Testing of Defensive Aids Sub-Systems for Small UAS to improve Combat Survivability

Francisco Javier Cruz Hernández
C. Marie Curie, 17, 28521 Rivas-Vaciamadrid, Madrid
SPAIN

fjcruz@oesia.com

ABSTRACT

So far, the military employment of UAS have been limited to benign airspace and benign electromagnetic environments where they have not encountered any demanding threat to their safety. However, any future conflict scenario is likely to have a more demanding air environment where the airspace and the electromagnetic spectrum will be contested.

UAS have become high-value assets, and their loss could be detrimental to the mission success. Because of that, most military small UAS probably will have to come equipped with some sort of self-defense system.

This paper exposes suitable self-protection systems to be installed in Small UAS, and the ground as well as fligh tests of such systems.

1.0 THE DILEMMA: UAS SURVIVABLE VERSUS EXPENDABLE

What military conflicts in Ukraine, Syria, Libya, and Armenia/Azerbaijan tell us, is UAS and Electronic Warfare (EW) played an important role across the four conflicts.

Missions executed with UAS across the four above conflicts:

1. ISTAR as flying sensors

- Situational awareness
- Find, fix, track adversarial targets
- Guiding precision-guided weapons

2. Effectors/Shooters (kinetic/non-kinetic)

- Air interdiction
- Attack lines of supply
- Attack adversarial targets
- Fire Support
- Supression of Enemy Air Defense (SEAD)

- Electronic warfare (including suppression of enemy air defense, jamming, deception)

3. Communications Relay function

Contrary to the prevalent discussion of UAS, the use of EW in all four conflicts receives much less attention. Overall, EW has been used in support of offensive operations, including attack of UAS.

In some of these conflicts, the close coordination of UAS missions with the use of Electronic Attack systems suggests an advanced understanding of the multiplying force of EW, while at the same time illustrating the need for UAS protection by other assets.

We can observe two trends, while some countries have bet on UAS to impose its superiority, others have pushed the employment of EW.

For NATO adversaries, EW has become an integral element of air defense solutions. In their military doctrine, EW is to become a primary means for countering UAS. This changes the future operating environment for the use of UAS, which will need be reflected in developments of self-protection modules for UAS. Since, for UAS are expected to find a heavy cluttered, congested, and contested electromagnetic spectrum that will be constitutive of future warfare.

Aircraft Combat Survivability is defined as the capability of an aircraft to avoid or withstand a man-made hostile environment.

So far UAS have flown against little opposition. Adversaries lacked of sophisticated anti-UAS defenses. Past operations were almost uniformly characterized by a permissive air environment. Now, UAS have to address how to carry out their missions in anti-access/area-denial (A2/AD) environments established by more advanced nation-state adversaries.

However, the recent conflicts between Armenia and Azerbaijan, and in Ukraine show that the days of both permissive airspace and electromagnetic spectrum are over. In fact, most of the missions the military UAS will fly in the foreseeable future will likely occur in a contested both airspace and electromagnetic spectrum.

Small UAS face serious challenges from rocket propelled grenades (RPGs), anti-aircraft artillery (AAA), heavy machine guns and small arms fire. It's estimated more than 60% of the UAS losses were caused by these threats. The rest losses were due to non-kinetic weapon systems, such as Electronic Attack.

In light of these recent conflicts, most military small UAS probably will have to come equipped with some sort of self-defense system.

Nevertheless, here is the dilemma: UAS survivable versus expendable?

In order to narrow down the discussion, we will focus on UAS Class I type Small (according to UAS NATO Classification this involves UAS with MTOW greater than 20 Kg but lesser than 150 Kg) with a payload capacity of, at least, 20 Kg in order to host the self-protection system.

Figure 1-1: UAS in contested environment.

The controversy regarding UAS Concept of Employment (CONEMP): low cost, large numbers and expendable versus moderate cost, less numbers and survivable, could be solved if in order to consider UAS as "expendable," their inability to survive against a credible air defense as well as an electronic warfare should not pose a problem; as long as they could fulfill its mission.

With expendable UAS, operator assumes every launch is a single-use and that asset is not coming back. While, for attritables UAS, operator considers a certain number of losses as acceptable if the mission is successful.

The thesis underlying this paper is that UAS have become high-value assets, and their loss could be detrimental to the mission success. Therefore, they can hardly be considered expendable.

Figure 1-2: Threats against UAS.

As the utility of UAS grow, the cost of losing these assets becomes increasingly important. Survivability of

the UAS, which has been considered a secondary issue for a disposable piece of gear, is now of primary importance due to that are performing mission essential tasks. More importantly, warfighters are depending upon these assets. The loss of a UAS directly affects combat effectiveness.

So far, the success of UAS missions have been based on the absence of electromagnetic operations in the air space (no denied, no degraded). However, the military doctrine of NATO adversaries points to massive use of EW to counter NATO assets.

This paper argues that the UAS Class I type Small are assets valuable enough to deserve survivability because they are a key enabler of Combat Cloud that improve the operational commander's capabilities since they allow to shorten the sensor-to-effector cycle; and therefore, gain an advantage over the enemy.

However, most of the current UAS are considered as expendable, or at most attritable. Only a minority can be considered as survivable. Because most UAS are designed deliberately. to be expendable, with acceptable cost a higher priority than survivability.

Indeed, current military small UAS have little or no survivability features incorporated into them. The small UAS were designed for a benign environment but as the threat spectrum increases, there's a need for greater survivability.

So the dilemma is: UAS still represent valuable assets sufficiently inexpensive and plentiful to be considered "attritable" (or dispensable) or else they must be able to survive if their missions require them to operate in hostile areas. Including survivability features in a UAS will generally increase the cost of an individual aircraft.

The most obvious restrictions on small UAS are those of size, weight and power consumption (SWaP), which imposes limitations on mission equipment hosted by the platform.

But SWaP is not the only constraint, cost is also a major obstacle for small UAS. The overall budget for any given platform tends to have around 5-10% allocated to self-protection equipment. If the cost of such equipment exceeds this amount, the tendency has been to not include it at all.

However, survivability could both reduce the overall cost of UAS systems (including the cost of replacing UAS lost through attrition) and increase their availability during operational campaigns. This trade-off needs to be considered in light of the cost and intended mission of the UAS system.

The thesis of this paper is that UAS merit the inclusion of capable EW self-protection systems as they are valuable assets to protect.

UAS lack the combat survivability features of manned aircraft. The Electronic Warfare equipment that manned aircraft rely on to survive — such as Radar Warning Receiver, Missile Warning System, Laser Warning System and Electronic Attack systems — were never priority items in current UAS designs.

While many threats against UAS are equal to those directed against manned aircraft, there are threats which are unique to UAS and haven't been addressed so far. For instance, if a manned aircraft is subject to an electronic warfare attack, it is still under control of the onboard pilot. However, if UAS lost communications they cannot continue to fulfill their task. So electromagnetic resilience is much more important for an unmanned system than for a manned one. So for all those threats, the appropriate defensive aids need to be introduced in order to improve their combat survivability.

2.0 SELF-PROTECTION SYSTEMS FOR UAS

The proposed survivability suite is composed by:

- In order to enhance engagement avoidance:

  1. Incorporate Radar Warning Receiver to increase Situational Awareness.

  2. Incorporate Identification, Friend or Foe Transponder with Mode 5.

- In order to enhance hit avoidance:

  1. Incorporate Laser Warning System.

  2. Incorporate Missile Warning System.

  3. Incorporate Countermeasures against RF/IR threats.

- In order to enhance detection avoidance:

  1. Incorporate military radio transceiver.

- In order to enhance hit tolerance:

  1. Incorporate military GNSS system.

Historically the high power and large size of airborne Electronic Warfare, IFF and military GNSS, military transceivers equipment has constrained its deployment to manned aircraft or large UAS. More recently the miniaturisation of RF components and small form factor processor boards has led to the development of EW, IFF, military GNSS and military transceivers, capable of installation in small UAS.

By incorporating Radar Warning Receivers (RWR) to UAS, they can be detected hostile radars and manoeuvre the UAS away from the threat before weapons can be employed. RWR systems can also collect information on the adversary's electronic order of battle and can contribute to the overall intelligence picture.

By incorporating Missile Warning Systems (MWS) and Hostile Fire Indicators (HFI) to UAS, they can detect incoming missiles regardless of whether they are radar, IR, laser- or visually-guided. They can also provide information on the time to impact as well as the direction of the approaching missile.

Small UAS are particularly susceptible to threat impact from small arms and unguided munitions due to their inherent low-and-slow flight parameters. It would be of immense value if the UAS could be quickly alerted to incoming fire so that they may take evasive maneuvers. MWS with Hostile Fire Indicator (HFI) allows to detect hostile fires from antiaircraft artillery, RPG and small arms.

By incorporating Laser Warning Systems (LWS), they can detect surface-based laser range finders, laser designators and laser beam riding weapons.

By incorporating IFF Transponder Mode 5 makes possible to determine if an inbound UAS is friend or foe. Due to the proliferation of UAS in combat theatres, users require an accurate means to identify them, in order to distinguish friendly UAS from enemy UAS, and avoid the risk of accidental fratricide of UAS between blue forces.

Mode 5 is an enhancement to legacy Mode 4. NATO require Mode 5 to replace Mode 4 from 2020.

Now that IFF technology has been miniaturized, we can finally distinguish between friendly and hostile UAS to take appropriate action. So far, IFF transponders were too large for use on anything but manned aircraft. However, small form factor IFF transponder enables to deploy Mode 5 capability on small UAS.

Figure 2-1: IFF Transponder Mode 5 with a weight of 190 gr.

Figure 2-2: IFF Transponder Mode 5 with a weight of 68 gr.

By incorporating military GNSS, we can protect UAS against GNSS jamming and spoofing threats in order to continue operating in GNSS denied environments. Because Inertial Navigation Systems (INS) and Visual Navigation systems are not designed to provide the sole source of position, navigation and timing information in GNSS denied environments.

UAS rely heavily on Global Navigation Satellite System (GNSS) for Guidance, Navigation and Control (GNC). In addition to this, GNSS also offers time synchronization. So, UAS using civil GNSS can fall prey to GNSS jamming and spoofing attacks.

Contrary to the civil GNSS, the military GNSS receiver uses Electronic Protection Measures withstanding or working around vulnerabilities to fend off spoofing and jamming attacks.

Currently there are two GPS security architectures. The first, Selective Availability Anti-Spoofing Module (SAASM), uses the GPS Precise Position Service (PPS), which is provided using encrypted signals (P(Y)

Code) on two frequencies: L1 (1575.42 MHz) and L2 (1227.6 MHz).

M-Code is the second one, utilizing the M-Code signals. M-Code is also an encrypted signal provided on L1 and L2 frequencies.

In addition to GPS, GALIEO uses Public Regulated Service (PRS) as an encrypted navigation service for governmental authorised users.

On the other hand, CRPA antenna eliminates interference by applying novel beamforming techniques. With a CRPA antenna, the system can assure the normal operation of GNSS receiver in presence of multiple jamming sources.

Low Size, Weight, And Power, (SWAP) military GNSS receiver and CRPA antenna can be installed in small UAS.

Figure 2-3: Military GPS receiver with a weight of 10 gr (left) and 4 Element CRPA Antenna Array (right) with a weight of 165 gr.

By using military radio transceivers with military waveforms, UAS can low both the Probability of Interception and Probability of Detection of UAS Data Links, as well as counter jamming radio communications.

SATURN (Second generation Anti-jam Tactical UHF Radio for NATO) is the most recent UHF coalition waveform for military airborne operations, defined by the Standardization Agreement (STANAG) 4372. SATURN is a fast frequency hopping waveform that was developed as a replacement for the HaveQuick waveform.

SATURN waveform provides Low Probability of Interception (LPI), Low Probability of Detection (LPD) and Anti-jamming against Electronic Attack in communications band.

Small form factor military radio transceivers can be installed in small UAS.

Figure 2-4: Military radio transceiver with a weight of 70 gr.

In some instances it may sufficient to install only the warning system to enhance combat survivability. For example, if RWR is installed, it may be able to detect that the UAS is being tracked by the adversary's radar. The operator can then decide to take evasive maneuvers like exiting the threat sphere before any weapon can be used on the UAS. However, in many other instances, it may be too late for the UAS to exit the threat volume or the mission requires it to stay on course. The adversary may then launch a missile or send its fighters out to intercept the UAS. In that cases, countering the incoming threat may be necessary.

By incorporating Countermeasures (ECM), they can avoid being hit by radar-, IR- or laser-guided weapons.

- IRCM – Flare: Flares are pyrotechnics designed to emit large amounts of radiation in the sensor bandwidth of an IR-guided missile to draw attacking IR-guided missiles away from the aircraft they are protecting.

- RFCM – Chaff: The simplest countermeasure against radar is chaff. Chaffs are small strips of conducting materials (normally dipoles made of aluminum or thin glass fibers coated with aluminum or zinc) whose length is selected to make them good reflectors of radar energy. This length is half the radar wavelength that it is trying to counter.

Industry already offers relatively small and lightweight RWRs, MWS, LWS and ECM equipment suitable for small UAS.

Figure 2-4: Threats and countermeasures.

Small form factor RWR and MWS bring radar and missile protection to platforms where it was previously unavailable for reason of cost or size. The small size eases the burden on UAS in particular and the reduced power consumption renders a double benefit, as a smaller, lighter power supply is required.

On the other hand, small-form dispenser system is capable of defeating IR seeking MANPADS and air-to-air missiles. With one-third the weight and length of standard flares, the mini stand-alone missile protection system provides protection for small UAS previously undefended due to weight constraints.

Digital RadioFrequency Memory (DRFM) are available in small form factors. DRFM can be used for Electronic CounterMeasures (ECM) / Electronic Attack (EA), as techniques generator for radar deception. The main handicap of ECM is its feature of high power jamming, and consequently its high power

consumption.

Three combat survivability enhancement have been proposed.

- Proposal #1 proposes the installation of an RWR system as the warning system and DRFM based ECM as countermeasures. This is the case with the most demanding power requirements when RWR and ECM are working simultaneously.

- Proposal #2 proposes the installation of an RWR system as the warning system and a chaff and flares dispenser as countermeasures. This case and the following one involve similar power requirements.

- Proposal #3 proposes the installation of a MWS system as the warning system and a chaff and flares dispenser as countermeasures.

Figure 2-5: Small Form Factor Radar Warning Receiver with weight of 975 gr.

Figure 2-6: Small Form Factor Missile Warning System + HFI with weight of 2 Kg.

Figure 2-7: Small Form Factor Laser Warning System with weight of 2 Kg.

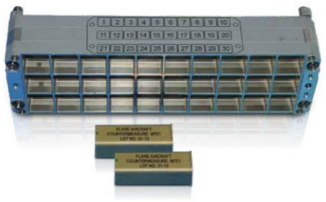

Figure 2-8: Chaff and Flares Dispenser with 1/3 the weight and length of standard flares

The UAS loss rate is an indication of the effectiveness of solution in enhancing UAS combat survivability. Modeling and simulation of possible operation scenarios allows one to measure the likely loss rate of the UAS when installed with each different solution.

The results show that UAS implementing proposal #1 has a loss rate of 0.02 kills per 1000 operation hours. The UAS implementing proposal #2 has a loss rate of 0.03 kills per 1000 and the last configuration of UAS has a kill rate of 0.01 kills per 1000 hours. All solutions meet the requirement of reducing the loss rate to at least 0.03 kills per 1000 operating hours. The result is used to rank the solutions according to their effective.

The UAS endurance is used to measure the effect of the solutions on the performance of the UAS. Models used to compute the maximum endurance of the UAS based on the new fuel consumption (due to the weight increase by the combat survivability enhancement features) and amount of fuel the UAS can now carry. Results show that the UAS has maximum endurance in proposal #1. While it has less endurance in proposal #2 and #3.

It is important that any solution implemented is compatible with the payload. Based on technical studies, there is insufficient electrical power to operate the sensor payload while the ECM is deployed (proposal #1). In this regard, proposal #1 is ranked the lowest in the compatibility aspect. Proposal #2 and #3 have no compatibility issues with the payload and therefore are ranked equal.

On the other hand, availability is an indication of UAS being available for mission tasking when it is needed. It is required that inherent availability of UAS after implementing the solution should be at least 85%. Analysis shows that the UAS will have an inherent availability of 93% when proposal #1 is implemented, 90% when proposal #2 is implemented and 95% when proposal #3 is implemented.

As can be seen, Proposal #3 is determined to have the most benefits to UAS combat survivability, followed by solution 2 and then solution 1.

3.0 GROUND TESTING OF SELF-PROTECTION SYSTEMS IN UAS

3.1 Ground Tests of EW payloads

For testing Threats Warning Sensors in UAS, there are failures that cannot be detected by the built-in test. These range from small frequency bands with high attenuation in cases of damaged cables, to contaminated

radomes and stop-band attenuation degradations of the optical filter in a missile warner, as well as other failures that dramatically reduce the system's protection capability. Although the different systems' built-in tests provide diverse levels of test coverage, these tests cannot cover the entire path from threat to alert to countermeasure.

A simple go/no-go test will already improve the level of confidence in the system's protection capabilities. Such a test covers just a part of what can be tested with a pre-mission test, however. Over time, EW system sensors lose a degree of sensitivity, thereby minimising the protection capability. A sensitivity check at least once a week is thus a highly beneficial supplementary test that, with suitable test equipment, will not consume much time and is practicable at the flight line.

The practical execution of pre-mission tests has to be easy and convenient, as the results will otherwise be degraded by test execution errors or even omission. Most people performing such tests, at e.g. the flight line, have to execute a lot of different tasks in a short amount of time, and are not EW experts – the test definition and operation concept must take this fact into consideration. The test device has to be light, compact and should not require a complicated setup. For such purpose, we can use an EW Test Set that can check all 4 threat types (missile, laser, radar and Hostile Fire Indication). The EW Test Set checks that EW system is operating correctly and provides reassurance before a mission.

For instance, the test protocol for MWS/LWS/RWR, the ground operator, using the EW threat simulator, must point and emit ultraviolet (solar blind UV band: 200-300 nm) or infrared emissions (MWIR band: 3-5 μm) towards the sensors of the MWS for a threat detection to occur in each quadrant.

1. Missile threats detection in the front left quadrant (AOA = [270º, 360º])

2. Missile threats detection in the front right quadrant (AOA = [0º, 90º])

3. Missile threats detection in right rear quadrant (AOA = [90º, 180º])

4. Missile threats detection in left rear quadrant (AOA = [180º, 270º])

After that, the ground operator, using the same EW threat simulator, must point and emit laser emissions (635 nm, 904 nm and 1550 nm to cover Laser Range Finder, Laser Target Designator, Laser Beam Riding) towards the sensors of the LWS for a threat detection to occur in each quadrant.

1. Laser threats detection in the front left quadrant (AOA = [270º, 360º])

2. Laser threats detection in the front right quadrant (AOA = [0º, 90º])

3. Laser threats detection in right rear quadrant (AOA = [90º, 180º])

4. Laser threats detection in left rear quadrant (AOA = [180º, 270º])

Finally, the ground operator, using the same EW threat simulator, must point and emit RF emissions (2 – 40 GHz pulsed/CW) towards the sensors of the RWR for a threat detection to occur in each quadrant.

1. Radar threats detection in the front left quadrant (AOA = [270º, 360º])

2. Radar threats detection in the front right quadrant (AOA = [0º, 90º])

3. Radar threats detection in right rear quadrant (AOA = [90º, 180º])

4. Radar threats detection in left rear quadrant (AOA = [180º, 270º])

Figure 3-1: Hand-Held EW Test equipment.

During the test, the ground station operator will visualize the simulated threat on the Electronic Warfare display and will hear the corresponding alert notice through the audio system.

For instance, the test protocol for Chaff and Flares Dispenser, is based on using chaff-and-flare simulator. The simulator does not use any pyrotechnics and is suitable for a wide range of scenarios.

1. Install chaff and flares simulator instead of actual countermeasure decoys. The test equipment relies on electronics rather than pyrotechnics to test the chaff and flares that are ejected from UAS to defeat attacking missiles.

2. Check on the display of the ground station that both the correct number and type of chaff / flares decoys are shown. Verify that the inventory of CHAFF / FLARE loads shown on the screen matches the one loaded into the dispensers.

3. Operate the chaff and flare dispenser in Manual Mode.

4. Select the indicated countermeasures program (number, type, sequence, interval of decoys) from the ground station.

5. Stimulate MWS/LWS/RWR in the different quadrants with the EW tester.

6. Execute the chaff and flare dispensing in Manual mode.

7. Check that the appropriate countermeasures are dispensed depending on the type of threat (Flares vs. Missiles and Chaff vs. Radar), as well as that they are dispensed on the side corresponding to the detection of the threat.

8. After executing the program, check the remaining chaff and flares indicated on the ground station screen, verifying that the program has been carried out correctly.

3.2 Ground Tests of IFF M5 payload

It is needed an IFF Test Set is used as an Interrogator Simulator for testing Mode 5 IFF Transponder in a Flight Line environment.

Mode 5 requires a crypto computer, either internal crypto, or an external crypto computer such as the KIV-

77 or KIV-79. When IFF is combined with a micro-crypto (such as KIV-79 Micro Crypto), small UAS can use Mode 5.

In order to carry out IFF tests, both IFF Test Set and IFF Transponder's crypto computer must have the correct Crypto Code of the Day. Crypto keys have a pre-defined duration. It should pay attention to the fact that crypto keys do not expire.

It should be observed if there is any notification of lack or failure of crypto keys on the display of the Ground Station.

Using an IFF Test Set as an IFF Interrogator, and commanding the IFF Transponder via the Ground Station, it was found all transponder modes – including Mode 5 Levels 1 and 2 – could be exercised, and keys were zeroized on command.

On the display of the IFF Test Set Tool, it can be read the test result. If the test result is

- “PASSED”, the IFF Transponder Mode 5 operates correctly and has the correct Crypto Code of the Day

- “FAILED”, the IFF Transponder Mode 5 does not work correctly or does not have the correct Crypto Code of the Day.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' IFF Transponder. After that, it should be displayed a message indicating that IFF's crypto keys are missing.

Figure 3-2: IFF Test Set.

3.3 Ground Tests of military GNSS payload

In order to carry out the tests, the appropriate crypto keys must be loaded into the military GNSS receiver in order to enable military codes of operation.

Crypto keys have a pre-defined duration. It should pay attention to the fact that crypto keys do not expire.

It should be observed if there is any notification of lack or failure of crypto keys on the display of the Ground Station.

By means of some special equipment is possible the creation of jamming and spoofing scenarios to simulate

Navigation Warfare (NAVWAR) for testing. It must be careful to avoid to deny service for other users in the vicinity. This method, however is more representative of the real world.

Using the above special equipment, it can be checked if once activated, the GNSS receiver operating with military codes (P(Y), M) shows the correct Present Position and the correct UTC time with an appropriate Time Figure Of Merit (TFOM) value. Or whether it's observed any degradation in UTC time / TFOM or any failure in position reporting.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' GNSS receiver. After that, it should be displayed a message indicating that GNSS' crypto keys are missing.

3.4 Ground Tests of military V/UHF transceiver payload

In order to carry out the tests, the appropriate crypto keys must be loaded into the V/UHF transceiver in order to enable military waveform SATURN.

Crypto keys have a pre-defined duration. It should pay attention to the fact that crypto keys do not expire.

It should be observed if there is any notification of lack or failure of crypto keys on the display of the Ground Station.

Both the UAS radio and the Ground Station radio must use the same keys, the same network number, and the same frequency plan in NATO UHF band.

During the tests, it was used the Ground Station's V/UHF transceiver to communicate with UAS' V/UHF transceiver on SATURN mode.

A Headset Interface Adaptor is used to connect a groundcrew headset to the audio interface of UAS' V/UHF transceiver. This lets the groundcrew communicate between the UAS and the Ground Station.

It was made sure that the reception on the V/UHF transceivers was loud and clear in SATURN mode.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' V/UHF transceiver. After that, it should be displayed a message indicating that V/UHF's crypto keys are missing.

4.0 FLIGHT TESTING OF SELF-PROTECTION SYSTEMS IN UAS

It is required that before starting the Flight Tests, the Ground Tests and the EMI/EMC Tests have been carried out successfully.

With the EMI/EMC tests, it will be verified that the new self-defense systems do not produce unwanted electromagnetic interference (noise) in the operation of the remaining electrical/electronic subsystems included in the UAS and that all are functionally compatible during their simultaneous operation.

4.1 Flight Tests of EW payloads

The objectives of the Flight Tests are:

1. Demonstrate successful launch and recovery of UAS carrying the Electronic Warfare payloads (self-

protection suite). In order to check airworthiness and safety aspects.

2. Determine the effectiveness of the Electronic Surveillance / Electronic Countermeasures payload installed on UAS.

When evaluating UAS self-protection systems in Flight Tests, we should address the following questions:

- What is the possibility of the system triggering a false alarm?
- What is the possibility of a threat not being detected?
- What is the detection range?
- How much time does the system require to detect and identify threats?
- Does the system indicate the correct angle of arrival for the threats?
- Does the system properly cover all the UAS or are there blind zones?
- Does the system properly cover all expected RF frequency bands, as well as UV bands and IR bands?
- Are the threats properly identified by the system according the Threats Library?
- What is the possibility of a threat being detected and proper countermeasures not deployed?
- What is the reaction time between the threat detection and the countermeasures dispense?
- How many simultaneous threats can the system deal with?
- What information is shown in the Ground Station for indicate threats alarm?
- Does the system properly report about the number of dispensed countermeasures and the total quantity of remaining available?

The necessary configuration for the flight tests that will be mounted on the UAS must be fully representative of the final installation of the system. The equipment used for Flight Tests will be those that correspond to the final installation to be carried out.

In the Flight Test phase, the ability of the self-defence system to detect RADAR, UV and LASER threats will be verified, as well as to discriminate between different threats and dispense programmed countermeasures.

Prior to carrying out Flight Test, an Experimental Airworthiness Certificate will have been obtained from the National Airworthiness Authority indicating that the UAS is ready for testing. This means that the installation is in accordance with the approved design documentation.

To carry out these tests, two types of flights will be carried out:

- Flight Type #1: to check Threats Warning Systems.

- Flight Type #2: to check Countermeasures Systems.

In the first type of flight, the UAS under test destined to be "illuminated by the threat", will describe a horizontal turn in such conditions that it takes time to corroborate that the warning system has detected the threat.

The threat generator will be positioned in an escort helicopter. The accompanying helicopter may be placed at the same flight level or above the UAS under test, and either to one side or the other of it. Said escort helicopter will have a threat simulator with the ability to "illuminate" the UAS with different types of "threats".

To carry out the flight tests, an accompanying helicopter could be used - equipped with RF, UV, Laser threat simulators - flying around the UAS while said UAS performs maneuvers to be illuminated by the different types of threats, in different positions of azimuth and elevation.

One of the challenges for the flight tests of these EW systems is the interaction between UAS and manned aircraft.

For UAS to be allowed to fly as close as they must to other aircraft in such airspace, UAS must include the ability to ”sense and avoid” other aircraft in order to prevent collisions between UAS and helicopter.

The question arises of how to deal with the integration of UAS in “non-segregated” airspace, sharing airspace with manned aircraft. To address this, the Sense & Avoid (SAA) systems are used in order to ensure safe separation between UAS and helicopter.

To this end, the UAS is equipped with collaborative Sense & Avoid systems such as ADS-B/Transponder Mode S and

TCAS/ACAS, in order to provide situational awareness of air traffic and avoidance solutions for UAS based on the surrounding aircraft in order to ensure the operational safety.

The collaborative SAA system means that the UAS is equipped with the same kind of sensors that those of the helicopter.

The Sense function is in charge of detecting possible intruders and determining as accurately as possible the position of the intruders.

The Avoid function is in charge of processing the information it receives from the Sense subsystem and the Flight Management System in order to determine if a conflictive situation may occur in the more or less near future and in that case, propose an evasion maneuver in order to prevent mid-air collision and ensure safe separation distance from helicopter.

There are currently miniature Transponders that provide Mode S and 1090 MHz ADS-B In/Out.

For safety reasons, the horizontal distance between the escort helicopter and the UAS will be, at least, the equivalent of two rotors.

Figure 4-1: Small Form Factor ADS-B/Transponder Mode S with a weight of 190 gr.

The following figure shows the diagram of the type of maneuver to be described by the UAS receiving the threat.

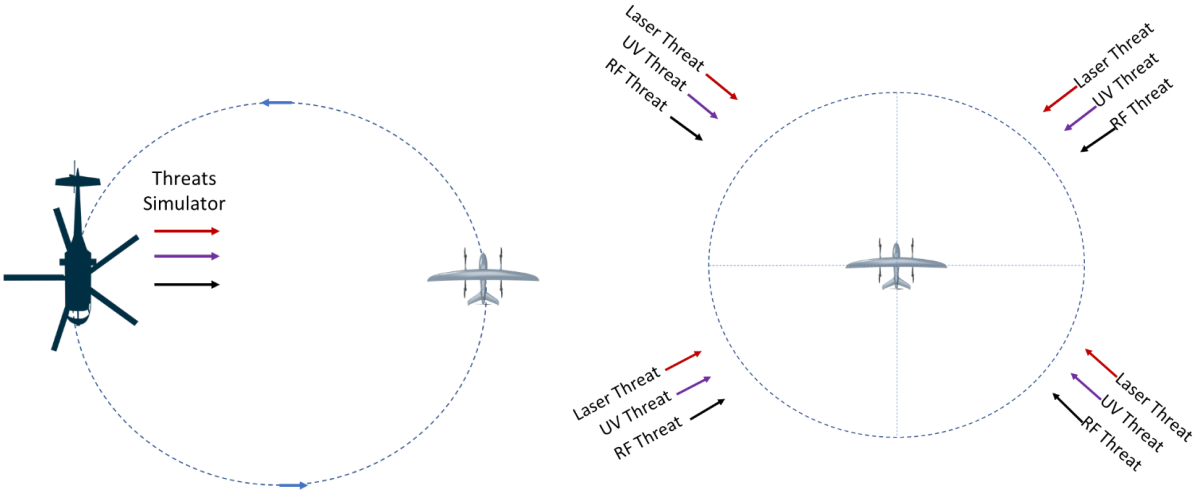

Figure 4-2: Maneuvers for EW payload during Flight Test.

The Flight Test Card would be the following:

- Step #1: Power-up in flight of UAS's self-defense systems.
- Step #2: Missiles threat test by illuminating the UAS from the accompanying helicopter sweeping 360º in azimuth, verifying that the UV threat appears on the ground station display with the correct angle of arrival and identification.

Figure 4-3: Missile threats displayed.

- Step #3: Laser threat test by illuminating the UAS from the accompanying helicopter sweeping 360º in azimuth, verifying that the Laser threat appears on the ground station display with the correct angle of arrival and identification.

Figure 4-4: Laser threats displayed.

- Step #4: Radar threat test by illuminating the UAS from the accompanying helicopter sweeping 360º in azimuth, verifying that the Radar threat appears on the ground station display with the correct angle of arrival and identification.

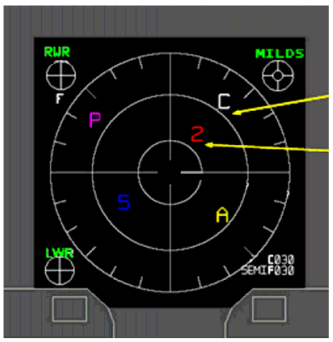

Figure 4-5: Radar threats displayed.

- Step #5: Test of dispensing countermeasures against threats. After carrying out the previous flight

test, the UAS will be brought to the ground in order to load the dummy countermeasures to be used in the dispensing tests. To do this, the magazines will be loaded with the dummies cartridges. After that, the UAS will be illuminated from the accompanying helicopter, sweeping 360º in azimuth, verifying that the countermeasures has been dispensed on the side corresponding to the illumination of the threat. And checking on the ground station display the correct number of countermeasures dispensed.

Figure 4-5: Countermeasures displayed.

Some aspects to highlight, the simulation of the UV and laser threats require a greater proximity than the simulation of the RF Radar threat. In addition, it should also be noted that the simulation of the laser threat requires directivity between the source and the victim.

4.2 Flight Tests of IFF M5 payload

The objectives of the Flight Tests are:

1. Demonstrate successful launch and recovery of UAS carrying the IFF Transponder Mode 5. In order to check airworthiness and safety aspects.

2. Determine the correct response in Mode 5 of the IFF Transponder from interrogations coming of IFF Interrogator.

When evaluating UAS self-protection systems in Flight Tests, we should address the following questions:

- Do the Crypto Keys are proper loaded and zeroized?
- Does the IFF Transponder replies properly in Mode 5 to interrogations?
- Does the system properly report about the crypto keys status, Mode 5 availability and Mode 5 responses?

The necessary configuration for the flight tests that will be mounted on the UAS must be fully representative of the final installation of the system. The equipment used for Flight Tests will be those that correspond to the final installation to be carried out.

An IFF Interrogator Mode 5 will be positioned in an escort helicopter. The accompanying helicopter may be placed at the same flight level or above the UAS under test -destined to respond in Mode 5-, and either to one side or the other of it. Said escort helicopter will have an IFF Interrogator with the ability to send Mode 5

interrogations. UAS and helicopter will describe horizontal turns.

Both, the UAS' IFF Transponder and helicopter's IFF Interrogator will be equipped with proper crypto computers and will use the same cryptos keys for Mode 5.

After Crypto Keys loading, it has to be checked that M5 Crypto Keys are present and M5 available in both IFF Transponder and Interrogator.

The following figure shows the diagram of the type of maneuver to be described by the UAS and helicopter.

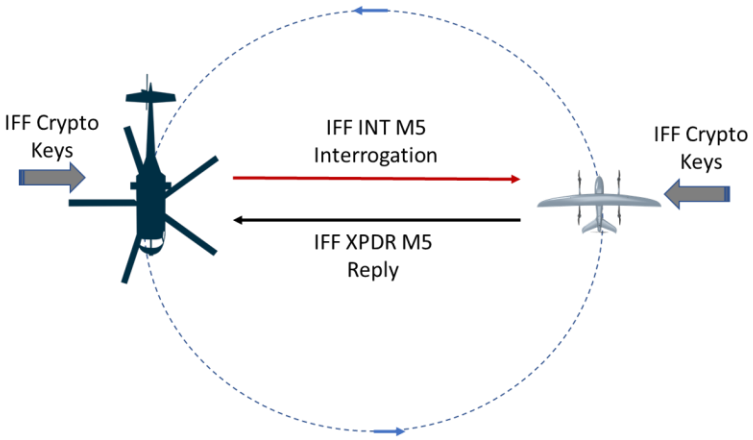

Figure 4-6: Maneuvers for IFF M5 payload during Flight Test.

During the flight tests, it was found all IFF transponder modes – including Mode 5 Levels 1 and 2 – could be exercised, and keys were zeroized on command.

It was displayed that the IFF Transponder Mode 5 replied properly to interrogations in Mode 5 and had the correct Crypto Code of the Day.

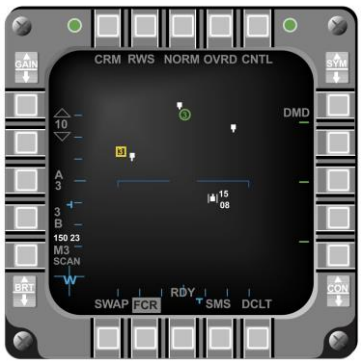

Figure 4-7: Example of IFF reply to interrogations.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' IFF Transponder. After that, it should be displayed a message indicating that IFF's crypto keys are missing.

4.3 Flight Tests of military GNSS payload

The objectives of the Flight Tests are:

1. Demonstrate successful launch and recovery of UAS carrying the military GNSS receiver. In order to check airworthiness and safety aspects.

2. Determine the correct operation of military modes in GNSS receiver.

When evaluating UAS self-protection systems in Flight Tests, we should address the following questions:

- Do the Crypto Keys are proper loaded and zeroized?
- Does the GNSS receiver operates properly (position and time) in military modes?
- Does the system properly report about the crypto keys status and military mode availability?

The necessary configuration for the flight tests that will be mounted on the UAS must be fully representative of the final installation of the system. The equipment used for Flight Tests will be those that correspond to the final installation to be carried out.

UAS' GNSS receiver will be loaded with cryptos keys for military mode.

The following figure shows the diagram of the type of maneuver to be described by the UAS and helicopter.

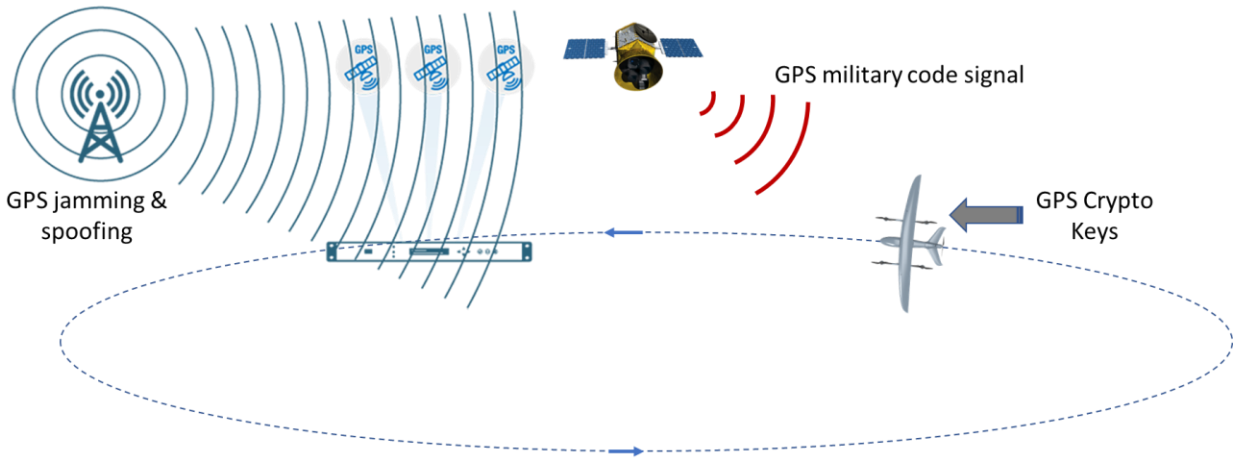

Figure 4-8: Maneuvers for military GNSS payload during Flight Test.

To carry out these tests, three types of flights will be carried out:

- Flight Type #1: operation with Normal Full GPS.
- Flight Type #2: operation with GPS-degraded.

- Flight Type #3: operation with GPS-denied,

The first type of flight was designed to demonstrate the normal capabilities of the military GNSS receiver. while operating in an environment without GPS degradation or denial. During the test, the UAS autonomously flown around a flight path, while ensuring that the UAS GPS reported properly position and time.

The second type of flight was designed to demonstrate the ability of the military GNSS receiver to operate properly in degraded GPS environments. The UAS was intended to complete one full circuit of the flight path with a non-degraded GPS signal. Upon the start of the second circuit, GPS military mode was enabled and a system was used to try to degrade the GPS information.

The GPS degradation was designed to remain in effect for the second, third, and fourth full laps of the flight path. Once the UAS began the fifth lap of the flight path, the system used to degrade GPS was turned off.

It was observed the contrast between normal and degraded GPS environment operations, by the GPS information presented in Ground Station.

In order to show the operation in GPS-denied environments, the third type of flight was designed in the same manner as the second type of flight. During the second, third, and fourth laps of the test, GPS military mode was enabled and a system was used to try to deny the GPS information.

The GPS denied was designed to remain in effect for the second, third, and fourth full laps of the flight path. Once the UAS began the fifth lap of the flight path, the system used to deny GPS was turned off.

It was observed the contrast between normal and denied GPS environment operations, by the GPS information presented in Ground Station.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' GNSS receiver. After that, it should be displayed a message indicating that GNSS's crypto keys are missing.

4.4 Flight Tests of military V/UHF transceiver payload

The objectives of the Flight Tests are:

1. Demonstrate successful launch and recovery of UAS carrying the military V/UHF transceiver. In order to check airworthiness and safety aspects.

2. Determine the correct operation of military waveform SATURN in V/UHF transceiver.

When evaluating UAS self-protection systems in Flight Tests, we should address the following questions:

- Do the Crypto Keys are proper loaded and zeroized?
- Does the V/UHF transceiver operates properly in SATURN mode?
- Does the system properly report about the crypto keys status and SATURN availability?

The necessary configuration for the flight tests that will be mounted on the UAS must be fully representative of the final installation of the system. The equipment used for Flight Tests will be those that correspond to the final installation to be carried out.

A V/UHF transceiver capable of SATURN will be positioned in an escort helicopter. The accompanying helicopter may be placed at the same flight level or above the UAS under test -destined to respond in SATURN mode-, and either to one side or the other of it. Said escort helicopter will have a V/UHF transceiver with the ability to operate in SATURN mode. UAS and helicopter will describe horizontal turns.

Both, the UAS' V/UHF transceiver, helicopter's V/UHF transceiver and Ground Station's V/UHF transceiver will use the same cryptos keys for net number and frequency plan for SATURN mode.

The following figure shows the diagram of the type of maneuver to be described by the UAS and helicopter.

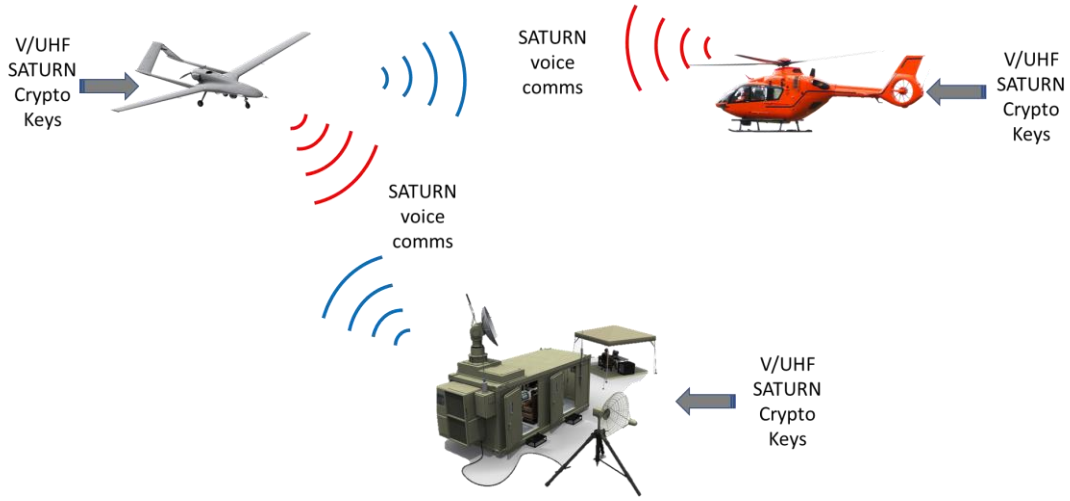

Figure 4-9: Maneuvers for V/UHF SATURN payload during Flight Test.

During the flight tests, helicopter's V/UHF transmits voice to the UAS' V/UHF, operating UAS as a communications relay to Ground Station's V/UHF. After that, Ground Station's V/UHF transmits voice to the UAS' V/UHF, operating UAS as a communications relay to helicopter's V/UHF.

It was made sure that the reception on the V/UHF transceivers was loud and clear in both helicopter and Ground Station.

After that, on the Ground Station, it was pushed the Secure Data Erase to erase crypto codes in UAS' V/UHF transceiver. After that, it should be displayed a message indicating that V/UHF's crypto keys are missing.

4.5 Combat Survivability Assessment

As a consequence of the fandom nature of combat, UAS survivability is measured by a probability. This probability is denoted by Ps, the probability the UAS to survive. The probability of survival varies from 0 to 1; the closer the value is to 1, then the more survivable is the UAS. We can measure Ps of an UAS as:

Ps = Probability of success of UAS self-protection system / Probability of defeat of enemy's counter-countermeasures

Where:

- Probability of success of UAS self-protection system = Probability of Threats Detection x [(Probability of activation of Countermeasures / Threats Detection) x Percentage of effectiveness of Countermeasures against Threats].

- Probability of defeat of enemy's counter-countermeasures = 1 – (Probability of enemy's Counter Countermeasures deployment x Percentage of effectiveness of enemy's Counter Countermeasures / Counter Countermeasures deployment).

For a mission, an UAS can successfully complete the assigned mission (measure of mission success, MOMS) only when the UAS survives the mission (Ps) and accomplishes the mission's objectives or goals (measure of mission accomplished, MAM).

From here, we could calculate:

$$MOMS = Ps \times MAM$$

Note than MOMS is directly proportional to mission survivability. The UAS must survive in order to accomplish its mission.

UAS that are effective in accomplished their mission will have a large MAM. If those same UAS have a relatively low mission survival rate, the MAM should be reduced intentionally by commanders to increase the Ps using management of attrition. If heavy losses are expected on a mission, commanders will have to manage attrition, that is, they will reduce MAM in order to increase the Ps.

With the information collected during the Flight Tests, it is possible to evaluate the probability of UAS survivability and mission success.

5.0 CONCLUSIONS

More and more, UAS have a vital role to play in the prosecution of military campaigns. In this regard, Electronic Warfare (EW) has a vital role to play in the protection of UAS'. To leverage this synergistic relationship it's needed to make use of the latest miniaturised EW equipment. EW needs UAS' and UAS' need EW.

EW payloads are getting smaller so that they can be inserted in small UAS, allowing much better protected UAS. It should be noted that some miniaturized EW equipment currently available allows its installation in small UAS, allowing to improve its combat survivability.

There are test equipment that allows to verify the correct operation of those EW equipment in UAS during ground tests and flight tests.

The Flight Tests of UAS equipped with EW pose certain challenges that differentiate them from manned aircraft. In order to stimulate the UAS self-protection system, is needed the interaction of the UAS with manned aircraft in the same airspace, and therefore requires equipping the UAS with Sense & Avoid systems such as ADS-B/Transponder Mode S and TCAS to guarantee the safety distance during tests.

The main parameters of the UAS self-defense system measured during the Flight Tests are:

- False alarm rate
- Misdetection rate
- Detection range
- Detection and identification time
- Angle of Arrival for the threats
- Spatial coverage (azimuth and elevation)
- Frequency coverage against Radar/RF threats
- Wavelengths coverage against UV and Laser threats
- Response of "Threats Library"
- Response of "Countermeasures Programs"
- Reaction time
- Maximum number of simultaneous threats that can be addressed
- Information related to system status, threats indications and countermeasures indications reported to the displays in Ground Station
- Crypto Keys proper loading and zeroize.
- Mode 5 responses to interrogations.
- Quality of communications in SATURN mode.
- Quality of Present Position and Time / TFOM provided.

Based on the above parameters, the probability of UAS survivability and mission success can be quantified.

We can conclude that:

1. The UAS with both the highest survivability and mission success rate are those that have Threats Warning Systems and Countermeasures against the threats.

2. UAS with Threats Warning Systems have some survivability and some chance of mission success but lower because they cannot counter the detected threat.

3. The UAS that lack both Threats Warning Systems and Countermeasures, have both much less chance of survivability and mission success.

REFERENCES

[1] Robert E. Ball, “The fundamentals of aircraft combat survivability analysis and design”, AIAA.

[2] Robert E. McShea, “Test and Evaluation of aircraft avionics and weapon systems”, Scitech.

[3] David L. Adamy, “EW against a new generation of threats”, Artech House.

[4] A.R. Jha, “Theory, Design and Applications of Unmanned Aerial Vehicles”, CRC Press.