ARMS – Anti RPAS Multisensor System

INDRA

Agenda Item 6.3 - P/08
ARMS

Anti RPAS Multisensor System
Some concepts about drones, UAV, UAS, RPAS

Multiple terms, different categories and performance with multiple applications

Different UAS groups classified by maximum weight, operating altitude, speed, etc (micro, mini, low and high end tactical, strategic)

<table>
<thead>
<tr>
<th>Weight</th>
<th>UAV Unmanned Aerial Vehicle</th>
<th>UAS Unmanned Aerial System</th>
<th>RPAS Remote Piloted Aircraft System</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 20 Kg</td>
<td>200 Kg</td>
<td>&gt; 14 Tn</td>
<td></td>
</tr>
<tr>
<td>40-150 m</td>
<td>&lt; 3.600 m</td>
<td>&lt; 18 kms</td>
<td></td>
</tr>
<tr>
<td>50-70 km/h</td>
<td>180 km/h</td>
<td>&gt; 500 km/h</td>
<td></td>
</tr>
<tr>
<td>&lt; 40 min</td>
<td>4-6h</td>
<td>&gt; 20 h</td>
<td></td>
</tr>
</tbody>
</table>
Multiple applications

Ref – “Plan Estratégico para el desarrollo del sector civil de los drones en España 2018-2021”, Ministerio de Fomento, España
... but not always so great

UAS/RPAS have become a real and significant threat for infrastructures and people due to their malicious or errant use.
We are facing a new kind of threat, and growing

Drone market is evolving fast
Technology improves and threat is increasing, automation and higher sophistication are the main challenge:
- GPS-denied navigation
- Swarm coordination
- Extended range and duration
- Heavier payloads

Multiple illegal and malicious uses
- Espionage and Intelligence
- Transport of explosive and biological payloads
- Air Traffic Interruption

Security Systems must be adapted according to the threat evolution
Civil aviation is NOT immune to this threat

“The drone scare at Gatwick airport that closed the runway for 33 hours shortly before Christmas cost over £50m.”

“Around 1,000 flights were cancelled during the busiest week of the winter for outbound departures from Gatwick”


Faced with this type of threat, different weaknesses and deficiencies in procedures, operations and systems were and are evident
And what is the role of an antidron systems (C-UAS)?

> 99%

UTM Collaborative UAS

Errant or Hostile
Non collaborative
Unmanned Aircraft Systems

< 1%

Air Space
Operation Modes

Different operation modes imply different challenges to be faced.

Remote Control
Piloted by one operator
(RF communications)

Waypoints
GNSS waypoints navigations (i.e.: GPS)

RF Datalink Control
Datalink Imágenes/Video
Waypoints
GPS
C-UAS ARMS
Operational Concept

ARMS is based on three key features: **Simple, Adaptable and Flexible**

Ready to face present and future threats

---

**ATM**
- Send of **ASTERIX** commands with tracks and identified threats and reception of whitelists

**ARMS**
- **Command & Control**
  - GIS based console displaying sensors information with threat analysis and countermeasures capabilities

**UTM**
- System integration sharing licit traffic information and drone flight plan non-conformance alarms

---

**Detection**
- Active and Passive sensors
  - Radar
  - RF Detector
  - Aeroscope

**Recognition and Tracking**
- Multiple sensors – including camera and videanalytics

**Countermeasures**
- Neutralization
  - SDR Jamming
  - GPS Spoofing

---

**(**) I.E UAS detection capability with primary radar PSR 3D Indra**
<table>
<thead>
<tr>
<th>TRK#</th>
<th>TYPE</th>
<th>DET. TIME</th>
<th>SRNGE (Nmi)</th>
<th>AZIM (°)</th>
<th>H3D (ft)</th>
<th>ANPL (dB)</th>
<th>RCS BEAM (m^2)</th>
<th>ELEV (°)</th>
<th>COURSE (°)</th>
<th>H.SPEED (km/h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1026</td>
<td>T5R-A</td>
<td>10:44:03.90</td>
<td>5.27</td>
<td>22.36</td>
<td>352.5</td>
<td>53.5</td>
<td>1.76</td>
<td>1</td>
<td>0.76</td>
<td>30.36</td>
</tr>
</tbody>
</table>

Slant Range: 920 Nmi  Azimuth: 25.09°
C-UAS ARMS Operational Concept

Each scenario requires specific considerations (civil vs military, fixed / mobile / portable)
### C4ARMS - Command and Control

**Simple and intuitive interface**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GIS based Interface</strong></td>
<td>Ruled based alarm and reactions</td>
</tr>
<tr>
<td><strong>Multisensor data fusion</strong></td>
<td>Manual, timed or automatic countermeasures</td>
</tr>
<tr>
<td><strong>Drawing tool to define areas</strong></td>
<td>Automatic and / or manual control of optronics</td>
</tr>
<tr>
<td><strong>Automatic trace tracking</strong></td>
<td>PlayBack tool</td>
</tr>
<tr>
<td><strong>Events log and reports</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Powerful Command and Control system providing an unified interface for assets protection**
C4ARMS - Command and Control

Powerful Command and Control system providing an unified interface for assets protection, supporting the complete C-UAS process from threat detection...
C4ARMS - Command and Control

... until the activation of the available and suitable countermeasures
Detection

**ACTIVE**
Radar based

- Detect any threat with high precision, both collaborative and non-collaborative, including Non-RF emission drones

**PASSIVE**
Radiofrequency analyzers, detection and location of RF datalinks. Specialized detector for DJI UAS

- **Multilateration and Goniometry** using technologies based on RF fingerprinting analysis. Geolocation of both UAS and operator
- **UAS Detector** specialized in DJI drones, providing information such as model, position, speed, heading, height, pilot location, …
Active Detection: MidRange y LongRange Radars

**Ku band radar**
- FMCW low power
- 360°, 60 rpm
- International recognition
  1º position Mitre Challenge

**Detection ranges**
- Micro UAS (RCS=0.01sqm)
- 3Km

**X band radar**
- FMCW low power
- 360°, 30 rpm
- Extended range

**Detection ranges**
- Micro UAS (RCS=0.01sqm)
- +5Km
Passive Detection

**RF Detection**
- Passive detection based on radiofrequency analysis
- Simultaneous detection of Uplink and Downlink communications
- Goniometry and Multilateration
- UAV and operator geolocation
- Identification of manufacturer and UAS model (Data Base)

**DJI Aeroscope**
- DJI UAS Detection
- Full integration with ARMS
- Full integrated in C4ARMS
- 100% detection of DJI UAS: 75% of marketshare
- Maximum detection ranges (aprox.): Suitcase (5Km), G8 (10Km), G16 (20Km)
- **UAS Information:** identifier, model, UAV and controller position, heading, height, etc
Recognition and Tracking

Electro Optical Surveillance System (EOSS)

• Based on high-quality and precision Infrared (IR) and Daylight cameras, IR based videoanalytics

• Analysis and confirmation (or doble confirmation) of detections provided by active and passive sensors

• Selectable configuration, several camera models, such as:
  – Indra CYCLOPS, advanced 3rd generation MWIR cooled
  – FLIR HRC family MWIR cooled
  – Other different uncooled models

• Positioner with 360° Azimuth range and wide elevation range

Optronics system

• Infrared and daylight
• 360° PTZ
• Wide FOV
• Day: Standard/HD
Countermeasures are based on **jamming (disturbance) or deception** of signals used by drone in both communications and navigation.

**DATALINKS (C2, VIDEO) JAMMING**

**GPS JAMMING/SPOOFING**
Countermeasures: Jamming

Software Radio Based (SDR) based Countermeasure System

- Inhibition focus on: RPAS **communications** (C2, datalinks) and **GNSS** bands.
- Different configurations: **Omnidirectional, Sectorial and Directive** Jamming.
- **Fixed, Mobile** (transport) and **Portable** versions.
- Highly adaptable thanks to its **SDR core**:
  - Jamming range: **70MHz to 6GHz**.
  - Generation of **fully programmable** signals based on **multiples types of waveforms** (white noise, chirps, used-defined arbitrary, etc).
  - Highly configurable in **number of signals and frequency bands** to be jammed.
  - Configuration of **multiple inhibition profiles** (different waveforms, bandwidth, bands, etc). Power control to adjust the inhibition range.
- Rule based **automatic** and **manual** activation modes.
Sectorial & Omni Jammer
• Sectorial and Omnidireccional
• Fast switching
• Range: +5Km

Directive Jammer
• High directive jammer with high performance camera (Indra CYCLOPS)
• 360° coverage based on PTZ positioner
• High range: +8Km

Portable Jammer
• 2 sectorial antennas
• Fast battery replacement
• Range: +3Km
Countermeasures: GPS Spoofing
Deception based on fake GPS signal.

- Real-time GPS signal generator focused on supplanting GPS L1 signal.
- Capabilities:
  - Generation and transmission of Civil C/A (Coarse / Acquisition) code of GPS signal in L1 band (1575.42 MHz).
  - Emulation of real GPS satellite constellation.
  - Generation rate of 10 positions/second.
  - Inhibition of other GNSS signals.
- Some features:
  - Full interaction with ARMS main detection sensors.
  - Omnidirectional or Directive antennas.
  - Power control.
  - Different use strategies.

GPS Spoofing
- GPS L1 C/A code
- GLONASS jammer
- Up to 16 satellites
Some ARMS Configurations

Elements for fixed deployment

Sectorial & Omni Jammer  Directive Jammer
Operational Experience

High-tech product with the aim of solving a global problem

Tested in operations area facing real threats.

Validated with positive evaluation by Spanish Penitentiary Institutions

Sold in Asian country (2018). Open leads in five continents

Participation in the Spanish MoD C-UAS program (CONDOR)
Key ideas for Civil Aviation (1)

• Facing this challenge is not easy and requires to apply the principle “The best is the enemy of the good”.

• The longer it takes to define and adopt solutions, the greater the risk becomes.

• Independently of the use case, unfortunately, 100% effective C-UAS technology does not exist, it is necessary a trade-off between performance and investment considering the balance between the most probable and the most dangerous threat.

• The best C-UAS strategy is based on:
  • Adaptation – “One configuration does not fit all the operational scenarios”.
  • Collaboration among different sensors/effectors.
  • Redundancy in number and location.

• Airport environments presents multiple specific and unique challenges to the use of C-UAS technologies.

• It is necessary specific regulation, overcoming legal restrictions (including use of spectrum), clarifying scenarios, terms of use and authority for supporting the deployment of C-UAS systems, both detection and countermeasures.
Key ideas for Civil Aviation (2)

- It is necessary to establish **common protocols and procedures** in order to face this kind of threat (Key for Seamless Sky Strategy).

- Under C-UAS Framework, **Situational Awareness and Neutralization demand different and complementary analysis** because their impact is clearly different.

- At least, as first step, let’s consider **situational awareness** (threat detection, identification and tracking).

- UAS neutralization with jamming in an airport environment could be evaluated in scenarios with runway closed for ops. This action would permit an operation impact much lower in time compared to a scenario with an operations interruption without neutralization of the UAS.

- Multiple **key questions** demand deep analysis and answers, such as i.e:
  - What is the **trigger** to take a counter-UAS action?.
  - What counter-UAS **actions** could be authorized?
  - Who may decide and take these counter-UAS actions?.