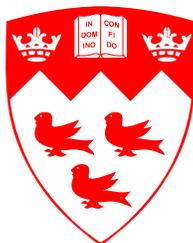


Aircraft Wireless Networks for Safety-Critical Systems

Ahmad Muannaki



Electrical Engineering
McGill University
Montreal, Canada

August 2020

A thesis submitted to McGill University in partial fulfillment of the requirements for the degree of Master of Engineering

© Ahmad Muannaki 2020

Abstract

Wireless avionics intra communication (WAIC) connects avionics integrated on board a single aircraft in a closed exclusive wireless network in lieu of heavy and expensive wired deployments. Recently, the International Telecommunication Union (ITU) approved the frequency band 4.2-4.4 GHz for WAIC which promises weight savings and cost reductions. However, wireless avionics must meet extremely high reliability requirements for flight certification by safety aviation authorities. Current industrial wireless networks, which are based on IEEE 802.15.4 and IEEE 802.11 standards, have been proposed as potential solutions for safety-critical systems. A promising candidate is IEEE 802.15.4e which uses Time-Slotted Channel Hopping (TSCH) to provide reliable packet transmission. We performed experiments consisting of IEEE 802.11 and IEEE 802.15.4e and utilized a recently published mathematical model to evaluate their failure probability with respect to loss of packets. Our results indicated that the allowed packet loss probability for IEEE 802.11 is between 0.045 and 0.35 for safety-critical systems to meet the DO-178C reliability standard. Furthermore, the IEEE 802.15.4e with TSCH protocol respects the DO-178C reliability standard with a failure probability of 10^{-5} per hour but failed the DO-160G standard due to electromagnetic interference.

Résumé

La communication intra avionique sans fil (WAIC) connecte l'avionique intégrée à bord d'un seul avion dans un réseau sans fil exclusif fermé au lieu de déploiements câblés lourds et coûteux. Récemment, l'Union internationale des télécommunications (ITU) a approuvé la bande de fréquences 4,2-4,4 GHz pour WAIC, ce qui promet des économies de poids et des réductions de coûts. Cependant, l'avionique sans fil doit répondre à des exigences de fiabilité extrêmement élevées pour la certification de vol par les autorités de l'aviation de sécurité. Les réseaux sans fil industriels actuels, basés sur les normes IEEE 802.15.4 et IEEE 802.11, ont été proposés comme solutions potentielles pour les systèmes critiques pour la sécurité. Un candidat prometteur est IEEE 802.15.4e qui utilise le saut de canal à intervalles temporels (TSCH) pour fournir une transmission de paquets fiable. Nous avons effectué des expériences consistant en IEEE 802.11 et IEEE 802.15.4e et avons utilisé un modèle mathématique récemment publié pour évaluer leur probabilité de défaillance par rapport à la perte de paquets. Nos résultats indiquent que la probabilité de perte de paquets autorisée pour IEEE 802.11 est comprise entre 0,045 et 0,35 pour que les systèmes critiques pour la sécurité satisfassent à la norme de fiabilité DO-178C. De plus, le protocole IEEE 802.15.4e avec TSCH respecte la norme de fiabilité DO-178C avec une probabilité de défaillance de 10^{-5} par heure mais a échoué à la norme DO-160G en raison d'interférences électromagnétiques.

Acknowledgments

First and foremost, I would like to express my sincere gratitude to Professor Brett H. Meyer for his support, guidance, and most importantly, patience. This work would not have been possible without his supervision and I am truly grateful for this opportunity.

I would also like to thank Professor Ioannis Psaromiligkos for taking the time to examine my thesis thoroughly, and for his valuable recommendations.

To my RSSL peers, thank you to Alex, Derek, and Shabbir. We had some very interesting discussions late evenings and during weekends. I'm glad to have spent time together during my research journey.

To my Montreal colleagues, I would like to thank Stéphane and Yannick for helping me manage work and academia. Your support during the beginning was crucial to my success.

To my Hamburg colleagues, a big thanks to Felix, Jan, Jörg, Peter, and Samer who taught me the German way of doing things. You were the last push I needed to complete my work.

To my friends Bassam, Dave, and both Sids, thank you guys for your true friendship and also your understanding whenever I could not hang out. From now on, there will be no more "The thing is..."

Lastly, to my father, mother, sister, and brother, no word can describe how thankful I am for your genuine, selfless, and unconditional love, and of course, for listening to me complain for more than three years.

Contents

1	Introduction	1
1.1	Challenges	4
1.2	Thesis Contribution	5
2	Related Work	6
2.1	Academic Research	6
2.1.1	Reliability Performance Comparison	6
2.1.2	Network Protocol Candidates	7
2.1.3	Surface Acoustic Wave	7
2.1.4	Coexistence with Radio Altimeters	7
2.1.5	Security Assessment	7
2.2	Industry Projects	8
2.3	Regulatory Oversight	8
2.4	Summary	9
3	Wireless Avionics	10
3.1	Background	10
3.2	Technical Characteristics and Challenges	11
3.2.1	Introduction	11
3.2.2	Frequency	11
3.2.3	Data Rate	12
3.2.4	Transmit Power	12
3.2.5	Reliability	13
3.2.6	Security	13
3.3	Major Components and Network Topology	14
3.4	Wireless Network Protocols	16
3.4.1	Introduction	16
3.4.2	IEEE 802.15.1	16
3.4.3	IEEE 802.15.4	17
3.4.4	IEEE 802.15.4e	17

4	Flight Certification and Failure Probability	18
4.1	Introduction	18
4.2	System Model	19
4.3	Flight Certification Reliability Model.....	21
5	Experiments and Results.....	23
5.1	Introduction	23
5.2	WISA Simulation.....	23
5.3	Low-Rate Wireless Experiment	25
5.3.1	Electromagnetic Interference	27
5.3.2	Join Duty Cycle	30
5.3.3	Time Delay.....	32
5.3.4	Reliability.....	34
6	Conclusion and Future Work	36
6.1	Conclusion.....	36
6.2	Future Work.....	37
7	Bibliography	38

List of Figures

Figure 1-1: Aircraft Loss Rates per Million Flights [54]	2
Figure 3-1: Major Components of an Aircraft [3]	14
Figure 3-2: Aircraft Wireless Network Topology.....	15
Figure 4-1: WAIC System Model	20
Figure 5-1: Failure Probability Performance for WISA.....	24
Figure 5-2: LR-WPAN Experimental setup with sending and received motes (left). Sending mote consisting of IEEE 802.15.4e TSCH based wireless board and Arduino due board (right).....	25
Figure 5-3: LR-WPAN LRU System Model	26
Figure 5-4: Data Packet of Transmitted Signal.....	27
Figure 5-5: 800 MHz to 6 GHz Sweep with Door Open.....	27
Figure 5-6: 800 MHz to 6 GHz Sweep with Door Closed and Limit Line	28
Figure 5-7: (a) Amplitude at 3 Minutes [Top Left], (b) Amplitude at 15 Minutes [Top Right], (c) Amplitude at 20 Minutes [Bottom Left], and (d) Amplitude at 40 Minutes [Bottom Right]	30
Figure 5-8: Join Duty Cycle Results	31
Figure 5-9: Time Delay for Data Packets with (a) 10s Period, (b) 5s Period, (c) 1s Period, and (d) 250ms Period	32
Figure 5-10: Average Time Delay Plot.....	33
Figure 5-11: Lost Packets with 250ms Data Period.....	34

List of Tables

Table 1-1: Wireless Avionics Specifications and Challenges	4
Table 4-1: Classification and Failure Rate of DAL.....	19
Table 5-1: WISA Probability Failure Equation Variables	24

List of Acronyms

6LoWPAN	IPv6 over Low Power Wireless Personal Area Network
ARNS	Aeronautical Radio Navigation Service
ASMT	Advanced Subminiature Telemetry
AVSI	Aerospace Vehicle Systems Institute
DAL	Design Assurance Level
DSSS	Direct Sequence Spread Spectrum
EASA	European Aviation Safety Agency
EFB	Electronic Flight Bag
EGPWS	Enhanced Ground Proximity Warning System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FBW	Fly-by-Wireless Alliance
FDD	Frequency Division Duplex
FLITE-WISE	Flight Instrumentation Test Wireless Sensor
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISM	Industrial, Scientific, and Medical Frequency Bands
ITU	International Telecommunication Union
LTE	Long Term Evolution
LR-WPAN	Low-Rate Wireless Personal Area Networks
LRU	Line-Replaceable Unit
MAC	Medium Access Control
MASPS	Minimum Aviation System Performance Standard
MOPS	Minimum Operational Performance Standard
NASA	National Aeronautics and Space Administration
OQPSK	Offset Quadrature Phase Shift Keying
PHY	Physical Layer
QoS	Quality-of-Service
RA	Radio Altimeters
RTCA	Radio Technical Commission for Aeronautics
SAW	Surface Acoustic Wave
SARPS	Standards and Recommended Practices
SCOTT	Secure Connected Trustable Things
TCAS	Traffic Collision Avoidance System
TCCA	Transport Canada Civil Aviation
TDMA	Time-Division Multiple Access
TSCH	Time-Slotted Channel Hopping
WAIC	Wireless Avionics Intra Communication
WICAS	Wireless Interconnectivity and Control of Active Systems
WISA	Wireless Interface for Sensors and Actuators

1 Introduction

Today, we live in the highest aviation safety era. The term aviation has become analogous to safety due to the full and constant cooperation among worldwide regulatory authorities, safety volunteer organizations, various industrial working groups, and international research collaboration. Government regulatory authorities such as the Federal Aviation Administration (FAA), Transport Canada Civil Aviation (TCCA), and European Aviation Safety Agency (EASA) are constantly forming new agreements under the umbrella of the International Civil Aviation Organization (ICAO) to govern most aviation activities as well as new technologies across the world. Examples of technical improvements that were introduced are the Enhanced Ground Proximity Warning System (EGPWS), Traffic Collision Avoidance System (TCAS), and Electronic Flight Bag (EFB) [40]. In the last decade, overall safety performance improved and industry measures have resulted in a 70% reduction in the accident rate, from 3.60 per million flights in 2008 to 1.08 per million flights in 2017 [54]. Moreover, as Figure 1-1 shows, total aircraft loss has been on a decline since 2012 and that the worst rate in 2017 was only 0.92 per million flights [54].

The terms “Fly-by-Wireless” and “All-Connected Aircraft” have become increasingly popular with the advent of the fourth industrial revolution or what is also known as “Industry 4.0” [67]. Recently, the aerospace industry has begun to research the idea of wireless avionics networks in lieu of the current wired deployments [55]. This is due to the benefits that wireless networks provide in terms of business, engineering, and environmental aspects. As a result, the aviation industry is developing wireless avionics intra-communication (WAIC) which is a development effort headed by the Aerospace Vehicle Systems Institute (AVSI) [1].



Figure 1-1: Aircraft Loss Rates per Million Flights [54]

Moreover, the Radio Technical Commission for Aeronautics (RTCA) and European Organization for Civil Aviation Equipment (EUROCAE) have formed working groups to develop, classify, and standardize this new system in order to meet the stringent requirements as set by this industry [56-57].

WAIC is an aircraft wireless system that connects avionics integrated on board a single aircraft in a closed exclusive network [1]. In 2015, the ITU voted to grant a frequency band for WAIC and the development of safety standards was initiated by ICAO [2]. For its part, the international telecommunication union (ITU) has defined important wireless system technical characteristics such as the frequency band (4.2 – 4.4 GHz), data rate (10 Kbps – 1 Mbps), and transmit power (10 – 50 mW) [3]. Moreover, extremely low failure probability is a must for safety-critical aircraft systems. Failure probability is defined as the likelihood that a system does not perform its intended function due to unintentional conditions and for the case of wireless avionics, the failure probability is mainly driven by loss of packets. There has not been sufficient research conducted in the direction of network reliability in this domain and until now, communication networks have been engineered with a focus on improving network capacity with little attention to latency or packet reliability [58].

Benefits:

There is a strong focus and immense interest from major aviation industry players in developing wireless avionics technology due to its many promising benefits. Aircraft manufacturers as well as avionics suppliers are laying the foundations for the future

aircraft to be more efficient, effective, and safer. For example, an Airbus A380 has around 530 km of cables due to 100,000 wires, 40,000 connectors, and 500,000 harness items [4]. However, aircraft wiring has severe drawbacks [5]:

- Cable routing is a daunting task where electromagnetic interference needs to be taken into account.
- A wire harness can only be installed in a specific location where it can be accessed and it needs to survive harsh environment conditions.
- Long wire installation in certain structures is time-consuming and labor-intensive.
- Degradation of wiring has the potential to cause unsafe flights.

It is estimated that between 2% to 5% of an aircraft's weight and all associated costs could be reduced by a reduction in complexity of electrical wiring harness design, harness fabrication, and wiring weight [6]. As an example, it is estimated that Blackhawk helicopters, which carry around 2,000 pounds of wires, will bring a 12% increase in terms of fuel efficiency and a 15% lighter design [7]. This leads to a measurable increase in maintenance efficiency, configurability, and environmental protection. Similarly, it was shown that using wireless control systems can eliminate around 90 and 267 pounds which is roughly between 1.5% to 2% of the total weight in Cessna 310R and SH60, respectively [12]. Another advantage is the reduction of installation time of aircraft systems, maintenance, repair, and overhaul [5]. Moreover, cabling fabrication and installation have a cost of 2,200 dollars per kg of aircraft and therefore savings can reach anywhere between \$14 to \$60 million dollars per aircraft [9].

Wireless avionics systems have the potential to improve flight safety and operational efficiency [2]. For example, deployment of wireless airflow actuators and sensors on certain locations to provide real-time information as well decision metrics leads to efficient closed-loop airflow control operation [23]. Furthermore, wireless actuators and sensors open up the possibility of other new functionality such as monitoring inaccessible moving, rotating parts, self-configuration, radio frequency tolerance, and maintenance troubleshooting [10, 24]. Wireless networks can add redundant links to any critical system which enhances their reliability as well as flexibility [5].

1.1 Challenges

Although wireless avionics systems promise many technical, business, and environmental advantages, there are challenges that arise as a consequence of their characteristics as well as system design. Table 1-1 summarizes the challenges that a wireless avionics system faces due to the defined technical specification.

First, the frequency band that has been granted by the ICAO for WAIC applications is also used by aeronautical Radio Altimeters (RA) which operate onboard the same as well as different aircraft [1]. This is a major concern by safety organizations due to the risk of harmful interference between 4200 MHz and 4400 MHz [13]. Second, the interior structure of an aircraft can cause severe propagation issues [2]. Third, wireless networks must respect the data rate and transmit power level conditions for each component based on their location and functionality as defined in the ITU report [2]. Fourth, security measures that need to be in place so that wireless networks can protect WAIC systems against malicious attacks [16]. Fifth and most importantly is the certification requirement that any wireless network responsible for the communication between safety-critical systems needs to have extremely low failure probability [6]. This probability will depend on the criticality of each component and thus will range from 10^{-9} to 10^{-3} per flight hour [17].

Table 1-1: Wireless Avionics Specifications and Challenges

Type	Range	Description	Challenge
Frequency	4.2 – 4.40 GHz	WAIC communicates through frequency band 4.2 – 4.4 GHz.	Interference between WAIC and radio altimeter systems due to shared frequency band. Coexistence between WAIC systems. Interference with other man-made technologies inside or outside an aircraft.
Location	Inside (I) – Outside (O)	Physical architecture comprised of nodes inside or outside an aircraft.	Obstructed radio propagation paths inside aircraft due to compartment structure. Severe propagation issues between nodes.
Data Rate	<10 Kbps - 1 Mbit/s	Data rates less than 10 Kbps are considered low data rate applications and high data rate applications have data rate higher than 10 Kbps up to 1 Mbps	Wireless networks to respect data rate conditions with respect to location of node. WAIC systems cannot require more than upper limit of high data rate.
Power	10 – 50mW	Low maximum transmit power levels range from 10mW to 50mW.	Each application must meet the maximum transmit power level assigned according to its classification.
Security	Security measures	Certification regulation regarding protection against inadvertent or deliberate control.	Security measures need to be set in place to protect against malicious attacks. Wireless networks must respect the DO-356 guideline [21]. Authentication, data encryption and integration capabilities need to be developed.
Safety	10^{-9} - 10^{-3} per flight hour	Certification regulation regarding reliability of wireless network protocols for safety-critical systems.	Extremely low failure probability of WAIC system between 10^{-9} and 10^{-3} per flight hour. Each system must meet its criteria based on the DO-178C guideline [17]. Required to show compliance for safety of flight certification.

1.2 Thesis Contribution

Due to the enormous field of wireless technology and the many complex factors of aircraft systems, research throughout the years has largely been tailored to specific subsystems as well as functions, thus taking into account only limited conditions. Currently, there is no wireless standard for extremely reliable communication between safety-critical systems. However, many existing wireless networks have been proposed for industrial automation systems and some are being considered a fundamental infrastructure technology for critical control systems such as avionics control systems [59]. These wireless communication technologies have the potential to be applied for the safety-critical flight control systems [6]. The most frequently adopted communication standards for those wireless networks are IEEE 802.15.4 and IEEE 802.11 [59]. A promising candidate is the IEEE 802.15.4e with some enhancements to provide reliable packet transmission guarantees [59].

We performed several experiments consisting of IEEE 802.15.4e wireless boards and analyzed radio-frequency emission, join duty cycle, time delay, and reliability with respect to safety regulation. Moreover, we performed a simulation based on IEEE 802.11 and derived its packet loss and failure probabilities. Afterwards, we utilized a recently published mathematical model [6] to evaluate both wireless protocols with respect to failure probability and flight certification.

Our results showed that under certain conditions, wireless boards based on IEEE 802.15.4e reached a failure probability of 10^{-5} per hour which is compliant with safety-critical systems classified as minor as well as major. The IEEE 802.11 simulation showed that the packet loss probability as per flight certification is between 0.045 and 0.35 for safety-critical systems classified as catastrophic and minor, respectively.

2 Related Work

A WAIC committee was formed in 2008, made up of safety authority organizations, key aerospace industry players, and academic institutes in order to develop wireless communication technology for safety-critical aircraft systems [61]. As a result, there has been an increase in the amount of academic research, industry projects, and regulatory oversight regarding wireless avionics.

2.1 Academic Research

Academic research revolved around wireless avionics with respect to several diverse fields in recent years. These fields are grouped into different categories such as reliability performance comparison, network protocol candidates, surface acoustic wave, coexistence with radio altimeters, and security assessment.

2.1.1 Reliability Performance Comparison

In 2017, Park and Chang proposed a mathematical model to evaluate and compare the reliability performance of potential WAIC protocols [6]. A similar study was performed in 2020 which evaluated different commercial off-the-shelf wireless protocols for introducing avionics wireless networks [11]. The initial paper concluded the importance for the performance analysis to consider the extremely high demand of flight certification while the latter indicated that IEEE 802.15.4 based Zigbee protocol is better suited for low-data applications [6][11].

2.1.2 Network Protocol Candidates

A 2016 paper identified network design issues and synergies with respect to existing technologies [20]. The feasibility of IEEE 802.11 protocols was analyzed in real aircraft environment [30]. In 2018, an extensive literature review discussed aircraft wireless networks with a specific focus on their requirements [5]. The suitability of Long Term Evolution (LTE) and 5G wireless technologies for low data rate WAIC applications was investigated through analytical models as well as hardware experiments [32].

2.1.3 Surface Acoustic Wave

A paper discussed the potential of 4.3 GHz passive wireless surface acoustic wave for WAIC sensors and systems [38]. Similarly, a sensor operating in the WAIC band using SAW was demonstrated [33].

2.1.4 Coexistence with Radio Altimeters

In 2014, WAIC systems compatibility with radio altimeters was investigated in the 4.2–4.4 GHz frequency band through simulation [62]. In the same year, a measurement campaign was carried out to assess the degree of coupling between WAIC and RA antennas involving one or two aircraft [63]. The year after, an assessment was presented which analyzed the impact of interference caused by transmissions of wireless avionics intra-communication systems onto aeronautical radio altimeter [39]. A team at Hokkaido University investigated EMC issues with WAIC and RA systems through the development of an electromagnetic field estimation method on large-scale finite-difference time-domain analysis [31]. Researchers in Hamburg proposed a scheduling algorithm as well as a radio channel access scheme with the goal to analyze the coexistence of WAIC networks [34]. A similar work was also performed but which considered the frequency hopping with collision avoidance approach [35].

2.1.5 Security Assessment

From a security perspective, a paper presented a framework for medium access control and physical cross-layer security design of WAIC [36]. Using the Secure Connected Trustable Things (SCOTT) approach, a study derived preliminary conclusions of the

vulnerabilities and security solutions across different entities and layers of the aeronautics wireless architecture [37]. Another paper proposed three approaches to establish such a secure channel based on pre-shared keys, trusted key distribution, and key-sharing protocols [24].

2.2 Industry Projects

Apart from academic research, industrial institutes began researching wireless systems in aircraft through different projects starting in early 21st century [5]. For example, the Wireless Interconnectivity and Control of Active Systems (WICAS) project applies wireless connectivity to aircraft wing active flow control [25]. The Flight Instrumentation Test Wireless Sensor (FLITE-WISE) project facilitates the continuous monitoring of European aircraft without the unnecessary burden presented by wires [26]. The SAHARA project targets wireless sensors applied on aircraft, helicopters, and space vehicles [27]. United States Air Force has started the Advanced Subminiature Telemetry (ASMT) program which is aimed at developing an aircraft wireless sensor network for aircraft ground and flight test monitoring [28]. The Flyby-Wireless (FBW) Alliance led by NASA Langley Research Center announced to fund four research projects to apply wireless sensor networks for aircraft health monitoring systems [29]. The European Project SCOTT aims to build trust of IoT in industrial applications which includes aeronautics [37]. A NASA team performed experiments to expose some of the challenges faced by a wireless communication system inside the reflective cavity of an aircraft and explored solutions that took advantage of that environment for constructive gain [15]. The WAIC program by AVSI is leading the technical development of wireless avionics and is open to organizations worldwide that have a stake in the use of wireless communications on board aircraft [1].

2.3 Regulatory Oversight

Since ITU completed the technical specifications of WAIC and approved the use of the 4.2 – 4.4 GHz frequency band, international safety standards were required to protect the operation of WAIC systems and radio altimeters [2]. ICAO is tasked with developing Standards and Recommended Practices (SARPS) to prevent interference between WAIC

systems and radio altimeters in order to ensure the safe operation of aircraft [2]. The other two important standards are the Minimum Aviation System Performance Standard (MASPS) and the Minimum Operational Performance Standard (MOPS) which provide high-level guidance to ensure coexistence of multiple WAIC systems on board different aircraft [2]. They are developed jointly by the RTCA and EUROCAE and overseen by the FAA and EASA, respectively [56-57]. At the time of writing, a draft of the MASPS was completed and sent to ICAO for review. These standards form the basis for certification of future WAIC systems [1].

2.4 Summary

The past work covers different aspects of wireless aircraft systems from research, industrial, and regulatory perspectives. The topic that has the most attention is the coexistence of wireless avionics and radio altimeters. Moreover, a considerable amount of work analyzed potential network protocols for aircraft networks. However, only a handful of those activities focused on the stringent reliability requirements of aircraft wireless networks for safety-critical systems. Even then, most of them were performed through theoretical means which is not sufficient for flight certification. Our work tackles this reliability challenge through a hybrid approach that includes simulation and experiments of existing network protocols and applies a novel mathematical model to link our reliability findings with flight certification. This is crucial for future WAIC systems to prove the same level of communication reliability as their wired counterparts as part of the airworthiness certification process.

3 Wireless Avionics

3.1 Background

Avionics started to be developed using digital techniques in the 1960s and the early 1980s saw the full authority digital engine control (FADEC) being commonly used [40]. The technological advancement of avionics went through several stages from hardwired relays, through analog electronics, and into embedded computing [40]. For example, a part-digital electronic engine control was applied ten years before FADEC was introduced [40]. The same applied to flight controls where there was always either a mechanical or digital backup control before backups were completely removed.

The objective of wireless avionics is to become the primary method of communication between safety-critical systems onboard an aircraft. However, since aviation is a highly regulated industry with safety as the number one priority, wireless communication can be initially utilized as additional redundancy to already existing wired systems in aircraft. This technology can then transition from a backup role to the primary means of communication only after it gains the required confidence and majority of support from governmental safety authorities as well as key industry players.

The WAIC initiative is laying the foundation of wireless avionics. One of the main steps is to specify the technical characteristics of such systems. Another important consideration is to define the overall topology of wireless systems in an aircraft environment. Furthermore, since WAIC introduces the wireless signal in lieu of signal wire, this raises a major concern in regards to packet reliability due to interference, fading, and noise. It should be noted that for the case of wireless avionics and to the extent of this study, the circumstances that

impacts reliability is assumed to be mainly loss of packets. Therefore, existing network protocols are identified as potential candidates to mitigate that risk. This section describes the technical characteristics, topology, and network protocols of wireless avionics.

3.2 Technical Characteristics and Challenges

3.2.1 Introduction

The technical characteristics of WAIC systems were discussed and provided by the ITU [3]. The ITU has the responsibility to provide the latest information regarding WAIC to the aviation industry [3]. This section details the most recent technical characteristics as specified by the ITU and describes their challenges.

3.2.2 Frequency

In a WAIC system, components communicate over short distances in a single aircraft in the frequency band 4.2 – 4.4 GHz [13]. This frequency band was selected based on an assessment of bands between 960 MHz and 15.7 GHz by the ITU [14]. The ITU concluded that frequency bands below 960 MHz were not considered feasible due to the fact that the required antenna sizes to operate in this band are incompatible with WAIC requirements and frequency bands above 6 GHz were not taken into consideration [14]. Moreover, the frequency bands 2.7 – 2.9 GHz and 5.35 – 5.46 GHz were not found to be appropriate candidates due to potential impact of radar systems on WAIC systems [14]. As a result, studies in [14] showed that compatibility between WAIC systems and already existing systems was in the frequency band 4.2 – 4.40 GHz and this was the only possible option under 15.7 GHz. However, the frequency band 4.2 – 4.4 GHz is currently allocated to the aeronautical radio navigation service (ARNS) for radio altimeters (RAs) installed on board aircraft, which causes coexistence problems and potential interference between WAIC and RAs [15]. Also, there is the problem where WAIC systems interfere with one another. Currently, mitigation techniques that are based on channel hopping are being developed in order to overcome this issue [34, 35]. Other challenges regarding the use of the frequency band 4.2 – 4.4 GHz are due to certain technologies such as portable electronic devices, satellite communications, and so forth, which are common inside as well as outside an

aircraft [16]. These factors result in the degradation of both data rate and quality-of-service (QoS) and in extreme cases, a network collapse [16].

3.2.3 Data Rate

Points of communication of WAIC systems may include integrated wireless components and/or installed components of the system [3]. The ITU classifies wireless avionics components as either low or high data rate [3]. Data rate applications are grouped into two categories: low and high data rate applications. Low data rate applications have a data rate less than 10 kbit/s and high data rate applications have data rate higher than 10 kbit/s [3]. The expected average data rates located inside and outside an aircraft range between 12.5 kbit/s and 1.6 Mbit/s and between 45 kbit/s to 1 Mbit/s per single data link, respectively [3]. WAIC systems must conform to the data rate requirements and are prohibited to exceed the specified limit based on their location and functionality.

3.2.4 Transmit Power

Wireless avionics faces another requirement which is the maximum allowed transmit power level [19]. A low rate application that is located outside will have a different power requirement than a high rate one located inside an aircraft. In short, the low maximum transmit power level is set to 10mW for low rate applications and the transmit power for high rate applications cannot exceed 50mW [19]. This is due to the fact that wireless avionics are designed to be low power so that signals do not reach ground stations or other aircraft flying nearby. This is in-line with the basic objectives of the WAIC committee, namely, that it does not provide off-board air-to-ground, air-to-satellite, or air-to-air service [19]. Since WAIC encompasses only on-board electronics of the same aircraft, off-board electronics transmitting to an aircraft cannot use the allocated WAIC frequency band [19]. Moreover, the low power specification also constrains data streaming inside an aircraft. This also follows one of the basic objectives that WAIC does not provide communications for passengers or in-flight entertainment [19].

3.2.5 Reliability

The reason why aerospace is such a highly regulated industry is due to the importance of safety of human beings. Aircraft components are classified in terms of criticality as set by the DO-178B/C Software Considerations in Airborne Systems and Equipment Certification [17]. Certification authorities require that any wireless network that is responsible for the communication between safety-critical systems will need to have extremely low failure probability [6]. In this study, the failure probability of wireless systems is assumed to be primarily due to loss of packets. Components classified from 'A' to 'D' are considered safety-critical and components classified as 'E' are considered as not safety-critical [17]. Moreover, the levels of safety-critical systems are subdivided between catastrophic, hazardous, major, and minor [17]. As an example, a level 'A' system is considered catastrophic and will require a failure probability of 10^{-9} per flight hour [18]. On the other hand, a level 'D' system is considered as minor and thus will require a failure probability of 10^{-3} per flight hour [18]. Therefore, in order for wireless avionics to meet this stringent reliability requirement and be allowed to fly, their network protocol should be designed to maintain high quality of service in terms of time delay, bandwidth utilization, join duty cycle, and data loss due to packet collisions [22].

3.2.6 Security

Security threats are emerging and must be covered by wireless avionics systems [42]. Security is vital because it directly deals with the safety of passengers on-board an aircraft. Since wireless avionics are responsible for the correct functioning, management and safety of an aircraft, they should be robust to all kinds of malicious attacks from on-board passengers as well as people on the ground or other aircraft [20]. There is a need to address security threats including safety threats, channel jamming attacks, unauthorized introduction and modification of data, denial or loss of service, gradual degradation of service and introduction of misleading or false data [22]. The FAA has released in 2014 an airworthiness and security methods and considerations guidance to recommend measures so that aircraft manufacturers and suppliers are protected from intentional unauthorized electronic interference [21].

3.3 Major Components and Network Topology

The term avionics can be thought of as a combination of aviation + electronics; in other words, an embedded system with application software which performs real-time functions in an aircraft. Avionics can be made up of one or many line-replaceable units (LRUs) which are hardware components that can be replaced in a relatively short amount of time. Wireless avionics add an additional layer which is the radio frequency component required to send and receive data through a reliable and secure wireless medium.

At the time of writing, there is no clear definition of what wireless avionics should consist of and whether or not it should have the capability to interface with wired systems. In this work, wireless avionics are defined as any already existing avionics that have the functionality to transmit and receive wireless data as well as sensors and actuators with the same capability albeit on a lesser scale regarding processing power. The controller and the memory make up the computing core of wireless avionics [5]. The controller transmits and receives data to and from other LRUs via wireless radio. Also, it process data sent from sensors and decides on the actuators' behaviors via the I/O interface [41].

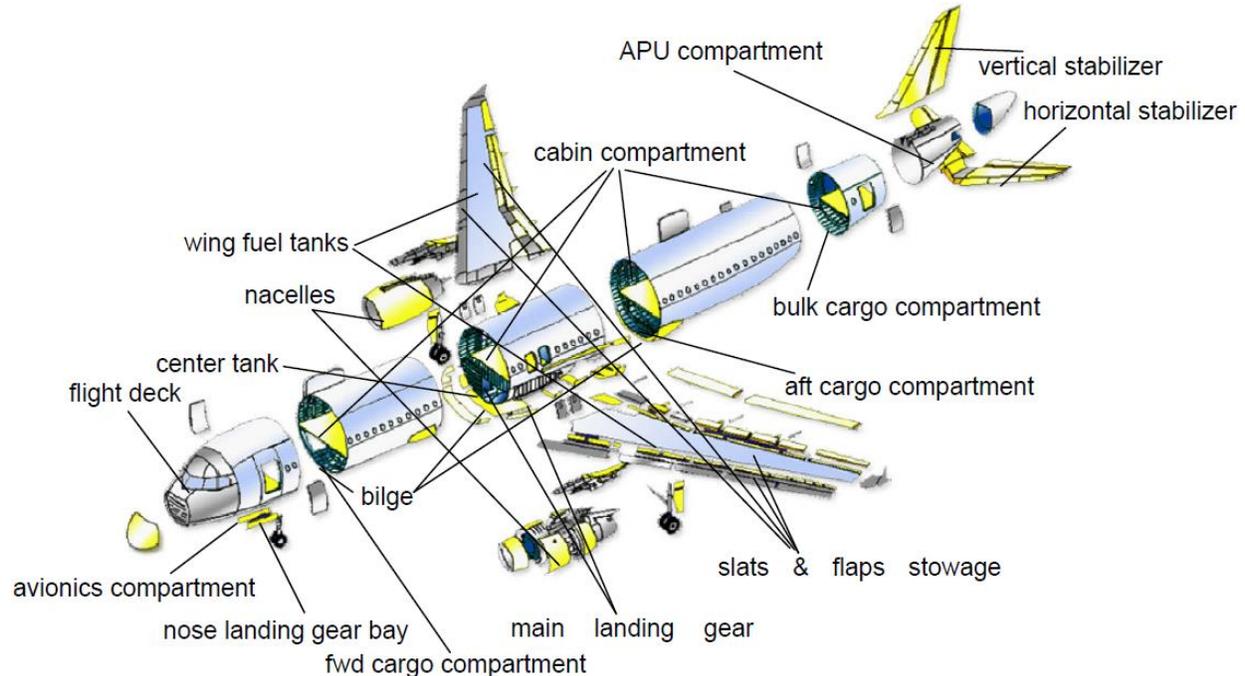


Figure 3-1: Major Components of an Aircraft [3]

An aircraft is comprised of many compartments and each compartment houses certain LRUs, sensors, and/or actuators. Figure 3-1 depicts the major compartments of a typical aircraft and their location. The ITU report anticipates that radio coverage is provided to those compartments via wireless networks which are made up of gateway nodes and connected to an onboard communication network [3]. All of these networks utilize the WAIC radio interface. Moreover, a radio cell is defined as the coverage area of a gateway node and depending on the compartment size, multiple radio cells could be required to provide sufficient coverage [3]. This is essential to the reliability of data sent from a medium or large compartment. The compartment size also impacts the type of topology. As an example, a star topology is suitable for small compartments, whereas large one will consider multi-hop topology due to radio propagation obstacles [3].

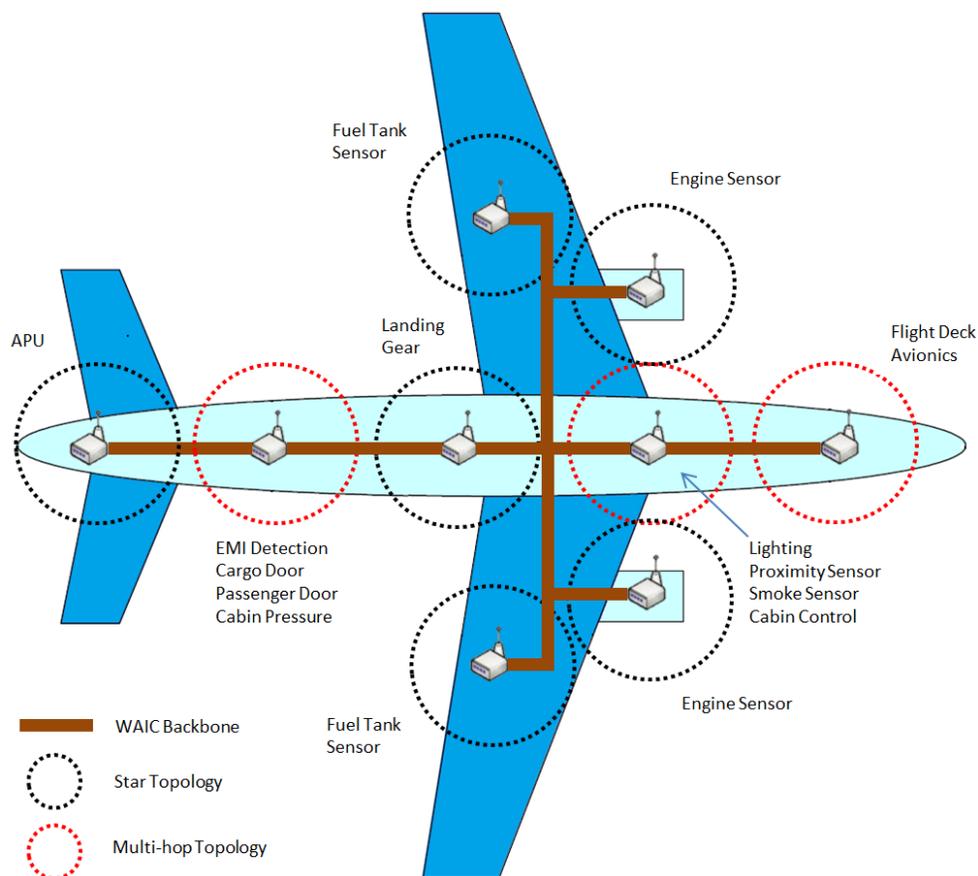


Figure 3-2: Aircraft Wireless Network Topology

Figure 3-2 illustrates the network topologies of different LRUs, sensors, and actuators and their connection to the WAIC backbone. This backbone represents the wireless link that can only be utilized by WAIC applications. The figure aims to provide an idea of the many activities that take place during a flight operation and the importance of coexistence between all systems due to the shared WAIC radio interface. The round circular is an example of the estimated radio coverage of the centered gateway node. Furthermore, when there is a high node density, then multi-hop topology is assumed in order for the radio coverage to reach its destination [3]. As an example, relay nodes connect different wireless sub-networks to overcome radio propagation obstacles [3].

3.4 Wireless Network Protocols

3.4.1 Introduction

Wireless network protocols define the means of communication between wireless avionics. The term protocol refers to the rules that govern what each device is allowed to do and how it should operate [43]. As of today, there is no agreed communication network standard for WAIC and this objective is under discussion by the committee. However, most wireless devices are either based on IEEE 802.11 Wi-Fi standards or IEEE 802.15 IoT standards [5]. Since Wi-Fi is not designed for avionics applications primarily due to reliability [5], IEEE 802.15 is considered as a potential standard for WAIC but it requires detailed analysis as well as experiments [45]. IEEE 802.15 is a working group for wireless networks formed by the IEEE [44]. It defines different wireless personal area network standards such as IEEE 802.15.1, IEEE 802.15.4, and IEEE 802.15.4e among others. These standards are described next.

3.4.2 IEEE 802.15.1

WISA stands for Wireless Interface for Sensors and Actuators and was developed by ABB to satisfy the rigorous demands of industrial environments [46]. It uses Time-Division Multiple Access (TDMA) with Frequency Division Duplex (FDD) so that all nodes can transmit simultaneously. Moreover, pseudorandom frequency hopping is implemented to mitigate coexistence issues and improve robustness and offers a tradeoff between a short

cycle time and a high node density [47]. WISA satisfies to a certain degree the stringent requirements set by the aerospace industry. This wireless network protocol has high reliability, fast response time, serves large numbers of nodes within short distances, and guarantees transmission integrity against obstacles as well as interference [46].

3.4.3 IEEE 802.15.4

IEEE 802.15.4 is a standard for wireless personal area networks, and defines the physical (PHY) and Medium Access Control (MAC) layers of the protocol stack. It is the basis of 6LoWPAN and various higher layer protocol suites [48]. Its physical layer supports 2.4 GHz ISM band where it offers a nominal data rate of 250 Kbps based on Offset Quadrature Phase Shift Keying modulation [48]. The WirelessHART protocol was developed based on the IEEE802.15.4 standard for factory and process automation systems. WirelessHART only defines operation in the 2.4 GHz band, employing Direct Sequence Spread Spectrum (DSSS) and Offset-Quadrature Phase Shift Keying (O-QPSK) modulation which allows for a bit rate of 250 kbit/s [49]. It can offer reliable communications for industrial applications but sacrifices latency and network throughput [50].

3.4.4 IEEE 802.15.4e

IEEE 802.15.4e is the latest generation of ultra-low power and reliable networking solutions for Low-Rate Wireless Personal Area Networks (LR-WPAN) and has been designed for low-power constrained devices [51]. The standard is suitable for industrial control applications since it improves support for low latency communications [52]. LR-WPAN uses Time-Slotted Channel Hopping (TSCH) which is based on time synchronization to achieve low-power operation and channel hopping to enable high reliability [51]. Using this scheme, wireless devices are kept time-synchronized at the MAC layer by scheduling in order to achieve low-power operation. As implied by its name, TSCH also implements channel hopping to defeat noise and interference [53].

4 Flight Certification and Failure Probability

4.1 Introduction

For aeronautical systems to be allowed to fly, they have to demonstrate safety compliance via a certification process defined by authorities such as FAA for the USA and EASA for Europe [1]. The airworthiness requirements depend on safety-criticality of a system and the potential consequences of its failure [1]. The FAA accepts the DO-178C “Software Considerations in Airborne Systems and Equipment Certification” as guideline for showing compliance with the applicable airworthiness regulations for airborne software [64]. This guideline classifies aircraft failure conditions in terms of the severity of their consequences and assigns design assurance levels (DALs) to software components from level A through B, C, D, to E [17]. Table 4-1 shows the classification, failure rate, and description of each DAL [17]. For example, a DAL A classification implies that a failure condition would result in multiple fatalities and most likely in the loss of the aircraft as well [17]. On the other hand, a DAL C means that a failure condition would reduce the capability of the aircraft or the crew to manage unfavorable conditions such as increase in crew workload, decrease in their efficiency, or cause physical distress to passengers [17].

Malfunction, unintended function, and loss of function can be caused by software components due to faults in the requirements, design, or implementation [18]. Since the circumstances which cause these faults are random, the failure probability, or failure rate per hour, is the probability of encountering them and thus contribute to a system failure [18]. This is described later with equation (9) as basis to link packet reliability with flight certification.

Table 4-1: Classification and Failure Rate of DAL

<i>Levels</i>	<i>Classification</i>	<i>Failure Rate</i>	<i>Description</i>
A	Catastrophic	$10^{-9}/h$	Failure may cause a crash. Error or loss of critical function required to safely fly and land aircraft.
B	Hazardous	$10^{-7}/h$	Failure has a large negative impact on safety or performance, or reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.
C	Major	$10^{-5}/h$	Failure is significant, but has a lesser impact than a Hazardous failure.
D	Minor	$10^{-3}/h$	Failure is noticeable, but has a lesser impact than a Major failure.
E	No Effect	N/A	Failure has no impact on safety, aircraft operation, or crew workload.

Wireless systems in aircraft which make use of radio communications between its components will have to prove the same level of reliability as its wired counterpart depending on its safety-criticality [1].

4.2 System Model

In this section, we develop a system model to define a WAIC network as well as its components and analyze the different types of traffic generated within this network. Figure 4-1 shows a physical network model made up of nodes that are generating traffic to the central base station. Nodes are of different types, such as gateway, relay, and end nodes. The role of the gateway node is to establish connection to the WAIC backbone. On the other hand, the role of an end node is to provide a connection between the gateway node and a sensor, actuator, or other LRU. For the case of LRUs, the end node is part of the same unit. Those nodes are either stand-alone, gateway central base station, or part of an LRU, sensor, or actuator.

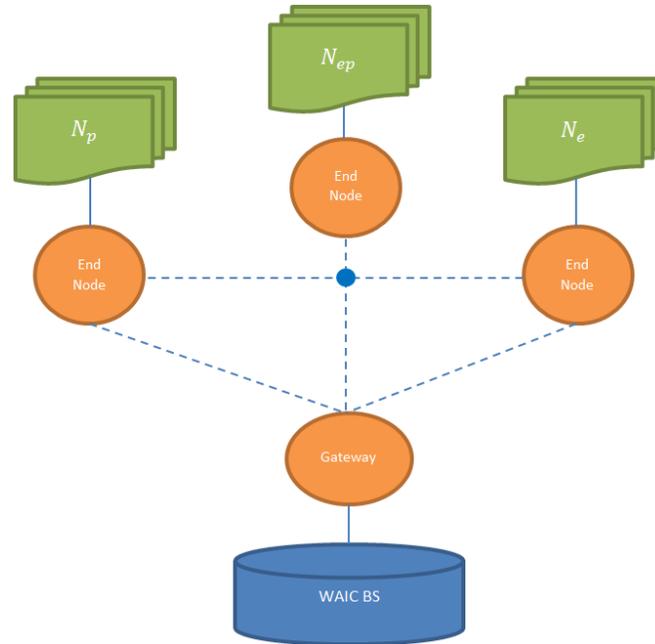


Figure 4-1: WAIC System Model

Another important note is the possibility of connecting wireless avionics to a physical avionics bus. One of the benefits of WAIC is the additional redundancy to wired connections where devices transfer packets to the gateway of an avionics bus which then allocates them to the receivers. The model in Figure 4-1 takes into account the assumption that devices communicate to the WAIC central base station. The following analysis is based on the works and investigation of [6].

Figure 4-1 shows three main types of traffic: periodic traffic N_p , event-triggered traffic N_e , and event-triggered periodic traffic N_{ep} . Each device within the network generates one type of traffic through end nodes. This traffic is based on the device's function and the compartment that it is located in as shown in Figure 3-2.

For the case of periodic traffic, T_h is defined as the interval between two consecutive transmissions. This is the most common type of avionics applications such as aircraft and engine health monitoring systems. Event-triggered traffic does not take place that often but should nevertheless still be accounted for and examples include smoke detection or lightning systems. In this model, it is assumed that an event-triggered LRU will generate event-triggered traffic according to a probability δ_e and that it is the same for all LRUs. Event-triggered periodic units are more complex since they switch between periodic traffic

after an event is triggered and no traffic at all [6]. For this case, δ_h is defined as the probability that periodic traffic is generated after an event is triggered. When this takes place, the node keeps generating periodic traffic with probability δ_q in each time interval. An example is the landing gear system. Therefore, the total number of nodes generating traffic at a given sample is described as:

$$N_{max} = N_{p,max} + N_{e,max} + N_{ep,max} \quad (1)$$

N_p is equal to the total number of nodes that are always generating periodic traffic as well as the event triggered periodic nodes that are actually generating periodic traffic due to probabilities δ_h and δ_q . Similarly, N_{ep} is the total number of nodes generating event-triggered periodic traffic minus those that switched to periodic traffic which was taken into account in the previous equation. N_e is the total number of nodes generating event-triggered traffic due to probability δ_e .

$$N_p(j) = N_{p,max} + \delta_h N_{ep}(j-1) + \delta_q \delta_h \times \sum_{k=0}^{j-1} N_{ep}(k) \delta_q^{j-k-2} \quad (2)$$

$$N_e(j) = \delta_e N_{e,max} \quad (3)$$

$$N_{ep}(j) = N_{ep,max} - \delta_h N_{ep}(j-1) - \delta_q \delta_h \times \sum_{k=0}^{j-1} N_{ep}(k) \delta_q^{j-k-2} \quad (4)$$

4.3 Flight Certification Reliability Model

In this section, we utilize recent mathematical model and derive the failure probability of wireless networks with respect to loss of packets from the works of [6] and [8]. This model links wireless network reliability with flight certification as per safety aviation authorities. This section goes over the flight certification reliability model as proposed in [6] and describes the main variables and formulas.

First, we define P_d^j as the deadline missing probability of the j -th sampled data which is the probability that a packet fails to reach its destination within a certain timeframe. The total number of samples in one flight is defined as $L = T_{dur}/T_h$. Here, T_{dur} is the flight duration in hours and T_h is the maximum duration of each time slot for wireless avionics to send or

receive packets. It is assumed to be equal for all LRUs. Then, the expected number of failures is derived as:

$$C_f = \sum_{j=1}^L P_d^j \quad (5)$$

Now, for the j -th sampled data, let m_j be the deterministic number of transmission attempts and $p_{i,j}$ be the packet loss probability of i -th transmission where $i \in [1, m_j]$ and $j \in [1, L]$. Therefore, after m_j tries, the deadline missing probability of the j -th sampled data is shown as:

$$P_d^j = \prod_{i=1}^{m_j} p_{i,j} \quad (6)$$

This implies that $1 - P_d^j$ is the probability that at least one packet was successfully received during m_j transmissions. Since wireless avionics generate traffic at periodic intervals T_h , the expected failure rate per hour is defined as:

$$P_f = \frac{T_h C_f}{T_{dur}} \quad (7)$$

The experiments performed in the next chapter are based on this function to analyze the failure probability of certain wireless networks with respect to loss of packets.

5 Experiments and Results

5.1 Introduction

In this chapter, we conduct experiments on wireless protocols based on both IEEE 802.11 and IEEE 802.15.4e standards to analyze their failure probability with respect to aviation safety requirements. The former consists of deriving the packet loss and failure probability through a simulation. The latter uses a physical experiment with a representation of a real LRU made up of IEEE 802.15.4e wireless boards where the radio-frequency emission, joint duty cycle, time delay, and reliability are analyzed. We utilized a recently published mathematical model [6] to evaluate both of them with respect to failure probability and flight certification.

5.2 WISA Simulation

We performed a simulation in MATLAB based on the WISA standard. We analyzed the failure probability of this standard while varying the probability of the packet loss with respect to DO-178C. Moreover, we validated the flight certification reliability model which was previously discussed.

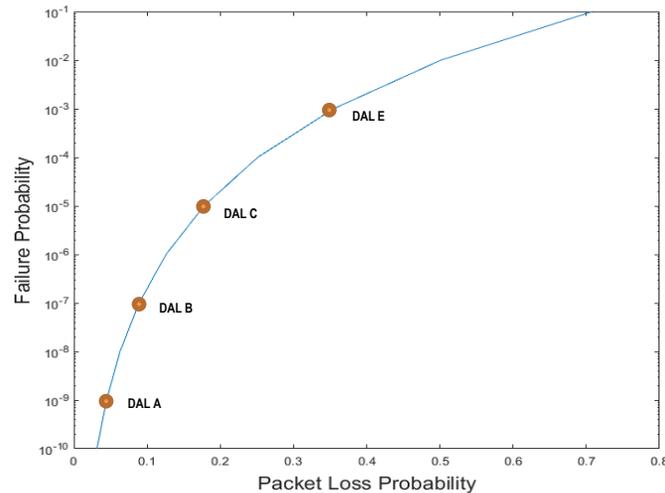
The failure probability equation was derived to be $P_f = p^{\frac{T_h}{T_{cyc}}}$ where $T_{cyc} = \frac{N_{max}T_s}{C_h}$ [6]. T_{cyc} is the length of the complete frame which includes the beacon and the different time slots. Each time slot has a size of T_s . C_h is set to 4 since the WISA protocol operates using 5 frequencies where 4 are used for uplink and 1 for downlink [6].

Table 5-1: WISA Probability Failure Equation Variables

<i>Parameter</i>	<i>Description</i>	<i>Value</i>
P_f	Failure Probability	$10^{-10}, \dots, 10^{-1}$
p	Packet Loss Probability	0, ..., 0.9
T_h	Application deadline timeframe (ms)	200
N_{max}	Total number of nodes	120
T_s	Slot size	1
C_h	Total Number of uplink frequencies	4

Table 5-1 lists each parameter used in the simulation and includes their description as well as and their values.

In this experiment, it is assumed that a total number of 120 nodes are present in the avionics compartment of an aircraft. This assumption is based on the node density estimation of the ITU report [2]. Figure 5-1 describes the failure probability of packet delivery before the expiration of its deadline for WISA as a function of packet loss probability p and application deadline T_h .

**Figure 5-1: Failure Probability Performance for WISA**

As expected, the graph shows that as the packet loss probability increases, so does the failure probability. An interesting observation is that for a critical system classified as 'Catastrophic', the maximum allowed packet loss probability must be equal to 0.045. On the

other hand, the packet loss probability of ‘Minor’ safety-critical systems cannot exceed 0.35. Therefore, this protocol meets the DO-178C standard if it can be demonstrated that the range of the allowed packet loss probability is between 0.045 and 0.35 for safety-critical systems.

5.3 Low-Rate Wireless Experiment

In this experiment, a low-rate wireless network was tested for several factors that impact reliability and safety requirements such as electromagnetic interference, join duty cycle, time delay, and loss of packets. Figure 5-2 shows the complete setup which comprises three main hardware components: wireless transmitter, wireless receiver, and a microcontroller board. The microcontroller board is an Arduino Due product and acts as an LRU. Furthermore, both wireless transmitter and receiver boards belong to the SmartMesh IP family product by Analog Devices and their network protocol is based on the IEEE 802.15.4e standard with TSCH medium access. They act as transmitter and receiver nodes connected to an LRU. The distance between both nodes was set to approximately 0.5 meters. It should be noted that the frequency band used by the wireless boards is 2.4 GHz and not 4.2 – 4.4 GHz. This is due to the fact that there is no commercial WAIC board at the time of this study and so they do not translate to a completely realistic WAIC scenario.

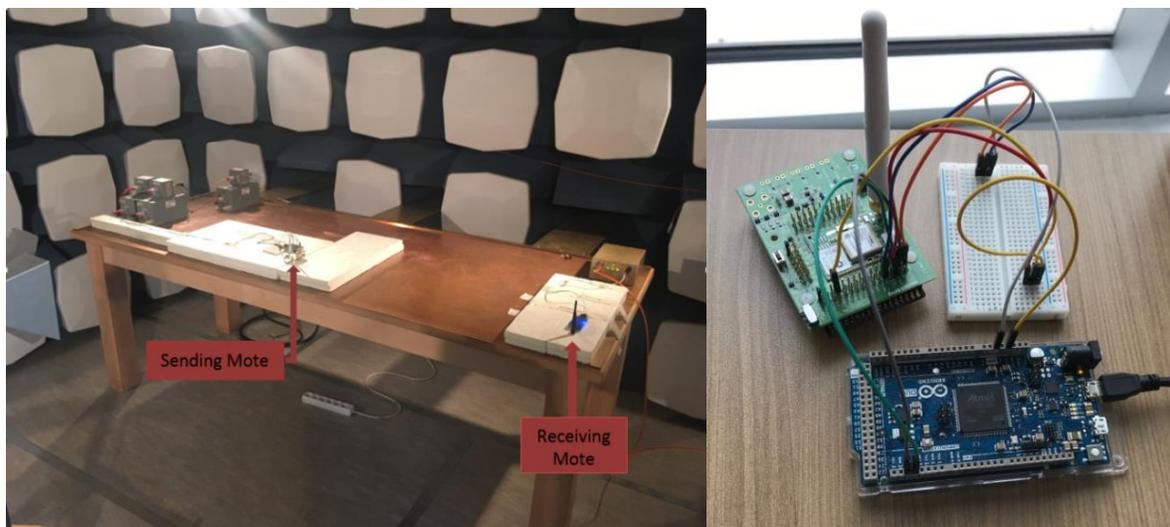


Figure 5-2: LR-WPAN Experimental setup with sending and received motes (left). Sending mote consisting of IEEE 802.15.4e TSCH based wireless board and Arduino due board (right)

This limitation needs to be taken into account as each frequency affects the propagation characteristics of wireless signals differently and interference will always be present.

The sending mote is made up of two components: LRU and End Node. The Arduino sends data packets to the end node through a serial interface. The end node then transmits the packets wirelessly to the receiving mote with the help of the SmartMesh IP board. The receiving mote is one full component that contains both the gateway node and a network manager. The network manager has a capability to analyze all received data packets. Figure 5-3 shows the complete experiment model and how the components are connected to one another.

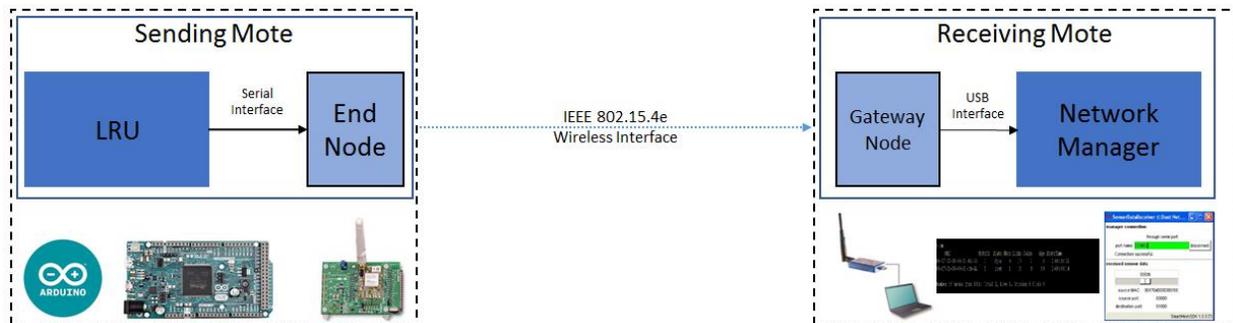


Figure 5-3: LR-WPAN LRU System Model

The sending mote transmits data packets at equal intervals and simulates a real LRU. The interval varies between 10s, 5s, 1s, and 250ms throughout the experiments. These periods provide a realistic transmission rates for avionics. The transmitted packet is made up of 31 bytes and the data load is the last 2 bytes. The load loops between 8 different hex values: 0x0000, 0x2000, 0x4000, 0x6000, 0x8000, 0xA000, 0xC000, and 0xE000. The bits do not matter more or less than the other. The purpose of this structure is to ensure that every consecutive transmission has a different data packet than the previous one in order to effectively analyze lost packets. The sending mote does not perform any other tasks. Figure 5-4 provides an example of a transmitted packet and shows the value and type of each sub-frame.

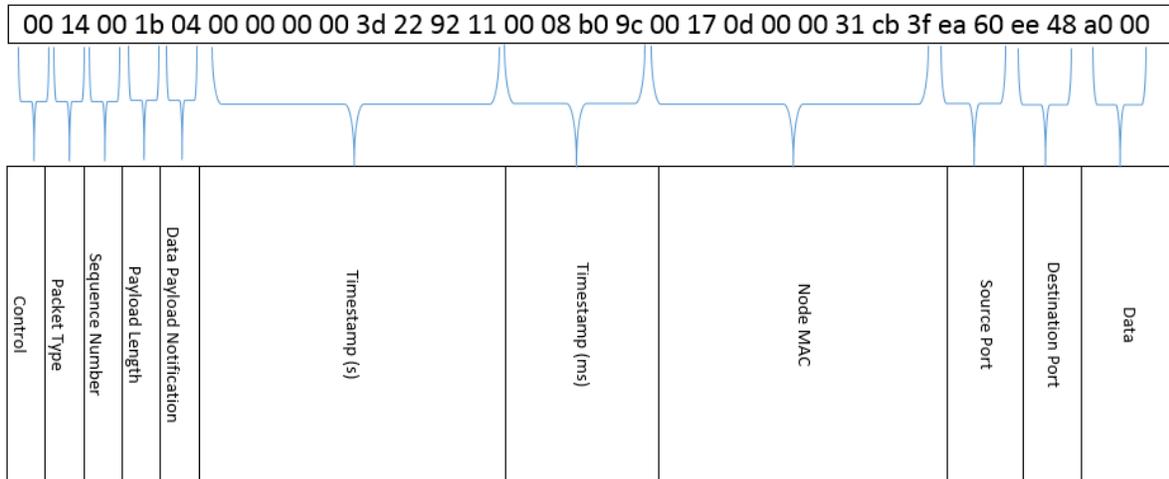


Figure 5-4: Data Packet of Transmitted Signal

5.3.1 Electromagnetic Interference

An experiment was performed to analyze the radio emission of an IEEE 802.15.4e wireless board with respect to safety regulation relating to power requirements. Authorities use the RTCA/DO-160G guideline to determine whether an electronic equipment on board an aircraft emits excessive RF signals when installed in a particular location [16]. The experiment was performed in a chamber and initially the measurements were taken with a horn-antenna in the 800 MHz to 6 GHz region with the door open as shown in Figure 5-5.

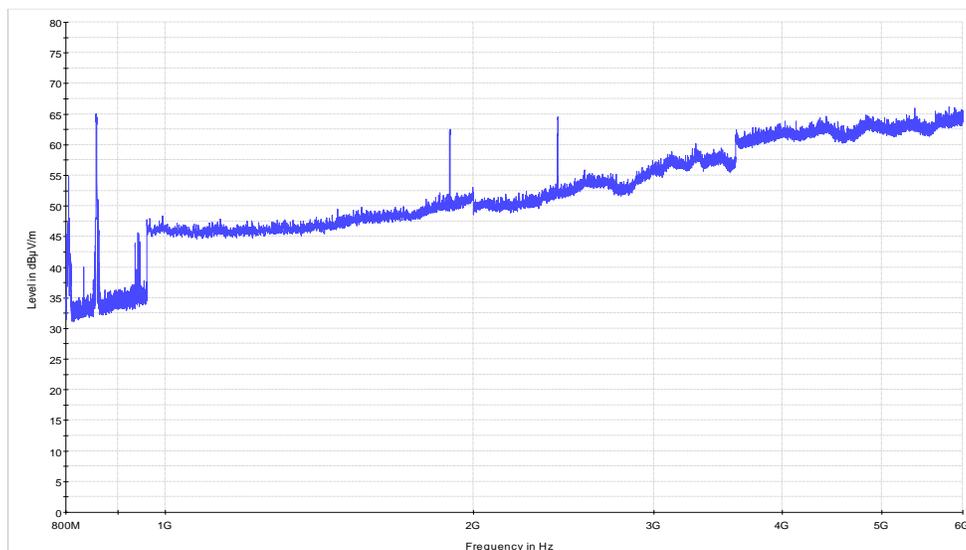


Figure 5-5: 800 MHz to 6 GHz Sweep with Door Open

The door is set to open to check random signals and the graph shows several spikes due to cellular and Wi-Fi frequencies. In order to ensure that only one frequency is present, which is sent by the wireless board, measurements were taken again but with the door closed. Figure 5-6 shows the result where only one spike is observed at approximately 2.4 GHz and proves that only the transmitting board is transmitting in the chamber. The chamber is designed for electromagnetic tests inside airplane cabin. It is semi-anechoic and includes a horn antenna which can measure between 800 MHz to 6 GHz . Moreover, it shows the maximum allowed amplitude level line with respect to each frequency as dictated by the DO-160G guideline [66].

The objective is to determine the maximum amplitude level of the radiated spurious emission and investigate whether this causes electromagnetic interference with other components onboard the same aircraft and measurement was taken at various random periods such as 3, 15, 20, and 40 minutes.

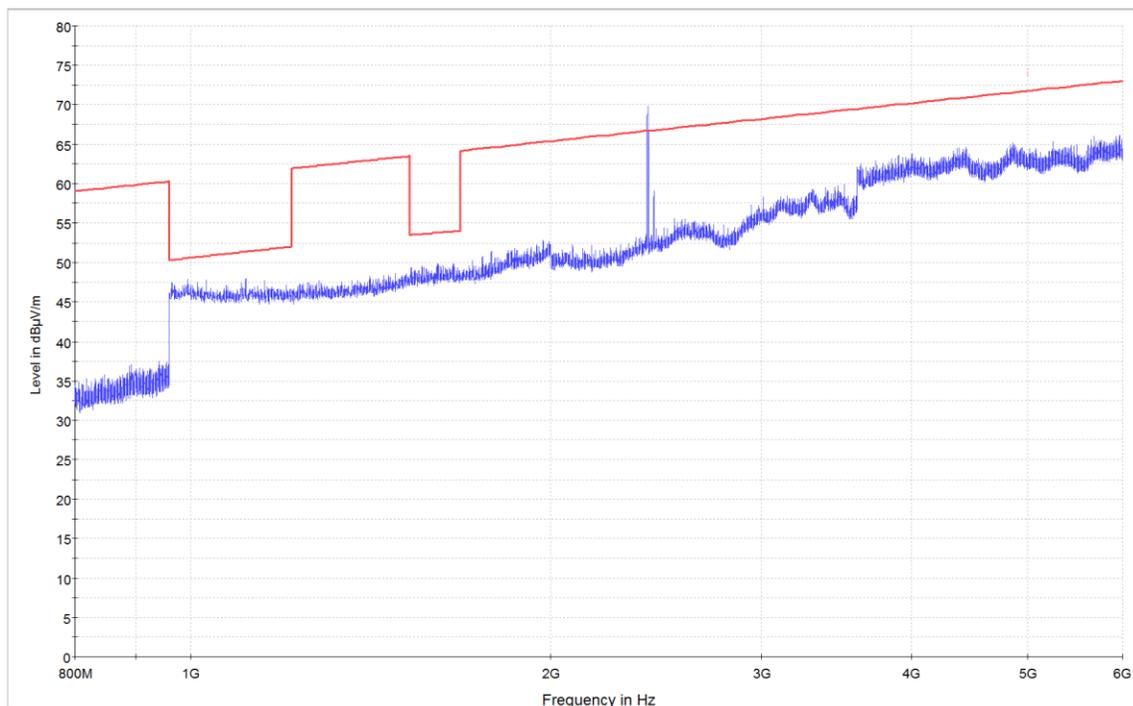


Figure 5-6: 800 MHz to 6 GHz Sweep with Door Closed and Limit Line

Aviation authorities accept the limit of 67 dBμV/m as compliant for wireless boards transmitting at the frequency of 2.4 GHz and that are located in passenger cabin and

cockpit. Although the limit for WAIC systems is yet to be defined, Figure 5-6 shows that the maximum allowed level for the frequency band between 4.2 and 4.4 GHz is equal to 72.5 dB μ V/m.

In Figure 5-7 (a) and (b), the amplitude ranges from 82 to 92.5 dB μ V/m and both exceed the limit of 72.5 dB μ V/m. Moreover, Figure 5-7 (c) and (d) show that additional sweeps of the transmitting power were obtained and it was observed that the amplitude eventually stabilized at around 97 dB μ V/m. The average of all obtained measurements is calculated to be 91.8 dB μ V/m and exceeds the safety requirement by 26%. This is not acceptable under flight certification since it implies electromagnetic interference can occur and thus impact the function and performance of electronics in the same aircraft. In this case, the protocol fails to meet the DO-160G standard.

In order to fix this issue, the source of the spurious emission needs to be investigated and that would potentially lead to a redesign of the wireless board to reduce harmonic emission and/or parasitic emission among others. It is important to note that the power requirement of IEEE 802.15.4e nodes are considered to be ultra-low power but one must also consider that their spurious radiated emission does not cause interference.

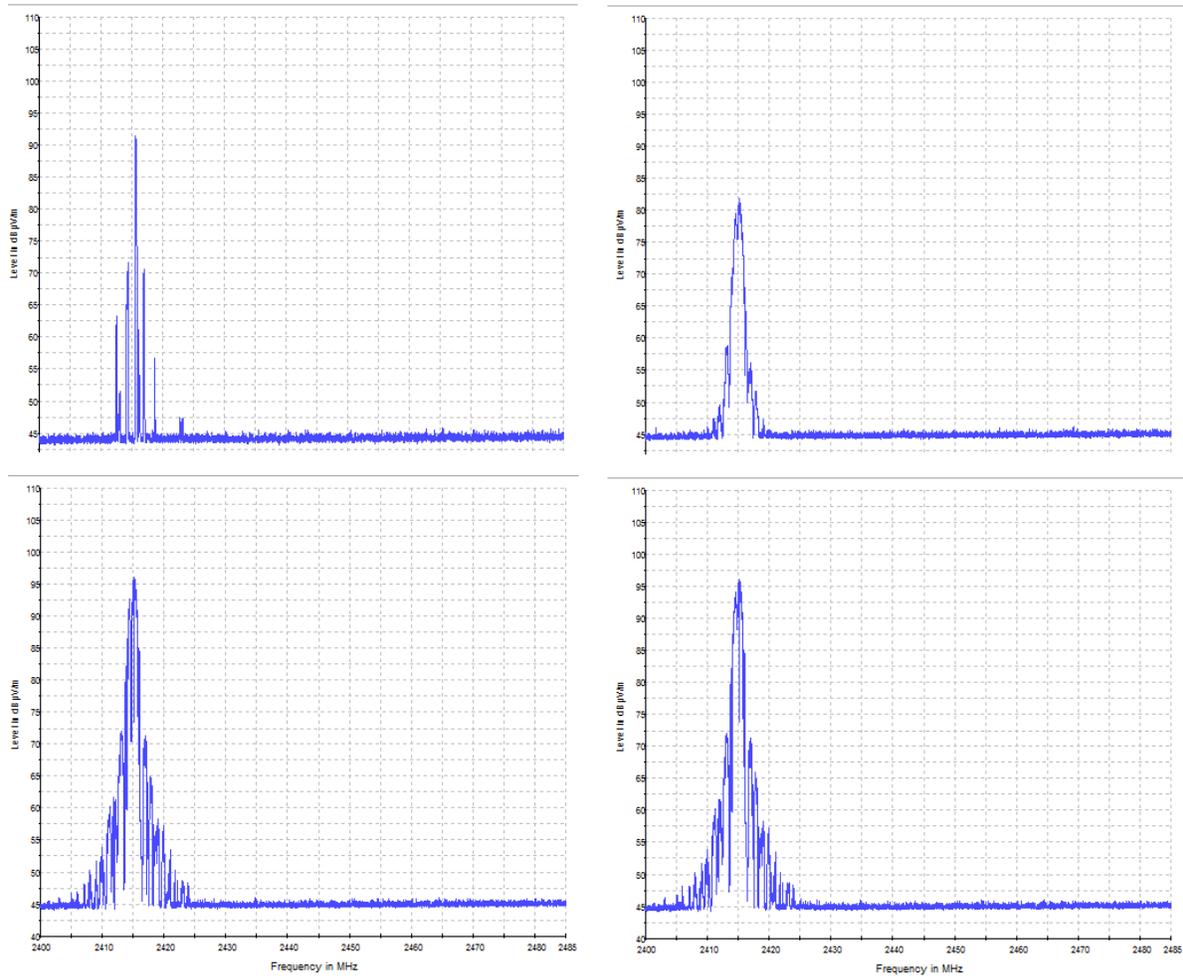


Figure 5-7: (a) Amplitude at 3 Minutes [Top Left], (b) Amplitude at 15 Minutes [Top Right], (c) Amplitude at 20 Minutes [Bottom Left], and (d) Amplitude at 40 Minutes [Bottom Right]

5.3.2 Join Duty Cycle

The join duty cycle is one of the most important aspects of a node join behavior since it estimates how much time it spends listening for a network versus sleeping. For wireless avionics, it is a tradeoff between energy and reliability. Therefore, it is critical to analyze the rate at which a node changes states from sleeping to ready. Moreover, it is equally critical to know the time a node needs in case it goes through a reboot because of a malfunction. This causes loss of packets during that period and thus increases the failure probability. Join duty cycle is a concern for wireless avionics which was not present before in a wired system. In order to analyze this case more thoroughly, we conducted an experiment to study the join duty cycle of the wireless boards. This is performed by setting

the join duty cycle at 5%, 25%, 50% and 100% while measuring the time it takes for a node to reboot and join a network [65]. In this experiment, we assume the reboot process to be indicative of a node switching from sleeping mode to listening mode. A low join duty cycle will result in a longer search times but at lower average current. On the other hand, higher values will shorten the time to reboot but increase average current since a node spends more time listening for a network than sleeping.

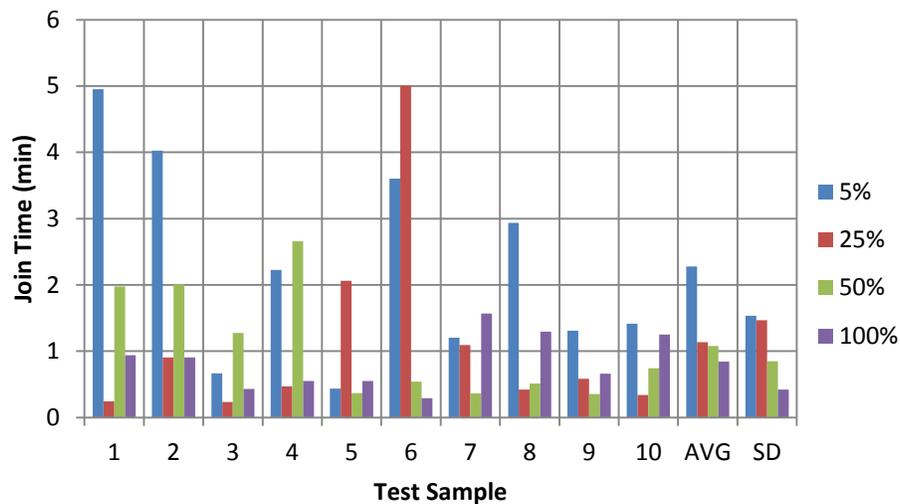


Figure 5-8: Join Duty Cycle Results

Figure 5-8 lists all join duty cycle levels as well as the average of them. The join duty cycle at 5% results the longest duration of around 2.3 minutes but is expected to save the most power at the end [65]. It is clear that with 100% join duty cycle, the time it reconnects to the network is lowest with an average of 50.7 seconds but using the most current to stay in listening mode. At 25% and 50%, the average join time was found out to be 1.13 and 1.08 minutes, respectively. Therefore, increasing the average current does shorten the join time with the minimum time being around one minute for those specific wireless boards. However, the experiments showed that there are high variations between test samples which can only be explained by either the test setup or the actual boards. In order to investigate further, more test samples are required. In this case, this result is not tolerable for wireless avionics as each function must be consistent with respect to its requirements

at all times during the flight. Furthermore, the shortest delay is still excessive for the case of wireless avionics since a lot of packets are lost in a span of 60 seconds.

5.3.3 Time Delay

Another consideration for wireless avionics is the time delay of a signal from the transmission source to the receiver. If a packet is not received before the deadline timeframe, then it will be ignored by the receiving node and thus constitutes as a lost packet. This section studies the time delay of the wireless boards while varying the sending frequency. There are many factors that influence time delay and they include number of nodes in the network, the network latency, the number of transmission errors, and so forth. It is assumed that these measurements are representative of a practical system since there is no interference. Figure 5-9 shows the four experiments where each had a data period of 10, 5, 1, and 0.25 seconds, respectively. The total amount of data packets sent for each experiment is equal to 357 and all packets are equal in size.

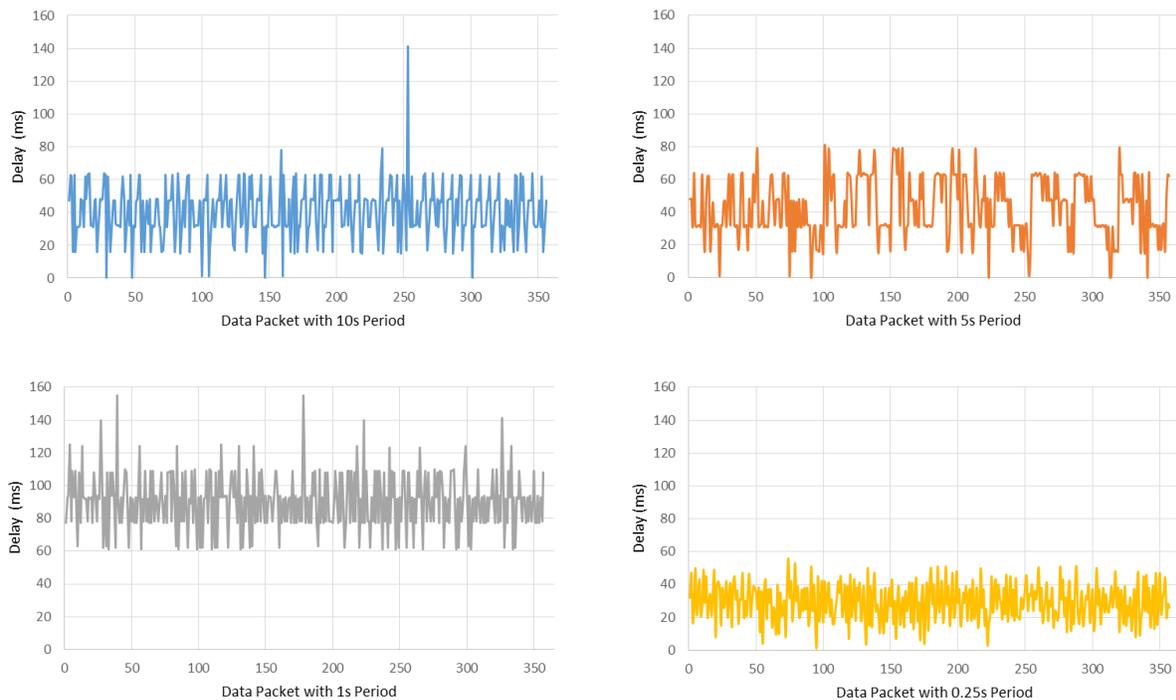


Figure 5-9: Time Delay for Data Packets with (a) 10s Period, (b) 5s Period, (c) 1s Period, and (d) 250ms Period

During the four experiments, all packets were received with the correct data load values. As such, there was no loss of packets for any data period. According to the experiments, data

packets with period 1 second had the longest time day with an average of 90.3ms while the data packets graph with period 0.25ms had the shortest average time delay of 29.3ms. The time delay of graphs (a) and (b) with periods equal to 10 and 5 seconds averaged at 40.5ms as well as 42.7ms, respectively. This shows that there is high variation in the time delay with respect to the data period. One question that arises is whether or not these results comply with flight certification. As an example, the shortest average time delay (250ms) constitutes 11.7% of its data period which is actually the highest rate. On the other hand, graph (a) has the lowest rate equal to 0.4% primarily due to its extremely long 10 seconds data period. This is an important observation since it can be argued that depending on the criticality of the system and the data period, a prolonged time delay can be tolerated.

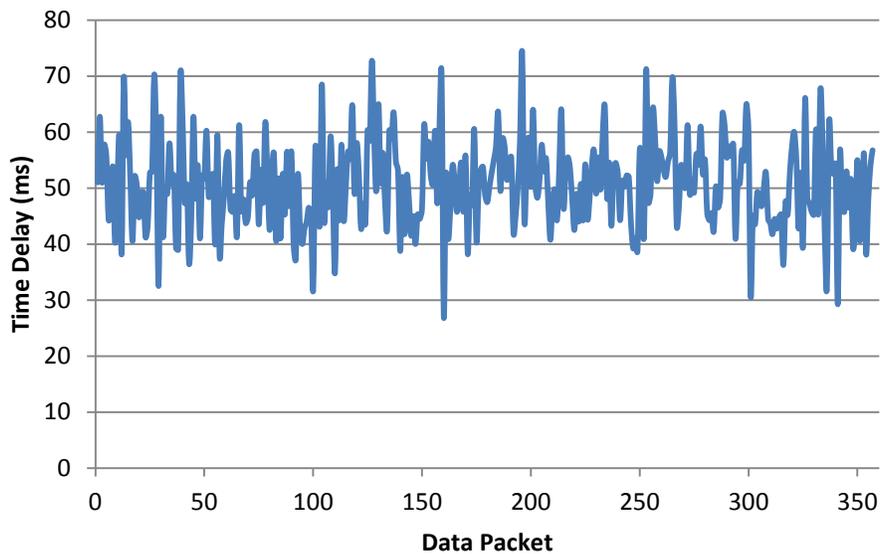


Figure 5-10: Average Time Delay Plot

Figure 5-10 plots the average time delay of each packet for all the data periods. The range of the delay varied between 27 and 74.25ms and the overall average was calculated to be 50.7ms. Considering the data period of 250ms, the average time delay constitutes about 20% which is now twice as large as the previous result. This leads to the previous question again regarding flight certification requirement. Although the time delay requirement is not yet defined for wireless avionics, it will be based on current wired configuration and the time delay of an electric signal moving through a typical aircraft cable as a reference.

5.3.4 Reliability

The purpose of this experiment is to analyze the reliability of the IEEE 802.15.4e based on TSCH wireless boards. This is performed by evaluating their failure probability with respect to loss of packets. It involved a transmitter to send roughly 10^5 packets to a network manager with a data period of 250ms. The term lost packets also includes received packets but with the wrong data loads. These lost packets were highlighted and examined afterwards. The time delay of each received packet was also taken into account. The idea behind this experiment is to simulate wireless transmission between two LRUs during a 7 hour flight.

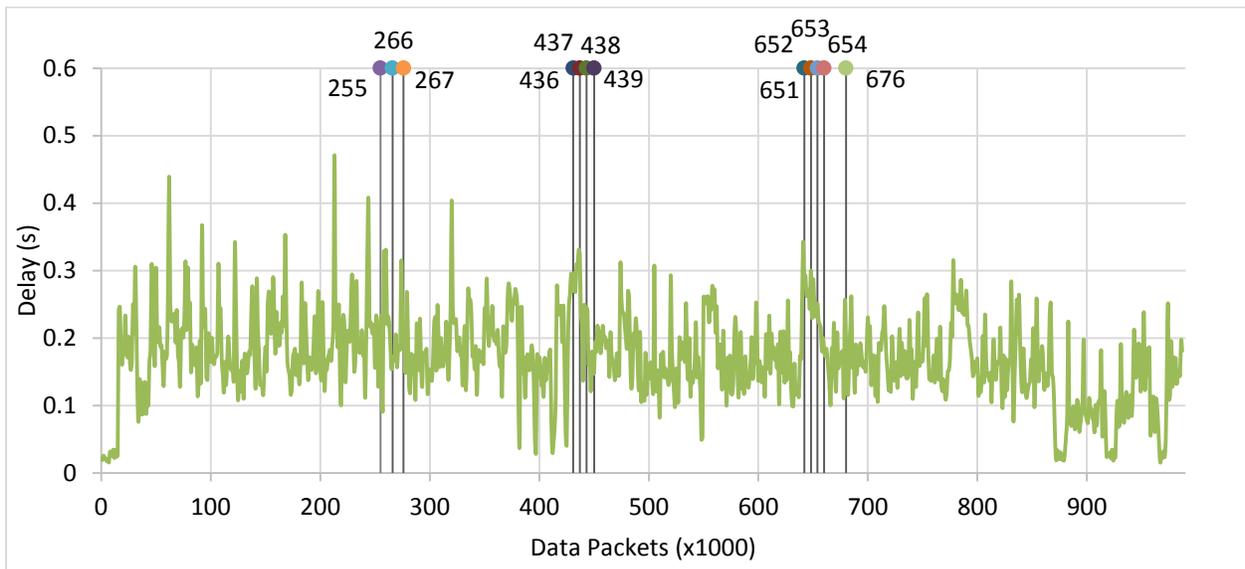


Figure 5-11: Lost Packets with 250ms Data Period

Figure 5-11 shows that 12 packets were lost in total during this experiment. However, a time window of 60 seconds was allocated for a node to become active again based on the result of the join duty cycle experiment in Section 5.3.2. Therefore, any packet that is lost during the 60 seconds period after the initial failure is not taken into account. As a result, the 12 errors were grouped into 3 packets lost. Thus, by using equation (7), the failure probability is calculated as:

$$P_f = \frac{T_h C_f}{T_{dur}} = \frac{(0.25)(3)}{24,661.5} \approx 3 \times 10^{-5}$$

According to Table 4-1, the DO-178C would classify this failure rate as “Major” with Level C. Therefore, this protocol meets the DO-178C reliability standard under the circumstance that only two nodes, located 0.5 m apart, are communicating with a frequency of 2.4 GHz in a closed chamber.

An additional criterion to consider is the average delay which was calculated to be 171.8ms and is more than the triple of the total average time delay result found in Figure 5-10. This implies that the amount of data transmission and the duration of the test can have an impact on the time delay since the former experiment used only fraction of the data compared to this experiment. Another observation is that at the very beginning of the experiment, the time delay is less than 40ms which is in-line with the previous experiments. Since the average delay is roughly 68.7% of the data period, this would likely be deemed as highly intolerable with respect to flight certification. So, although this experiment claims that the current system complies with a failure rate of 10^{-5} /hr, other factors such as data rate, time delay, and amount of data being transmitted have to be taken into account to analyze whether or not the system complies with respect to its time delay.

6 Conclusion and Future Work

6.1 Conclusion

Our work studied the technical characteristics, challenges, and network protocols of wireless avionics. We analyzed the latest requirements of the WAIC standard and their impact on certification regulations. Moreover, we performed simulation and physical experiments on potential wireless protocol candidates such as IEEE 802.11 and IEEE 802.15e for wireless avionics. In those experiments, we primarily analyzed electromagnetic interference, reliability, and time delay. Regarding reliability, we utilized a mathematical model to link failure probability with flight certification and the used metric was based on the DO-178C safety guideline.

Our results indicated that the allowed packet loss probability for IEEE 802.11 is between 0.045 and 0.35 for safety-critical systems to meet the DO-178C reliability standard. This was based on a simulation with a total number of nodes equal to 120. The wireless boards based on IEEE 802.15.4e with TSCH did meet the DO-178C reliability standard with a classification of 'Major' since it reached a failure probability of 10^{-5} per hour. However, it failed the DO-160G standard because of electromagnetic interference. This was due to radiated spurious emissions where the amplitude of the received signals averaged at 97 dB μ V/m which exceeded the limit by 26%. The time delay of around 350 transmitted and received packets averaged at 50.7 ms. However, when simulating a 7 hour flight, the time delay results were problematic and thus deemed invalid. The join duty cycle experiment was performed in order to estimate the time it takes for a node to cycle through a reboot and the result of approximately 60 seconds was used in the calculation of the failure

probability. In this case, it was a physical experiment with only two nodes separated by 0.5 m and using the frequency 2.4 GHz.

Wireless avionics needs to provide wired-equivalent reliability depending on the classification of the safety-critical system. The current wireless industry standards are not qualified to achieve the failure rate requirement to meet certification regulations. Furthermore, special attention is required during the design of WAIC boards in regards to power so that no spurious emissions lead to electromagnetic interference. The same applies to join duty cycle and time delay where it is necessary to reduce both factors as they impact the failure probability and thus the overall reliability of the system.

6.2 Future Work

The design of network protocols for WAIC with focus on reliability instead of capacity is vital for the success of wireless avionics. It is the fundamental component that achieves communication between avionics without the need for wires. Therefore, future work should be focused primarily on that topic. This is also in-line with aviation regulation since reliability is one of the main factors that define safety. The proposed flight certification reliability model is an important initiative in linking wireless reliability with flight certification but there is room for improvement. In order to obtain a more realistic model, it has to include the time delay parameter between the sender and receiver and show how this impacts the failure probability of a system. The network protocol design should also take into account the topology depending on the size and location of each compartment. Several networks include star, mesh, and tree with the insertion of multi-hop capability. Another crucial factor that deals with safety is security measures to protect against inadvertent or malicious attacks via authentication, data encryption, and integration.

There are many activities ongoing regarding the development of new safety guidelines that deal primarily with coexistence of radio altimeter and security measures. However, future certification work should also include a specific guideline on how to show safety compliance of wireless avionics in regards to reliability and failure probability.

7 Bibliography

- [1] Aerospace Vehicle Systems Institute: Wireless Avionics Intra-Communications. Retrieved from <http://waic.avsi.aero/> on January 13th, 2020.
- [2] International Telecommunication Union-Recommendation: Final Acts WRC-15. Retrieved from <http://www.itu.int/pub/R-ACT-WRC.12-2015> on January 13th, 2020.
- [3] Technical characteristics and operational objectives for Wireless avionics intra-communications (WAIC), International Telecommunication Union (ITU-R) 2010: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2197-2010/PDF-E.pdf.
- [4] M. Heinen, "The A380 program," Global Investor Forum, 2006. Retrieved on January 13th from <https://wettengl.info/Blog/Dokumente/D126-Airbus-Global-Investor-Forum-2006-A380-Financials.pdf>
- [5] Gao, Shang & Dai, Xuewu & Hang, Yu & Guo, Yuyan & Ji, Qian. (2018). Airborne Wireless Sensor Networks for Airplane Monitoring System. *Wireless Communications and Mobile Computing*. 2018. 10.1155/2018/6025825.
- [6] Pangun Park and Woohyuk Chang, "Performance Comparison of Industrial Wireless Networks for Wireless Avionics Intra-Communications", *IEEE Communications Letters* (Volume: 21, Issue: 1, Jan. 2017), pp. 116-119.
- [7] D. Graham-Rowe, "Fly-by-wireless set for take-off," *New Scientist*, vol. 203, no. 2724, pp. 20-21, 2009.
- [8] F. Bai and H. Krishnan, "Reliability analysis of DSRC wireless communication for vehicle safety applications," in *Proc. IEEE International Transportation Systems Society*, Oct. 2006, pp. 355-362.
- [9] O. Elgezabal. "Fly-by-Wireless (FBWSS): Benefits, risks and technical challenges.," *CANEUS Fly-by-Wireless Workshop*, August 2010, USA.
- [10] R. N. Akram et al., "Challenges of security and trust in Avionics Wireless Networks," 2015 *IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, Prague, 2015, pp. 4B1-1-4B1-12
- [11] Reji, Peter & Natarajan, K. & Shobha, K.. (2019). Performance Evaluation of Wireless Protocols for Avionics Wireless Network. *Journal of Aerospace Information Systems*. 17. 1-11. 10.2514/1.1010752.
- [12] K. Kiefer, "Real-world experience in wireless instrumentation and control systems," in *Proceedings of the CANEUS "Fly-by-Wireless" Workshop*, 2007.
- [13] L. Hanschke, L. Krüger, T. Meyerhoff, C. Renner and A. Timm-Giel, "Radio altimeter interference mitigation in wireless avionics intra-communication networks," 2017 15th *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Paris, 2017, pp. 1-8.
- [14] Consideration of the Aeronautical Mobile (route), Aeronautical Mobile, and Aeronautical Radio Navigation Services Allocations to Accommodate Wireless Avionics Intra-Communication, International Telecommunication Union (ITU-R) 2014: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2318-2014-PDF-E.pdf

- [15] Omar Torres, Truong Nguyen, and Anne Mackenzie: "Enabling Wireless Avionics Intra-Communications," NASA/TM-2016-219364. Langley Research Center, Hampton, Virginia (December 2016).
- [16] Dinh-Khanh Dang, A. Mifdaoui and T. Gayraud, "Fly-By-Wireless for next generation aircraft: Challenges and potential solutions," 2012 IFIP Wireless Days, Dublin, 2012, pp. 1-8.
- [17] RTCA/DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," January 5, 2012.
- [18] John Rushby, "New Challenges in Certification For Aircraft Software", Computer Science Laboratory - SRI International. Retrieved from <http://www.csl.sri.com/users/rushby/slides/emsoft11.pdf> on April 5, 2018.
- [19] Michael R. Franceschini, (May 2015) "Wireless Avionics Intra-Communications (WAIC): Overview and Application." Future of Instrumentation & Internet Workshop. Retrieved from https://www.icao.int/MID/Documents/2014/AFSWS%20and%20FSMP32/FSMP-WGF32-21-SpectrumWorkshop_AI%201-17%20WAIC-briefing%20Cairo%202015.pdf on January 18th, 2020.
- [20] R. Samano-Robles, E. Tovar, J. Cintra, and A. Rocha: "Wireless Avionics Intra-Communications: Current Trends and Design Issues," The Eleventh International Conference on Digital Information Management (ICDIM 2016).
- [21] RTCA/DO-356, "Airworthiness and Security Methods and Considerations," September 23, 2014.
- [22] Yedavalli, Rama K. and Belapurkar, Rohit K. "Application of wireless sensor networks to aircraft control and health management systems", Journal of Control Theory and Applications", 2011.
- [23] A. Arce, A. J. Del Real, C. Bordons, and D. R. Ramirez, "Realtime implementation of a constrained MPC for efficient airflow control in a PEM fuel cell," IEEE Transactions on Industrial Electronics, vol. 57, no. 6, pp. 1892–1905, 2010.
- [24] R. N. Akram, K. Markantonakis, K. Mayes, P. Bonnefoi, D. Sauveron and S. Chaumette, "Security and performance comparison of different secure channel protocols for Avionics Wireless Networks," 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, 2016, pp. 1-8.
- [25] "Wireless Interconnectivity and Control of Active Systems (WICAS) Active Aircraft". Retrieved from <https://www.qub.ac.uk/research-centres/EPIC/Research/IntelligentSystems/WirelessInterconnectivityandControlofActiveSystemsWICASActiveAircraft/> on January 19th, 2020
- [26] "FLite Instrumentation TEst Wireless Sensor". Retrieved from <https://cordis.europa.eu/project/id/338527/de> on January 19th, 2020.
- [27] "SAHARA: Cordless Sensors Network for Aerospace platforms". Retrieved from <http://www.globalsys.fr/sahara/> on January 19th, 2020.
- [28] S. Musteric and A. Berdugo, "The advanced subminiature telemetry system (ASMT): a wireless, network based, miniaturized instrumentation system," AIAA Journal, vol. 5, no. 32, pp.123–135, 2013.
- [29] M. Pimprikar and I. Valenta, Fly-by-Wireless for Aerospace Vehicles, A Report of the CANEUS Fly-by-Wireless 2009 Workshop, CANEUS, Montreal, Canada, 2009.
- [30] I. Bang, H. Nam, W. Chang, T. Kim, J. Woo, C. Kim, T. Ban, P. Park, B. Jung, "Channel Measurement and Feasibility Test for Wireless Avionics Intra-Communications". Sensors (2019).
- [31] T. Sekiguchi, T. Hikage, S. Futatsumori, A. Kohmura, N. Yonemoto. A large scale FDTD analysis of propagation characteristics for wireless link design of 4.4 GHz-band WAIC installed on passenger aircraft. In Proceedings of the IEEE USNC-URSI Radio Science Meeting (Joint with AP-S Symposium), Boston, MA, USA, 8–13 July 2018; pp. 153–154.
- [32] Baltaci, A., Zoppi, S., Kellerer, W., & Schupke, D. (2019). Evaluation of Cellular IoT for Energy-constrained WAIC Applications. 2019 IEEE 2nd 5G World Forum (5GWF), 359-364.

- [33] J. Friedt, G. Goavec-Merou, G. Martin, W. Feng and M. Sato, "Passive RADAR acoustic delay line sensor measurement: demonstration using a WiFi (2.4 GHz) emitter and WAIC-band (4.3 GHz)," 2018 6th IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Huntsville, AL, USA, 2018, pp. 54-61.
- [34] S. Mersch, T. Meyerhoff, L. Krüger and A. Timm-Giel, "Coexistence of Wireless Avionics Intra-Communication Networks," 2018 6th IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Huntsville, AL, USA, 2018, pp. 18-23.
- [35] Olulana, F. (2018). Coexistence of Wireless Avionics Intra-Communications Networks Based on Frequency Hopping with Collision Avoidance. 2018 IEEE 38th International Conference on Electronics and Nanotechnology (ELNANO), 483-488.
- [36] R. Sámano-Robles, "MAC-PRY Cross-Layer Design for Secure Wireless Avionics Intra-Communications," 2019 Eighth International Conference on Emerging Security Technologies (EST), Colchester, United Kingdom, 2019, pp. 1-7.
- [37] Samano Robles, Ramiro & Neves, J.. (2018). Secure wireless avionics intra-communications: The SCOTT approach. *Ada User Journal*. 39. 267-276.
- [38] D. C. Malocha and S. Malocha, "SAW Sensor Development at 4.3 GHz for the Wireless Avionics Intra-Communications Band," 2019 IEEE International Ultrasonics Symposium (IUS), Glasgow, United Kingdom, 2019, pp. 619-622.
- [39] T. Meyerhoff, H. Faerber and U. Schwark, "Interference Impact of Wireless Avionics Intra-Communication Systems onto Aeronautical Radio Altimeters," SCC 2015; 10th International ITG Conference on Systems, Communications and Coding, Hamburg, Germany, 2015, pp. 1-6.
- [40] Moir, I., Seabridge, A., & Jukes, M. (2013). *Civil avionics systems (2nd ed., Aerospace series) [2nd ed.]*. Hoboken: Wiley. (2013).
- [41] Karl H, Willig A (2007) *Protocols and architectures for wireless sensor networks*. Wiley-Interscience, New York
- [42] Emerging security threats in the aviation industry. Retrieved from https://www.icao.int/Meetings/LegalSeminar/Documents/JN_General_overview_-_Emerging_security_threats_in_the_aviation_industry-1.pdf on February 16th, 2020.
- [43] Sharing a Common Medium: Media Access Protocols. MIT Lecture Fall 2010. Retrieved from <http://web.mit.edu/6.02/www/f2010/handouts/lectures/L10-11.pdf> on February 16th, 2020.
- [44] IEEE 802.15 Working Group for Wireless Specialty Networks (WSN): Retrieved from <http://www.ieee802.org/15/> on August 28th. 2019).
- [45] Technical characteristics and spectrum requirements of Wireless avionics intra-communications systems to support their safe operation, International Telecommunication Union (ITU-R) 2010: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2283-2013-PDF-E.pdf
- [46] Richard Steigmann and Jan Endresen, "Introduction to WISA – Wireless Interface for Sensors and Actuators," White Paper, V2.0 (July 2006).
- [47] R. Budampati and S. Kolavennu. "Industrial Wireless Sensor Networks: Monitoring, Control and Automation." Woodhead Publishing (19th October 2015).
- [48] F. Xenophon et al. (2016). BLE or IEEE 802.15.4: Which Home IoT Communication Solution is more Energy-Efficient?. *EAI Endorsed Transactions on Internet of Things*. 2. 10.4108/eai.1-12-2016.151713.
- [49] Petersen, Stig & Carlsen, Simon. (2009). Performance evaluation of WirelessHART for factory automation. 1 - 9. 10.1109/ETFA.2009.5346996.

- [50] Bin Xie (May 14, 2018). L2Wireless: Enabling Low-Latency High-Reliability Wireless for Industry Communication Systems. Retrieved from <http://cqr.committees.comsoc.org/files/2018/05/06-Roundtable-Bin-Xie-v2.pdf> on September 2nd, 2019.
- [51] RFC 7554 – Using IEEE 802.15.4e Time-Slotted Channel Hopping in the Internet of Things (IoT) Problem Statement: <https://tools.ietf.org/html/rfc7554>
- [52] Kurunathan, Harrison & Severino, Ricardo & Koubaa, Anis & Tovar, Eduardo. (2018). IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2800898.
- [53] A. Mavromatis et al.:Impact of Guard Time Length on IEEE 802.15.4e TSCH Energy Consumption. Retrieved from <http://georgiospapadopoulos.com/docs/poster/ieeesecon2016-poster.pdf> on September 2nd, 2019.
- [54] IATA: Annual Review 2018. Retrieved from <https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2018.pdf> on February 22nd, 2020.
- [55] Aerospace America: War on Wiring (May 2017): Retrieved from <https://aerospaceamerica.aiaa.org/features/war-on-wiring/> on February 22nd, 2020.
- [56] SC-236, Standards for Wireless Avionics Intra-Communication System (WAIC) within 4200-4400 MHz. Retrieved from <https://www.rtca.org/content/sc-236> on February 21st, 2020.
- [57] EUROCAE: Working Group 96 – Wireless On-Board Avionics Networks. Retrieved from <https://www.eurocae.net/about-us/working-groups/>.
- [58] Bennis, M., Debbah, M., & Poor, H. (2018). Ultrareliable and low-latency wireless communication: Tail, risk, and scale. Proceedings of the Ieee, 106(10), 1834-1853.
- [59] P. Park, S. Coleri Ergen, C. Fischione, C. Lu and K. H. Johansson, "Wireless Network Design for Control Systems: A Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 978-1013, Secondquarter 2018.
- [61] K. Elliot. Development of Wireless Avionics Intra-Communications Retrieved from <http://interactive.aviationtoday.com/development-of-wireless-avionics-intra-communications/> on March 27th, 2020
- [62] N. Raharya and M. Suryanegara, "Compatibility analysis of Wireless Avionics Intra Communications (WAIC) to radio altimeter at 4200 – 4400 MHz," 2014 IEEE Asia Pacific Conference on Wireless and Mobile, Bali, 2014, pp. 17-22.
- [63] J. Engelbrecht, T. Fuss, U. Schwark and O. Michler, "Measurement of Interference Path Loss between Wireless Avionics Intra-Communications system and aircraft systems at 4.2-4.4 GHz band," 2014 Loughborough Antennas and Propagation Conference (LAPC), Loughborough, 2014, pp. 119-123.
- [64] AC 20-115D - Airborne Software Development Assurance Using EUROCAE ED-12() and RTCA DO-178() Document Information. Retrieved from https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1032046 on March 30th, 2020.
- [65] SmartMesh IP Application Notes. Retrieved from https://www.analog.com/media/en/technical-documentation/application-notes/SmartMesh_IP_Application_Notes.pdf on April 14th, 2020.
- [66] RTCA/DO-160G, "Environmental Conditions and Test Procedures for Airborne Equipment," December 2010.
- [67] Rosa Arnaldo Valdés, Víctor Fernando Gómez Comendador, Alvaro Rodriguez Sanz and Javier Perez Castán (March 9th 2018). Aviation 4.0: More Safety through Automation and Digitization, Aircraft Technology, Melih Cemal Kuşhan, IntechOpen. Available from: <https://www.intechopen.com/books/aircraft-technology/aviation-4-0-more-safety-through-automation-and-digitization>