IFALPA
The Global Voice of Pilots

Position

18POS21 5 December 2018

UAS Security

Note: This paper supersedes 17POS05 - UAS Security

BACKGROUND

This Security-specific Position Paper on Unmanned Aircraft Systems (UAS), which should be read in conjunction with the general IFALPA Position Paper ***17POSO8 - Unmanned Aircraft Systems***, provides detailed IFALPA guidelines on both regulated UAS and UAS for which Regulation is either limited, not possible or non-existent. As Remotely Piloted Aircraft Systems (RPAS) are a subset of UAS, the provisions below also apply to RPAS.

REGULATED UAS

1. General

- A security threat and risk assessment of all types of UAS should be undertaken to identify and understand the threat and risk for civil aviation.
- This risk based UAS security should be regulated robustly. Where regulation is limited, not possible or non-existent, the UAS should be restricted in its operational capability.
- A Security Management System (SeMS) should be in place and a security threat and risk assessment should be integral part of operation.
- The security standards of UAS should be equivalent to those applied to similar operation of manned aircraft.
- All factors should be considered including, but not limited to, employees, location, accessibility, technology, design properties, data link protocols, command structure including responsibilities, etc.

2. UAS storage

- The UAS should be stored and prepared for flight in a manner that will prevent and detect tampering and ensure the integrity of vital components.

3. Remote pilot station

- A remote pilot station is similar in purpose to a typical aircraft cockpit; it should therefore likewise be secured from threats, sabotage, or unlawful interference.
- IFALPA strongly opposes the use of CCTV in the control room of remote pilot stations. See 18POS19-CCTV.

4. Access to UAS storage area, remote pilot station or programming station

- The premises where UA, RPS (remote pilot station) or system components are programmed, operated, stored, serviced or maintained should be regarded as a security-restricted area (ICAO Annex 17) and should have access and security controls and procedures to prevent unauthorized entry, sabotage and unlawful interference, to detect tampering and ensure the integrity of vital components.

- Persons, together with their items carried, entering these premises should be subject to identity control, screening and security controls.
- A background check should be conducted for persons granted unescorted access to these premises.

5. Personnel

- Personnel responsible for programming, preflight preparation and servicing as well as operating and remotely controlling the UAS should be security background checked.
- Security should be part of the training and awareness programs for all personnel involved in UAS operation.

6. UAS and data link

- All UA should be registered and have markings & identification.
- The UA should have a 'fall back system' in case of system failure (eg a 'fly me home system').
- The UA system should be able to prevent 'denial of service', assure 'integrity of data' and provide security of operation against jamming/spoofing etc. and to detect and react to such a breach.
- The immunity of the data (e.g. command and control) C2-link, the authenticity of the user and the correctness of data transfer and processing should be protected against threats, attacks and acts of unlawful interference.
- Steps should be taken to ensure that no additional software and/or hardware can be, or have been, added to any system component for malicious use at a later date, and that hardware and software within all system components will only perform the intended function. It is therefore essential to ensure that:

  - No other function other than the one intended can be performed;
  - All uploaded functions are verified to ensure correctness and authenticity of transfer;
  - All users of the system are authenticated to the system as authorized users of that system;
  - All commands between the system components are protected against corruption and not interfered with;
  - All commands and/or transmissions between the system components are acknowledged;
  - All system and components are separated from the public internet.

7. Security occurrence reporting

- Mandatory reporting of security occurrences should be implemented. Related data should be kept in a SeMS environment.

8. Transportation of goods

- The transportation of goods carried should meet similar security standards as those applied to manned aviation (ICAO).

UAS FOR WHICH REGULATION IS LIMITED, NOT POSSIBLE, OR NON-EXISTENT, (INCLUDING RECREATIONAL DRONES)

- All UAS should be registered
- All UAS should be identifiable (eg with sim-card technology)
- Technical (built-in) standards should be mandated to limit the capabilities of UAS with regards to their geographical position, range, speed and altitude, in order to prevent unauthorized operations in areas such as airports, heliports and airspace used by manned aviation.
- The UA should have a system that makes it detectable to other airspace users.
- Mandatory reporting of security occurrences should be implemented. Related data should be kept in one database.
- Strict enforcement should be in place if UA is used in an unsafe and/or unsecure manner.