Impact of the Electromagnetic Environment on UAV’s Datalink

I. Bennageh*, H. Mahmoudi and M. Labbadi

Department of power electronics, intelligent control techniques, automation and robotics, Mohammed School of Engineers, Mohammed V University of Rabat, Morocco

E-mail: imranebennageh@research.emi.ac.ma

Abstract-The deployment of drones for any mission relies heavily on a ground control system. The UAV must therefore maintain a stable datalink with the ground control station to allow it to be controlled in real time by the ground operator. The evolution of drones in specific electromagnetic environments can seriously compromise data linkage, giving rise to electromagnetic susceptibility (EMS) issues. This article presents a review of the exploratory literature of electromagnetic interferences that the datalinks between UAVs and the ground station can face from the point of view of electromagnetic compatibility (EMC). The goal is to understand the effects of a given EM environment on the datalinks of an UAV system in order to predict its behaviour and perform the necessary precautions and improvements.

1. INTRODUCTION

Today, the influx of connected electrical systems into the environment we live in has allowed a wide spectrum of electromagnetic waves to propagate at different frequencies and powers. Each country regulates the use of the electromagnetic spectrum through some special organizations. All this to say that the environment in which we live already presents a place characterized by noise in its various colours [1]. The introduction of drones in such an environment greatly reduces its performance in terms of datalink (Ground Control datalink, Video datalink, GPS datalink, etc.). In order to predict its behaviour, several research works have relied on analytical, experimental and simulation approaches, putting drones under different conditions.

An electromagnetic disturbance can become embedded within the drone by two coupling paths: Front door (through the antenna) and Back door (through channels not intended for receiving RF energy). It has been shown by [2] that most of the interferences of UAVs come from its reception system (Antenna) or through the “Front Door”. This will therefore be the subject of this article. Very little research concerns the electromagnetic susceptibility of the UAV system datalinks. This document aims to provide the essential points relating to the electromagnetic environment likely to interfere with the UAV datalinks and reduce its performance, based on a detailed analysis of the related literature. To this end, the present work is organized as follows. Section 2 proposes to characterize the studied system taking into account the types of drones, the datalinks and the physical communication layer. Section 3 provides an overview of the different environments for which the UAV is deployed, as well as the sources of intentional and unintentional radiated electromagnetic interference. Section 4 proposes the means of measuring the quality of the datalink and the characteristics that should be taken into account to improve its performance. Finally, conclusions and future works are presented in section 5.

2. UAV: TYPES, DATALINK AND TRANSMISSION TECHNIQUES

In the literature, there are several criteria regarding the categorization of drones. Thus, for [5], a drone can be categorized according to the following criteria:

- Type of wing: fixed, multirotor or hybrid
- Autonomy: from a few minutes to tens of hours
- Size: from the size of a mosquito to the size of commercial airplanes
- Weight: from a few grams to hundreds of kilograms
- Energy source: solar energy, battery or fuel.

Whether the drone is one type or another, the common thread remains the same: a drone uses datalinks to operate without a pilot on board. In case of a breakage of an important datalink, there is often a back-up system to recover the UAV. The main types of datalinks are as follow [6]:

- GCS datalink: Datalink between the UAS and Ground Control Stations (GCS)
- GPS datalink: Datalink between the UAS and GPS satellites
- UAS datalink: Datalink between an Unmanned Aerial System and other aircraft
- ADS-B datalink: Datalink between the UAS and ADS-B ground stations

Of course, there are many other types of datalinks. However, particular importance will be given to the GCS datalink, as it is the most widely used main datalink in the majority of drones. It ensures communication between a drone and its ground control station. Communication between a ground station and a drone (for telemetry, control or video stream data) in “Line of Sight”
(LoS) mode is based on frequency waves generally belonging to the L, S and C bands. In “Beyond Line of Sight” (BLoS) mode, the datalink requires much higher frequencies (Ku, K and Ka band). In this physical communication layer (Open Systems Interconnection model), several transmission techniques can be applied to strengthen this type of datalink:

- Transmission techniques (antenna side):
  - SISO: Single Input Single Output (01 transmitting antenna and 01 receiving antenna)
  - SIMO: Single Input Multiple Output (01 transmitting antenna and several receivers)
  - MISO: Multiple Input Single Output (several transmitting antennas and 01 receiving)
  - MIMO: Multiple Input Multiple Output (several transmitting antennas and several receiving)

- Transmission techniques (EM wave):
  - FHSS: Frequency Hopping Spread Spectrum
  - DSSS: Direct-Sequence Spread Spectrum
  - THSS: Time Hopping Spread Spectrum
  - CSS: Chirp Spread Spectrum

- Modulation techniques:
  - FM: Frequency Modulation
  - ASK / FSK / PSK: Amplitude / Frequency / Phase Shift Keying
  - BPSK: Bit Phase-Shift Keying
  - QPSK: Quadrature Phase-Shift Keying
  - QAM: Quadrature Amplitude Modulation

- Multiplexing techniques:
  - FDM: Frequency-Division Multiplexing
  - OFDM: Orthogonal Frequency-Division Multiplexing
  - TDM: Time-Division Multiplexing
  - CDMA: Code-Division Multiplexing

- Encryption technique:
  - AES: Advanced Encryption Standard

Given the remarkable progress in terms of transmission techniques, the manufacturer is faced with a wide range of choices. As a result, the decision on the method of modulation, transmission and data protection becomes a rather delicate exercise for the engineer in charge of the project. Indeed, it must collect the various data on the environment in which the drone is predestined.

3. ELECTROMAGNETIC ENVIRONMENT

3.1 Noise and interferences

A drone can accomplish various missions such as the surveillance of the high voltage transport lines, catenaries, radioactive emission installations, borders of an area or a country, and many other missions. Note that workplaces can have very disparate EM characteristics, depending on the strengths of the electric and magnetic fields there. The presence of these electromagnetic fields generates noise for the transmission of UAS datalinks. Thus, it alters the communication between the drone and the ground station, causing a reduction in the performance of the drone.

Noise can be classified differently, and this, according to various criteria. For example, depending on its frequency range, for [7], the noise can be classified as:

- Narrowband noise: a noise with a restricted bandwidth
- White noise: random noise at flat or spread power over the entire frequency spectrum
- Band-limited white noise: noise with a bandwidth limited to a spectrum of interest
- Coloured noise: non-flat spectrum noise, where the power is concentrated at a determined bandwidth. For example, we find red, pink, brown, blue noise, etc.
- Impulsive noise: short-term impulse noise of random amplitude and duration
- Transient noise pulses: Long duration noise pulses

For drones, the EM interference can be divided into two main categories depending on its origin:

- Unintentional interference: this is natural noise (thermal, lightning, cosmic, etc.) or from electrical and radio equipment (television, radio, radar, etc.)
- Intentional interference: This is any source of noise targeting the equipment (a drone in this case) to cause electromagnetic interference. It is the very basis of all jamming instruments.

3.2. Jamming techniques:

There are dozens of electromagnetic jamming techniques. It is therefore important to know these techniques for an UAS manufacturer in order to put in place the necessary measures to completely override most of them.

It should be noted that the two concepts “interference” and “jamming” induce the same physical consequences. Their difference lies in the context in which they are evoked. Thus, the term “interference” is used when the topic concerns the EMC, while the term "jamming" is used in the field of electronic warfare.

Moreover, [8] organized the types of interference as described in fig.1.
Fig. 1 – Most important types of jammers

- **Proactive**: the jammer is always active
  - **Constant Jammer**: Sends packets of incomprehensible random bits
  - **Deceptive Jammer**: Sends understandable but false packets
  - **Random Jammer**: Can send regular or random packets and pseudo-periodically switch between activity and passivity to save energy

- **Reactive**: Activates as soon as a transmission on a given channel is detected
  - **RTS / CTS Jammer**: Request To Send / Clear To Send. The Jammer waits for the receiver to send RTS to distort it and prevent it from reaching the transmitter
  - **Data / ACK Jammer**: Acknowledgment of Package. After the transmission from the transmitter, the jammer can scramble the transmitted message. Otherwise, it scrambles the reception confirmation message from the receiver causing a “buffer overflow” at the level of the transmitter which will continue to send the same message indefinitely.

- **Function-Specific**: The Jammer can operate on multiple channels
  - **Follow-on Jammer**: Scrambles several channels for a short period of time, in a random manner and at high speed (effective against FHSS modulation with slow hopping rate)
  - **Channel-hopping Jammer**: Jumps between multiple channels to jam multiple tracks simultaneously
  - **Pulsed-noise Jammer**: Can jam multiple channels with different bandwidths over multiple periods of time. It turns on and off automatically to conserve energy

- **Smart Hybrid Jammer**: these jammers can alter an entire network by using the energy wisely:
  - **Control channel Jammer**: targets the control channel in a multi-channel communication network. Altering the control channel can cause severe damage to all channels on the same network
  - **Implicit Jammer**: after deactivation of the intended target, this jammer passes to other nodes of the network to cause a denial-of-service state
  - **Flow Jammer**: Takes information from the network layer to block the flow of network traffic by multiple jammers

**3.3. Noise model**

In order to reproduce the different types of noise, it is not cost-effective to procure the same noise source for testing with the UAS under test. Easily reproducible noise models are used to come close enough to real effects. Thus, most of the simulation models rely on mathematical models. Most noise models are statistically based, and come in the form of noisy channels:

- **AWGN (Additive White Gaussian Noise)**: In information theory, this model is often used for its simplicity in solving complex problems. It is used to model a channel whose component will be added (additive) to the signal being studied. White noise is uniform (white) with a Gaussian distribution. In reality, all of these parameters change.
- **Rayleigh channel**: This is a mathematical model which takes into account the phenomena resulting from multiple signal propagation paths. This channel takes into account the phenomena of multiple reflections, fading, fluctuations and the
Doppler effect.
- HMMs (Hidden Markov models): the non-stationarity of noise induces that its statistical parameters such as the mean, the variance and the power vary over time. The HMM is a series of stationary models marking the different states of noise over time.
Many other models exist to suit specific situations for the studied environment.

3.4. EMC Level indicator
Having learned about the types of interference that a drone can face, as well as some methods of modelling them, we now place ourselves in the context of the EMC of UAV datalinks.
Currently, no recognized standard such as RTCA DO-160G or MIL-STD-461G addresses EMC issues specific to drones. Therefore, studies, evaluations and EMC tests are carried out on the components of the drone for its certification. It is therefore eligible to be situated in this context.
For [9] the problems of EMC for electrical equipment can be divided into 03 broad categories:
- Intra-system EMC issues: compatibility problems inherent to the internal components of the studied system
- Inter-system EMC issues: compatibility problems between several studied systems
- EMC issues between the system and the environment: problems relating to attacks on the environment to the system studied.
The last issue perfectly illustrates our scenario, which is the EMC study of the drone datalink in an EM environment.

3.5. Coupling paths for the Electromagnetic Interference (EMI)
As mentioned above, there are two radiated coupling paths of EM interference from an EMC point of view:
- Front-door: interference enters the victim's circuits through his RF energy reception path (antenna or receiver). It constitutes the main EM interference coupling path for a drone [10][11].
- Back-door: Interference becomes embedded in the victim's internal system through channels that are not designed for receiving RF energy (electronic speed controllers (ESC), flight controller, etc.). Usually, a very high-power EM disturbance must be injected to be able to destabilize a drone by this route.

In order to ensure that the Front-door is the main coupling-path for the penetration of EM disturbances, the following experiment can be carried out either in OATS (Open area Test Site) or in an anechoic chamber:

Fig. 2 – UAV’s Front-Door interference test setup

In the experiment, the aerial channel (transmission by antennas) between the drone and the ground station is replaced by a wired channel (transmission by shielded coaxial cable). Here are some guidelines for the experiment:
- The drone must be fixed to avoid its movements
- We must have an indicator of the state of the UAV datalink. The majority of GCUs have this functionality.
Otherwise, the interruption of communication will prevail
- The EM interference generator must be able to generate a sufficiently large electric field (around 200 V/m in continuous) and sweep the working frequency (L, S and C band)

Carrying out the experiment using the 02 above-mentioned channels gives the following results:
- Via the air channel: Communication must be interrupted for a given interference power, especially if the frequency of the disturbing signal is close to the working signal [4]
- By the wired channel: Communication must remain maintained even for an amplitude field of 200 V / m continuously.

The components of the UAV forming the receive and transmit path (antenna, duplexer, amplifier, transmitter and receiver) of the datalink is the main element that is susceptible to the EM environment [4]. Efforts must be directed towards this terminal in order to increase its electromagnetic susceptibility threshold as much as possible. To this end, we must have the means to measure the right parameters in order to act effectively.

4. DATALINK ENHANCEMENT

4.1. Quality parameters for the datalink

There is no specific mathematical expression based on given parameters of a system to determine its EMC level, much less the electromagnetic susceptibility (EMS) of a UAV datalink. Several research works are still in progress to find the indicators that objectively reflect the overall EMC level of a system. This is the case for a research team at Beihang University in China. The researchers were able to provide a preliminary result, after 10 years of research, for the definition of an indicator of the overall EMC of a system based on the following parameters: electromagnetic susceptibility, electromagnetic emission, isolation, and safety margin.

The means currently available consist of measuring certain parameters of the signal of the system studied (datalink in our case) to form an idea of its EM susceptibility. Among these parameters, we cite:
- RSSI (Received Signal Strength Indicator) [3]
- SNR (Signal to Noise Ratio) [11]
- SIR (Signal to Interference Ratio) [12]
- SINR (Signal to Interference and Noise Ratio): Combination of SIR and SNR.
- SINAD (Signal to Interference, Noise and Distortion Ratio)
- BER (Bit Error Rate) [13]

BER is certainly the best suited parameter for evaluating the performance of communication between a drone and its ground station. Indeed, the data transmission between the drone and the ground station is done by digital data packets transmitted by the various binary modulation techniques mentioned above (BPSK, QAM, OFDM, ...). The BER measures the number of erroneous bits in a unit of time for a transmission. As a result, we can know the critical BER level where the datalink fails.

SINR also gives satisfactory results. The advantage of this technique lies in the ease of measuring the powers of noise (unintentional) and interference (intentional generated by a source).

4.2. Improvement of the electromagnetic susceptibility

As demonstrated in the previous section, the dedicated circuit for receiving and transmitting RF energy in a drone is the primary coupling path for radiated electromagnetic interference. The improvement of the EMS of the datalink can be granted by various means:
- Shielding of all the components of the reception / transmission equipment and the antenna on the drone;
- Installation of filters at the reception / transmission terminal of the drone
- Conceal the datalink in the environment using spread spectrum techniques
- Protect physically the ground station by securing a perimeter against users of equipment generating EM disturbances
- Knowing the EM environment to be flown over as well as the drone's EMS threshold will allow the vector to be kept under control without any unexpected loss of communication

More specifically still, [14] states that there are 07 properties that a UAS Datalink must have:
1. Global Radio Frequency Functionality and Adaptability
2. Resistance to unintentional interference
3. Low Probability of detection and interception: achievable by several techniques: FHSS, DSSS, etc.
4. Signal Encryption and Security: To thwart hacking operations such as Maldrone, GPS Spoofing and Zigbee.
5. Anti-Deception Capability
6. Anti-Radar Missile (ARM) Resistant Capability
7. Anti-Jam Capability
The measures to protect the drone's datalink or to improve the drone's EMS threshold may vary from one UAS to another depending on its type and the environment for which it is intended.

5. CONCLUSION
The electromagnetic environment is the main source of interference for the drone datalink. It was introduced that any type of UAS uses different types of datalink protected by different techniques against noise as well as intentional interference. It was also noted the multitude of noise sources as well as interference techniques that the EM environment could present. It is therefore obvious to model these noisy channels by models approaching the studied channel as closely as possible. In order to target the component of the UAV that is susceptible to the radiated electromagnetic interference, an adequate experimental bench is made. It appears that the components dedicated to the reception / transmission of RF signals constitute the main gate for this type of interference. Therefore, we must quantify the data transmission parameters to come out of the threshold of electromagnetic susceptibility of the datalink studied. Based on this crucial data, the manufacturer can realize several means to strengthen the datalink. Finally, in the next work, a study will focus on the statistical estimation of the EMS to be able to refine the results and predict in advance the loss of the dynamic datalink.

ACKNOWLEDGEMENT
The authors would like to gratefully acknowledge the extremely helpful comments from the anonymous reviewers.

REFERENCES
[1] M. F. da Silva, L. M. Honório, A. L. M. Marcato, V. F. Vidal, and M. F. Santos, “Unmanned aerial vehicle for transmission line inspection using an extended Kalman filter with colored electromagnetic interference,” ISA Trans., vol. 100, 2020, doi: 10.1016/j.isatra.2019.11.007.
[2] P. Kay, “EMC Considerations for Unmanned Aerial Vehicles,” in Handbook of Aerospace Electromagnetic Compatibility, 2018.
[3] J. Dixon, V. Rajamani, and C. Bunting, “Performance test of unmanned aerial systems communication links in a severe multipath environment,” in IEEE International Symposium on Electromagnetic Compatibility, 2016, vol. 2016-September, doi: 10.1109/ISEMC.2016.7571763.
[4] Y. Chen, D. Zhang, E. Cheng, and X. Wang, “Investigation on susceptibility of UAV to radiated IEMI,” 2018, doi: 10.1109/ISEMC.2018.8393875.
[5] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, “Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments,” 2016.
[6] M. Riahi Manesh and N. Kaabouch, “Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,” Computers and Security, vol. 85, 2019, doi: 10.1016/j.cose.2019.05.003.
[7] S. Vaseghi, “Chapter 12, Advanced Digital Signal Processing and Noise Reduction, Second Edition,” Adv. Digit. Signal Process. Noise Reduction, Second Ed., vol. 9, no. c, 2000.
[8] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, 2014, doi: 10.1504/IJAHUC.2014.066419.
[9] D. Su, S. Xie, F. Dai, Y. Liu, and Y. Jia, Theory and methods of quantification design on system-level electromagnetic compatibility. 2019.
[10] Y. Wang, L. Ma, and Z. Meng, “Effects of UWB electromagnetic pulse on UAV data link system,” in IEEE International Symposium on Electromagnetic Compatibility, 2019, vol. 2019-November, doi: 10.1109/ISEMC48616.2019.8986049.
[11] D. Zhang, E. Cheng, H. Wan, X. Zhou, and Y. Chen, “Prediction of Electromagnetic Compatibility for Dynamic Datalink of UAV,” IEEE Trans. Electromagn. Compat., vol. 61, no. 5, 2019, doi: 10.1109/TEMPC.2018.2867641.
[12] D. Zhang, M. Zhao, E. Cheng, and Y. Chen, “GPR-Based EMI Prediction for UAV’s Dynamic Datalink,” IEEE Trans. Electromagn. Compat., pp. 1–11, 2020, doi: 10.1109/TEMPC.2020.3000919.
[13] J. G. Wang et al., “Suppressing Intentional Electromagnetic Interference (IEMI) in Wireless Communication System Using Complex Signal Spectrum Shifting Technique,” 2018, doi: 10.1109/EMCSI.2018.8495174.
[14] P. G. Fahlstrom and T. J. Gleason, Introduction to UAV Systems: Fourth Edition. 2012.