Politechnika Warszawska

WYDZIAŁ ELEKTRONIKI
I TECHNIK INFORMACYJNYCH

Instytut Informatyki

Praca dyplomowa magisterska

na kierunku Informatyka
w specjalności Inżynieria systemów informatycznych

{Tytuł pracy}

Imię Nazwisko
Numer albumu XXXXXX

promotor
prof. dr hab. inż. Imię Nazwisko

Warszawa 2019

Analiza jakości sterownika manipulatora o 6 stopniach swobody

Streszczenie

W tej pracy zostaną zbadane ...

Słowa kluczowe:
XXX

Analysis of 6 degrees of freedom manipulator control driver

Abstract

This thesis is focused on ...

Keywords:
XXX

załącznik nr 10 do zarządzenia
nr 46 /2016 Rektora PW

Politechnika Warszawska
Warsaw University of Technology

Warszawa, dd.mm.yyyy r.
miejscowość i data
place and date

Imię Nazwisko
imię i nazwisko studenta
name and surname of the student
XXXXXXX
numer albumu
student record book number
Informatyka
kierunek studiów
field of study

OŚWIADCZENIE

DECLARATION

Świadomy/-a odpowiedzialności karnej za składanie fałszywych zeznań oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie, pod opieką kierującego pracą dyplomową.
Under the penalty of perjury, I hereby certify that I wrote my diploma thesis on my own, under the guidance of the thesis supervisor.

Jednocześnie oświadczam, że:
I also declare that:

- niniejsza praca dyplomowa nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.) oraz dóbr osobistych chronionych prawem cywilnym,
- *this diploma thesis does not constitute infringement of copyright following the act of 4 February 1994 on copyright and related rights (Journal of Acts of 2006 no. 90, item 631 with further amendments) or personal rights protected under the civil law,*
- niniejsza praca dyplomowa nie zawiera danych i informacji, które uzyskałem/-am w sposób niedozwolony,
- *the diploma thesis does not contain data or information acquired in an illegal way,*
- niniejsza praca dyplomowa nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów lub tytułów zawodowych,
- *the diploma thesis has never been the basis of any other official proceedings leading to the award of diplomas or professional degrees,*
- wszystkie informacje umieszczone w niniejszej pracy, uzyskane ze źródeł pisanych i elektronicznych, zostały udokumentowane w wykazie literatury odpowiednimi odnośnikami,
- *all information included in the diploma thesis, derived from printed and electronic sources, has been documented with relevant references in the literature section,*
- znam regulacje prawne Politechniki Warszawskiej w sprawie zarządzania prawami autorskimi i prawami pokrewnymi, prawami własności przemysłowej oraz zasadami komercjalizacji.
- *I am aware of the regulations at Warsaw University of Technology on management of copyright and related rights, industrial property rights and commercialisation.*

Politechnika Warszawska
Warsaw University of Technology

załącznik nr 10 do zarządzenia
nr /2016 Rektora PW

Oświadczam, że treść pracy dyplomowej w wersji drukowanej, treść pracy dyplomowej zawartej na nośniku elektronicznym (płycie kompaktowej) oraz treść pracy dyplomowej w module APD systemu USOS są identyczne.

I certify that the content of the printed version of the diploma thesis, the content of the electronic version of the diploma thesis (on a CD) and the content of the diploma thesis in the Archive of Diploma Theses (APD module) of the USOS system are identical.

.....
czytelny podpis studenta
legible signature of the student

Spis treści

1 WPROWADZENIE **8**
- 1.1 Motywacja . . . 8
- 1.2 Plan pracy . . . 9

2 ANALIZA TRENDÓW **10**
- 2.1 Rozwój awioniki . . . 10
- 2.2 Technologia WAIC . . . 11
- 2.3 Niezawodność systemów . . . 12
  - 2.3.1 Analiza FMEA . . . 13
  - 2.3.2 Sieci Petriego . . . 15
  - 2.3.3 Zarządzanie błędami w awionice . . . 16

3 SYSTEM AHRS **18**
- 3.1 Zasada działania . . . 18
- 3.2 Redundancja . . . 18
- 3.3 Mechanika . . . 18
  - 3.3.1 Moduł pilota . . . 18
  - 3.3.2 Moduł akwizycji danych . . . 18
- 3.4 Elektronika . . . 18
  - 3.4.1 Moduł pilota . . . 18
  - 3.4.2 Moduł akwizycji danych . . . 18
- 3.5 Oprogramowanie . . . 19
  - 3.5.1 Moduł pilota . . . 19
  - 3.5.2 Moduł akwizycji danych . . . 19

4 ARCHITEKTURA OPROGRAMOWANIA **20**
- 4.1 Struktura projektu . . . 20
- 4.2 Wykorzystane narzędzia . . . 20
- 4.3 Moduł pilota . . . 20
  - 4.3.1 Struktura oprogramowania . . . 20
  - 4.3.2 Interfejs użytkownika . . . 20
  - 4.3.3 Komunikacja . . . 20
- 4.4 Moduł akwizycji danych . . . 20
  - 4.4.1 Struktura oprogramowania . . . 20
  - 4.4.2 Kąty orientacji przestrzennej . . . 21
  - 4.4.3 Odbiornik GPS . . . 21
  - 4.4.4 System uzgadniający . . . 21
- 4.5 Redundancja oprogramowania . . . 21
  - 4.5.1 Zakłócenia SEU . . . 21
  - 4.5.2 Watchdog . . . 21
  - 4.5.3 Oprogramowanie symulacyjne . . . 21

5 TESTY **22**
- 5.1 Symulacje . . . 22
- 5.2 Testy w locie . . . 22
- 5.3 Podsumowanie . . . 22

6 OPRACOWANIE WYNIKÓW **23**
6.1 Analiza FMEA 23
6.2 Sieć Petriego 23
6.3 Analiza bezpieczeństwa 23
6.4 Wiarygodność technologii WAIC 23

7 PODSUMOWANIE **24**

DODATEK A. ZAWARTOŚĆ PŁYTY CD **25**

BIBLIOGRAFIA **26**

WYKAZ SYMBOLI I SKRÓTÓW **27**

SPIS RYSUNKÓW **28**

SPIS TABLIC **29**

1 WPROWADZENIE

Systemy lotnicze w przeciągu ostatnich lat uległy znaczącemu rozwojowi. Wraz ze wzrostem osiągów statków powietrznych inżynierowie musieli dostosowywać systemy sterowania do krytycznych warunków lotu. Początkowe mechaniczne układy zostały wyparte przez elektroniczne systemy sterowania (*ang. fly – by – wire*). Jednym z najważniejszych elementów podczas projektowania obiektów latających jest optymalizacja jego masy. W tym celu ciężkie przewody służące do wymiany informacji zastąpiono światłowodami. Współczesny samolot zawiera na swoim pokładzie wiele urządzeń elektronicznych, które wymieniają między sobą gigabajty danych na sekundę. Zapewnienie niezawodnych systemów awionicznych stało się wyzwaniem, od którego zależy bezpieczeństwo załogi i pasażerów.

Kolejny etap rozwoju systemów lotniczych skupia się na redukcji sieci przewodów w samolocie. Bezprzewodowa wymiana danych pomiędzy urządzeniami pozwala na znaczącą oszczędność kosztów serwisowych oraz na zwiększenie masy ładownej.

Niniejsza praca poświęcona jest zagadnieniu komunikacji bezprzewodowej urządzeń awionicznych (*ang. Wireless Avionics Intra – Communication, WAIC*). Badanie tej technologii zostało przeprowadzone na podstawie autorskiego systemu wyznaczania położenia samolotu w przestrzeni (*ang. Attitude Heading Reference System, AHRS*). Na podstawie testów lotnych został wyznaczony stopień niezawodności systemu AHRS.

1.1 Motywacja

Celem pracy magisterskiej jest opracowanie oraz stworzenie w pełni redundantnego systemu AHRS, stosując w nim komunikację bezprzewodową, przy wykorzystaniu gotowych urządzeń elektronicznych dostępnych na rynku (*ang. Commercial – Off – The – Shelf, COTS*). Zaletą tego rozwiązania jest możliwość skupienia się na tworzeniu architektury systemu, z pominięciem zagadnień związanych z wytwarzaniem dedykowanego sprzętu.

Opracowany system znajduje zastosowanie w lotnictwie lekkim. Wyposażenie samolotów tej klasy w dodatkowy sprzęt elektroniczny, komunikujący się przewodowo wiąże się z modernizacją miejsca w kokpicie, które jest ograniczone. Urządzenia wykorzystujące technologię WAIC pozwalają na łatwiejszy montaż oraz nie posiadają ograniczeń związanych z poprowadzeniem wiązki przewodów, w ciasnej kabinie pilota. Zaprojektowany system AHRS składa się z dwóch modułów komunikujących się bezprzewodowo. Wykorzystanie nowej technologii w awionice posiada zarówno wiele potencjalnych zalet jak i problemów, które nie zostały jeszcze w pełni rozwiązane. Jednym z nich jest wyznaczenie odpowiedniego pasma

częstotliwości, które nie zakłóci pracy innych urządzeń na pokładzie samolotu oraz systemów znajdujących się w innych samolotach w przestrzeni powietrznej. Na podstawie systemu AHRS badaniu zostanie poddane pasmo częstotliwości 2.4 GHz oraz 5 GHz w samolotach klasy lekkiej. Ponadto przebadana zostanie niezawodność redundancji systemu, która zapewnia zmianę wykorzystywanego pasma w przypadku pogorszenia jakości transmisji danych, bądź interferencji z innymi systemami.

Projekt został stworzony przy współpracy z pilotem – Jackiem Mainką, który na potrzeby badawcze testował opracowywany system na samolotach szkolno-treningowych de Havilland Canada DHC – 1 Chipmunk oraz de Haviland Tiger Moth. Pozwoliło to na weryfikację poprawności systemu oraz informacji przekazywanych do pilota.

1.2 Plan pracy

Dokument ten stanowi raport z przeprowadzonej pracy magisterskiej. Składa się on z następujących części:

- rozdział 2 zawiera wprowadzenie teoretyczne do dziedziny systemów lotniczych oraz technologi WAIC stanowiącej nowy trend w inżynierii lotniczej; zostały w nim również opisane metody wyznaczania niezawodności systemów lotniczych,
- rozdział 3 opisuje działanie autorskiego systemu AHRS oraz budowę poszczególnych modułów systemu,
- rozdział 4 przedstawia architekturę oprogramowania; metody przetwarzania danych wykorzystane do wyznaczania orientacji przestrzennej płatowca oraz zastosowane rozwiązania redundancji systemu,
- rozdział 5 stanowi szczegółowy opis przeprowadzonych testów w środowisku symulacyjnym oraz podczas działania systemu w trakcie lotu płatowca,
- rozdział 6 opisuje wyniki zebrane podczas testów; dogłębną analizę przypadków testowych oraz obliczenie niezawodności systemu AHRS,
- rozdział 7 poświęcony jest podsumowaniu pracy.

2 ANALIZA TRENDÓW

Zanim rozpocznie się szczegółowe studium tego, w jaki sposób został zaprojektowany system wyznaczania położenia samolotu w przestrzeni, warto wspomnieć o aktualnych trendach, które pojawiają się w branży lotniczej. Tworzenie niezawodnego oprogramowania, wiąże się z dużą ilością testów, walidacji, weryfikacji oraz dokumentacji, która jest tworzona na każdym z etapów procesu. Stąd koszty produktu w branży awionicznej związane są przede wszystkim z zapewnieniem odpowiedniego poziomu bezpieczeństwa. W celu tworzenia krytycznego oprogramowania stosuje się dedykowane przepisy, które opisują podejścia projektowe dla danego poziomu bezpieczeństwa (*ang. Design Assurance Level, DAL*). Najważniejszym z nich jest dokument DO – 178C, który definiuje zasady projektowania oprogramowania, według których instytucje tj. FAA (*ang. Federal Aviation Administartion*) lub ICAO (*ang. International Civil Aviation Organinzation*) przeprowadzają procesy certyfikacyjne.

Przede wszystkim, ze względów bezpieczeństwa nowe narzędzia, technologie oraz metodologie, które pojawiają się w branży IT, wprowadzane są do branży lotniczej z dużym opóźnieniem. Producenci awioniki częściej stawiają na bezpieczne rozwiązania, które zostały sprawdzone podczas wielu prób w locie i są niezawodne.

W niniejszym rozdziale zostaną przedstawione aktualne trendy rozwijane w awionice, ze szczególnym uwzględnieniem technologii bezprzewodowych. W ramach wprowadzenia w dziedzinę niezawodności systemów zostaną opisane najpopularniejsze techniki wykorzystywane podczas wytwarzania oprogramowania.

2.1 Rozwój awioniki

Ciągły postęp technologiczny w branży IT spowodował uzależnienie niemalże każdej dziedziny od komputerów. W podobnej sytuacji znajduje się branża lotnicza, a w szczególności awionika. Komputery odgrywają istotną rolę podczas startu oraz lądowania każdego samolotu wyposażonego w zaawansowane systemy. Jednak używanie najnowszych trendów IT w krytycznych elementach awioniki jest ryzykownym podejściem. Niemniej jednak, inżynierowie cały czas dążą do poprawy bezpieczeństwa. Osiągają to poprzez stopniowe dodawanie takich technologii jak sztuczna inteligencja, blockchain oraz komunikacja bezprzewodowa do mniej krytycznych elementów systemów.

Dzięki zwiększeniu mocy obliczeniowej komputerów oraz wykorzystaniu kart graficznych w celu zrównoleglenia obliczeń, sztuczna inteligencja w ostatnich latach zaczęła być wykorzystywana na szeroką skalę w wielu gałęziach przemysłu. Z uwagi na niedeterministyczność tego

narzędzia, nie jest ono stosowane bezpośrednio w urządzeniach awionicznych. Jednak, w niektórych przypadkach zastosowanie sztucznej inteligencji poprawia poziom bezpieczeństwa oraz zmniejsza koszty eksploatacji. Jednym z nich jest badanie niezawodności części mechanicznych. Każdy z elementów lotniczych posiada maksymalny czas użytkowania, po którym daną część należy wymienić. Biorąc pod uwagę dodatkowe czynniki pogodowe, eksploatacyjne, związane ze starzeniem się elementów ten czas może się skracać, bądź wydłużać [**mlMechanical**]. Zastosowanie metod predykcji opartych o elementy uczenia maszynowego pozwala na dokładne oszacowanie konieczności serwisu danych elementów samolotu. Takie narzędzie umożliwia poprawę bezpieczeństwa oraz oszczędność kosztów dla linii lotniczych. Kolejne zastosowanie sztucznej inteligencji wiąże się ze zmniejszeniem błędów związanych z czynnikiem ludzkim. Na ten rodzaj błędów najczęściej narażeni są piloci, od których zależy los pasażerów. Firma General Electric opracowała system wspomagający pracę pilotów. Monitoruje on aktualny stan lotu, pogodę oraz czynności wykonywane przez załogę. Poprzez ciągły monitoring kokpitu, system wykrywa zmęczenie pilotów oraz inne parametry będące przyczyną błędów [**mlPilots**]. W przypadku wykrycia anomalii, oprogramowanie oparte o sztuczną inteligencję informuje załogę, obsługę samolotu oraz obsługę naziemną.

Technologia blockchain, która zyskała zaufanie na rynkach finansowych jest rozpatrywana jako narzędzie, które może wpłynąć na poprawę bezpieczeństwa w lotnictwie. Jedną z firm, która rozpoczęła prace w tym kierunku jest Aeron. Eksperci zauważyli, że kluczową przyczyną wypadków lotniczych jest zaniżanie godzin lotu, oszczędzając ogromne koszty utrzymania samolotu przez linie lotnicze [**aeron**]. Obecnie na rynku nie istnieje znormalizowany elektroniczny system monitorowania pracy pilotów. Aby zapobiec fałszowaniu danych, zaproponowano wdrożenie technologii blockchain. Jej zadaniem byłoby gromadzenia informacji na temat lotów oraz pracy pilotów. Zapewni to większy poziom bezpieczeństwa oraz efektywniejszy przepływ informacji.

Wyposażenie samolotu ma największy wpływ na jakość oraz cenę lotu. W przypadku urządzeń awionicznych, cena utrzymania statku powietrznego może zostać zredukowana poprzez zmniejszenie masy oraz kosztów serwisowych urządzeń. Technologia komunikacji bezprzewodowej wpływa zarówno na zmniejszenie masy urządzeń danego systemu oraz na koszty serwisowe. Spośród technologii wymienionych w tym rozdziale, największy potencjał rozwojowy posiada technologia WAIC, której zastosowanie może znacząco obniżyć koszty eksploatacji. Z tego względu stała się ona głównym tematem badań niniejszej pracy magisterskiej. Szczegółowy opis koncepcji technologii WAIC znajduje się w rozdziale 2.2.

2.2 Technologia WAIC

Technologia komunikacji bezprzewodowej urządzeń awionicznych stanowi kolejny etap rozwoju lotnictwa. Nowa koncepcja ma wiele zalet oraz stwarza dodatkowe problemy, z którymi muszą się zmierzyć inżynierowie. Główną zaletą wykorzystania WAIC jest redukcja sieci przewodów. Według danych [**waicDesign**], waga okablowania w helikopterze Sikorsky UH – 60 Black Hawk jest szacowana na około 900 kg, co stanowi 18% jego masy startowej [**blackHawk**]. Wykorzystanie technologii bezprzewodowej skutkuje zmniejszeniem masy, co wpływa na zmniejszenie zużycia paliwa nawet do 12%. Ponadto proces planowania oraz rozmieszczenia wiązek elektrycznych kosztuje około 2200$ na kilogram masy samolotu [**waicDesign**]. Szacuje się, że każdego roku zostaje przeznaczonych około dwóch miliona roboczo – godzin na znalezienie oraz wyeliminowaniem usterek związanych z awarią sieci przewodów [**waicDesign**].

Wraz z pojawieniem się przemysłu internetu rzeczy (*ang. Industry Internet of Things, IIoT*), rozwiązanie WAIC może być wykorzystywane do gromadzenia danych z urządzeń awionicznych

oraz ich analizie w chmurze po zakończonym locie. Pozwala to zaoszczędzić czas i umożliwia natychmiastowe wsparcie serwisowe w momencie wykrycia artefaktów. Temat ten jest przedmiotem badań i rozwoju kluczowych firm w sektorze lotniczym. Jedną z nich jest firma General Electric, która w 2017 roku wprowadziła na rynek platformę Predix – to oprogramowania do gromadzenia i analizy danych w chmurze z maszyn przemysłowych oraz systemów awioniki.

Jednym z kluczowych elementów, z którym muszą się zmierzyć inżynierowie podczas opracowywania technologii WAIC jest interferencja z urządzeniami znajdującymi się na pokładzie samolotu, oraz z innymi samolotami znajdującymi się w przestrzeni powietrznej. Światowa organizacja telekomunikacyjna (*ang. International Telecomunication Union, ITU*) rozważała wykorzystanie pasm 2.7 – 2.9 GHz, 4.2 – 4.4 GHz oraz 5.35 – 5.46 GHz dla technologii WAIC [**itu**]. Okazało się, że dla zakresu 2.7 – 2.9 GHz oraz 5.35 – 5.46 GHz istnieją niezgodności z innymi systemami awioniki [**itu**]. Przyjęto, że pasmo 4.2 – 4.4 GHz nie spowoduje krytycznych w skutkach interferencji dla samolotów pasażerskich [**itu**], [**waicModulation**]. Jednak, jest ono również wykorzystywane przez radiowe wysokościomierze (*ang. Radio Altimeters, RAs*) na pokładzie cywilnych i państwowych statków powietrznych. Ważne jest przeanalizowanie odpowiednich mechanizmów sprzęgania między antenami systemu WAIC i wysokościomierzy na pokładzie samolotów. Kolejny problem stanowi określenie regulacji prawnych przez instytucje FAA oraz ICAO, w celu użytkowania technologii bezprzewodowej w awionice. Jednym z najważniejszych wyzwań wykorzystania tej technologii w lotnictwie cywilnym stanowi zabezpieczenie sieci przed niepożądanymi osobami. Biorąc pod uwagę zagrożenia atakami hakerów może stanowić to jedną z przyczyn, która będzie opóźniała wprowadzenie tej technologii na rynek.

W niniejszej pracy magisterskiej badania technologii bezprzewodowej zostały przeprowadzone na samolotach klasy lekkiej, które nie są wyposażone w zaawansowaną awionikę. Testom została poddana bezprzewodowa sieć lokalna 802.11 b/g/n oraz 802.11 a/h/j/n/ac/ax, dla częstotliwości 2.4 GHz i 5 GHz. Zgodnie z raportem opublikowanym przez Międzynarodowe Zrzeszenie Przewoźników Powietrznych (*ang. International Air Transport Association, IATA*) częstotliwości powyżej 5 GHz są obsługiwane przez system wspomagający lądowanie MLS (*ang. Microwave Landing System*) oraz radar pogodowy [**iata**]. Samoloty klasy lekkiej nie są wyposażone w system MLS, zatem wykorzystanie częstotliwości 5 GHz nie wpłynie na pracę tego systemu. Działanie systemu może zostać jedynie zakłócone przez interferencję z systemem radarów meteorologicznych POLRAD, które rozmieszczone są na terenie Polski, rys.**??**. Ich częstotliwość pracy wynosi 5.42 – 5.82 GHz [**polrad**]. W przypadku wykrycia niekorzystnych interferencji system AHRS przełączy się w tryb redundantny i zmieni pasmo częstotliwości komunikujących się komponentów, co poprawi jakość pracy systemu oraz przestanie zakłócać system POLRAD. Wadą przyjętego rozwiązania jest zakłócanie radaru meteorologicznego przed wejściem w tryb redundantny. Może to spowodować chwilowe pogorszenie jakości danych meteorologicznych.

2.3 Niezawodność systemów

Badanie niezawodności jest kluczowym elementem podczas rozwoju systemów, od których zależy ludzkie życie. Niewielki błąd w oprogramowaniu może być katastrofalny w skutkach. Przykładem jest system rakietowy Patriot, który 25 lutego 1991 r. zawiódł przez arytmetyczny błąd wyznaczania czasu w komputerze, przez co zginęło 28 żołnierzy a ponad 98 zostało rannych [**catastrophes**]. Kolejnym przykładem, którego skutkiem była strata około 500 milionów dolarów był start rakiety Ariane 5. Po 37 sekundach od startu rakieta uległa autodestrukcji, spowodowanej przekroczeniem zakresu jednej ze zmiennych [**catastrophes**]. Jak ważną rolę

odgrywają testy podczas projektowania systemów awionicznych przekonali się studenci Politechniki Warszawskiej, koła naukowego awioniki MelAvio. Tworząc oprogramowanie do autorskiego autopilota dla bezzałogowych statków powietrznych nie przeprowadzili testów, związanych ze zmianą półkuli z północnej na południową. Będąc na zawodach UAV Outback Challenge w Australii samolot rozpoczął autonomiczny lot w kierunku przeciwnym niż został zadany. Problem związany był z błędną interpretacją kierunków nawigacyjnych w oprogramowaniu.

Aby zmniejszyć ryzyko wystąpienia błędów katastrofalnych w skutkach, inżynierowi stosują liczne testy oraz analizy, które mają na celu wykrycie błędów na etapie projektowania. Najpopularniejsze z nich to analiza FMEA (*ang. Failure Mode and Effects Analysis*) oraz sieci Petriego, których szczegółowe opisy znajdują się w rozdziałach 2.3.1 oraz 2.3.2. Zastosowanie narzędzi do analizy niezawodności systemu AHRS pozwoli na wyznaczenie odpowiedniego poziomu bezpieczeństwa. Szczegółowa analiza wiarygodności projektowanego urządzenia znajduje się w rozdziale 6.

2.3.1 Analiza FMEA

Koszty rozwijania systemów lotniczych zależą przede wszystkim od poziomu bezpieczeństwa jakie muszą spełniać. Im poziom krytyczności systemu jest wyższy, tym koszty związane z weryfikacją produktu znacząco rosną. Przynależność oprogramowania systemu do danego poziomu DAL, zostaje określona na podstawie analizy funkcjonalności według normy DO – 178C, zgodnie z tablicą 1.

W tradycyjnym podejściu, weryfikacja produktu sprawdza czy wszystkie wymagania zostały spełnione. Odmienne podejście zaproponowała firma Honeywell. Nie polega ono na skupieniu się tylko na wymaganiach, lecz na opracowaniu także analiz systemu, które mogą sprawdzić potencjalnie wadliwe elementy [**honeywellFMEA**]. Nowatorskie podejście inżynierowie wy-

Poziom bezpieczeństwa	**Rodzaj awarii**	**Efekt awarii**
A	Katastrofalny	Utrudnia poprawny lot samolotu oraz lądowanie. Ofiary śmiertelne.
B	Niebezpieczny	Bardzo niski poziom bezpieczeństwa. Zwiększone obciążenie załogi. Poważne lub śmiertelne obrażenia.
C	Umiarkowany	Znaczące obniżenie poziomu bezpieczeństwa. Zwiększone obciążenie załogi. Dyskomfort lub możliwe obrażenia pasażerów.
D	Niewielki	Nieznaczne obniżenie bezpieczeństwa. Niewielki wzrost obciążenia załogi. Dyskomfort pasażerów.

Tablica 1: Poziomy bezpieczeństwa – DAL. *Źródło: [***honeywellFMEA***]*

korzystali w procesie projektowania systemu zarządzania komunikacją (*ang. Communications Management Function, CMF*). CMF odpowiedzialny jest za kierowanie komunikatów łącza danych między różnymi systemami na pokładzie samolotu oraz różnymi systemami naziemnymi, w tym kontrolą ruchu lotniczego (*ang. Ait Traffic Control, ATC*). System został zakwalifikowany wg. standardu DO – 178B do poziomu D. W tym poziomie, w standardowym podejściu

weryfikacja systemu sprawdza jedynie wysokopoziomowe wymagania. W celu lepszej weryfikacji defektów w oprogramowaniu postanowiono wykorzystać model FMEA. To rozwiązanie pozwoliło na dokładniejszą weryfikację systemu. Nie zwiększając przy tym znacząco kosztów, co byłoby nieuniknione podczas zmiany poziomu bezpieczeństwa, z D na C.

FMEA jest to analiza możliwych rodzajów oraz przyczyn błędów pojawiających się w oprogramowaniu. Proces składa się z następujących etapów [**honeywellFMEA**]:

1. **Przegląd analizy bezpieczeństwa**. Identyfikacja obszarów objętych ryzykiem wystąpienia błędów.

2. **Zdefiniowanie awarii**. Określenie wszystkich potencjalnych awarii, które mogą doprowadzić do niepoprawnej pracy systemu.

3. **Warunki prowadzące do awarii**. Zdefiniowane sytuacji, w których dochodzi do wystąpienia anomalii systemu, warunków wejściowych oraz wyjściowych. Ocena wpływu awarii na cały system.

4. **Przygotowanie scenariuszy testowych**. Stworzenie przypadków testowych, które mogą odtworzyć błędną pracę systemu.

5. **Wykonanie oraz analiza testów**. Sprawdzenie działania systemu w krytycznych dla niego warunkach. Określenie ryzyka występowania wady oraz działań zapobiegawczych.

Analiza danego scenariusza testowego składa się z następujących elementów [**honeywellFMEA**], [**fmeaWiki**]:

- nazwa testu,

- opis możliwego błędu,

- opis skutków błędu,

- przypisanie uciążliwości błędu (*ang. Severity Classification Category, SEV*) w skali 1 – 10; krytyczne błędy powinny posiadać wyższą wartość,

- opis przyczyny wystąpienia danego błędu,

- zdefiniowanie częstotliwości występowania (*ang. Occurrence Risk Category, OCC*) w skali 1 – 10; awarie pojawiające się częściej mają wyższą wartość,

- opisanie procedur zapobiegających wystąpieniu danego błędu,

- zdefiniowanie skuteczności wykrywania (*ang. Detectability Risk Category , DRC*) w skali 1 – 10; wada, która jest łatwiejsza w wykryciu powinna mieć przypisaną niższą wartość,

- obliczenie wartości ryzyka (*ang. Risk Priority Number, RPN*); $RPN = SEV \cdot OCC \cdot DET$.

FMEA jest narzędziem, które pozwala na ustalenie potencjalnych przyczyn oraz warunków awarii. Priorytet scenariuszy testowych jest zdefiniowany przez metrykę RPN. Im wyższa wartość tym wystąpienie danej awarii jest bardziej ryzykowne. Obliczenie wartości ryzyka jest kluczowe do określenia błędów, które powinny zostać poddane dalszym analizom.

2.3.2 Sieci Petriego

Systemy czasu rzeczywistego stały się istotnym elementem automatycznych technologii wykorzystywanych w samochodach autonomicznych, urządzeniach medycznych czy w lotnictwie. Proces projektowy tego typu systemów jest trudny ze względu na dużą złożoność komponentów, wymóg deterministyczności działania oraz spełnienie ograniczeń czasowych. Takie systemy muszą polegać na skutecznych metodach weryfikacji, które potwierdzą spełnienie wszystkich wymagań. Do tego celu wykorzystuje się sieci Petriego, które stanowią formalną reprezentację modelowanego systemu i pozwalają na analizę rozproszonych komponentów.

Model klasycznej sieci Petriego jest dwukierunkowym grafem zdefiniowanym przez trzy typy obiektów: miejsca, przejścia i łuki skierowane. Łuki łączą miejsca z przejściami lub przejścia z miejscami. W najprostszej postaci sieć Petriego może modelować zachowanie systemu podczas wystąpienia zdarzenia, definiując stany wejściowe oraz wyjściowe. W celu zbadania dynamicznego zachowania sieci stosuje się tzw. żetony, które mogą definiować dodatkowe parametry związane z danym miejscem podczas wystąpienia zdarzenia, może być to np. warunek prawda lub fałsz. Formalna definicja sieci składa się z 5 elementów $N = (P, T, I, O, M_0)$ [**petriIntro**]:

(1) $P = \{p_1, p_2, \ldots, p_m\}$ skończona liczba miejsc,

(2) $T = \{t_1, t_2, \ldots, t_n\}$ skończony zbiór przejść; $P \cup T \neq \emptyset$ oraz $P \cap T = \emptyset$,

(3) $I : P \times T \rightarrow N$ jest to funkcja wejściowa definiująca kierunek od miejsca do przejścia; N jest nieujemną liczbą całkowitą,

(4) $O : T \times P \rightarrow N$ jest to funkcja wyjściowa definiująca kierunek od przejścia do miejsca,

(5) $M_0 : P \rightarrow N$ jest to stan początkowy.

Graf sieci Petriego jest strukturą w postaci dwukierunkowego multigrafu, mającego dwa typy węzłów. Okrąg reprezentuje miejsce a prostokąt reprezentuje przejście. Ukierunkowane łuki (strzałki) łączą miejsca i przejścia. Łuk skierowany z miejsca p_j do przejścia t_i definiuje p_j jako miejsce wejściowe do t_i, oznaczone $I(t_i, p_j) = 1$. Łuk skierowany od przejścia t_i do miejsca p_j definiuje p_j jako miejsce wyjściowe t_i, oznaczane przez $O(t_i, p_j) = 1$ [**petriIntro**]. Przykładowy graf sieci Petriego został zaprezentowany na rys. **??**.

Matematyczny opis przejść w grafie przedstawionym na rys. **??** przedstawia się następująco:

$P = \{p_1, p_2, p_3, p_4\}$;

$T = \{t_1, t_2, t_3\}$;

$I(t_1,p_1) = 2$, $I(t_1,p_i) = 0$ dla $i = 2,3,4$;

$O(t_1,p_2) = 2$, $O(t_1,p_3) = 1$, $O(t_1,p_i) = 0$ dla $i = 1,4$;

$M_0 = (2\ 0\ 0\ 0)^T$.

Przykład przejścia t_1 został przedstawiony na rys. **??**. Stan sieci uległ zmianie i po wykonaniu przejścia jest określony przez $M_1 = (0\ 2\ 1\ 0)$.

Jako narzędzie matematyczne, sieci Petriego pozwalają projektantowi systemu na wnikliwą analizę oraz identyfikację właściwości funkcjonalnych, specyficznych dla domeny danej aplikacji. Bazowanie na standardowych grafach sieci Petriego, zaprezentowanych na rys. **??** oraz **??** może być niewystarczające, do modelowania rozbudowanych systemów czasu rzeczywistego.

Dla bardziej wymagających modeli stosuje się wysokopoziomowe sieci Petriego, które dodatkowo wprowadzają rozróżnialność żetonów oraz zależności czasowe. Wysokopoziomowe sieci to: kolorowe sieci Petriego (*ang. Colored Petri Net, CPN*), czasowe sieci Petriego (*ang. Timed Petri Net, TPN*), w których wyróżnia się sieć deterministyczną (*ang. Deterministic Timed Petri Net, DTPN*) oraz stochastyczną (*ang. Stochastic Timed Petri Nets, STPN*) [**petriIntro**].

Sieć CPN charakteryzuje to, że każdy żeton przynależy do danego koloru, co określa jego przynależność do danej grupy. Ponadto każde miejsce oraz przejście posiada dołączony zestaw kolorów. Podczas wykonywania przejść żetony są umieszczane w wyjściowym miejscu analogicznie jak w podstawowej sieci Petriego. Z tą różnicą, że zmianie ulegają jedynie żetony o kolorze, który jest określony w danym miejscu oraz w zadanym przejściu [**petriIntro**].

Kolejny rodzaj sieci – TPN charakteryzuje się wykorzystaniem zmiennych, określających zależności czasowe. Sieć deterministyczna – DTPN wykonuje przejścia co określony kwant czasu. Składa się ona z tych samych elementów co zwykła sieć, lecz dodatkowo zawiera parametr $\tau : T \rightarrow R^+$, który jest funkcją przejścia w deterministycznej dziedzinie czasu. Sieci STPN wykonują przejścia bazując na losowym prawdopodobieństwie. Czasowo wykładnicze, stochastyczne sieci Petriego zwane są SPN (*ang. Stochastic Petri Nets*). Składają się one z tych samych elementów co standardowa sieć, lecz dodatkowo zawierają parametr $\Lambda : T \rightarrow R$. Określa on szybkość wykładniczego indywidualnego rozkładu czasu przejść [**petriIntro**].

Sieci Petriego, które rozważają wpływ czasu podczas analiz, są jedną z najpopularniejszych metod wykorzystywanych do opisu systemów czasu rzeczywistego. Analizując sieci TPN projektant ma możliwość określenia dostępności danego systemu w dziedzinie czasu. Ocenie podlega przepływ informacji pomiędzy modułami oraz czy system jest w stanie przetworzyć określoną ilość zadań, zdefiniowaną w wymaganiach. Mając takie dane możliwe jest wyznaczenie poziomu wiarygodności systemu. Przykład wykorzystania sieci SPN w modelowaniu urządzeń awionicznych został opisany w rozdziale 2.3.3.

2.3.3 Zarządzanie błędami w awionice

Pomimo wszelkich starań inżynierów, stworzenie urządzeń, które będą działać bezbłędnie jest zadaniem bardzo trudnym. Nawet najlepiej opracowane systemy mogą być ofiarą czynników losowych, tj. promieniowanie kosmiczne, które może spowodować wystąpienie zjawiska SEU (*ang. Single Event Upset*) i wprowadzić urządzenie w stan nieokreślony. Aby przeciwdziałać takiemu zjawisku w systemach awionicznych wprowadza się moduły monitorowania (*ang. Health Monitoring, HM*) oraz zarządzania błędami (*ang. Fault Management, FM*).

Przykład zastosowania modułów HM/FM, które zostały oparte o stochastyczne sieci SPN został zaprezentowany przez chińskich naukowców, dla koncepcji zintegrowanej awioniki (*ang. Integrated Modular Avionics, IMA*) [**stochasticHMFMPetri**]. Podejście do tworzenia urządzeń w modelu IMA zakłada odejście od tradycyjnego modelu tworzenia odrębnej aplikacji dla każdego systemu, lecz tworzenie systemu, który wspiera różne rodzaje aplikacji. Dzięki takiemu rozwiązaniu wzrasta oszczędność masowa poprzez redukcję wielu podsystemów. Wprowadzenie modułów monitorowania oraz zarządzania błędami ma na celu zapewnienie wiarygodności, że system jest zdolny do prawidłowego działania nawet w przypadku wystąpienia błędów. Moduł HM jest odpowiedzialny za monitorowanie, identyfikację, lokalizację błędu oraz zgłoszenie go do modułu FM. W przypadku zgłoszenia awarii aktywowany jest moduł zarządzania błędami, którego zadaniem jest podjęcie odpowiedniej akcji mającej na celu przywrócenie poprawnej funkcjonalności systemu. Moduł monitorowania systemu odpytuje cyklicznie moduły na temat ich aktualnego stanu. W przypadku wykrycia anomalii procedura zapewnia aktywowanie systemu FM.

Wykorzystanie stochastycznych sieci Petriego w warstwie HM/FM umożliwia tworzenie zintegrowanego modelu, weryfikującego działanie systemu w dziedzinie czasu. Ponadto daje możliwość podzielenia systemu na warstwy i analizowanie ich wpływu na cały model [**stochasticHMFMPetri**]. Takie podejście zastosowali inżynierowie z Beijing dzieląc system na niezależne warstwy, gdzie każda z nich składa się ze współpracujących modeli HM oraz FM [**stochasticHMFMPetri**].

Moduł odpowiedzialny za monitorowanie błędów został podzielony na trzy części, przedstawione na rys. **??**. Część CQ (*ang. Current Layer Query*) odpowiedzialna jest za sprawdzanie stanu obiektów w losowych odstępach czasu. Podczas sprawdzania obiektu, po wywołaniu przejścia *Timer_C* zostaje wykonane przejście *Query_C* i bezpośredni powrót do stanu *Idle*, gdy nie występują żadne anomalie. W przypadku, gdy zostaje wykryty błąd aktywowany jest moduł FM poprzez przejście *Activate_FM1*, strzałka 3 wskazuje na obsługę błędu. Raport z przechwyconego błędu zostaje zlokalizowany w przejściu *Sub_Report*. Moduł RP (*ang. Reply*) odbiera zapytania od warstwy nadrzędnej, zbiera informacje i odsyła je do warstwy odpytującej. Ostatnia część SQ (*ang. Subordinate Layer QUery*) jest wykorzystywana przy ścisłej współpracy z pozostałymi warstwami systemu. Cyklicznie wysyła zapytania (strzałka 5) do innych warstw i po otrzymaniu pozytywnych odpowiedzi (strzałka 6) powraca do stanu *Idle*, w przeciwnym razie następuje obsługa błędu.

Moduł odpowiedzialny za zarządzanie błędami został przedstawiony na rys. **??**. Składa się on wielu mniejszych modułów, z których każdy jest odpowiedzialny za obsługę określonego błędu. Każda akcja naprawcza kończy się stanem pozytywnym lub negatywnym. Rezultaty działania modułu FM są kolekcjonowane w *Error_Report_Pool* i przesyłane do modułu HM.

Komunikacja między warstwami jest specyfiką danego systemu. Stosuje się rozwiązania, które zakładają, że moduły zarządzania błędami mogą odnosić się do pozostałych warstw w przypadku negatywnej obsługi danej anomalii. Zostało to przedstawione na przykładzie części SQ modułu HM.

Zaprezentowany model wykorzystania sieci Petriego w urządzeniach IMA znajduje zastosowanie w przypadku badania technologii WAIC w systemie AHRS. Moduły monitorowania oraz zarządzania błędami posiadają duży potencjał do zarządzania komunikacją bezprzewodową. Wykorzystanie analizy FMEA oraz sieci SPN umożliwia przeprowadzenie procesu weryfikacji systemu. Skorzystanie z tych narzędzi pozwala na wstępną analizę problemu oraz sporządzenie modelu obsługi błędów. Wynikiem tego procesu jest wyznaczenie metryk związanych z oszacowaniem średniego czasu naprawy systemu, dostępności systemu oraz prawdopodobieństwem wystąpienia awarii.

3 SYSTEM AHRS

3.1 Zasada działania

TO DO

3.2 Redundancja

TO DO

3.3 Mechanika

TO DO

3.3.1 Moduł pilota

TO DO

3.3.2 Moduł akwizycji danych

TO DO

3.4 Elektronika

TO DO

3.4.1 Moduł pilota

TO DO

3.4.2 Moduł akwizycji danych

TO DO

3.5 Oprogramowanie

TO DO

3.5.1 Moduł pilota

TO DO

3.5.2 Moduł akwizycji danych

TO DO

4 ARCHITEKTURA OPROGRAMOWANIA

4.1 Struktura projektu

TO DO

4.2 Wykorzystane narzędzia

TO DO

4.3 Moduł pilota

TO DO

4.3.1 Struktura oprogramowania

TO DO

4.3.2 Interfejs użytkownika

TO DO

4.3.3 Komunikacja

TO DO

4.4 Moduł akwizycji danych

TO DO

4.4.1 Struktura oprogramowania

TO DO

4.4.2 Kąty orientacji przestrzennej

TO DO

4.4.3 Odbiornik GPS

TO DO

4.4.4 System uzgadniający

TO DO

4.5 Redundancja oprogramowania

TO DO

4.5.1 Zakłócenia SEU

TO DO

4.5.2 Watchdog

TO DO

4.5.3 Oprogramowanie symulacyjne

TO DO

5 TESTY

5.1 Symulacje

TO DO

5.2 Testy w locie

TO DO

5.3 Podsumowanie

6 OPRACOWANIE WYNIKÓW

6.1 Analiza FMEA

TO DO

6.2 Sieć Petriego

TO DO

6.3 Analiza bezpieczeństwa

TO DO

6.4 Wiarygodność technologii WAIC

TO DO

7 PODSUMOWANIE

DODATEK A. Zawartość płyty CD

Wykaz symboli i skrótów

AHRS Attitude Heading Reference System

COTS Commercial–Off–The–Shelf

CPN Colored Petri Net

DAL Design Assurance Level

DTPN Deterministic Timed Petri Net

FAA Federal Aviation Administartion

FM Fault Management

FMEA Failure Mode and Effects Analysis

HM Health Monitoring

ICAO International Civil Aviation Organinzation

IIoT Industry Internet of Things

IMA Integrated Modular Avionics

ITU International Telecomunication Union

RAs Radio Altimeters

SEU Single Event Upset

SPN Stochastic Petri Nets

STPN's Stochastic Timed Petri Nets

TPN Timed Petri Net

WAIC Wireless Avionics Intra–Communication

Spis rysunków

Spis tablic

1 Poziomy bezpieczeństwa – DAL. *Źródło: [***honeywellFMEA***]* 13