnou sběrnici pro účely distribuovaného Fly-by-Wire systému. V rámci práce budou porovnány různé druhy sběrnic a komunikačních protokolů na základě kriterií důležitých pro distribuovaný Fly-by-Wire systém. Pro vybranou sběrnici bude navržena topologie a provedena analýza rizik. Navržený koncept bude podložen simulací komunikace provedenou v prostředí Simulink, která bude využita k analýze zpoždění přenosu mezi komunikačními uzly a ověření předpokládaného dopadu chyb na systém.

DOPORUČENÁ LITERATURA:

[1] PROAKIS, J., G. Digital Communications. 4th ed., New York (USA) : McGraw-Hill, 2001. 1002 p. ISBN 0-07-232111-3.
[2] SPITZER, C., R. Digital Avionics Handbook. 2nd ed., Boca Raton (USA) : CRC Press, 2006. 680 p. ISBN 9780849350085.

Termín zadání:	29.1.2010	***Termín odevzdání:***	26.5.2010

Vedoucí práce: Ing. Radim Číž, Ph.D.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Práce se zabývá výběrem vhodného komunikačního prostředku pro distribuovaný systém řízení letu Fly-By-Wire. Jsou zde definovány vhodné parametry takové sběrnice a uveden popis jednotlivých vhodných sběrnic. S ohledem na definované parametry je vybrána vhodná sběrnice. Dále je uvedena bezpečnostní a časová analýza vybrané sběrnice.

KLÍČOVÁ SLOVA

sběrnice, Fly-by-Wire systém, distribuovaný Fly-by-Wire systém, AFDX, analýza zpoždění, Analýza rizik systému

ABSTRACT

This thesis is dealing with selection of proper airplane data bus for distributed Fly-by-Wire system. The parameters of such data bus are defined here and description of such data buses are given as well. The proper data bus which fulfils the given parameters is selected. Next the safety and time-delay analysis are provided.

KEYWORDS

data bus, Fly-by-Wire system, distributed Fly-by-Wire system, AFDX, Time-delay Analysis, Functional Hazard Assessment

FUNDERÁK, M. *Výběr vhodné sběrnice pro Distribuovaný Fly-by-Wire systém.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 62 s. Vedoucí diplomové práce Ing. Radim Číž, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Výběr vhodné sběrnice pro Distribuovaný Fly-by-Wire systém“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji doktoru Janu Tomášovi za odborné vedení a dohled při zpracování diplomové práce.
Dále děkuji vedoucímu diplomové práce doktoru Radimovi Čížovi za užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne .....

.....
(podpis autora)

OBSAH

Úvod **9**

1 Teoretický úvod do problému **10**
1.1 Úvod . . . 10
1.2 Systém Fly-By-Wire . . . 10
1.3 Distribuovaný systém Fly-By-Wire . . . 12
1.4 Definování parametrů sběrnice . . . 14

2 Sběrnice využívané v avionice **16**
2.1 Controller Area Network Bus . . . 16
2.1.1 Hardwarové vlastnosti . . . 17
2.1.2 Přenosový protokol . . . 17
2.2 MIL-STD-1553B Digital Time Division Command/Response Multiplex Data Bus . . . 18
2.2.1 Hardwarové vlastnosti . . . 19
2.2.2 Přenosový protokol . . . 21
2.3 ARINC 429 . . . 23
2.4 ARINC 664 . . . 24
2.4.1 Koncový uzel . . . 24
2.4.2 Přepínač AFDX . . . 26

3 Výběr vhodné sběrnice **28**
3.1 Definice sledovaných parametrů . . . 28
3.2 Parametry jednotlivých sběrnic . . . 30
3.3 Zhodnocení výběru sběrnice . . . 32

4 Simulace sběrnice AFDX **34**
4.1 Výpočet CRC . . . 34
4.2 Přepínač . . . 35
4.3 Koncový systém . . . 36
4.4 Zhodnocení simulace . . . 37

5 Analýza rizik **38**
5.1 Topologie analyzovaného systému . . . 38
5.2 Pravděpodobnosti chyb v systému . . . 39
5.3 Simulace selhání systému . . . 47
5.4 Vyhodnocení bezpečnosti sběrnice . . . 50

6 Analýza časového zpoždění **51**
6.1 Výpočet zpoždění plánovače 52
6.2 Vyhodnocení analýzy časového zpoždění 52

7 Závěr **55**

8 První příloha **56**
8.1 Stromová struktura chyb systému FHA1A 56
8.2 Stromová struktura chyb systému FHA11 56
8.3 Stromová struktura chyb systému FHA2A 56
8.4 Stromová struktura chyb systému FHA4A 56
8.5 Stromová struktura chyb systému FHA13 56

9 Druhá příloha **57**
9.1 Rozmístění chybových bloků 57

Literatura **58**

Seznam symbolů, veličin a zkratek **60**

ÚVOD

Vývoj v leteckém průmyslu není tak rychlý jak v ostatních technologických odvětvích, což je dáno hlavně tím, že vývoj samotného letadla trvá dlouhou dobu - i 10 let. Toto způsobuje, že nasazování nových technologií do letadel má určitou setrvačnost a přesně nekopíruje nejnovější dostupné technologie.

To, že není možné implementovat nejnovější technologie komunikačních systémů je dáno také specifickými požadavky v leteckém průmyslu a nutností jejich důkladného prověření z hlediska bezpečnosti letu a letového provozu.

Distribuované systémy řízení letu ale představují velký krok dopředu v leteckém průmyslu a představují budoucnost létání jako takového a proto je nutné vývoji těchto systémů věnovat pozornost.

Proto se tato práce se z velké části věnuje výběru vhodné datové sběrnice, která bude určena jako páteřní komunikační prostředek v systému řízení letadla.

V první části bude stručně popsán systém FBW (Fly-By-Wire – druh řídicího systému letadla) jakož i jeho distribuovaná podoba, jejíž vlastnosti budou brány v potaz při výběru vhodné sběrnice. Budou zde rovněž uvedena kritéria, která by měla vhodná sběrnice naplňovat.

Druhá část bude věnována popisu jednotlivých vhodných sběrnic a popisu jejich vlastností s ohledem na definovaná kritéria, která musí splňovat.

Dále je proveden podrobný rozbor definovaných kritérií sběrnic, provedeno srovnání vhodných sběrnic dle těchto parametrů, z kterého je poté určena nejvhodnější sběrnice, která je dále analyzována.

Pro vybranou sběrnici je pak implementován její model v prostředí Simulink, který je použit pro srovnání se závěry provdené bezpečnostní analýzy v následující kapitole. Ta je věnována rozboru jednotlivých možných selhání systému ovlivněných sběrnicí a definování možných elementárních chyb sběrnice. Poté je uveden příklad implementace těchto chyb do modelu sběrnice.

Poslední část je věnována rozboru časového zpoždění vybrané sběrnice.

1 TEORETICKÝ ÚVOD DO PROBLÉMU

1.1 Úvod

V této části bude popsán jak systém FBW, tak i obecný distribuovaný systém a dále zde budou vyvozeny nejdůležitější parametry, jaké musí komunikační systém takovýchto systémů splňovat jak z pohledu technického řešení, tak z bezpečnostního hlediska.

1.2 Systém Fly-By-Wire

Systém řízení letadel je založen na ovládání hlavních řídicích ploch - směrovky, výškovek a křidélek. V důsledku toho je potřeba určitým způsobem převádět řídicí pokyny od pilota (příp. od kopilota) k těmto ovládacím plochám.

V konvenčních systémech jsou ovládací plochy řízené za pomocí mechanických systémů (jako jsou různá táhla, dráty a řetězy), které jsou přímo spojeny s ovládacími prvky letadla - pedály a řídicí sloupek[1]. Toto uspořádání má svou výhodu v tom, že pilot má přímou odezvu z ovládacích ploch. Nevýhoda tohoto systému je v tom, že lze použít jen pro nižší letové rychlosti (při vyšších rychlostech nelze kvůli aerodynamickému tlaku dosáhnout požadovaných výchylek řídicích ploch).

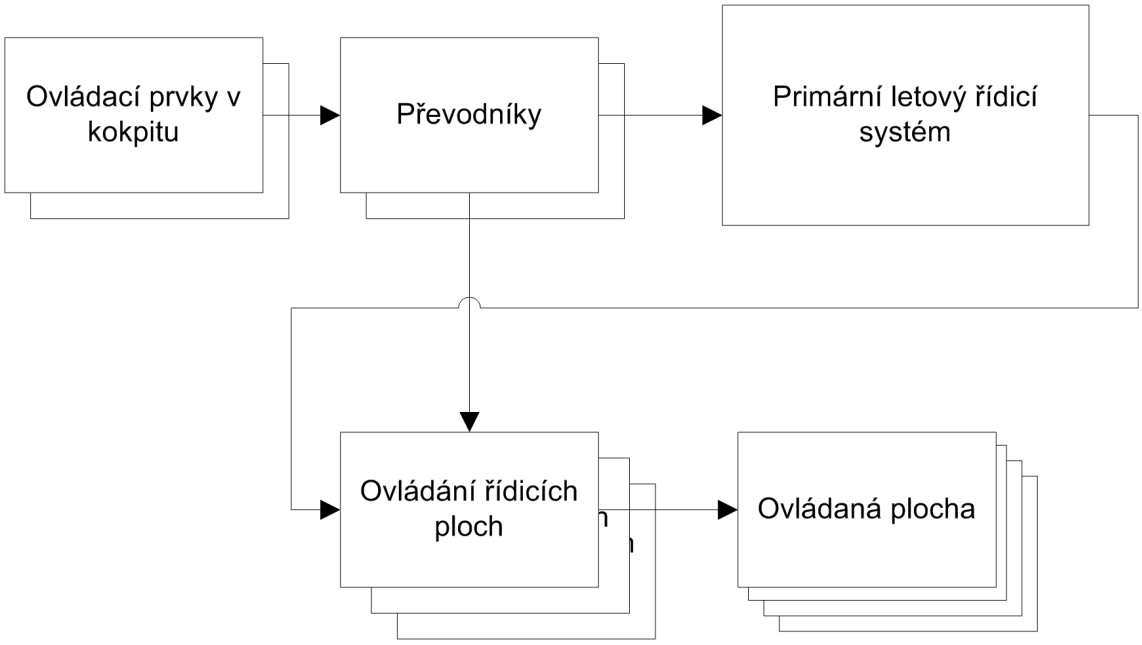
Další vývoj směřoval k mechanicko-hydraulickým systémům. Takovéto systémy obsahují hydraulický systém, který ovládá řídicí plochy. Toto řešení již není závislé na pilotově síle, což umožňuje větší manévrovatelnost letadla i při vyšších letových rychlostech. Nevýhoda tohoto systému spočívá především v jeho značné hmotnosti. Dále je nutno pro zvýšení bezpečnosti letu zdvojit (někdy i ztrojit) hydraulické i mechanické systémy, což se odráží na ceně a navíc dochází k dalšímu zvýšení zatížení letadla. Mezi další nevýhody patří nutnost opakovaných servisních zásahů - zejména promazávání mechanických spojů. Dále je zřejmé, že přídavné systémy jako např. „yaw damper“ (tlumič kmitů směrovky) musí mít své vlastní hydraulické a mechanické systémy, což dále zvyšuje hmotnost celého systému[12].

Dnešní systémy přenášejí povely od pilota k řídicím plochám jako elektrický signál, který ovládá elektro-hydraulické servo spojené mechanicky s řídicí plochou. Tento systém se nazývá Fly-By-Wire – druh řídicího systému letadla. Dále je možné systém upravit tak, že přebírá určité funkce od pilota a tím ho zbavuje nadbytečné zátěže. FBW systém poskytuje následující výhody oproti konvenčním mechanicko-hydraulickým systémům[12]:

[1] Někdy označován také jako knipl

- Celkové snížení hmotnosti řídicího systému letadla
- Sdružení několika separovaných systémů do jednoho
- Podstatné zlepšení ovladatelnosti letadla
- Jednodušší údržba
- Jednodušší výroba
- Snadnější přidávání nových funkcí do již dokončeného letadla

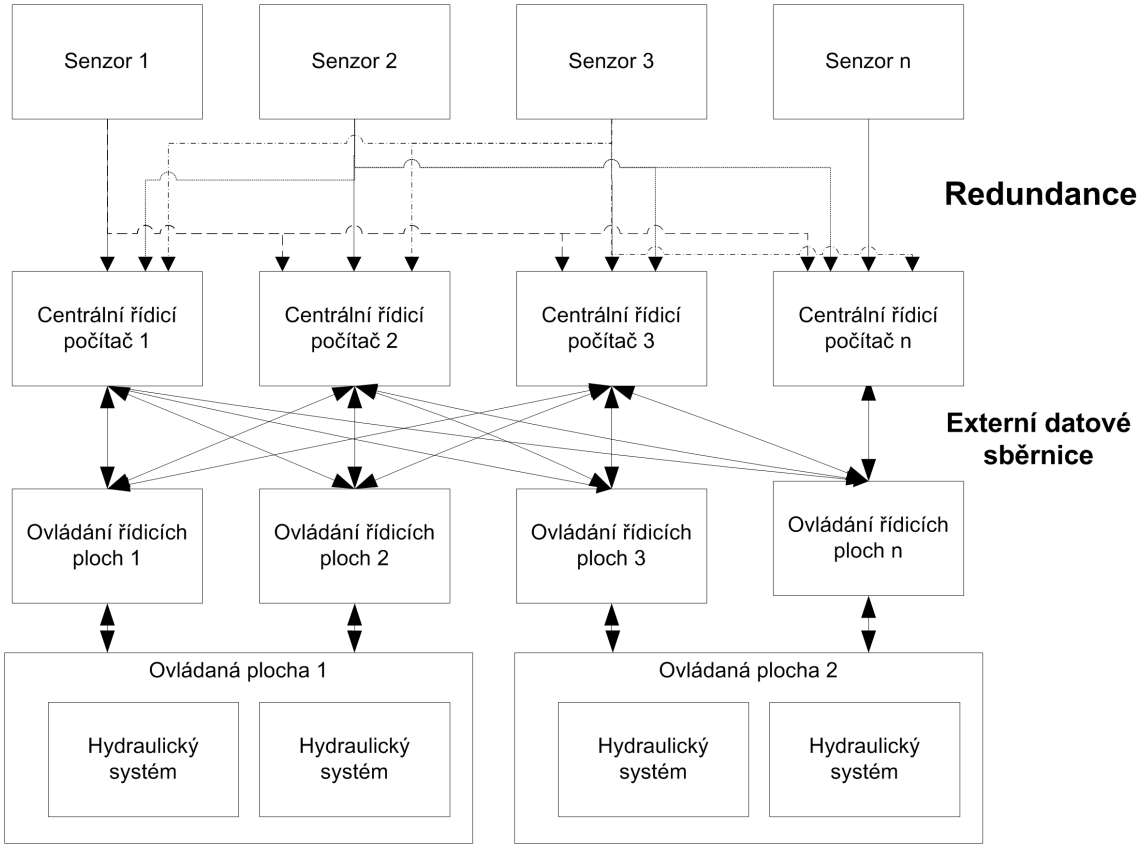
Základní schéma centralizovaného systému FBW je uvedeno na obr. 1.1. Takovýto systém umožňuje implementaci ochrany před překročením letové obálky[2](pomocí úpravy pokynů od pilota) a tím zvýšení bezpečnosti letu. Dále systém poskytuje možnost utlumení nežádoucích signálů od pilota[3] a provádění úkonů, jež by od pilota vyžadovaly stálé úsilí (např. trimování[4] - toto je možné i u konvenčních systému, ale je to nutné řešit přidáním speciálních systémů, kdežto u FBW může být implementováno jako samostatná funkce) - tím se snižuje zátěž pilota.



Obr. 1.1: Zjednoušené schéma FBW.

[2]Konstrukční limity letadla v závislosti na přetížení, rychlosti, ...
[3]Pilot-induced oscillation - pilotem vyvolané oscilace.
[4]nastavení ovládané plochy do stálé pozice

Na obr. 1.2 je uvedeno blokové schéma primárního letového řídicího systému při použití centralizovaného systému FBW ve kterém je obsažena většina funkcí ovládání letadla - tento systém je značně složitý a vyžaduje množství propojení s okolními systémy. Dále je běžné, že systém je v letadle duplikován[6] pro zvýšení celkové bezpečnosti a z toho vyplývá nutnost synchronizace mezi těmito redundantními systémy. Letový počítač obsahuje svou vnitřní sběrnici pro přenos dat, což přidává na jeho složitosti. Takovýto systém je již obsažen v mnoha současných letadlech, která jsou v provozu[5].



Obr. 1.2: Blokové schéma centralizovaného FBW systému.

1.3 Distribuovaný systém Fly-By-Wire

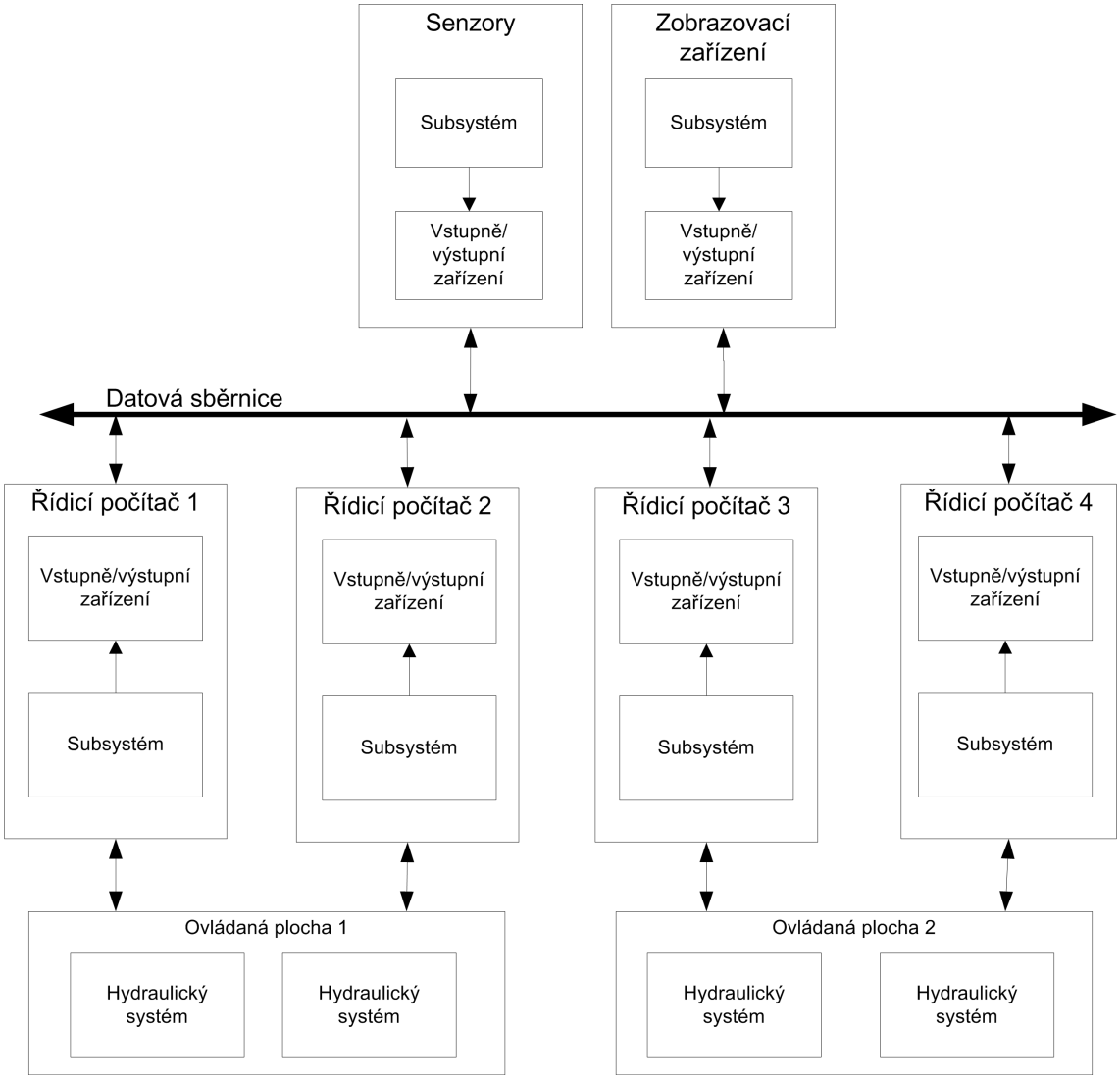
Pokud jednolitý systém rozdělíme do několika samostatných funkčních bloků (ne nutně se stejnou složitostí a funkcí), dostaneme distribuovaný systém FBW. Takovéto rozdělení je naznačeno na obr. 1.3.

Tato distribuce spočívá především v přenesení některých nebo všech výpočetních úkonů z centrálního řídicího systému směrem k jednotlivým řídicím jednotkám

[5]např. Boeing 777, Airbus A340, Dassault Falcon 7X

ovládaných ploch. Tímto postupem může být centrální řídicí systém/počítač úplně vynechán. Poté ale vznikne potřeba zvýšené komunikace mezi jednotlivými řídicími jednotkami - navzájem si poskytují data a mohou se ovlivňovat.

V důsledku toho je potřeba v takovémto systému umístit komunikační sběrnici, která by tuto komunikaci umožňovala.



Obr. 1.3: Blokové schéma distribuovaného FBW systému.

1.4 Definování parametrů sběrnice

Sběrnice vhodná pro nasazení v distribuovaném FBW systému by měla splňovat následující kritéria:

- Vysoká míra bezpečnosti
- Dostatečná datová propustnost mezi jednotlivými uzly systému
- Transparentnost pro vyšší vrstvy systémů na jednotlivých uzlech[6]
- Možnost adresovat všechny uzly z kteréhokoliv uzlu
- Nízká hmotnost
- Jednoduchost nasazení
- Možnost rozšíření systému o další uzly
- Snadná výměna komponent (při údržbě)
- Systém sběrnice musí být schopen projít certifikačním procesem[7].

Vysoká míra bezpečnosti V případě leteckých systémů je bezpečnost na prvním místě. Je proto nutné zajistit, aby komunikační sběrnice byla schopna zajistit dostatečnou míru integrity dat - tzn. poškozená/chybná data se nesmějí dostat k příjemci zprávy, pokud nejsou označena jako chybná. Pravděpodobnost takového selhání by neměla být větší než 10^{-11}. Dále je nutné zajistit vysokou dostupnost komunikačního systému.

Dostatečná datová propustnost Letecké systémy nejsou tolik náročné na dostatečnou šířku pásma pro přenos jako jiné technologie, ale s ohledem na budoucí rozšiřování systému a větší množství obsažených uzlů by sběrnice měla dosahovat přenosových rychlostí alespoň 100 kbit/s.

Transparentnost Pro usnadnění návrhu systémů vyšších vrstev by pro ně měla být komunikační vrstva co nejvíce transparentní. Systémy navazující na komunikační vrstvu tedy pouze předávají svá data pro jiné uzly a spoléhají na zajištění kvality služby od tohoto komunikačního systému. Vyšší vrstvy systému tak nemusí mít podrobný přehled o komunikačním systému, což umožňuje snazší implementaci koncových zařízení a tím snížení nákladů na uvedení systému do provozu

[6] vyšší vrstva systému nemusí mít znalost o uspořádání komunikační vrsrtvy

[7] např. u FAA (Federal Aviation Administration, USA) nebo EASA (European Aviation Safety Agency)

Nízká hmotnost Z ekonomických důvodů jsou všechny systémy letadla konstruovány i s ohledem na jejich hmotnost, proto by komunikační systém měl být co nejjednodušší - obsahovat co nejmenší počet součástí (avšak nesmí tím utrpět bezpečnost). Proto by také měl být co nejmenší počet fyzických spojů mezi jednotlivými uzly systému.

Certifikace Všechny zde uváděné druhy komunikačních sběrnic byly již v minulosti nasazeny v leteckém průmyslu. Proto již byly certifikovány pro použití v leteckém průmyslu.

2 SBĚRNICE VYUŽÍVANÉ V AVIONICE

2.1 Controller Area Network Bus

Sběrnice Controller Area Network[1] je používána hlavně v automobilovém průmyslu, ale její použití v leteckém průmyslu je také možné. Tato sběrnice je založena na sériovém principu (jednotlivé uzly jsou řazeny za sebou).

Sběrnice má následující hlavní vlastnosti[10]:

- přístup na sběrnici podléhá prioritě zprávy
- nedestruktivní rozhodování o výběru přenášené zprávy
- všesměrové rozesílání rámců (jednotlivé uzly je pak filtrují)
- možnost požádat vzdálený uzel o data
- volnost v nastavení parametrů
- jednotnost dat v celém systému
- detekce chyb a jejich ohlašování
- automatický nový přenos rámců s nižší prioritou a těch, co obsahovaly chybu
- rozlišování mezi dočasnými a trvalými chybami v přenosu, schopnost vypnout špatné uzly.

Po CAN sběrnici jsou přenášeny rámce s různou, zato však omezenou délkou. Tyto mají vždy stejný formát a mohou být vyslány kterýmkoliv z uzlů, pokud je zrovna sběrnice bez provozu. Pokud nastane situace, kdy chtějí komunikovat dva uzly zároveň, je toto řešeno výběrem uzlu s vyšší prioritou, který dále pokračuje v komunikaci (druhý přestává okamžitě přenášet data) - tímto při kolizi nedojde k žádné ztrátě dat ani času.

Na sběrnici CAN jsou jednotlivé přenášené bity označené jako dominantní - logická „0“, nebo recesivní - logická „1“. Úrovně signálů nejsou standardem definovány. Uzel při zápisu na sběrnici provádí bitový součin[2] s hodnotou na sběrnici a zároveň všechna data ze sběrnice čte (čtení provádí všechny uzly). Pro toto volení prioritního uzlu je určeno pole pojmenované Arbitration Field („volební pole“), které obsahuje identifikátor (označení obsahu zprávy) a RTR BIT (rozlišení, zda jde o Data Frame nebo Remote Frame). Pokud však při přenosu zprávy dojde ke kolizi (uzel vyslal

[1] dále jen CAN
[2] AND

recesivní bit, ale čte dominantní), uzel přestává dále vysílat a o opakovaný přenos se pokusí až po uvolnění sběrnice[7].

Přenos po CAN je pro všechny uzly konzistentní[3], protože přenos všech rámců je prováděn všesměrově a je prováděno chybové hlášení vadných rámců. Dále sběrnice CAN umožňuje, aby uzel požádal jiný uzel o data pomocí rámce Remote Frame. Tázaný uzel odpoví pomocí Data Frame se stejným identifikátorem zprávy.

Detekce chyb přenosu se provádí pomocí následujících opatření:

- monitorování sběrnice (dominantní a recesivní bity na sběrnici a v posílané zprávě)
- 15 bitová CRC
- vkládání bitů (po každých 5 stejných bitech se vloží jeden bit opačné hodnoty)
- kontrola rámců
- kontrola pomocí ACK.

Pokud je zaznamenán chybný rámec (ať vysílacím uzlem, nebo kterýmkoliv přijímacím uzlem), je tento označen jako chybný a zahozen. Poté je přenos opakován.

Vadný uzel může být od sběrnice automaticky odpojen, takže nemůže přijímat ani vysílat žádné rámce.

2.1.1 Hardwarové vlastnosti

Použití konkrétní fyzické vrstvy není pro sběrnici CAN definováno.

2.1.2 Přenosový protokol

Typy rámců na sběrnici CAN:

- Data Frame
- Remote Frame
- Error Frame
- Overload Frame.

Datový rámec (Data Frame) obsahuje Start of Frame (počátek rámce) - jeden dominantní bit. Dále volební pole (Arbitrary Field) - vysvětleno v úvodu kapitoly, kontrolní pole (Control Field) - 6 bitů značících počet bytů v datovém poli (využity

[3] všichni „vidí“ vše, nebo nic

jsou tu jen 4 bity, 2 jsou rezervovány), pak datové pole (Data Field), CRC pole - 15 bitů CRC a jeden bit jako CRC Delimiter (tento je nastaven jako recesivní). Za těmito je pak ACK pole sestávající z jednoho bitu pro označení správně přijaté zprávy a jednoho bitu pro ACK Delimiter (opět recesivní bit). Konec datového rámce představuje 7 recesivních bitů po sobě.

Remote Frame (žádost o poslání dat) rámec se od datového rámce liší v tom, že neobsahuje žádné datové pole a v Arbitrary Field má RTR BIT nastaven jako recesivní.

Chybový rámec (Error Frame) obsahuje dvě pole: první se skládá z chybových hlášení od jednotlivých stanic a druhé je Error Delimiter sestávající z 8 následných recesivních bitů.

Overload Frame (rámec přetížení) obsahuje stejně jako chybový rámec dvě pole: první je Overload Flag - 6 dominantních bitů a druhé je Overload Delimiter - 8 recesivních bitů. Overload Frame může přijímací stanice vyslat, pokud potřebuje pozdržet vyslání dalších datových rámců. Po sobě mohou následovat maximálně 2 rámce přetížení.

Jednotlivé bity jsou na sběrnici kódovány kódem NRZ

2.2 MIL-STD-1553B Digital Time Division Command/Response Multiplex Data Bus

Sběrnice podle standardu MIL-STD-1553B[4], vyvinutého americkou armádou, je určena pro přenos signálů a zpráv mezi jednotlivými systémy a subsystémy letadel. Počátky vývoje tohoto standardu jsou datovány ke konci 60. a začátku 70. let 20. století, kdy se neustále zvyšoval počet jednotlivých systémů letadla a jejich vzájemné propojení se stalo velkým problémem. Navíc bylo nadmíru složité takovéto systémy rozšiřovat.

Proto byl v roce 1973 vydán standard MIL-STD-1553, následován revizí A v roce 1975 a nakonec revizí B (aktuální verze) v roce 1978, který definuje sběrnici, umožňující vzájemnou komunikaci leteckých systémů[12].

Tento standard je založený na časovém multiplexování (TDM, Time Division Multiplex). Tato metoda umožňuje využití jediného komunikačního kanálu pro větší množství jednotek a proto tak šetří množství spojovacích kabelů a konektorů nutných k propojení všech systémů.

[4] v této kapitole zkráceně jen standard

2.2.1 Hardwarové vlastnosti

Podle standardu jsou definovány 4 jednotky datové sběrnice: přenosové médium, vzdálený terminál, řídicí terminál a monitorovací terminál. V tab. 2.1 jsou uvedeny nejdůležitější hardwarové parametry datové sběrnice podle standardu MIL-STD-1553B.

Frekvence	1 MHz
Délka slova	20 bitů
Počet datových bitů ve slově	16 bitů
Délka zprávy	Maximálně 32 slov ve zprávě
Technika přenosu	Poloviční duplex
Mód	Asynchronní
Kódování	Bipolární Manchester
Kontroler sběrnice	Jeden nebo více
Počet vzdálených terminálů	Maximálně 31
Přenosové médium	Stíněná kroucená dvoujlinka
Zapojení terminálů	Přímo, nebo galvanicky oddělené

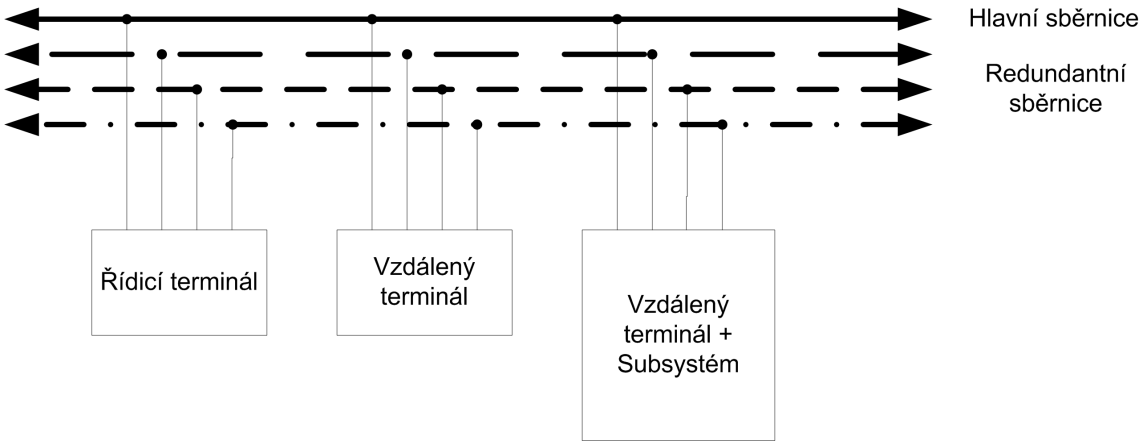
Tab. 2.1: Hardwarové vlastnosti datové sběrnice podle MIL-STD-1553B

Přenosové médium Přenosové médium (sběrnice) je tvořeno stíněnou kroucenou dvojlinkou, která je použita jak na hlavní vedení, tak pro odbočení k jednotlivým koncovým terminálům. Každé odbočení obsahuje právě jeden terminál a je nutné ho ukončit charakteristickou impedancí Z_0. Tímto sběrnice získá vlastnosti nekonečného vodiče a nebudou se na ní projevovat odrazy signálů na konci vodičů. Jenže odbočení k terminálům mění charakteristickou impedanci sběrnice, proto je nutné s každým dalším odbočením měnit i přizpůsobení vodičů. Toto se stává tím složitější, čím máme více terminálů.

Terminály můžeme podle standardu připojit na hlavní vedení jak přímo, tak galvanicky oddělené za použití vhodného oddělovacího transformátoru. Pokud terminál připojíme přímou metodou, může být jeho vzdálenost od hlavního vedení pouze 1 stopa[5]. Jestliže však využijeme galvanického oddělení, vzdálenost vzroste na 20 stop[6]. Tyto vzdálenosti musí být vzaty do úvahy při návrhu rozmístění jednotlivých systémů podél hlavní sběrnice a v trupu letadla.

[5] 30,48 cm
[6] 609,6 cm

Vzdálený terminál Vzdálený terminál je vše ostatní na sběrnici, co není řídicím terminálem ani monitorovacím terminálem. Je to takové zařízení, co předává a posílá data ke zpracování k jemu připojenému subsystému. Vzdálený terminál může být implementován jako samostatná jednotka, ale také může být i jako součást daného subsystému, jak je vidět na obr. 2.1.



Obr. 2.1: Připojení jednotlivých zařízení na sběrnici MIL-STD-1553B.

Vzdálený terminál většinou obsahuje přijímač, kodér/dekodér, protokolový kontroler, zásobník na příchozí/odchozí zprávy a rozhraní pro komunikaci s přidruženými subsystémy. Ke zvýšení redundantnosti jsou některé části obsaženy vícekrát.

Pro správnou komunikaci vzdáleného terminálu s řídicím terminálem je potřeba, aby vzdálený terminál byl schopen správně odpovídat na řídicí signály a také musí umět detekovat chyby vzniklé při přenosu a vysílat svůj stav pomocí stavových zpráv.

Komunikace vzdáleného terminálu je řízena pouze řídicím terminálem - zprávy vysílá pouze na požadavek. Dále nesmí při chybně přijaté zprávě tato data předat dále ke zpracování subsystému.

Řídicí terminál Dle standardu je řídicí terminál zodpovědný za řízení komunikace po sběrnici. Takovýto terminál musí být na sběrnici aktivní pouze jeden, jinak by docházelo k chybám při přenosu. V systému však může být více zařízení schopných vykonávat funkci řídicího terminálu - v případě výpadku původního terminálu ho dokáží nahradit a tím zajistit další bezproblémový chod celého zařízení.

Stejně jako koncový terminál může být řídicí terminál součástí jiného zařízení a tím dále šetřit množství nutných rozhraní.

Řídicí terminál může být navržen ke zpracování tří typů komunikace:

- zpracování slov
- zpracování zpráv
- zpracování rámců.

Zpracování slov je nejjednodušší typ řídicího terminálu a dnes se používá jen zřídka. U tohoto typu se přenáší najednou pouze jednotlivá slova a jejich zpracování je úlohou pro přidružený řídicí systém.

Při zpracování zpráv jsou již přenášeny celé zprávy najednou a rozhraní řídicího terminálu komunikuje s řídicím systémem pouze na konci jednotlivých zpráv nebo pokud dojde k chybě při přenosu. Jednotlivé zprávy jsou doprovázeny kontrolními slovy.

Nejmodernější typy řídicích terminálů jsou schopny zpracovávat několik zpráv najednou - tzv. rámců.

Monitorovací terminál Tento typ terminálu podle standardu přijímá všechny (nebo jen vybrané) zprávy na sběrnici a zpracovává je pro další použití - záznam průběhu letu, údržba, atp.

Pokud tento terminál přijímá data, musí stejně jako vzdálený terminál provádět jejich ověřování a o případných chybách v přenosu informovat přidružený subsystém.

2.2.2 Přenosový protokol

Standard MIL-STD-1553B definuje tři druhy posílaných zpráv:

- řídicí slovo
- stavové slovo
- datové slovo.

Všechny tři druhy mají podobnou strukturu, ale navzájem se liší svým obsahem a podle toho jsou také interpretovány. Každé slovo má 20 bitů. Z toho jsou první 3 bity určeny k synchronizaci (nastavení časového signálu v dekodéru), dalších 16 bitů je použito pro informační pole a poslední bit slouží k určení liché parity tohoto slova.

Jednotlivé přenášené bity jsou kódovány pomocí Manchester kódování - logická „0“ je kódována jako přechod z nízké úrovně do vysoké a logická „1“ naopak. Tento přechod se nachází v polovině časového rámce určeného pro jednotlivý bit. Dále je tímto kódováním zajištěna nulová stejnosměrná úroveň signálu - takovýto signál je vhodný pro přenos případnými oddělovacími transformátory na vedlejších větvích sběrnice.

Přijímač v každém typu terminálu předává připojenému subsystému pouze 16 bitů obsažených v informačním poli, avšak poskytuje mu informace o správnosti parity a průběhu synchronizace.

Synchronizační pole obsahující 3 bity je tvořeno kmitem, který neodpovídá kódování Manchester[8] - díky tomuto poli je dekodér schopný obnovit svou synchronizaci na začátku každého slova a udržet tak stabilitu přenosu. Řídicí a stavová slova mají v synchronizačním poli kladnou úroveň po dobu trvání 1,5 bitu a zápornou úroveň v následujícím úseku stejné délky, datová slova naopak.

Řídicí slovo je pokynem pro vzdálený terminál a je vysíláno pouze aktivním řídicím terminálem. Toto slovo obsahuje informačním poli 5 bitů s adresou terminálu (31 možných adres terminálů, hodnota 11111_2[7] je určena pro všesměrové vysílání). Další bit označuje Vysílací/Přijímací režim (z pohledu vzdáleného terminálu). Následujících 5 bitů je určeno pro podadresu/řídicí režim. Posledních 5 bitů informačního pole nese informaci o čítači slov/číslu módu.

Datové slovo má na rozdíl od řídicího slova opačný synchronizační signál. V informačním poli je všech 16 bitů určeno pro přenášená data. Standard nedefinuje, jak mají být data interpretována, vše záleží na návrhu systému. MSB je přenášen jako první.

Stavové slovo je přenášeno vzdáleným terminálem jako reakce na správně přijatou zprávu - je zde použito jako kontrola správnosti přenosu a také k přenosu informací o vzdáleném terminálu.

Komunikace mezi jednotlivými systémy na sběrnici probíhá za pomocí zpráv. Veškerou komunikaci řídí a začíná řídicí terminál (i pro komunikaci mezi jednotlivými vzdálenými terminály). Tyto mohou být přenášeny těmito směry:

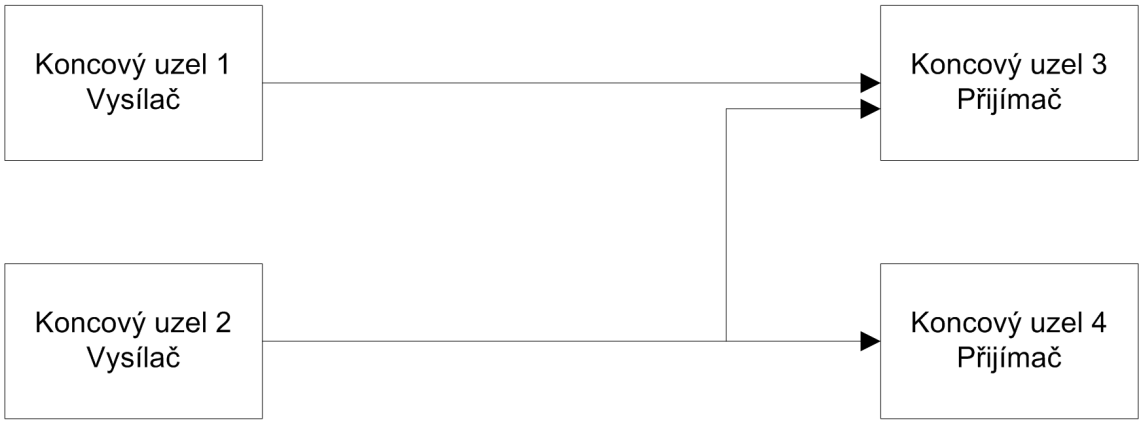
- Řídicí terminál - Vzdálený terminál
- Vzdálený terminál - Řídicí terminál
- Vzdálený terminál - Vzdálený terminál.

[7] index „2“ označuje dvojkovou soustavu

2.3 ARINC 429

Sběrnice dle standardu ARINC 429, plným názvem Mark 33 Digital Information Transfer System (DITS) je velmi široce používaná v mnoha dnešních letadlech. Její první specifikace byla publikována roku 1978.

Na obr. 2.2 je vyobrazen základní princip přenosu zpráv na sběrnici ARINC 429. Zprávy jsou posílány jen jedním směrem po samostatných médiích - na jedné přenosové lince je jen jeden vysílač a až 20 přijímačů.



Obr. 2.2: Základní topologie sběrnice ARINC 429.

Zprávy jsou na sběrnici posílány jako 32 bitová slova, kde prvních 8 bitů je označení typu slova. Bity 9 a 10 jsou využívány k označení přijímače/vysílače[8].

Bity 11 - 29 nesou samotný obsah zprávy - její význam záleží právě na označení typu slova a číselné hodnoty zde mohou být reprezentovány jak binárním číslem, tak i binárně kódovaným decimálním číslem[9]. Bity 30 a 31 slouží podle druhu vysílané zprávy k označení znaménkové konvence (plus/mínus, sever/jih, ...) přenášených dat nebo také k určení statutu zprávy.

Bit 32 každého vysílaného slova se používá k nastavení liché parity - pokud je zpráva přenesena s chybou, přijímač ji zahodí.

Bitová rychlost Sběrnice podporuje dvě rychlosti přenosu:

- Pomalý - 12-14,5 kbit/s
- Rychlý - 100 kbit/s.

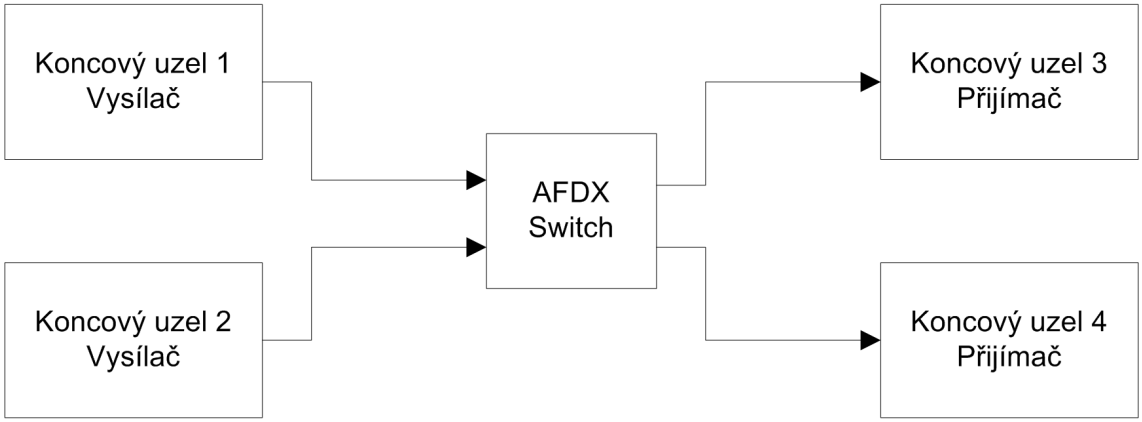
Jako fyzické médium slouží u sběrnice stíněná kroucená dvojlinka. Tento typ média vykazuje vysokou integritu přenosu a má nízkou pravděpodobnost chybovosti[2]. Pro další zvýšení integrity dat je možno přidat kontrolu pomocí CRC.

[8]Source/Destination Identifier
[9]Binary Coded Decimal

Sběrnice ARINC 429 využívá pro kódování signálu na fyzickém médiu bipolární signál s návratem k nule[10], kde logická „1“ je kódována pomocí vysoké úrovně signálu v první půlce trvání jednoho bitu a v druhé je úroveň rovna 0. Logická „0“ má naopak v první polovině intervalu nízkou (zápornou) úroveň.

2.4 ARINC 664

Sběrnice dle standardu ARINC 664, část 7[3] je založena na technologii Ethernet. Tato je definována široce používaným standardem IEEE 802.3 který definuje fyzickou vrstvu a podvrstvu přístupu k médiu[11] linkové vrstvy. Sběrnice ARINC 664, komerční název firmy Airbus v angličtině: Avionics Full-Duplex Switched Ethernet - AFDX, je deterministická síť tvořená uzly a přepínači vhodná pro nasazení v leteckém průmyslu. Zjednodušená topologie sběrnice AFDX je na obr. 2.3.



Obr. 2.3: Základní topologie sběrnice AFDX.

2.4.1 Koncový uzel

Hlavní úlohou koncového uzlu je poskytování spolehlivé a bezpečné komunikace řídicím systémům k nim připojeným. Jelikož je v datové komunikaci řídicích systémů potřeba přenášet data se stejnou prioritou (není zde rozdíl v kategoriích dat), musí takovýto koncový uzel poskytovat garantovanou službu:

- garantování maximálního zpoždění vysílač-přijímač
- garantování minimální šířky pásma
- garance nepřekročení maximální hodnoty jitter[12].

[10]Return-to-zero
[11]MAC - Media Acces Control
[12]jitter - odchylka mezi jednotlivými hodnotami zpoždění v datovém toku

Virtuální linka Pomocí virtuálních linek (VL) je zajištěna determinovanost přenosu z pohledu linkové vrstvy. Tyto linky představují zapouzdření přenosu do jednotlivých kanálů. Koncový uzel může být buď zdrojem, nebo příjemcem VL. Avšak těchto VL může z/do koncového uzlu vystupovat/vstupovat více. VL může mít pouze jeden zdroj, ale více příjemců (představuje jednosměrný tok dat 1:M) a má svou definovanou šířku pásma, přidělenou při návrhu systému. Tímto je zajištěna šířka pásma pro různé směry přenosu.

Každá VL má definovány dva parametry: BAG[13] a jitter. Pokud má vysílající koncový uzel více VL, pak je potřeba pomocí časového multiplexu rámce těchto VL skládat za sebou - tento způsob přenosu se projeví zvýšením jitteru (je způsoben plánovačem multiplexování). Tento jitter však musí být maximálně 500 μs, což při velkém počtu VL a objemných rámcích klade vysoké nároky na vhodnou implementaci plánovače.

Na VL lze vkládat dle standardu rámce o velikosti o maximální velikosti 1518 B. BAG může nabývat hodnot od 1 ms do 128 ms (ale pouze hodnoty mocnin 2). Z tohoto plyne, že maximální přenosová rychlost jedné VL (na linkové vrstvě) je

$$R = (1518/0{,}001)/1024 = 1482{,}42 \text{ [kB/s]}.$$

Proto nemůžeme určit celkovou nejvyšší rychlost sítě, ale naopak můžeme určit nejvyšší možný počet VL v dané síti - toto záleží na volbě fyzické vrstvy[14].

Zpoždění Z pohledu vysílače je zpoždění definováno jako časový interval mezi příjmem posledního bitu ze zdroje signálu a vysláním posledního bitu ethernetového rámce na médium. Toto zpoždění musí být nejvýše 150 μs.

Zpoždění u přijímače je interval mezi přijetím posledního bitu z ethernetového rámce a časem, kdy je poslední bit daných dat poslán ke zpracování cílovou stanicí. Toto zpoždění musí být rovněž nejvýše 150 μs.

Adresování Každý koncový uzel, který vysílá, musí mít přidělenu svou unikátní MAC[15] adresu. Při posílání rámců se použije cílová MAC adresa dle tab. 2.2 a zdrojová adresa dle tab. 2.3. ID rozhraní se volí pouze z hodnot: 001_2 a 010_2. Tyto pak označují využití dvou různých fyzických připojení - redundance.

Redundance Jelikož jednotlivé linky mezi koncovými uzly a přepínačem a taky samotné přepínače mohou selhat, je přenos dat uskutečňován pomocí dvou nezávislých fyzických spojení.

[13] Bandwith Allocation Gap – časový interval generování rámce - minimální časový odstup mezi následujícími rámci v jedné VL

[14] Např. pro 100BASE-TX je teoretické maximum 69 VL

[15] Media Access Control

48 bitů	
Konstantní pole 32 bitů	ID VL 16 bitů
xxxx xx11 xxxx xxxx xxxx xxxx xxxx xxxx	-

Tab. 2.2: Multicastová cílová MAC adresa AFDX, ID VL se přidělí při návrhu systému

48 bitů			
Konstantní pole	ID koncového uzlu	ID rozhraní	Konstantní pole
24 bitů	16 bitů	3 bity	5 bitů
0000 0010 0000 ...	xxxx xxxx xxxx xxxx	yyy	00000

Tab. 2.3: Zdrojová MAC adresa AFDX, ID koncového uzlu se vhodně přidělí při návrhu systému

Jednotlivé ethernetové rámce jsou očíslovány od 1 do 255 a poslány po dvou linkách. Takovéto rámce pak dorazí do koncového uzlu, který poté předá ke zpracování první správný rámec dané sekvence.

2.4.2 Přepínač AFDX

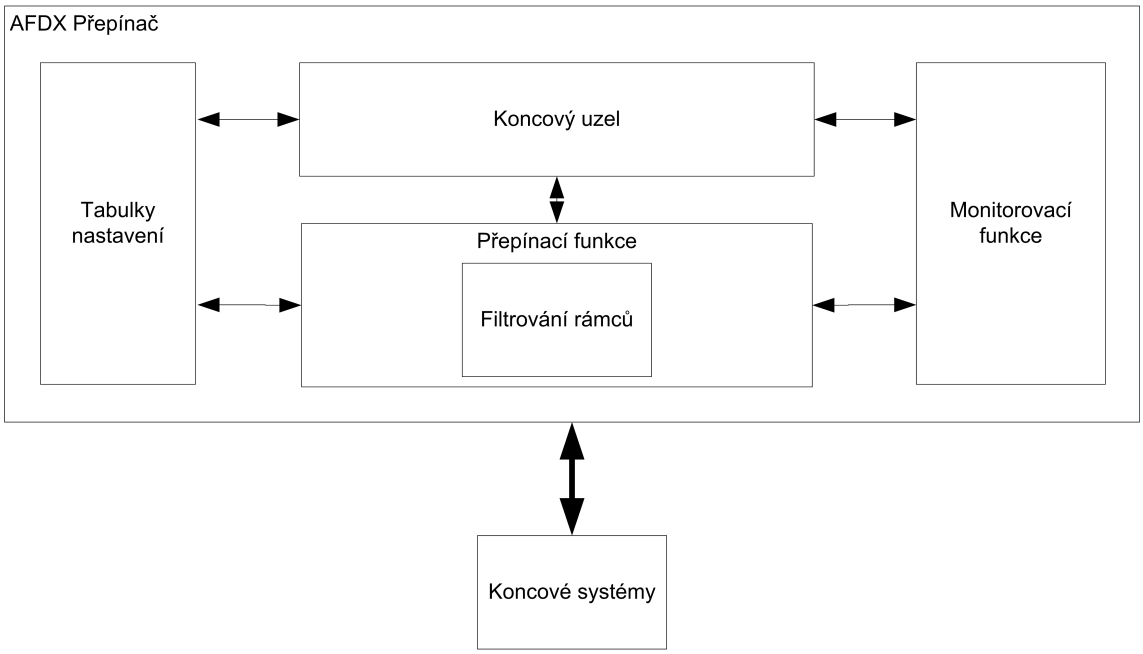
Na obr. 2.4 je uvedeno blokové schéma AFDX přepínače. AFDX přepínač obsahuje 5 hlavních funkcí, které mezi sebou komunikují. Příchozí rámce jsou nejprve filtrovány na základě pravidel uvedených v příslušné tabulce nahrané do programu přepínače.

Dále jsou rámce zpracovány přepínací funkcí a poslány na příslušný výstupní port. Toto přepínání je také řízeno podle údajů v tabulce.

V přepínači je obsažena monitorovací funkce, která zaznamenává různé události - příchody rámců, chybné CRC a z těchto údajů sestavuje statistiky, které mohou být využity nezávislou monitorovací funkcí sítě.

Přepínač dále obsahuje koncový uzel pro možnost komunikace s ostatními prvky sítě - možnost nahrání konfiguračních tabulek.

Hlavní úlohou přepínače je zajištění správného pořadí vysílaných rámců, aby zůstala zachována správná sekvence.



Obr. 2.4: Blokové schéma AFDX přepínače.

3 VÝBĚR VHODNÉ SBĚRNICE

Pro výběr vhodné přenosové sběrnice byly odvozeny z 1.4 a zadavatelem definovány následující parametry a jejich váhy:

- Bezpečnost (váha 9)
- Přenosová rychlost (váha 5)
- Hmotnost systému (váha 7)
- Implementace (váha 5)
- Propojitelnost uzlů (váha 7)
- Údržba systému (váha 3).

Tyto vlastnosti jsou dále popsány pro jednotlivé datové sběrnice, které poté mají přiřazenou bodovou hodnotu podle splnění definovaného kritéria. Pro dostatečné rozlišení byly vybrány následující hodnoty bodů za splnění kritérií:

- 9 - Splňuje výborně
- 7 - Splňuje nadprůměrně
- 5 - Splňuje průměrně
- 3 - Splňuje podprůměrně
- 1 - Splňuje nevyhovuje.

3.1 Definice sledovaných parametrů

Bezpečnost Bezpečnost je komplexní parametr určující celkovou bezpečnost systému sběrnice. Zahrnuje jednak celkovou bitovou chybovost - Bit Error Rate (která je v případě dokonalého systému nulová) tak i celkovou náchylnost systému na chyby jako jsou výpadky napájení, selhání kabeláží i jednotlivých řídicích prvků (pokud jsou obsaženy). Systém, v němž nejsou centrální prvky je v tomto případě považován za bezpečnější, jelikož tyto nemohou selhat. Při hodnocení bezpečnosti systému uvažujeme zejména na následující parametry:

- Bitová chybovost
- minimální počet součástí - menší pravděpodobnost poruchy
- neexistence centrálního uzlu, pokud je potřeba, měl by být redundantní

Z pohledu zadavatele je tento parametr kritický a je na něj proto při výběru sběrnice brán největší zřetel - má největší váhu. Váha nastavena na 9.

Rychlost přenosu Rychlost přenosu je dána největší možnou dosažitelnou rychlostí komunikace mezi jednotlivými komunikujícími uzly. Průměrná dosažitelná rychlost je stanovena na 1 Mbit/s. Takováto rychlost je z pohledu celého systému dostačující pro přenos všech důležitých parametrů. Při této rychlosti je možné například přenést přibližně 30 32-bitových parametrů 1000x za sekundu, nebo analogicky více parametrů méně často. Vyšší rychlosti pak umožňují případné rozšíření systému v budoucnosti a také snadnější implementaci systému - vyšší systémy nejsou omezeny přenosovou rychlostí.

Přenosová rychlost byla hodnocena jako průměrná vlastnost vybrané sběrnice, jelikož definuje průměrně důležitou vlastnost systému. Váha nastavena na 5.

Hmotnost systému Tato vlastnost vybrané sběrnice je důležitá především z pohledu provozovatele konkrétního letadla, ve kterém by sběrnice byla umístěna. Zákazník požaduje co nejmenší hmotnost celého systému z ekonomických důvodů - letadlo s nižší hmotností spotřebuje méně paliva nebo je v něm možno přepravit větší množství nákladu.

Hmotnost systému je dána jednak celkovou hmotností kabeláže, tak i jednotlivých centrálních prvků a možných karet rozhraní. Hodnotí se především fyzická struktura sítě - pokud je možné připojit všechny prvky systému na jediný kabel (sběrnicová struktura), pak je potřeba méně kabeláže, než u systému s hvězdicovou strukturou. Ta navíc obsahuje centrální prvek, který dále přispívá k hmotnosti celého systému.

Hmotnost byla hodnocena jako nadprůměrně důležitá vlastnost. Váha nastavena na 7.

Implementace Implementace je parametr hodnotící snadnost nasazení systému do letadla. Toto obsahuje jak hardwarovou část (kabeláž, karty rozhraní, centrální prvky, atd.) tak část softwarovou - jak snadné je stávající systém řízení letadla přizpůsobit danému přenosovému systému. Hodnotíme především náročnost softwarové konfigurace jednotlivých koncových prvků, použití speciálních karet, speciálních konektorů/kabeláže a také celkové finanční náklady spojené s vybranou přenosovou sběrnicí (použití speciálních karet, kabelů a aktivních prvků).

Implementace byla hodnocena jako průměrná vlastnost vybrané sběrnice. Váha nastavena na 5.

Propojitelnost uzlů Propojitelnost uzlů je z hlediska distribuovaného FBW systému důležitá vlastnost. V ideálním případě je možné, aby navzájem komunikovaly jakékoliv dva koncové body systému. Jednotlivé koncové systémy si poskytují data pro řízení letu a o stavu letadla a neexistuje centrální uzel pro sběr dat a jejich zpracování - proto je komunikace mezi jakýmikoliv uzly kritická. Propojitelnost uzlů úzce souvisí se síťovou topologií systému sběrnice.

Zadavatel tuto vlastnost hodnotí jako nadprůměrně důležitou. Váha nastavena na 7.

Údržba systému Komunikační systém letadla bude podléhat pravidelným kontrolám a možným budoucím rozšířením. Proto je nutné, aby byl systém snadno přístupný obsluze, výměna jednotlivých částí byla jednoduchá a případná změna konfigurace či přidání nových prvků nebylo spojeno s podstatným zásahem do tohoto systému. Hodnotí se především síťová topologie - pokud jsou všechny koncové uzly systému na společném kabelu, pak výměna tohoto kabelu s sebou nese podstatný zásah do všech těchto připojených koncových uzlů.

Údržba systému je hodnocena jako méně důležitý parametr. Váha nastavena na 3.

3.2 Parametry jednotlivých sběrnic

Údaje v této části vychází z [7], [8], [3], [1].

CAN Bus Sběrnice CAN využívá sériové sběrnicové topologie. Všechny komunikující uzly mohou být umístěny na jednom komunikačním vedení, což by přispělo k vysoké bezpečnosti systému. Avšak sběrnice nevyužívá žádný řídicí uzel pro řízení komunikace (pouze prioritu uzlů), což může mít za následek neschopnost komunikace některých uzlů. Toto omezení může být zmenšeno využitím většího počtu jednotlivých sběrnic CAN, což má ale za následek jednak zvýšení počtu použitých vodičů, hmotnosti, ale i složitosti propojení.

Rychlost přenosu je hodnocena průměrně, protože sběrnice podporuje přenosovou rychlost maximálně 1 Mbit/s. Tato rychlost je ale sdílena pro všechny komunikující uzly na jednom vedení a navíc je omezena délkou maximálně 40 metrů (při větší vzdálenosti rychlost přenosu klesá). Počet použitých vodičů je konstantní v závislosti na počtu uzlů a rychlost v závislosti na počtu uzlů klesá.

Implementace je hodnocena pouze průměrně, protože sběrnice je více výhodná pro komunikaci 2 koncových zařízení, než pro komunikaci množství rovnocenných koncových uzlů.

MIL-STD-1553B Ze všech porovnávaných sběrnic používá sběrnice MIL-STD-1553B nejmenší počet vodičů, protože jednotlivé koncové uzly jsou všechny připojeny na společné vedení. Takováto konfigurace zvyšuje bezpečnost, protože není nutné používat žádné centrální uzly. Centrální vedení může být pro zvýšení bezpečnosti zdvojeno. Veškerá komunikace však musí být řízena z řídicího uzlu (tento však může být při poruše nahrazen jiným). Údržba systému je hodnocena průměrně, protože při změně konfigurace nebo opravě vedení je nutné zasáhnout do všech uzlů.

Rychlost přenosu je hodnocena průměrně, protože sběrnice podporuje přenosovou rychlost maximálně 1 Mbit/s. Tato rychlost je sdílena pro všechny komunikující uzly, tj s počtem uzlů přenosová rychlost klesá. Počet použitých vodičů je konstantní v závislosti na počtu uzlů.

ARINC 429 Sběrnice ARINC 429 využívá pro komunikaci jednotlivých uzlů samostatné vodiče, přičemž jedno takové vedení obsahuje až 20 přijímačů, ale pouze jeden vysílač. Pokud by tedy měly komunikovat jakékoliv dva koncové body systému, je nutné použít velké množství kabelů. Z hlediska bezpečnosti sběrnice nepoužívá žádný centrální prvek, což snižuje náchylnost systému proti poruchám. Pro zabezpečení integrity dat je v protokolu zavedena lichá parita bitů v posílané zprávě a možnost zabezpečit posílanou zprávu pomocí CRC. Údržba systému ARINC 429 je hodnocena podprůměrně protože pokud by došlo k přerušení jednoho vodiče (nebo by byl jiný důvod jej vyměnit), pak je nutné zasáhnout až do 21 koncových uzlů. V případě změny konfigurace systému jsou změny mnohem zásadnější.

Rychlost přenosu je hodnocena podprůměrně, protože sběrnice podporuje maximálně 100 kbit/s, ale je nezávislá na počtu uzlů. Počet použitých vodičů je stejný jako počet uzlů (pokud je počet uzlů menší než 20).

Implementace sběrnice ARINC 429 do systému je hodnocena průměrně, sběrnice je sice dnes široce využívána, ale je zde limitace v podobě nutnosti využívat pouze malá (32 bitů, samotná data pouze 18 bitů) slova.

ARINC 664 Sběrnice ARINC 664 využívá hvězdicovou fyzickou topologii. Z tohoto důvodu je potřeba využít speciální (AFDX) přepínač, který přepíná jednotlivé přijaté rámce z koncových uzlů do cílových uzlů. Proto není tato sběrnice hodnocena maximálně z hlediska bezpečnosti (má více prvků než ideální systém). Použití centrálního přepínače je kompenzováno jednak jeho zdvojením, tak i zdvojením přenosových kabelů. Tím je zajištěna dostatečná bezpečnost systému - pravděpodobnost výskytu nedetekované chyby na obou přenosových vedení během jednoho rámce je dána součinem pravděpodobností výskytu těchto chyb na jednotlivých vedeních. Použití zdvojených prvků však vede k navýšení celkové hmotnosti systému, která je dále zvýšena nutností využití AFDX přepínače. Při použití hvězdicové topologie

je možno navzájem propojit jakékoliv dva koncové uzly systému, avšak není nutné používat samostatných kabelů pro jednotlivá spojení koncových uzlů. Koncový uzel stačí připojit pouze k AFDX přepínači. Z této vlastnosti pak vyplývá snadná údržba systému, protože pokud je nutné vyměnit jakoukoliv část (vyjma centrálního přepínače), není nutné zasahovat do ostatních částí systému.

Sběrnice ARINC 664 podporuje virtuální linky (VL), kterým lze jednotlivě přiřadit různé přenosové rychlosti (viz kap. 2.4). Počet použitých vodičů lineárně roste v závislosti na počtu uzlů (2 vodiče pro každý koncový uzel).

Z pohledu implementace systému je na rozdíl od ostatních sběrnic ARINC 664 náročnější na implementaci. Toto vyplývá z nutnosti použití speciálních komunikačních karet (ovšem systém může být zabudován do vyššího celku, ten ale musí být také pozměněn), speciálních AFDX přepínačů a také díky nutnosti vyvinout potřebný software pro tyto prvky.

3.3 Zhodnocení výběru sběrnice

Tabulka 3.1 je vytvořena upravenou aplikací zásad vytváření C&E Matrix[1]. Tato je součástí principů Six Sigma pro dodržování a zlepšování kvality nejrůznějších procesů. Postup vytváření C&E Matrix lze nalézt na internetu, např. zde[15].

Po sečtení všech parametrů z tabulky 3.1 vyplývá, že nejvhodnější sběrnice podle definovaných kritérií je sběrnice dle standardu ARINC 664. Tato sběrnice vyniká především ve vysokých přenosových rychlostech a velmi dobré celkové propojitelnosti koncových uzlů. Naopak implementace této sběrnice do systému bude náročnější než u ostatních sběrnic, protože je nutné nově vyvinout software koncových uzlů a přepínačů.

Proto byla vybrána k dalšímu zpracování (především analýzu rizik použité sběrnice) a následné implementaci v simulačním nástroji Matlab Simulink sběrnice ARINC 664. Tato sběrnice staví na technologii Ethernet, což usnadňuje její implementaci - technologie je snadno dostupná. Sběrnice nabízí dostatečnou kapacitu přenosového pásma již při použití 100BASE-TX fyzického média. Další výhoda spočívá v jednoduché implementaci vyšších systémů, jelikož ty mohou transparentně implementovat síťovou vrstvu protokolové rodiny TCP/IP.

[1] Cause and Effect Matrix – matice příčin a důsledků

	Relevance	ARINC 429		ARINC 664		CAN Bus		MIL-STD-1553B	
		Splňuje	Body	Splňuje	Body	Splňuje	Body	Splňuje	Body
Bezpečnost	9	9	81	7	63	9	81	7	63
Rychlost přenosu	5	3	15	9	45	5	25	5	25
Počet vodičů/hmotnost	7	3	21	3	21	3	21	7	49
Implementace	5	5	25	3	15	5	25	5	25
Propojitelnost uzlů	7	5	35	9	63	5	35	5	35
Údržba systému	3	3	9	7	21	5	15	5	15
Celkový počet bodů		186		228		202		212	

Tab. 3.1: Srovnání vlastností jednotlivých sběrnic

4 SIMULACE SBĚRNICE AFDX

Simulace přenosu pomocí sběrnice AFDX je naprogramována v prostředí Simulink při využití toolboxu SimEvents. Tento nástroj umožňuje vytváření, přenos, kontrolu a řízení datových jednotek – entit. Těmito jsou simulovány ethernetové rámce dle specifikace ARINC 664[3].

AFDX rámce mají datovou strukturu podobnou běžnému ethernetovému rámci, doplněnou o speciální části (pole sériového čísla). Navíc jsou pozměněny zdrojové a cílové MAC adresy (viz 2).

4.1 Výpočet CRC

CRC je vypočteno dle specifikace IEEE 802.3. Je uloženo do v 32 bitech, které jsou připojeny na konec AFDX rámce.

CRC je možno vypočítat pro libovolně dlouhou sekvenci příchozích bitů zprávy tak, že jsou postupně vyčítány jednotlivé bity zprávy, které se exklusivně sčítají[1] s bitovou maskou dle specifikace (zde v hexadecimální podobě: 0xEDB88320). Po zpracování všech bitů zprávy je výsledek takovýchto součtů roven CRC dané zprávy a je připojen na její konec.

Prostředí Simulink nabízí již předpřipravené bloky pro výpočet a kontrolu CRC, avšak v simulaci nebyly využity. Jejich vstupem musí být sekvence jednotlivých bitů zprávy uložených v jediném vektoru, jehož vytvoření je poměrně časově náročné z důvodů konverze parametrů uložených v jednotlivých entitách (jsou uloženy jako proměnné typu double).

Proto byla pro výpočet CRC vytvořena samostatná funkce, která v příchozí entitě nastaví poslední 4 byty na hodnotu kontrolního součtu. Tato funkce byla nejprve implementována pomocí rozdělení příchozí zprávy na jednotlivé bity, avšak tento přístup byl časově náročný, protože bylo nutné znovu používat konverze příchozích entit na vektor jednotlivých bitů. Časová náročnost vyplývá z nutnosti vytvoření rozsáhlého jednorozměrného vektoru, který je poté naplněn jednotlivými bity. Tyto bity musí být získány postupným bitovým posunem jednotlivých příchozích parametrů (převedených na typ uint8) a jejich násobení s bitovou maskou. Takovýto přístup je časově náročný a zbytečně složitý na implementaci.

Z výše uvedených důvodů bylo přistoupeno k implementaci výpočtu CRC po jednotlivých bytech, což výrazně urychlí výpočet CRC. Tento postup spočívá v nalezení odezvy všech možných hodnot vstupních bytů s binární maskou zvolenou pro daný typ CRC. Tyto odezvy jsou pak uloženy do tabulky (pro byty velikosti

[1] XOR, exclusive or, $\oplus$

8 bitů má tabulka 256 hodnot). Tuto tabulku je potřeba vypočítat pouze jednou (například před spuštěním simulace) a při výpočtu CRC z ní pouze vyčítat hodnoty.

Samotný výpočet CRC pro příchozí byty spočívá v nalezení příslušné hodnoty ze CRC tabulky a exkluzivním součtu s dočasnou hodnotou vypočteného CRC (na začátku inicializována na nejvyšší možnou hodnotou – obsahuje pouze binární „1“).

Zapouzdřená funkce pro výpočet CRC z příchozích bytů má následující kód:

```
function y = fcn(u, crcTable)

temp = uint8(u);
pocetBytu = size(temp,1);

crc = uint32(4294967295); %0xFFFFFFFF
for i = 1:pocetBytu
    index = uint8(bitxor(uint8(bitand(crc, 255)), temp(i)));
    crc = uint32(bitxor(bitshift(crc,-8), crcTable(index+1)));
end
y = uint8(zeros(4,1, 'uint8'));
y = typecast(bitcmp(crc),'uint8')';

end
```

Po zpracování všech bytů zprávy je vypočítán jednotkový doplněk[2] z vypočteného CRC, který je následně použit k dalšímu zpracování (připojení na konec rámce).

CRC je počítáno ze všech polí AFDX rámce, kromě preambule. Protože je zdrojová MAC adresa pro obě linky (A a B) AFDX sítě rozdílná, bude se také lišit CRC v jednotlivých tocích dat v těchto linkách (pro odpovídající si rámce se stejnými daty, VL i pořadovým číslem).

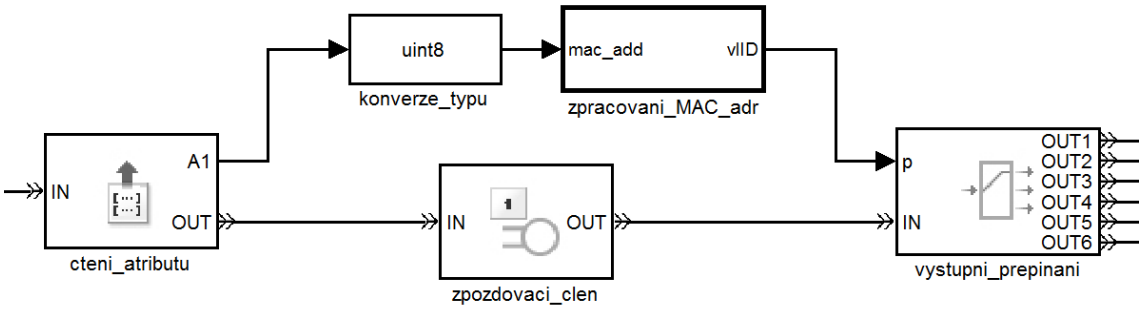
Implementace výpočtu CRC po bytech je přepracována pro Matlab z kódu pro jazyk C [14].

4.2 Přepínač

Hlavní funkcí AFDX přepínače je přepínání příchozích rámců ze vstupních portů na výstupní porty. Přepínač ze vstupních rámců přečte cílovou MAC adresu, ve které je uloženo číslo VL. Dle tohoto čísla pak posílá rámce na jeden nebo více výstupních portů. Přepínač také může poslat rámec zpět ke koncovému uzlu, který jej poslal (koncový uzel tak může testovat funkčnost linky).

[2] funkce bitcmp() v Matlabu

Nastavení, které rámce posílat na jaké výstupní porty by v reálném systému bylo uloženo v konfiguračním souboru. Tento je možné nahrát do přepínače speciálním protokolem[3]. Kvůli zjednodušení je toto v simulaci nastaveno přímo uspořádáním funkčních bloků a jejich propojením. Pokud je tedy potřeba změna konfigurace, je nutné změnit propojení bloků.



Obr. 4.1: Realizace přepínání rámců v prostředí SimEvents.

Na obr. 4.1 je zobrazena realizace přepínání rámců v prostředí SimEvents. Nejprve je z příchozího rámce přečtena cílová MAC adresa pomocí bloku Get Attribute. Ta je v rámci reprezentována proměnnou typu double a je nutné ji pro správné zpracování překonvertovat na typ uint8. V bloku vlid_mac je z adresy separováno číslo VL, které je následně použito pro přepnutí rámce na výstup. Rámec je nutné při zpracování MAC adresy zpozdit. Bez tohoto zpoždění dochází v systému k nesprávnému přepnutí nebo dojde k chybě posílání rámců – následující bloky za přepínačem se zablokují, protože příchozí rámce nejsou správně synchronizovány.

4.3 Koncový systém

Koncový systém na sběrnici AFDX plní jeden hlavní úkol – přijímají data z vyšších vrstev systému a vytvářejí rámce pro přenos v síti. Tyto rámce jsou přiděleny do jednotlivých VL a poslány po duplicitních linkách sběrnice.

Pokud je nějaký koncový systém i příjemcem některé z VL, pak tyto příchozí rámce zpracovává a předává vyšším vrstvám, pokud nejsou poškozené.

V simulaci jsou pro zjednodušení vytvářeny rámce z náhodných dat přímo v koncovém systému. Velikost těchto dat je možné zadat před spuštěním simulace (počet bytů).

Model simulace obsahuje bloky pro vytváření toků dat jednotlivých VL, kdy každý takový blok vytváří dva toky dat pro linku A a linku B AFDX sítě. Tyto

[3] ARINC 615A-3

datové toky jednotlivých VL jsou pak spojeny do jednoho toku dat pro každou linku AFDX sítě. Avšak před jejich spojením musí být jednotlivé toky dat VL navzájem zpožděny, aby nedocházelo ke kolizím. Tímto je simulována funkce plánovače, který rámce jednotlivých VL předává k výstupu dle určitého klíče. Při použití rozdílných zpoždění pro každou VL je simulováno round-robin vybírání rámců (rámce nejsou vybírány dle žádné priority).

V přijímací části koncového systému jsou umístěny bloky pro výpočet kontrolního CRC a blok porovnávacího monitoru (Comparison monitor). Tento porovnává obě vypočtená CRC a pokud se neshodují, nastaví u přijatého rámce atribut informující o této neshodě. Dále tento monitor srovnává přijatá data v rámcích z obou linek. Pokud jsou data rozdílná (tato neshoda se nemusí v některých případech projevit v rozdílném CRC), je u obou rámců toto poznačeno.

Dále již mohou být rámce využity k dalšímu zpracování. V simulaci jsou příchozí rámce uloženy do matice pro zpracování v Matlabu.

4.4 Zhodnocení simulace

Implementovaná simulace sběrnice slouží jako základ pro bezpečnostní analýzu, kde jsou do simulace vloženy bloky způsobující základní chyby. Tyto pak slouží k ověření správné odezvy systému na tyto chyby.

Dále simulace může sloužit pro názorné objasnění principů fungování sběrnice AFDX. Toto je důležité pro počáteční fázi implementace reálné sběrnice. V reálném systému budou jednotlivé funkce sběrnice implementovány odlišnými způsoby, princip fungování je však zachován.

5 ANALÝZA RIZIK

Cílem této kapitoly je poskytnout bezpečnostní analýzu vybrané sběrnice ARINC 664. Bezpečnostní analýza vychází z požadavku zadavatele na vysokou bezpečnost použitých zařízení v letadle. Proto je nutné každé zařízení podrobit důkladnému bezpečnostnímu rozboru, a to na základě standardizovaných metod[11].

Pro sběrnici ARINC 664 bude na základě použité topologie a definovaných možných chyb v systému (FHA, Functional Hazard Assessment – „Analýza rizik systému“, od zadavatele) navržena stromová struktura jednotlivých chyb a jejich příspěvků k pravděpodobnosti vzniku definované chyby (FTA, Fault tree analysis – „Analýza stromové struktury chyb“).

Závěrečná část bude srovnávat analyzované chyby se simulovanou topologií sběrnice ARINC 664 pro potvrzení zde definovaných bezpečnostních rizik.

5.1 Topologie analyzovaného systému

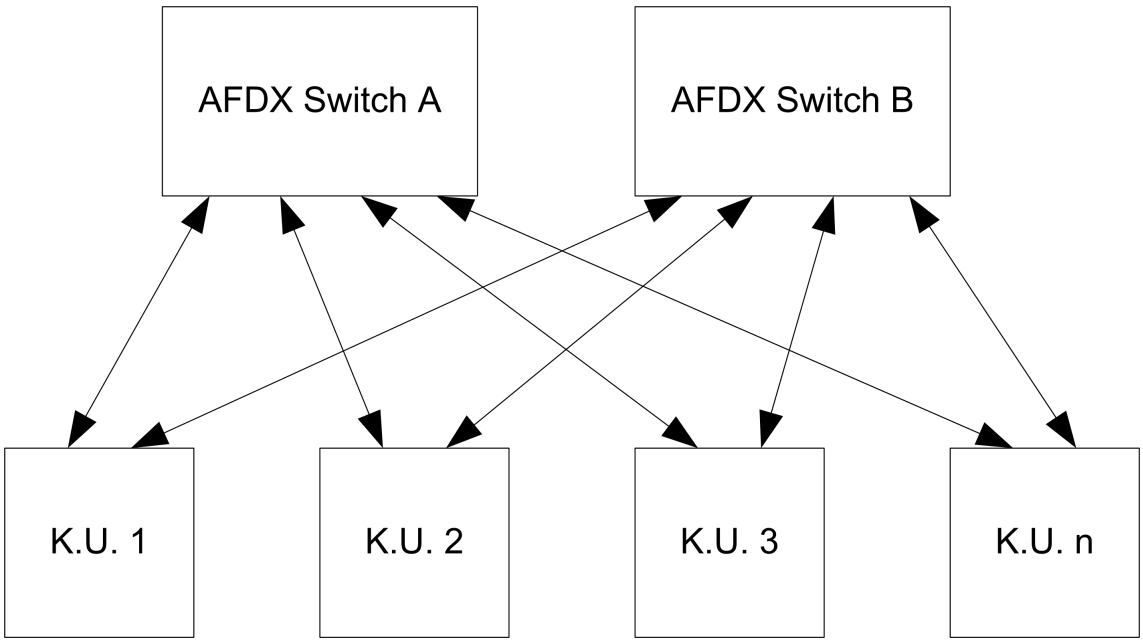
Analyzovaná topologie vychází přímo ze standardu [3] a je zobrazena na obr. 5.1. Systém obsahuje 2 AFDX přepínače (Switch A a Switch B), ke kterým jsou připojeny jednotlivé koncové uzly systému. Každý koncový uzel je tedy připojen k oběma přepínačům (jedním vedením). Takto je zajištěna nezávislost obou přenosových cest - přepínače i vedení jsou zdvojena. Celkový počet koncových uzlů je zadavatelem odhadován na maximálně 20.

Takováto topologie splňuje veškeré parametry definované v [3]. Je zřejmé, že systém není dokonalý, protože při selhání jakékoliv jeho části dochází k vysokému zvýšení pravděpodobnosti chyby v přenosu. Tomuto faktu se ale nelze vyhnout s žádným reálným systémem. Bezpečnostní analýza s tímto faktem počítá a předpokládá, že ke vzniku jakékoliv chyby může dojít, ale takováto chyba je nezávislá na ostatních. Dalším z předpokladů je, že dvě různé na sobě nezávislé chyby se mohou vyskytnout pouze s velmi malou pravděpodobností. Proto musí být systém letadla schopen případné chyby odhalit a oznámit posádce nutnost údržbářského zásahu vedoucího k odstranění této závady a tím k obnovení celkové bezpečnosti letadla.

Koncový uzel, kde dochází ke zpracování přijímaných dat, je připojen k řídicí jednotce (DACU, Digital Actuator Control Unit – Digitální řídicí jednotka aktuátoru), která ovládá jednotlivé řídicí plochy. Proto je na něj z hlediska bezpečnosti kladen vysoký důraz a musí splňovat kritéria podložená následující bezpečnostní analýzou.

Analyzované vnitřní schéma koncového uzlu společně se základním náčrtem DACU je uvedeno na obr. 5.2, část B). DACU obsahuje dvě nezávislé jednotky, z nichž každá provádí stejné výpočty/operace, které se navzájem kontrolují. Každá jednotka obsahuje svou nezávislou AFDX vrstvu, pro zajištění vyšší bezpečnosti systému. Každá

tato vrstva obsahuje nezávislou porovnávací jednotku, která srovnává data z obou částí a je schopna označit chybějící nebo špatná vstupní data.



Obr. 5.1: Analyzovaná topologie AFDX sítě.

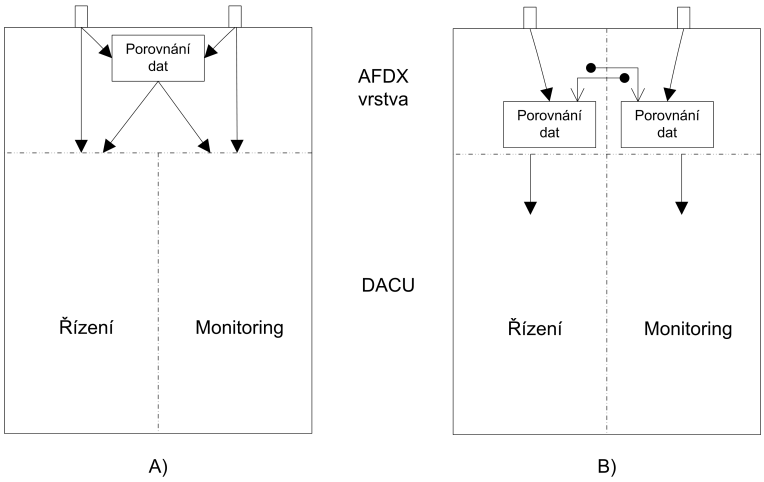
5.2 Pravděpodobnosti chyb v systému

Pravděpodobnosti vzniku jednotlivých chyb systému letadla byly analyzovány na základě požadavků zadavatele (jsou odvozeny z FHA). Těmto jednotlivým chybám byl definován příspěvek sběrnice AFDX k jejich vzniku. Seznam těchto chyb je uveden v tab. 5.1. Dále byly vytvořeny FTA pro tyto chyby, v nichž jsou identifikovány jednotlivé základní možné příčiny jejich vzniku („basic event“). Poznámka v tabulce určuje bezpečnostní riziko pro posádku a cestující v letadle - I – katastrofické selhání[1], II – závážné selhání[2]. Méně závažné chyby zde nejsou analyzovány.

Nesprávná vstupní data v jedné řídicí cestě

Analyzovány byly příspěvky sběrnice k následujícím chybám: FHA1A, FHA1B, FHA3, FHA6A, FHA6B, FHA10 (viz tab. 5.1). Tato chyba znamená, že přenášená data byla mezi odesílatelem a příjemcem pozměněna, ale pouze v jednom přenosovém kanálu, a pro všechny DACU tomuto kanálu náležící. Může vzniknout, pokud: AFDX switch chybně přečte data z připojeného média, AFDX switch pozmění data

[1] catastrophic failure, viz [11]
[2] hazardous failure, viz [11]



Obr. 5.2: Srovnání přístupu k návrhu topologie koncového uzlu. A) společná vsrtva AFDX; B) rozdělená vrstva AFDX

(HW chyba) během zpracovávání rámce, AFDX chybně zapíše data na výstupní připojené médium, bitová chyba při přenosu rámce médiem, chybně zapsaná data koncovým uzlem a chybně přečtená data rámce koncovým uzlem.

Všechny chyby mají podobným efekt – vznikne bitová chyba v přenášených datech (data jsou nesprávná a neměla by být použita při výpočtech) a zároveň vznikne takové CRC, že tato chyba není odhalena. Toto je možné pouze pokud zůstane CRC stejné, ale odpovídá i pozměněným datům nebo v CRC vznikne taková bitová chyba, že odpovídá pozměněným datům.

V první příloze, část 1, je uveden FTA pro takovýto typ chyby (viz FTA1A).

Neoznačená nesprávná vstupní data pro jedno DACU

Analyzovány byly příspěvky sběrnice k následujícím chybám: FHA2B, FHA4B, FHA5B, FHA8B, FHA9, FHA11, FHA12 (viz tab. 5.1). Tato chyba znamená, že DACU přijme data, která jsou nesprávná (došlo k jejich pozměnění) a také neoznačená (selhání porovnání dat z obou přenosových cest).

To může nastav ve dvou případech: pokud nastane naprosto stejná bitová chyba v obou přenosových cestách (velmi malá pravděpodobnost, dále není analyzováno) nebo pokud jsou neoznačená nesprávná data pouze v jednom přenosovém kanálu. Z FTA stromu je vidět, že k takovémuto porušení dat dojde pouze pokud nastane chyba odpovídající například chybě FHA1A a zároveň dojde k chybnému zpracování přijatých rámců porovnávacím monitorem.

Ten může selhat ve dvou případech: neoznačí neshodné rámce z obou cest (HW chyba) nebo neoznačí ztracený rámec.

V první příloze, část 2, je uveden FTA pro takovýto typ chyby (viz FTA11).

Neoznačená nesprávná vstupní data pro obě DACU

Analyzovány byly příspěvky sběrnice k následujícím chybám: FHA2A, FHA7A, FHA7B, FHA8A (viz tab. 5.1). Tato chyba vznikne, pokud dojde k různým chybám typu FHA2B pro dvě různá DACU zároveň. Pravděpodobnost takovéto chyby je dána součinem pravděpodobností pro jednotlivé chyby. Proto je tento typ chyby považován za dostatečně málo pravděpodobný.

V první příloze, část 3, je uveden FTA pro takovýto typ chyby (viz FTA2A).

Neoznačená nesprávná vstupní data pro všechny tři DACU

Analyzovány byly příspěvky sběrnice k následujícím chybám: FHA4A, FHA5A (viz tab. 5.1). Protože pravděpodobnost vzniku chyby pro tři DACU je menší než pravděpodobnost vzniku chyby pro dvě DACU, je tento scénář považován za stejně pravděpodobný jako například vznik chyby FHA2A.

V první příloze, část 4, je uveden FTA pro takovýto typ chyby (viz FTA4A).

Neoznačená nesprávná vstupní data alespoň pro dvě DACU

Analyzovány byly příspěvky sběrnice k následujícím chybám: FHA13 (viz tab. 5.1). Protože pravděpodobnost vzniku chyby pro tři DACU je menší než pravděpodobnost vzniku chyby pro dvě DACU, je tento scénář považován za stejně pravděpodobný jako například vznik chyby FHA2A.

V první příloze, část 5, je uveden FTA pro takovýto typ chyby (viz FTA13).

Tab. 5.1: Definice příspěvků chyb sběrnice k systémovým chybám

Letová funkcionalita	**Číslo systémové FHA chyby**	**Chyba D-FBW systému**	**Příspěvek sběrnice k chybě**	**Pozn.**
Ovládání klonění (křidélka a spoilery)	FHA 1A	Selhání všech DACU pro křidélka (vypnuté)	Nesprávná vstupní data v jedné řídicí cestě	I
Pokračování na další straně				

Tab. 5.1 – pokračování z předchozí strany

Letová funkcionalita	**Číslo systémové FHA chyby**	**Chyba D-FBW systému**	**Příspěvek sběrnice k chybě**	**Pozn.**
Ovládání klonění (křidélka a spoilery)	FHA 1B	Selhání 2 DACU pro řízení jednoho křidélka a selhání DACU pro řízení 3 párů spoilerů.	Nesprávná vstupní data v jedné řídicí cestě	I
Ovládání klonění (křidélka)	FHA 2A	Nedetekovaný nesprávný řídicí pokyn z obou DACU současně pro jedno křidélko (obě DACU ovládají plochu).	Neoznačená nesprávná vstupní data pro obě DACU.	I
Ovládání klonění (křidélka)	FHA 2B	Nesprávný řídicí pokyn z jednoho DACU pro jedno křidélko (druhé DACU toto křidélko neovládá - je odpojeno)	Neoznačená nesprávná vstupní data pro jedno DACU.	I
Ovládání zatáčení (směrovka)	FHA 3	Selhání všech DACU pro směrovku (vypnuté)	Nesprávná vstupní data v jedné řídicí cestě	II
Ovládání zatáčení (směrovka)	FHA 4A	Všechny aktivní DACU umožňují ovládáni směrovky bez limitace	Neoznačená nesprávná vstupní data pro všechny tři DACU.	I
Ovládání zatáčení (směrovka)	FHA 4B	Jedno aktivní DACU umožňuje ovládání směrovky bez limitace (ostatní 2 jsou odpojené)	Neoznačená nesprávná vstupní data pro jedno DACU.	I

Pokračování na další straně

Tab. 5.1 – pokračování z předchozí strany

Letová funkcionalita	**Číslo systémové FHA chyby**	**Chyba D-FBW systému**	**Příspěvek sběrnice k chybě**	**Pozn.**
Ovládání zatáčení (směrovka)	FHA 5A	Nedetekovaný nesprávný řídicí pokyn ze všech tří DACU současně pro směrovku.	Neoznačená nesprávná vstupní data pro všechny tři DACU.	I
Ovládání zatáčení (směrovka)	FHA 5B	Nesprávný řídicí pokyn z jednoho DACU pro směrovku (zbylé dvě DACU směrovku neovládá - jsou odpojené)	Neoznačená nesprávná vstupní data pro jedno DACU.	I
Ovládání klopení (výškovky a HS)	FHA 6A	Selhání všech DACU pro výškovky (vypnuté)	Nesprávná vstupní data v jedné řídicí cestě	I
Ovládání klopení (výškovky a HS)	FHA 6B	Selhání 2 DACU pro řízení jedné výškovky a selhání DACU pro vyvažovací funkci.	Nesprávná vstupní data v jedné řídicí cestě	I
Ovládání klopení (výškovky)	FHA 7A	Rozdílný řídicí pokyn pro levou a pravou výškovku plynoucí z chyby DACU	Neoznačená nesprávná vstupní data pro dvě DACU.	I
Ovládání klopení (výškovky)	FHA 7B	Neoznámené rozdělení výškovek díky různým pokynům od pilota, nebo je jedna výškovka zasekнutá/nefunkční	Neoznačená nesprávná vstupní data pro dvě DACU.	I

Pokračování na další straně

Tab. 5.1 – pokračování z předchozí strany

Letová funkcionalita	**Číslo systémové FHA chyby**	**Chyba D-FBW systému**	**Příspěvek sběrnice k chybě**	**Pozn.**
Ovládání klopení (výškovky)	FHA 8A	Nedetekovaný nesprávný řídicí pokyn z obou DACU současně pro jednu výškovku (obě DACU ovládají plochu).	Neoznačená nesprávná vstupní data pro dvě DACU.	I
Ovládání klopení (výškovky)	FHA 8B	Nesprávný řídicí pokyn z jednoho DACU pro jednu výškovku (druhé DACU tuto výškovku neovládá - je odpojeno)	Neoznačená nesprávná vstupní data pro jedno DACU.	I
Ovládání klopení (HS)	FHA 9	Trvalý nedetekovaný nesprávný řídicí pokyn z DACU řídicího HS	Neoznačená nesprávná vstupní data pro jedno DACU.	I
Vzdušné brzdy (spoilery)	FHA 10	D-FBW systém nemůže řídit dostatečný počet spoilerových párů k zajištění funkce vzdušné brzdy kvůli selhání několika DACU	Nesprávná vstupní data v jedné řídicí cestě	II
Spoilery	FHA 11	Nesprávný současný řídicí pokyn ze všech DACU řídicích spoilerové páry	Neoznačená nesprávná vstupní data pro DACU řídicí spoilerové páry.	I
Asistence klonění (spoilery)	FHA 12	Nesprávný řídicí pokyn z DACU způsobí kmitání spoilerového páru	Neoznačená nesprávná vstupní data pro jedno DACU.	I

Pokračování na další straně

Tab. 5.1 – pokračování z předchozí strany

Letová funkcionalita	**Číslo systémové FHA chyby**	**Chyba D-FBW systému**	**Příspěvek sběrnice k chybě**	**Pozn.**
Asistence klonění (spoilery)	FHA 13	Nesprávný řídicí pokyn z alespoň dvou DACU řídicích spoilerové páry	Neoznačená nesprávná vstupní data alespoň pro dvě DACU.	I

V tab. 5.2 jsou uvedeny jednotlivé základní chyby (např. Chybně přeneseno CRC na médiu) s uvedenou předpokládanou hodnotou pravděpodobnosti jejich výskytu v systému. V tabulce je dále uveden systémový efekt takovéto chyby (např. Data označena jako nesouhlasná v obou linkách) a v kterém stromu FHA se tato chyba vyskytuje. Pro příklad je uveden výpis základních chyb z FHA11. Pro ostatní chyby FHA je nutné vycházet z příslušných FTA stromů (viz první příloha).

Tab. 5.2: Pravděpodobnosti základních chyb systému a systémový efekt

Chyba	**Předpokládaná pravděpodobnost**	**Systémový efekt**	**FHA**
Stejná bitová chyba v obou přenosových kanálech	$10e^{-16}$	Neoznačená nesprávná vstupní data	FHA11
Chybně přečtená data (payload) u AFDX switche	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
CRC odpovídá chybným datům	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně přečteno CRC u AFDX switche	$10e^{-16}$	Data označena jako nesouhlasná v obou linkách	FHA11

Pokračování na další straně

Tab. 5.2 – pokračování z předchozí strany

Chyba	**Předpokládaná pravděpodobnost**	**Systémový efekt**	**FHA**
AFDX switch poškodí data při zpracování rámce	$10e^{-5}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně zapsaná data (payload) u AFDX switche	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně přenesená data (payload)	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně zapsáno CRC u AFDX switche	$10e^{-16}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně přeneseno CRC na médiu	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně přečtená data (payload) u koncového uzlu	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně přečteno CRC koncovým uzlem	$10e^{-16}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně zapsaná data (payload) koncovým uzlem	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně zapsáno CRC koncovým uzlem na médium	$10e^{-16}$	Data označena jako nesouhlasná v obou linkách	FHA11
Monitor neoznačí chybějící rámec	$10e^{-5}$	Data označena jako nesouhlasná v obou linkách	FHA11
Rámec má nesprávnou velikost	$10e^{-12}$	Data označena jako nesouhlasná v obou linkách	FHA11

Pokračování na další straně

Tab. 5.2 – pokračování z předchozí strany

Chyba	**Předpokládaná pravděpodobnost**	**Systémový efekt**	**FHA**
Rámec nemá správný identifikátor VL	$10e^{-14}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chyba při přenosu	$10e^{-9}$	Data označena jako nesouhlasná v obou linkách	FHA11
Chybně zapsáno CRC u AFDX switche	$10e^{-16}$	Data označena jako nesouhlasná v obou linkách	FHA11
Monitor neoznačí nesouhlasné rámce	$10e^{-5}$	Data označena jako nesouhlasná v obou linkách	FHA11

Výskyt bitové chyby na médiu byl uvažován $\leq 10^{-9}$. Tento předpoklad vychází ze závěrů [4].

Pravděpodobnost, že CRC bude odpovídat chybným datům je spočítána z předpokladu, že počet všech kombinací CRC je konečný. Pro 32 bitové CRC je počet kombinací $4,295 \cdot 10^9$. Pravděpodobnost shody CRC je pak dána inverzí této hodnoty – $2,3283 \cdot 10^{-10}$.

Pravděpodobnosti chyb při čtení a zápisu dat jednotlivými komponenty byly uvažovány $\leq 10^{-16}$. Tento předpoklad vychází z porovnání reálných síťových prvků a jejich vlastností[3]. Zde záleží na skutečné implementaci hardwarových součástí.

Pokud se základní chyba vyskytne samostatně, nemusí naznačená systémová chyba nastat, protože některé základní chyby musí nastat současně (tato logika je opět naznačena ve stromech FTA, viz první příloha).

5.3 Simulace selhání systému

V této části jsou ověřeny předpokládané dopady jednotlivých základních chyb na systém sběrnice AFDX pomocí simulace těchto chyb.

[3]například zde: `http://www.cisco.com/en/US/products/hw/modules/ps2710/products_data_sheet09186a008019ad1a.html`

K tomu, abychom mohli tyto základní chyby pozorovat ve výsledcích simulace z kap. 4, musí se stávající model upravit. Tato úprava spočívá v doplnění o bloky, které způsobují různé (většinou náhodné) chyby uvnitř přenášených AFDX rámců. Jednotlivé základní chyby byly implementovány dle tab. 5.2, ve které jsou obsaženy chyby objevující se ve všech FHA. Pro přehlednost nebyly implementovány všechny chyby, například chyby „Chyba při přenosu“, „Rámec nemá správný identifikátor VL“ a „Rámec má nesprávnou velikost“ mají stejný dopad na systém (ztráta AFDX rámce), a proto jsou v modelu zastoupeny jen jedním blokem.

Dále nebyla implementována chyba „CRC odpovídá chybným datům“. Tato chyba nastane, pokud dojde k porušení (chybě) v přenášených datech (payload), ale CRC připojené k AFDX rámci odpovídá i těmto chybným datům. Jelikož tento případ nastane pouze pro specifickou chybu v datech, je pravděpodobnost takovéto chyby velmi malá a navíc i její implementace by byla značně náročná (například ve srovnání s prostým výpočtem CRC). Z těchto důvodů nebyla tato chyba v simulaci zahrnuta.

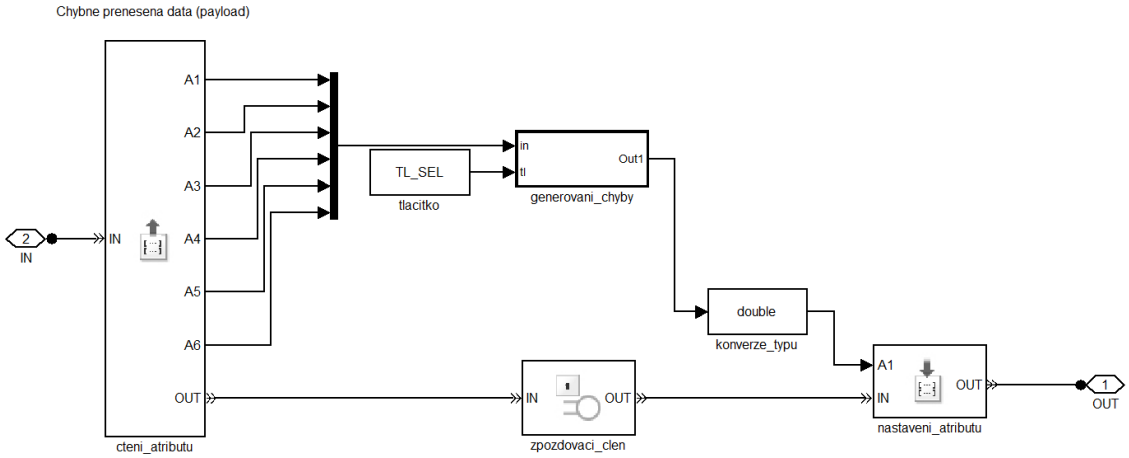
Simulace umožňuje výskyt pouze jedné základní chyby v jednom okamžiku během běhu simulace. Toto omezení vychází z předpokladu, že základní chyby jsou na sobě nezávislé a proto je zkoumán systémový dopad pouze jedné chyby v daném okamžiku. Během běhu simulace lze mezi jednotlivými základními chybami přepínat pomocí grafického rozhraní. Zde může uživatel nastavit požadovanou chybu, nebo také veškeré chyby odstranit.

Přepínání chyb je implementováno jako funkce buttons(). Tato funkce je bez vstupních parametrů a je spuštěna při otevření modelu simulace, což způsobí zobrazení grafického prvku s tlačítky.

Grafické rozhraní je navrženo jako soubor přepínatelných tlačítek, kdy zapnutí jednoho způsobí vypnutí předešlého[4]. Každé tlačítko má přiřazenou svoji unikátní hodnotu, dle které je následně umožněno působení základní chyby spojené s tímto tlačítkem. Při přepnutí některého z tlačítek se spustí obslužná funkce, která způsobí změnu globální proměnné (tato je použita jako vstup do jednotlivých bloků základních chyb, které jsou jí řízené). Globální proměnná je použita výstupní hodnota bloku Simulink/Sources/Constant. Obslužná funkce tuto hodnotu (respektive řetězec znaků jména globální proměnné) nastaví nejprve na řetězec „0“ a poté na „TL_SEL“. Toto řešení způsobí změnu v parametru výstupního bloku, avšak tato změna se projeví během simulace pouze pokud dojde k otevření a zavření nabídky parametrů (Block parameters) tohoto bloku. Obslužná funkce automaticky vyvolá otevření všech těchto nabídek ve všech blocích způsobujících základní chyby. Proto také dojde při přepnutí některého z tlačítek k pozastavení simulace, otevření nabídek

[4]takzvaný „radio button“

a jejich následnému uzavření. Po uzavření poslední nabídky simulace automaticky pokračuje.



Obr. 5.3: Příklad bloku způsobujícího základní chybu.

Na obr. 5.3 je zobrazen příklad bloku způsobujícího základní chybu – konkrétně chybu v přenášených datech. Tento blok je umístěn na médiu mezi koncovým systémem a AFDX přepínačem a simuluje náhodnou bitovou chybu v přenášených datech.

Nejprve jsou z příchozí entity zkopírovány všechny atributy, které jsou následně zpracovány ve vnitřním bloku err_gen. Ten obsahuje zapouzdřenou Matlab funkci[5].

Kód této funkce je následující:

```
function y = fcn(u, tlacitko)
temp = uint8(u);
pocetBytu = size(temp,1);
jedna = ones(1,1,'uint32');
if bitand(uint32(tlacitko),bitshift(jedna,6)) > 0
    y = temp(15:15+pocetBytu-20);
    zmena = uint8(round(rand(1,1)*255));
    y(uint8(ceil(rand(1,1) * size(y,1)))) = zmena;
else
    y = temp(15:15+pocetBytu-20);
end

end
```

[5]Embedded Matlab Function

Funkce nejprve otestuje, zda je hodnota stisknutého tlačítka rovna číslu přiřazenému tomuto chybovému bloku (zde testuje hodnotu 64[6]). Pokud je podmínka splněna, je vygenerováno náhodné [7]číslo. Tímto je nahrazen jeden náhodný byte v přenášené zprávě (ale pouze na pozici, kde leží užitečná data – payload).

Bloky generující základní chyby vnáší do přenosu určité zpoždění, což by v koncovém systému způsobilo nesouběžnost jednotlivých toků dat (jak z jednotlivých VL, tak i v oddělených cestách). Proto jsou tyto chybové bloky umístěny symetricky v celém modelu, avšak aktivovány jsou pouze některé. Takto je dosaženo synchronizace jednotlivých příchozích rámců a tím i zjednodušení řídicí logiky.

Rozmístění jednotlivých chybových bloků je uvedeno v druhé příloze.

5.4 Vyhodnocení bezpečnosti sběrnice

V simulaci bylo vyzkoušeno působení všech základních chyb z tab. 5.2. Pokud tyto chyby působily samostatně, pak došlo k naznačenému systémovému efektu dle analýzy, kromě jednoho případu.

Při analýze základní chyby – AFDX switch poškodí data při zpracování rámce bylo nesprávně uvažováno i následné přepočítání CRC na výstupu přepínače. Běžné ethernetové přepínače provádí přepočítání CRC, protože došlo minimálně ke změně zdrojové a cílové MAC adresy při zpracování rámce přepínačem. Naopak u AFDX přepínače zůstávají MAC adresy stejné během celé cesty rámce, a proto se CRC nepřepočítává. Proto také při vzniku uvedené základní chyby dojde k zahození příslušného rámce v koncovém systému (nesouhlasí CRC).

Oproti standardní sběrnici AFDX byl do simulace přidán porovnávací monitor. Tento významně přispívá k zvýšení schopnosti sběrnice detekovat rozdíly v přijatých rámcích. V reálném systému by však jeho implementace byla složitější, protože je nutné počítat s odlišnou dobou příjmu rámců z obou sítí a ztracenými rámci. Tento nedostatek by se dal překonat využitím vyrovnávací paměti, která by rámce jednotlivých sítí ukládala, dokud nedojde k příjmu rámce z druhé sítě. Toto by však znamenalo zvýšení zpoždění celého datového provozu a složitější uspořádání komunikace mezi jednotlivými porovnávacími uzly obou sítí AFDX.

[6]hodnoty tlačítek mají podobu 2^k, pro možné budoucí rozšíření, kde bude umožněno více chyb zároveň

[7]pseudonáhodné, Matlab využívá generátor pseudonáhodných čísel, ovšem pro tuto simulaci je dostatečný

6 ANALÝZA ČASOVÉHO ZPOŽDĚNÍ

V této kapitole bude provedena analýza časového zpoždění vysílaných rámců v AFDX síti na základě specifikace [3].

Časové zpoždění rámců mezi jednotlivými koncovými uzly AFDX sběrnice je jedním z hlavních faktorů, které určují determinismus síťové komunikace této sběrnice. Tento parametr je také třeba určit pro úspěšnou certifikaci sběrnice pro letecký průmysl.

Maximální zpoždění mezi přijetím posledního bitu zprávy z vyšší vrstvy koncového systému (odesílatel) a doručením posledního bitu do vyšší vrstvy koncového systému (příjemce) je v obecném případě, kdy je mezi oběma koncovými systémy n přepínačů, definováno jako:

$$t_{\text{max}} = t_{\text{ES1}} + t_{\text{plánovač}} + (n+1) \cdot t_{\text{médium}} + n \cdot t_{\text{přepínač}} + t_{\text{ES2}}.$$

Dále je uvažován případ s jedním přepínačem, kde je doba zpoždění určena:

$$t_{\text{max}} = t_{\text{ES1}} + t_{\text{plánovač}} + 2 \cdot t_{\text{médium}} + t_{\text{přepínač}} + t_{\text{ES2}},$$

kde t_{ES1} je maximální zpoždění vysílajícího koncového systému, $t_{\text{médium}}$ je doba přenosu rámce médiem, $t_{\text{přepínač}}$ je doba zpracování a přepnutí rámce v AFDX přepínači a t_{ES2} je maximální zpoždění přijímajícího koncového systému. Takto vypočtená hodnota zpoždění platí pro architekturu uvedenou na obr. 5.1 – mezi dvěma koncovými uzly je jen jeden AFDX přepínač. Pokud by mezi koncovými uzly bylo více přepínačů, bylo by nutno přičíst další hodnoty zpoždění v přepínačích a doby přenosu médii.

Doba zpoždění t_{ES1} je shora ohraničena hodnotou 150 μs[3]. Tato doba je nutná pro příjem dat z vyšší vrstvy, zpracování těchto dat (přiřazení správného VL ID), vytvoření AFDX rámce a jeho vyslání na médium.

Zpoždění způsobené plánovačem[1] $t_{\text{plánovač}}$ může mít maximální hodnotu až 500 μs. Plánovač opožďuje jednotlivé rámce přijaté z virtuálních linek, aby nedošlo ke kolizi při jejich vkládání na medium. Hodnota tohoto kolísání závisí na počtu VL a velikosti posílaných AFDX rámců na jednotlivých VL.

Doba zpoždění médiem $t_{\text{médium}}$ je hodnota závislá na velikosti AFDX rámce. Velikosti těchto rámců mohou nabývat pouze hodnot od 84 B (17 B užitečných dat[2]) do 1538 B (1471 B užitečných dat). Hodnota zpoždění médiem je dále závislá na přenosové rychlosti - zde je počítána rychlost 100 Mbit/s. Pro rámec délky 84 B je doba zpoždění vypočtena jako[13]:

$$t_{\text{medium}} = 84 \cdot 8/100000000 = 6,72\,[\mu\text{s}].$$

[1] scheduler

[2] bez hlavičky síťové vrstvy

Pro rámec délky 1538 B je doba zpoždění:

$$t_{\text{medium}} = 1538 \cdot 8/100000000 = 123,04\,[\mu\text{s}].$$

Doba zpoždění $t_{\text{přepínač}}$ je doba nutná pro příjem rámce přepínačem, jeho zpracování a přepnutí na správný výstupní port. Tato doba je shora ohraničena 100 μs.

Doba zpoždění t_{ES2} je shora ohraničena hodnotou 150 μs[3]. Tato doba je nutná pro příjem dat z media, zpracování těchto dat (třídění rámců dle VL IDpro vyšší vrstvy) a samotné předání do příslušné vyšší vrstvy.

6.1 Výpočet zpoždění plánovače

Zpoždění plánovače je definováno [3] jako:

$$t_{\text{plánovač}} \leq 4,0 \cdot 10^{-5} + \frac{\sum_{i \in \text{VL ID}} L_{\text{i}} \cdot 8}{B}\,[\text{s}],$$

kde L_{i} je velikost AFDX rámce v příslušné VL (hodnoty od 84 B do 1538 B). Tato je vynásobena 8, protože přenosová rychlost B je zadána v bit/s. Toto zpoždění není závislé na BAG. V grafu na obr. 6.1 jsou zobrazeny hodnoty tohoto zpoždění pro celý rozsah velikostí rámců a pro prvních 100 VL. Pro jednoduchost je brán v potaz jen případ, kdy všechny VL mají stejnou velikost rámců.

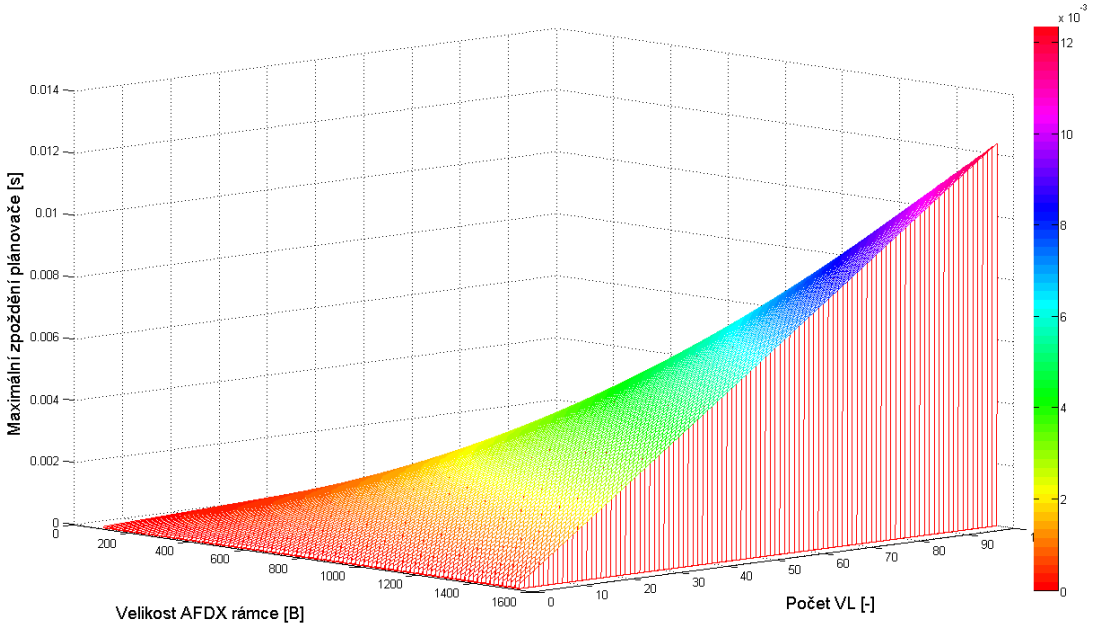
Zpoždění plánovače je nutno považovat za nejvyšší možnou dobu zpoždění jednotlivého AFDX rámce z určité VL. Pro jiný rámec toto zpoždění bude nabývat menších hodnot, protože rámec nemusí v plánovači čekat na poslání dalších rámců.

Maximální hodnota zpoždění plánovače je omezena 500 μs. V grafu na obr. 6.2 jsou zobrazeny pouze hodnoty zpoždění, které odpovídají tomuto kritériu. Hodnoty zpoždění plánovače omezené na 500 μs poté vymezují definiční obor pro velikost AFDX rámců a počet VL. Tyto se dají určit z grafu na obr. 6.3, který je průmětem grafu na obr. 6.2 do roviny X-Y.

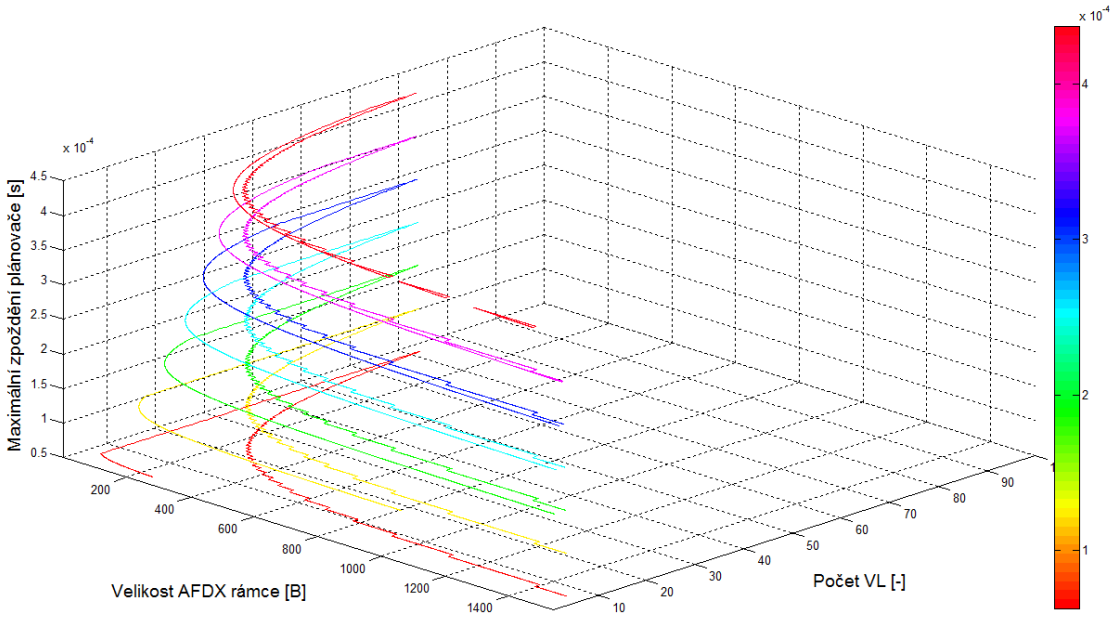
Například pro nejvyšší možnou velikost AFDX rámců (1538 B) můžeme použít pouze 4 VL s touto velikostí. Naopak pro nejnižší velikost rámců (84B) lze použít až 68 VL.

6.2 Vyhodnocení analýzy časového zpoždění

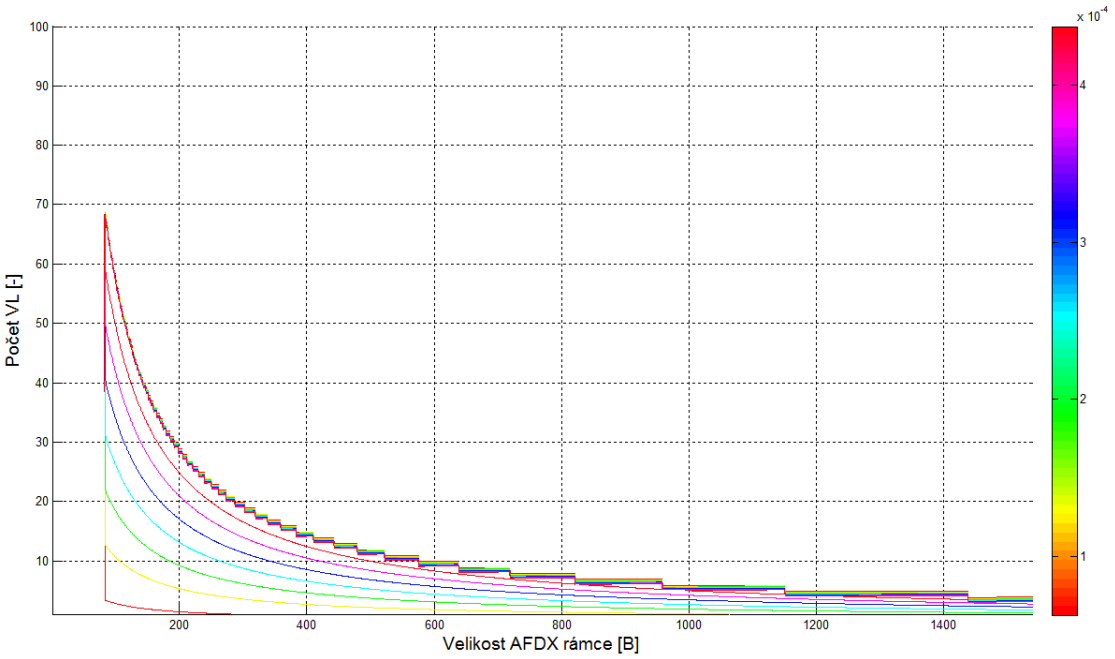
Časové zpoždění mezi komunikujícími koncovými uzly sítě AFDX je důležitým parametrem pro určení determinovaného přenosu. Zpoždění deterministického systému proto musí být ohraničené a určitelné. Tato kapitola naznačila postup, jakým je možno toto zpoždění určit z dílčích zpoždění jednotlivých komponent sítě pro jednoduchou topologii sítě. Analýza složitějšího uspořádání je uvedena například v [5].



Obr. 6.1: Hodnoty zpoždění plánovače v koncovém systému - neomezeno.



Obr. 6.2: Hodnoty zpoždění plánovače v koncovém systému.



Obr. 6.3: Hodnoty zpoždění plánovače v koncovém systému, průmět do roviny XY.

7 ZÁVĚR

V této práci byly popsány jednotlivé druhy systémů řízení letadel a také definovány parametry datové sběrnice pro distribuovaný systém FBW. Dále byly popsány jednotlivé druhy sběrnic využívaných v leteckém průmyslu.

Z těchto sběrnic byla vybrána k další analýze a k implementaci v prostředí Simulink sběrnice ARINC 664, která splňuje všechna definovaná kritéria a představuje vhodný a moderní komunikační systém pro letecké systémy.

Implementace sběrnice v Simulinku byla zaměřena výhradně na vrstvu síťového rozhraní, ve které se sběrnice liší od normální sběrnice typu TCP/IP. Do simulace byly následně umístěny jednotlivé bloky způsobující základní chyby, kterými se ověřovaly analyzované chyby systému.

Ze závěrů bezpečnostní analýzy lze odvodit, že vybraná sběrnice svým zdvojeným uspořádáním významně snižuje pravděpodobnost výskytu chybných dat, anebo v případě výskytu chyby přispěje k jejímu označení. Toto je velmi důležitá vlastnost, protože letecké systémy mohou po určitý časový úsek pracovat s předchozími daty a chybná data nebrat v potaz.

Z bezpečnostní analýzy dále plyne, že porovnávací monitor v koncovém systému sběrnice zvyšuje pravděpodobnosti odhalení vzniklých chyb a jeho použití přispívá k navýšení bezpečnosti vybrané sběrnice nad rámec samostatného protokolu ARINC 664. V reálném systému by však jeho implementace byla složitější, protože je nutné počítat s odlišnou dobou příjmu rámců z obou sítí a ztracenými rámci. Tento nedostatek by se dal překonat využitím vyrovnávací paměti, která by rámce jednotlivých sítí ukládala, dokud nedojde k příjmu rámce z druhé sítě. Toto by však znamenalo zvýšení zpoždění celého datového provozu a složitější uspořádání komunikace mezi jednotlivými porovnávacími uzly obou sítí AFDX.

V poslední části byla provedena analýza časového zpoždění sběrnice. Tato analýza vyplývá s deterministických parametrů jednotlivých součástí sběrnice, avšak pouze s neměnnými parametry. Pro složitější uspořádání s ohledem na časově proměnné parametry (měnící se velikosti rámců, počet adresovaných VL, změna v nastavení přepínačů) by však uvedené vztahy měly být přezkoumány.

8 PRVNÍ PŘÍLOHA

8.1 Stromová struktura chyb systému FHA1A

Volně vloženo k dokumentu.

8.2 Stromová struktura chyb systému FHA11

Volně vloženo k dokumentu.

8.3 Stromová struktura chyb systému FHA2A

Volně vloženo k dokumentu.

8.4 Stromová struktura chyb systému FHA4A

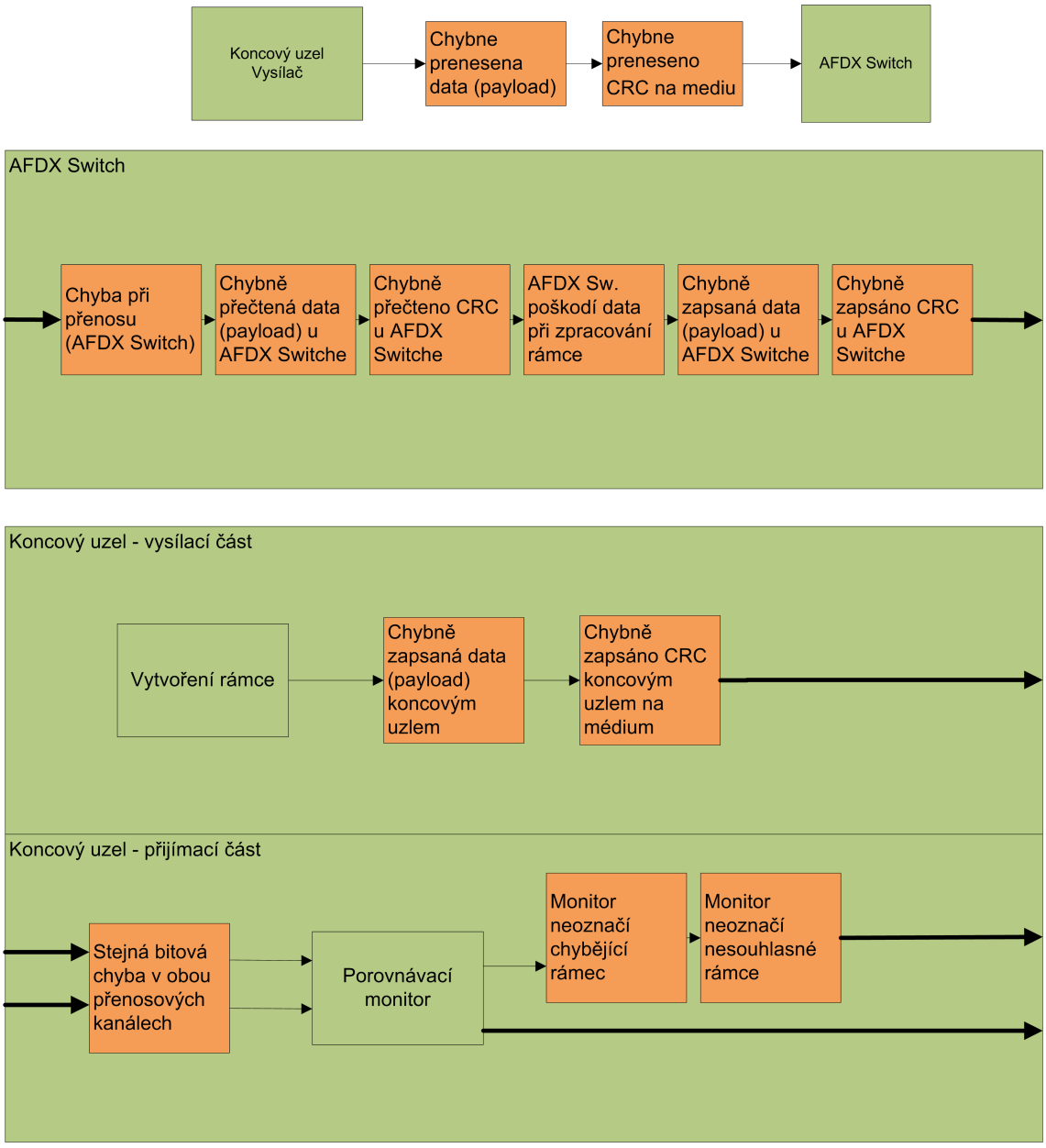
Volně vloženo k dokumentu.

8.5 Stromová struktura chyb systému FHA13

Volně vloženo k dokumentu.

9 DRUHÁ PŘÍLOHA

9.1 Rozmístění chybových bloků



Obr. 9.1: Rozmístění chybových bloků v systému (médium, AFDX Switch, Koncový uzel.

LITERATURA

[1] AIRLINES ELECTRONIC ENGINEERING COMMITTEE *ARINC Specification 429 Part 1-17 Mark 33 Digital Information Transfer System*. Annapolis (Maryland, USA): Aeronautical Radio, 2004. 309 s.

[2] AIRLINES ELECTRONIC ENGINEERING COMMITTEE *ARINC Specification 429 Part 3-19 Mark 33 Digital Information Transfer System - File Data Tranfer Techniques*. Annapolis (Maryland, USA): Aeronautical Radio, 2009. 184 s.

[3] AIRLINES ELECTRONIC ENGINEERING COMMITTEE *ARINC Specification 664P7-1 - Avionics Full-Duplex Switched Ethernet Network*. Annapolis (Maryland, USA): Aeronautical Radio, 2009. 150 s.

[4] BENNETT, D., NAIR, R. *Bit Error Rate and Signal Integrity of Cat-5 based DVI/HDMI Cables*. Mesa (Arizona, USA): ComLSI Inc. 7 s.

[5] BAUER, H., SCHARBARG, J.-L., FRABOUL, Ch. *Worst-case end-to-end delay analysis of an avionics AFDX network*. Toulouse (France): Université de Toulouse, 2010. 5 s.

[6] BRIER, D., TRAVERSE, P. *AIRBUS A320/A330/A340 Electrical Flight Controls - A Family of Fault-Tolerant Systems*. Toulouse (France): Aérospatiale, 1993. 8 s.

[7] *CAN Specification*. Stuttgart: Robert Bosch GmbH, 1991. 73 s.

[8] DEPARTMENT OF DEFENSE *INTERFACE STANDARD FOR DIGITAL TIME DIVISION COMMAND/RESPONSE MULTIPLEX DATA BUS*. Washington DC (USA), 1996. 51 s. MIL-STD-1553B

[9] FIELDS, L. *Airplane Digital Ditributed Fly-By-Wire Flight Control Systems Architectures*. Phoenix (Arizona): [s.n.], 2005. 20 s.

[10] *ISO 11898-1*. ISO, 2003. 51 s. ISO 11898-1:2003(E)

[11] SAE International *GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT*. Warrendale, PA (USA), 1996. 331 s. ARP4761.

[12] SPITZER, C., R. *The Avionics Handbook*. Boca Raton (USA): CRC Press, 2001. 542 s. ISBN 0-8493-8348-X.

[13] SCHUDEL, Greg. *Bandwidth, Packets Per Second, and Other Network Performance Metrics* [online]. 2009, poslední revize 5.8.2009 [cit. 2010-05-11]. http://www.cisco.com/web/about/security/intelligence/network_performance_metrics.html.

[14] BARR, Michael. *CRC Implementation Code in C* [online]. 2000 [cit. 2010-05-11]. http://www.netrino.com/Embedded-Systems/How-To/CRC-Calculation-C-Code.

[15] PEREIRA, Ron. *Need Help Making Decisions?* [online]. 2007, poslední revize 11.6.2007 [cit. 2010-05-11]. http://lssacademy.com/2007/06/11/need-help-making-decisions/.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AFDX Avionics Full-Duplex Switched Ethernet – Plně duplexní Ethernet sběrnice pro avioniku

ACK acknowledgment - potvrzení

BAG Bandwith Allocation Gap – časový interval generování rámce

CAN Controller Area Network

CRC Cyclic redundancy check – Cyklický redundantní součet

DACU Digital Actuator Control Unit – Digitální řídicí jednotka aktuátoru

FBW Fly-By-Wire – druh řídicího systému letadla

FHA Functional Hazard Assessment – „Analýza rizik systému“

FTA Fault tree analysis – „Analýza stromové struktury chyb“

MAC Media Access Control

MSB Most Significant Bit - nejvýznamější bit

NRZ Non-return-to-zero - bez návratu k nule

VL Virtuální linka

TDM Time Division Multiplex

Z_0 charakteristická impedance

SEZNAM OBRÁZKŮ

1.1 Zjednoušené schéma FBW. 11
1.2 Blokové schéma centralizovaného FBW systému. 12
1.3 Blokové schéma distribuovaného FBW systému. 13
2.1 Připojení jednotlivých zařízení na sběrnici MIL-STD-1553B. 20
2.2 Základní topologie sběrnice ARINC 429. 23
2.3 Základní topologie sběrnice AFDX. 24
2.4 Blokové schéma AFDX přepínače. 27
4.1 Realizace přepínání rámců v prostředí SimEvents. 36
5.1 Analyzovaná topologie AFDX sítě. 39
5.2 Srovnání přístupu k návrhu topologie koncového uzlu. A) společná vsrtva AFDX; B) rozdělená vrstva AFDX 40
5.3 Příklad bloku způsobujícího základní chybu. 49
6.1 Hodnoty zpoždění plánovače v koncovém systému - neomezeno. . . . 53
6.2 Hodnoty zpoždění plánovače v koncovém systému. 53
6.3 Hodnoty zpoždění plánovače v koncovém systému, průmět do roviny XY. 54
9.1 Rozmístění chybových bloků v systému (médium, AFDX Switch, Koncový uzel. 57

SEZNAM TABULEK

2.1 Hardwarové vlastnosti datové sběrnice podle MIL-STD-1553B 19
2.2 Multicastová cílová MAC adresa AFDX, ID VL se přidělí při návrhu systému 26
2.3 Zdrojová MAC adresa AFDX, ID koncového uzlu se vhodně přidělí při návrhu systému 26
3.1 Srovnání vlastností jednotlivých sběrnic 33
5.1 Definice příspěvků chyb sběrnice k systémovým chybám 41
5.2 Pravděpodobnosti základních chyb systému a systémový efekt 45