International Civil Aviation Organization

WORKING PAPER

RPASP/5-WP/06
WG-2
18/06/16

REMOTELY PILOTED AIRCRAFT SYSTEMS PANEL (RPASP)

FIFTH MEETING (RPASP/5)

San Diego, United States – 13 to 17 June 2016

Agenda Item ..: C2 Link

CANDIDATE SECURITY RELATED SARPS

(Presented by Edward Falkov and Sergey Shavrin)

SUMMARY

C2 Link information security candidate SARPs are being proposed to be united with the organizational kind of candidate SARPs and to be included to Annex 10 Vol VI.

1. INTRODUCTION

1.1 Interception of aircraft coordinates together with its identification allows unauthorized users to guide destruction means on any certain aircraft according to periodically broadcasted surveillance signals.

1.2 An unauthorized user may use RPA as a means of remote access to the information about aircraft coordinates and identifier in case when the receiver at the remote pilot station is beyond the radio access to the signals from aircraft-victim

1.3 Launching of phantoms – when an unauthorized user transmits coordinates of a non-existing aircraft – may instigate pilots of other aircraft and ATC personnel to execute inadequate actions leading to an accident. Launching of phantoms does not need expensive equipment and high skills; to start to perform that it's enough to be educated in radio engineering.

1.4 An unauthorized user may overwhelm a pilot's or controller's display sending multiple phantoms by his transmitter at the remote pilot station or by RPA transmitter if it is necessary to transmit a phantom signal to a greater distance inaccessible for the transmitter at the remote pilot station. In this case RPA may be used both to broadcast a phantom signal and to relay it in chain order on greater distances.

1.5 The candidate SARPS being proposed are designed to overcome these threats.

2. DISCUSSION

2.1 If the C2 Link is carrying aircraft identification and temporal and spatial coordinated, then this information should be protected.

2.2 .

2.3 The C2 Link security means and procedures should provide:

2.3.1 Confidentiality of the messages, exchanged between the RPS and RPA.

It is important that C2 Link security algorithms and protocols are robust against interception of RPA position reporting and any other official data, rebroadcasting of the earlier messages recorded by the intruder, phantom induction and spam. Interception of aircraft coordinates together with its identification allows to guide destruction means on any certain aircraft according to periodically broadcasted surveillance signals.

2.3.2 Access control to authorize the RPS access to the RPA.

The C2 Link RPS-RPA establishment procedure shall be designed to avoid any unauthorized control of the RPA during this phase.

2.3.3 Mutual peer entity authentication between the RPS and the RPA.

The receiver shall use data only if the originator of the data has been positively identified. The C2 Link should be protected from the enforcement of wrong information from unauthorized sources; sources of all messages should be authenticated; use of information from unauthenticated sources should be made impossible. Providing authentication, it should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.

2.3.4 Identification to provide the integrity of data traffic between the RPS and the RPA.

When using service provider network with the risk of significant packet jitter to organize C2 Link the C2 messages should include identification means (e.g. timestamping of their generation, sequence numbering,…). Received C2 commands in this case should be executed according to their identification means. This is proposed to avoid wrong order of commands execution and to protect from the duplication or retransmission of earlier transmitted commands by the unauthorized user as well as from heaps of spam on pilot's and air controllers' displays.

2.3.5 Robustness against the possibility of design of a "dictionary" assigning the commands transmitted to the actions executed by the RPA.

2.4 The security control means shall additionally be implemented with the following characteristics:

2.4.1 All security actions have to be based on the main principle that security measures implemented should be commensurate with ARP 4754A/ARP4761.

For Catastrophic, Hazardous, Major, Major, Minor and No Safety Effects failure condition classes corresponding probabilities have to be designated in a manner uniformally for all highly-integrated aircraft systems.

A security management should lead to a threat-based, risk-managed approach under which RPAS users can assess and best manage their own security risks, threats and impacts. In a risk-based approach a risk is not zero and can never be zero, and a risk policy should be transparent, predictable and controllable, focused on the largest risk and equitable.

2.4.2 Using cryptographic algorithms with algorithm strength and key length sufficient to protect data in transit against the identified safety effect.

The C2 communication system shall provide safeguards that deny unauthorized users the ability to command and control the RPAS. First of all the RPAS should provide for the protection of C2 Link from commands sent by an unauthenticated remote pilot and guarantee impossibility of unlawful seizure of aircraft.

2.4.3 Using formally validated cryptographic modules.

C2 Link security algorithms and protocols shall provide with confidentiality, access control, integrity, authentication and nonrepudiation of transmitted data. The public key algorithms used must be robust against attempts by the cryptanalyst to create and then to use the “dictionary attacks”.

2.4.4 The necessary cryptographic strength should be provided on the message length used within the RPAS.

2.4.5 The security system should detect cyber-attacks on the system provide for adequate virus and “malware” protection (security events logging, analyses and development of appropriate countermeasures). The cyber-attack may be aimed at the system software of the RPS.

2.4.6 The RPAS must alert the pilot if the C2 link is being influenced by an unauthorized user.

3. ACTION BY THE MEETING

3.1 The working group WG-2 is invited to:

a) note and review the contents of this working paper;

b) unite it with the organizational kind of candidate SARPs earlier adopted;

c) propose the united SARPs for Annex 10 Vol VI .

— END —