Report for
80NSSC20M0261

Unmanned Aerial System (UAS) Research for Public Safety Applications

Task 6: Command, Control & Communications Options Assessment
Final Report

Program Manager: Christine Dillard
Principal Investigator: Kenny Cheung

Prepared for NASA Ames Research Center
Moffett Field, California 94035

Technical Report Documentation Page

Title: Task 6: Command, Control & Communications Options Assessment

Report Date: 3/31/2025

Performing Organizations: University of North Dakota

Authors: Dr. Naima Kaabouch

Performing Organization and Address:
College of Engineering and Mines
University of North Dakota
Upson II Room 165
243 Centennial Dr Stop 8155
Grand Forks, ND 58202-8155

Sponsoring Agency Name and Address:
Universities Space Research Association
7178 Columbia Gateway Drive
Columbia, MD 21046

National Aeronautics and Space Administration
NASA Ames Research Center
Moffett Field, California 94035

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF ACRONYMS

Acronym	Meaning
AES	Advanced Encryption Standard
ASTM	American Society for Testing and Materials
BER	Bit Error Rate
C2	Command-and-Control
CA	Carrier Aggregation
DJI	Da-Jiang Innovations
DoS	Denial of Service
FAA	Federal Aviation Administration
GCS	Ground Control Station
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ISI	Inter-Symbol Interference
LOS	Line of Sight
KPI	Key Performance Indicator
NATO	North Atlantic Treaty Organization
NLOS	Non-line of Sight
RAIM	Receiver Autonomous Integrity Monitoring
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RTCA	Radio Technical Commission for Aeronautics
Rx	Received
SNR	Signal to Noise Ratio (received)
sUAS	small Unmanned Aircraft System
SWaP	Size, Weight, and Power
Tx	Transmitted
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicles
UTC	Coordinated Universal Time

TABLE OF SYMBOLS

Symbol	Meaning
$h_{Vertical}$	Vertical Height
$d_{Horizontal}$	Horizontal Distance

EXECUTIVE SUMMARY

The rapid integration of Unmanned Aircraft Systems (UAS) into public safety applications has generated varied research across multiple domains. These systems are increasingly utilized in emergency response, disaster relief, law enforcement, and search-and-rescue missions, necessitating reliable operational frameworks. A key focus of this research, designated as Task 6, aims to assess various command, control, and communications options, ensuring reliable data transmission with minimal errors and least latency while using a diverse set of wireless technologies over varying operational conditions.

The research activities associated with Task 6 are primarily guided by three core research questions: What existing technologies can support the command and control (C2) requirements in UAS operations? How might the operational density of UAS evolve in the foreseeable future, and how can the available spectrum accommodate this growth while maintaining communication quality? What significant insights can be derived from actual UAS flight tests regarding the efficacy of available wireless technologies for C2 support?

These three questions were addressed over the course of three years through in-depth research. As such, Task 6 was addressed under Tasks 6.1, 6.2, and 6.3, corresponding to first, second, and third years of research works, respectively. Task 6.1 investigated the available wireless technologies suitable for UAS C2 applications while Task 6.2 studied C2 operational density and spectrum quality. Finally, the results culminated in Task 6.3 focusing on flight testing and analysis of the flight test data to derive key conclusions.

Task 6.1 evaluated 99 C2 products using eight performance metrics, assessed three wireless technologies using four metrics, examined the likelihood and severity of 14 cybersecurity attacks with countermeasures, and evaluated C2 products across five maturity levels of cybersecurity. The team identified key gaps in C2 systems. Few exist for multivehicle control, including swarms, and most lack cybersecurity measures against cyberattacks. A security analysis found 57.6% of C2 products unprotected from common threats. As UAS use in sensitive areas grows, integrating cybersecurity features in C2 systems will be crucial for safety and reliable missions, particularly authentication techniques and methods that mitigate GPS and Remote Id attacks, spoofing attacks, and jamming attacks.

Task 6.2 studied the factors that suboptimize bandwidth availability. The results showed that increasing transmitter-receiver distance increases pathloss. Higher frequency results in higher pathloss. resulting in decreased signal to noise ratio (SNR) and increased bit error rate (BER). Multipath propagation, Doppler shift, and interference bring additional degradation to SNR. In terms of atmospheric weather conditions, below 10 GHz, rain is the only dominant signal attenuator. The findings advocate for strategies that prioritize lower modulation orders and operating frequencies, which inherently offer greater resilience to factors suboptimizing the operating bandwidth such as rain. Furthermore, the integration of anti-jamming techniques and adaptive transmission strategies is recommended to enhance signal robustness and ensure reliable connectivity in dynamic environments.

Task 6.3 flight tests were conducted, collecting signal metrics and data volumes transmit/receive operations. Tests showed 4G and 5G can support C2 operations under specific conditions, while satellite communication is unreliable for primary Unmanned Aircraft (UA) control. These findings emphasize the need for environment-specific communication strategies and careful UAS platform selection to ensure reliable C2 links. To address inconsistencies, future UAS should integrate multi-link redundancy for reliable connectivity under changing conditions. Additional studies should explore enhancements in satellite communication, possibly using adaptive antennas or hybrid multi-technology systems. Future evaluations should assess communication performance at extended distances to simulate real-world UAS mission scenarios. By refining communication strategies and optimizing UAS selection, future operations can achieve more reliable C2 links, enhancing unmanned flight mission safety and effectiveness.

1 INTRODUCTION & BACKGROUND

Task 6 aims to evaluate the current state of Command-and-Control (C2) communication technologies to produce a comparative structure for evaluating a cross-section of technologies related to C2 activities, ultimately resulting in the flight testing of candidate systems evaluated against these performance criteria as well as an evaluation of the criteria themselves. The objectives of this Task 6 are as follows:

Sub-task 6.1 –C2 Technology Survey (Year 1)

- Identify key technical parameters that contribute to the overall acceptability of a given solution.
- Benchmark available commercial C2 options and classify them according to the characteristics above.

Sub-task 6.2 – C2 Operational Density and Spectrum Quality Study (Year 2)

- Select specific solution(s) identified in Sub-task 6.1.
- Calculate peak bandwidth demand for the selected system.
- Calculate the theoretical limit of bandwidth availability.
- Identify phenomena that sub-optimize bandwidth availability.
- Establish a practical limit for the number of air vehicles using a single C2 solution within the defined volume.

Sub-task 6.3 – C2 Flight Test Experiment (Year 3)

- Conduct flight testing on up to six Uncrewed Aircraft (UA) based on the findings from Task 6.1.
  - Select and procure commercially available UA with C2 systems suitable for this Sub-task.
  - Integrate systems into existing, mature UA platforms where integrated solutions are not readily available.
  - Define flight test operation concepts, which will be used to evaluate C2 suitability.
  - Define performance criteria to be monitored during flight testing.
  - Execute flight tests and record results.

2 UAS EMERGENCY USE CASES

Among the beneficial use cases for UAS includes emergency operations. In certain environments, UAS can prove a linchpin for a successful mission, minimizing risk to rescue workers, covering large areas, providing access to hazardous locations, and ensuring quick response times. Yet the challenges of these environments also point to the necessity for robust C2 communications which the research that follows contributes to resolving. Therefore, discussion about them should be made.

Six such use cases have been identified by this research team, each benefiting from the presence of UAS while presenting specific challenges. Wildfire/incident intervention where ground access to impacted areas can be hazardous or difficult places to operate, opens the door to larger demands on the performance of the UA. Search and rescue use cases present similar advantages. Large areas may again be well suited to small UAS (sUAS) or sUAS swarms quickly scanning areas, however, the complexity of communications over the same area poses challenges requiring robust C2 communication. Incidents in enclosed spaces can be uniquely suited toward sUAS operations in certain instances but require GPS-denied position awareness and control links that must overcome signal blocking obstacles.

Continuing, sUAS in law enforcement situations provide agile solutions to time critical situations, yet these same environments raise the risk of C2 link jamming and spoofing. Disaster response and recovery presents similar environmental challenges. UAS can be ideal for human communication links where infrastructure may be degraded. This also presents a noisy signal environment for which C2 will need to be robust. Finally, short distance transport of critical supplies, such as emergency medicines, is also a role suited to UAS. This is especially true in urban environments, highlighting the need for strong C2 links.

Ensuring performance reliability in the application scenarios as discussed above necessitates benchmarking of existing C2 systems, developing key performance metrics for comparing and assessing their performance, with the objective of enhancing our understanding about the impact of factors that influence the quality of UAS communication, and demonstrate the potential adequacy of C2 systems in adverse environments. This project accomplishes this by showing which C2 technologies would be most effective in such adverse environments.

3 TASK 6.1 C2 TECHNOLOGY SURVEY

3.1 Survey Methodology

The Year 1 (2021-2022) Task 6.1 objective was to conduct a survey of C2 technologies, focusing on complete systems as well as components and sub-systems with new features. While this focus remained primarily on sUAS, some products intended for larger systems were included as candidate technologies that could be useful for sUAS usage in the future in some capacity. The methodology used included a variety of keywords and search methods to comprehensively find appropriate documents and websites (articles, reports, and datasheets from companies). The results were aggregated using the Zotero reference management software platform to pull links, papers, reports, and other information into documents. This information was then categorized into multiple groups aligning with appropriate C2 components.

3.2 C2 Components and Metrics

The research team identified 99 different C2 products varying in size, weight, power consumption, design characteristics, built-in cybersecurity features, and other features. These characteristics were divided into a series of key performance indicators (KPI): band diversity, data rate, range/broadcast power, size, weight, and power (SWaP), temperature, humidity, packet loss, and cybersecurity, as shown in Table 1. Cybersecurity required separate consideration, given that C2 systems can be the target of cyberattacks that may jeopardize mission success and airspace safety. The categorization was iterated over the course of the research, but the essentials of this structure were consistently used. More in-depth discussion of this process and other aspects of the methodology may be found in the Year 1 Task 6.1 report.

Table 1. Metrics for C2 Technologies Evaluation and Corresponding Priority.

Metrics	**Priority**	**Justification**
Band Diversity	Low	ASTM Standards F3002 - 14a and RTCA DO-377.
Data Rate	High	The minimum data rate for a single unmanned aircraft in manual mode, as defined in DO-377A as 3.4 kbps.
Range/ Broadcast Power	Medium	At least 0.5km is required for an unaided pilot in command for a line-of-sight mission (14CFR part 107 definition).
SWaP	High	UAS have SWaP limitations for C2 systems.
Temperature	Medium	UAS are used in harsh environments, where weather conditions can degrade their performance.

Humidity	Medium	The C2 system's operations may be compromised under certain weather conditions.
Packet Loss	High	The minimum requirement for aerial vehicle connectivity services is 10^{-3}.
Cybersecurity	High	UAS is subject to cyberattacks resulting in severe consequences.

In this project, only standard wireless communication techniques were used to maximize the interoperability and existing wireless communication infrastructures: 4G and 5G mobile, Wi-Fi, and satellite communications. Comparison of cellular, Wi-Fi, and satellite communication standards regarding UAS operation suggests that different technologies could be effectively used for UAS C2 link operation, with specific restrictions in those KPIs.

To make it easier to evaluate the 99 C2 products and their varying representation of performance and specification data. The metrics are broken into 5 levels. 1 indicates a poor level of performance while 5 indicates the best level of performance for a given metric. If applicable, an explanation is provided for why each range of values was chosen for each level of the metrics scale. Table 2 and Table 3 are examples of these metrics.

Table 2. Data Rate Levels.

Level	**1**	**2**	**3**	**4**	**5**
Value (Kbps)	3.4 to 2500	2500 to 5000	5000 to 15000	15000 to 25000	> 25000
Explanation	3.4 Kbps constitutes the minimum rate for a single unmanned aircraft in manual mode as defined in DO-377A.	2500 Kbps is the recommended data rate for 720p video streaming.	5000 Kbps is the recommended data rate for 1080p video streaming.		

Table 3. Broadcast Power Levels.

Level	**1**	**2**	**3**	**4**	**5**
Value (mi/km/nmi)	< 0.31/0.5/0.27	cat 1 < range <= 21.29/34.26/18.5	cat 2 < range <= 56.39/90.75/49	cat 3 < range <= 77.1/123.08/67	cat 4 < range
Explanation	Requirement for unaided PIC line-of-sight (14CFR part 107 definition)	DO-362A CNPC Low Altitude Service Volume	DO-362A CNPC Medium Altitude Service Volume	DO-362A CNPC High Altitude Service Volume	

For example, data rate was assessed at three different performance levels with possible C2 operations. In the case of user experienced rate and radio interface latency, only the top Level 3 performance tier was adequate for C2 operation. In any case, these KPIs could demonstrate how to adequately address future growth in the UAS market. As before, more in-depth discussion can be found in the Year 1 Task 6.1 report.

Table 4. Wireless Communication Standards and Their KPIs.

Wireless Network		Radio Frequency Bands	Data Rate (Gbps)	Peak Data Rate (Gbps)	User Experienced Rate (Mbps)	Radio Interface Latency (ms)
Cellular	3G	1920 - 1980 MHz 2010 - 2070 MHz	0.0003 - 0.014	0.014	5.76	10
	4G	2500 - 2570 MHz 2620 - 2690 MHz	0.07 - 1	1	10	10
	5G	410 - 7125 MHz 24250 - 52600 MHz	1 - 10	20	100	1
	6G	100 GHz - 10 THz Visible Light	≥ 1000	1000	1000	0.1
Wi-Fi	ISM	2.4GHz, 5 GHz, 5.8GHz, 60GHz, TV Bands: 54 to 698 MHz	0.011 - 8	8	240 - 2400	10 - 100
Satellite	LEO	L, S, C, X, Ku-, extended Ku, Ka, UHF	8 - 40	9 - 45	100 - 200	10 - 30
	MEO	L, S, C, X, Ku-, extended Ku, Ka, UHF	0.08 - 0.8	0.8	500	70 - 200
	GEO	L, S, C, X, Ku-, extended Ku, Ka, UHF	0.005 - 0.1	0.1	60	447 - 600

3.3 Cybersecurity

UAS communicate with ground control stations through various communication channels using C2 systems. This diversity in communication methods expands the attack surface, increasing the vulnerability of UAS to cyberattacks that can jeopardize airspace safety, confidentiality, and mission success. These cyberattacks can target multiple components of the UAS network, or in some cases, focus on a specific element to increase the impact. Therefore, it is crucial to understand the types of attacks that directly or indirectly affect C2 systems, as well as their potential impacts, likelihood, severity, and possible countermeasures to mitigate these risks.

A total of 14 distinct attacks were identified and classified into five categories: Denial of Service, Adversary-in-the-Middle, Intrusion, Social Engineering, and Spoofing. Most of these attacks primarily target the Ground Control Station (GCS), as it is more accessible compared to the C2 system itself (Figure 1). A risk assessment was conducted to evaluate the likelihood and severity of these identified cyberattacks, helping to pinpoint the most dangerous threats. Finally, critical countermeasures and recommended cybersecurity protocols were proposed to protect C2 systems and mitigate the impact of the most severe cyberattacks. More details about the attacks shown in Figure 1 can be found in Year 1 Report, Section 6.1.

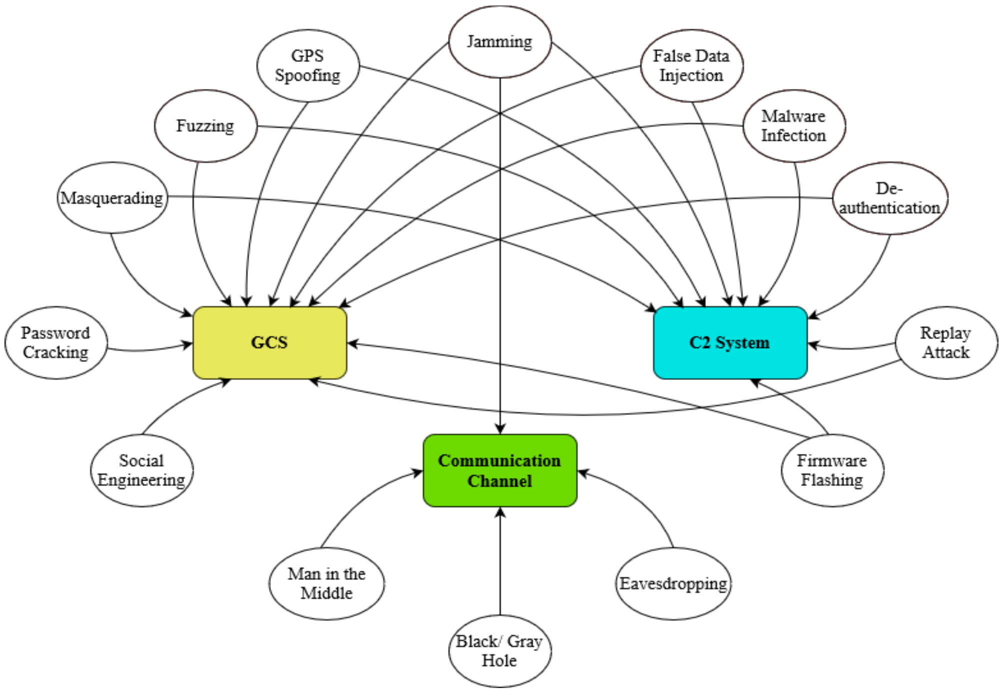


Figure 1. Attacks on C2 systems, Ground Control Stations (GCS), and the communication channel.

3.3.1 Risk Assessment of Cyber-Attacks on C2 Technologies

A cybersecurity risk assessment is essential to identify the most damaging threats to C2 technologies and determine appropriate mitigation strategies. This assessment evaluates potential security risks to the C2 system, analyzing their likelihood and severity. The team used a three-level scale—low, medium, and high—to rate the likelihood and severity of each threat, enabling a clear understanding of the most critical vulnerabilities and guiding effective countermeasure development.

The likelihood evaluation in this study was based primarily on each attack's statistics from articles and news, ease of launching the attack, and system vulnerabilities. One challenge the team faced during this search was the low number of reported attacks in the news since media and news primarily target the general public; therefore, they tend to focus on the assault's impact rather than providing adequate technical information to identify and categorize the reported attacks. In addition, C2 technology manufacturers do not disclose their product's vulnerabilities since it may harm their reputation; therefore, the actual number of attacks may be much higher than those reported. Based on the reported attacks the team could find, denial of service (DoS) attacks are the most common at 47%, followed by intrusion attacks with 29%, while adversary-in-the-middle assaults were third with 14%. Spoofing attacks accounted for 10% of all attacks. Social engineering assaults occur daily; however, none were reported. The calculation of the attack's percentage in each category is based on the relative frequency of each attack type within a dataset of recorded UA security incidents. For example, for a total number of recorded attacks N_a, and the number of attacks in DoS category N_{DoS}, the percentage attack for DoS is given by: $\frac{N_{DoS}}{N_a}100$.

Likelihood is defined as the possibility that an attack will occur. Several studies have attempted to develop a general approach for evaluating the likelihood of various cyberattacks under different circumstances; however, it was found that the attack likelihood is fundamentally different for distinct types of networks (Javaid, 2012). Several factors must be evaluated to determine the likelihood of cyberattacks in C2 technologies, particularly the attack frequency, network topology, and expertise and knowledge required for a successful attack. The likelihood evaluation in this study is based primarily on each attack's statistics, ease of launching the attack, and system vulnerabilities.

Severity denotes the level of impact following an assault. The attack severity is low if the assault causes minor issues, such as listening to the channel; medium if it causes a user to lose control for an extended period, such as jamming attacks; and high if the attacker takes complete control of the C2 system or GCS, such as with GPS spoofing attacks.

This risk of an attack was defined as:

$$\text{Risk} = \text{Likelihood} \times \text{Severity}$$

Risk matrix results for cyber-attacks on C2 technologies are represented in Table 5. GPS spoofing and false data injection attacks are the most common and severe attacks that target C2 technologies, where their risk level is critical, followed by jamming and masquerading with a high risk. All other attacks have medium risk, except for the black/gray hole and fuzzing attacks, which are considered low risk.

Table 5. Risk Matrix of Cyber-Attacks on C2 Technologies.

		Severity		
		Low	**Medium**	**High**
Likelihood	**High**	Eavesdropping Social Engineering*	Jamming	GPS Spoofing False Data Injection
	Medium	De-authentication attack	Man-in-the-middle Password Cracking Malware Infection	Masquerading
	Low	Black hole/gray hole Fuzzing	Replay Attack	Firmware Flashing

* Social engineering attacks occur only on GCS.

3.3.2 C2 Technologies Cybersecurity Evaluation

The team surveyed and provided a list of countermeasures to mitigate the most dangerous attacks with high and critical risks resulting from the risk assessment (Year 1, Section 6.3). This list shown in Table 6 includes methods from each of the three categories: cryptography, anti-jamming, and anti-GPS spoofing.

Our research shows that a significant number of C2 products surveyed (57.6%) lack any cybersecurity features. In contrast, 15.3% offer encryption, and 4.3% provide anti-jamming capabilities. Additionally, 22.8% of the products incorporate both encryption and anti-jamming techniques.

Table 6. Countermeasures Against Most Severe Attacks.

Attack or Category	**Examples of Countermeasures**
Cryptography	• Advanced Encryption Standard (AES) (Khoei, 2021) (Daemen, 1999) • Data Encryption Standard (Khoei, 2021) (D. E. Standard, 1999) • Rivest, Shamir, and Adleman (Khoei, 2021) (Rivest, 1978) • Elliptic-Curve Cryptography (Koyama, 1991)
Jamming	• Game-Theoretic (Jia, 2017) • Channel Hopping (Pärlin, 2019) • Spread Spectrum (Luo, 2020) • Regulated Transmitted Power (Rezgui, 1978) • Spatial Retreat and Decoy (Kang, 2016) • Antenna Polarization (Rezazadeh, 2019) • Antenna Array (Ni, 2018) • Beamforming Smart Antennas (Zhang, 2019) • Artificial Intelligence (Johansson, 2017) • Detection of cyber attacks targeting avionics systems (Kaabouch, 2024)

	• Autonomous vehicle control attack detection and countermeasures (Kaabouch, 2022)
GPS Spoofing	• Game-Theoretic (Eldosouky, 2019) • Signal Elimination Based on Signal Strength (Sathaye, 2020) • Receiver Autonomous Integrity Monitoring (RAIM) (Khanafseh, 2014) • Predictive Model (Jovanovic, 2014) • Multi-Antenna Spoofing Discrimination (Magiera, 2019) • Adaptive Filtering for Signal Spoofing Discrimination (Mosavi, 2016) • Detection of cyber attacks targeting avionics systems (Kaabouch, 2024) • Detection of spoofing and meaconing for geolocation positioning system signals (Kaabouch, 2022) • Autonomous vehicle control attack detection and countermeasures (Kaabouch, 2022)

The team also proposed a five-level cybersecurity framework for C2 systems based on these findings. Table 7 provides a five-level cybersecurity framework for C2 systems. A C2 system of level 1 lacks security measures due to UAS's SWaP constraints. The second level integrates software-based encryption, adhering to SWaP limitations. The third level includes anti-jamming techniques, often using antenna-based solutions like antenna arrays and smart antennas. The fourth level C2 system combines both encryption and anti-jamming methods. The fifth level incorporates protection against GPS spoofing, as well as encryption and anti-jamming countermeasures.

Table 7. C2 Product Cybersecurity Maturity Levels.

Level	**1**	**2**	**3**	**4**	**5**
Cybersecurity Feature	None	Encryption	Anti-Jamming	Encryption Anti-Jamming	Encryption Anti-Jamming Anti-GPS Spoofing
Explanation	Due to UAS's SWaP constraints	Minimum security feature: simple, software-based, meets SWaP constraints	Antenna-based signal cancellation countermeasure, power consuming	Combines encryption (software) and jamming (antenna-based) countermeasures	High security level, includes GPS spoofing countermeasure, power consuming

3.4 Task 6.1 Conclusion

C2 products vary greatly in terms of available options, such as size, weight, and power consumption, number of supported vehicles and users, and cybersecurity features, whereas some UAS missions require meeting specific criteria to be successful. Therefore, different communication standards should be adapted based on the mission and the operational area: cellular network technologies, Wi-Fi networks, and satellite communications, each of which may offer different data rates, ranges, and broadcast power.

In Year 1, the focus was primarily on commercial products and integration and the evaluation of the suitability of candidate standards-based communication technologies for general C2 use in UAS operations. Additionally, the team identified and assessed the risk of cyber-attacks on C2 systems and proposed a 5-level approach for evaluating C2 systems. Furthermore, a list of countermeasures to mitigate the most severe cyberattacks was provided.

As a result of this study, the team identified several gaps. Currently, very few C2 systems are designed for controlling multiple UA simultaneously, including swarm operations. This limits the efficiency and scalability of sUAS operations in complex configurations. Moreover, a significant portion (57.6%) of C2 products lack adequate cybersecurity measures as many existing systems do not incorporate countermeasures to mitigate common and severe cyber threats. In terms of standardized evaluation of C2 systems, although a common approach has been proposed in the report, there is currently no widely adopted framework to assess C2 communication technologies effectively. Standardized benchmarks and performance evaluation criteria for commercial C2 products are still needed. An additional gap is inadequate adaptation to mission-specific communication requirements. For example, different missions may require specific communication standards (e.g., cellular, Wi-Fi, satellite), yet there is no clear strategy for selecting or integrating the most appropriate technology for each mission type. Secure and reliable C2 communication is critical in emergency use cases, however, currently there is a lack of real-world validation of C2 performance in emergency applications. These gaps highlight the need for further research and development in multivehicle C2 systems, cybersecurity enhancements, mission-adaptive communication strategies, and emergency operation capabilities, ensuring seamless connectivity across diverse environments.

4 TASK 6.2 – C2 OPERATIONAL DENSITY AND SPECTRUM QUALITY STUDY

Year 2 (2022-2023) Task 6.2 objectives consisted of selecting the C2 systems for evaluation during flight testing, calculating the peak bandwidth demand and theoretical limit of bandwidth availability for the selected systems, identifying phenomena that sub-optimizes the bandwidth availability, and establishing practical limits for the number of UAS using a single C2 solution within a defined volume.

4.1 Task 6.2.1: Selected C2 Systems Identified in Sub-Task 6.1

Five C2 systems were selected for testing, including the Sky Drones Airlink, Qualcomm Flight RB5 5G Platform, Elsight Halo, Botlink XDR2, and IRIDIUM SBD 9523. These systems were selected to include a wide range of communication technologies: 4G, 5G, Wi-Fi, and Satellite.

4.2 Task 6.2.2: Calculation of Peak Bandwidth Demand

4.2.1 Peak Bandwidth for a Single UA

Bandwidth demand is especially relevant to certain use cases that mandate high-quality communications and may be forced to share available bandwidth. Understanding and appropriately managing this bandwidth is fundamental for seamless and effective UA operation. The data exchange can be classified in three categories while the UA operates in five phases of flight, which is outlined below with bandwidth demand characteristics in Table 8.

Table 8: Peak Bandwidth Demand of a Single UA with QPSK ¼ Modulation.

Functional Category Traffic Class		Throughput T			Redundancy Factor R	Security Over-head	Spectral Efficiency	Bandwidth (MHz)		
		Up link	Down link	Total				Up link	Down link	Total
Command and Control	Control Data	0.692	1.170	1.862	2	8%	0.490	0.00305	0.005158	0.00821
	NavAid Data	0.247	0.328	0.575	2	8%	0.490	0.001089	0.001446	0.00254
ATC Relay	ATC Voice Relay			4.800	2	8%	0.490			0.02116
	ATS Data Relay	0.024	0.031	0.055	2	8%	0.490	0.000106	0.000137	0.00024
Sense and Avoid	Target Tracks		9.120	9.120	2	8%	0.490		0.040202	0.04020
	Weather Radar Data		8.729	8.729	1	8%	0.490		0.019239	0.01924
	Non-payload Video		270.000	270.000	1	8%	0.490		0.595102	0.59510

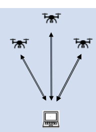
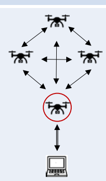
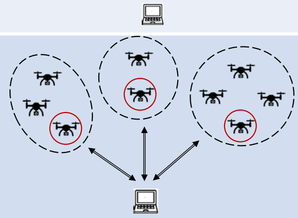
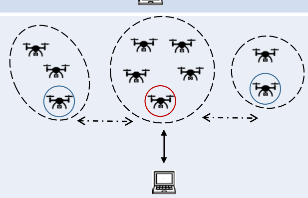
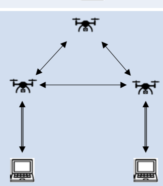
Total Bandwidth (MHz)		**0.004245**	**0.661284**	**0.68669**

One notable trend in the data is that, as modulation order increases, peak bandwidth demand exhibits a decreasing pattern. This is likely due to high spectral efficiency achieved through more complex modulation schemes.

4.2.2 Peak Bandwidth for Multiple UAS

UAS swarms are sometimes used in emergency scenarios such as search and rescue missions, disaster response, and damage assessment. They can cover large areas quickly, gather real-time data from hard-to-reach locations, and provide coordinated support for tasks like locating survivors or delivering supplies. These swarms can be configured to communicate using different topologies with different advantages and disadvantages versus single aircraft operation. Five types of UA swarm configurations were identified, as shown in Table 9, along with their bandwidth demand characteristics as compared to single UAS requirements.

Table 9: Summary of UA configurations and bandwidth demand.

Configuration	Architecture		Bandwidth Demand
Star		N UAS 1 GCS	$B_{P\_Total} = \sum_{i=1}^{N} \left(B_{P\_UL_i} + B_{P\_DL_i}\right)$
Mesh		N UAS 1 GCS	$B_{P\_Total} = \sum_{i=1}^{1} \left(B_{P\_UL_i} + B_{P\_DL_i}\right) + 2 * \sum_{i=1}^{N(N-1)/2} B_j$
Multi-Star		M Stars Ni UAS/Star 1 GCS	$B_{P\_\text{Total}} = \sum_{i=1}^{M} \left(B_{P\_UL_i} + B_{P\_DL_i}\right) + 2 \sum_{i=1}^{M} \sum_{j=1}^{N_i(N_i-1)/2} B_j$
Hierarchical Mesh		M Stars (Leads) Var. N UAS/Star M Leads' Network 1 GCS	$B_{P\_\text{Total}} = \sum_{i=1}^{1} \left(B_{P\_UL_i} + B_{P\_DL_i}\right) + 2 * \sum_{j=1}^{M(M-1)/2} B\_L2_j + 2 * \sum_{i=1}^{M} \sum_{k=1}^{N_i(N_i-1)/2} B\_L1_k$
Multi-UAS Multi-GCS		N UAS M GCS	$B_{P\_\text{Total}} = \sum_{i=1}^{M} \left(B_{P\_UL_i} + B_{P\_DL_i}\right) + 2 * \sum_{i=1}^{N(N-1)/2} B_j$

4.3 Task 6.2.3: Theoretical Bandwidth Availability

UA operations are regulated by the standards applicable to 3GPP, Wi-Fi, and satellite communication. In this scheme, various factors come into play, influencing bandwidth availability, including communication standards (such as 6G/5G, LTE, Wi-Fi, cellular, or satellite), the comm direction (uplink or downlink), and whether aggregation is involved or not.

4.3.1 Available Bandwidth Without Aggregation for The Selected Systems

The manufacturer's product specifications play a crucial role in determining the frequency bands supported by each C2 system. These supported channels are important for identifying the appropriate Carrier Aggregation (CA) channel according to the standards defined by 3GPP. These characteristics for the products, including their supported technologies, are shown in Table 10. The candidate products are outlined in the discussion of subtask 6.2.3 of the Year 2 report.

Table 10. C2 Product Frequency Bands Maximum Bandwidth.

C2 Product	Supported Communication Technology	Maximum Upload (MHz)	Maximum Download (MHz)	Maximum total (MHz)
Sky Drones Airlink	4G	20	20	40
	5G	100	100	100
Qualcomm Flight RB5 5G Platform	4G	20	20	40
	5G	400	400	400
Elsight Halo	4G	20	20	40
	5G	100	100	200
Botlink XRD2	4G	20	20	40
Iridium SBD 9523	Satellite	10.5	10.5	21

4.3.2 Available Bandwidth with Carrier Aggregation

The maximum available bandwidth that can be achieved using the considered communication technologies is limited and can only achieve hundreds of Mbit/s data rates. The 3GPP group introduced the concept of CA in LTE-advanced mobile communication systems to solve the issue of bandwidth scarcity, which allows wide frequency bandwidths of up to 100 MHz, achieving data rates of up to 1 Gbps. This group defined three main types of CA according to the carrier component operating frequency placement: intra-band contiguous CA, intra-band non-contiguous CA, and inter-band CA. The aggregation combinations defined by the 3GPP standards may not always be possible due to operator-allocated frequencies (Iwamura, 2010).

It should be noted that the selected C2 systems did not support CA. The absence of CA in C2 systems restricts communication to a single carrier, resulting in reduced data rates and potential congestion in high-traffic areas. The lack of CA support forces the C2 system to rely on a single carrier, thereby increasing its vulnerability to interference, congestion, or network degradation. Furthermore, the absence of CA prevents the UA from effectively utilizing multiple network layers (e.g., low-band for coverage, mid/high-band for speed), which elevates the risk of link loss in areas with weak signals.

CA plays a crucial role in optimizing latency by selecting the most suitable carrier or combining multiple carriers to enhance data flow; thus, its absence may lead to delayed commands, which is critical for real-time UAV operations. Another disadvantage of the lack of CA is the reduction in mission flexibility, particularly in challenging environments where a single carrier may prove insufficient. In scenarios where multiple UAs lacking CA operate simultaneously within a given geographical region, the limited bandwidth availability on a single carrier may result in network bottlenecks and degraded performance. In such circumstances, the probability of total link failure due to increased outage probability becomes significantly high, posing a danger in critical applications such as emergency response operations. In summary, the absence of CA in a UA C2 system substantially diminishes communication robustness, increases latency, and compromises mission success in critical operations.

4.4 Task 6.2.4: Factors that Sub-optimize Bandwidth Availability

In wireless communications, the channel through which the signal propagates from transmitter to receiver includes all types of physical mechanisms that attenuate, reflect, refract, scatter, and modify the signal as it propagates (Wang, 2019). The transmitted signal naturally weakens as it travels farther from the transmitter, even in the absence of obstacles that cause reflection, refraction, and scattering. Attenuation occurs because the net energy within the transmitted signal gets distributed over the increasing surface area of the three-dimensional space traveled by the propagating signal (Bullington, 1947).

Therefore, bandwidth availability is susceptible to various factors, including pathloss, interference, Doppler shift, weather conditions, multipath effects, and shadowing (Figure 2). Considerations such as distance, antenna technology, and spectrum allocation can further influence UA communication reliability and capacity.

In this study, to evaluate the impacts of these factors on bandwidth availability for UA communications, several mathematical models were developed, and three qualitative and quantitative metrics were used: constellation diagrams, Bit Error Rate , and attenuation.

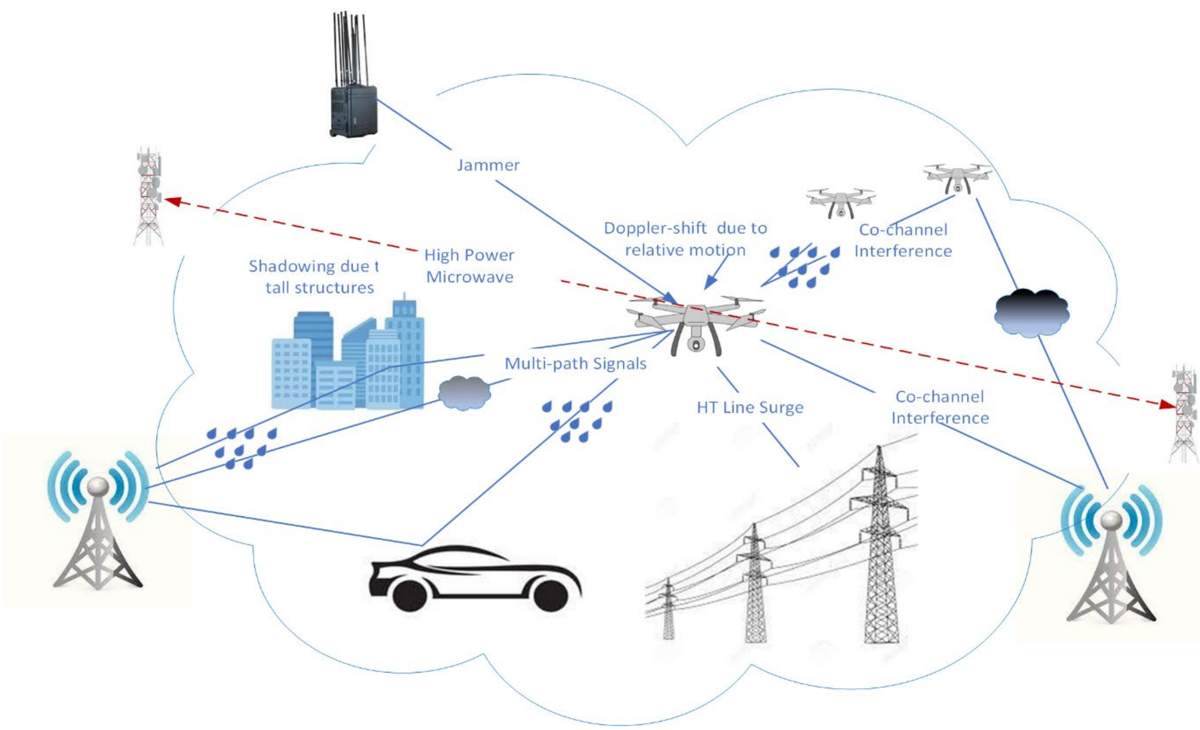


Figure 2: Key sub-optimizing phenomena encountered in the wireless propagation channel.

4.4.1 Pathloss

Several simulations were performed to understand how pathloss affects the bandwidth availability for UA and GCS using the IQ Constellation and BER. These spanned parameters include propagation distance, carrier frequencies, antenna height, and modulation schemes. Results indicate that pathloss becomes more pronounced with greater propagation distances, resulting in a more dispersed IQ constellation and an elevated BER. Lower carrier frequencies exhibit reduced pathloss, leading to a lower BER over extended distances. Higher-order modulation schemes are more susceptible to pathloss, contributing to a higher BER than their lower-order counterparts. Furthermore, the impact of pathloss increases as UA altitude increases. These effects are illustrated in Figure 3. More details can be found in Year 2 Report, Section 5.1.

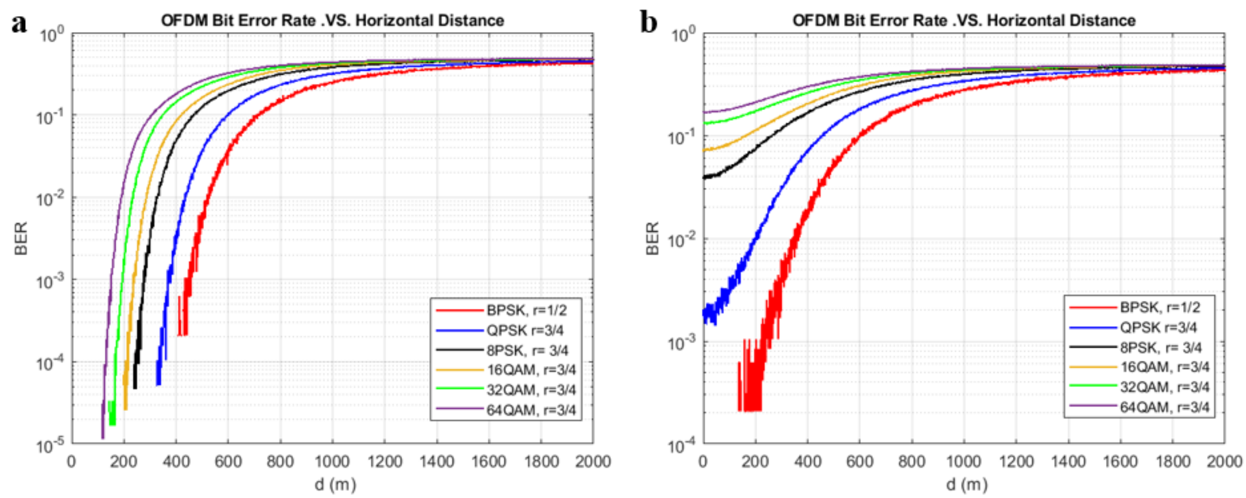


Figure 3: BER as a function of propagation distance with different modulation orders at 2.4GHz and a UA altitude of 100 (a) and 400 (b) meters.

4.4.2 Interference

The impact of interference on bandwidth availability was also examined using a combination of quantitative and qualitative metrics. These metrics included power and channel gain for both the transmitted and interference signals, as well as noise, interference overlap, and modulation orders. The findings indicate that interference exerts a significant effect on available bandwidth, particularly when the degree of overlap increases, the interference power intensifies, or both overlap and interference power increase concurrently. This scenario can lead to a deterioration in signal integrity. This effect exists across different modulation schemes and interference scenarios, highlighting that higher-order modulation schemes are particularly susceptible to interference-induced BER degradation, as shown in Figure 4. It also emphasizes the need for robust countermeasures and strategies in the presence of interference.

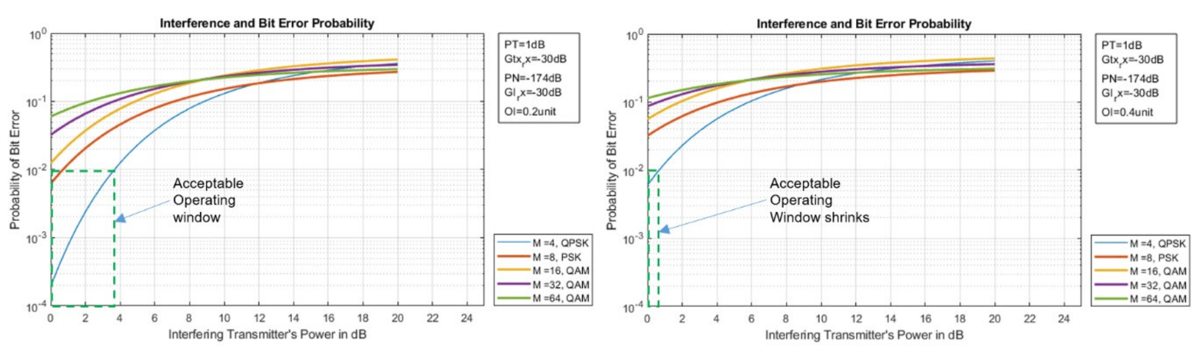


Figure 4: BER vs. Interference Power for different modulation schemes. Left figure corresponds to an interference overlap of 40%, whereas, the right figure shows the impact on operating bandwidth reduction as the overlap factor at the same interference power increases to 60%.

4.4.3 Doppler Shift

This study investigated the impact of Doppler shift on UAS communications, revealing how the IQ constellation and BER of received signals change under the influence of Doppler shift across different velocities and modulation orders. The dispersion of data points within the IQ constellation intensifies with increased relative speed between the transmitter and receiver, leading to a higher BER. The acceptable operating frequency range for UA depends on SNR, the speed of the UA, and the modulation schemes employed. This range expands with higher SNR values and lower UA speeds. Figure 5 illustrates two distinct UA speeds. At a lower speed of 50 km/h, shown by the left figure, the C2 communication is achievable for all assumed frequencies and modulation schemes. However, as the speed increases to 150 km/h (right figure), the BER crosses the maximum allowed threshold, resulting in non-availability of an operating window. There are tradeoffs, however. Lower order modulation reduces spectral efficiency and necessitates broader bandwidth allocation for data transmission. This increase may limit bandwidth availability for other UA and restrict their operation due to unavailability of carrier frequency. This study underscores the need for careful resource management and trade-off analysis in UA communication systems to ensure both BER performance and equitable resource allocation in the presence of Doppler shift challenges. Different techniques can address the impact of Doppler shift, including speed reduction, transmitter power amplification, and adoption of a lower-order modulation scheme.

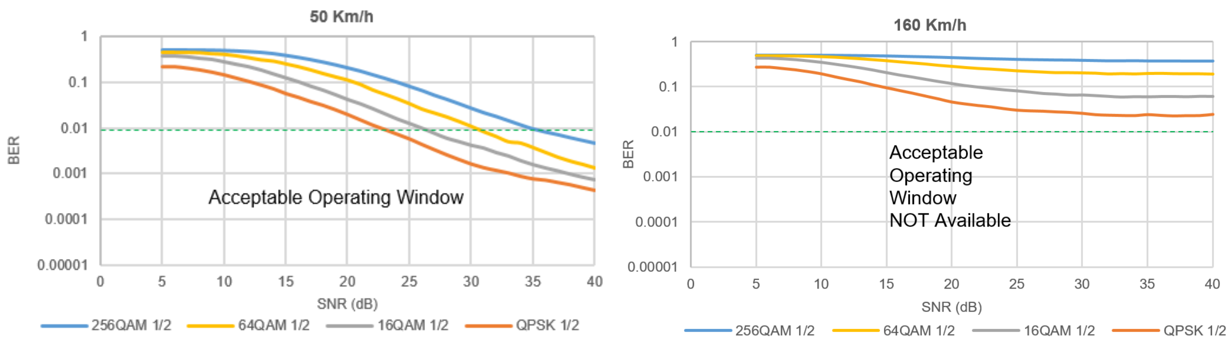


Figure 5: BER vs. SNR of different modulations at fixed speeds. Left figure illustrates the BER performance at 50 km/h, with operable window available for all modulation schemes. The Right figure shows the effect of UA speed at 160 km/h, where increased Doppler shift results in BER threshold being crossed by all modulation schemes.

4.4.4 Multipath

The multipath investigation examined the random variations in path gain and propagation delay via modeling and simulations, revealing the challenges these variations pose to UAS communication. Variations in path gain and propagation delay can lead to deep fading (Figure 6) and introduce Inter-Symbol Interference (ISI), making communication unreliable and unstable. These adverse effects are particularly pronounced for UAS missions in urban environments with dense buildings or in areas with complex topography, where signal reflections and interference are more likely to occur. The findings emphasize the importance of adaptive communication strategies to mitigate the challenges of multipath signal propagation. Specifically, based on the worst-case deep fade, the link budget requires to be adjusted to avoid outage due to signal power dropping below the minimum threshold. The power delay profile presents a snapshot in time-domain about the wireless channel's fading characteristics. Since the channel condition varies randomly, robust link budgeting demands analysis of power delay profile over longer periods, and at different locations to ensure UA's operation under all conditions.

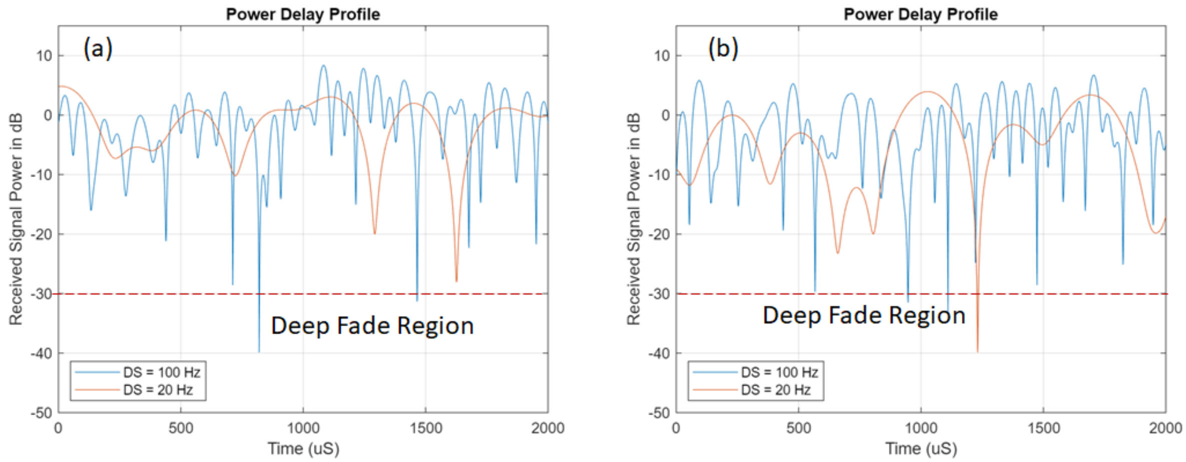


Figure 6: Power delay profile of received signal and fading. Left and right figure shows the power delay profiles corresponding to two different times, and the differences between the two illustrates the variability of channel states.

4.4.5 Weather Impact

Extensive simulations were conducted to evaluate the impact of diverse weather conditions on the availability of bandwidth. The study concentrated on quantifying the impact of signal impairment on BER in relation to various modulation schemes, coding rates, distance, and frequencies. The findings revealed that atmospheric gases, including temperature and pressure variation, have a minimal influence on the bandwidth pertinent to short-range C2 communications. Clouds and fog, instead, cause more attenuation compared to atmospheric gases. Despite this, the impact of standard cloud and fog conditions on wireless communication remains minimal. However, given the necessity of line-of-sight operations and the requirement to maintain visibility of the UA throughout its flight, weather conditions that have a negligible effect on wireless signals may still render operations unfeasible due to visibility issues faced by the operator. Rain intensity, on the other hand, causes considerable attenuation. The outcome of an exhaustive analysis shows a substantial increase in BER that correlates with increased rain intensity, particularly at high carrier frequencies and with advanced modulation schemes. This effect is less marked at low carrier frequencies under 10GHz, suggesting that these frequencies are more advantageous in mitigating the influence of rain and other atmospheric disturbances. In the context of UA operations under fluctuating weather conditions, there is a need for an effective mechanism to balance these trade-offs, given that lower carrier frequencies typically correspond to limited bandwidth availability. Figure 7 shows examples of results of BER as a function of frequency for gas, cloud/fog, and rain-based attenuation as well as their corresponding reductions of operating bandwidth. More details about the weather impact can be found in Year 2 Report, Section 5.5.

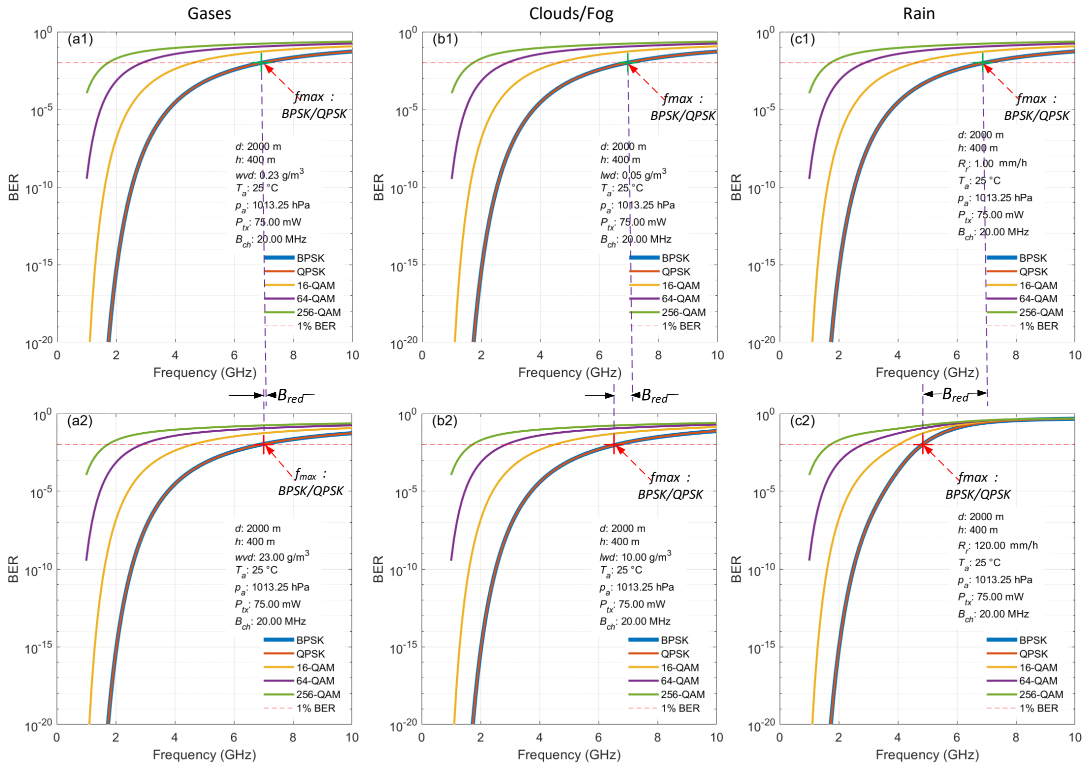


Figure 7: BER as a function of frequency for gas, cloud/fog, and rain-based attenuation. Top row (a1 to c1) represents BER resulting from attenuations due to gas, cloud/fog, and rain, respectively, with atmospheric parameter values causing relatively lesser attenuation. Bottom row (**a2** to **c2**) represents BER resulting from attenuation due to gas, cloud/fog, and rain, respectively, with atmospheric parameter values causing higher attenuation, resulting in reduction of operating bandwidth.

4.5 Task 6.2.5: Calculation of the Number of Vehicles Supported by One C2 System

In this subtask, the capacity of each of the selected C2 system to control multiple UA was calculated. The upper limit of vehicles manageable by a given C2 system is contingent on various factors, including: the configuration of the UA swarm, the bandwidth available to the C2 system, and the employed modulation scheme.

In the evaluation of each C2 product, five swarm configurations were considered: star, mesh, multi-star, hierarchical mesh, and multi-UA-GCS. For each configuration, the team calculated the maximum number of vehicles manageable under five different modulation schemes: QPSK, 8PSK, 16QAM, 64QAM, and 256QAM. To align the analysis with actual application, it was assumed that only a portion of the total bandwidth allocated to a specific system would be dedicated to the UA swarm.

There is a notable disparity in the maximum number of UA that can be supported by various C2 products, attributable to their respective bandwidth ranges. The Qualcomm product is capable of supporting the highest number of UA, accommodating up to 183 vehicles in star configuration, fewer in all other topographies. The Sky Drones and Elsight products each could support a maximum of 91 UA in a star configuration. By contrast, the Botlink product, utilizing 4G technology and operating on the B band, offers a more restricted bandwidth, limiting its capacity to 18 UA in a star configuration, tenfold less than Qualcomm's capability. Finally, Iridium, the satellite communications technology, could support up to 9 UA in a star configuration, 12 UA in mesh.

The data revealed that in general (Figure 8), the star configuration across all C2 systems facilitates support for a larger number of UA, the caveat being a topology characterized by higher latency and a heightened risk of link blockages. Additionally, the issue of path-loss might impede communication between the UA and the GCS, rendering the star configuration more appropriate for short-range missions. By contrast, while the mesh configuration supported fewer aircraft, its inherent redundancy can ensure sustained communication even in the event of failure of an intermediary node. This gives the mesh topology advantages in challenging terrains, such as urban structures and mountainous areas.

In every setup, it is noted that the highest number of supported UAs rises with the modulation order, except for 16 QAM, where the number of supported UAs falls compared to 8PSK. This decline is due to the application of a code-rate of one-half in this scenario, which effectively doubles the data to be transmitted because of increased redundancy aimed at better error recovery. Typically, it is the spectral efficiency that determines the maximum number of supported UAs for a given bandwidth. The spectral efficiency η, expressed in bps/Hz in terms of code rate R and modulation order M, is provided by the equation $\eta = R.\log_2 M$.

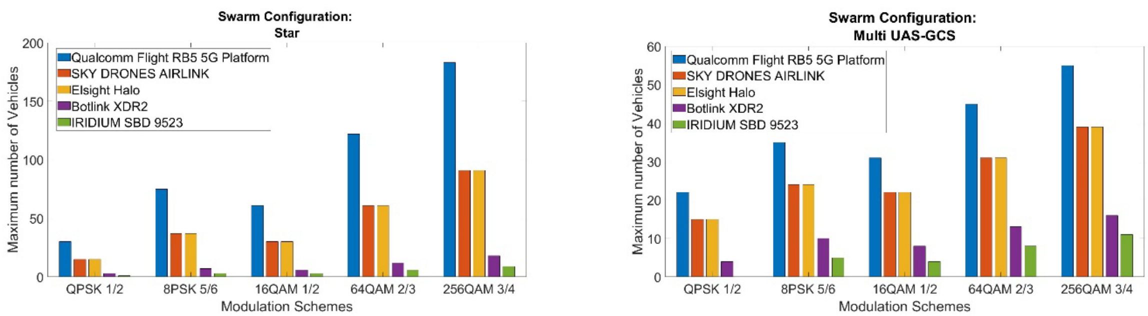


Figure 8. Maximum number of vehicles for C2 products for Star (left) and Multi-UAS-GCS (right) swarm configurations.

4.6 Task 6.2 Conclusion

In the second year of this study, five C2 systems were selected from Sub-task 6.1 to assess and compare their performance. The peak bandwidth demand was calculated for both single aircraft as well as for UA swarms in five different configurations. Additionally, theoretical bandwidth limits were estimated for each of these systems which was instrumental in estimating the practical maximum number of UA that could be effectively managed by a single C2 solution within a specified operational volume.

As part of this subtask, the research group studied various phenomena that sub-optimized the bandwidth availability. While prior studies attempted to study bandwidth sub-optimization, they focused on limited phenomena. In this investigation, we considered an exhaustive set of phenomena including pathloss, Doppler shift, multipath propagation, interference, and atmospheric weather conditions, each of which independently impacts bandwidth availability. Pathloss simulation results indicated that increasing the distance between transmitter and receiver increases the pathloss and BER; and increasing the frequency with constant distance results in increased pathloss, BER, and reduced SNR at the receiver.

Higher UA speeds caused an increase in Doppler shift. Thus, synchronization issues become more challenging at higher speeds and result in higher BER. Increased carrier frequency offset caused by Higher Doppler shift also results in increased IQ constellation distortions and BER for a given distance, frequency, and modulation order. Additionally, for any given combination of distance, modulation order, and speed, higher BER is observed at a higher frequency.

Interfering signals act as noise, and an increase in frequency overlap between the received signal and interfering one causes an increase in BER. Higher BER is seen with higher-order modulation for a given interference power and frequency overlaps. This is due to reduced energy per bit and reduced Euclidean distance between the constellation points associated with higher-order modulation.

For the multipath phenomenon, an increased number of paths of the original signal causes an increase in the randomness of the received signal's power delay profile. The variation of objects and obstacles creates different fading characteristics. For example, flat fading impacts all frequency components nearly uniformly, whereas frequency-selective fading impacts only specific frequency components. Additional negative effects of multipath include increased inter-symbol interference and BER for Encoded messages of longer durations.

Attenuation caused by atmospheric gases increases with propagation, distance and frequency. Additionally, as the precipitation increases, atmospheric attenuation also increases. The results show that variations in temperature and pressure have a minimal impact on attenuation when propagation distances are small, and within line of sight. They also show that atmospheric attenuation is mainly dependent on distance, frequency, and precipitation, which causes an increase in BER. Attenuation peaks and higher BER are observed at 22 GHz and 60 GHz due to resonant absorption by water and oxygen molecules at these frequencies. It was also observed that attenuation caused by clouds/fog is higher than the attenuation caused by standard atmospheric conditions.

Meanwhile, the attenuation caused by rain still exceeds that of clouds/fog, causing a bigger increase in BER. This could be explained by the larger size of raindrops leading to increased scattering and energy absorption. Effects of phase dispersion and scintillation caused by atmospheric variation become more significant at higher order modulation due to its effect on signal energy and phase. This effect is apparent with the shrinkage of symbol boundaries because more symbols have to be accommodated in the same space, causing higher BER.

In summary, while each phenomenon impacts bandwidth availability independently, in realistic scenarios, they can impact it collectively. In this study, the research team also performed simulations combining several phenomena to measure the BER and other metrics. Observations showed that BER is highly dependent on the environment. For the same propagation distance, pathloss varies significantly across rural, sub-rural, and urban areas. Further, different use cases may demand different UA speeds, subjecting them to different levels of Doppler shifts. They may also be subject to line of sight (LOS) and non-line of sight (NLOS) flight conditions, causing them to experience different types of fading. The addition of mmWave spectrum in 5G has promoted the use of smaller cells, necessitating more frequent reuse of frequencies within a smaller geometric area. This exposes the UA to an increased level of interference. Last but not least, UA are required to operate in a wide range of environmental conditions.

5 TASK 6.3 – C2 FLIGHT TESTING

5.1 Task 6.3.1 – Select and Procure Commercial C2 Systems

The evaluation process that stemmed from the C2 technology survey in Year 2 resulted in a selection of initial C2 products that could be evaluated during flight tests. The final equipment inventory was the result of a process of changes, prioritizing their suitability and availability for integration on available flight platforms. During the acquisition and integration process for the initially selected devices, issues were encountered that resulted in dropping some of them from consideration and in some cases required the sourcing of new C2 systems to evaluate. By the end of the integration process, three C2 devices were selected that represented the three main types of communication technologies being tested including 4G, 5G, and satellite as shown in Table 11 and Figure 9.

Table 11. Flight tested C2 systems.

C2 Product	Supported Communication technologies	Frequency Bands	Size	Weight
Botlink XRD2 4G Modem	4G	B Band: LTE CAT 4 FDD B2[1900], B4[1700], B12[700], B13[700], B14[700], B66[1700], B71[600].	25.4 x 68.6 x 58.6 mm	83 g (2.93 oz)
Botlink XRD2 Telit 5G Modem FN920C04	5G	N Band: 5G Sub.6 FDD and TDD operation in 5G NR	30 x 42 x 2.3 mm	83 g (2.93 oz)
Skylink 7100	Satellite	L Band: Iridium Certus 100 services	127 x 203 x 32 mm	725.75 g (25.6 oz)

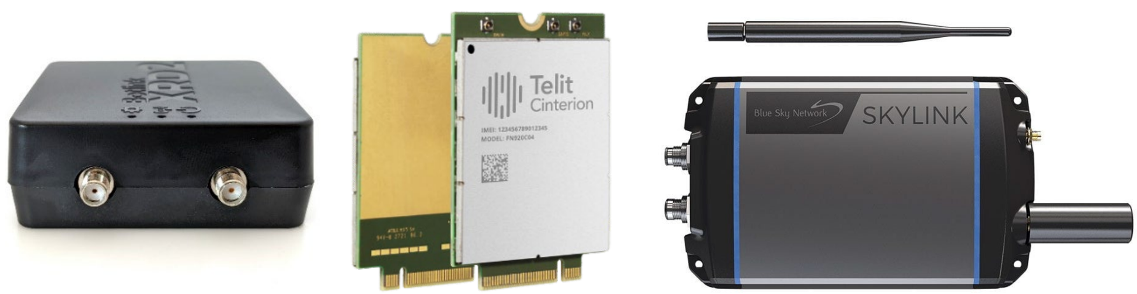


Figure 9. Tested C2 systems: Botlink XRD2 (Left), Telit 5G Modem (Middle), and Skylink 7100 (Right).

5.2 Task 6.3.2 – Integrate Selected C2 Systems

UAS selection followed, as with the payloads, an iterative process, testing one UAS after the other from payload integration to initial stability and systems flight testing. After one or another inadequacy was exposed during this process, the team chose a different UAS platform. The most difficult component to integrate proved to be the Skylink C2 system. In a commercial environment, a fully integrated C2 system would presumably not require the XRD2 for operation, saving weight. However, the Skylink system remains a fairly large one and this has an impact on the UAS that can support satellite C2 capable aircraft. As described, it proved to be the final limiting factor on successful integration, requiring the research team to cycle through several potential UAS and this fact should be taken into consideration when classifying potential UAS using satellite communications for operation.

Other major issues to reiterate, compiled in Table 12, were the GPS accuracy issues exhibited by the Acecore Zoe that was mitigated with a new GPS unit and the X8 sluggish response and higher than expected wind susceptibility. While this primarily affected the Skylink satellite system, this behavior was an early indicator that the X8 might not perform reliably even with lighter payloads. These issues were only finally solved by adopting the M600 as the final UAS test platform.

Table 12. Candidate UAS Platforms Specifications.

	Acecore Zoe	**X8 Octocopter**	**DJI M100**	**DJI M600**
Flight Time	47 Minutes	30 Minutes	40 Minutes	40 Minutes
Max Take Off Weight	23.15 lbs (10.5 kg)	22 lbs (10 kg)	7.93 lbs (3.6 kg)	33.3 lbs (15.1 kg)
Max Payload Weight	9.26 lbs (4.2 kg)	17 lbs (8 kg)	2.2 lbs (1 kg)	12.1 lbs (5.5 kg)
Wind Resistance	30 knots (15.4 m/s)	13 knots (6.7 m/s)	19.44 knots (10 m/s)	15.6 knots (8 m/s)
Flight Testing Issues	• GPS accuracy is insufficient for proper testing. • Exhibited flight instability due to size and weight of Skylink payload. • Flight time significantly reduced due to payload weight.	• Exhibited sluggish speed and unsteady flight due to weight of payload. • Higher susceptibility to wind gusts resulting in frequent groundings. • Flight time significantly reduced due to payload weight.	• Unsteady during flight due to size and weight of Skylink payload. • Unable to reach altitude with the Skylink due to its weight. • Flight time significantly reduced due to payload weight.	• No Issues

The biggest issue during the integration process for the C2 systems was the size and weight of the Satellite C2 system. As briefly mentioned, this prompted consideration of the need for small UAS subclasses besides the simpler taxonomies used in 14 CFR Part 107. The issue shows that depending on the size and weight of the C2 system, larger UAS may be required and need to be identified. To address this problem, the team classified the UAS candidates tested for this project using the NATO UAS classification, shown in Table 13, as a basis to determine what class of UAS works with a C2 systems for flight testing.

Table 13. Candidate UAS Platform NATO Classification.

C2 System	**Max Take Off Weight**	**Nato Classification**
Acecore Zoe	23.15 lbs (10.5 kg)	Class I – Mini (< 15kg)
X8 Octocopter	22 lbs (10 kg)	Class I – Mini (< 15kg)
DJI M100	7.93 lbs (3.6 kg)	Class I – Mini (< 15kg)
DJI M600	33.3 lbs (15.1 kg)	Class I – Small (15kg < weight < 150kg)

Based on this UAS classification, Table 14 shows the minimum UAS class required for the tested C2 systems. The 4G and 5G C2 systems could be flown on the Class I - Mini UAS platforms but the Satellite C2 system requires stepping up to a Class I - Small UAS platform to accommodate its size and weight. In the future, this could be used as a method of classifying limits on which aircraft may support which C2 technologies.

Table 14. C2 System Required UAS Platform Class.

C2 System	Size	Weight	Power	Minimum UAS Class and Category
Botlink XRD2	1 x 2.7 x 2.3 in (25.4 x 68.6 x 58.6 mm)	0.18 lbs (83 g)	• Typical Power: 2.5 W • Peak Power: 20.5 W	Class I – Mini
Telit 5G Modem	1.2 x 1.7 x 0.1 in (30 x 42 x 2.3 mm)	0.18 lbs (83 g)	• Typical Power: 4 W • Peak Power: 14 W	Class I – Mini
Skylink 7100 (Iridium)	5 x 8 x 1.3 in (127 x 203 x 32 mm)	1.6 lbs (726 g)	• Typical Power: 7 W • Peak Power: 18 W	Class I – Small

5.3 Task 6.3.3 – Define Flight Test Operations

Each flight test day was performed within a 3-hour window with all three C2 systems being tested in order to keep the environmental conditions similar between the tested C2 systems. Flight tests were performed in a holding pattern with the drone flying at a minimum height of 300 ft and with the drone reaching at least 1,500 ft from the ground position at a slant range distance, as shown in Figure 10. For each system tested, a minimum flight duration of 10 minutes with the drone flying at its highest possible speed was required for adequate data collection.

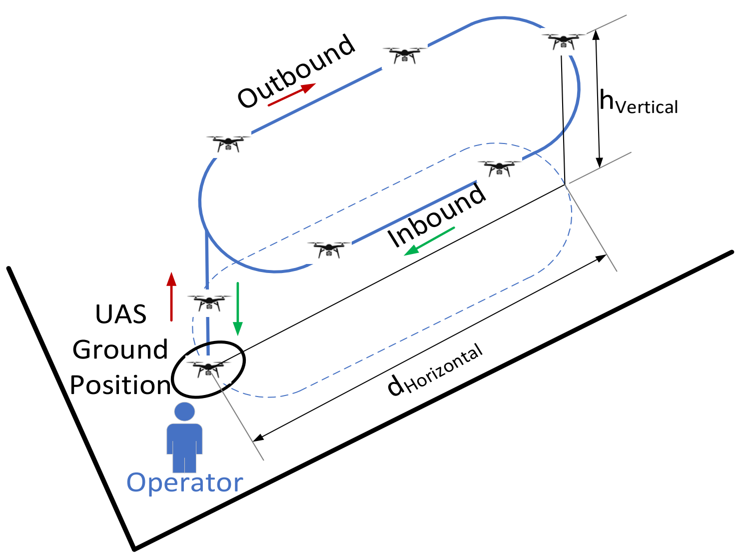


Figure 10. Flight Test Operation Pattern and Requirements.

Flight tests were conducted over a period of three days at three different locations: rural, suburban, and urban environments. This approach addresses the necessity to evaluate and compare performance variations resulting from potential pathloss and interference which arise from different infrastructure densities. These include the effects of buildings, trees, and other obstacles present on the path of signal propagation, as well as sources of electrical and communications infrastructures. The modeling and estimation related to these factors is detailed in the Year 2 report.

5.4 Task 6.3.4 – Define Performance Criteria

During integration of the 5G and Satellite systems, the research team determined that they could not provide all of the required signal and performance data for the original set of test metrics based on the 4G modem outputs shown in Figure 11. The 5G C2 system provided less data than the 4G C2 system, as shown in Figure 12. The satellite C2 system provided even less data than the 5G with additional signal and packet information missing compared to the 5G system as shown in Figure 13.

Timestamp	Modem Model	APN	CPU Serial	Latitude	Longitude	Altitude	RSSI	RSRQ	RSRP	SNR	RSCP	ECIO	Connected Tower	Neighboring Towers	RxBytes	RxPackets	RxPacketsDropped	TxBytes	TxPackets	TxPacketsDropped
1741279446	QUALCOMM IN			4.8E+08	-9.68E+08	258660	-73	-12	-100	7.6	0	0	[NET: T-Mobile RSI	[[RSRP:-111 RSRQ:-14	552	5	0	220	3	0
1741279447	QUALCOMM IN			4.8E+08	-9.68E+08	258710	-73	-12	-100	7.6	0	0	[NET: T-Mobile RSI	[[RSRP:-119 RSRQ:-13	880	8	0	791	8	0
1741279448	QUALCOMM IN			4.8E+08	-9.68E+08	258730	-73	-12	-100	7.6	0	0	[NET: T-Mobile RSI	[[RSRP:-108 RSRQ:-14	9440	27	0	3928	30	0
1741279449	QUALCOMM IN			4.8E+08	-9.68E+08	258780	-73	-12	-100	7.6	0	0	[NET: T-Mobile RSI	[[RSRP:-109 RSRQ:-13	17538	46	0	8989	52	0
1741279450	QUALCOMM IN			4.8E+08	-9.68E+08	258820	-70	-13	-100	4.6	0	0	[NET: T-Mobile RSI	[[RSRP:-103 RSRQ:-11	21344	60	0	10153	65	0

Figure 11. 4G Log Data for Botlink XRD2.

Timestamp	Modem Model	APN	CPU Serial	Latitude	Longitude	Altitude	RSSI	RSRQ	RSRP	SNR	RSCP	ECIO	Connected Tower	Neighboring Towers	RxBytes	RxPackets	RxPacketsDropped	TxBytes	TxPackets	TxPacketsDropped
1740691201	FN920C04-WW	T-Mobile		4.8E+08	-9.71E+08	258160		-11	-81	12.5			#MONI T-Mobile	NR_BAND:25 NR_BW:1	56	1	0	80	2	0
1740691202	FN920C04-WW	T-Mobile		4.8E+08	-9.71E+08	257990		-11	-81	12.5			#MONI T-Mobile	NR_BAND:25 NR_BW:1	56	1	0	80	2	0
1740691203	FN920C04-WW	T-Mobile		4.8E+08	-9.71E+08	257920		-11	-81	12.5			#MONI T-Mobile	NR_BAND:25 NR_BW:1	56	1	0	80	2	0
1740691204	FN920C04-WW	T-Mobile		4.8E+08	-9.71E+08	257920		-11	-82	12.5			#MONI T-Mobile	NR_BAND:25 NR_BW:1	56	1	0	80	2	0
1740691205	FN920C04-WW	T-Mobile		4.8E+08	-9.71E+08	257560		-11	-82	12.5			#MONI T-Mobile	NR_BAND:25 NR_BW:1	56	1	0	80	2	0

Figure 12. 5G Log Data for Telilt 5G C2.

Timestamp	Modem Model	APN	CPU Serial	Latitude	Longitude	Altitude	RSSI	RSRQ	RSRP	SNR	RSCP	ECIO	Connected Tower	Neighboring Towers	RxBytes	RxPackets	RxPacketsDropped	TxBytes	TxPackets	TxPacketsDropped
1740694757	Skylink 7100			4.8E+08	-9.71E+08	247300			-103						166			30		
1740694758	Skylink 7100			4.8E+08	-9.71E+08	247100			-103						166			30		
1740694759	Skylink 7100			4.8E+08	-9.71E+08	247300			-103						166			30		
1740694760	Skylink 7100			4.8E+08	-9.71E+08	247200			-102						166			298		
1740694761	Skylink 7100			4.8E+08	-9.71E+08	247200			-102						166			298		

Figure 13. Satellite Log Data for Skylink 7100.

Metrics that were initially selected were based on the logging information provided by the Botlink C2 system. The team revised the metric list to accommodate the outputs that the Skylink system provides and still stems from those adopted from Year 1 and used during the evaluation and selection of C2 systems. The selection of nine metrics resulted from an evaluation process used to gauge the overall quality and performance of a given C2 system communication signals. The specific cellular network C2 systems (4G and 5G) have additional metrics that can be calculated such as reference signal received power (RSRP) and reference signal received quality (RSRQ). However, these specific metrics are not applicable for the Skylink Satellite C2 system, so a more generalized set of metrics based on the ones used during the initial C2 system search and selection were used, as shown in Table 15 below.

Table 15. Flight Test Performance Metrics.

Parameter	Description
RSSI (Received Signal Strength Indicator)	Linear average of total received power from all sources, including co-channel non-serving and serving cells, adjacent channel interference and thermal noise, within measurement bandwidth over N number of resource blocks. Represented by: $$RSSI_k = \frac{1}{I} \sum_{i=kI}^{(k+1)I-1} \left(P_{S,i} + P_{Z,i}\right) \quad (1)$$

SNR (Signal to Noise Ratio)	Ratio of signal power to noise power at the receiver
Carrier Frequency	Frequencies and bands the C2 system is utilizing for communication
Latency	Time delay between when a C2 message is sent by the device and when it's received by the operator on the ground
Tx and Rx Throughput	Number of packets or bytes transmitted and received by the C2 system
Security	Available security measures on the C2 system. (encryption, anti-jamming, etc.)
Service Availability	Operational area of the C2 systems underlying communication technology. For an LTE C2 system, this is the coverage area of the LTE network provider.
Multi-User	The number of UAS or ground stations the C2 system can support during operation.
Size, weight, and power (SWaP)	These metrics can be used to determine whether a UAS aircraft is capable of supporting a given C2 system.

5.5 Task 6.3.5 – Execute Flight Tests

Suburban flights were conducted in February 2025, while rural and urban flights completed in March 2025, given adequate winter and early spring weather once all three systems were complete and operating nominally. Flight testing was completed successfully and C2 link data provided for analysis. Some data may indicate minor deviations from planning, but still within the needs and requirements of the research. Examples of photographs of the flight tests are given in Figure 14.

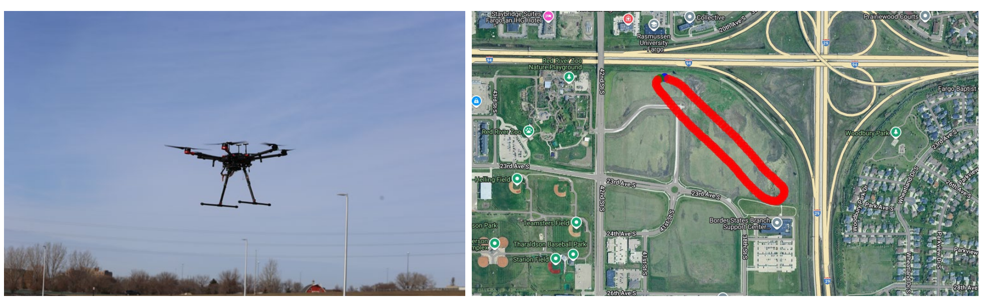


Figure 14: M600 UA during urban flight (left) and path flown (right).

In summary, 4G performed the most reliably across all environments, while 5G may be best suited for suburban areas and may outperform in urban areas given sufficient build-out of the infrastructure. Satellite-based C2 communication, on the other hand, struggled to meet minimum signal requirements, posing reliability challenges for UAS operations with current technology and demonstrating the need for future technological improvements.

For the received 4G data, average volumes are similar across the three flight environments, but rural flights show higher variability, indicating fluctuating bandwidth. Suburban and urban flights maintain more consistent bandwidth. Transmitted 4G data shows urban flights sending high volumes in the first 100 seconds, aligning with higher SNR, suggesting better channel conditions for data transmission. 4G results indicate that transmitted volumes consistently exceed received volumes across all environments, highlighting a need for greater bandwidth allocation for transmission.

For satellite communication, low SNR results in significantly lower data rates than 4G and 5G. Sporadic spikes correspond to brief SNR improvements. The consistently low data volumes suggest that satellite communication is unsuitable for UA C2 systems requiring high data rates.

The tested C2 systems had varying feature sets that were sometimes technology specific. As far as service availability goes, the Satellite had the largest coverage area of the three tested and only required a clear view of the sky to operate. The 4G C2 system had the next largest service area due to being a more mature cellular network technology. 5G has the smallest service area but will improve as more 5G infrastructure is installed. For security, all three devices provided some form of signal encryption but did not have any other advanced security features. The number of drones and users supported by the C2 system are dependent on the ground control station or C2 system.

The 4G and 5G modems had similar SWaP due to both of them being modules designed to be installed within an existing C2 system. The satellite C2 system is significantly larger and heavier than the 4G and 5G modems even after they were integrated into the C2 systems with additional subsystems.

The size and weight of the satellite system is the primary reason for the initially selected UAS platforms being unsuitable for flight testing due to stability and safety concerns. This is mainly because the initially selected UAS platforms were Class I – Mini UAS and the satellite C2 system tested requires at least a Class I – Small UAS in order to safely fly. More details about the flight tests results can be found in Year 3 Report.

5.6 Task 6.3 Conclusion

Contemporary Command and Control products integrate a variety of wireless technologies, including 4G, 5G, and satellite-based communication systems. The adoption of these technologies for reliable UA operations is contingent upon several factors, including their physical characteristics (e.g., dimensions, weight), operational reliability, resistance to interference, and onboard security mechanisms. The primary aim of Year 3 research was to establish the flight test operational specifications necessary to gather critical performance indicators and determine the most suitable wireless technologies for C2 communications, undertaking several tasks culminating in the collection and analysis of flight test data.

The flight tests were conducted in rural, suburban, and urban settings, each lasting a minimum of 600 seconds. Key performance indicators collected during these tests included GPS coordinates and wireless signaling metrics such as RSSI, RSRQ, RSRP, SNR, and data transmission and reception volumes.

A thorough analysis of the data suggests that 4G technology offers reliable C2 operation across all three environments. Based on existing infrastructure, 5G technology is more suitable for suburban and urban operations. However, the current satellite communication systems on C2 platforms do not meet the necessary performance criteria due to weak satellite signals. Consequently, the study recommends the utilization of 4G systems for broader coverage and the combined use of 4G and 5G systems for suburban and urban coverage.

6 CONCLUSION, LESSONS LEARNED, AND RECOMMENDATIONS

6.1 Year 1

C2 products vary widely, not just in terms of size, weight, and power, but in supported features such as the number of vehicles and users that are supported as well as the security features on offer. When considering which system to procure, mission needs, from normal operations to a variety of potential emergency operations, must be considered. The capabilities of different communication technologies must therefore be robust and capable across the spectrum of these operations. In the evaluation of available C2 products, the research team identified several gaps in the commercially available systems. For example, very few commercial C2 systems support multi-vehicle control, including swarm configurations. Also, 57.6% of the products surveyed lack any form of cybersecurity against the most common and serious cyberattacks. Also, in developing metrics for normal and cybersecurity features, the research team has created a structure of potential standards usable in future evaluation of C2 systems and to address any technological gaps that remain.

6.2 Year 2

From this survey, five C2 systems and their associated technologies were evaluated extensively in terms of several metrics, including peak bandwidth demand for individual UAS and 5 different configurations of UAS swarms, theoretical bandwidth limits, and maximum number of aircraft a single C2 solution can effectively manage.

This evaluation was expanded to include an in-depth, comprehensive investigation on various phenomena and their associated parameters that sub-optimize bandwidth availability, including path loss, doppler shift, multipath propagation, interference, and atmospheric weather conditions. The individual impact and combined impact of the phenomena identified from this study was evaluated qualitatively and quantitatively using constellation diagrams, received signal power, and BER.

Communication performance was also affected by environmental factors including altitude, flight distance, rain, fog, and atmospheric attenuation. This effect was seen even at lower altitudes and within visual line of sight with the effect become more severe as altitude increased. The reduction in performance was also more pronounced for higher operating frequencies and increased modulation orders which are more vulnerable to adverse weather conditions, Doppler shift, and path loss.

The consequence of these factors established by the research is that mitigating such effects should be prioritized to provide greater resilience toward sub-optimizing factors and combined with anti-jamming techniques and adaptive transmission strategies to provide reliable, robust C2 performance.

6.3 Year 3

C2 systems using 4G, 5G, and satellite link technology were chosen and integrated onto a UAS platform for flight testing. These C2 systems were flight tested on three different days in three operational environments including rural, suburban, and urban. Analysis was performed using nine metrics that evaluated the C2 performance, signal characteristics, security, feature set, and SWaP.

The 4G C2 system performed the best in rural and suburban areas, 5G performed the best in suburban areas, and the satellite system performed the worst out of the tested devices. These flights demonstrated that 4G and 5G can effectively support C2 operations with 4G currently providing the best coverage area but will change as more 5G infrastructure is installed. The satellite C2 system was unreliable for the operations due to its low data rates, poor signal, and high latency.

From the integration and flight testing, it was determined that not all UA systems can support a given C2 payload effectively and the required class of UAS should be taken into consideration during C2 selection. It also showed that wireless performance is heavily influenced by technological limitations and environmental conditions.

The outcomes of the preceding research point to the need to prioritize stability and resilience for a multitude of potential sUAS operations. Not only will the static factors prove important, but the research has established that mitigations are necessary including multi-link redundancy and reliable connectivity under changing meteorological conditions for higher frequency control bands studied, especially 4G and 5G. Satellite communication will need additional studies related to potential enhancements through means such as adaptive antennas or hybrid multi-technology systems. Long-range operations assessment of C2 systems would also be useful for future evaluations. More reliable C2 links can be achieved by refining communication strategies and optimizing UAS selection for future operations to improve UAS mission safety and effectiveness.

PUBLICATIONS

Mishra, Lalan, and Naima Kaabouch. "Impact of Weather Factors on Unmanned Aerial Vehicles' Wireless Communications." *Future Internet* 17, no. 1 (2025): 27.

Mishra, Lalan, Selma Benouadah, and Naima Kaabouch. "Modeling and analysis of pathloss effect on UAS communication signals." In *2024 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1-6. IEEE, 2024.

Mishra, Lalan, Selma Benouadah, J. Alghazo, and Naima Kaabouch. "Interference Effects on Bandwidth Availability for UAV Communications." In *2024 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1-6. IEEE, 2024.

Benouadah, Selma, Lalan Mishra, and Naima Kaabouch. "Doppler shift effect on bandwidth availability for UAV communications." In *2024 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1-6. IEEE, 2024.

Mishra, Lalan, and Naima Kaabouch. "Impact of Weather Factors on Unmanned Aerial Vehicles' Wireless Communications." Future Internet 17, no. 1 (2025): 27.

Mishra, Lalan, and Naima Kaabouch. "Multi-Parameter Optimization Using Metaheuristic Algorithms to Improve Unmanned Aerial Vehicles' Wireless Communications: A Performance Analysis." Submitted to the IEEE Access Journal, Status Pending.

Mishra, Lalan, and Naima Kaabouch. "Communication Standards for UAS: A Key Performance Indicator-based Perspective." Submitted to the WSEAS Transaction on Communications journal, Status Pending.

REFERENCES

Acecore. (2025). Acecore Zoe. Retrieved from https://acecoretechnologies.com/zoe/

ASTM. (2025). *ASTM F3002-14a Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS)*.

Blue Sky Network. (2025). Skylink 5100 and 7100. Retrieved from https://blueskynetwork.com/

Botlink. (2023). XRD2: Connected drones over cellular. Retrieved from https://botlink.com/xrd2

Bullington, K., (1947). Radio propagation at frequencies above 30 megacycles. *Proceedings of the IRE*, 35(10), 1122-1136.

Daemen, J., and Rijmen, V. (1999). AES Proposal: Rijndael.

D. E. Standard. (1999). Data Encryption Standard. *Federal Information Processing Standards Publication*, vol. 112.

DJI. (2025). DJI M100 and M600. Retrieved from https://www.dji.com/

Eldosouky, A., Ferdowsi, A., and Saad, W. (2019). Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. arXiv preprint arXiv:1904.11568.

Elsight. (2023). Unmanned Connectivity. Retrieved from https://www.elsight.com/unmanned-connectivity/

Iridium. (2023). Iridium Core 9523 Module. Retrieved from https://www.iridium.com/products/iridium-core-9523/

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., and Alam, M. (2012). Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. *Proceedings of IEEE Conference on Technologies for Homeland Security (HST)*, pp. 585-590.

Jia, L., Yao, F., Sun, Y., Xu, Y., Feng, S., and Anpalagan, A. (2017). A Hierarchical Learning Solution for Anti-Jamming Stackelberg Game With Discrete Power Strategies. *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 818–821.

Johansson, R., Hammar, P., and Thorén, P. (2017). On Simulation-Based Adaptive UAS Behavior During Jamming. *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, pp. 78-83, doi: 10.1109/RED-UAS.2017.8101647

Jovanovic, A., Botteron, C., and Fariné, P.-A. (2014). Multi-Test Detection and Protection Algorithm Against Spoofing Attacks on GNSS Receivers. *Proc. IEEE/ION PLANS*, Monterey, CA, USA, pp. 1258–1271, May.

Kaabouch, N., Manesh, M.R. and Kenney, J.R., University of North Dakota UND and Raytheon Co, 2022. Detection of spoofing and meaconing for geolocation positioning system signals. U.S. Patent 11,500,109.

Kaabouch, N. and Manesh, M.R., University of North Dakota UND, 2022. Autonomous vehicle control attack detection and countermeasures. U.S. Patent Application 17/183,926.

Manesh, M.R. and Kaabouch, N., University of North Dakota UND, 2024. Detection of cyber attacks targeting avionics systems. U.S. Patent 12,149,560.

Kang, J.-H. and Park, K.-J. (2016). Spatial Retreat of Net-Drones Under Communication Failure. *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, pp. 89–91.

Khanafseh, S., Roshan, N., Langel, S., Chan, F.-C., Joerger, M., and Pervan, B. (2014). GPS Spoofing Detection Using RAIM With INS Coupling. *Proc. IEEE/ION Position Location Navig. Symp.*, pp. 1232-1239.

Khoei, T. T., Ghribi, E., Ranganathan, P., and Kaabouch, N. (2021). A Performance Comparison of Encryption/Decryption Algorithms for UAV Swarm Communications.

Koyama, K., Maurer, U. M., Okamoto, T., and Vanstone, S. A. (1991). New Public-Key Schemes Based on Elliptic Curves Over the Ring Z N. *Annual International Cryptology Conference*, Springer, pp. 252-266.

Luo, S., Zhang, S., Ke, S., Wang, S., Bu, X., and An, J. (2020). Optimum Combining for Coherent FFH/DS Spread Spectrum Receivers in the Presence of Multi-Tone Jammer. *IEEE Access*, vol. 8, pp. 53 097–53 106.

Magiera, J. (2019). A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing. *Sensors*, vol. 2411, pp. 2 – 17.

Mosavi, M. R., Nasrpooya, Z., and Moazedi, M. (2016). Advanced Anti-Spoofing Algorithms in Tracking Loop. *J. Navig.*, vol. 69, no. 4, pp. 883–904, Mar.

Ni, S., Cui, J., Cheng, N., and Liao, Y. 2018: Detection and Elimination Method for Deception Jamming Based on an Antenna Array. *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, p. 150147718774466.

Pärlin, K., Riihonen, T., and Turunen, M. (2019). Sweep Jamming Mitigation Using Adaptive Filtering for Detecting Frequency Agile Systems. *IEEE International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6.

Qualcomm. (2023). Flight RB5 Platform. Retrieved from https://www.qualcomm.com/products/internet-of-things/industrial/industrial-automation/flight-rb5-platform

Quectel. (2025). Quectel RG255C-GL. Retrieved from https://www.quectel.com/product/5g-redcap-rg255c-series/

Rezazadeh, N. and Shafai, L. (2019). A Compact Antenna for GPS Anti-Jamming in Airborne Applications. *IEEE Access*, vol. 7, pp. 154 253–154 259.

Rezgui, G., Belmega, E. V., and Chorti, A. (1978). Mitigating Jamming Attacks Using Energy Harvesting. *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 297–300.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, vol. 21, no. 2, pp. 120-126.

RTCA. *DO-377A Minimum Aviation System Performance Standards (MASPS) for C2 Link Systems Supporting Operations of Unmanned Aircraft Systems in U.S. Airspace*.

Sathaye, H., Lamountain, G., Closas, P., and Ranganathan, A. (2020). SemperFi: A Spoofer Eliminating Standalone GPS Receiver. *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, pp. 353-35.

Sky Drones. (2023). Airlink. Retrieved from https://sky-drones.com/airlink

Telit. (2025). Telit FN920C04. Retrieved from https://www.telit.com/devices/fn920c04/

United States Government Publishing Office. (2020a). *Electronic Code of Federal Regulations Title 14 : Aeronautics and Space Part 107: Small Unmanned Aircraft Systems*. United States Government.

Wang, H., Zhang, P., Li, J., & You, X. (2019). Radio propagation and wireless coverage of LSAA-based 5G millimeter-wave mobile communication systems. *China Communications*, 16(5), 1-18.

Zhang, L., Huang, L., Li, B., Huang, M., Yin, J., and Bao, W. (2019). Fast-Moving Jamming Suppression for UAV Navigation: A Minimum Dispersion Distortionless Response Beamforming Approach. *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7815–7827.