International Civil Aviation Organization

RPASP/10-WP/6
23/02/18

WORKING PAPER

REMOTELY PILOTED AIRCRAFT SYSTEMS PANEL (RPASP)

TENTH MEETING

Montréal, Canada 12 to 16 March 2018

Agenda Item 4: Development of proposals related to detect and avoid
(Ref: Job card RPASP.003.04)

RPAS SURVEILLANCE AND DETECT AND AVOID (DAA) SYSTEM FOR CYBERSECURE RPAS INTEGRATION INTO CIVIL AIRSPACE

(Presented by Edward Falkov)

SUMMARY

Given document is prepared in accordance with Plenary RPASP/9 decision. Realization of surveillance is considered from ATC and remote pilot points of view. Present Manual and draft standards do not provide for the cybersecure RPAS integration into civil airspace. It is shown how cybersecurity stipulates the selection of a solution in the surveillance system. There is described an interface of C2 channel and ATC voice and data transmittance using VDL-4 only for RPAS. Solution of combined ground and airborne DAA is proposed. It is shown that VDL-4 use for RPAS only has no effect on manned aviation and ATC operation and provides for a cybersecure PRAS integration into civil airspace.

Priority: urgent

Actions: RPASP actions are stated in item 3 of given document

1. INTRODUCTION

1.1 The activities of various Working Groups (WGs) in RPASP Panel are insufficiently coordinated. For example, WG-2 is engaged in the cybersecurity of communication between a remote pilot station (RPS) and remotely piloted aircraft (RPA); a message from RPA to RPS containing, for instance, information about RPA identifier and its coordinates, must be encrypted; while at the same time the same information in ATC is left open, available to non-authorized users. No requirements are made on the cybersecurity of voice and data communication between ATC and RPA and further in C2 Link thus allowing non-authorized users to affect RPA flights management.

1.2 Against the absence of a general decision on manned aviation security the proposal is given on cybersecure integration of remotely piloted aircraft systems (RPAS) into civil airspace.

1.3 The goal of given proposal is not to touch the cybersecurity provision problem for all civil aviation, it only concerns RPAS and does not worsen the general situation while integrating into civil aviation such a sensitive to cyberactions segment as RPAS.

Note: Appendices to this paper are not all referenced in the main body of the paper, but are cross-referenced in other Appendices.

(21 pages)

2. DISCUSSION

2.1 Mandatory conditions of RPAS integration into civil airspace

2.1.1 Mentioned conditions are given in Appendix A.

2.2 Cybersecurity provision in RPAS integration into civil airspace

2.2.1 Fig 1 shows the scheme of RPA-RPS and RPA-ATC interaction in compliance with RPAS Manual [1].

2.2.2 Fig 2 shows a relevant possible hacker-RPA interaction through a penetration in an unprotected C2 (Command and Control) channel and in voice and data exchange channel in VHF band (in case such an data exchange takes place). For the interaction scheme in Fig. 1 there are foreseen no cybersecurity actions. A hacker is able to receive information and affect RPAS flights via upward and downward C2 Link between RPA and RPS as well as through voice and data exchange system between RPA and ATC.

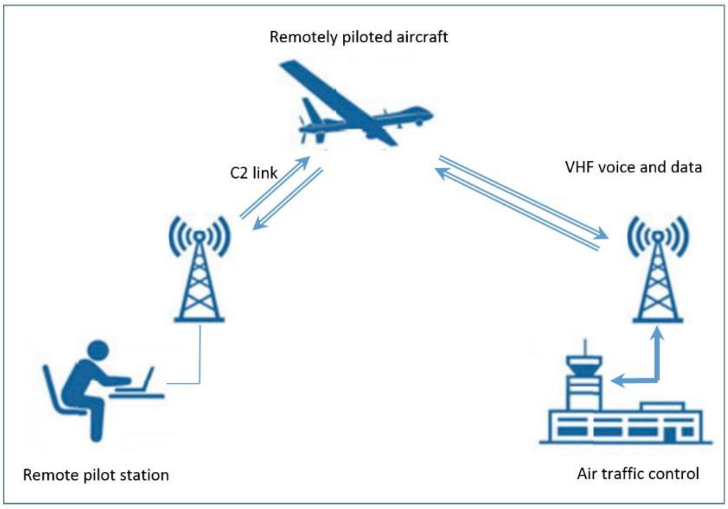

Fig. 1. RPA, RPS and ATC interaction according to Doc 10019.

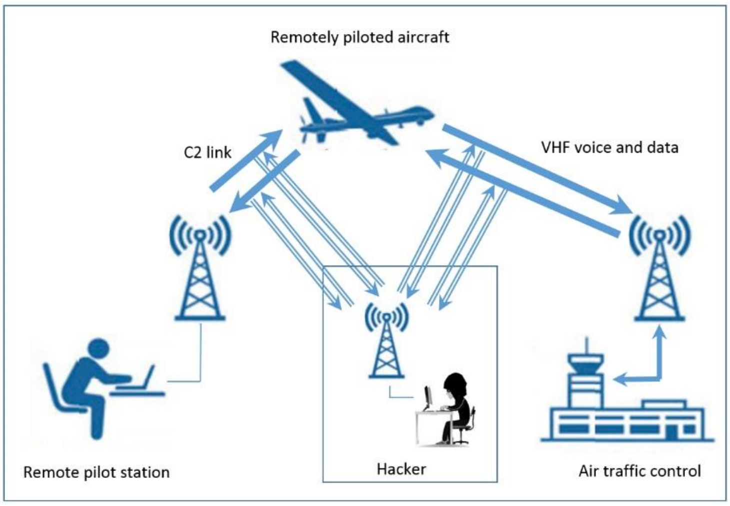

Fig. 2. Hacker-RPAS interaction via C2Link and voice and data messages between RPA and ATC.

2.2.3 Note that up to 2018 beginning WG2 has developed a package of documents and draft standards determining requirements for C2 Link cybersecurity (see Fig 3). If these requirements are implemented, a hacker will be unable either receive downlinked RPA information or uplink any command in RP-RPA channel in order to change the flight route (that causes the greatest fear when RPA appears in airspace); meanwhile there are no changes either in on-board equipment of manned aircraft, or in ATC equipment and procedures. Some cybersecurity problems get solved. However there remains a possibility of cyber effect on RPAS via RPA-ATC channel. The situation worsens further because there is no cybersecurity of ATC voice and data transmittance in civil aviation.

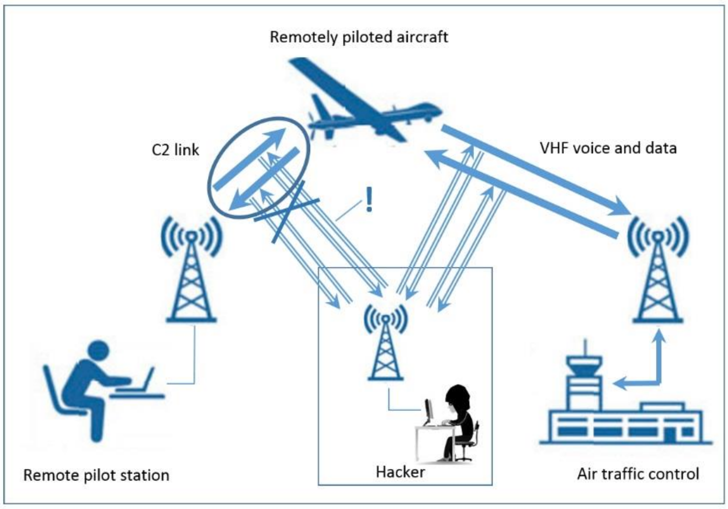

Fig. 3. Cybersecure RP-RPA interaction, voice and data exchange channel between RPA and ATC is not cybersecure.

2.2.4 To be protected from cyber intervention in RPAS operation we propose a solution which eliminates the possibility to acquire information and intervene in RPAS operation in their flights management in civil airspace (Fig. 4). Fig. 3 and 4 show that before broadcasting the messages are encrypted, so that they were available to authorized users only. The above said concerns RPAS only and has no effect on manned aviation flights management. The content of the proposal is described below in 2.4-2.6.

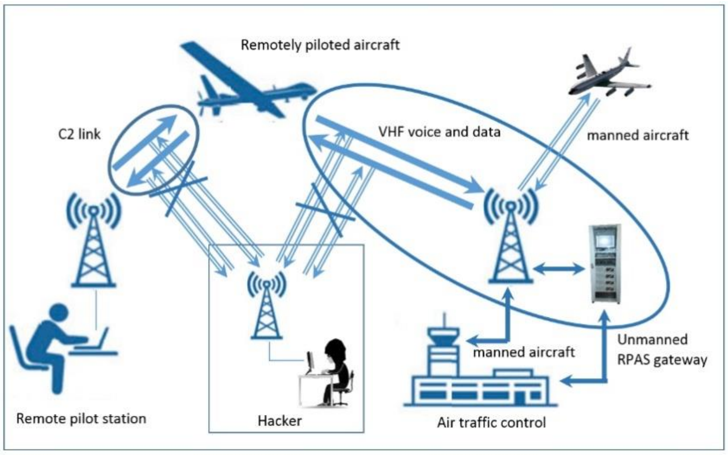

Fig. 4. Cybersecure integration of RPAS in civil airspace.

2.3 Main methods and means of aircraft surveillance

2.3.1 Since surveillance and DAA problem is one of the main problems in given WP and this problem faces some disagreement in different RPASP groups, it is studied in Appendix B.

2.3.2 After consideration of ICAO approved methods of aircraft surveillance the analysis showed that as concerns RPAS, the most preferable surveillance method under ATC and RPS is the automatic dependent surveillance – broadcast (ADS-B).

2.4 Analysis of various data links for ADS-B implementation from ATC and RPS points of view

2.4.1 This analysis is given in Appendix C. It is shown that with the account of cybersecurity requirements and other factors the preferable method is VDL-4 application.

2.5 Remote pilot – ATC voice and data interaction

2.5.1 We have analyzed the remote pilot-ATC voice interaction according to Doc 10019. Analogue voice is digitized before entering C2 Link at each RPA. This type of interaction is not cybersecure, so a hacker is able to listen to an ATC controller’s instructions as well as to give his own false instructions to the remote pilot. The same concerns voice information from a remote pilot. Data exchange between ATC and RPS is not cybersecure too.

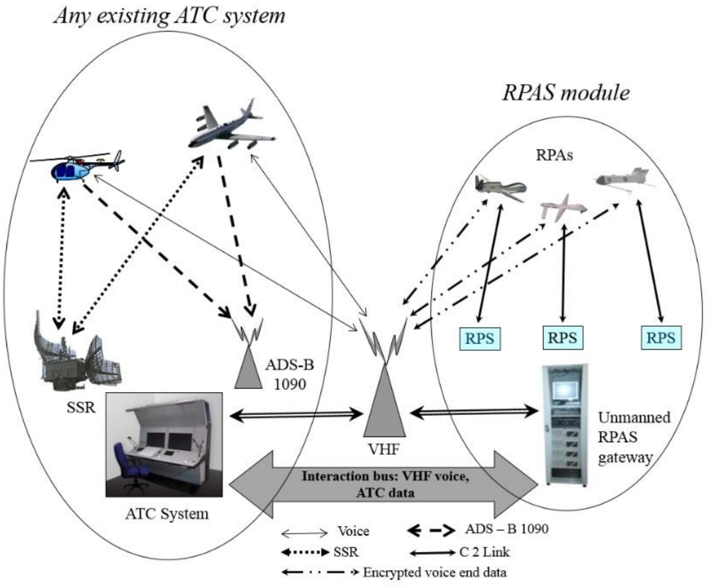

Fig. 5. Cybersecure ATC-RPA-RPS interface

2.5.2 For cybersecurity provision it was proposed to apply additional ATC equipment concerning exclusively RPAS – unmanned ground RPAS gateway. The related to RPAS module includes all RPA with relevant RPS and ground RPAS gateway performing “unique window” functions for all RPAS when interacting with ATC. All voice information from ATC to the remote pilot is centrally encrypted in the gateway; having passed RPA voice messages are decoded at RPS. In the opposite direction encrypted at RPS messages are sent via RPA to the gateway where they are decoded and synthesized in analogue messages and enter ATC as such. ATC-RPS data exchange is done in the same two-way cybersecure manner. Description of this interaction is given in Appendix D. Presence of a ground RPAS gateway which has to be developed and certified has no influence on manned aircraft flights management, though it provides for the situational awareness of remote pilots.

2.6 DAA management with the help of RPAS module

2.6.1 Proposals on the management of combined detect and avoid system both airborne and ground-based are given in Appendix E.

Note: All the list of used references is given in Appendix I.

3. RPASP ACTIVITIES

The RPASP is invited to:

a) Take in mind the contents of this working paper;

b) To agree to organize a joint discussion of given WP with WG2, WG3, and other WG within RPASP;

c) To delegate this document to SP, FMSP, AVSECP proposing to organize a joint discussion of suggested in this document solutions for the early implementation of B1-RPAS module;

d) To endorse lines of activities given in items 2.3-2.6 concerning management of cybersecure RPAS surveillance and DAA;

e) To agree that work continues as outlined in this document on suggestions concerning RPAS integration into civil airspace and that a final report be submitted at the next RPASP meeting

— — — — — — — —

APPENDIX A

1. Mandatory conditions of RPAS integration into civil airspace

It seems that conflict-free and efficient integration of RPAS into civil airspace in a foreseeable and time-acceptable period indicated in ICAO Global Air Navigation Plan (B1-RPAS module) is possible on following conditions:

– availability of proved by ICAO standards technologies, applicable both for piloted aircraft and for RPAS; these technologies must first of all pertain to basic flight functions of any aircraft, that is communication, navigation, surveillance as well as to RPA-remote pilot and RPA-ATC (voice and data) interaction;

– innovations, implemented in order to solve the above integration task, should neither concern current ATC procedures, nor require for modifications of equipment on-board piloted aircraft and in ATC in the part of manned aircraft flights;

– due to specifics of RPAS operation, first of all absence of pilot on board an aircraft and resulting increased sensitivity of RPAS to all kinds of cyber effects, applied engineering solutions must be to the most extent protected from consequences of unintentional mistakes of well-meaning users (remote pilot, ATC, other legal users of airspace) as well as from intentional cyberattacks which can arise during RPAS flights.

— — — — — — — —

APPENDIX B

1 Main methods and means of aircraft surveillance

1.1 Let's consider one of main ATM functions, that is aircraft surveillance; regarding RPAS it is necessary to consider both RPA surveillance by ATC and RPA surveillance management by RPAS remote pilot. Notionally this consideration was given in [2] in 2015.

1.2 Let us operate like a bulldozer or like a fine-meshed fishing net, that is we'll investigate <u>all</u> available for this purpose technical solutions approved by ICAO standards.

1.3 General position of ICAO concerning any aircraft surveillance by ground ATC involves following technical methods and means: secondary surveillance radars (SSR) in A/C/S modes; multilateration (MLAT); satellite navigation data allowing to implement automatic dependent surveillance-broadcast (ADS-B).

1.4 ATC may conduct RPA surveillance by any of the three methods mentioned above. In this way it is enough to have an SSR transponder, or MLAT transmitter, or ADS-B transceiver on board a RPA.

1.5 To control an RPA the remote pilot should also know the position, velocity and other parameters of RPA, that is the pilot should conduct RPA surveillance in its classical consideration, whereas meeting required surveillance performance (RSP) in given airspace. It would seem strange if these requirements differed. For example, ATC determines an aircraft position once 5 seconds with 50 m accuracy, while the pilot determines his aircraft position once 5 minutes with 5 km accuracy. In such a case it is needless to demand secure air traffic management from ATC. For considered airspace it is necessary that both remote pilot and ATC observed the same aircraft surveillance requirements.

1.6 Use of equipment in SSR transponder mode on board an RPA entails a necessity to install a secondary surveillance radar type system at every RPS. Not infrequently this idea meets some discussions. Sometimes this function is delegated to a future and thus misty and magic telemetric C2 (Command and Control) datalink. What features shall possess this mysterious datalink?

a) First of all, this datalink must work without reference to ATC, and the remote pilot must be able to determine RPA position independently of ATC in case of potential ATC failures, radar coverage breaks, etc. In event of such failures in ATC, the manned aviation pilot continues his flight with the help of own satellite navigation means or a FMS; the remote pilot also should continue his flight in the same manner, using his own independent of ATC navigation means;

b) Secondly, independently of such a datalink's name it should:

1) apply an SSR transponder;

2) volume of information transmitted from PRA to the remote pilot will evidently be greater than the volume of information transmitted from RPA to ATC due to presence of additional information about control surfaces, health of on-board systems, etc.);

3) such a datalink should operate approximately at the same ranges as in RPA-ATC interaction with SSR help, if, for instance, RPS is within ATC area. It would be quite strange, if the range of ATC-RPA interaction was, say, 400 km, while the range of RPA-RPS interaction was, for instance, 50 km – such a situation would require for too frequent RPS displacement in the area of ATC activities.

1.7 SSRs being developed for many years are characterized by some perfection, so emerging datalinks will have to reach the same characteristics concerning power, sensitivity, physical dimensions and power consumption. Let's assume that it is also necessary to install some SSR type systems at RPS. Usually such a station is at best based on a small van or RPA surveillance/control is done with the help of handheld apparatus carried by the remote pilot. From a practical standpoint, neither dimensions/consumed power and other technical parameters nor cost allow to use secondary radars for RPAS from RPS position. Besides, and it is more important, simultaneous operation of many SSRs (regular ATC and additional RPAS) will lead to a significant over-load of the radar field.

1.8 Mobile RPS also excludes the possibility to use MLAT, which represents a set of time-synchronized spaced wide apart (15-20 km or more) receivers of radio radiation.

1.9 So, among above studied and approved by ICAO methods of surveillance from RPS point of view, the only acceptable method of RPA surveillance is ADS-B. The use of SSR transponder and MLAT transmitter functions on board a RPA which the remote pilot does not apply for RPA control because of on-board restrictions on mass, power consumption, cost, etc., is counter-productive. It seems that an attempt to force the unmanned aviation society to install SSR transponders or MLAT transmitters on board RPA separately from the solution of remote pilot-RPA interaction problem will be inacceptable. In conformance with NextGen and SESAR, since 2020 the unmanned aviation society will be authorized to call for mandatory use of ADS-B.

— — — — — — — —

APPENDIX C

Analysis of different data links to realize ADS-B for RPA surveillance from RPS and ATC points of view

1 All data links for ADS-B will be considered

1.1 ADS-B implementation is possible with the use of several various data links, approved by ICAO. Let us operate in the same (as in Appendix B) bulldozer-like style – that is we'll study **all** data links approved by ICAO for ADS-B implementation. Successive review of standardized data links for ADS-B implementation shows the following.

2 ADS-B/1090 implementation for RPAS from ATC point of view

2.1 When using ADS-B based on 1090 ES data link (ADS-B/1090) in conformance with ICAO Doc 9924 [3] it is necessary to bear in mind following possibilities to validate ADS-B/1090 data.

From [3]: *"3.3.2 Since in critical segments of their operation many surveillance systems rely on electronic means depending on the outcome of the security analysis, it is necessary to manage protection of surveillance data from malicious electronic attacks or unlawful intervention. Recommended measures to be taken against those malicious threats include:*

a) Anti-spoofing
Some surveillance systems such as SSR and ADS-B are vulnerable to spoofing. ATM automation systems can reduce this vulnerability by correlating targets with other data such as flight data, flight profiles within the flight data processing system, and overlapping surveillance data from other sources such as radar and multilateration, where available.
ATC further reduces this vulnerability by correlating the surveillance picture with voice communication, inter-centre coordination, etc. to estimate the situation…".

2.2 In the framework of informal discussions of Doc 9924 at ICAO Panel it is proposed to mitigate ADS-B/1090 data vulnerability by correlating the surveillance picture with voice messages (so what ATC automated operation can we then speak about) and other data in ATC center. If an aircraft is being surveyed by several ADS-B stations simultaneously it is proposed to apply multilateration for the aircraft position verification.

3 RPA surveillance with ADS-B/1090 from RPS point of view

3.1 If above rather abstract possibilities may (if ever) be somehow applied for ADS-B/1090 data verification in ATC, RPAS remote pilot evidently has no such capabilities, so there remain no other ways of ADS-B/1090 data verification except SSR or MLAT. The replacement of MLAT receiving stations by ADS-B stations working in a group and transition to multilateration methods just worsens the situation for remote pilots.

3.2 Besides, according to currently developed drafts of ICAO standards for RPA cyber security planned to be issued in 2018 [4], RPA message to the pilot with aircraft identification and coordinates must be available to authorized users only, and this can be achieved only encrypting the messages. In fact, multiple attempts to encrypt ADS-B/1090 messages proved their unavailability, and it might be because cybersecurity provision here could be based on two-key cryptographic technologies. Such technologies necessitate a dialogue protocol for the information exchange between pairs of objects with minimum length of encrypted messages not less than 160 bits. ADS-B/1090 works with shorter messages and does not support dialogue protocols for the information exchange that's why it is not able to provide for ADS-B/1090 cybersecurity.

3.3 Since ADS-B/1090 cybersecurity cannot be provided otherwise than by a symmetric cryptography method reinforced by time stamps, implementation of which demands for information exchange in a dialogue mode and longer messages, 1090 data link does not support the necessary robustness of security.

4 Cybersecurity provision under ADS-B/1090 – additional aspects

4.1 As shown above, one of main reasons of the unacceptability of ADS-B/1090 use for RPAS is the lack of cybersecurity. Let us enlarge upon this point.

4.2 [4] says, “C2 Link security is the main challenge in the provision of RPAS operations security”. Lately ICAO RPAS WG2 has issued several working papers (WP) and drafts of SARPs concerning RPAS C2 Link cybersecurity. A document with C2 Link requirements is scheduled for adoption in 2018 with implementation in 2019. Certain statements of C2 link cybersecurity in SARPs ICAO draft may be briefly given as follows.

a) It is necessary to define procedures of time reference establishing, time stamping of information, hardware and software, and verification of date and time.

b) Procedures for encryption systems: statement and implementation of cryptographic controls (keys) management policy, identification of purposes of keys, who and how applies them by defining associations between people, objects and roles. Therewith it is necessary to define procedures for key generation that assure the authenticity (provenance) of software, hardware (including cryptography devices) and storage information, keys including; procedures of distribution, deletion, invalidation and recovery of keys.

c) For operations: digital certificates and cryptographic keys must be generated according to processes and practical recommendations given in ED-204, the receiver should use the data if only their source was exactly identified and validated. It is necessary to bear in mind robustness to cyber-attacks as well.

d) C2 Link security algorithms and protocols shall provide adequate levels of security goals such as confidentiality, access control, integrity, authenticity and accountability (including non-repudiation) of transmitted data, for those kinds of operation which require certification.

4.3 Earlier RTCA DO-242A considered replacement of SSR by ADS-B/1090. Numerous researches of ADS-B/1090 from Costin to Strohmeier [5-6] confirmed total insecurity of ADS-B/1090 applications. On this reason it is necessary to confirm ADS-B/1090 data. The last phrase from [7], devoted to possibility to encrypt ADS-B/1090 messages, looks as follows, “ADS-B will continue to rely on radars for authentication— ironically, just the very technology it had to replace”.

4.4 Till now we discussed air-ground surveillance. However to provide for the situational awareness of pilots, including RPAS ones, it is necessary to provide for air-air surveillance. If before the cybersecurity challenge it was planned to apply “any” ADS-B/1090 data surveillance, now due to the need of verification these data may be applied only in case of TCAS use, thus significantly decreasing the operation range and nomenclature/types of interacting aircraft. Equipping of RPA by TCAS looks mandatory, thus radically increasing RPAS cost. Situational awareness of pilots beyond TCAS range (40-50km) is impossible. RPAS interaction with helicopters and general aviation falls out from the study, and it is especially critical in G class airspace.

5 Cybersecurity provision for UAT data link use

5.1 Global use of UAT datalink seems unacceptable due to following reasons:

- 978 MHz frequency used in UAT datalink for surveillance contradicts statements [8] where this frequency belongs to a band intended not for surveillance, but for navigation;
- given frequency is globally used in DME navigation receivers; according to this reason Eurocontrol stated that UAT will never be used in Europe;

- at present the author has got no information about the possibility to encrypt ADS-B messages on UAT basis.

6 *RPAS integration into civil airspace with VDL-4 use*

6.1 The only not discarded still not yet studied ADS-B for RPAS remains ADS-B based on VDL-4 (ADS-B/4). The analysis shows that only this data link answers requirements stated in SARPS draft [4] and provides for the cybersecurity of RPAS application by encrypting ADS-B data for authorized users. To prevent spoofing, if necessary, in ATC system there may be performed an additional check of estimated distance between the transmitter and receiver of ADS-B/4 messages with the help of time stamps inserted in these messages in conformance with ICAO standard for VDL-4 (Doc 9816). Such a possibility was confirmed by the results of computer simulation performed in FGUP “GosNIIAS”, see Appendix F. In fact, distance estimation is an optional procedure for aircraft-ATC surveillance, since encrypted ADS-B/4 messages provide for secure surveillance while messages without appropriate keys are not taken into account. Meanwhile given method of ADS-B messages verification is quite valuable for air-air surveillance because there are no other ways to execute such verification.

6.2 How do we suppose to manage RPAS surveillance considering practical absence of ADS-B/4 use for manned aviation and the demand not to change anything in avionics of manned aircraft and ATC equipment connected with manned aircraft management, in the world? The answer to this question was given in [9], which proposals in brief can be stated as follows: avionics and flight rules for manned aircraft remain unchanged, VDL-4 data link use has no effect on them; ATC equipment and flight support procedures also stay the same, excluding the introduction of a supplementary ground equipment unit which is applicable only to RPAS, does not belong to ATC equipment for manned aircraft and serves as a unique common ground unit for all RPAS, something like a “unique window” for the acquisition and transmittance of information from all RPAS to ATC via computer-computer interface, as well as for the transmittance of ATC indications to all remote pilots through relevant RPAs. Description of the interaction mechanism of RPAS set as a part of civil airspace including the case of self-organizing airborne networks (SOAN) use and including the BRLOS case [10] and [9] is given in Appendixes D and E.

— — — — — — — —

APPENDIX D

1.1 Remote pilot-ATC voice and data interaction with the help of unmanned ground RPAS gateway.

1.1 First of all let us see how it was supposed to manage voice interaction between remote pilot and ATC according to Doc 10019 Manual.

1.2 The document foresees following interface between ATC communication (data + voice) and C2 data link. It is supposed that RPA has got at least one VHF radio and C2 data link has VHF frequency to provide for voice and data communications, if needed.

Here (Fig, 1) analogue VHF voice messages from ATC controller to remote pilot (RP) first go to ATC VHF antenna, then to RPA, are digitized and then are relayed to remote pilot station (RPS) via C2 data link where they are converted in an analogue form to be perceived by remote pilots. Voice messages from RP to ATC are digitized at RPS, sent to RPA via C2 link, converted to analogue voice messages on RPA and then transmitted to ATC VHF antenna and go to ATC VHF radio receiver.

1.3 Asymmetrical approach (ATC staff send and receive voice messages in an analogue form while RP does the same in a digital form) is explained by the wish not to change anything in ATC equipment and procedures in the global scale. Nevertheless, this significantly complicates the equipment of all RPAs, both large and small ones, and should be executed considering limitations on mass, size, installation in RPA, consumed power, control, maintenance, etc.

1.4 One of main disadvantages of given in Manual 10019 method of RP-RPA-ATC communication management is its vulnerability to cyberatacks. Later WG2 has developed requirements for C2 link cybersecurity in RPAS, thus providing for the cybersecurity of transmittance of “internal”, created at RPA data to the remote pilot and control commands from the remote pilot to RPA. Meanwhile, since C2 Link is the only source of information for remote pilot, this channel shall transfer data and voice from ATC in both directions. Here it does not matter whether these data and voice are encrypted in C2 Link or not. Illegal user (Fig. 2) may intercept data from/to ATC and from/to RPA and send wrong information to the same addresses. Wrong information sending may be organized both from the ground and in the air with the help of special RPAS, for instance. Received by RPAS information is not controlled by any means. The same concerns RPAS information sent to ATC.

1.5 Another possible method may be the one when voice messages from ATC to RPS are digitized not on board every RPA but at a common site near ATC ground facility. Surely it will demand to install new certified ground equipment. Digital voice communications are much easier and more efficient in use; it is a common way in all sound-recording industry as well as in wireless telephone communications. New equipment located on the ground will not affect the operation of piloted aircraft and will concern only RPAS activities. Along with VHF voice communications it will be also possible to relay data in a cybersecure way from ATC to RPA and then to the remote pilot via C2 link. Thus, it is necessary to have a gateway between ATC communications (voice + data) and C2 datalink, and here we can study two approaches. The first is to change nothing in ground equipment and to assign all tasks to RPAS with due attention to above mentioned limitations on installation, etc. The second approach is to simplify the on-board part of RPAS and delegate some tasks to the ground though not to former ATC but to certain ground modules of RPAS, in order to establish an **unmanned ground RPAS gateway** (Fig. 5).

1.6. Here it looks proper to give a following analogy. While establishing aircraft surveillance it is possible to make significant investments in the upgrade of primary surveillance radars (PSR) not touching aircraft. However, organization of cooperative surveillance based on secondary surveillance radars (SSR) where the surveillance upgrade work was split between ground and on-board means turned be much more efficient.

1.7 Organization of an unmanned ground RPAS gateway will have no effect on the management of piloted aircraft flights but will provide for cybersecure information entry in both directions – from RPAS to ATC to build up a complete ATC picture and from ATC to RPAS to perform flights under total ATC control. Instead of many gateways on board RPAS under significant restrictions we will apply one common unmanned ground gateway providing cybersecure transfer of ATC-RPAS communication. Hackers (compare with Fig. 2) will be unable either to intercept RPAS messages to ATC and ATC indications to RPAS, or to send wrong information to ATC and RPAS. Mentioned service is achieved through the use of self-organizing airborne networks and encryption of information, the requirements are described in [11-12] and foresaw by SARPs drafts [4]. All RPAS are served in both directions through a "unique window", meanwhile it becomes possible to cybersecurely integrate RPAS into civil airspace regardless of the cybersecurity in given airspace (generally speaking, not cybersecure at present).

1.8 RPAS module includes:

- RPAS systems which control RPA from relevant RPS with the help of C2 data link;
- unmanned ground RPAS-gateway providing for RPAS-ATC interaction.

Within RPAS module every remote pilot station controls relevant RPA operation with the help of C2 link including ADS-B/4 use for surveillance. Note that in Russia VDL-4 is actually used to also transmit commands in flight.

1.9 Besides voice communications interface the ground RPAS gateway also solves the task of surveillance interface. Let's consider the case when in certain airspace piloted aircraft are under SSR surveillance. ATC gets information about RPAs from the gateway. The gateway receives ADS-B/4 data from RPA and sends it to ATC; additionally, ATC fulfills TIS-B function, sending information to all unmanned aircraft and finally to all RPSs with ADS-B/4 In function. Thus RPAS and ATC have got an interface both for communication and surveillance.

1.10 Cybersecurity in RPAS integration into civil airspace is achieved by the following:
Digital ADS-B messages based on VDL-4 (ADS-B/4) after their creation at RPA are encrypted there and then transmitted to RPS providing for the cybersecurity of C2 Link. At RPS ADS-B/4 messages are decoded and go to the disposal of the remote pilot. At the same time these encrypted messages from RPA go to the ground RPAS gateway where they are decoded in a centralized manner and then sent to a feeder between gateway computer and ATC computer. Voice messages from the remote pilot to RPS are transformed in digital form, are overlaid on VDL-4 protocol, then are encrypted and through C2 Link are transmitted to RPA; then from RPA encrypted digital voice messages are relayed to the ground gateway. In ground gateway encrypted messages are decoded, transformed to analogue form and then through the feeder go in analogue form to ATC system to be used by the controller. In opposite direction voice messages in analogue form go from the controller through the feeder to the ground RPAS gateway, where they are digitized and encrypted, then these messages through RPA enter RPS, where they are decoded and used in analogue form by the remote pilot. ATC digital/data messages of TIS-B, FIS-B, DGNSS, A-SGMCS, CPDLC, AOC, S&R, etc. type enter the feeder, get encrypted in the ground gateway, and are transmitted to RPA, then they are relayed to RPS, decoded and used by the remote pilot. At last the information circulating within RPAS is fully cybersecure as well as information between RPAS and ATC. The consequent use of this information in such ATC services as TIS-B, Party line for piloted aviation from the point of cybersecurity is under ATC responsibility.

1.11 According to Fig.5, the implementation of given scheme provides for following operational benefits:

- present ATC (left envelope) acquires needed information about all aircraft positions: in traditional for concerned ATC way for piloted aircraft, and using digital ADS-B/4 messages via a ground gateway and a feeder between the gateway computer and ATC computer - for RPAS; voice messages from RPAS pilots are digitized at RPS, get encrypted and enter RPA via C2 channel, from where they are relayed to the ground gateway get decoded and then through the feeder of gateway computer - ATC computer connection they enter ATC in an analogue form. All information entering ATC from all RPAS is cybersecure. If necessary, under ATC responsibility RPAS voice messages may be relayed to the air via ATC VHF antenna to provide for the situational awareness of manned aviation pilots by the help of voice messages. Nothing is changed here in ATC system as itself, except acquisition of information from the ground RPAS gateway. If needed, RPAS digitized voice messages may be transmitted via a gateway to other RPAs. RRA and remote pilots will receive digital and voice messages in the opposite direction from ATC (with the transformation of analogue voice messages into digital ones in the ground gateway). After entering RPAS gateway the messages go to relevant RPS.

1.12 As a result, we have following functioning:

- ATC controller possesses all digital information about manned and unmanned IFR aircraft; the controller is able to send voice messages to any pilot and hear their voice messages; all pilots of manned and unmanned aviation are able to hear voice messages from controller and all other pilots (considering above restrictions about cybersecurity of voice message transmittance from RPAS pilots for Party Line provision), procedures of ATC operator’s work remain unchanged;

- pilots of manned aircraft interact with controllers and with each other in conformance with procedures approved for given airspace;

- remote pilots interact with controllers by voice messages; besides, with the help of ADS-B/4 messages transmitted via said feeder, they may receive controller’s commands and TIS-B information about positions of piloted aircraft for situational awareness; remote pilots are able to listen to voice information from all airspace users. Separate of flight rules in given ATC system (left envelope), remote pilots of RPAS will be aware of the situation concerning all RPAs thanks to direct interaction with RPAs by ADS-B/4 function.

2 Necessary innovations demanding development and certification of ATC equipment for cybersecure RPAS integration into civil airspace

2.1 The only change in the ground part is the creation of a non-serviced ground RPAS gateway and connecting feeder between the gateway computer and the ATC one. Ground RPAS gateway and communication feeder (which, as it has been mentioned already, are not used for manned aircraft flight management but provide services just for the RPAS ground segment as well as their connection with ATC and delivery of TIS-B information from ATC, if it has not taken place earlier), will demand for development, standardization and certification.

2.2 The problem of frequency channels congestion in VHF band is well known. According to Fig. 5, innovations in given scheme of RPAS integration in civil airspace concern VDL-4 use only within RPAS module, ATC system for manned aircraft management remains unchanged. In this case it will be enough to have no more than two dedicated VHF frequencies; all main functions are planned to be executed in one frequency. In conformance with [8], item 4.1.3.3.2, “…136.925 MHz and 113.250 MHz frequencies will be provided as common signaling channels (CSCs) to the VHF digital link Mode 4 digital link (VDL Mode 4). These CSCs use the VDL Mode 4 modulation scheme”. So RPAS integration with VHF band use will be performed in frequencies globally dedicated for VDL-4. If there are many RPAS near ATC center or ground RPSs, geographical dimensions of the cell around said ground receiving sites automatically get narrower, according to VDL-4 Manual [13]. Application of above self-organizing airborne network [9] automatically solves the problem of necessary messages delivery through a set of appropriate nodes of the airborne network.

— — — — — — — —

APPENDIX E

DAA management with RPAS module application

1.1 Some notes to suggestions in [14] before DAA RPAS consideration.

«3.2 Surveillance of aircraft equipped with SSR transponder”

From [14] follows that SSR transponder will be mandatory installed in RPA. Insights of that are given in sections 2.3-2.4 of this WP from the remote pilot’s point of view and show that the use of SSR transponder for RPAS from the remote pilot’s point of view might be inefficient.

«3.3 Surveillance of aircraft equipped with ADS-B Out»

Analysis of ADS-B based on different data links is given in sections 2.3-2.5 of this WP. Once again insights from the remote pilot’s point of view concerning the cybersecurity and other factors cause doubts about ADS-B/1090 use for RPAS.

2 DAA proposal

2.1 It is proposed to review following RPAS and **DAA** system combination (partly airborne, partly ground-based) with the participation of ground RPAS gateway:

2.1.1 “Piloted aircraft – piloted aircraft” conflict. This case might be also reviewed as RPAS-free airspace. DAA algorithm is being solved here according to existing rules.

For aircraft equipped with TCAS it should be taken into account that at the first step of TCAS operation there are used input ADS-B/1090 data in order to decrease of number of interrogations; this data are vulnerable to spoofing, they can’t be validated at ranges beyond TCAS capability, actually, the first step must be deleted.

2.1.2 “RPA - RPA” conflict, or piloted aircraft-free airspace. In general, the responsibility for this conflict solution should be delegated to an ATC controller because he has an access to all secured and reliable data about RPA position, velocity vector, intents and others. ADS-B/4 data persistently and without delays enter ATC from RPA through a ground RPAS gateway. After an analysis of the flight situation the controller may give voice or/and digital/data commands to remote pilots about how to resolve the conflict.

At the same time however two conflicting RPAs have got two independent sources of information in the form of coordinates from secured ADS-B/4 messages and the distance between two RPAs calculated on time stamps, so it is possible to develop and implement an additional direct airborne DAA system; as a result ground-based DAA will be replaced (or complemented) by an airborne one. If due to any reason piloted aircraft (helicopter or GA) was equipped with ADS-B/4, DAA for it and RPA would be solved by airborne DAA in given manner.

Now it makes sense to turn to the definition from [14], item 1.1:

«*Airborne collision avoidance system (ACAS).* An aircraft system based on secondary surveillance radar (SSR) transponder signals that operates independently of ground-based equipment and provides advice to the pilot on potentially conflicting aircraft equipped with SSR transponders.

Note.— SSR transponders referred to above operate in Mode C or Mode S.»

The airborne collision avoidance system is toughly connected with the only technical solution based on SSR transponder in Mode C or S. As we could see, above collision avoidance task can be successfully solved by other methods and means, besides SSR transponder. At the joint meeting of RPASP and SP the approach based on the simultaneous review of ADS-B data (at that time not encrypted) use and independently providing the distance between airspace users was marked as an acceptable one for DAA. From the perspective to apply not specific technical solutions, but a performance based approach it is necessary to change ACAS definition.

2.1.3 “Piloted aircraft – RPA” conflict or mixed airspace. This case shall be delegated to an ATC controller. He has an access to all information. It should be taken into account that only secured RPAS data are transmitted with two independent sources of information – by GPS/GLONASS navigation data with ADS-B/4 function and by estimating of the distance between RPA and the ground gateway (directly or along a chain of nodes in case of SOAN in BRLOS mode) using time stamps in ADS-B/4 messages. Information about piloted aircraft must be secure under the responsibilities of ATC controllers, for example, ADS-B/1090 must be estimated by SSR or MLAT data. It is necessary to develop and implement given ground DAA.

2.2 Requirements concerning cybersecurity provision for DAA on the basis of methods developed by WG2 and stated in WPs, have been discussed at WG2 and WG3 joint meeting. Summary of mentioned documents is given in Appendixes G and H.

— — — — — — — —

APPENDIX F

ADS-B/4 distance measuring between the traffic participants

ADS-B messages within the VDL Mode 4 datalink are transmitted referenced to the UTC. This fact can be used to provide distance measuring between aircraft or even between any pair of objects participating in ADS-B procedure. The distance between two objects – transmitter and receiver – can be calculated as a product of message propagation time and the speed of light. As soon as VDL Mode 4 message transmission start is referenced to the beginning of a timeslot, so the reception time is to be measured to evaluate the propagation time.

The propagation time measurement accuracy is very much influenced by time scale scattering for different objects. In order to reduce (or theoretically eliminate) this influence the following procedure is proposed.

1. Object A transmits an ADS-B message at t_1 of object A time scale, corresponding to the beginning of a time slot.

2. Object B receives this message at t_2 time of object B time scale (this time should be measured) and as soon as possible (typically within a frame) transmits his own ADS-B message at t_3 time of object B time scale (beginning of another timeslot) containing a time stamp t_2.

3. Object A receives the object B ADS-B message at t_4 of object A time scale.

If necessary, the t_1 and t_3 originating time stamps can be included to appropriate ADS-B messages.

Time scale scattering elimination can be expressed as follows.

If T is some absolute (and unknown) time, current time t_A for object A is $t_A = T + \delta_A$ of object A time scale and $t_B = T + \delta_B$ of object B time scale (where δ_A and δ_B are unknown values of time scattering), then the message propagation time t_{prop} between objects A and B and back is expressed as:

$$t_{prop} = [(t_4 - \delta_A) - (t_1 - \delta_A)] - [(t_3 - \delta_B) - (t_2 - \delta_B)] = (t_4 - t_3) + (t_2 - t_1)$$

The main advantage of the algorithm proposed is the possibility of measurements automation during the periodical broadcasting of ADS-B messages and, besides, it requires no changes of the equipment operation.

One more factor of measurement accuracy reduction is noise influence. It is to state the message time position and to reference it to the common time scale, causing random time position jitter.

This problem can be softened by correlation signal processing principles employment on signal reception. Correlation processing should be implemented to the invariable segments of the message – such as training sequence and opening flag.

The results of computer simulations of distance measuring are presented in Table 1.

Table 1. The results of computer simulations of distance measuring

Distance, km	σ, m	δ,%
0	0	0
5	3	0.06
10	15	0.15
50	10	0.02
100	30	0.03
200	120	0.06
400	250	0.07

— — — — — — — —

APPENDIX G

2.1.2. Cybersecurity for DAA

2.1.2.1. [Standard] Cybersecurity principles shall be observed throughout the design and operational use of the DAA system.

Note. – Guidance material on cybersecurity principles can be found in Chapter 18 of Doc 8973, CYBER THREATS TO CRITICAL AVIATION INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS

2.1.2.2. [Standard] Information exchange between components of the DAA system, e.g. through the C2 Link, shall be cryptographically protected.

Note 1. – It is assumed that the C2 Link is secure.

Note 2. – In cases where technical means can not be used to achieve this, operational means may have to be used.

2.1.2.3. The cybersecurity means and procedures should provide:

2.1.2.3.1. Confidentiality of the messaged, exchanged between the components of the DAA system.

It is recommended that security algorithms and protocols used 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.

2.1.2.3.2. Access control to authorize the components of the DAA system.

The initiation and all time of DAA establishment procedure shall be designed to avoid any unauthorized access during this phase.

2.1.2.3.3. Mutual peer entity authentication between the DAA systems.

The receiver shall use data only if the originator of the data has been positively identified. DAA system 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.

2.1.2.3.4. Protection from rebroadcasting of the earlier messages recorded by the intruder.

Position report messages should be supplemented with a time stamp corresponding to the coordinates' determination moment. This is proposed in order to increase of the aircraft movement restoration and the accident location accuracy, security strength and protection from the duplication of earlier transmitted commands and heaps of spam by the terrorists.

2.1.2.3.5. Protection from the possibility of design of a "dictionary" assigning the commands transmitted to the actions executed by the RPA.

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

2.1.2.4.1. All security actions have to be based on the main principle when security measures implemented should be commensurate with the threats according to ARP 4754A.

For Catastrophic, Hazardous/Severe Major, Major, Minor and No Safety Effects failure condition classes corresponding probabilities have to be designated in a manner uniform 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.

2.1.2.4.2. Using formally validated cryptographic modules.

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

2.1.2.4.3. The necessary cryptographic strength should be provided on the message length used within the DAA system.

2.1.2.4.4. The security system should detect cyber-attacks on the system providing for adequate virus and “malware” protection carrying out records, analyses and development of appropriate countermeasures. The cyber-attack may be aimed to the system soft of RPS

2.1.2.4.5. The RPAS system must support the pilot in having a indication if the DAA system is being influenced by an intruder. A cryptosystem shall provide a warning to the operator if any of the events – phantom induction or attempt of cryptoattack – is detected.

2.1.2.4.6. The RPAS system should render support to the identification function providing for the possibility to distinguish phantoms from real aircraft. The system should allow to locate the source of phantom signals in order to suppress it in appropriate manner.

2.1.2.5. [Standard] If surveillance data is not collected through a secure means, the data shall be validated through a second means.

— — — — — — — —

APPENDIX H

Collision Avoidance In The Lost C2 Link State

ADS-B protocols (for RPAS applications) should include a flag LC2LS – Lost C2 Link state active.

During the Lost C2Link state the LC2LS flag should be set active in the ADS-B messages, transmitted by both RPA and RPS.

On the flight in the Lost C2 Link State (by preprogrammed route) the RPA should transmit regular authenticated position report messages with LC2LS flag set active.

The messages shall be timestamped to prevent "playback" phantoms formed by rebroadcasting of earlier recorded messages.

Authentication is executed using the public key of RPA out of control.

If the DAA system of an aircraft receives the ADS-B message with LC2LS set active, it should inform the pilot about it and initiate the intent request to the originator of the message.

The RPA should respond to intent requests coming from any other aircraft, the intent messages should reflect the Lost C2Link State route.

As a rule the intent request/reply process should not be encrypted as confidential to make it possible for every aircraft in the radio access zone to see the out of control route (Lost C2 Link State route) of RPA.

If necessary, it can be encrypted as confidential using the public key of the intent request originator.

The SOAN should support the C2Link connection reestablishment procedure for RPAS in Lost C2Link state in case both RPA and RPS are accessible within the same network.

The SOAN should initiate the procedure of RPS (RPA) searching and C2Link connection reestablishing procedure on detecting the ADS-B message with active LC2LS flag from RPA (RPS).

— — — — — — — —

APPENDIX I

Reference

1. Manual on Remotely Piloted Aircraft Systems (RPAS), ICAO Doc 10019, 2015.
2. E. Falkov. Surveillance of remotely piloted aircraft under RLOS. RPASP-3-WP/10, 23/11/15.
3. ICAO Doc 9924 Aeronautical Surveillance Manual Second Edition, 2017.
4. RPASP WG2 (D. Colin, M. Neale). Preliminary review of proposed amendments to annex 10 related to remotely piloted aircraft systems (RPAS), RPASP-WP, 2017.
5. A. Costin, A. Francillon, Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices, EURECOM
6. M. Strohmeier. Security in Next Generation Air Traffic Communication Networks, Trinity, 2016
7. K. Wesson, T. Humphreys, B. Evans. Can Cryptography Secure Next Generation Air Traffic Surveillance? IEEE Security & Privacy, Vol. X, no.X, 2014
8. Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation, Volume V Aeronautical Radio Frequency Spectrum Utilization, Third Edition July 2013.
9. E. Falkov, S, Shavrin. RPAS service under BRLOS with use of self-organizing airborne networks, RPASP-4, 2016.
10. E. Falkov, S, Shavrin. Candidate SARPS for service under BRLOS using airborne networks, RPASP-4, 2016.
11. E. Falkov, S, Shavrin Candidate security related SARPS for airborne networks. RPASP/5-WP/005, WG2, 07/05/16.
12. RPAS and C2 link security protocols for airborne networks. Presented by WG2. RPASP/3- WP/006, 14/12/15.
13. ICAO Doc 9816 Manual on VHF Digital Link (VDL) Mode 4 PART II, Detailed technical specifications, 2004.
14. Candidate Annex 10 Vol 4 Part 2 SARPS, Presented by WG-3, RPASP/9-WP/6 5/10/17.

— END —