UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

Protection and Safety of Small UAS in Complex Electromagnetic Environments: Modeling and Experiments

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

Morgan Lau
Norman, Oklahoma
2025

Downloaded from SHAREOK. Persistent Handle URL: https://hdl.handle.net/11244/341334

Protection and Safety of Small UAS in Complex Electromagnetic Environments: Modeling and Experiments

A THESIS APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY THE COMMITTEE CONSISTING OF

Dr. Yan Zhang, Chair

Dr. Jessica Ruyle

Dr. Hernan Suarez

©Copyright by Morgan Lau 2025
All Rights Reserved.

This page is intentionally left blank

Acknowledgments

I would like to express my gratitude to Dr. Rockee Zhang, my advisor, for invaluable guidance and mentorship throughout this work. My sincere thanks to Dr. Hernan Suarez, who provided insight and expertise which greatly enriched this research. I am thankful to Keegan for his support and assistance with testing, and to Jake for his valuable advice. Finally, I'd like to thank my committee members for their support and encouragement.

Contents

List Of Tables viii

List Of Figures ix

Abstract xiii

1 Introduction 1
- 1.1 Challenges of safe operation and survivability of small UAS in EMOE 1
- 1.2 Existing Radiation Safety Standards 7
- 1.3 Thesis Outline 8

2 Description of General sUAS Electronics System and Operational Electromagnetic Environment 10
- 2.1 RFI/EMI Spectrum Modeling Measurements 10
  - 2.1.1 sUAS spectrum modeling 11
    - 2.1.1.1 Other Spectrum Examples 12
  - 2.1.2 RFI Spectrum Examples and Initial Modeling 12
    - 2.1.2.1 Air-surveillance Radar(ASR) 12
    - 2.1.2.2 EMI and RFI from UAS Onboard Electronics 15
    - 2.1.2.3 Computation of RFI EMF parameters 16
- 2.2 General Structure and Components of UAS 17
- 2.3 Weak Spot Detection and Sensitive Component Analysis 20

3 RF Communication Risk Model and Theory 22
- 3.1 General Approach 22
- 3.2 Generic Behavior Modeling of C2 Radios 24
  - 3.2.1 Combined Modeling of Radio System Simulation and Analytical Models 24
    - 3.2.1.1 CAT I Radio Modeling 24
    - 3.2.1.2 DSSS- CAT II 26
    - 3.2.1.3 FHSS-CAT III 32
  - 3.2.2 Simplified and Parameterized Link Behavior Model 39
    - 3.2.2.1 Simplified Behavior Model for Bit-Error-Rate (BER) 39
    - 3.2.2.2 Simplified Behavior Model of Radio Link Quality . . 40

4 EMI/RFI/HIRF Risk Mitigation **42**
4.1 Levels of Mitigation . . . 43
4.1.1 Level I: No Mitigation . . . 43
4.1.2 Level II Mitigation: RFI Filtering Mitigation and C2 Radio Enhancement. . . . 44
4.1.3 Level III: RFI/EMI filtering + Shielding . . . 47
4.1.4 Mitigation Level Selection and Considerations . . . 48

5 Measurements and Verification Techniques **50**
5.1 Basic Designs . . . 50
5.2 Setup of Test Instruments . . . 52
5.2.1 Broadband Noise (BBN) Generator . . . 52
5.2.2 Inspired Flight C2 Radios . . . 58
5.2.3 Commercial C2 Radios . . . 59
5.2.4 Receiver Parameters . . . 63
5.2.5 Identification of C2 Radio Categories . . . 67
5.2.6 EMI/Jamming Test Setup . . . 69
5.2.7 Software-Defined Radio/SDR . . . 71
5.2.8 EMF probe . . . 73
5.2.9 EMF Probe Antenna and Orientation . . . 76
5.3 Field Tests and Experiments Setup . . . 77

6 Results and Data Analysis **79**
6.1 Results of Commercial C2 Radios on UAS . . . 79
6.1.1 Jamming Test: SIR thresholds for C2 link loss . . . 79
6.1.2 Throughput Under Jamming/RFI . . . 81
6.2 Other Commercial C2 Radios: Result and Discussion . . . 82
6.2.1 FS-IA6B Telemetry . . . 82
6.2.2 Jamming Test: EM Field Strength Thresholds . . . 84
6.2.3 Modeling Results . . . 87
6.3 SDR-Based Emulation Test Results . . . 91
6.4 Field Operation Test Results: Summary . . . 94
6.4.1 Summary of Loss-Link Conditions . . . 94

7 Conclusion and Future Work **105**
7.1 Summary of Contributions . . . 105
7.2 Future Work . . . 106

References **107**

Appendix A - List Of Symbols **111**

Appendix B - List Of Acronyms and Abbreviations **112**

List Of Tables

1.1 Summary of electromagnetic radiation sources in a typical airport environment. 6
1.2 EMF safety thresholds and recommended actions. 8

3.1 Categorization of Communication Protocol and Respective Hardware Associated with Protocols 23
3.2 Variable Values for Equation 3.13 Plotted in Figure 3.8 35

5.1 Laboratory Emulation Measurement System Power Levels for Motor and Fan Impacts. 51
5.2 Output Power of NC1111b across different frequency ranges. 53
5.3 Commercial C2 Radio Pairings Present in this study. 60
5.4 FS-iA6B Receiver Specifications 64
5.5 R88 Receiver Specifications 65
5.6 JETI Duplex REX12 Receiver Specifications 66
5.7 DSSS Parameters for PLUTOSDR Emulations 73
5.8 Electric and Magnetic Field Occupational Hazard Levels Defined for the Utilized Frequency Band 74

6.1 Measured loss of link threshold conditions of the commercial radios (including the radios on UAS) based on the RFI noise EIRP and the E-field intensity. 86
6.2 Horizontal ASR Flights (Sweep between 300 ft to 100 ft in horizontal distance to the radar antenna), Day 1: Level III mitigation is applied. 95
6.3 Vertical ASR-11 Flights (Between 39.37 and 78.74 feet) Day 1: Level III mitigation. 97
6.4 ASDE, TACAN Tower, ILS Site Flight Test Records Day 1: Level III mitigation. 98
6.5 ILS, TACAN, LOC, ASDE Flight Test Record Day 2: No Mitigation (Removed shielding, filter) (Normal and hot weather, temp up to 100 F wind gust up to 10 mph) 99
6.6 ASR 11 Flight Test Day 2: no mitigation (Various Relaunch Heights) 101
6.7 ASR 11 Flight Test Day 2: Testing EMI Filters (Additional Launch Heights) 103

List Of Figures

1.1 Summary of Potential Electromagnetic threats a typical sUAS faces. . 3

2.1 Spectrum parameters of sUAS C2 link and the RFI sources. 12
2.2 ASR-11 radar system parameters. 13
2.3 Example of the evaluation radiation patterns of ASR-9/11 radars [1]. 14
2.4 ARS-11 radar spectrums.(a) FCC spectrum mask, (b) A measured spectrum from ASR-11 radar compliant with the spectrum mask, (c) A measured spectrum from ASR-11 radar that is not compliant with the spectrum mask. (d) Measured the time-frequency spectrum of ASR-11 radar using a spectrum analyzer payload on a drone. 15
2.5 A simplified diagram of general structures of small UAS. 16
2.6 General architecture element of sUAS. 18
2.7 Internal circuit and board structure of electronics of an example sUAS. 19
2.8 Typical "weak spots" of a small UAS subject to the RFI/EMI/HIRF threats. 21

3.1 BER For BPSK, Coherent FSK, and Non-coherent FSK in a Standard AWGN Channel. 25
3.2 Block diagram of the DSSS Transmitter using a Generic Modulation. 27
3.3 Block diagram of the DSSS Receiver with Generic Demodulation. . . 27
3.4 Simulation of modulation and demodulation process of a DSSS C2 link. 29
3.5 DSSS C2 Link Utilizing BPSK Modulation communication system Experimental Bit-Error-Rate vs Empirical Bit-Error-Rate. 31
3.6 Block diagram for a Frequency Hopping Spread Spectrum Transmit Chain. 33
3.7 Block diagram of the Receiver Side of Frequency Hopping Spread Spectrum Communication Protocol Utilizing FSK 33
3.8 Example of BER For FHSS BFSK communication links under the Broad-Band Noise Jamming (BBNJ) Comparing a Specific Case of Receive Power and Frequency Hops. 34
3.9 Side-by-side comparison of modulation and demodulation in an FHSS C2 link utilizing BPSK. 36
3.10 Example of BER For FHSS BFSK communication links under the Broad-Band Noise Jamming (BBNJ) for a realistic receiver. 37

4.1 Summary of RFI/EMI/HIRF mitigation and reinforcement techniques. 43

4.2 Examples of the "Level I", No RFI mitigation (default installations) (a) Commercially available IF1200A Hexcopter without RFI mitigation. (b) Commercially available IF750 Quadcopter without RFI mitigation. 44
4.3 Example of "Level II" HIRF/EMI mitigation, focusing on protecting the C2 link and RF channel. 45
4.4 Example of the minimal requirements of the identical EMI filters used in the onboard C2 radio channels, response measurements in the insertion loss and return loss format. 46
4.5 Examples of the "Level III", Aluminum tape shielding (a) Aluminum Shielding on the upper part of the IF750. (b) Aluminum shielding on the bottom side of the IF750. 47

5.1 Block Diagram of noise generation and amplification for 2.4 GHz ISM band as a part of the RFI emulation test. 52
5.2 Example images of the laboratory test setup - Noise generation as RFI source. 53
5.3 Measured EIRP in the 2.4 GHz ISM Band with various TX attenuator settings of the RFI emulation transmitter. 54
5.4 Initial verification of the behaviors of the lab-measurement system of noise transmit power measured using a portable spectrum analyzer (TinySA). 56
5.5 Initial verification of the behaviors of the lab-measurement system of transient behavior of logged telemetry data from quadcopter sUAS. . 57
5.6 Reciever's used in this studies analysis of command-and-control links (a) Fly-Sky FS-iA6B (b) Jeti Duplex REX 12 (c) Radiomaster R88. . 60
5.7 Transmitter units used, in this study, for analysis of C2 link (a) Jeti Duplex X Radio control system 2.4GHz & 900 MHz (b) Radiomaster TX16S 61
5.8 Telemetry data available on the two transmitter used to record data and verification of RSSI and Noise values (a) Telemetry data as it is presented on the FS-i6 transmitter from the FS-iA6B receiver (b) Telemetry data as it is presented on the Radiomaster TX16S using the FS-iA6B receiver. 62
5.9 Lab-measured signal spectrum examples for the two types of spread spectrum radios using SDR emulator and testbed. (a) FHSS example. (b) DSSS example. 68
5.10 The measured C2 radio spectrum under normal conditions (lab environment and no RFI) for the UAS systems, (a) IF1200A C2 link (b) IF750 C2 link. 68
5.11 Initial laboratory diagram test set up for Inspired Flight sUAS. Slight variation exist between the IF750 and IF1200A, with a particular difference being the presence of a 900 MHz telemetry radio for the IF1200A sUAS. 69
5.12 Anechoic chamber setup for RFI lab test using commercial sUAS devices. 70

5.13 Anechoic chamber setup for RFI lab test using commercial radio devices utilizing a model sUAS structure for elevation and emulating reflection and interference from the frame. 71
5.14 Example of RSSI measurements vs TX noise power levels. 72
5.15 Narda RadMan 2XT 2281/102 EMF meter. 74
5.16 Narda RadMan 2XT 2281/102 EMF meter E-Field Measurements Compared to Electric Field Calculations using Equation 2.3. 75
5.17 Field measurement geometry and link modeling parameters. 77
5.18 Field measurement sites (a) ASR-11 radar, (b) Google map site location. 78

6.1 Relationship between the measured SIR and RFI EIRP for two commercially available sUAS (IF750 and IF1200A). 80
6.2 Transmit and Receive throughput of the IF750 drone under varying RFI EIRP levels. 81
6.3 Telemetry data logged from FS-iA6B receiver using TX-16S Transmitter (a) Link Quality and SNR (b) RSSI and noise in dBm, calibrated by a factor of 135 for transmitter offset. 83
6.4 Measured E-field strength levels needed to disable the C2 links for IF750 and IF1200A UAS. 84
6.5 Measured E-field strength vs EIRP for testing with commercial radios, the thresholds of loss of radio link are marked. 85
6.6 FHSS-FSK Modeling with parameters for FS-iA6B components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (16 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 500 kbaud (using binary-GFSK, which results in a bit rate of 500 kbits/second) and a 500 kHz channel bandwidth. The gain for both curves is calculated to be between 20 to 23 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB. . . . 87
6.7 FHSS-FSK Modeling with parameters for R88 components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (20 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 250 kbaud (using binary-GFSK, which results in a bit rate of 250 kbits/second) and a 500 KHz channel bandwidth. The gain for both curves is calculated to be between 23 to 26 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB. . . . 89

6.8 FHSS-FSK Modeling with parameters for R88 components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (20 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 2 Mbps and a 48 MHz spread bandwidth. The gain for both curves is calculated to be between 15.8 to 18.8 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB. 90
6.9 C2 link statistics emulation using Pluto SDR to emulate DSSS BPSK signal with 16 bit length pseudorandom spreading code. 92
6.10 BER using Pluto SDR to emulate DSSS BPSK signal with 16 bit length pseudorandom spreading code. 93
6.11 Diagram of Horizontal ASR Flights (Sweep between 300 ft to 100 ft in horizontal distance to the radar antenna), performed on Day 1: Level III mitigation is applied. 95
6.12 Vertical ASR-11 Flights (Between 39.37 and 78.74 feet) Day 1: Level III mitigation. 96
6.13 ASR 11 Flight Test Day 2: no mitigation (Various Relaunch Heights) 100
6.14 ASR 11 Flight Test Day 2: Testing EMI Filters (Additional Launch Heights) 102

Abstract

The survivability of small Unmanned Aerial Systems (sUAS) in high-intensity radio-frequency (HIRF) environments is a significant characterization that determines the operability in critical environments. The existing sUAS system designs do not consider the complexity of adversary electromagnetic environments, such as Radio Frequency (RF) interference, electromagnetic interference (EMI), Counter-UAS (C-UAS) electromagnetic attack (EA), and other potential sources of noises in the radio frequency spectrum. This study aims to identify practical approaches for improving the resilience of existing small UAS against HIRF. These improvements are to be evaluated through both controlled laboratory experiments and in situ flight testing. The initial investigation of this study focuses on identifying the weak spots of the existing flight vehicles, from the propeller, motors, and controllers, as well as the internal electronics, especially the RF communication systems and power supplies. The second step emulates the HIRF environment expected in multiple domains (such as air, sea, or ground airport) in laboratory environments. A lab-based emulation test bed is introduced with higher power and better configurations than the previous work [2,3] and installed for the new emulation experiments. The third step performs careful power level calibrations and measures the effects of laboratory-produced HIRF environment on the commercial radios acquired for testing. These results are then compared to the theoretical models. The system setup and size focus on the S-band (2.4 GHz ISM band) radio links, electronic components, onboard GPS, and navigational sensors. This approach is frequency agnostic and can be applied to any radio frequency

device. From this study, three levels of mitigation are introduced. (1) Minimal protection. (2) Shielding solution. (3) Shielding and EMI filtering solution. Laboratory and in-situ testing provide evidence of the effectiveness of these mitigation methods in promoting the survivability and operability of sUAVs in HIRF environments near high-power radars. Meanwhile, laboratory testing generates a vendor-independent radio behavior model that may be used for prediction and comparison of radio performance in RFI/EMI/HIRF conditions.

Chapter 1

Introduction

1.1 Challenges of safe operation and survivability of small UAS in EMOE

The survivability of small Unmanned Aerial Systems (sUAS) in high-intensity electromagnetic environments (HIRF) is a significant characterization that determines the capabilities of sUAS in critical operation situations. The existing sUAS system designs do not consider the complexity of adversary electromagnetic environments, such as Radio Frequency (RF) interference, electromagnetic interference (EMI), Counter-UAS (C-UAS) electromagnetic attack (EA), and other nearby sources of noises in the frequency spectrum of operation [4–11]. The prior art in this area includes limited laboratory measurements and highly limited field studies. The existing work in this area is still limited since the normal focus has been either on developing large aircraft [10] or counter-drone tools [5–7]. The key challenges are: (1) Many of the existing industrial and government standards in EMC/EMI domain, as well as many of the existing EMI/HIRF mitigation measures that are designed for larger and manned aircraft systems do not apply to sUAS, (2) Lack of technical information, test data, and evaluation data for the highly diversified commercial market of sUAS, including the specific information of the C2 radios being used by the operators of sUAS.

(3) Lack of prior operational and flight experience within or proximity to real-world RF radiation sources or facilities. The consequence of these drawbacks is a lack of useful guidelines for governmental agencies (both civilian and military) when critical decisions need to be made regarding safe deployment or operations of sUAS.

This study aims to identify practical approaches for improving the resilience of existing small UAS against HIRF. These improvements are to be evaluated through both controlled laboratory experiments and in situ flight testing. The initial investigation of this study focuses on identifying the weak spots of the existing flight vehicles, from the propeller, motors, and controllers, as well as the internal electronics, especially the RF communication systems and power supplies. The second step emulates the HIRF environment expected in multiple domains (such as air, sea, or ground airport) in laboratory environments. A lab-based emulation test bed is introduced with higher power and better configurations than previous work [2, 3] and installed for the new emulation experiments. The third step performs careful power level calibrations and measures the effects of laboratory-produced HIRF environment on the commercial radios acquired for testing. These results are then compared to the theoretical models. The system setup and size focus on the S-band (2.4 GHz ISM band) radio links, electronic components, onboard GPS, and navigational sensors. This approach is frequency agnostic and can be applied to any radio frequency device. From this study, three levels of mitigation are introduced. (1) Minimal protection. (2) Shielding solution. (3) Shielding and EMI filtering solution. Laboratory and in-situ testing provide evidence of the effectiveness of these mitigation methods in promoting the survivability and operability of sUAVs in HIRF environments near high-power radars. Meanwhile, laboratory testing generates a vendor-independent radio behavior model that may be used for prediction and comparison of radio performance in RFI/EMI/HIRF conditions.

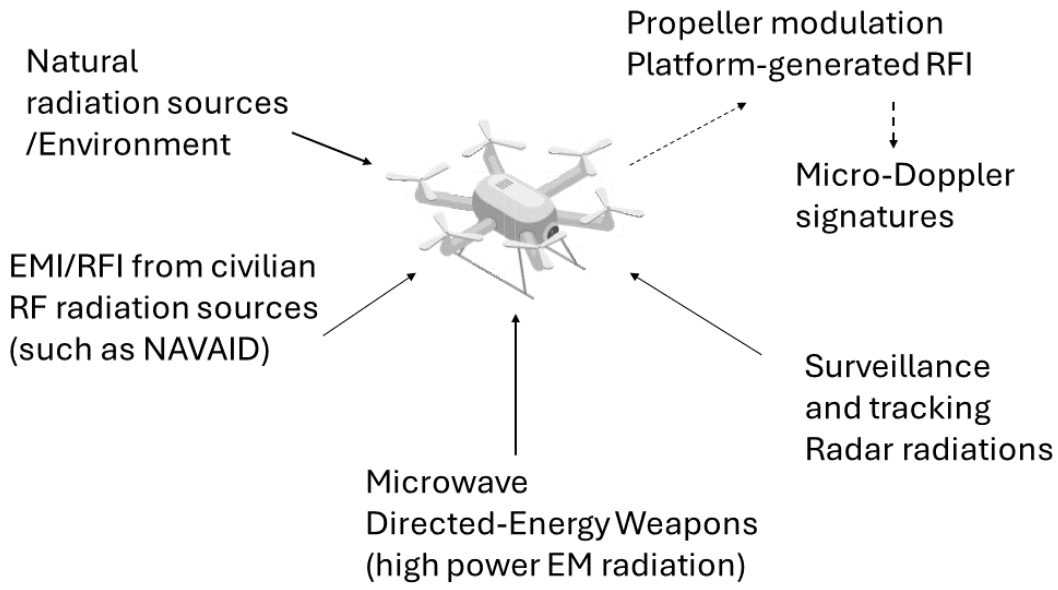


Figure 1.1: Summary of Potential Electromagnetic threats a typical sUAS faces.

Figure 1.1 encompasses some threats a sUAS platform may face in today's electromagnetic environment in which it operates. These threats arise from the complex electromagnetic environments caused by various radiation sources. Many of the existing counter-UAS systems have had the capabilities of using directed-energy beams, carrying high power impulse or other strong electromagnetic counter-measures [8, 9] to disable the UAS operation. Most commercially available sUAS platforms are not designed with the intent to withstand HIRF environments. The need for civilian and commercial operations in the airport facility environment necessitates official approval. To provide an adequate endorsement of potential operations, potential sources of EMC and RFI within the airport facility must be analyzed. Some of these sources include surveillance radars, ILS (Instrument Landing System), and TACAN (Tactical Air Navigation System) transmitters. Natural radiation sources, such as lightning, are another significant threat to onboard electromagnetic on a sUAS, as they are generally not designed with the same electromagnetic compatibility standards as large

and medium-sized UAS. This provides an obstacle to sUAS operations in adverse weather environments for atmospheric sampling. In this study, potentially novel techniques are investigated that may enhance the survivability of sUAS in counter-UAS electromagnetic environments. This includes the protection of command and control (C2) links under RFI and jamming, using advanced C2 radio modulation, and using anti-jamming antenna radar. This study also investigates cross-section control related to the sUAS airframe and electromagnetic shielding. These techniques are combined and integrated with aerodynamic optimization. Additionally, the solution for emission control (EMCON) for the UAS platform, such as the impact of propeller modulation must be addressed.

Table 1.1 summarizes the potential RFI sources in a typical airport environment. In such an environment, the key missions of sUAS are NAVAID and infrastructure inspections. Each RFI source can be further analyzed based on the operation frequency ranges, in-band and out-of-band (OOB) spectrum power levels, and waveform characteristics. Another potential civilian operation of particular interest is using a small unmanned aerial vehicle (otherwise known as sUAS) for the inspection of airport facilities. This is a promising application for government agencies. The current operational rules of 14 CFR Part 107, which applies to the operation of sUAS in general, have serious drawbacks when used for operating inspection UAS within the airport environments. The biggest safety concern is the potential loss of Command and Control (C2) links of the small UAS, caused by the airport radio navigational aid facilities (such as transponders, ILS, TACAN, etc.) as Electromagnetic Interference (EMI) and radars (such as ASR and NEXRAD radars) as High-Intensity Radio Frequency (HIRF) sources. Both threaten sUAS's regular C2 radio links, which can operate in any of three bands: 915 MHz, 2.4 GHz, and 5.8 GHz frequency bands. A majority of sUAS C2 links operate at the 2.4 GHz ISM band as it offers a fair trade-off between bandwidth and range. This thesis study aims to fill the EMI/HIRF operational risk

management gap, provide initial guidelines and procedures to ensure safe operations within the electromagnetic environments in the airport and provide a framework for the Safety Management System (SMS) to support future sUAS operation needs.

RFI Categories	**RFI Sources**	**Comment**
Surveillance Radars	ASR-8, ASR-9, ASR-11, TDWR, ASMR3/ ASDE-X Radar, NEXRAD Radar, Maritime Radio Navigation Radar	Radars pose the highest threat to C2 radio links for link quality and HIRF-based electronic malfunction.
Satellite Links	LEO - Globalstar	Not a significant threat.
Telecom and Communication	LTE (band 40 & 41), 4G, 3GPP, GSM (downlink), UMTS (downlink)	It may cause minor disruptions to the state-of-the-art sUAS C2 links but is not considered a significant HIRF threat.
Commercial Wireless	Airport Wi-Fi/ Hotspots, WiMax (802.16d, e), ZigBee, Bluetooth	Not considered as a significant threat to C2 links after analysis.
Military Radios	UWB Radio, JTIDS (*Joint Tactical Information Distribution System*)	Not considered as a significant threat to C2 links after analysis.
Navigation	TACAN/DME Beacon, Mode-S Transponder, ATCRBS Interrogator/Transponder, ADS-B/TIS-B, VOR and Localizer, Glide Slope (GS)	Potential threats to C2 link qualities when operating at near distances. Not considered as significant HIRF threats.

Table 1.1: Summary of electromagnetic radiation sources in a typical airport environment.

1.2 Existing Radiation Safety Standards

As the key element for safety assurance, the guidance for performing C2 link risk mitigation measures is provided in this section. Examples of current regulations and standards for HIRF-related requirements include 14 CFR Part 23 23.2520 and IEEE Standard 299-2006. Since these are the only currently available guidelines from the government and industry, we'll use these guidelines in the following chapters to determine the key safety thresholds for operation. On the other hand, these requirements are mainly designed for large aircraft and traditional avionics and are not necessarily suitable for sUAVs (unmanned ariel vehicles). Also, these thresholds mainly address the HIRF/EMI safety for the onboard electronics. At the same time, we will point out in the following chapters that the radio and control links need fewer field levels to cause malfunction. There are still clear reference values on the primary shielding method for electronics and human operators, as well as the requirements of threshold radiation levels. Table 1.2 lists the EMF radiation threshold levels derived from these previous studies and is used in this document as the standard guideline for safety risk levels. Note these safety risk levels are not the same as the radio link quality (SIR) thresholds we have been using for C2 radios and the EMI safety levels for the risk of damaging electronics, motors, and human operators. These threshold levels are primarily used for high power sources (such as radar) to compute the risk factors and safe ranges. In contrast, the SIR and link quality-based thresholds are used primarily for operating near wireless communication towers and NAVAID transponders.

Table 1.2: EMF safety thresholds and recommended actions.

E-Field Strength	Magnetic Field Level	RF Power Density Level	Threshold action for electronics, payloads, motor, and batteries	Threshold action for human operators
< 10 V/m	< 2.5mG	< 10 mW/m^2	Safe, low risk	Safe, low risk
Between 10 V/m and 100 V/m	Between 2.5mG to 3mG	Between 10 mW/m^2 and 100 mW/m^2	Medium risk must be mitigated for sensitivity parts	Medium risk, reduced time of exposure.
> 100 V/m	> 3mG	Higher than 100 mW/m^2	High risk must be mitigated and protect all components	High risk, avoid or wear protection.

The threshold values listed in Table 1.2 are compiled from previous studies and established sources [12, 13]. Through testing and analysis performed in this study, it will be shown that while these standard thresholds may be a good general standard for mitigating back-end interferences, the values listed for a safe operations must be closer analyzed for out-of-band (OOB) emissions falling within the frequency band used for C2 link operation. These standards offed helpful thresholds for harmful frequency agnostic electric and magnetic power, however, radio frequency power in the band of operation required to disable a C2 link is lower than the values listed in Table 1.2. This is because The true threshold of in-band power for safe flight operations will be dependent on several factor, including: communication protocol, distance from source, sUAS to ground control distance, receiver sensitivity, maximum transmit power, and antenna characteristics.

1.3 Thesis Outline

The rest of this thesis is organized as follows: Chapter 2 will describe typical sUAS electronics systems and electromagnetic environments, with an elaborate description of the radio, control, and communication units typically used in the sUAS. Chapter

3 will focus on the command and control (C2) link of small UAS and theoretical background, including DSSS and FHSS application to the C2 links and the existing simulation models. The goal of Chapter 3 is to develop a generic and high-level radio and communication channel model for small UAS. Chapter 4 will discuss the RFI/EMI/HIRF risk mitigation solutions. Chapter 5 introduces the laboratory measurement setup and general flight test configurations. Chapter 6 presents the data results and an analysis of these tests. Conclusion and future work will be provided in Chapter 7.

Chapter 2

Description of General sUAS Electronics System and Operational Electromagnetic Environment

2.1 RFI/EMI Spectrum Modeling Measurements

The first step in addressing the RFI/EMI/HIRF challenges is understanding the spectrum models for both the RFI sources and the victim UAS platforms. Here, we provide general information on both while focusing on radar as the main RFI source. For this section, our focus is still on the C2 radio link. Risk analysis is critical for preparing the sUAS inspection operation under complex EM environments. The risks related to the C2 link are estimated based on two criteria; one is the degradation of the link quality (LQ), specifically when the signal-to-interference power ratio (SIR) is lower than 10 dB. Another criterion is based on the HIRF, specifically when the electric field intensity is higher than 10 V/m. Both conditions would lead to high risks of loss or disruptions of the C2 link of sUAS. It is emphasized, however, that not all the sUAS flight profiles would be considered high-risk, and the high risk only occurs when the sUAS or the radio link is exposed to the main radiation beams of the emitter. Therefore, the first step of risk control is to examine the intersection of the sUAS flight profile vs the RFI radiation zones.

2.1.1 sUAS spectrum modeling

The 2.4-GHz frequency band is favored for control of small UAVs for both up-link and down-link radio operations based on many reasons: radio modules are readily available, spectrum access is open to the public as the 2.4-GHz band is one of the internationally harmonized industrial, scientific, and medical ISM bands, and international regulations on transmission power are such that an inexpensive system can provide decent communication ranges under line-of-sight conditions. Furthermore, the wavelength lends itself to conveniently sized, affordable, practical omnidirectional antennas.

Since the 2.4 GHz ISM band is highly congested, a generic spectrum overlapping model would be required to guide the following analysis. The spectrum overlapping model shown in Figure 2.1 contains the channel models of the UAS radio link and the typical RFI spectrum. The generic model will need the spectrum masks of each RFI source, analyze the frequency overlap with specific C2 radio channels, and then compute the predictions of essential parameters such as bit-error-rate (BER), RSSI, SNR/SIR, link quality, and E-field intensity. Some commercial radios already provide these estimations, but their accuracy and reliability are limited.

2.1.1.1 Other Spectrum Examples

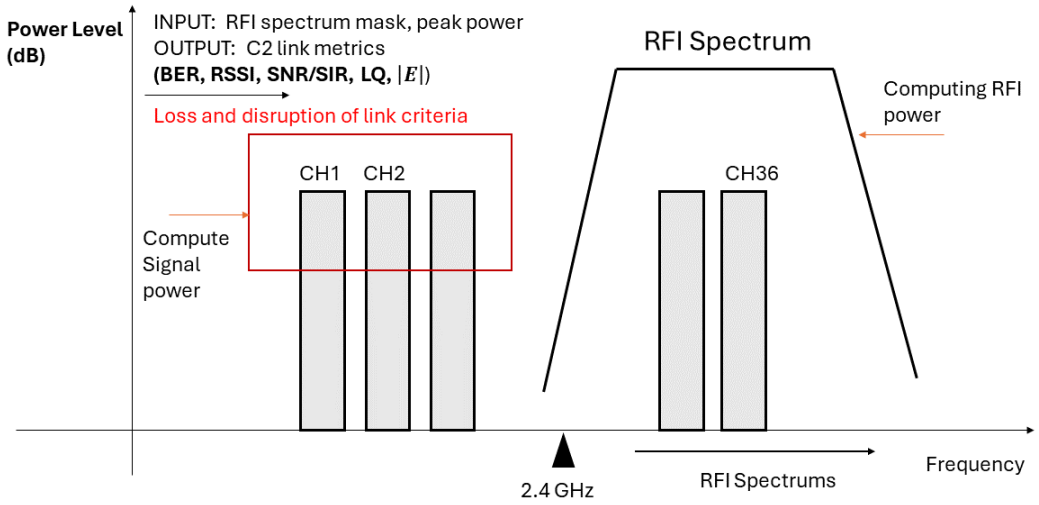


Figure 2.1: Spectrum parameters of sUAS C2 link and the RFI sources.

Despite many standard spectrum masks defined and required by the FCC, actual measurements of the RFI spectrums are still critical to the inputs to the spectrum models. These measurements are done using either a high-performance spectrum analyzer, a low-cost and portable spectrum analyzer, or EMF probes. Chapter 5 will discuss more details on the measurement data collection.

2.1.2 RFI Spectrum Examples and Initial Modeling

2.1.2.1 Air-surveillance Radar(ASR)

Air Surveillance Radar(ASR) is one of the most widely used radars for US airspace surveillance and air traffic control. System information of ASR radar is listed in the following Figure 2.2. ASR-11 radar is a particularly interesting RFI source since the government teams currently desire to perform near-range inspections of this facility without disrupting the radar operation.



Center Operating Frequency	2.7 to 2.9 GHz
Maximum EIRP	25 KW plus 34 dB antenna gain
Nominal OOB Emission Level (dBc)	Up to – 47 dBc
Pulsewidth	1 µs, 80 µs
Maximum duty cycle	9 %
Nominal modulation bandwidth	5.1 MHz
Scanning	360 deg rotation 4.8 sec per rotation

Figure 2.2: ASR-11 radar system parameters.

The RFI spectrum model would need first to compute the spectrum power level based on the relative geometries between the drone and the ground radar. The antenna radiation pattern, as shown in Figure 2.3, needs to be considered for the computation. This radiation pattern shows that when the drone is flying low, it can avoid the radiation from low and high main beams. However, higher main-beam HIRF risks would be expected as the drone flies higher. For example, if the drone operation distance is 100 ft from the radar, only 52 feet of flight altitude is needed to reach the main beam. This factor is incorporated into the modeling processing in the following chapters.

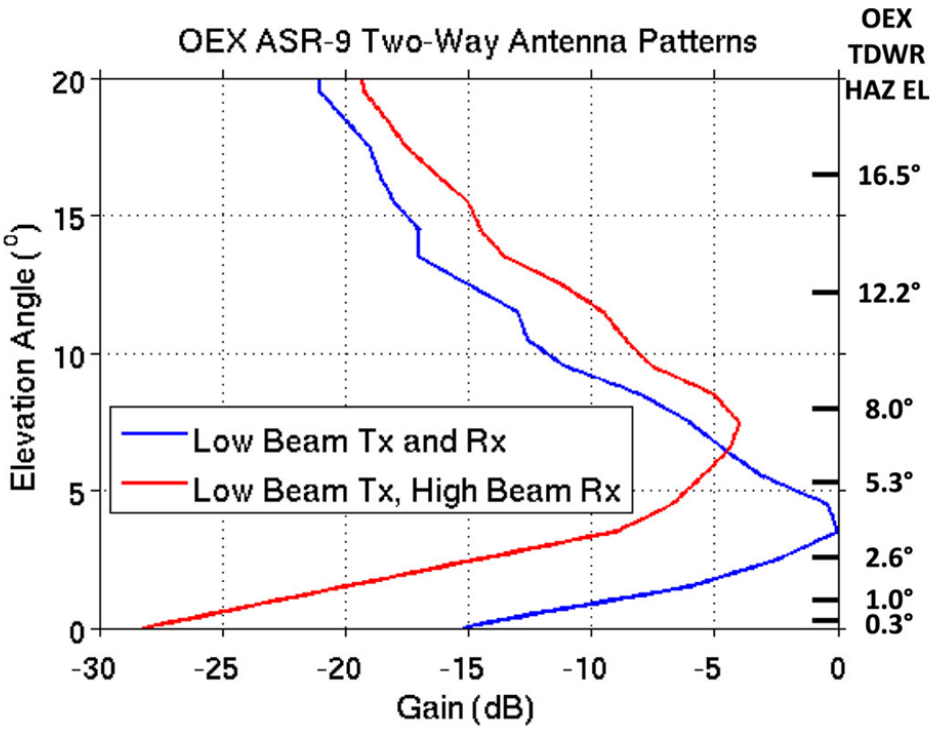


Figure 2.3: Example of the evaluation radiation patterns of ASR-9/11 radars [1].

As an example of the ASR-11 radar spectrum data inputs, Figure 2.4 depicts some spectrum data from actual sites. It is important to emphasize the actual radiating spectrum is more complicated than merely the FCC/NTIA spectrum masks (Figure 2.4(a)). Even though the majority of the measured radar spectrum may be compliant with the standard requirements, at some times, the spectrum harmonics may cause non-compliance to the spectrum masks (Figure 2.4(b)). Also, the time evolution of the spectrum depends on the particular frequency band the radar operates (Figure 2.4(c)) and the out-of-band (OOB) radiation levels at the specific time.

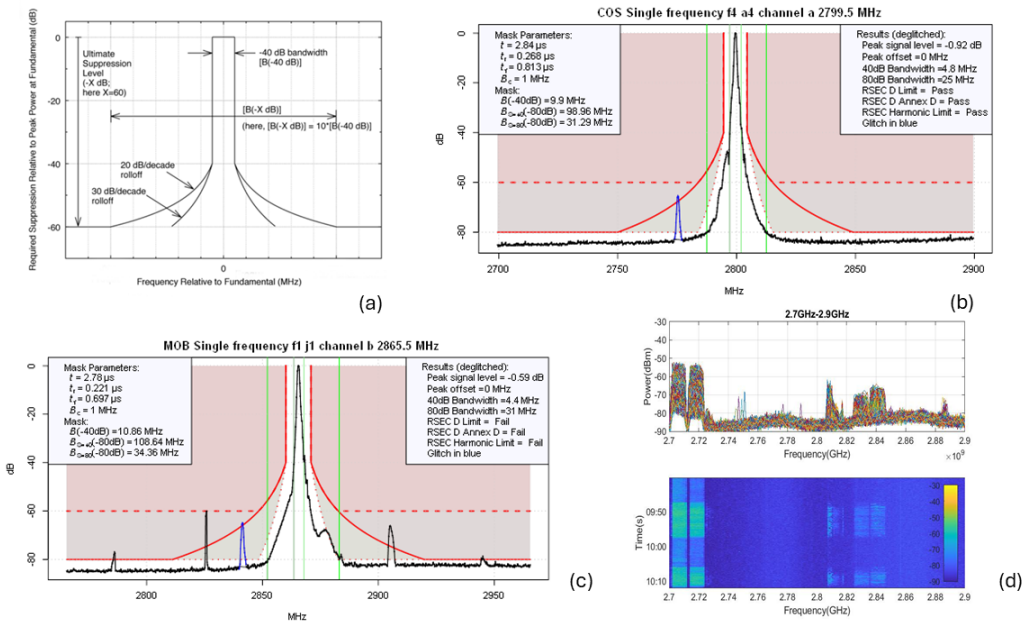


Figure 2.4: ARS-11 radar spectrums.(a) FCC spectrum mask, (b) A measured spectrum from ASR-11 radar compliant with the spectrum mask, (c) A measured spectrum from ASR-11 radar that is not compliant with the spectrum mask. (d) Measured the time-frequency spectrum of ASR-11 radar using a spectrum analyzer payload on a drone.

2.1.2.2 EMI and RFI from UAS Onboard Electronics

The UAS's onboard electronics can be another possible source of EMI/RFI based on all the *active* components listed in Figure 2.5. Initial investigations were focused on reflectivity and the resulting interference from propellers in motion. While propeller material composition affects the electromagnetic reflectivity of a drone in the form of micro-Doppler, there were no significant indicators that varying the material of the propeller affected RSSI of a C2 link.

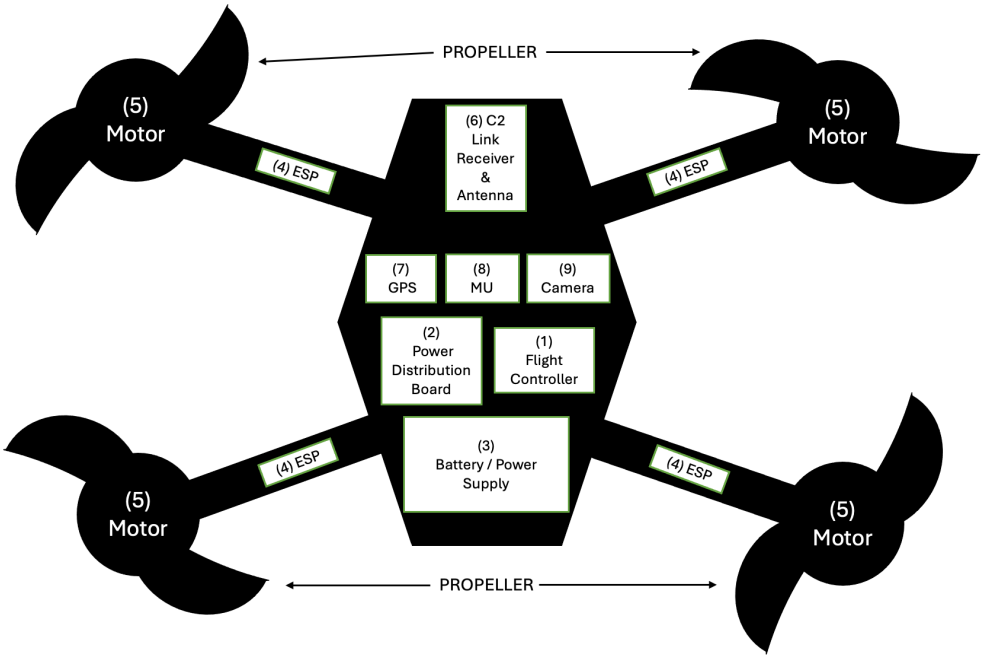


Figure 2.5: A simplified diagram of general structures of small UAS.

Figure 2.5 shows a simplified model of mission-critical and potentially sensitive components onboard a sUAS.

2.1.2.3 Computation of RFI EMF parameters

Equivalent Isotropic Radiated Power (EIRP) measures the total power a transmitter antenna would need to radiate to produce the same power density as a beam antenna. The section develops the basic and simplified formulas that calculate the EM (electromagnetic) field power density (S), magnitude of electric field strength ($|E|$), and magnitude of magnetic field strength ($|H|$), which are used in the radiation safety standards. Firstly, the electromagnetic power density in a unit of $W \Big/ m^2$ is given by:

$$S = \frac{P_t G}{4\pi d^2} = \frac{EIRP}{4\pi d^2} \tag{2.1}$$

In Equation 2.1, P_t is the transmit power of the radiation source in watts, G is the antenna far-field gain relative to an isotropic radiator in linear scale, and d is

the distance from the radiator in meters. Based on the free-space wave impedance $\eta = \frac{E}{H} = 377\Omega$, it can be said that

$$S = \frac{|E|^2}{\eta} = |H|^2\eta. \tag{2.2}$$

From above, the electric field intensity E (in V/m) is related to the EIRP as:

$$|E| = \sqrt{S\eta} = \sqrt{\frac{P_t G}{4\pi d^2} \times \eta} = \frac{\sqrt{EIRP \times 30}}{d} \tag{2.3}$$

Or, simplified to:

$$|E| = \frac{5.5\sqrt{EIRP}}{d} \tag{2.4}$$

Similarly, the magnetic field intensity (in A/m) can be derived in simplified form as:

$$|H| = \frac{\sqrt{EIRP}}{68.8d} \tag{2.5}$$

Equation 2.4 and 2.5 are used as the basic guide for the measurement procedures in the following section and are compared to Table 1.2 to determine compliance with safety requirements. It is noted that, when a wide band RFI source is utilized, the EIRP calculation needs to be carefully adjusted, which will be further discussed in Sections 5.1 and 5.2.

2.2 General Structure and Components of UAS

A small UAS (sUAS) contains various components as part of the airframe and onboard electronics.

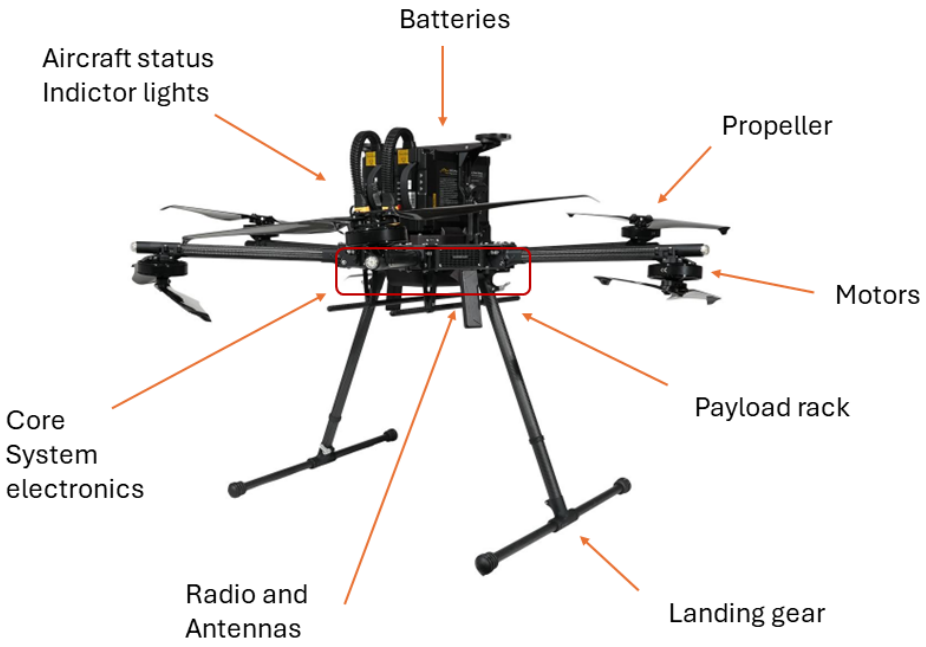


Figure 2.6: General architecture element of sUAS.

Figure 2.6 illustrates a general description of the architecture. The airframe structure is typical among different sUAS/drone types, while the electronics parts, including battery packs and power circuitry, are the more interesting elements for this study. Front-end interference is of particular importance when considering the radio and antennas. This includes the C2 link radio and antennas, GPS, Telemetry, and redundant systems. Back-end interference will likely affect electronics grouped into the 'core systems electronics' and batteries.

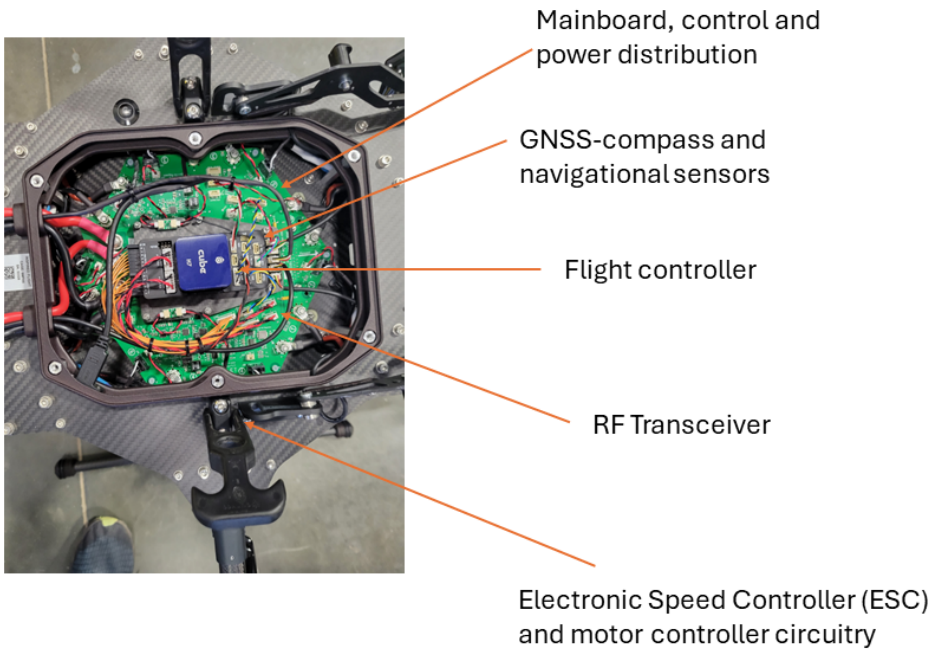


Figure 2.7: Internal circuit and board structure of electronics of an example sUAS.

A breakdown of the electronics system for a specific example of sUAS is shown in Figure 2.7. While generally, UAS of all sizes are designed to perform reliably in various environments, congested environments and environments with HIRF and near sources of EMI can cause significant issues with C2 link reliability and overall function. For this reason, individual circuit elements are subject to these threats and should be analyzed for weakness to front-end and back-end interference in these environments.

2.3 Weak Spot Detection and Sensitive Component Analysis

In this study, a sUAS platform's "EM weak spot" refers to a sensitive component or element highly likely to fail under external electromagnetic interference. Figure 2.8 shows some typical weak spots for sUAS. Weaknesses described in Figure 2.8 can be classified as "front door" or "backdoor" interference types. A disruption to the C2 (Mav/Telemetry) link primarily occurs via the antennas, often called a "front door" interference. This term can describe any RF "entrance" through an antenna port, including GPS, telemetry data transmission, and video/image transmission. For example, the drone controller and associated electronics are sensitive to external high-intensity electric fields (as described in the previous chapter. The C2 link, the focus of tests and experiments in this work, has been subject to the relatively lower power of interference and jamming. A crucial weak spot that may be ignored is the motors, actuators, and related electric speed controller (ESC), which may fail or malfunction under the strong magnetic field disturbance. Protection of these spots is more challenging since they usually involve moving parts in the airframe structures or require airflow to maintain appropriate thermal equilibrium.

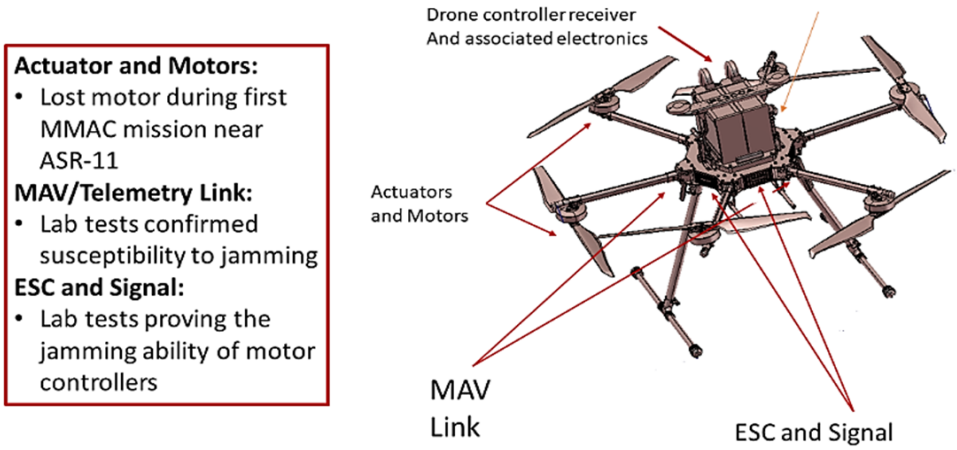


Figure 2.8: Typical "weak spots" of a small UAS subject to the RFI/EMI/HIRF threats.

Chapter 3

RF Communication Risk Model and Theory

3.1 General Approach

The main focus of this chapter is the theory and generic simulation modeling of the control and communication (C2) link performance of the sUAS under the RFI/EMI/HIRF environments. The radio link performance model (RLPM) is defined as a hybrid physical and mathematical model that can predict the C2 radio link performance (in terms of BER, RSSI, SNR/SIR, LQ, and E-field strength at the receive antenna) based on the inputs such as RFI source spectrum information, C2 radio spec sheets, and the relative operating geometry between RFI sources and the C2 radios. The challenges of developing such models are primarily rooted in the unknown specific system and radio parameters, technologies, and operating environments. To provide a "generic" and "platform agnostic" link performance model to the industry, we used the following approach in this study:

(1) Perform the basic spectrum overlapping analysis based on the information from the RFI source and the C2/telemetry radio manufacturer.

(2) Classify the UAS C2 radios using the following categories based on the available specification or datasheet information: In this step, we classify the UAS C2 radio into one of the Categories in Table 3.1. Information from the radio datasheets should be sufficient to perform such classifications. Table 3.1 may not be fully comprehensive,

but it encompasses the majority of sUAS C2 link radios on the market. Each category contains signal modulation schemes, Examples of RF chipset used, and representative vendor protocols. The difficulty of being "jammed" by the RFI sources from Wi-Fi bands is that CAT I is the easiest, and CAT IV is the most difficult. However, an actual C2 radio may belong to multiple categories by combining different radio techniques or having options for various protocols (such as the "Open-TX" and "Edge-TX" offered in Radio Master RM 4-in-1). We analyze the critical individual mode if such multi-protocol RC radios are used. Note that since the majority of C2 radio on the market falls into the CAT I to III, we'll mainly focus on these three categories

Table 3.1: Categorization of Communication Protocol and Respective Hardware Associated with Protocols

Classifications	Modulation	Chipsets	Protocols
CAT I: Basic Radio	Basic FSK/GFSK	A7105, CC2500, nRF24L01	Flysky FS-i6 6CH 2.4GHz AFHDS
	FSK, GFSK, MSK, GMSK and OOK modulations	RFM69, SX1262MB2CAS	RFD-900 Telemetry
CAT II: DSSS	Direct sequence spread spectrum (DSSS)	Cypress, CYRF6936	Spektrum DSM/DSMX
CAT III: FHSS	Fast frequency hopping	MAX2240/2244/2245/2246	Futaba S-FHSS, LoRa
	FHSS and proprietary	Wi-Fi chipset and FPGA-based SDR	Union Robotics Herelink Blue
CAT IV: MIMO	BPSK/QPSK/16-64 QAMwith MIMO	pMDDL2450	Wireless Ethernet extension

(3) Using *generic* radio link models, Compute the reference radio link performance vs. the RFI power (or jamming power) levels. The generic models use a set of parameters to describe the performance metrics (such as BER, data rate, SNR, and loss link threshold) against the RFI signal power or jamming radiating power levels. These parameters are critical to reducing the amount of proprietary information needed from specific radio manufacturers and the workload for laboratory measurements while still providing an effective way to compare the performance of different C2 radios.

3.2 Generic Behavior Modeling of C2 Radios

3.2.1 Combined Modeling of Radio System Simulation and Analytical Models

3.2.1.1 CAT I Radio Modeling

The general theory of link quality versus the signal-to-interference ratio (SIR) is usually based on the Bit-Error-Rate (BER) analysis. For example. BER for Basic BPSK-QPSK (CAT I) and BPSK or QPSK-based DSSS (CAT II) C2 radio link can be calculated in general as:

$$P_e = Q\left\{\sqrt{\frac{2E_b}{N_T}}\right\} \tag{3.1}$$

Here, Q is the tail distribution function of the standard normal distribution, E_b is the BPSK signal/symbol energy, and N_T is the total noise and jamming power.

If we assume the RFI or jamming signals are also Gaussian, it is thus a combination of the receiver thermal noise power N_0 and jamming noise power J_0, calculated by:

$$N_T = N_0 + J_0 \tag{3.2}$$

Meanwhile, the BER for binary orthogonal frequency shift keying (FSK) with noncoherent detection can be calculated with the equation

$$P_b noncoh = \frac{1}{2} e^{-\frac{E_b}{2N_T}} \tag{3.3}$$

Where values are similarly defined. E_b is still the energy per bit, and N_T is the noise and jamming power. Likewise, for coherent detection, the bit error rate of a binary orthogonal FSK signal can be estimated using

$$P_b coh = Q\left(\sqrt{\frac{E_b}{N_T}}\right) \tag{3.4}$$

Where the variables have been previously defined. For binary representations of signals utilizing these modulation and receiver styles, these equations offer an estimation of an upper bound expected under additive white Gaussian noise conditions.

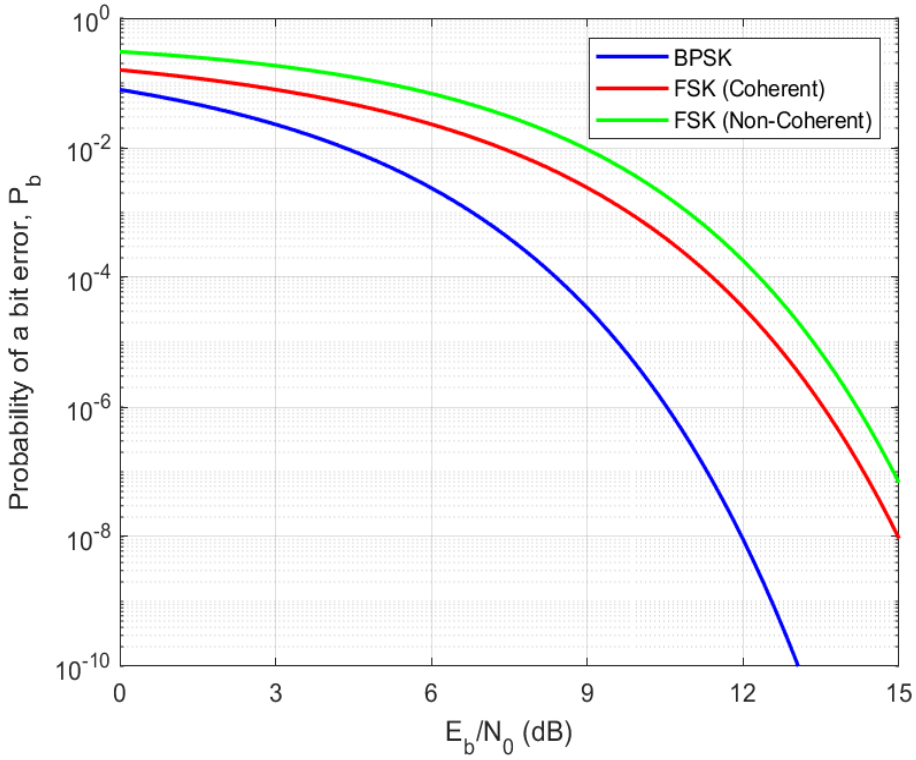


Figure 3.1: BER For BPSK, Coherent FSK, and Non-coherent FSK in a Standard AWGN Channel.

The simple BPSK-BER curve vs. signal-to-total noise power ratio is shown in Figure 3.1. While typical C2 radios utilize at least some type of spread spectrum technique, all utilize a type of modulation. BPSK is one of the most straightforward modulation schemes that exist, providing a simple basis for further comparison. The three modulation techniques modeled here are Binary-Phase Shift Keying (BPSK), coherent Frequency Shift Keying (FSK), and Non-Coherent Frequency Shift Keying. From Figure 3.1, it is shown that in AWGN or equivalent BBN, BPSK modulation is expected to perform the best. Coherent FSK follows this, followed by non-coherent FSK. The complexity of the hardware required tempers the improved

resilience of a BPSK signal. Since the demodulation of a BPSK signal depends on a careful phase measurement of the received signal, a coherent demodulation process is required. Likewise, coherent FSK requires additional hardware for coherent demodulation. While non-coherent FSK performs the worst, the technical trade-off for low-power, low-complexity devices often outweighs the reduced performance of non-coherent demodulation. The end-to-end C2 communication link simulation is required for more accurate analysis and simulations. An example of the QPSK-DSSS-based end-to-end simulation is used to evaluate the typical sUAS C2 radio performance under RFI, with the example waveforms at different stages showing in the Figure 3.4, Figure 3.9(a) and Figure 3.9(b). The RFI signals (or noise) can be injected at any point in this chain, including the channel fading model. The recommended simulation procedure and the demonstrative example plots are shown in the following Figure. Again, these simulations' settings and parametric models must be tuned for specific radio products based on actual measurements from field or laboratory tests.

3.2.1.2 DSSS- CAT II

Direct Sequencing Spread Spectrum is a spread spectrum technique that directly spreads the signal over a larger bandwidth than the initial modulation requires by representing each bit transmitted by multiple chips. A chip in DSSS is defined by the spreading sequence selected for the application. This technique enhances RFI performance and improves susceptibility to interception [14]. Ideally, a random binary sequence is chosen as the spreading code; however, given that the synchronization requirements of a UAS compel the selection of a periodic code. Mixing the modulated data with the selected spreading code can produce a direct spread signal. This is then up-converted to a carrier frequency and can be transmitted as a DSSS signal.

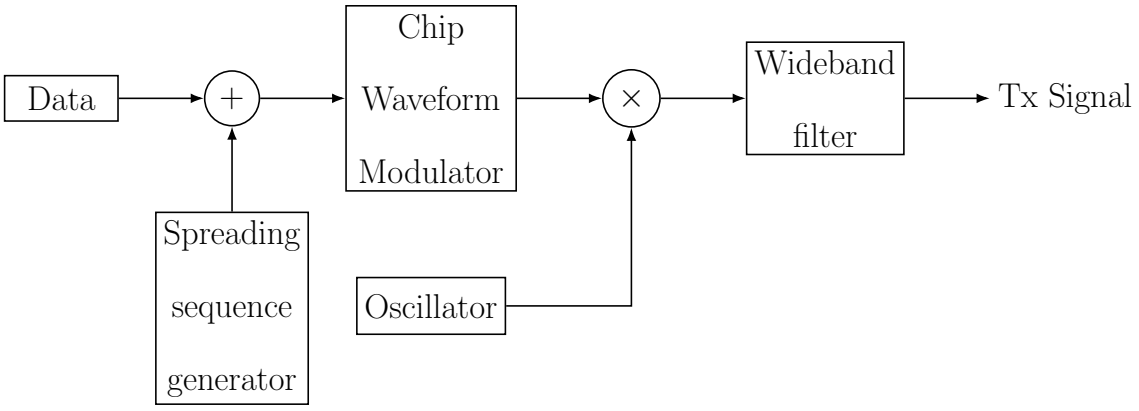


Figure 3.2: Block diagram of the DSSS Transmitter using a Generic Modulation.

The diagram in Figure 3.2 displays the transmit chain, starting with binary data. The binary data is first spread with the sequence generator. Each bit is represented by the 'direct spread' signal. The signal is then modulated with whatever modulation scheme is preferred. This study analyzes BPSK. This modulated and spread data is mixed up to the carrier frequency and filtered before transmission.

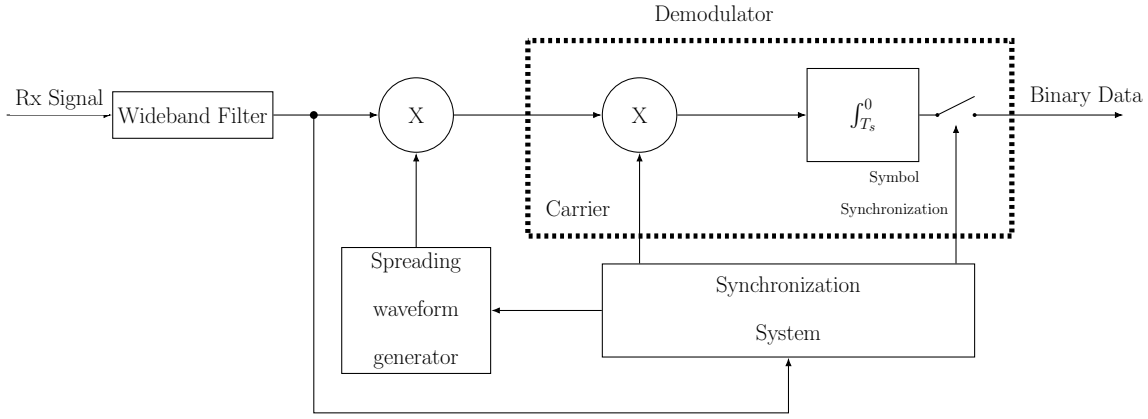


Figure 3.3: Block diagram of the DSSS Receiver with Generic Demodulation.

The receiver chain displayed in Figure 3.3 gives a generic model for receiving a DSSS signal. The spread-modulated and up-converted signal is received first. A filter is used to reduce out-of-band signal (spectral splatter). The signal is then down-converted

A direct sequence BPSK signal can be represented as:

$$s(t) = Ad(t)p(t)\cos(2\pi f_C t + \theta) \tag{3.5}$$

where in Equation 3.5 ([14]) A is the amplitude of the signal, $d(t)$ is the data to be transmitted, $p(t)$ is the spreading code, f_C is the carrier frequency, and θ is the phase of the signal for $t = 0$. The equations described below are used to construct a spreading sequence that performs according to the expected specifications of the specific UAS C2 radio. The bit rate, or bit frequency, is calculated based on:

$$R_b = \frac{1}{T_b}, \tag{3.6}$$

where R_b is the bit rate, and T_b is the bit period (duration of one bit). Meanwhile, the chip rate (chip frequency) dictates the rate at which eat bit is spread and can be defined as

$$R_C = N \cdot R_b, \tag{3.7}$$

where R_C is the chip rate, N is the spreading factor, which can also be considered processing gain, and R_b is the bit rate. The spreading factor will define the degree of spreading.

$$N = \frac{R_C}{R_b} \tag{3.8}$$

where N represents the spreading factor or processing gain.

$$R_S = M \cdot R_C \tag{3.9}$$

where R_S is the sampling rate, M is the oversampling factor, and R_C is the chip rate.

$$B \approx R_C \tag{3.10}$$

where B is the approximate signal bandwidth.

$$T_c = \frac{T_b}{N} \tag{3.11}$$

where T_c is the chip duration and T_b is the bit duration. These parameters are independent of the modulation performed and dictate the robustness of the signal in dynamic noise by increasing the bandwidth of the transmit signal.

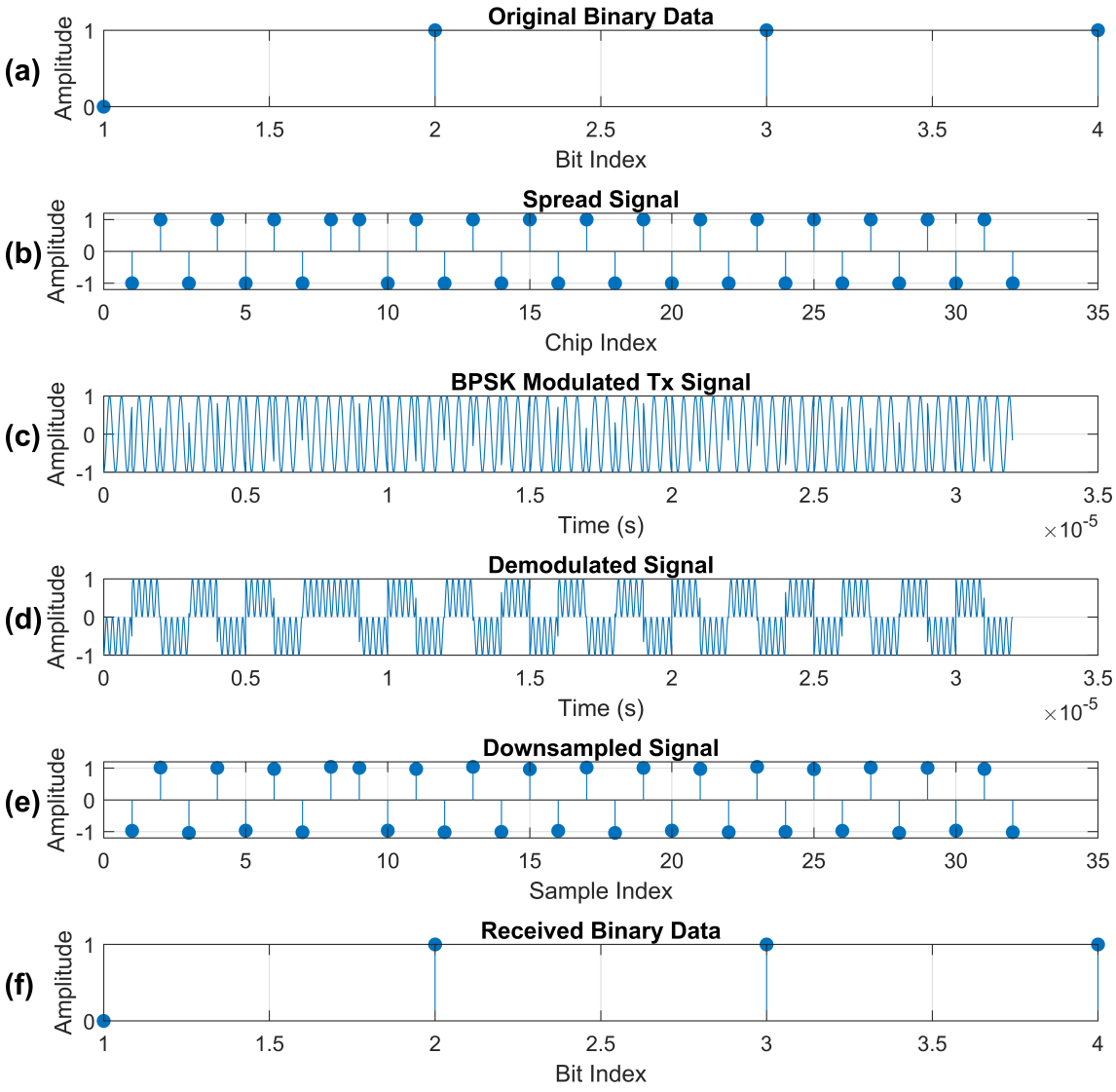


Figure 3.4: Simulation of modulation and demodulation process of a DSSS C2 link.

A simulated C2 link is presented in Figure 3.4. Parameters for this simulation were selected to allow for visibility of the changes to the signal to perform modulation and

direct sequence spreading. In Figure 3.4 4 bits are transmitted. The signal is then spread with a pseudo-random spreading code of length 8. The signal is sampled with 10 samples per chip, and a 8 chips per bit. The mock simulation shown in Figure 3.4 involve small scale values, simulations used for analysis of BER utilize the values described in the respective sections. The simulations are performed in Matlab and are directly mixed to the carrier signal with BPSK modulation.

For DSSS systems applied to current UAS C2 radios, the equation is given by ([15], Equation (10.42)) as:

$$P_e = Q\left\{\sqrt{\frac{2G_p}{\frac{1}{\nu}+\xi}}\right\} \tag{3.12}$$

In Equation (3.12), the BER is represented by $P_e.G_p$ as a spreading factor or processing gain. A typical number is 64 for small UAS C2 controllers. ν is the signal-to-noise-ratio (SNR) computed from the waveform spectrum bandwidth (for example, use 1 MHz for sUAS), and ξ is the inverse of the signal-to-interference ratio (SIR), which is calculated based on the C2 link signal waveform bandwidth as well. Equation 3.12 can be applied to both BPSK and QPSK modulation under BBN.

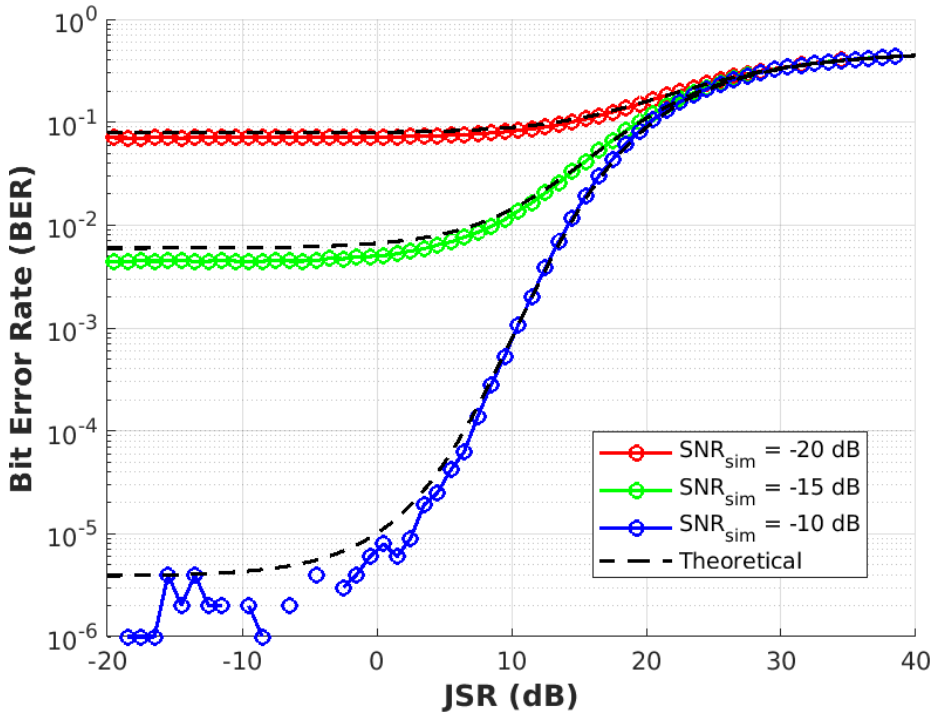


Figure 3.5: DSSS C2 Link Utilizing BPSK Modulation communication system Experimental Bit-Error-Rate vs Empirical Bit-Error-Rate.

Figure 3.5 compares the theoretical and experimental bit-error-rate results given SNR values (-20, -15, -10 dB) evaluated at varying levels of "jamming power". Theoretical curves were constructed using Equation 3.1. The simulated curves displayed in this figure were created utilizing the end-to-end simulations in Section 3.2.1.2, utilizing Equation 3.1 with values of P_e obtained by varying noise and jamming power applied to the end-to-end simulation in the previous section. As the jamming power increases, the probability of error, P_e, for all three cases converge on an upper asymptote. As the probability of error approaches 50%, it is evident that the signal power (including processing gain) is overwhelmed with the jamming power. The asymptote established at 50 % is a result of using only binary phase shift keying. If there are only 2 phases that can be selected in demodulation, there is a 50 % chance that the phase will be correct if chosen at random, therefore, a 50% bit error rate is equivalent to a 100 % jamming effectiveness. The first two cases of lower SNR (-20, -15 dB) exhibit

a strong correlation between the theoretical and experimental. Meanwhile, the value of P_e for SNR = -10 dB is realized along the same general curve but diverges as the theoretical plot approaches a lower asymptote at approximately 3.78×10^{-6}. This is equivalent to 1 bit lost in every 280,000. Due to computational limitations, only 1,000,000 symbols are transmitted, which limits the P_e resolution. As the number of transmitted and received bits increases, the experimental plot will approach the visible theoretical values. With sufficient computing power, this convergence can be further enhanced. Testing results displayed in Section 6.1 is performed in an anechoic chamber and a realistic SNR value is much higher than the -10 dB. For the case of the DSSS, a measured SNR of about 55 dB is presented in Section 5.1.

3.2.1.3 FHSS-CAT III

The frequency hopping spread spectrum (FHSS) is another popular anti-interference scheme in RC radios. The frequency hopping spread spectrum is a communication protocol in which the transmitted signal's frequency is rapidly changed or "hopped" over a defined frequency range. This can be paired with various modulation techniques to produce the desired communication protocol. There are two forms of FHSS: Fast FHSS and Slow FHSS. A Fast FHSS (FFHSS) signal will be hopped at least once over transmitting a single symbol. This provides better protection against narrow-band jamming and makes using a "following jammer" particularly difficult. Meanwhile, a slow FHSS will transmit multiple symbols over a single frequency, hopping to a new frequency every few symbols. The diagram in Figure 3.6 represents a simple FHSS transmitter/modulator.

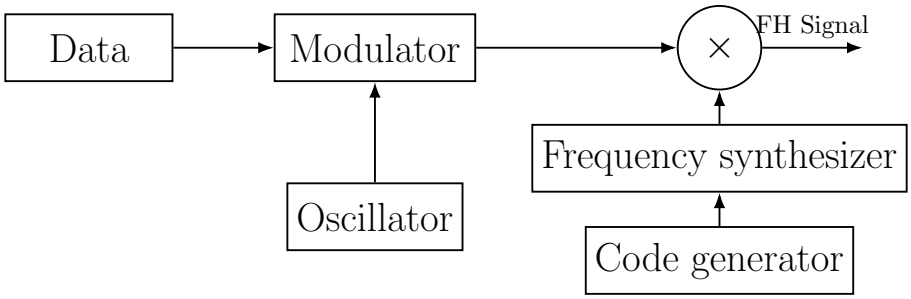


Figure 3.6: Block diagram for a Frequency Hopping Spread Spectrum Transmit Chain.

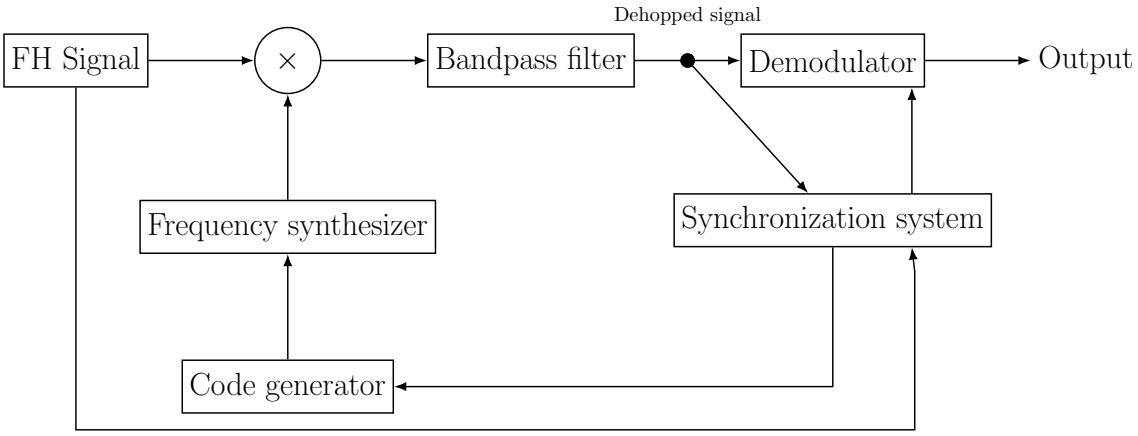


Figure 3.7: Block diagram of the Receiver Side of Frequency Hopping Spread Spectrum Communication Protocol Utilizing FSK .

BER for a fast FHSS-based C2 radio using binary frequency shift keying (BFSK) modulation under broadband RFI/Jamming condition can be calculated based on ([15], Chapter 10 and 11):

$$P_e = 1 - \sum_{k=\left[\frac{L_F}{2}\right]+1}^{L_F} \binom{L_F}{k} \left[\frac{1}{2}\exp\left(-\frac{1}{2}\frac{R}{P_N+J}\right)\right]^{L_F-k} \left[1-\frac{1}{2}\exp\left(-\frac{1}{2}\frac{R}{P_N+J}\right)\right]^{k} \tag{3.13}$$

Where P_e is the Bit-Error Rate (BER), L_f is the number of frequency hops per data bit. It is usually assumed that L_f is less than the number of channels, typically

15-36 for sUAS radios. R is Received C2 link radio signal power (Watts), P_N is Full-band noise power level in Watts, J is RFI/Interference/Jamming power in Watts.

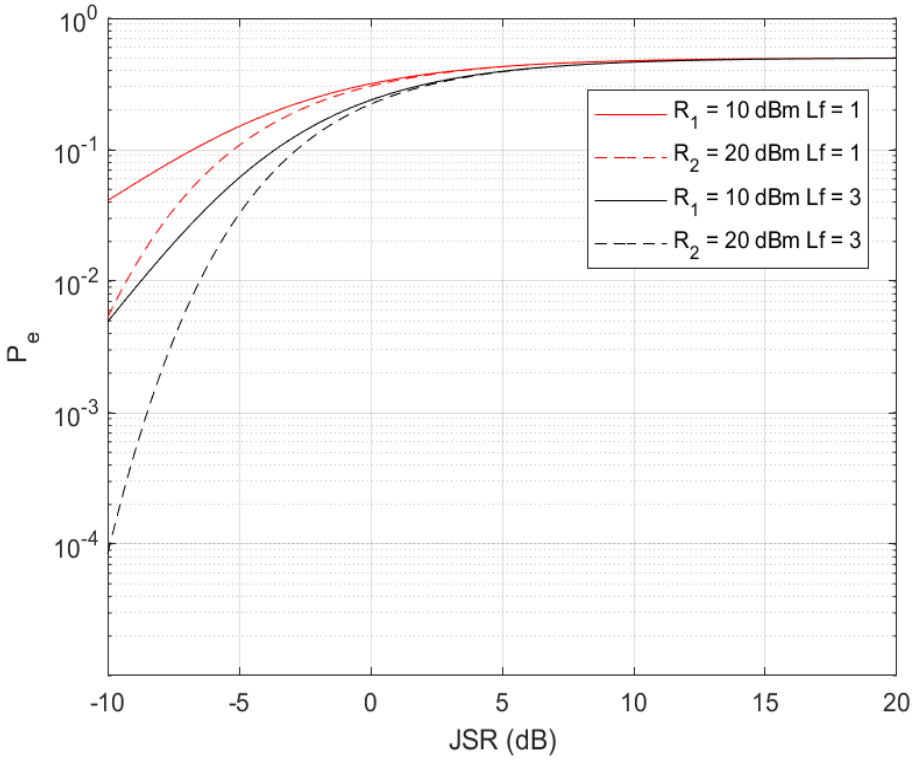


Figure 3.8: Example of BER For FHSS BFSK communication links under the Broad-Band Noise Jamming (BBNJ) Comparing a Specific Case of Receive Power and Frequency Hops.

The parameter values used to fulfill Equation 3.13 are listed in Table 3.2, where the corresponding Jamming power required to achieve the specified JSR can be calculated using Equation 3.14. Fast-FHSS is defined as a frequency hopping spread spectrum signal that hops frequency

$$J_{\text{dBm}} = \text{JSR}_{\text{dB}} + R_{\text{dBm}} \tag{3.14}$$

Variable	Value
L_F	1,3
P_N	-80 dBm
R	-70, -60 dBm
ν	10, 20 dB
JSR	-10 - 20 dBm

Table 3.2: Variable Values for Equation 3.13 Plotted in Figure 3.8

Figure 3.8 represents two plots displayed in [4], elucidating the AJ (anti-jamming) characteristics of utilizing this spread spectrum technique. As can be seen, the BER decreases as the number of hops per bit (L_f) increases. The intended advantage of frequency hopping is the ability to disperse the signal over a large bandwidth, reducing the potential effects of narrow-band noise. It is common for modern frequency hopping systems to perform adaptive frequency hopping, where when a channel is especially congested, an alternate channel will be selected, further improving the protocol robustness in narrow-band noise [14]. This study does not consider narrow-band noise as the RFI source analyzed are expected to produce out-of-band across the operating bandwidth. In Figure 3.9, BBN (broad band noise) power is assumed to be -80 dBm. A more accurate and objective-oriented BER model can be constructed using radio controller (RC) transceiver-specific parameters and measured noise levels in the testing environment.

Meanwhile, the probability of bit error (P_e) for a slow FHSS using MFSK can be calculated for a specific protocol can be computed using

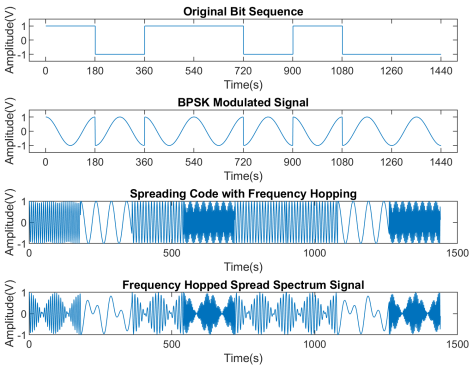
$$P_e = \frac{1}{2(M-1)} e^{-\frac{lE_b}{2N_T} \sum_{q=2}^{M} \binom{M}{q} (-1)^q e^{\frac{lE_b(2-q)}{2qN_T}}}. \tag{3.15}$$

Where M is the number of frequencies used for modulation, E_b is the energy per bit, N_t is the total power, which can be calculated according to Equation 3.2, l is defined by

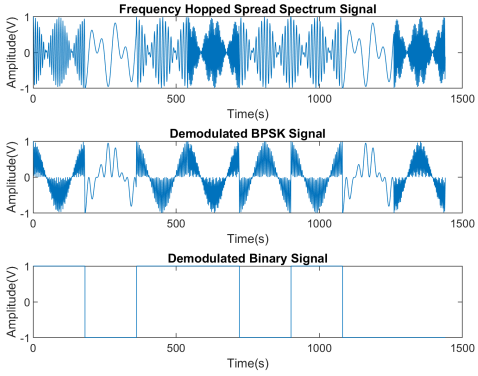
$$l = \log_2 M. \tag{3.16}$$

When a Binary-FSK modulation scheme is considered, this equation is simplified to the bit error rate probability in Equation 3.4. If demodulation within a hop is non-coherent, the BER can be calculated with Equation 3.3, which is sufficient for a signal operating under broad-band noise as each hop will experience the same conditions as long as it is in the band of the noise produced. The energy per bit (E_b) can be calculated as a function of the average jamming power (J_av), average transmit power (P_av), bit rate (R), and spreading bandwidth of a single hop (W_{ss}).

$$\gamma_b = \frac{E_b}{N_T} = \frac{2W/R}{J_{\text{av}}/P_{\text{av}}} \tag{3.17}$$



(a). End-to-end simulation flow for general FHSS C2 link and communication system: information modulation.



(b). End-to-end simulation flow for general FHSS C2 link utilizing BPSK modulation: information demodulation.

Figure 3.9: Side-by-side comparison of modulation and demodulation in an FHSS C2 link utilizing BPSK.

Figure 3.9 shows the steps to transmit and receive an FHSS BPSK modulated signal used for BER simulation. Where the values used for this simulation are toned down significantly from real life values. This simulation provides a simple visual of the steps in producing the FHSS signal with BPSK and down converting and demodulating said signal. This can subsequently be used to simulate a realistic channel under broadband noise.

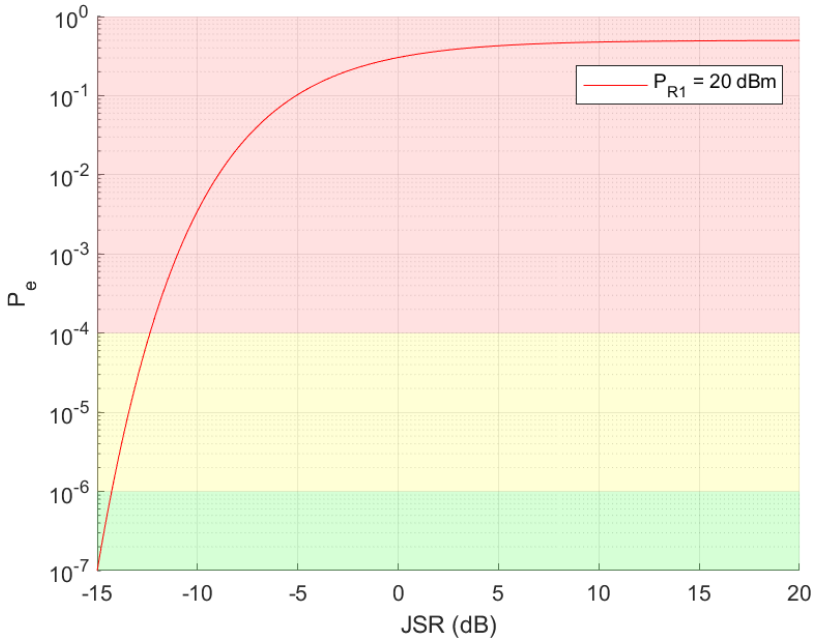


Figure 3.10: Example of BER For FHSS BFSK communication links under the Broad-Band Noise Jamming (BBNJ) for a realistic receiver.

The curve plotted in Figure 3.10 represents simulated BER using realistic C2 radio parameters, where the transmit power is 20 dBm. Receivers in the United States are bound by FCC part 15 [16], which allows for a maximum transmit power of 1 Watt (30 dBm), with exceptions for antenna gain. However, the United Kingdom has stricter transmission requirements. The maximum allowed EIRP is 100 mW (20 dBm) [17] for UK standard. For this reason, many transmitters and receivers will limit the EIRP to the UK standard or, if the system is sufficiently complex, allow for switching between FCC and LBT via software control. In Figure 3.10, it is

assumed that the transmit power of the receiver is 20 dBm, where the noise power is assumed to be -80 dBm). The shading in Figure 3.10 represents three categories of bit error rates. In the red, the BER is greater than 10^{-4}, or 1 in 10,000 bits are demodulated incorrectly. When the Bit Error rate is greater than this value, it can be assumed that the communication between the transit and receiver is sufficiently disrupted that the link can be considered unusable for significant communications. Meanwhile, when the BER ranges from 10^{-4} to 10^{-6}, the link is likely maintained, but there will be some degree of latency as the receiver may send an automatic repeat request, decreasing the data rate [18]. Lastly, communication is normal when the bit error rate is less than 10^{-6}, or 1 in 1 million. Bit error rates are an incredibly useful metric, with acceptable standards heavily dependent on the application. For industrial and military operations, a bit error rate of $10^{-}6$ may be acceptable; Less mission-critical systems like video streaming and payload performance may allow for more errors without significant degradation to flight operations [18]. Figure 3.10 also indicates the transitions from red shading to yellow and yellow to green. These values can indicate a signal-to-interference ratio (SIR) that will provide sufficient data throughput for an sUAS. On the lower end, the model for a generic sUAS indicates that an SIR of at least 12 dB must be present. Meanwhile, a C2 link is maintained from 12 dB to 14.3 dB, but there may be potential packet drops and increased latency. The link can be maintained reliably with a SIR greater than 14 dB. This model does not include processing gain or coding gain, as these values can vary significantly depending on the receivers. Although the communication protocols that determine processing and coding gains are proprietary, appropriate values can be estimated using expected metrics for FHSS GFSK systems, FCC filings, and manufacturer-provided specifications, and then compared with test results.

3.2.2 Simplified and Parameterized Link Behavior Model

The previous Section has established a basic BER/Pe (or link quality) model under RFI or jamming conditions that can be applied to the three basic C2 radio categories. In the following chapters, different tests, experiments, and measurements will further validate these models' basic behaviors and trends. On the other hand, the previous sections explain the motivation for establishing a more generalized link performance model. This model is needed to compensate for the vendor's lack of specific and proprietary technical data. At the same time, it still provides a way to customize when more data is available, allowing the standardization and certification workflow in government agencies. Based on these outputs, we may develop a generic and general-purpose model to describe the performance and loss of link risks of sUAS C2 radios. So far, these performance parameters include:

3.2.2.1 Simplified Behavior Model for Bit-Error-Rate (BER)

The Q-function ([19]) solution for the example equations can be applied to almost all scenarios of radio links for BER modeling. For a given JSR or operational range, this model may be described by:

$$P_e = aQ\left[\frac{b}{(c+\xi)^d}\right] \tag{3.18}$$

The generalized equation Equation 3.18 contains four parameters (a,b,c, and d). The inverse of SIR is estimated based on the analytical or simulation model. Parameters a,b,c,d must be determined based on laboratory test measurements or field measurements. In field operation, for example, we adjust the model parameters to ensure that P_e is calibrated to high values (e.g., 0.9) when the distance to the RFI emitter leads to the actual loss of the C2 link. The generic model in the Equation 3.18 can be applied to characteristics beyond the BER and be used to model other C2

link performance vs the RFI power levels, as well as serving as a basis for modeling the loss of C2 link risks.

3.2.2.2 Simplified Behavior Model of Radio Link Quality

The standard UAS C2 radio link quality metrics are similar to general communication links, characterized by the following measures. The simplified models we derived or utilized are also described as follows:

Throughput/Data rate: Throughput is the actual rate at which data is successfully delivered over a C2 radio link. Throughput is affected by radio system speed, bandwidth, and latency. Under the RFI/EMI/Jamming condition, it is a common practice to determine the behavior models of throughput through experiments. In this study, we use a highly simplified behavior model based on the studies in [20]:

$$R = \begin{cases} R_1 & SJR \geq \eta \\ \sim 0 & SJR < \eta \end{cases} \tag{3.19}$$

It shows that the throughput R is stable if the RFI power is lower than a threshold but almost zero when the in-band RFI power exceeds the threshold; this is when the loss of the C2 link occurs.

RSSI/SNR/RFI Power/E-field intensity: These are closely related measures of how the C2 link signals compete with the RFI/EMI/Jamming powers in the same frequency bands. For example, RSSI (Received Signal Strength Indicator) measures the strength of a received signal and is crucial in determining how much range is left during a flight. RSSI is measured in dBm (decibel milliwatts). Although different radio manufacturers (and open-source controllers such as ArduPilot) claim to provide real-time logs for these metrics, investigations found the specific algorithms are different from vendor to vendor and are usually poorly documented. Therefore, the measurements we perform for these parameters are only for qualitative evaluations of the radio performance. The only exception is E-field intensity, which can be more

precisely measured and compared to the industry standards based on the theoretical model described in equation 2.4.

LQ (link quality) measures the percentage of uncorrupted data that passes through the receiver. In RC receivers, LQ is displayed in a format such as 9:100, where the first number represents "RFMD" (or RF mode), and the second number represents the actual link quality value (it's in percentage between 0 and 100). Like RSSI/SNR, LQ calculation and recording highly depend on the specific manufacturer's implementation and would not have a generic behavior model other than empirically measured data.

Loss-of-link Behaviors: The Loss of C2 Link is the consequence of a combination of conditions based on all the quality metrics above BER is lower than a threshold, throughput (R) is very low or close to zero, RSSI is below a threshold (e.g., -70 dBm), SNR is below a threshold (such as 6 dB), RFI power or E-field intensity is higher than a threshold (such as 1.5 V/m). These behavior model parameters need to be measured for each specific radio under investigation and would be the basis for comparing the performance of the C2 radios of UAS.

Effectiveness RFI/EMI/HIRF mitigations: As this study focuses on the remote inspection mission of sUAS, the critical behavior model parameter to measure the effectiveness of RFI migration solution of UAS C2 radio is the safety operation (C2 link operates normally, no loss of link) distance of the UAS to the RFI sources, i.e., E (mitigation effectiveness) is a function (f) of the safe operation distance to the RFI emitter before and after the mitigation measure:

$$E = f\left(\Delta R\right), \Delta R = R_O - R_M \tag{3.20}$$

Again, such model parameters can only be experimentally determined for specific emitter environments with specific sUAS platforms.

Chapter 4

EMI/RFI/HIRF Risk Mitigation

This chapter focuses on the detailed background of mitigating the EMI/RFI/HIRF risks of sUAS using a combined shielding and filtering technique. Examples of current regulations and standards for HIRF-related requirements include 14 CFR Part 23 23.2520 and IEEE Standard 299-2006. These requirements are mainly designed for large aircraft and traditional avionics. There are still clear reference values on the primary shielding method for electronics and human operators, as well as the requirements of threshold radiation levels. Table 5 lists the EMF radiation threshold levels derived from these previous studies and is used in this document as the standard guideline for safety risk levels. Note these safety risk levels are not the same as the radio link quality (SIR) thresholds we have been using for C2 radios and the EMI safety levels for the risk of damaging electronics, motors, and human operators. These threshold levels are used mainly for high power sources (such as radar) to compute the risk factors and safe ranges. In contrast, the SIR and link quality-based thresholds are used primarily for operating near wireless communication towers and NAVAID transponders.

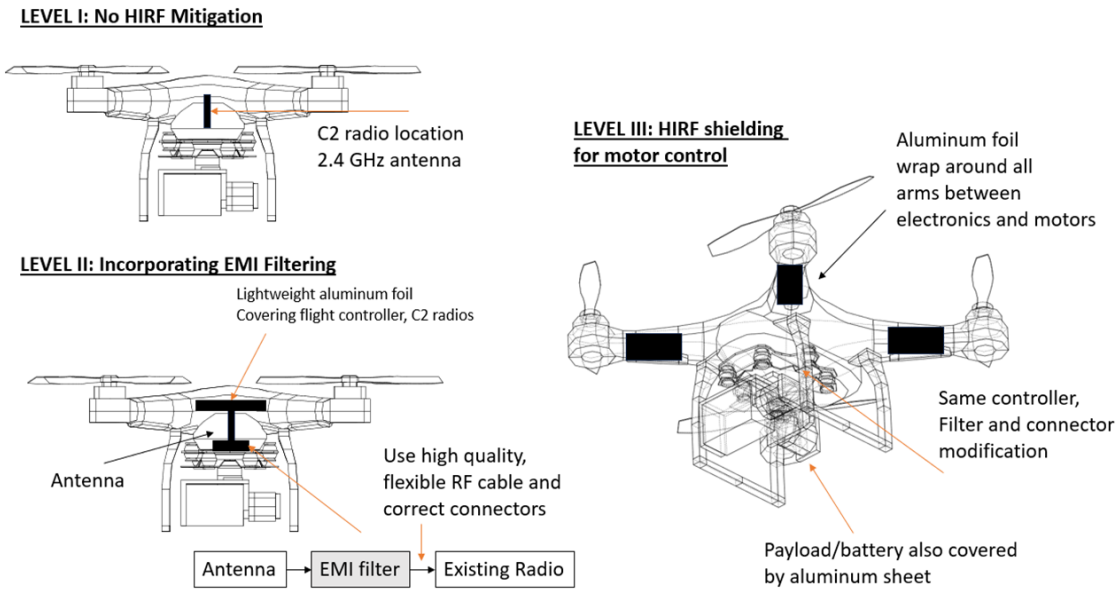


Figure 4.1: Summary of RFI/EMI/HIRF mitigation and reinforcement techniques.

4.1 Levels of Mitigation

4.1.1 Level I: No Mitigation

Level I mitigation is used when a sUAS is used "as is" to operate in potential HIRF environments. Although the sUAS has not been modified, the operator should be aware of the risks and consider them using operational distance as minimal mitigation (Based on the link budget calculations). The examples of Level I mitigation, as shown in Figure 4.1, are the "default" payload installation of the RF receivers without any protection. As the operational distance gets closer, Level I mitigation may become insufficient for the safety of the C2 link and UAS internal electronics.



(a) (b)

Figure 4.2: Examples of the "Level I", No RFI mitigation (default installations) (a) Commercially available IF1200A Hexcopter without RFI mitigation. (b) Commercially available IF750 Quadcopter without RFI mitigation.

Typical sUAS operations should not require additional EMI protection as long as EMC practices are adhered to for individual components of the sUAS (general components found in Figure 2.5 [21].

4.1.2 Level II Mitigation: RFI Filtering Mitigation and C2 Radio Enhancement.

The Level II mitigation requires modifying sUAS's C2 radio system by adding EMI filtering. The following Fig.4.3 illustrates examples of such mitigation.

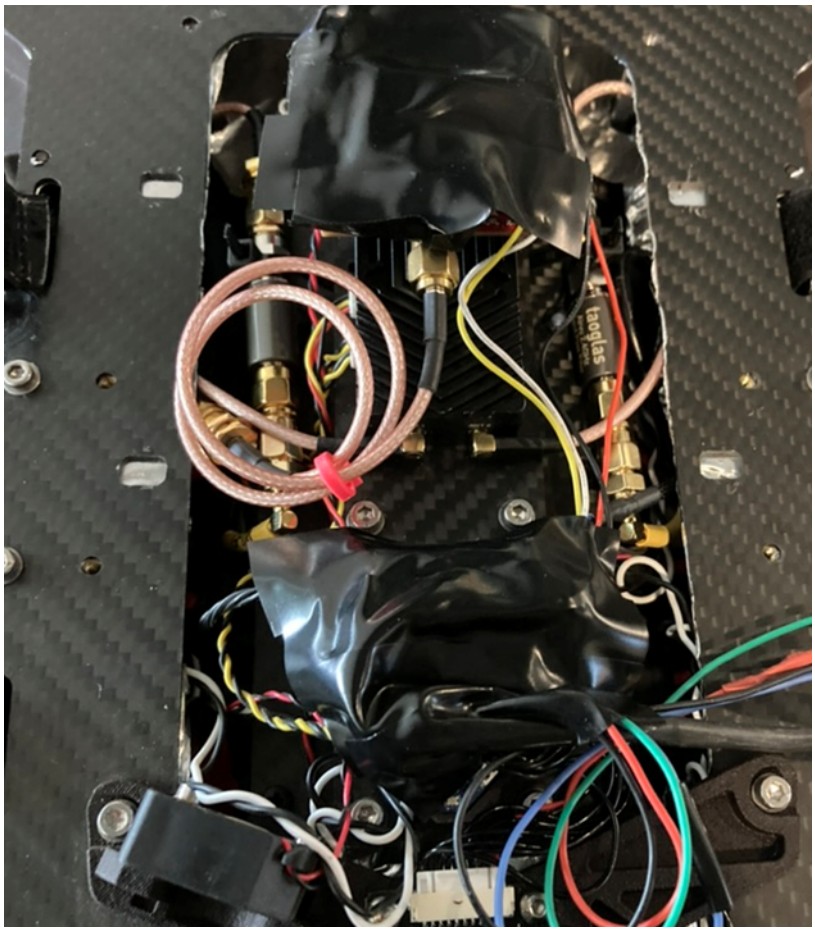


Figure 4.3: Example of "Level II" HIRF/EMI mitigation, focusing on protecting the C2 link and RF channel.

As one of the standard solutions, the C2 link is typically a band pass EMI filter with a passband covering the 2.4 GHz Wi-Fi frequency. While it is assumed that there is an internal filter on the sUAS receiver, the addition of the band-pass filter will further improve the out-of-band emission rejection. The example in Figure 4.4 captures the basic requirements of such filters. This example uses two band pass filters in the two radio channels for the IF750 UAS. The two filters have identical specifications, as shown in Figure 4.4, which shows the filter requirements as both insertion loss and return loss for the two filters used. In addition to the filter response requirements, the physical size of the filter must ensure that it can fit into the enclosures of the UAS onboard controllers.

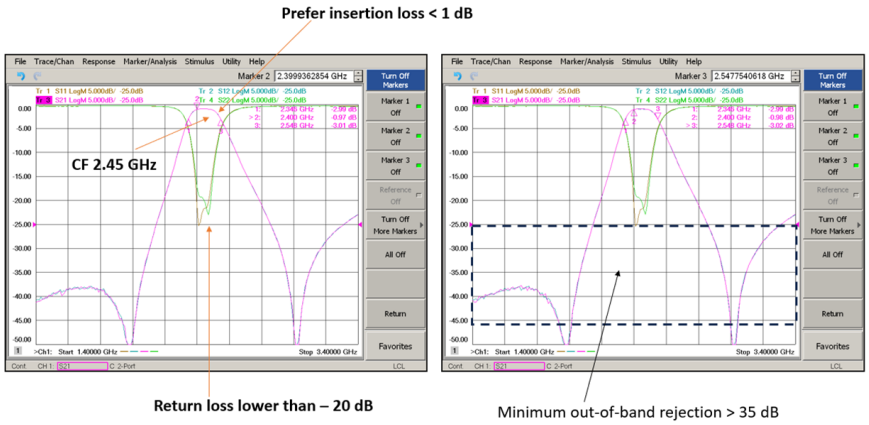


Figure 4.4: Example of the minimal requirements of the identical EMI filters used in the onboard C2 radio channels, response measurements in the insertion loss and return loss format.

Figure 4.4 displays S11 and S21 of the filters utilized in mitigation method II. These S11 measurements indicate the filters offer less impedance to signals in the range 2.354 GHz to 2.548 GHz, with a minimum value of -25 dB. Meanwhile, both S21 and S12 are low values over the same frequency band (near 0 dB). Together these values indicate that the filters offer good rejection of out of band signals, while promoting in band signals. The filter is a passive component so we expect the S11 and S22 curves as well as the S12 and S21 curves to be identical. The different in S11 and S22 values is likely due to the manufacturing of these filters. Since only one filter is measured there is not enough data do draw definite conclusions, however, it is likely that the impedance at each port is different as a function of machining tolerances as the frequency range is the same, with a slight difference in location of minimum S11 and S22 values.

4.1.3 Level III: RFI/EMI filtering + Shielding

The RFI/EMI filtering and the shielding protections are used in Level III mitigation. The shielding technique would take the reference of the existing EMI and HIRF shielding standards but consider the following unique requirements for sUAS: (1) Selecting appropriate shielding materials to ensure the materials do not add excessive weight to the overall system weight as well as the balance of weights. For this reason, we recommended general-purpose adhesive aluminum foil or aluminum tapes as shielding materials instead of other materials. (2) The primary protection area should be the motor and motor controllers. These areas on the sUAS airframes are also critical and subject to the HRFI effects.



(a) (b)

Figure 4.5: Examples of the "Level III", Aluminum tape shielding (a) Aluminum Shielding on the upper part of the IF750. (b) Aluminum shielding on the bottom side of the IF750.

Figure 4.5 shows examples of Level III shielding treatment in a sUAS. Shielding effectiveness is measured in decibels (dB) and indicates the effectiveness of a shield in preventing electromagnetic interference (EMI) from interfering with a device's performance. The effectiveness of a shield is determined by the amount of attenuation it achieves, which is the difference in the intensity of electromagnetic signals before and after the shield is installed.

4.1.4 Mitigation Level Selection and Considerations

While in this study no ill affects were noted while testing with Mitigation Levels II and III, it is important to consider potential adverse affects of implementing filters and shielding as well as the proper environment for each. In context of mitigation level II (filtering) we must consider the effects of adding an additional filter to the front of the receive chain. Typically, a receiver frontend is designed to have the lowest noise. This is described in Friis's formula for noise factor, which equates total noise as a function of gain and noise factor for individual components,

$$F_{\text{total}} = F_1 + \frac{F_2 - 1}{G_1} + \frac{F_3 - 1}{G_1 G_2} + \frac{F_4 - 1}{G_1 G_2 G_3} + \cdots + \frac{F_n - 1}{G_1 G_2 \cdots G_{n-1}}, \tag{4.1}$$

Where F_{total} is the total noise figure of the receive chain, and F_1, F_2, F_3, to F_n describe the noise figure of each component in the order the received signal experiences the components. The gain for each component is similarly defined by G_1, G_2, G_3, and G_n [22]. The noise figure of the first component has the greatest effect on the total noise figure as subsequent noise figures are reduced by the cascading gain of the previous components. For this reason, a low noise amplifier (LNA) is often an ideal choice for the first component on a receive chain. When receiving a low-power signal, this improved the SNR by reducing noise caused by the receiver hardware. This can be advantageous when operating in an environment with low ambient noise in the frequency of operation. Meanwhile, it may be ideal to utilize a low noise filter when there are strong levels of noise around the frequency of operation. In the context of this study, a low noise band-pass filter may be advantageous when the sUAS is flown in an Electromagnetically complex and strong environment where OOB emissions may result in in-band frequency as well as in the surrounding frequencies. If only in-band noise is present (like in the case of broadband or narrow-band jamming) the selection of an LNA as the first element in the receive chain will improve SNR to a greater degree.

Meanwhile, level III mitigation involves the "shielding" of sensitive components using aluminum foil. While there were no negative effects from this addition observed in this study, it is important to understand the potential unintended results of mitigation level III. Firstly, many sUAS require some level of airflow to keep components at the correct operating temperatures. This is particularly important for moving components like motors. If the motors do not receive adequate cooling, they may overheat causing damage and potentially reducing the life of the motor. Maintaining the operability of sUAS motors is incredibly important as motor failures can cause serious damage to equipment and personnel. Significant research has gone into improving the thermal regulation of motors specifically [23], therefore it is important to consider the effects of shielding on thermal regulation.

Chapter 5

Measurements and Verification Techniques

5.1 Basic Designs

The previous chapters (1-4) establish the essential background of sUAS operation in the adversary electromagnetic environment, basic RFI/EMI impacts theories, and basic mitigation methods. This chapter describes the design and setup of laboratory and field measurements that validate and verify the fundamental theories. The results and discussions of these experiments will be discussed in the next chapter. A laboratory test and verification setup is used for in-depth verification of the specific radio performances from the vendors. Such verification has unique values compared to the field test evaluations. For example, it can be placed in highly controlled environments to exclude unwanted environmental factors. It can realistically emulate various EMI/RFI/HIRF sources and the responses of C2 radios to them without the risks of damaging the sUAS. It is essential to have a sufficiently high power level or EIRP in the lab tests. Table 5.1 lists the transmit power level required for the lab tests if an exact duplication of the radar transmitter sources is desired. For example, if we want to duplicate the same impact of ASR-11 radar on the C2 link of the IF750 drone at 91 meters, the transmit peak power from the laboratory emulation setup before sending it into the 2.4 GHz antenna setup should be close to 600 watts. This requirement is unrealistic for most of the lab and chamber test setups. However,

based on the measured relationship between the SNR/SIR and the transmit power level, we can extrapolate the condition that verifies the safe ranges of operation (The curves are similar to previous sections but have an X-axis as the RFI power level from a transmitter, Y-axis as SNR/SIR measured in the lab, together with the indicators from the UAS log file at the specific condition). This estimated relationship in the lab can be obtained using lower power levels. For example, we can use the filtered noise jamming power levels up to 30 watts peak power to emulate the conditions of loss C2 link and obtain the required trend curve.

Table 5.1: Laboratory Emulation Measurement System Power Levels for Motor and Fan Impacts.

Properties	IF 1200A drone system	IF 750 drone system
Distance [m (ft)]	15.24(50)	91(300)
Peak Power [kW]	25	25
Antenna Gain [dB]	34	34
EIRP [Watts] to be emulated	63 Megawatts	63 Megawatts
Power Density @ Distance [W/m^2 (using Peak Power) to be emulated	21515	603
Event of drone system HIRF impact	Motor Failure	Fan Failure
Power is Required to replicate the impact on the drone system in the lab test setup. (distance about l.5 m) Based on the analytical model	19.24 KW	539.56 W

5.2 Setup of Test Instruments

5.2.1 Broadband Noise (BBN) Generator

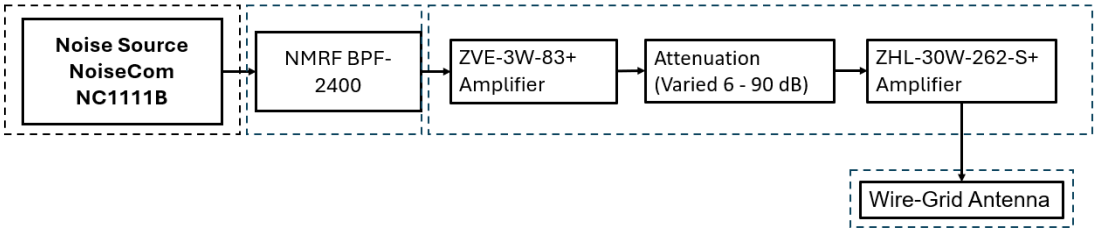


Figure 5.1: Block Diagram of noise generation and amplification for 2.4 GHz ISM band as a part of the RFI emulation test.

A block diagram is displayed in Figure 5.1, highlighting the general layout of the "noise generator" or "jammer" used for RFI testing in this study. The hardware is visible in Figure 5.2. Two power supplies are required to supply the required voltage for both amplifiers and the noise source. The hardware system is illustrated in Figure 5.2. Two power supplies are needed to supply the required voltage for both amplifiers and the noise source.



Figure 5.2: Example images of the laboratory test setup - Noise generation as RFI source.

The broadband noise is produced by an NC1111B module, which produces white Gaussian noise between the frequencies 1 GHz to 2 GHz with 2 dB of flatness [24]. This setup can produce -90 dBm/Hz noise power density, with an aggregate output power of 0 dBm for its intended bandwidth. The intended operating of the noise generator is 2.4 GHz to 2.5 GHz or just 500 MHz outside of the operative frequency of the NC1111B. The output of the NC1111B is characterized both inside and outside of the intended operating frequency, and results are listed in Table 5.2.

Table 5.2: Output Power of NC1111b across different frequency ranges.

Frequency Range	**1.5-1.6 GHz Values**	**2.4-2.5 GHz Values**	**1-2 GHz Values**
Bandwidth [GHz]	0.1	0.1	1
Output Power [mW]	0.0837	0.0105	1
Output Power [dBm]	-10.7727	-19.7881	0

The flatness of the noise from 2.4 GHz to 2.5 GHz was characterized to be ±5 dB. The 3-watt amplifier then provides a typical (nominal) gain of 35 dB [25], resulting

in an output power of 15.212 dBm. The maximum input power for the 30 Watt amplifier (ZHL-30W-262-S+) is 9 dBm [26]; therefore, at least 6 dB of attenuation must be used, which will result in an output power of 30 Watts (44.77 dBm). A bandpass filter is utilized directly after the noise source [27], but some 'out of band' noise is still amplified throughout the chain. To asses the output power in the band of interest a spectrum analyzer was used to measure power spectral density from 2.4-2.5 GHz for each level of attenuation utilized. A TinySA spectrum analyzer was used to finalize the power density to reduce the risk of excessive power levels. A 100 W 40 dB attenuator is used for each test, and the value is added back to the output power. Again, EIRP is calculated using the equation:

$$\text{EIRP} = P_{\text{tx}} + G_{\text{tx}} - L_{\text{c}} \tag{5.1}$$

where $P_{\text{TX, BW}}$ is the transmitter power calculated in the bandwidth from the Power Spectral Density (PSD), G_{TX} is the gain of the antenna (24 dB in this case), and L_{c} is the cable loss.

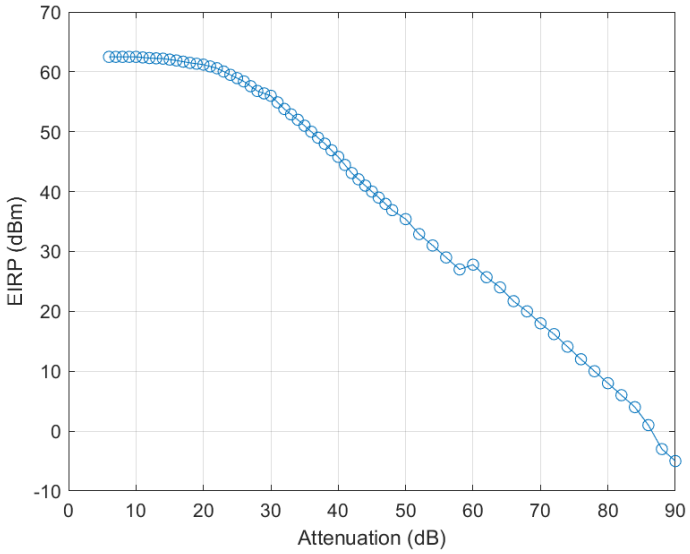


Figure 5.3: Measured EIRP in the 2.4 GHz ISM Band with various TX attenuator settings of the RFI emulation transmitter.

The resulting EIRP value derived from Equation 5.1 are displayed in Figure 5.3, where typical behavior expected from an amplifier is visible. As the attenuation increases, EIRP decreases. The linear region of the amplifier is visible from attenuation values 30 to 90 dB. Meanwhile, compression in the saturation region can be viewed from 6 dB attenuation to about 30 dB. The nominal output power of the 30-watt amplifier at 3 dB compression is 45 dBm (31 Watts), which results in an EIRP of 67 dBm, given antenna gain of 24 dBi [28] (with a conservative cable loss of 2 dB). Meanwhile, the maximum EIRP displayed in Figure 5.3 is 62.5 dBm. The observed 4.5 dB difference can be attributed to out-of-band noise propagating through the RF amplifier chain while not being part of the 2.4 - 2.5 GHz frequency band of concern.

The TX attenuator setting from 10 to 70 dB in the chamber tests allows a 60 dB variation of the RFI transmits power levels. The noise plus interference level reduces significantly when the RFI power level reduces. However, the SNR and Noise+RFI power levels at long range tend to become flat when the RFI level is below a certain threshold (about 50 dB attenuation setting), since the RFI noise power becomes negligible at these ranges.

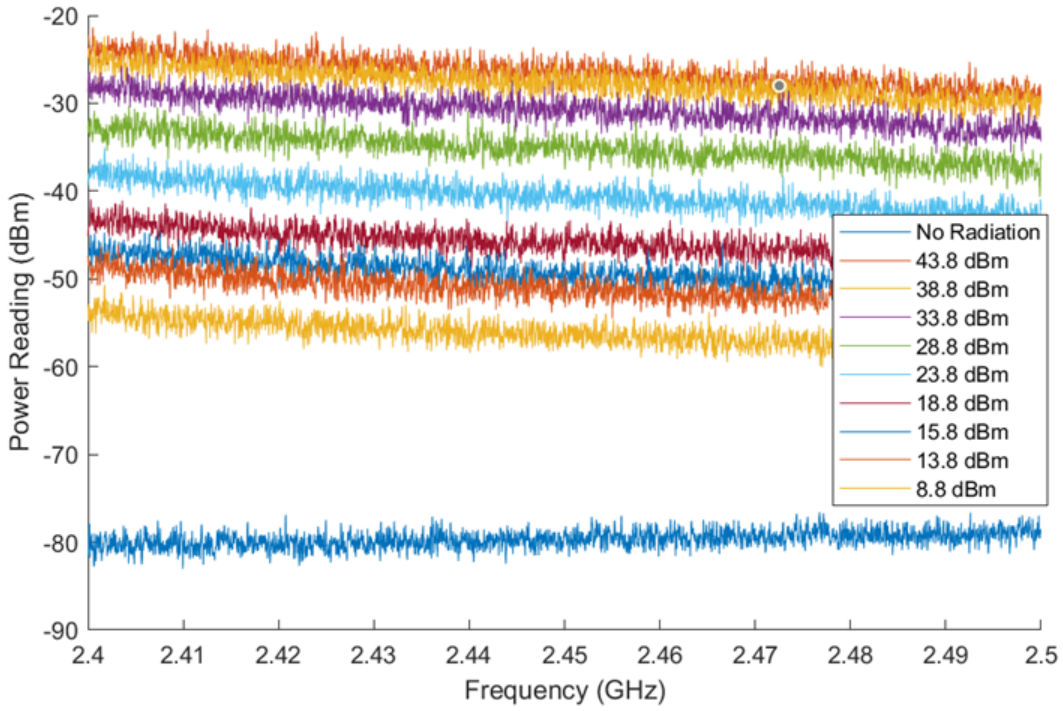


Figure 5.4: Initial verification of the behaviors of the lab-measurement system of noise transmit power measured using a portable spectrum analyzer (TinySA).

The initial behavior plot of the RFI power level control is illustrated in Figure 5.4. In these tests, a spectrum analyzer is used to record the spectral density at the location of the sUAS under test. The noise generator described in Section 5.2.1 is used to transmit the noisy signal used in Section 6.1. Transmitted noise is expected to range in the 2.4 GHz ISM band (2.4 GHz to 2.5 GHz) and transmit power to vary with the level of attenuation applied. Various attenuation levels were utilized, resulting in an expected output power of 8.8 dBm to 43.8 dBm. The measurements associated with the predicted power level validate decreasing noise power as the attenuation level increases.

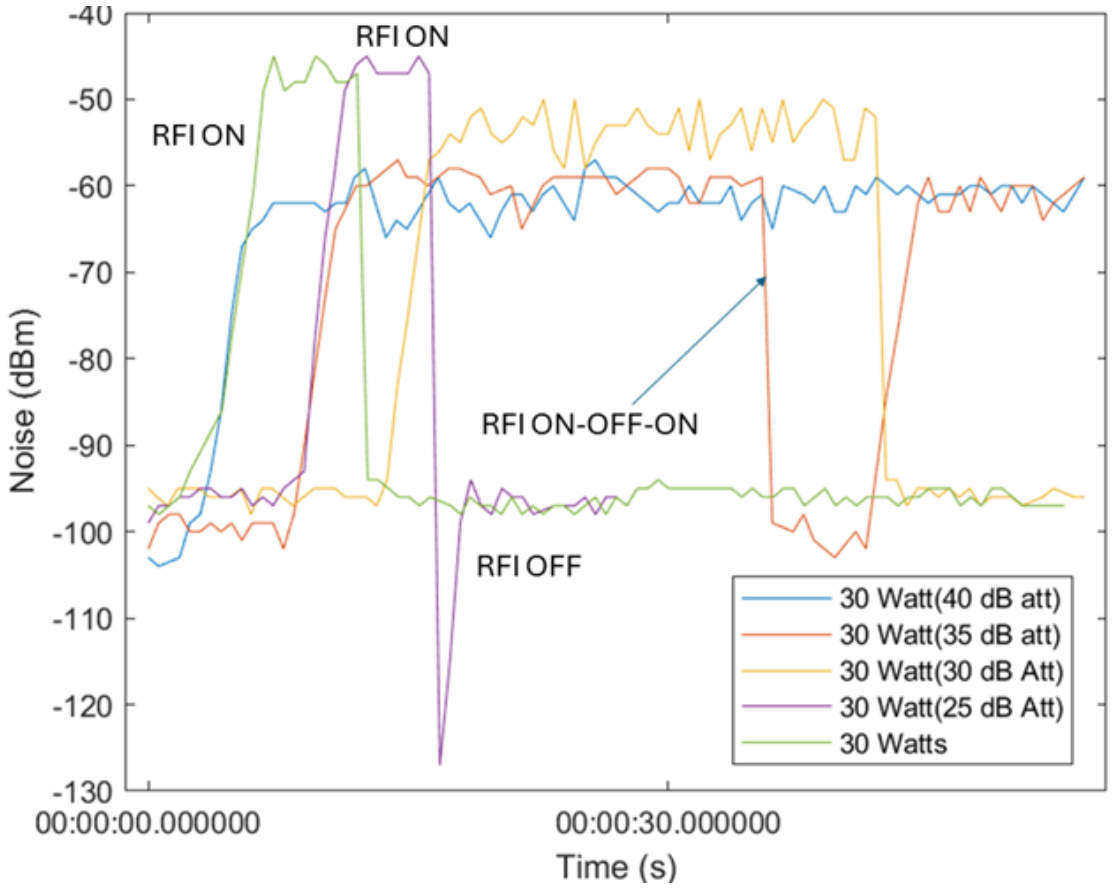


Figure 5.5: Initial verification of the behaviors of the lab-measurement system of transient behavior of logged telemetry data from quadcopter sUAS.

The effects of the transmitted noise power on the C2 link of a commercial receiver are also shown in Figure 5.5. The quad-copter sUAS (IF750) is placed in front of the noise generator described in Section 5.2.1 is turned on in short periods. This verifies the ability of the sUAS to indicate the level of noise power transmitted. Also, for the commercial radio examples, we found that at least a 7 to 10 dB Signal to Noise Plus RFI level is needed for the Flysky C2 radio to maintain operation, and levels less than that will cause loss of link or severe link disruptions.

These preliminary tests were intended to provide evidence of the precision and accuracy of the telemetry values provided by the commercial radio's tested in this study. While there is a clear indicator of noise levels, it was found that these values

can not be used to distinguish finer resolutions of attenuation. This preliminary testing demonstrates the need for additional measurement devices during "jamming tests" described previously in this section.

5.2.2 Inspired Flight C2 Radios

The two sUAS analyzed in this study are the Inspired Flight model 750 and 1200A. These state-of-the-art sUAS exceed the performance characteristics of typical sUAS of this size. These drones are highly configurable and can be purchased with various internal equipment. The IF750 analyzed in this study was purchased with a HereLink package. The HereLink is an integrated handheld controller and ground station. The HereLink is robust and reconfigurable for various sUAS as it is compatible with both Ardupilot and PX4. The HereLink system comprises the Controller (HereLink Ground System) and the receiver (HereLink Air System). This system logs telemetry, including RSSI and noise [29]. The maximum transmit power for this device is 23 dBm, with 2 dB of gain through the antennas [16]. The frequency of operation is 2.402 - 2.483 GHz. The HereLink air system is capable of transmitting over 11 channels, with adjustable channel bandwidth of 10 MHz or 20 MHz with QPSK modulation. The channel bandwidth utilized by this receiver is an indicator of the DSSS technique as DSSS typically utilizes a larger bandwidth than the FHSS counterpart [30]. The option to select 10 MHz and 20 MHz indicates the DSSS parameters are alterable for differing environmental situations and operations. For this radio using DSSS the spreading factor will determine the data rate, which in turn gives the processing gain for this system. The equations for defining the processing gain from the previous variable are defined in Section 3.2.1.2.

The IF1200A utilizes dual-band hardware. The DS-12 Jeti controller utilizes a 2.4 GHz C2 link. A ground station is also present as a redundant command and control link. Telemetry is available through both systems, with values such as RSSI and

noise available. A distinct advantage of this setup is maintaining a ground station link, allowing the pilot to perform immediate return to land (RTL) commands when the 2.4 GHz C2 link is interrupted. The flight controller used in this sUAS is the Cube Blue H7, which is capable of operability with various receivers. However, official documents for the Cube Blue H7 recommend usage with Spektrum / DSM [31]. The current state-of-the-art DSM protocol is DSMX which utilizes a hybrid DSSS-FHSS system with GFSK modulation. Previous versions of the Spektrum DSM protocol, utilize dual frequency bands to further spread a DSSS signal. Typical sUAS receiver systems with frequency hopping utilize slow frequency hopping as it reduces complexity and requires hardware, therefore, it can be assumed that this new version utilizes slow frequency hopping. Therefore, a typical DSSS probability of bit error rate is utilized to estimate the probability of bit error for this receiver, where it is well established that hybrid systems perform worse than either system in AWGN given all other parameters and hardware remain constant [32].

5.2.3 Commercial C2 Radios

The risk of using commercial C2 radios for the tests is the lack of access to the internal data and reliable data recording. However, it is crucial to incorporate them into the test procedures since they are the actual equipment used in operations. Table 5.3 lists the radios under test in this study. Only qualitative and behavioral measurements are performed on these radios, and the primary results are summarized as follows. First, the power level must be identified to cause the loss of the C2 link under broadband noise.

Table 5.3: Commercial C2 Radio Pairings Present in this study.

Transceiver + Receiver	Communication Protocol	Spreading Technique	Modulation
Jeti Duplex + Jeti REX12	Jeti Duplex 2.4 EX	FHSS	GFSK
Radiomaster Ts16S + FS-IA6B	AFHDS 2A	FHSS	GFSK
Radiomaster TS16S + R88	FrSky D8	FHSS	GFSK



(a) (b) (c)

Figure 5.6: Reciever's used in this studies analysis of command-and-control links (a) Fly-Sky FS-iA6B (b) Jeti Duplex REX 12 (c) Radiomaster R88.

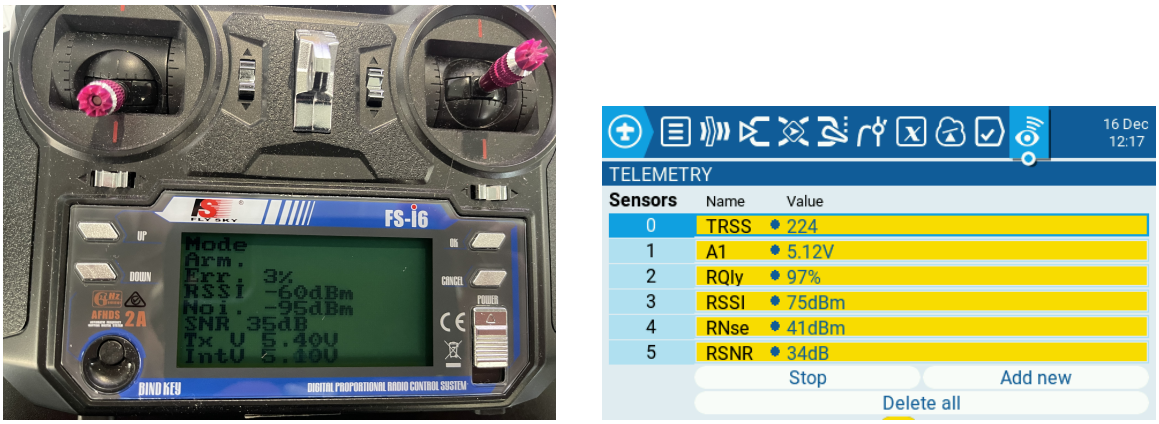
Figure 5.6 presents the commercial receivers used in this study. To better understand the capabilities of these receivers and how they adhere to models in Chapter 5, the transmit power and receiver sensitivity are investigated. While it is commonplace to use the term "receiver" to indicate a device presented in Figure 5.6, the device operates as both a receiver of control commands and a transmitter of telemetry and sensory data back to the ground station. To uphold convention, the term "receiver" is used throughout this study to indicate the sUAS side transceiver. Meanwhile, "transmitter" means the ground station or ground control and command transceiver.



(a) (b)

Figure 5.7: Transmitter units used, in this study, for analysis of C2 link (a) Jeti Duplex X Radio control system 2.4GHz & 900 MHz (b) Radiomaster TX16S .

The transceivers presented in Figure 5.7 display the handheld controllers used in this study. Both the handheld transceivers (commonly called transmitters) allow data logging and can present real-time data to the operator. The FS-IA6B receiver is one of the cheapest and most popular C2 radios. It operates over the 2.4 GHz ISM band using the proprietary FlySKy communication protocol, AFHDS 2A (Automatic Frequency Hopping Digital System). This communication protocol supports up to six channels and two devices operating with the same protocol within the same band. Another advantage this receiver has over alternative entry-level receivers is the ability to report telemetry data. The ground controller radio counterpart for the FS-IA6B is FLysky FS-i6X. However, the Radiomaster Transceiver can operate with the proprietary communication protocol required by the receiver and will also log telemetry values. Thus, a fair comparison is achieved by using the RadioMaster controller.



(a) (b)

Figure 5.8: Telemetry data available on the two transmitter used to record data and verification of RSSI and Noise values (a) Telemetry data as it is presented on the FS-i6 transmitter from the FS-iA6B receiver (b) Telemetry data as it is presented on the Radiomaster TX16S using the FS-iA6B receiver.

The FS-i6 transmitter is designed to work with the communication protocol utilized by the FS-iA6B receiver (AFHDS 2A) and reports the telemetry data as is expected. Figure 5.8(a) presents the telemetry data available in this setup. Where the receiver and transmitter were placed within a meter and low levels of noise were expected. Meanwhile, the telemetry data differs significantly when the TX16S transmitter is paired with the same receiver and placed at a similar distance. The SNR is nearly the same, proving evidence that the RSSI and RNse(Noise) are off by the same scalar value. In both cases, the RSSI remains constant over at least 30 seconds, for Figure 5.8(a) -60 dBm and for Figure 5.8(b) 75 dBm. The difference between these two numbers is 135 when the telemetry values of Noise and RSSI acquired from the FS-iA6B and TX16S pairing are subtracted by 135, values consistent with the Figure 5.8(a) pairing are adopted. This allows for the use of the TX16S controller, which provides telemetry data logging. Both the R88 and Jeti Rex12 can display some link quality indicators, with the R88 displaying RSSI and link quality (LQ as a percent

of 100). The Jeti Rex12 offers a link quality (A) value out of 9. These indicators are sufficient for a general aviator to determine whether the environment is safe for flight; however, these values do not provide enough precision to warrant plotting as a function of EIRP.

5.2.4 Receiver Parameters

The receiver radios analyzed in this study are introduced in Sections 5.2.3 and 5.2.2. Typical models for both Dsss and FHSS are introduced in Section 3.2, where the models predict BER performance as a function of jamming to signal ratio. These models include only the relationship between broadband additive white Gaussian noise, and neglect improvements in performance as a result of processing and coding gain. The world of commercial C2 radios is broad, and often, the specific communication protocols and hardware are proprietary. For the IF-iA6b and Radiomaster R88, these components are accessible and processing gain and coding gain is estimated based on component data sheets and assumptions about the spread spectrum technique and data rate. These value will be used to improve models introduced in Section 3.2 to match the receiver under test better. An FHSS receiver using GFSK modulation can typically provide 10 to 20 dB of gain, depending on the bit rate and spread spectrum bandwidth, which can be calculated using as a function of the two,

$$G_P = \frac{W_{ss}}{R}, \tag{5.2}$$

where W_{ss} is the bandwidth of the spread spectrum and R is the bit rate. It is possible to acheive very high levels of processing gain at the sacrifice of transmit speed. For example, given a FHSS signal using binary GFSK modulation with a bit rate of 20 kbps and spread spectrum bandwidth of 60 MHz, the gain can be calculated to be 32 dB [18].

Category	Specifications
Model Name	FS-iA6B
Protocol	AFHDS 2A (Automatic Frequency Hopping Digital System, 2nd Generation)
Frequency Band	2.4 GHz ISM (2.408 GHz to 2.475 GHz, 67 MHz total bandwidth)
Modulation	GFSK (Gaussian Frequency Shift Keying)
Channel Bandwidth	500 kHz
Data Rate	2 - 500 kbps
Sensitivity	-98 dBm (typical)
Radio	AMICCOM A7105
RF Front-End	SKYWORKS RFX2402E
FEC	(7,4) Hamming code
Estimated Gain	20 - 23 dB

Table 5.4: FS-iA6B Receiver Specifications

The first receiver analyzed is the FS-iA6B, where characteristics of the receiver and utilized communication protocol are displayed in Table 5.4. Specific values like bandwidth, data rate, and hop separation are proprietary and cannot be used to calculate an accurate processing gain for the receiver. However, there is speculation that AFHDS 2A utilizes a data rate of 500 kbps and FCC filings indicate that 140 channels are utilized over a bandwidth of 70 MHz [33]. Not all of these channels are used for AFHDS 2A protocol used for FS-iA6B for the six communication channels used by the FS-iA6B. It is estimated that only 50 Channels are used, where the

remaining 20 channels are unutilized. The gain value estimated for this receiver is therefore composed of 20 dB of processing gain assuming 500 kbps with 50 MHz, where an additional 3 dB of coding gain is assumed as an upper limit, providing an estimated range of total gain of 20 to 23 dB. FCC filings for this device indicate that the maximum power output is 16.07 dBm for a single channel, therefore the maximum output power is estimated to be 16 dBm for this communication protocol.

Likewise, the R88 receiver is considered at a component level.

Category	**Specifications**
Model Name	R88
Protocol	D8/D16/ Futaba SFHSS
Frequency Band	2.4 GHz ISM (2.400 GHz to 2.483 GHz, 83 MHz total bandwidth)
Modulation	GFSK (Gaussian Frequency Shift Keying)
Channel Bandwidth	NA
Data Rate	1.2 - 500 kbps
Sensitivity	-104 dBm (typical)
Radio	CC2500
RF Front-End	RFX2411N
FEC	Convolution Coding
Estimated Gain	23 - 26 dB

Table 5.5: R88 Receiver Specifications

The communication protocol used during testing for this receiver was D8, a proprietary communication protocol utilizing the FHSS and GFSK modulation. D8 is an

older version of Radiomaster's proprietary communication protocol where data transmission speeds are slower and fewer channels are available. The maximum transmit power of the TX-16S transmitter used with this receiver is 20 dBm, this provides an EIRP of 22 dB. Likewise, the D8 uses a lower data rate supporting a processing gain. While FCC filings for this specific device are unavailable, a closer look at the CC2500 data sheet provides evidence of improved processing gain over the FS-iA6B. The CC2500 data sheet reports that the maximum bit rate for GFSK is 250 kbps [34]. A processing ain of 23 dB can be estimated using the same bandwidth. Likewise, this radio chip's convolution coding used for FEC is assumed to provide from 0 to 3 dB of gain. This leads to a total gain of 23 to 26 dB. There is less information publicly available for the radio systems used for inspired flight and the remaining commercial radio (Jeti Duplex REX 12). A JETI DS-12 is utilized for testing the REX12 receiver and the internal proprietary IF1200A receiver. The processing and coding gain for both these systems are unknown, however, it can be estimated that they operate with similar characteristics to other known receivers.

Receiver	**Transmitter Power (dBm)**	**Estimated Gain (dB)**
REX12	20	15.8

Table 5.6: JETI Duplex REX12 Receiver Specifications

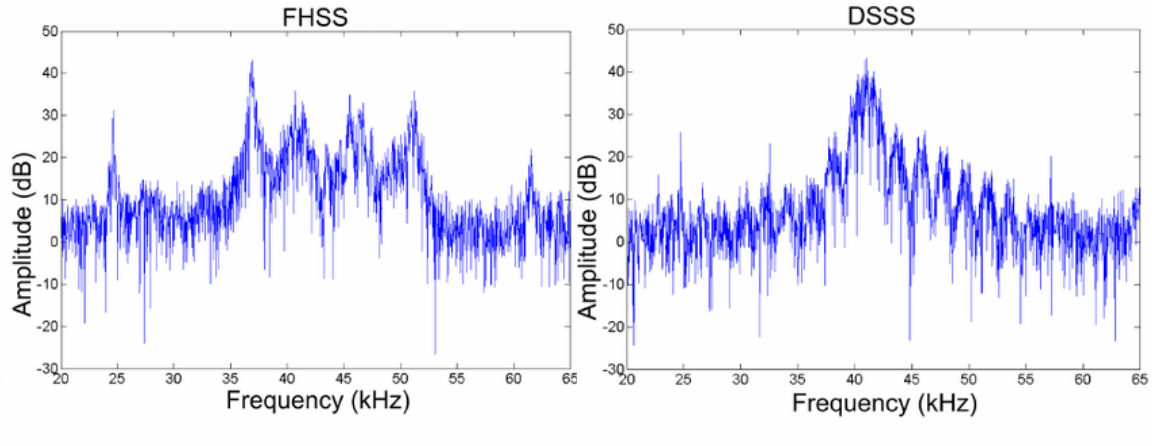
For these receivers presented in Table 5.6, the transmitter EIRP values are acquired directly from the transmitter data sheet [35], where the transmit power is adjustable from 10 to 20 dBm. The antenna gain is reported to be 2 dB [35]. Meanwhile, we will assume that the spread bandwidth occupies less than the entire operational bandwidth of 75 MHz. FCC Filings suggest that this receiver operates with 16 channels, where each channel spans roughly 2.6 MHz [36]. Resulting in a spread bandwidth of 48 MHz. The maximum bit speed is 2 Mbps. Since this receiver is much

more expensive than the previous receivers it is expected to perform better than the previous receivers. While this study focuses heavily on performance under broadband noise, most typical operators will not experience the same conditions we're subjecting these receivers to. Rather, this 2 Mbps data rate provides significantly improved latency value. This results in a 'quicker' sUAS that responds to user controls much quicker. While this provides significantly less gain, it is assumed that the improvement to latency is more important than operability in RFI congestion to a typical user. There is a fundamental limitation described by Equation 5.2, where the data rate and gain are inversely proportional. Given a larger bandwidth, latency can be reduced without reducing processing gain, but this receiver operates within roughly the same bandwidth as the previous receivers. Therefore, we expect lower levels of total gain. The processing gain available from FHSS is calculated to be 13.8 dB with an additional antenna gain of 2 dB. The previous commercial receivers indicated FEC in the form of coding, however, there is no direct evidence this receiver utilized FEC. Some form of coding is likely utilized, therefore it is expected that the receiver will outperform the estimated probability of bit error given the total gain calculation. Since the previous FEC improvement was estimated to be up to 3 dB, this same value is applied to this model.

5.2.5 Identification of C2 Radio Categories

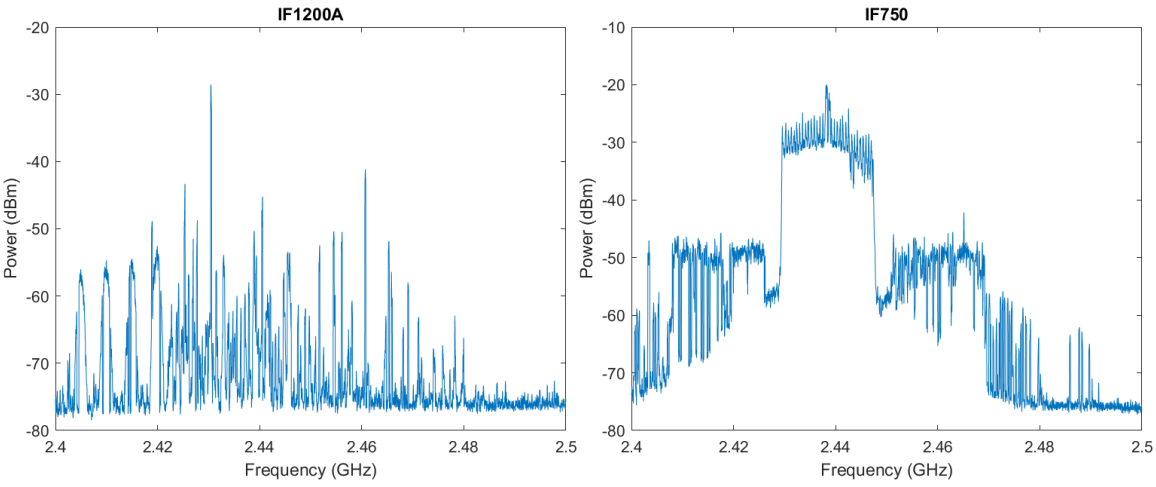
The results of the initial SNR measurements initiated an investigation to identify frequency spread spectrum techniques used by the controller receiver pair for each drone. The drones were placed independently in the large anechoic chamber with an established C2 link to identify the particular technique. A Signal Hound USB-SA124B spectrum analyzer was mounted to each drone to record the frequency spectrum from 2.4 to 2.5 GHz. An identical monopole antenna utilized for the IF1200A drone C2 link was used on the spectrum analyzer to collect the data over several minutes. Figure

5.10 shows the average maximum value recorded by the spectrum analyzer over several minutes. The sample rate selected for the spectrum analyzer is approximately 1 Hz (the frequency range is scanned each second). The results show apparent different behaviors of the spread spectrum radios for the two drone platforms.



(a) (b)

Figure 5.9: Lab-measured signal spectrum examples for the two types of spread spectrum radios using SDR emulator and testbed. (a) FHSS example. (b) DSSS example.



(a) (b)

Figure 5.10: The measured C2 radio spectrum under normal conditions (lab environment and no RFI) for the UAS systems, (a) IF1200A C2 link (b) IF750 C2 link.

When compared to the Figure 5.10 presented by Segers et al. [14], as well as the spectrums measured using the SDR testbed (Figure 5.9, it is evident that the IF1200A and IF750 are utilizing two distinct spread spectrum techniques. The received power recorded for the IF1200A reaches a consistent peak defined by the first three frequency "hop" humps at -55dBm. Meanwhile, the IF750 testing provides evidence of a much higher transmit power level based on the spectrum peak power levels near -30 dBm. This measurement indicates that the noise floor level required for jamming the IF750 is slightly higher than that of the IF1200A.

5.2.6 EMI/Jamming Test Setup

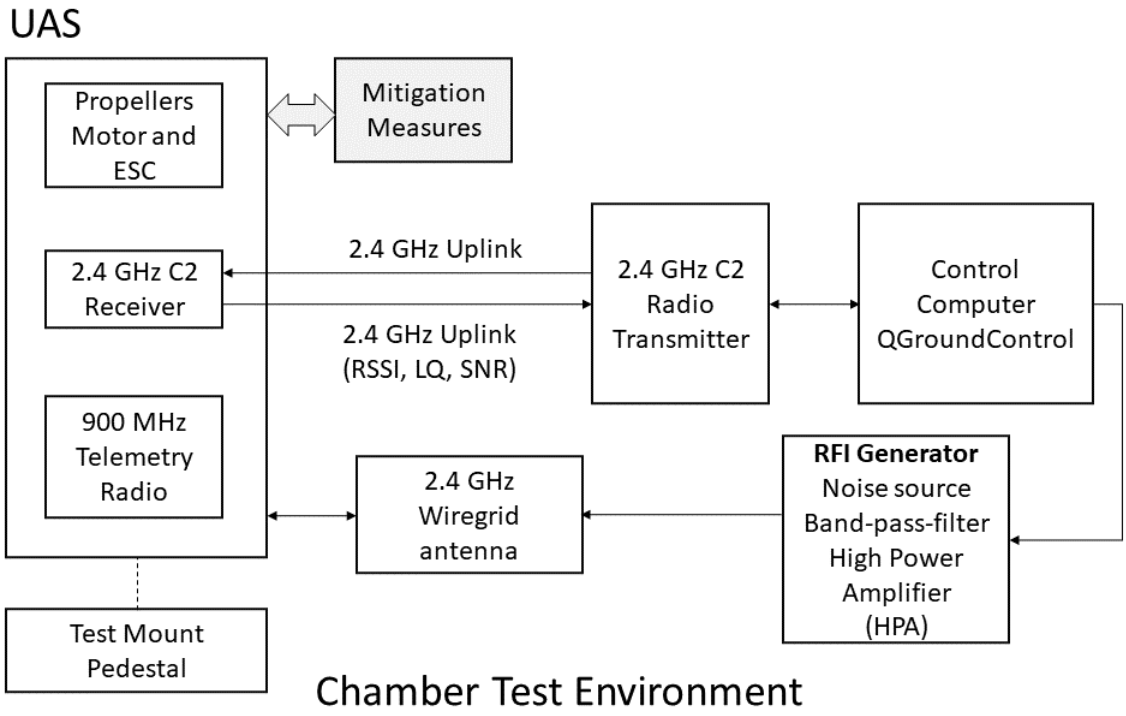


Figure 5.11: Initial laboratory diagram test set up for Inspired Flight sUAS. Slight variation exist between the IF750 and IF1200A, with a particular difference being the presence of a 900 MHz telemetry radio for the IF1200A sUAS.

The setup in Figure 5.11 shows a basic reference laboratory test system that uses a noise source to emulate the RFI/HIRF radiation power source. The figure shows the typical C2 Jamming hardware set up referenced throughout the study. While the diagram explicitly explains the IF1200A system, the IF750, and other commercially available radios operate similarly. The main difference is the presence of an additional 900 MHz telemetry radio that serves as a redundant C2 link for long-range operations.

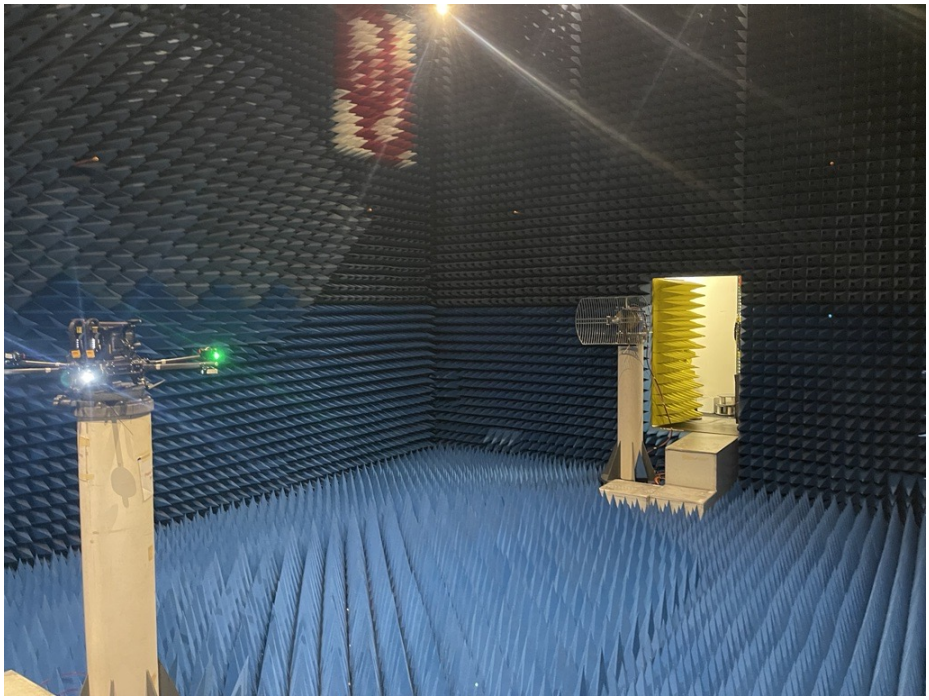


Figure 5.12: Anechoic chamber setup for RFI lab test using commercial sUAS devices.

Figure 5.12 displays the general test setup using commercial radios (which in this example was also mounted into an airframe) and a 2.4 GHz wire grid antenna for the RFI transmission. In this test set up the sUAS under test is placed on the DUT pedestal (near-side) in a large anechoic chamber. The transmitting antenna is mounted on the AUT pedestal (Far-side). The RFI generator is placed on a cart outside of the chamber and connected to the wire-grid antenna. The door is closed as far as possible to reduce the amount of external interference. While this setup permits some Wi-Fi and other external noise to penetrate the chamber, it reduces

it significantly and effectively mitigates electromagnetic interference (EMI) from the noise generator itself.

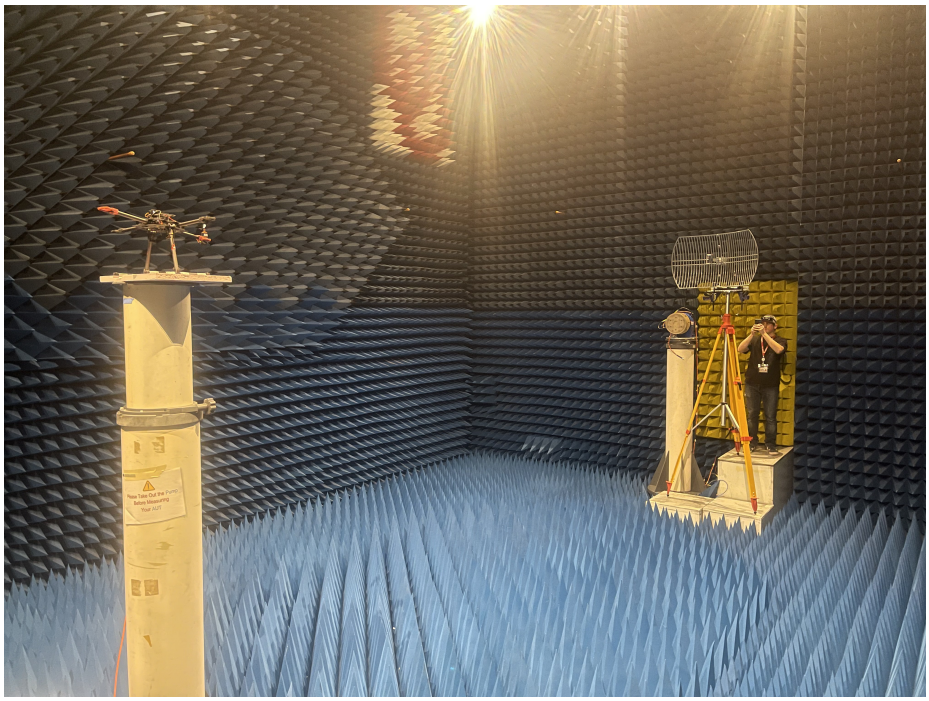


Figure 5.13: Anechoic chamber setup for RFI lab test using commercial radio devices utilizing a model sUAS structure for elevation and emulating reflection and interference from the frame.

The Figure 5.13 is very similar to the setup displayed in Figure 5.12, where instead of using the AUT (Far side) pedestal to mount the wiregrid antenna, the antenna is mounted on an adjustable tripod.

5.2.7 Software-Defined Radio/SDR

The lack of quantitative data logged from commercial small UAV receiver's data transmission necessitates emulating said C2 link to acquire more adequate data concerning the number of bits maintained in a "Jammed" environment. Utilizing a software-defined radio (SDR) for testing and evaluation significantly improves the

quality of data obtained. A sufficiently robust SDR can flexibly implement different modulation schemes and communication protocols. This will allow for a more rigorous investigation of multiple types of communication protocols. Compared to commercially available transceiver/receiver pairs, SDRs are "transparent and fully controlled". This study uses ADALM-PLUTO SDR to facilitate the emulation of basic modulation schemes and spread spectrum techniques. A primary focus is placed on emulating and analyzing BPSK modulation with direct spread sequence spread spectrum at the ISM band beginning at 2.4 GHz. Additional verification and testing of the effects of RFI/EMI was performed for this simulation. The detailed setup of the SDR emulation testbed is shown in the following Figure 5.14.

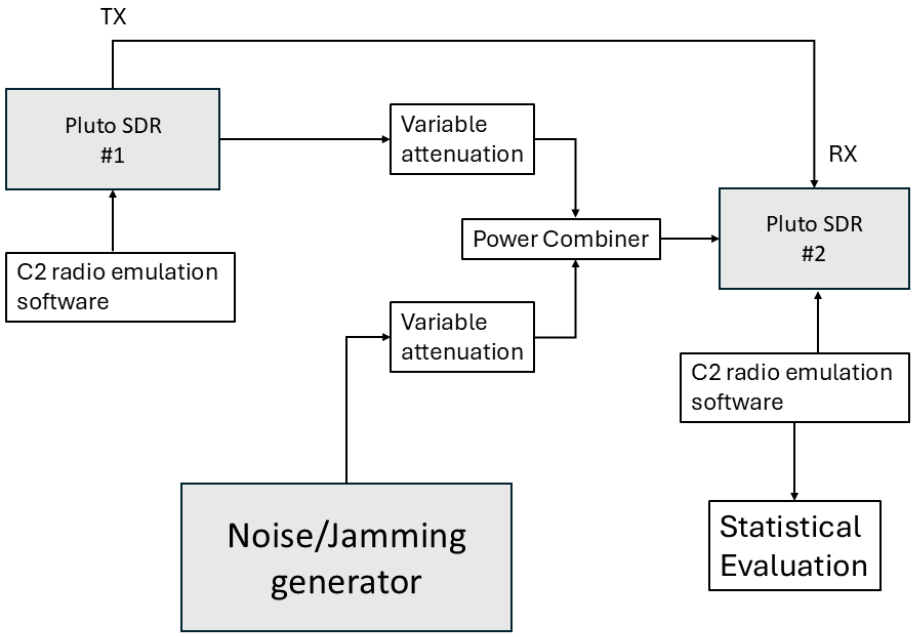


Figure 5.14: Example of RSSI measurements vs TX noise power levels.

Communication protocols used in UAS are often proprietary. The exact chip rate, bit rate, sample rate, and spreading code are not shared by the manufacturer to protect the reproducibility of their device. The characteristics of the DSSS signal produced by the SDR is constructed according to the following specifications. The

parameters used for the PlutoSDR emulation tests are described in Table 5.7. A typical commercial C2 radio operating with a direct spread spectrum technique and BPSK operating in the 2.4 GHz ISM band is emulated, where the parameters are tuned to the extent of the SDR used for analysis.

Table 5.7: DSSS Parameters for PLUTOSDR Emulations

Parameter	**Value**
Chip Rate	8 Kbps
Bit Rate	1 kbps
Sample Rate	8 Mbps
Spreading Code Length	16 chips
Number of Bits Tested	$\geq$ 100,000
Spreading Factor (Chips per Bit)	16

A typical DSSS technique using BPSK defined by IEEE 802.11 [30] will use a 1 or 2 MHz, however, a typical commercial radio will utilize hardware designed to deal with higher data rates and will often include a data buffer. This hardware can allow for quicker modulation/demodulation as well as allow for higher data rates to be processed over time. The PLUTOSDR is limited first by the type of connection it utilizes with the PC and while the vast functionality of the SDR provides greater ability than a standard RF chip used in commercial radio, it lasts some of the hardware required to operate with higher data rates and over large bandwidth.

5.2.8 EMF probe

A Narda RadMan 2XT EMF probe is also utilized to characterize the electromagnetic field intensity of the transmitted jamming source. The Nardo 2XT probe is capable of detecting Electromagnetic field intensity from 1 MHz to 60 GHz [37]. This device,

shown in Figure 5.15, is designed to alert professional personnel of an occupation hazard defined by FCC-96-32A1-4 [38] based on the field intensity measurements.



Figure 5.15: Narda RadMan 2XT 2281/102 EMF meter.

This probe device records EMF data as a percentage of the values defined by the FCC standard. This device has an accuracy of $< 1\%$ of the occupational hazard standard defined by the FCC [37]. Therefore, the accuracy of the Narda RadMan 2XT EMF probe is $< 200\,\mathrm{V}^2/\mathrm{m}^2$ or < 14.14 V/m. This device will be used as a reference to provide validity to the EIRP calculations referenced throughout this study. A portion of the table used to define occupational hazard is displayed in Table 5.8.

Table 5.8: Electric and Magnetic Field Occupational Hazard Levels Defined for the Utilized Frequency Band

Frequency Range (MHz)	**Electric Field Strength** E^2 ($\mathrm{V}^2/\mathrm{m}^2$)	**Magnetic Field Strength** H^2 ($\mathrm{A}^2/\mathrm{m}^2$)	**Power Density (S)** E-field; H-field ($\mathrm{mW/cm}^2$)	**Averaging Time** (minutes)
1500-100,000	20,000	0.125	5.0	6

f = frequency in megahertz (MHz)
E^2 = electric field strength squared
H^2 = magnetic field strength squared
$\mathrm{V}^2/\mathrm{m}^2$ = volts squared per meter squared
$\mathrm{A}^2/\mathrm{m}^2$ = amperes squared per meter squared
$\mathrm{mW/cm}^2$ = milliwatts per centimeter squared

The probe was placed within the transmit antenna beam and set to record the electromagnetic fields' average, maximum, and minimum percentage values. This data is imported into MATLAB and converted to the RMS value's electric and magnetic field strength.

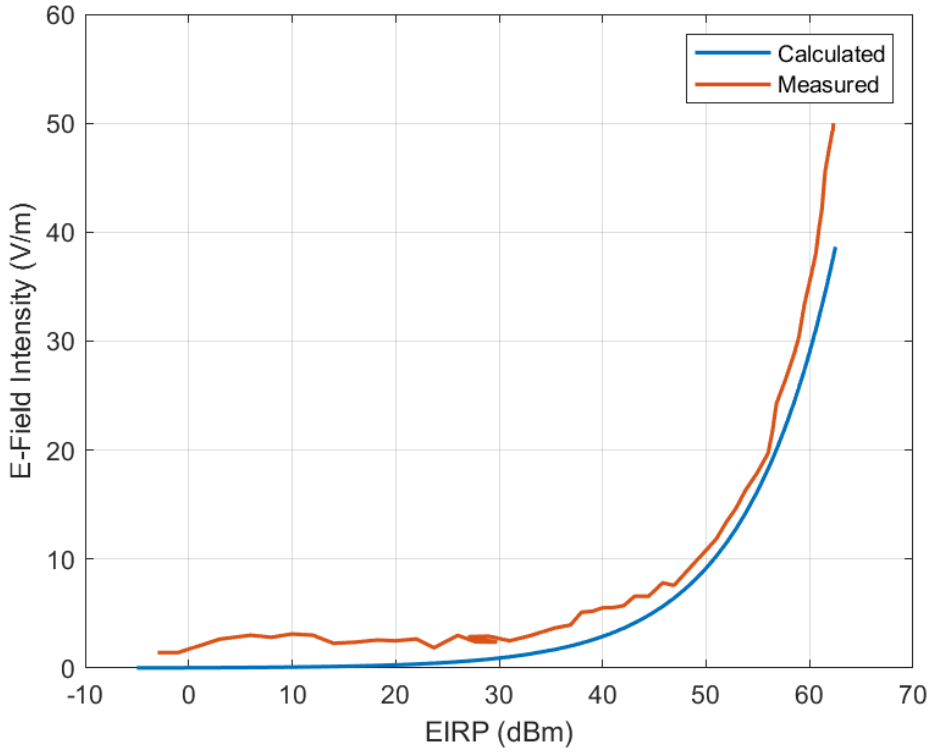


Figure 5.16: Narda RadMan 2XT 2281/102 EMF meter E-Field Measurements Compared to Electric Field Calculations using Equation 2.3.

Using the noise generator described in Section 5.2.1 together with the wire grid antenna, the electric and magnetic field values were measured with the Narda RadMan 2XT. The measured values are plotted in Figure 5.16, where the shape of the measured and calculated curve show strong agreement. The measured value of the electric field is consistently slightly higher than the estimated value. This results from out-of-band power propagating through the amplification chain. The EIRP only includes power from 2.4 GHz to 2.5 GHz, whereas it is understood that the true transmit power includes some density outside of the band of interest. Additionally, the Narda probe

provides less than 14.14 V/m's of accuracy. Some of the discrepancies between the measured and calculated electric field near the lower EIRP values can be attributed to the limitations of the probe accuracy. While the calculated and measured plots do not display exact values, the overall shape and trend are sufficient to provide the confidence we're measuring near values being transmitted.

5.2.9 EMF Probe Antenna and Orientation

In this study, the Narda RadMan 2XT personal EMF meter is utilized for electromagnetic field measurements. The use case for this device seems to make it an ideal selection for EMF measurements for this study. This device is intended as an isotropic receiver for personal protection in high-intensity electric and magnetic field environments. It is important to note that while this probe boasts an impressive isotropic sensor with a 0 to 60 GHz range of electromagnetic fields and total power, established antenna literature suggests that this claim warrants further investigation. In 1951 and 1954 Mathis argued that an antenna that radiates all polarizations in all directions is not feasible [39,40]. Later contributors to the field admit that under the strictest definition of isotropic, there is truth in Mathis' proof [41,42]. However, these authors argue to varying degrees, that an effectively isotropic antenna can be realized with the understanding that at some locations, the antenna will not transmit and receive all polarizations [41–43]. The wire grid antenna used in this study is linearly polarized. It can be inferred from the literature that despite the claims of an isotropic sensor, there is most certainly an orientation of the sensor that will receive less of the particular polarization from the transmitting antenna. Therefore it is important when orienting the antenna to consider the orientation that will most closely collect the energy transmitted. In this study, the process of orienting the probe is preceded by the placement of the transmitting antenna. For each test, the position and orientation of the transmit antenna were carefully maintained. The probe was then placed

on the pedestal and orientation was manually adjusted under low transmit power to determine the minimum and maximum values recorded by the probe. The orientation resulting in the maximum received power was used.

5.3 Field Tests and Experiments Setup

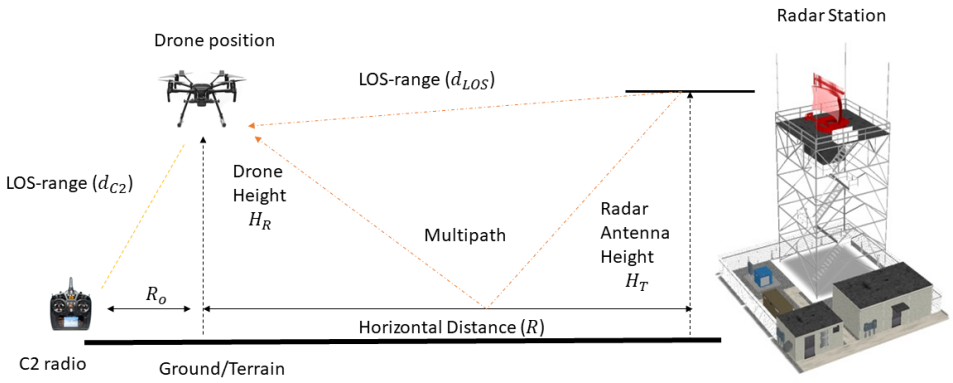


Figure 5.17: Field measurement geometry and link modeling parameters.

In the last step of the experiments, we operate the sUAS platforms near the FAA's ASR-11 radar site at the Oklahoma City facility, as shown in the following Figure 5.17. The facility also includes other ground navigational aid transmitters such as VOR and ILS (which are less of a concern in our study since the transmit power level is much lower). The key elements of an airport deployment geometry are the launch locations of the sUAS, the location of the facility (radar or ILS), and the altitude/distance of the UAS flight trajectory to the facilities. These elements are depicted in Figure 5.17 and Figure 5.18. Although these example test facilities are not actual airports, they are identical to the layouts of any general airport. They can be used as references for actual UAS launching and deployments.

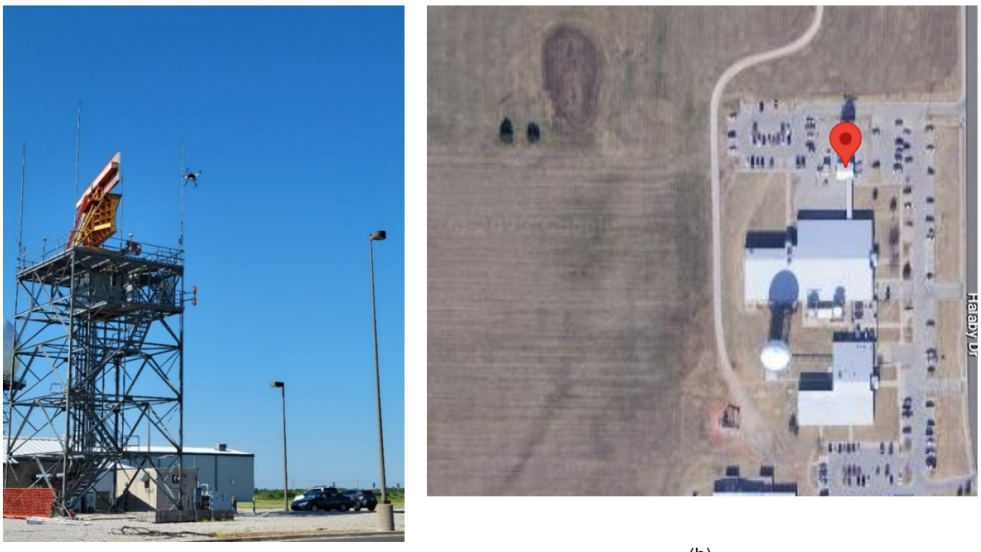


Figure 5.18: Field measurement sites (a) ASR-11 radar, (b) Google map site location.

The collection of flight test data using this geometry led to a detailed test data record, which will be provided in the next chapter. The most critical data from the flight tests is the deemed safe operation distances from each airport facility under the COA constraint of location and flight altitude ceiling. "safe distance" in these data means that the risks of loss of C2 links due to RFI/EMI are mitigated based on physical/ground operational distances from the specific facility. These safe distance data are essential for measuring and calibrating the overall risk factors of the C2 link, as discussed in Section 6.1. The safe distance results are compared with the theoretical link models using the model parameters listed in Figure 5.17.

Chapter 6

Results and Data Analysis

6.1 Results of Commercial C2 Radios on UAS

6.1.1 Jamming Test: SIR thresholds for C2 link loss

Initial investigations of the C2 link were performed on the two sUAS platforms using the experimental setups described in the previous chapters. Both sUAS's, described in Section 5.2, were analyzed under varying EIRP where all built-in telemetry data was logged via their respective flight controllers. Figure 6.1 displays the relationship between the signal-to-noise ratio values recorded with respect to the transmission power of noise. In this section, the two drone model analyses are compared. The IF750 drone's radio generally exhibits better resistance to EMI than the IF1200A's since the IF750 needs about 7 dB higher RFI power than 1200A to cause it to lose the radio link. The enhanced performance of the IF750 is probably due to the specific RF channel, the transmit power and receiver sensitivity for the sUAS, and the applied spread spectrum technique, as discussed in Section 5.1.

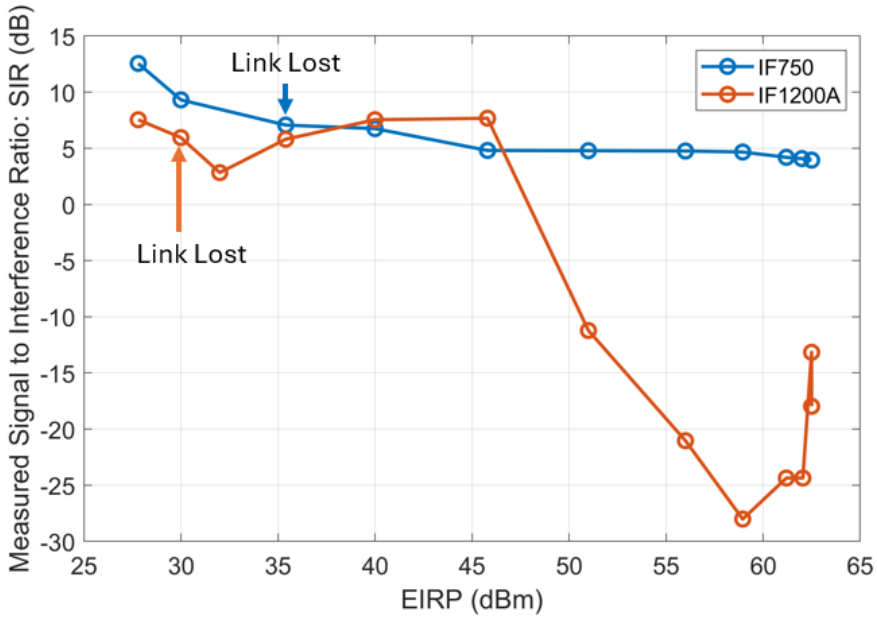


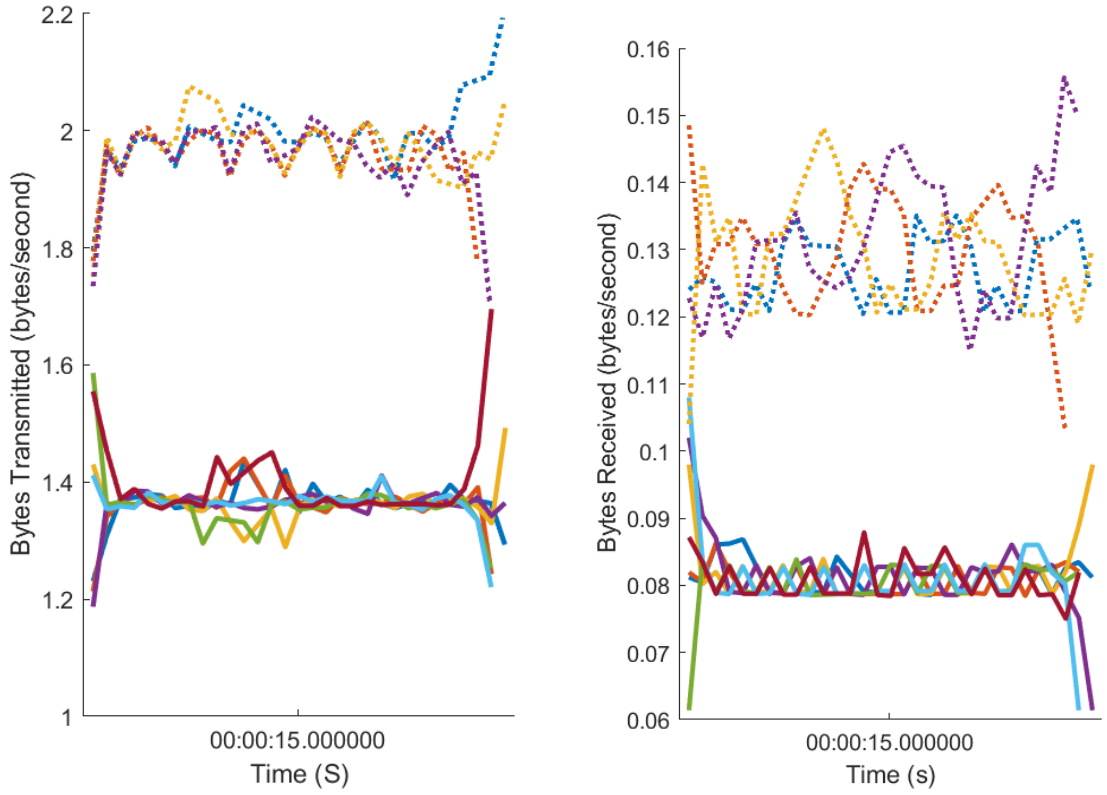
Figure 6.1: Relationship between the measured SIR and RFI EIRP for two commercially available sUAS (IF750 and IF1200A).

Figure 6.1 comprises 11 test cases (variations in attenuation) for the IF750 and 13 test cases (variations in attenuation) for the IF1200A case. The RSSI and noise values are recorded directly from the flight controller for each drone. SNR values are calculated by subtracting the noise from the RSSI value. The RSSI value should remain relatively consistent over each test as the strength of the C2 link signal is set, and transient behavior due to multi-path should be mitigated by using the anechoic chamber. This value is a more useful measurement when the distance between the transmitter and receiver is changed. The strange behavior of the SNR exhibited in the curve presented for the IF1200A sUAS is not fully understood. Despite the SNR recovering up to 7 dBm, the C2 link is not regained at EIRP values higher than 30 dBm. This is partly due to the variation in logged samples of RSSI and noise power level. The observation is consistent with the discussions in Section 5.2.3 since the measured spectrum features show that IF750 used DSSS. In contrast, 1200A used FHSS, and IF750 radio has a higher radio link transmitter power level. The curve

displaying the performance of the IF750 C2 link under broadband noise shown in Figure 6.1 fits the expected behavior of a receiver under increasing noise. The logged signal-to-interference ratio decreases as the transmitted EIRP increases. The IF750 on-board transceiver fails to maintain C2 link when it experiences an EIRP of about 35 dBm. The SNR value reported C2 link failure was

6.1.2 Throughput Under Jamming/RFI

As discussed in Section 3.2.2.2, C2 radio link throughput is affected by the RFI/EMI power levels. The measurement results presented here are based only on the measurements of the IF750 radio since they are more representative.



(a) (b)

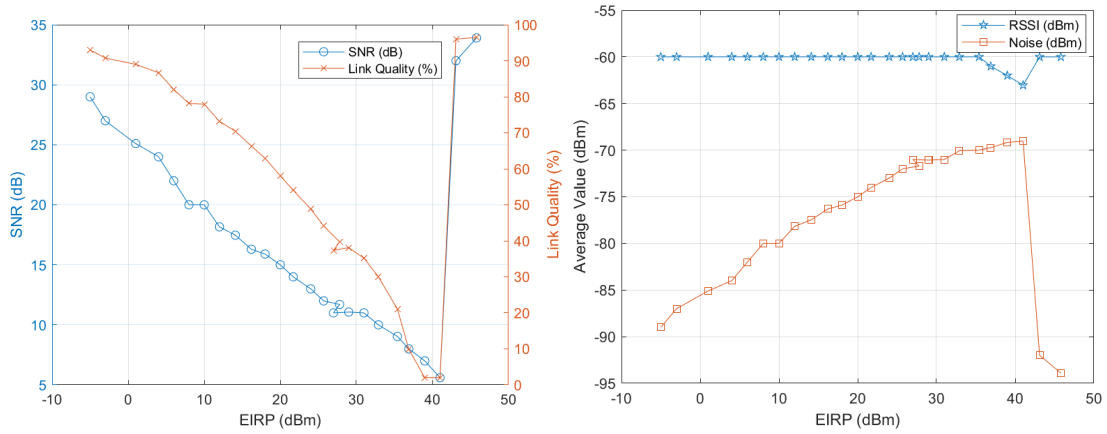
Figure 6.2: Transmit and Receive throughput of the IF750 drone under varying RFI EIRP levels.

Figure 6.2 shows the data rates achieved from both the transmit and receive sides. The reported and logged values show variations in the transmit and receive rates as the EIRP changes. Unfortunately, it was found that most commercial C2 radios do not record precise and quantitative values. On the other hand, both the transmit and receive throughput have two distinct levels. One level is when the C2 link is normal (2 bytes/sec for TX and 0.13 byte/sec for RX), and another level is when the C2 link is disrupted (1.4 bytes/sec for TX and 0.08 type/sec for RX), regardless of the RFI power levels. This is consistent with the observations of the simplified model behaviors described in Section 3.2.2.2 (equation 3.14).

6.2 Other Commercial C2 Radios: Result and Discussion

6.2.1 FS-IA6B Telemetry

The specific telemetry recording values for FS-IA6B are described in detail in Section 5.2.3, which includes SNR, LQ, RSSI, and Noise Level. In Figure 6.3, the results of the jamming test performed in the large anechoic chamber described in Section 5.2.6 are plotted. The simplified model can fit the SNR and link quality (equation 3.13) behaviors. However, both show abrupt and unexpected increases as RFI power (or EIRP) exceeds the 40 dBm threshold. This is because when the loss of a C2 link occurs, the radio log readings become unreliable. Similar behavior happens to the noise power level, consistent with the increase of RFI EIRP. The recorded RSSI level is stable when the radio link is normal, which is expected, but it is completely disrupted at the 40 dBm threshold. The trends are consistent with the simplified link quality behavior models discussed in Chapter 5.



(a) (b)

Figure 6.3: Telemetry data logged from FS-iA6B receiver using TX-16S Transmitter (a) Link Quality and SNR (b) RSSI and noise in dBm, calibrated by a factor of 135 for transmitter offset.

RSSI displays a constant value of -60 dBm over the range of EIRP values. Meanwhile, the noise value increases from nearly -90 dBm to -69 dBm. The SNR value follows an inverse relationship with noise value, where a received SNR value of > 30 dB is present when no noise is transmitted. When the transmitted EIRP value is greater than 40 dBm, the logging of telemetry values is unavailable. The RSSI is only available from the A7105 RF chip in the FS-iA6B when at least one frame is captured [44], otherwise, the value recorded before the loss of C2 link is maintained. Therefore, at an EIRP of greater than 40 dBm, it is understood that no frames are received and correctly demodulated. Meanwhile, some frames are correctly captured at the point of C2 link loss (27 dBm EIRP), but not enough to keep the C2 link maintained. These results provide additional insight into the operations of the receiver under varying levels of broad-band AWGN. Further comparisons to analytical models are presented in Section 6.2.3.

6.2.2 Jamming Test: EM Field Strength Thresholds

Section 1.2 has introduced a preliminary electric field threshold of 10 V/m for general UAV safety. The measurement results using the Narda field strength meter (Section 5.2.6) here show that the electric field strength is capable of significant disruption, and the specific threshold levels would depend on the particular radio products and test environment setup. The general behavior model discussion in Section 3.2.2.2 and the relationship between E field strength and EIRP (Section 2.1.2.2) are compared/evaluated here for reference.

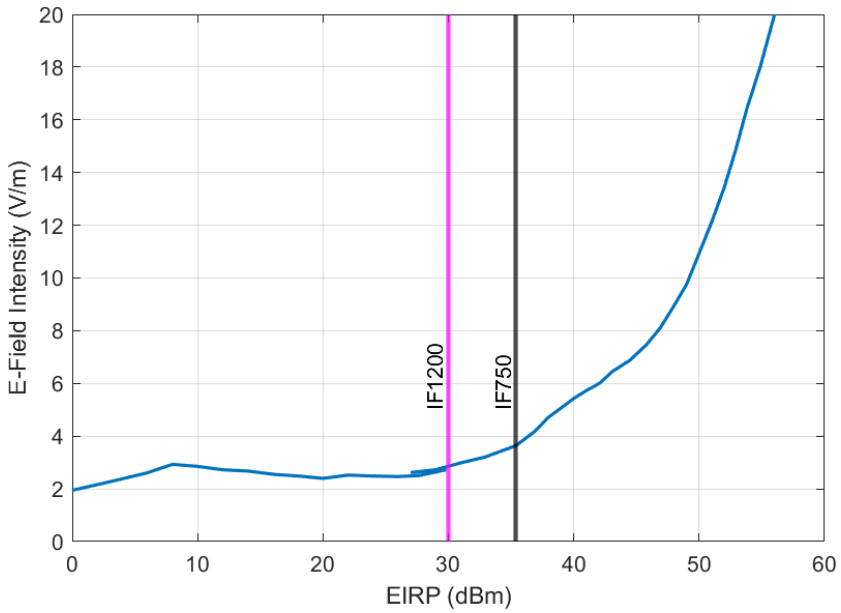


Figure 6.4: Measured E-field strength levels needed to disable the C2 links for IF750 and IF1200A UAS.

Figure 6.4 shows the measured loss-of C2 link thresholds for the two UAS platforms under test (IF750 and IF1200A), based on the threshold EIRP of the RFI emulator (x-axis) and the measured E-field intensity values (y-axis). It shows that IF750 requires higher RFI power and E-field intensity to cause loss of the C2 links, and the E-field intensity thresholds are lower than the nominal model in previous chapters.

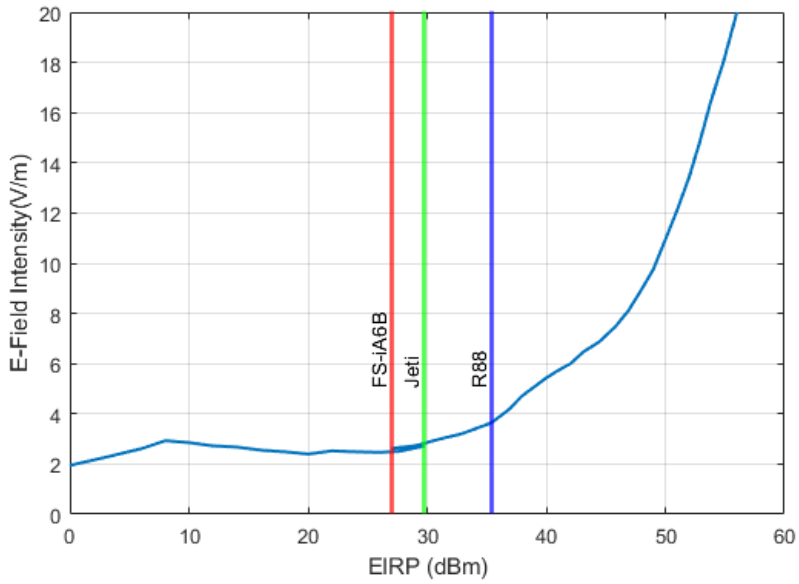


Figure 6.5: Measured E-field strength vs EIRP for testing with commercial radios, the thresholds of loss of radio link are marked.

In Figure 6.5, the EIRP value resulting in the disabling of the three tested commercial radios is shown on a cropped plot, showing the EIRP and E-field value at which the C2 link for each radio was lost. The IF-i6AB displayed the most significant degree of susceptibility to in-band interference from RFI, followed closely by the Jeti receiver at close to 30 dBm EIRP and an electric field strength of 2.8 V/m. The Radiomaster R88 performs the best in in-band RFI, with the C2 link sustained until the EIRP reaches 35.4 dBm and the E-field strength of 3.6 V/m. These electric field intensity values are far below the standards asserted in previous sections. This indicates that while the electric field strength can indicate frequency-independent power in the environment, sufficient power in the band of operations can disrupt communications despite falling below the 10 V/m range. A more detailed comparisons of this result for different commercial radios are summarized in the following Table 6.1. The results show that different commercial radios have different loss of link threshold

levels, while the RadioMaster R88 V2.0 8ch SFHSS radio seems to be the most robust under broadband radio-frequency interference.

Table 6.1: Measured loss of link threshold conditions of the commercial radios (including the radios on UAS) based on the RFI noise EIRP and the E-field intensity.

Receiver	**EIRP (dBm)**	**Calculated E-Field Intensity (V/m)**	**Measured E-Field Intensity (V/m)**
FS-iA6B	27	0.65	2.5
Jeti Duplex REX12	30	0.92	2.8
IF1200A	30	0.92	2.8
IF750	35.4	1.71	3.6
R88	35.4	1.71	3.6

Table 6.1 displays the 5 systems under test in this study as a function of EIRP in dBm. Each receiver experiences the full range of RFI. As previously discussed, the FS-iA6B has a threshold of 27 dBm indicating the receiver loses link at a relatively lower RFI power. Meanwhile, R88 and IF750 exhibit the highest EIRP threshold of 35.4 dBm, indicating these receivers are more resilient under RFI. The calculated electric field intensity is used as a reference for calibrating power experienced by the receiver at a distance of 6.223 meters.

6.2.3 Modeling Results

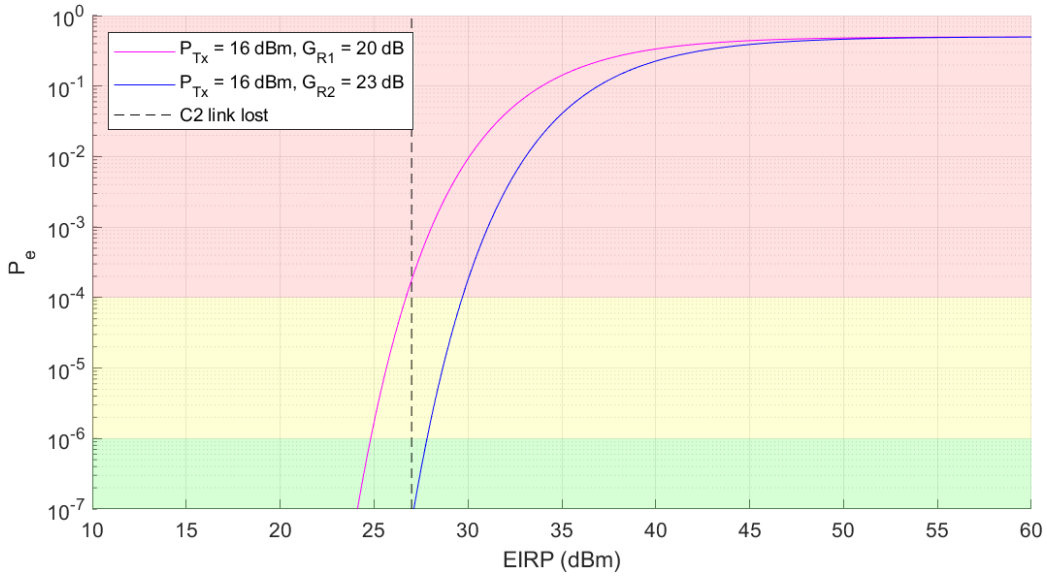


Figure 6.6: FHSS-FSK Modeling with parameters for FS-iA6B components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (16 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 500 kbaud (using binary-GFSK, which results in a bit rate of 500 kbits/second) and a 500 kHz channel bandwidth. The gain for both curves is calculated to be between 20 to 23 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB.

The results of the jamming test displayed in Figure 6.6 show the point of C2 link jamming as a function of EIRP. Since the radio does not provide BER data logging, this model provides a reference for BER required for effective communication between the receiver on the sUAS and ground station control. The two curves plotted in this figure represent an estimated transmit power for the handheld transceiver. This Figure utilizes the Equation 3.3, instead of plotting over jamming to signal ratio (JSR) the Figure is plotted as a function of EIRP used for testing. As reported in

Section 5.2.3 the maximum transmit power of the TX-16S is 250 mW or 24 dBm with an additional 2 dB of antenna gain, where transmit power may be lower depending on the RF protocol used or regional regulations. However, the transmit power for this device is dependent on the communication protocol. FCC records for the intended transmitter indicate that the maximum transmit power for the FS-i6X is 16 dBm. The two transmitters use the same A7105 RF chip set. Therefore in this model, it is assumed that the transmit power is 16 dBm. Therefore, curve P_{TX}, G_{R1} represents the lower bound of transmit power and P_{TX}, G_{R2} represents the upper bound. Since the hardware is set in this case, it is assumed that the Hamming (7,4) code used for FS-iA6b using A7105 chipset will improve the BER slightly, represented by 3 dB. In Figure 6.6, the point of C2 link loss falls between the upper and lower bounds of curves defined by the pink and blue curves. This indicates that the EIRP of the transmitter is likely bounded by the two curves where transmitter power, processing gain, and coding gain are used to estimate the probability of bit error. As described in Section 3.2, it is expected that the C2 link will be certainly lost given a BER of 10^{-4}, and the C2 link is susceptible to failure in the range of 10^{-4} to 10^{-6}. A majority of the area bounded by both curve falls within this range, suggesting that the estimated values for this model describing the behavior of the FS-iA6B under BBN are fairly accurate. It is likely that the true EIRP of the transmitter in this case falls somewhere in between the two curves, falling closer to the lower bound represented by the curve indicated by P_{TX}, G_{R1}.

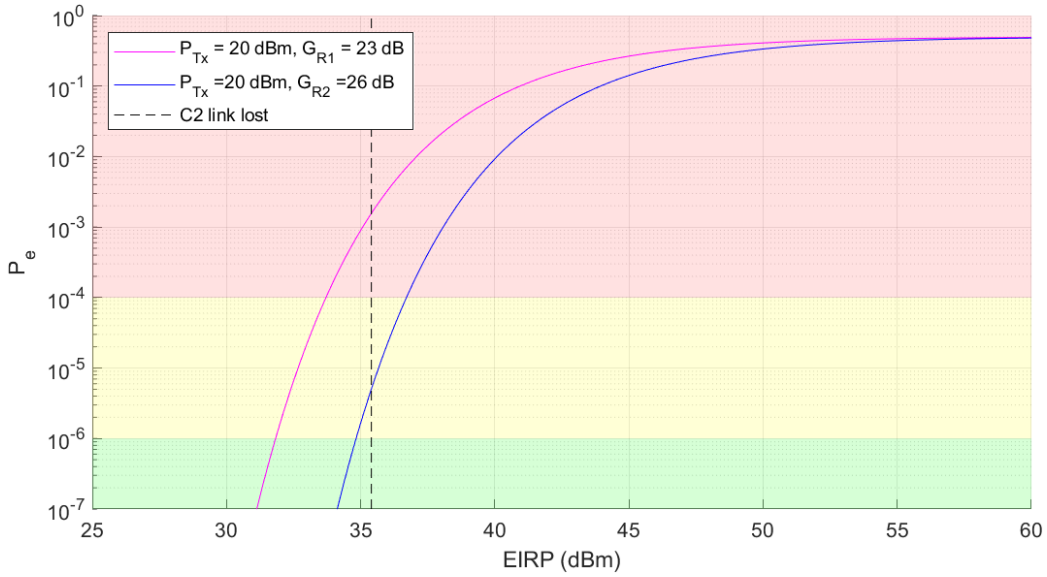


Figure 6.7: FHSS-FSK Modeling with parameters for R88 components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (20 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 250 kbaud (using binary-GFSK, which results in a bit rate of 250 kbits/second) and a 500 KHz channel bandwidth. The gain for both curves is calculated to be between 23 to 26 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB.

Figure 6.7 displays the modeled behavior of the R88 receiver under broadband noise where it is assumed a transmit power of 20 dBm and gain is estimated to be between 23 to 26 dB including antenna gain, processing gain, and coding gain. The rationale for these values is fully explored in Section 5.2.4. The C2 link was recorded to present loss when exposed to an EIRP of 35.4 dBm. This value falls within the middle area bound by the upper limit (defined by a transmit power of 20 dBm, with a total gain of 26 dB) and the lower bound (defined by a transmit power of 20 dBm, with an additional gain of 23 dB). The improved processing gain for this case can be

attributed to the lower bit rate, which improves the processing gain proportionally. This D8 protocol provides a greater degree of latency but improves the operability of the receiver under noise significantly. The true curve describing the bit error rate of this receiver likely falls pretty much in the middle of the upper and lower bound. If the lower bound were correct, the link would be lost at a bit error rate of about $10^{-}3$, which would be quite low for sensitive communications like command and control. Alternatively, the upper bound signifies a bit error rate of roughly $10^{-}5$, which is likely within the realm of sufficient communication such that the C2 link would be expected to operate.

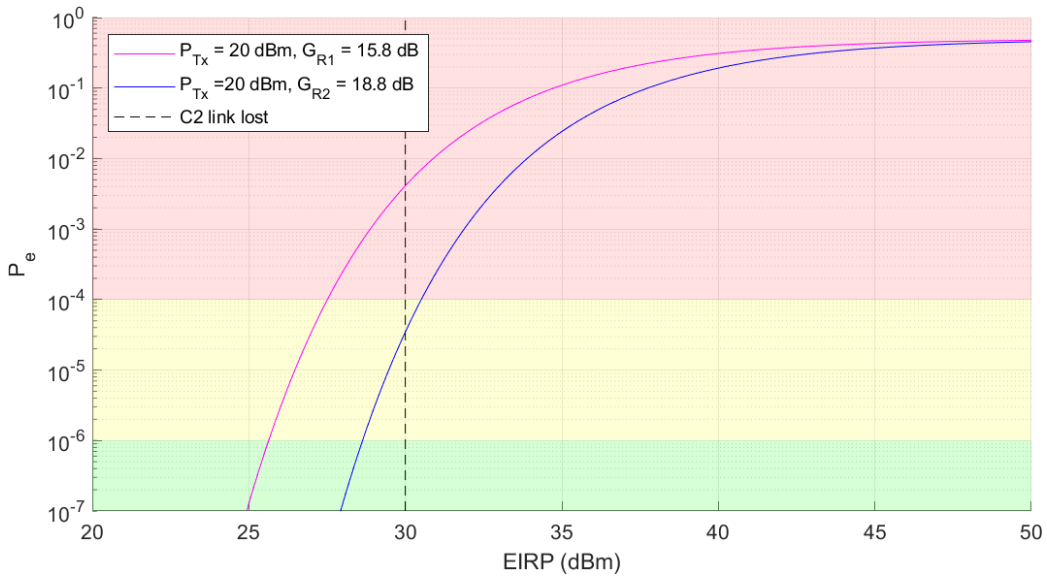


Figure 6.8: FHSS-FSK Modeling with parameters for R88 components. Noise power is modeled as -80 dBm, and an upper and lower receive power value is modeled (20 dBm). Jamming power is selected from the range of tested power levels. These setups are implemented over the testing chamber at a distance of 6.223 meters. Processing gain from the receiver is calculated by using a baud rate of 2 Mbps and a 48 MHz spread bandwidth. The gain for both curves is calculated to be between 15.8 to 18.8 dB. Forward-error correction codes are used for the device, and its effects are included in the gain curve as 3 dB.

Figure 6.8 displays the modeled BER with corresponding highlighted regions correlating to the probability of bit error that is likely to harm the C2 link. This figure aligns well with the values acquired from the receiver data sheet as well as FCC filings for this device. In this plot, it is evident that a majority of the line intersecting the region bound by the upper and lower curves defined by gain values of 15.8 dB (lower) and 18.8 dB (upper) lies in the red highlighted region. While this indicates the C2 link is overcome with noise power, a genuine curve should fall right at the intersection between red and yellow at the probability of bit error of $10^{-}4$. This discrepancy between the modeled curve and the measured results is likely due to the inaccuracy of the spreading spectrum parameters. While the FCC filing for this device reports a maximum bit rate of 2 Mbps, likely, that the device does not utilize the full speed. Unfortunately, it is not possible to confirm without further physical investigation of this device as these values are proprietary. Still, this receiver does follow the trend established by the upper bounding curve. It is therefore likely, that the total gain including processing gain, antenna gain, and coding gain is closer to 18.8 dBm than 15.8 dBm.

6.3 SDR-Based Emulation Test Results

The PlutoSDR-based tests, with their setup described in Section 5.2.5, mainly focus on the bit-error-rate (BER) related measurements under different noise power levels (which are assumed to be combined noise and RFI power). This is because the SDR only has the physical layer of implementation but does not yet have the link and transport layers of implementation as a complete C2 radio. The measurement, however, is also affected by the basic radio protocol. Thus, the "bit difference" is considered a better metric than traditional BER in this test since the preamble detection is also a factor that has an impact. Nevertheless, the measurements provided

valuable verifications of the generic model behaviors regarding the spread spectrum techniques from the C2 radios.

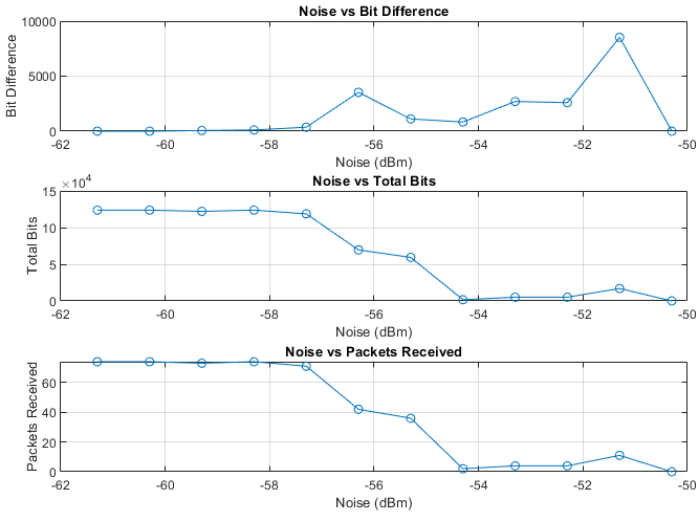


Figure 6.9: C2 link statistics emulation using Pluto SDR to emulate DSSS BPSK signal with 16 bit length pseudorandom spreading code.

Basic BPSK, DSSS, and FHSS schemes were tested using the SDR test radio based on the typical or assumed UAS C2 radio parameters. As an example, Figure 6.9 displays three critical parameters for characterizing the performance of DSSS signal transmission in the presence of broadband noise. This emulation test uses a shorter (16-bit) preamble for synchronization. This allows the receiver to identify the preamble quickly but increases the rate of falsely identifying a message. This configuration helps identify small bit differences (the number of erroneously received bits) and determine whether the signal is overcome with noise. The bit difference plotted over the noise shows an increasing difference between the number of transmitted and received bits as the noise levels increase. On the other hand, when the noise power is low, all 120,000 test-transmitting bits are received properly and correctly. Also, our radio test discards the entire message if at least 50 % of that message is not received.

As a result, when the noise power increases, the number of messages recognized reduces, limiting the number of data packets received. For instance, in the case of the -51.3 dBm noise power, 11 packets were received, which further affected the number of bits received. Still, the BER was found to be greater than 50 %, indicating that performance under this noise level follows the trend of increasing the BER as the noise power increases, regardless of the number of packets received, as predicted by the generic behavior models.

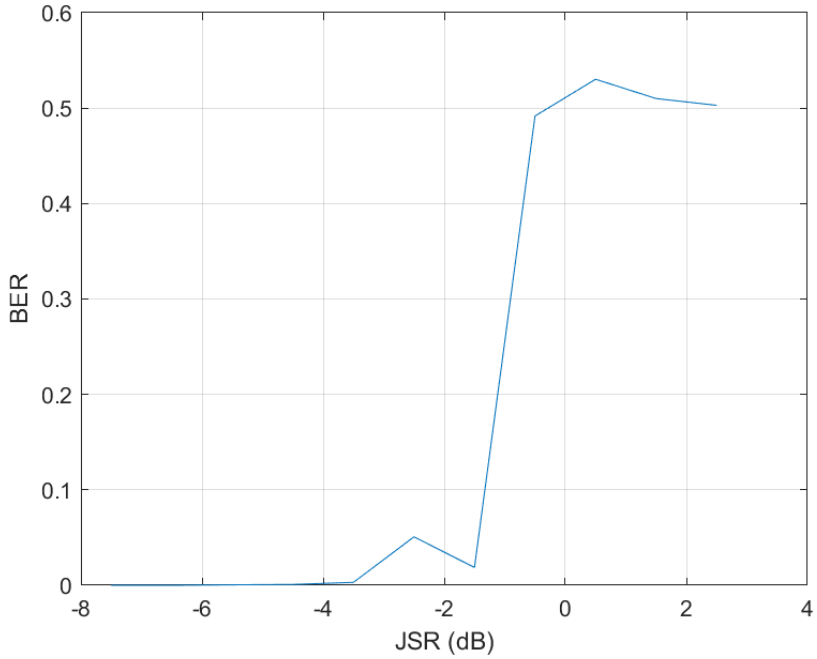


Figure 6.10: BER using Pluto SDR to emulate DSSS BPSK signal with 16 bit length pseudorandom spreading code.

The BER from this analysis is displayed in Figure 6.9 where the bit error rate is plotted as a function of JSR. In this plot, there is a sharp increase is BER as the JSR approaches zero. While this emulation encompass most of the physical layer of the communication protocol, the processing gain is not realized. This is an envelope detector is employed in the processing of the received signal. This throws away all phase information and relies entirely on the amplitude and total energy within a time period. Still some useful information does emerge. It can be stated that without the

additional processing or coding gain realized by commercial radio receivers, the SNR must be a positive value for the survival of a C2 link. In this case, when the JSR is -2 dB, SNR is 2 dB nearly all symbols are correctly demodulated. This displays the importance of proper implementation of spreading technique and provides evidence improvement due to processing and coding gain visualized in Section 6.2.3.

6.4 Field Operation Test Results: Summary

Field and flight tests are operational tests performed during August 2023. These tests focused mainly on loss-of-link conditions and safe operation distances from different RFI emitting sources. The FAA UAS operation group uses these data as a key reference for developing a safety management system (SMS) for sUAS operations within the airport areas. These modifications were made to the IF750 UAV, and testing was performed at the Mike Monroney Aeronautical Center in Oklahoma City. It is important to note that the electromagnetic environment around the MMAC is congested. Several ASRs, ILS, and other RFI sources operate in the area. While these flights performed on the first day are closest to an ASR-11, the effects of alternative RFI may still have an effect. Generally, these results are only for the high-level, qualitative evaluation of the specific UAS platform (IF750) used in the test and not for accurate model validation purposes. However, it does confirm the key behavior trends of the loss-link conditions.

6.4.1 Summary of Loss-Link Conditions

The modified drone with EMI mitigation was used for the first day of test flights. On this day, horizontal and vertical flight paths were manually performed. Observations of horizontal flight paths performed in front of the ASR-11 are listed in Table 6.2.

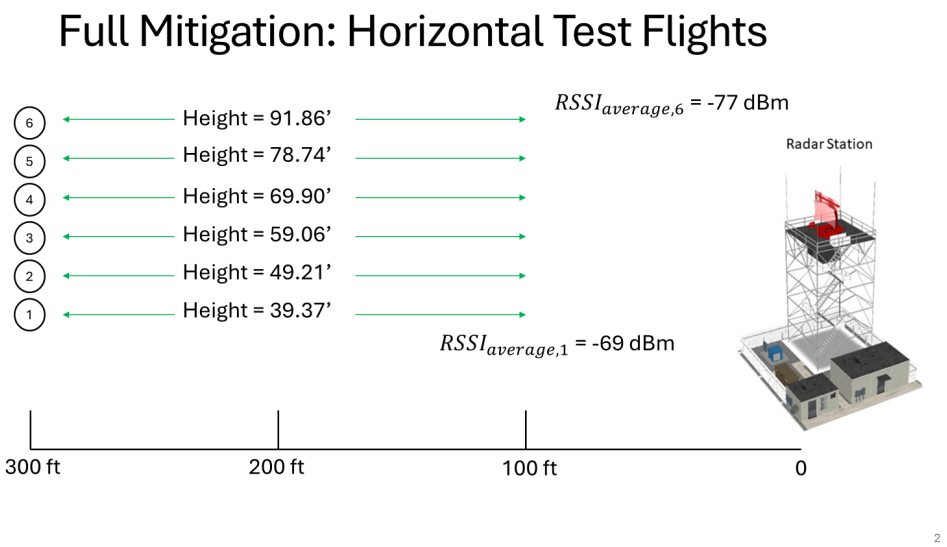


Figure 6.11: Diagram of Horizontal ASR Flights (Sweep between 300 ft to 100 ft in horizontal distance to the radar antenna), performed on Day 1: Level III mitigation is applied.

The first set of test were performed with horizontal flights where the individual flight paths are shown in Figure 6.11.

Table 6.2: Horizontal ASR Flights (Sweep between 300 ft to 100 ft in horizontal distance to the radar antenna), Day 1: Level III mitigation is applied.

Location	**RSSI Behavior**	**Drone Behavior**
39.37 ft height	-63 to -75 dBm	Normal, speed set 0.5 m/s actual about 0.7 m/s
49.21 ft height	NA	Normal
59.06 ft height	-69 to -73 dBm	Normal
68.90 ft height	-70 to -74 dBm	Normal
78.74 ft height	-69 to -76 dBm	Normal
91.86 ft height	-74 to -80 dBm	Small compass correction when near radar at 100 ft, but in normal control

The only issue observed during the test flight happened at a vertical height of 28 meters, while the UAV was 100 ft from the ASR-11. A minor compass correction occurred that was quickly reoriented. No loss of control occurred, and it is suspected that this was a small compass drift, which corrected itself quickly, indicating it was likely due to the magnetic field associated with the pulse of the ASR-11 being observed. With the mitigation modifications, there were no other observable issues with the test flights during horizontal scanning.

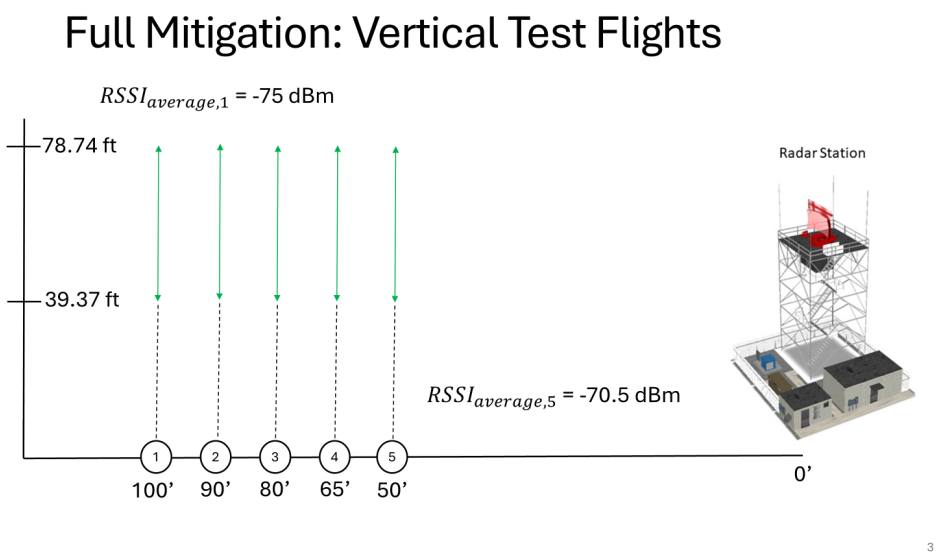


Figure 6.12: Vertical ASR-11 Flights (Between 39.37 and 78.74 feet) Day 1: Level III mitigation.

The verticle flights in-front of the ASR-11 are shown in Figure 6.12, where, average RSSI for the first and fifth flight are shown.

Table 6.3: Vertical ASR-11 Flights (Between 39.37 and 78.74 feet) Day 1: Level III mitigation.

Location	**RSSI Behavior**	**Drone Behavior**
100 ft to radar, 39.37 to 78.74 ft height	-71 to -79 dBm	Normal
90 ft to radar, 39.37 to 78.74 ft height	-70 to -71 dBm	Normal
80 ft to radar, 39.37 to 78.74 ft height	NA	Normal
65 ft to radar, 39.37 to 78.74 ft height	-69 to -73 dBm	Normal
50 ft to radar, 39.37 to 78.74 ft height	-61 to -80 dBm	Normal

As shown in Table 6.3, no C2 link disruption was observed during the vertical flight patterns in the beam of the ARS-11. However, UAS with and without shielding mitigation has significantly different minimal safety distances (no link loss) in these tests (Comparing to the detailed records in Tables 6.5 to 6.7). The observation of 'NA' in the third flight listed in Table 6.3 does not indicate an unacceptable RSSI value; rather, the value range was not noted for this particular flight.

Table 6.4: ASDE, TACAN Tower, ILS Site Flight Test Records Day 1: Level III mitigation.

Location	**RSSI Behavior**	**Drone Behavior**
ASDE-3 (1.2 KW), 50 ft to radar, 16.4 to 78.74 ft height	-58 to -73 dBm	Normal
ASDE-X (150 watts), 50 ft to radar, 16.4 to 78.74 ft height	-68 to -77 dBm	Normal
South of TACAN tower, 50 ft to the tower, ground to 120 ft height (with Will-Rogers ASR operating at distance, backside of LOC array)	-62 to -77 dBm	Normal
North of ILS site with all ILS TX turned on, in the middle of the LOC array, ground to 120 ft in height, the operator on the small road	-72 to -80 dBm	Drone had some circling behavior at about 32.81 ft

Additional flights with level III mitigation applied were performed around 4 additional sites. These sites include the ASDE-3 with can transmit up to 1.2 KW of power, ASDE-X with a maximum transmit power of 150 watts, TACAN tower, and just north of an ILS site. No significant disruptions were noted during these flights. While these systems are not the main focus of this study, their inclusion in the results serve to demonstrate the lack of error and interference during operations at the airport site, serving as an additional control for the removal of the mitigation methods applied for these test flights.

The mitigation modifications were removed over the evening in preparation for unmodified flight tests on the second day. The results are summarized below. Various loss-of-link situations were observed, and their RSSI values experienced large fluctuations.

Table 6.5: ILS, TACAN, LOC, ASDE Flight Test Record Day 2: No Mitigation (Removed shielding, filter) (Normal and hot weather, temp up to 100 F wind gust up to 10 mph)

Location	**RSSI Behavior**	**Drone Behavior**
South of ILS site, 50 ft to the emitters, flight 15 m up and down slowly (there was a truck onsite but no people)	Between -58 to -77 dBm observed	Normal
Launched 50 ft from the low-power TACAN (3 KW, 7.5 KHz) on the ground, 15 m up and down. Will-Rogers ASR radar operating from 340 yards away.	-52 to -76 dBm observed	Normal
Launched 50 ft distance from the center of LOC array, 15 m up and down. Will-Rogers ASR radar operating from 395 yards away.	-66 to -77 dBm	Similar to yesterday, saw minor circling behavior at about 5 m off the ground, circling stopped 0848, no other issue, believed not related to RFI. Overall, the C2 link is normal.
Launched 50 ft distance to ASDE-3, 2700 watts peak, ASDE-X off. 15 m up and down slowly	-64 to -75 dBm	Normal
Launched 50 ft distance from ASDE-X with ASDE-X off	-63 to -77 dBm	Normal

The results displayed in Table 6.5 are not particularly interesting. No serious RFI is expected throughout these flights. Still operating in the airport environment can be risky due to spurious emissions from various radars and communication stations. There were no incidents at the ILS site, TACAN¡ or ASDE sites. Some slight circling was noticed when flying at a distance of 50 ft from the LOC array. This is not an indication of strong RFI, rather it is believed that some EMI caused slight deviation in performance of the compass. Overall, there was no indication that the C2 link was harmed.

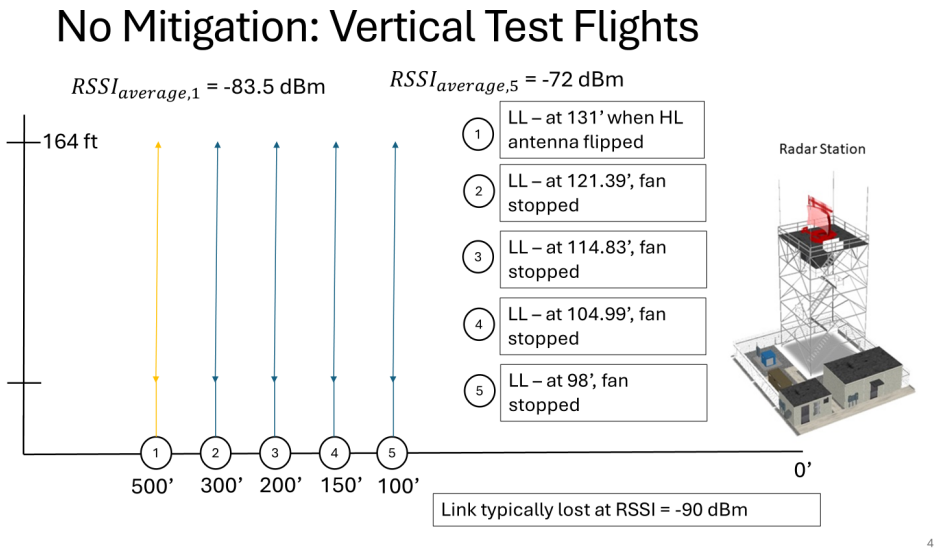


Figure 6.13: ASR 11 Flight Test Day 2: no mitigation (Various Relaunch Heights)

In Figure 6.13 the flight path used on the second day to determine safe flight distances with no mitigation applied from the ASR-11 are shown.

Table 6.6: ASR 11 Flight Test Day 2: no mitigation (Various Relaunch Heights)

Location	**RSSI Behavior**	**Drone Behavior**
Launched 100 ft from ASR, planned 164.04 ft up and down slowly	-59 to -85 dBm, RSSI about -90 dBm when loss of link	Lost C2 link at 98.43 ft, switched to RTH mode, regained control at 108.27 ft and 10 ft height, gradually and manually landed safely. The flight controller fan stopped during the flight.
Launched 150 ft from ASR, 164.04 ft up and down. Fan turned on when launching	-65 to -88 dBm	Lost C2 link at 104.99 ft height, switched to RTH. Manually landed. Fan off again
Launched 200 ft from ASR, 164.04 ft up and down, Fan turned on when launching	-60 to -90 dBm	Lost C2 link at 114.83 ft height, RSSI about -90 dBm at that point, manually landed, fan OFF again
Launched 300 ft from ASR, 164.04 ft up and down, Fan turned on when launching	-70 to -90 dBm	Lost C2 link at 121.39 ft height, RSSI about -90 dBm at that point, manually landed, fan OFF again
Launched 500 ft from ASR, 164.04 ft up and down, Fan turned on when launching	-74 to -93 dBm to -78 dBm when losing C2 link	Never lose C2 link at 500 ft distance. Then we tried (1) flip Herlinz TX antenna to horizontal polarization, which leads to 10 dB increase in RSSI reading. (2) Flipped horizontal toward ASR at about 131.23 ft height, we lost the C2 link and stopped at between 300 and 400 ft range (with radio antennas laying horizontally).

The flight test's listed in Table 6.6 describe the second day of testing where all mitigatio methods were removed. From launch distances 100ft to 300 ft from the ASR-11, link was lost when the sUAS entered the path of the beam. This is a stark difference from descriptions in Table 6.3. The vertical height is slightly higher in

this Table 6.6 as the antenna is angled up slightly, therefore at further distances the drone must travel higher to reach the beam path of the antenna. Still, the sUAS flights directly into the beam in both cases, where there is a significant loss of C2 link for all cases of flight until a distance of 500 ft is reached. This indicates that the additional band pass filters provide meaningful improvement to the C2 link when installed. Meanwhile, an internal fan experiences failure during flights within 300 ft to the radar. This phenomenon was not experienced the previous day when level II mitigation (shielding) is applied to the sUAS. This indicates that the shielding provides some additional RFI resilience for sensitive internal components.

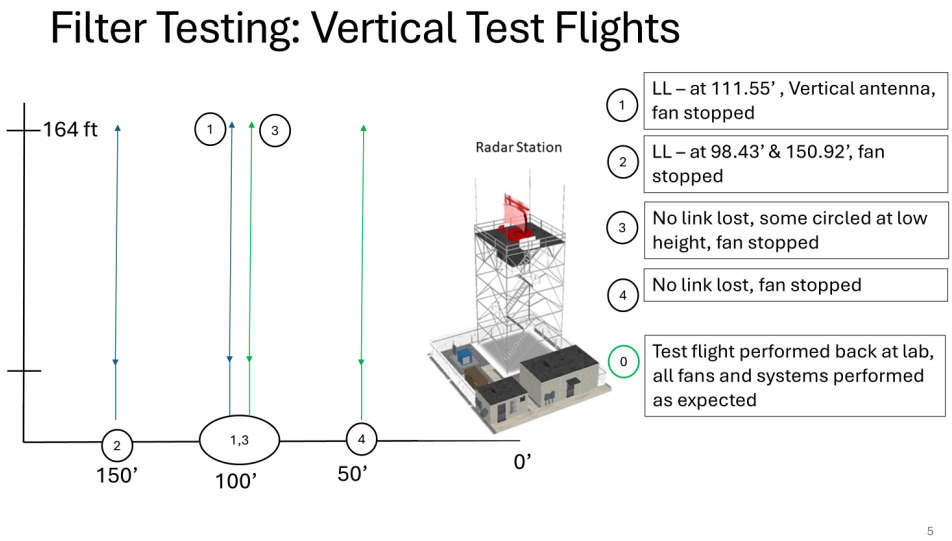


Figure 6.14: ASR 11 Flight Test Day 2: Testing EMI Filters (Additional Launch Heights)

Figure 6.14 displays the flight paths utilized to test the efficacy of the EMI filters.

Table 6.7: ASR 11 Flight Test Day 2: Testing EMI Filters (Additional Launch Heights)

Location	**RSSI Behavior**	**Drone Behavior**
Launched 100 ft ASR, Vertical Antenna Orientation, up and down 164.04 ft. Fan turned on when launching	-69 to -77 dBm	Lost C2 link at 111.55 ft height, RSSI about -76 dBm at that point, manually landed after RTH, fan OFF again and GPS recording stopped
Launched 200 ft from ASR, Horizontal Antenna Orientation. Up and down 164.04 ft	-67 to -90 dBm	Loss of C2 link occurred at two heights: 98.43 ft and 150.92 ft. RSSI was -79 dBm at 98.43 ft, and -86 dBm at 150.92 ft. Noticed that at 98.43 ft during ascending, there was no C2 loss due to ASR antenna pointing away, but when descending, the link was lost since ASR antenna was pointing to the drone now. Also hovered at 82.02 ft and 91.86 ft heights for 10 secs, no loss of links. Fan was again stopped during the flight.
Launched 100 ft from ASR. 164.04 ft vertical scan. 2.4 GHz ISM filters installed	-74 to -90 dBm	Minor circling behavior at a low height during the auto hovering at the beginning, then stopped quickly; all normal for the rest of the flights, NO C2 loss. Hovered at 46.33 ft and 32.81 ft heights each about 10 secs to confirm. Fan still stopped during flight.
Launched 50 ft from ASR. 164.04 ft vertical scan. With EMI filters added back into the system	-66 to -93 dBm	All normal and No C2 link loss. Fan still stopped during the flight.
Return to lab and launched test flights at campus east of RIL	NA	Verified that the fan operates normally, it was just temporarily disabled during the ASR flights.

In an effort to establish the improvements due to level II mitigation, the EMI filters were replaced on the sUAS utilized in Day 1 flight tests. The sUAS was then flown closer to the ASR-11 to establish if the filters affected the resilience of the C2 link. The first two flights listed in Table 6.7 did not include the the addition of the filters. As a result the C2 link as lost for both test flight when the sUAS entered the path of the beam. After the inclusion on the filters, the sUAS was flown at 100 ft and 50 ft with no C2 link loss. Indicating the effectiveness of the filters when operating in congested environments where the OOB emissions are expected to be near the operating frequency of the sUAS C2 link. While the addition of the filters improved C2 link maintenance, the internal cooling fan continued to terminate function during flight. This indicates that while the primary command and control link can be protected with the addition of band pass filters, sensitive internal components require additional shielding to protect from RFI/EMI in HIRF environments.

Chapter 7

Conclusion and Future Work

7.1 Summary of Contributions

This study opened the path to using a novel behavior modeling approach to evaluate and develop sUAS "EM-hardening" challenges. The main contribution is a collection of generic behavior models of the sUAS system and the radio link that can be applied to different vendors and platforms without needing specific proprietary information. To support this modeling effort, laboratory measurements and field experiments of the actual sUAS platforms were performed, and the data were analyzed. An SDR-based versatile testbed was also developed and used with the random-noise-based RFI/EMI emulator. Although it is difficult to obtain precise and quantitative verifications of the specific models, the overall trends of the measurement data and the behaviors are comparable. This study is the first time to characterize and record the "threshold levels" of RFI/EMI that disabled the C2 links of actual UAS platforms and verified that based on different classes and categories, the threshold levels vary depending on different commercial radio products. This study is also the first time, through actual flight tests in the airport facilities, that the proposed mitigation solutions (basic shielding and filtering) can effectively reduce the risks of loss of C2 links.

7.2 Future Work

Future work should include improvements in the generic C2 link radio models, improvements in laboratory measurement, and more rigorous field flight test verifications. Specifically, these would include:

- Improve the agnostic model for generic C2 link radio modules.
- Better theoretical modeling based on the most recent C2 radio technologies, including hybrid DSSS-FHSS communication protocols and more complex modulation techniques.
- Improved Bit Error Rate / Packet Error Rate testing for both common spreading techniques (FHSS & DSSS) as well as more advanced modulation schemes.
- More rigorous flight test operations at more representative field test sites and different UAV platforms. The current flight tests are limited based on the current FAA rules and restrictions. Following flight tests and measurements would provide further validation data to the continuously improved generic and behavior C2 link performance models with respect to more realistic airport facility emitter sources.
- Risk control and management system development. A safety Risk Management System (SMS) for UAS-based inspection is a critical goal of government agencies (such as the FAA). This work has contributed to this goal, but it will need more effort to be analyzed, tested, and verified until it becomes an operational standard.

References

[1] J. Y. N. Cho, "Asr-9 refractivity measurements using ground targets," Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, MA, USA, Project Report ATC-328, November 2006, prepared for the Federal Aviation Administration, Washington, D.C. [Online]. Available: https://www.ll.mit.edu/

[2] M. Lau, Y. Zhang, H. Suarez, R. Rucker, and S. Boyle, "Rf stealth for small uas: Characterization and evaluation of the impacts of rfi and rcs," in *Proceedings of the SPIE: Radar Sensor Technology XXVIII*, vol. 12535. SPIE, June 2023, p. 125350D, 11 pages.

[3] M. Lau, H. Suarez, Y. R. Zhang, and K. Reynolds, "Rf-hardening of small uas for mitigation of hirf impacts," in *Proceedings of Radar Sensor Technology XXVIII*. Orlando, FL, USA: SPIE, June 2024. [Online]. Available: https://www.researchgate.net/publication/381276891_RF-hardening_of_small_UAS_for_mitigation_of_HIRF_impacts

[4] M. A. Richards, *Fundamentals of radar signal processing*. Tata McGraw-Hill Education, 2005.

[5] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect your sky: A survey of counter unmanned aerial vehicle systems," *IEEE Access*, vol. 8, pp. 168 671–168 710, 2020.

[6] J. Wang, Y. Liu, and H. Song, "Counter-unmanned aircraft system(s) (c-uas): State of the art, challenges, and future trends," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 4–29, 2021.

[7] N. Souli, R. Makrigiorgis, A. Anastasiou, A. Zacharia, P. Petrides, A. Lazanas, P. Valianti, P. Kolios, and G. Ellinas, "Horizonblock: Implementation of an autonomous counter-drone system," in *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2020, pp. 398–404.

[8] J. Jang, M. Cho, J. Kim, D. Kim, and Y. Kim, "Paralyzing drones via emi signal injection on sensory communication channels," in *Network and Distributed System Security (NDSS) Symposium 2023*, San Diego, CA, USA, February 2023. [Online]. Available: https://dx.doi.org/10.14722/ndss.2023.24616

[9] O. Šimon, T. Götthans, and M. Popela, "Commercial uav jamming possibilities," in *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2022, pp. 1–6.

[10] J. David Lynch, *Introduction to RF Stealth*. SciTech Publishing Inc., 2004.

[11] R. J. Perez, *Handbook of Aerospace Electromagnetic Compatibility*. Wiley-IEEE Press, 2018.

[12] T. U. of North Dakota, T. U. of Kansas, and D. University, "Evaluate unmanned aircraft systems (uas) electromagnetic interference (emi) final report," The University of North Dakota, The University of Kansas, Drexel University, 243 Centennial Drive, Stop 7165, Grand Forks, ND 58201; 2335 Irving Hill Road, Lawrence, KS 66045; 3141 Chestnut Street, Philadelphia, PA 19104, Tech. Rep., June 2023, contract No. 15-C-UAS. Final Report, January 1, 2022 through April 1, 2023.

[13] P. Kay, "Emc considerations for unmanned aerial vehicles," in *Handbook of Aerospace Electromagnetic Compatibility*, 2nd ed., R. J. Perez, Ed. Hoboken, NJ, USA: Wiley, 2017, ch. 11, pp. 603–617.

[14] D. Torrieri, *Principles of Spread Spectrum Communication Systems*, 2nd ed. New York, NY, USA: Springer, 2011, comprehensive coverage of spread spectrum techniques and applications.

[15] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed. Norwood, MA, USA: Artech House, 2011, comprehensive coverage of jamming techniques and principles for modern communication systems.

[16] Federal Communications Commission (FCC), "Part 15 - radio frequency devices," https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15, 2023, accessed: 2024-11-19.

[17] European Telecommunications Standards Institute (ETSI), *Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission Systems; Data Transmission Equipment Operating in the 2.4 GHz ISM Band and Using Wide Band Modulation Techniques*, v2.2.2 ed., ETSI, 2021, accessed: December 17, 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_en/300300_300399/300328/02.02.02_60/en_300328v020202p.pdf

[18] J. G. Proakis, *Digital Communications*, 4th ed. Boston, MA: McGraw-Hill Education, 2001, a widely used textbook on digital communication theory and techniques.

[19] E. W. Weisstein, "Normal distribution function," https://mathworld.wolfram.com/NormalDistributionFunction.html, 2024, accessed: 2024-12-10.

[20] T. Matsumura, K. Ibuka, K. Ishizu, H. Murakami, and F. Kojima, "Experimental throughput evaluation of ieee 802.11af channel aggregation with prototype radio device," in *2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2019, pp. 1–4.

[21] T. Williams, *EMC for Product Designers*, 5th ed. Elsevier, 2016.

[22] D. M. Pozar, *Microwave Engineering*, 4th ed. Wiley, 2011.

[23] J. D. Fifield, J. G. Wilkins, and S. P. Cikanek, "Electric motor thermal management research," National Renewable Energy Laboratory (NREL), Tech. Rep. NREL/TP-5400-67121, 2018. [Online]. Available: https://www.nrel.gov/docs/fy18osti/67121.pdf

[24] Noisecom, *NC1000 Series*, N/NC1000/719/EN, 2019, [Revised 2022].

[25] Mini-Circuits, *ZVE-3W-83+*, ECO-013026, 2021, [REV J].

[26] ——, *ZHL-30W-262-S+*, Data Sheet REV D ECO-017583, June 2009, [Revised April 2024].

[27] TAOGLAS, *Datasheet Airvu BPF.24*, SPE-15-8-038/B/WY, 2012.

[28] TP-Link, "Tl-ant2424b 2.4ghz 24dbi grid parabolic antenna datasheet," Online, 2024, available: https://www.tp-link.com/us/business-networking/antenna-and-accessory/tl-ant2424b/.

[29] Cubepilot, "Herelink blue," n.d., accessed: 2024-12-04. [Online]. Available: https://docs.cubepilot.org/user-guides/cubepilot-ecosystem/cubepilot-partners/union-robotics/herelink-blue

[30] IEEE Standards Association, "Ieee 802 lan/man standards committee standards," 2023, standards for Local and Metropolitan Area Networks, including Ethernet (802.3), Wi-Fi (802.11), and others. [Online]. Available: https://standards.ieee.org/802/

[31] CubePilot, "The Cube Module Overview," 2024, [Accessed: 30-Dec-2024]. [Online]. Available: https://docs.cubepilot.org/user-guides/autopilot/the-cube-module-overview

[32] A. U. Bello, K. A. Kamarudin, M. T. Aliyu, and M. S. Ahmed, "FHSS, DSSS, And Hybrid DSFH Performance Evaluation For VSAT," *International Journal of Scientific and Technology Research*, vol. 4, no. 9, pp. 145–151, 2015, [Accessed: 30-Dec-2024]. [Online]. Available: {https://www.ijstr.org/final-print/sep2015/Fhss-Dsss-And-Hybrid-Dsfh-Performance-Evaluation-For-Vsat.pdf}

[33] L. FLYSKY RC MODEL TECHNOLOGY CO., "Fcc filing report for fs-i6s," 2016, fCC ID: N4ZFLYSKYI6S. Testing and certification report conducted under FCC CFR Title 47 Part 15 Subpart C Section 15.247:2014. Report No.: GTS16000033E01. Global United Technology Services Co., Ltd. [Online]. Available: https://fccid.io/N4ZFLYSKYI6S

[34] Texas Instruments, *CC2500: Low-Cost Low-Power 2.4 GHz RF Transceiver Datasheet (Rev. C)*, Technical Datasheet, 2023, accessed: December 17, 2024. [Online]. Available: https://www.ti.com/lit/ds/symlink/cc2500.pdf

[35] RadioMaster, *TX16S MKII User Manual*, Shenzhen RadioMaster Co., Ltd, 2021, accessed: December 17, 2024. [Online]. Available: https://www.radiomasterrc.com

[36] Federal Communications Commission, "FCC Application for Jeti Duplex REX 12 Receiver," 2015, [Accessed: 30-Dec-2024]. [Online]. Available: https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=2715152

[37] Narda Safety Test Solutions, *RadMan 2LT/2XT Datasheet: Warning Device for Electric and Magnetic Fields*, Data Sheet, April 2024, available: https://www.narda-sts.com/.

[38] F. C. Commission, "Guidelines for evaluating the environmental effects of radiofrequency radiation," FCC Std OET Bulletin 65, Federal Communications Commission, Washington, DC, USA, Tech. Rep., 1996, accessed: Month Day, Year. Available: https://www.fcc.gov/.

[39] H. F. Mathis, "A short proof that an isotropic antenna is impossible," *Proc. IRE (Correspondence)*, vol. 39, p. 970, August 1951.

[40] ——, "On isotropic antennas," *Proc. IRE (Correspondence)*, vol. 42, p. 1810, December 1954.

[41] W. K. Saunders, "On the unity-gain antenna," *Electromagnetic Theory and Antennas*, vol. 42, no. 2, pp. 1125–1130, 1963.

[42] W. G. Scott and K. M. SooHoo, "A theorem on the polarization of null-free antennas," *IEEE Trans Antenna and Propagation*, vol. AP-14, pp. 587–590, September 1966.

[43] G. Deschamps, J. Dyson, and P. Mas, "Two-port isotropic radiator for unpolarized waves," *IEEE Trans Antenna and Propagation*, vol. 17, p. 809, 1969.

[44] AMICCOM Electronics Corporation, *A7105: 2.4GHz FSK/GFSK ISM Band Wireless Transceiver Datasheet*, Technical Datasheet, April 2008, accessed: December 17, 2024. [Online]. Available: https://www.amiccom.com/products/A7105

Appendix A - List Of Symbols

$\vec{E}_{\hat{\boldsymbol{\theta}}}$	θ component of the electric field
$\vec{E}_{\hat{\boldsymbol{\phi}}}$	ϕ component of the electric field
j	Imaginary number equal to $\sqrt{-1}$
$\boldsymbol{\theta}$	θ phase shift in radians
$\boldsymbol{\phi}$	ϕ phase shift in radians
$E_{\boldsymbol{\theta}}$	Magnitude of the electric field in units of (V/m)
$E_{\boldsymbol{\phi}}$	Magnitude of the electric field in units of (V/m)
$\overline{E}$	Electric field of antenna

Appendix B - List Of Acronyms and Abbreviations

ADC	Analog to Digital Conversion
AFHDS-2A	Automatic Frequency Hopping Digital System - 2A
AJ	Anti-Jamming
ARRC	Advanced Radar Research Center
ASMR3	Airport Surface Movement Radar Model 3
ASR	Airport Surveillance Radar
ASR-11	Airport Surveillance Radar Model 11
ASR-9	Airport Surveillance Radar Model 9
AUT	Antenna Under Test
AWG	Arbitrary Waveform Generator
AWGN	Additive White Gaussian Noise
BBN	Broad-Band Noise
BBNJ	Broadband Noise Jamming
BER	Bit Error Rate
BFSK	Binary Frequency Shift Keying
BPEMIF	Broadband Performance EMI Filter
BPSK	Binary Phase Shift Keying
CAT	Category
C2	Command and Control
CDMA	Code Division Multiple Access
CFR	Code of Federal Regulations

COA	Certificate of Authorization
C-UAS	Counter-Unmanned Aircraft Systems
DPSK	Differential Phase Shift Keying
DSM2	Digital Spread Modulation 2
DSMX	Digital Spread Modulation X
DSSS	Direct-Sequence Spread Spectrum
DUT	Device Under Test
EA	Electronic Attack
ECE	Electrical and Computer Engineering
EIRP	Equivalent Isotropically Radiated Power
EM	Electromagnetic
EMF	Electromagnetic Field
EMI	Electromagnetic Interference
ESC	Electronic Speed Controller
FAA	Federal Aerospace Administration
FCC	Federal Communications Commission
FEC	Forward Error Correction
FHSS	Frequency-Hopping Spread Spectrum
FFHSS	Fast Frequency-Hopping Spread Spectrum
GFSK	Gaussian Frequency-Shift Keying
GPS	Global Positioning System
HIRF	High-Intensity Radiated Fields
IEEE	Institute of Electrical and Electronics Engineers
ILS	Instrument Landing System
ISM	Industrial, Scientific, and Medical
JSR	Jamming-to-Signal Ratio
km	kilo-meter

LQ	Link Quality
MCU	Microcontroller Unit
NAVAID	Navigational Aid
NTIA	National Telecommunications and Information Administration
OU	University of Oklahoma
OOB	Out of Band
PFSK	Phase Frequency Shift Keying
Q	Q-function
QPSK	Quadrature Phase Shift Keying
RC	Radio Controller
RF	Radio Frequency
RFI	Radio Frequency Interference
RLPM	Radio Link Performance Model
RMS	Root Mean Square
RSSI	Received Signal Strength Indicator
Rx	Receive
SDR	Software Defined Radio
SFHSS	Slow Frequency-Hopping Spread Spectrum
SIR	Signal-to-Interference Ratio
SMS	Safety Management System
SNR	Signal-to-Noise Ratio
SPA	Single Point of Access
SS	Spread Spectrum
sUAS	Small Unmanned Aircraft Systems
TACAN	Tactical Air Navigation
TDWR	Terminal Doppler Weather Radar
Tx	Transmit

UAS	Unmanned Aircraft Systems
VHF	Very High Frequency
VNA	Vector Network Analyzer
VOR	VHF Omnidirectional Range