International Civil Aviation Organization

WORKING PAPER

RPASP/7-WP/3
9/12/16

REMOTELY PILOTED AIRCRAFT SYSTEMS PANEL (RPASP)

SEVENTH MEETING

Montréal, Canada 13 to 17 March 2017

Agenda Item 3: Development of proposals related to command and control (C2) *(Ref: Job card RPASP.002.04)*

CANDIDATE SARPS FOR THE SECURITY OF THE RPAS C2 LINK

(Presented by WG-2)

SUMMARY

This paper is proposing a process to define the final list of candidate security SARPs applicable to the RPAS C2 Link and additional candidate standard requirements or recommended practices which have been identified as relevant in regulatory or standardisation contexts outside of ICAO. It refers to WPE RPASP 02.004.1497

Priority: Urgent

1. INTRODUCTION

1.1 RPASP WG-2 has been tasked by the RPASP Secretariat to provide candidate SARPs related to the C2 Link of the RPAS (WPE RPASP 02.004.1497).

1.2 One of the major identified concern is the security of the C2 Link. An RPAS may fail to meet safety requirements if the security of the assets (human and commercial, tangible and intangible) involved in the production and operation of the RPAS become compromised resulting in the RPA experiencing technical failures or (hazardous) operations, not controlled or intended by the Remote Pilot.

1.3 Such compromises can arise through attacks upon the assets of the RPAS. An attack may occur at any stage of the RPAS life-cycle from initial design, through development and certification, then manufacture, operation, and maintenance to eventual decommissioning.

1.4 Successful defence of the RPAS against attacks is achieved by security measures that are implemented with an appropriate level of rigour and maturity to fulfil a range of security requirements that apply in various ways to the actors and assets involved in the RPAS.

1.5 The measures to secure the RPAS are derived by a security risk assessment that is outside the scope of this WP. Nonetheless, it is likely that much of the information will be confidential between the RPAS manufacturer and operator and the certification and administration authorities.

1.6 Certain applications may already provide sufficient RPAS security protection but for other applications additional security protection will be required. RPAS security effectiveness relies on a chain of secured organisations, processes, users, systems, techniques and protocols. They must all be addressed in parallel during the design, manufacture, operation, maintenance and decommissioning of the RPAS to achieve the RPAS level designed security objective.

1.7 The RPAS Panel is assessing the vulnerabilities of RPAS and WG-2's expertise allows some mitigation means to be proposed.

1.8 But since security must be commensurate to the threat and the security objectives, it is not realistic to envisage that security for RPAS will be resolved by RPASP/WG-2 solely at the SARPs level. The update of the SARPs in Annex 10, as well as any RPAS security related document, has to be put in the wider comprehensive context of security in aviation, committing all of the relevant regulatory and standardisation actors. A coordinated approach is required, between RPAS Panel WGs, other ICAO Panels, and between regional aviation authorities and technical standardisation organizations.

1.9 In addition, the development of effective SARPs for the entire regulatory and standardisation framework, requires implementation in a security context which commits all parties in the RPAS business, from the design to the operation.

2. **DISCUSSION**

2.1 Since 2015, within the RPAS Panel, WG-2 identified many of the detailed items that will need to be addressed to efficiently address security for the C2 Link. This work can only be seen as an input to a coordinated effort towards RPAS security, focusing on either high-level considerations about the security of the RPAS or more specifically on some technical solution for the C2 Link that has already discussed within WG-2.

2.2 The outcome of this work, contained in this WP, is hereby presented to the regulatory and the standardisation community to help them publish a set of documents which will eventually complement the WG-2 proposed security SARPs from Annex 10.

2.3 At this time WG-2's conclusion, is that it cannot alone propose detailed candidate SARPs to be included in the Procedures Part I or for the Systems Part II solutions in Annex 10 Volume VI without those SARPS being complemented by standards and procedures from other ICAO Panel and from the RPAS community, outside of ICAO.

2.4 The outcome of WG-2 work on security for the C2 Link is presented in Appendix A and Appendix B. Both Appendices have been structured by domains or activities for better readability:

- Appendix A pre-identifies security statements which are proposed to be included in ICAO documents.

- Appendix B pre-identifies security statements which are proposed to be included in documents other than ICAO as they are more technical or solution based.

2.5 WG-2 may later propose some additional SARPs related to the procedural aspects of the C2 Link operations to be included in the Annex 10 Volume VI.

2.6 It is obvious that some of the proposals are relevant for activities other than RPAS operations. They shall not be duplicated in other ICAO documents or annexes. Therefore, RPASP WG-2 proposes the RPASP Secretariat to organize further work on RPAS security with other relevant ICAO panels, groups and Task Forces interested in RPAS Security, with the aim to decide which requirements should be contained within either of the:

- Annex 10 SARPs;
- RPAS Manual (ICAO Doc 10019);
- AVSEC Panel documents; or
- technical standards developed outside of – but in coordination with – ICAO.

2.7 Moreover, adding a significant number SARPs related to security in Annex 10 is not deemed by WG-2 as the most efficient approach. WG-2 proposes to limit the Annex 10 update on security to some procedural aspects of security and to high level SARPS which either refer to:

- a dedicated ICAO Document (dedicated to RPAS Physical and Cybersecurity as well as an update of Doc 10019)
- industry standards.

WG-2 already identified placeholders for such SARPs in the updated Annex 10 structure (cf. RPASP/2-WP/2, WG-2 18/06/2015) approved by the RPAS Panel.

2.8 WG-2 believes that this approach:

- ensures maximum security for RPAS by having the right expertise/skills at the right level of regulation and standardisation, and by organizing a full consistency between relevant parties;

- provides the wider RPAS community with high level guidance and coordination from ICAO;

- provides more flexibility to quickly adapt to any technological evolution of either a threat or a protective solution;

- contributes to simplify Annex 10 content; and

- will facilitate future maintenance of Annex 10.

3. ACTION BY THE MEETING

3.1 The RPAS Panel is invited to:

a) endorse the approach on RPAS C2 Link Security discussed in this working paper;

b) propose the Secretariat to organize further work on RPAS security with other relevant ICAO panels, groups and Task Forces interested in RPAS Security. That work would:

- consider the candidate SARPs listed in Appendices A and B; and

- select from the candidate SARPs which ones can be proposed for inclusion in the Annexes or in other ICAO Documents.

— — — — — — — —

APPENDIX A

SECURITY ITEMS WHICH ARE PROPOSED TO BE INCLUDED IN AN ICAO DOCUMENT

1. <u>Organisational level:</u>

Note 1: The term “organisational” is applicable to - but is not limited to - manufacturers, operators, and service providers involved in RPAS businesses. It may also include businesses that interact indirectly with RPAS and/or have access to the systems and interfaces between RPAS component systems.

Note 2: Some of the proposed SARPs below are related to the RPAS security assurance as a whole and not only to the C2 Link. They are included here to provide a more comprehensive view of RPAS security.

Note 3: “Users” are any person having access to the RPAS information, including that carried on the C2 Link.

- **Standards**
  - General
    - RPAS security encompasses the following elements:
      - Physical Security (PHYSEC) of installations and premises not associated with communications
      - Information Security (INFOSEC)
      - Communications Security (COMSEC), and where specific to communications equipment and systems:
        - Physical Security (PHYSEC) Transmissions Security (TRANSEC)
      - Electro-Magnetic Security (EMSEC)
    - Procedural, personnel, physical and technical security measures together contribute to achieve the target level of security.
  - Security objectives
    - RPAS shall be secured against identified threats, commensurate with the risk to operational and organizational objectives
    - RPAS C2 Link security aims to protect and alert against:
      - Unauthorized access to the RPA Command and Control system.
      - Negative mutual peer entity identification and authentication between the RPS and the RPA.
      - Failure of accountability in transactions requested of and executed by the RPA Command and Control system.
      - Loss of integrity of data traffic between the RPS and the RPA.
      - Loss of confidentiality of the messages, exchanged between the RPS and RPA.
      - Loss of availability (denial of service) of the C2 Link.

    Note: When information carried by the C2 Link is communicated through the RPA or the RPS to and from sources external to the RPAS then a global security assessment may be required.
  - User and other device access:

    - Access by people and by electronic objects (on portable media or through a network) shall be controlled and recorded.
    - A means of preventing logical intrusion and means of detecting that logical intrusion has happened shall be implemented.
    - Multifactor methods shall be used to identify and authenticate users locally and remotely.
    - Electronic objects shall be identified and authenticated.
  - Protection of information
    - RPAS shall be protected against corruption and snooping of stored and snooping of transmitted information
  - C2 Link Communications Service Provision robustness and cybersecurity
    - An owned communication service provision shall be sufficiently resilient to survive security hazards
    - A full inventory of approved connections shall be maintained.
  - Third Party Communication Service provision
    - A full inventory shall be compiled of the Third Party Communication Service Provider organisation, including its network architecture, the number and type of connections used, and protocols and applications that are deployed.
    - Any sub-contracting to external providers or equipment suppliers shall be documented.
    - A Service Level Agreement shall be contracted with Third Party Communication Service Providers under defined Service Level Objectives, which includes security requirements for confidentiality, availability, integrity, authenticity and accountability.
    - The Service Level shall be commensurate with the risk presented by loss of the platform or the data passed across the C2 Link.
  - Organisation robustness to cyber attacks
    - The organisation shall establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.
    - The organisation shall establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.
  - Procedures for organisations
    - Procedures shall be defined for continuing certification, accreditation of security measures and their effectiveness.
    - There shall be a defined process to establish, operate, and maintain an enterprise cybersecurity risk management program with the objectives to identify, analyse, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
    - Plans, procedures, and technologies commensurate with the risk to the organization’s infrastructure shall be established and maintained to detect, identify, analyse, manage, and respond to cybersecurity threats and vulnerabilities and organizational objectives.
    - The overall threat environment shall be reviewed and updated regularly.

  - Vulnerabilities shall be continuously updated, and equipment scanned with assurance of complete coverage of vulnerabilities and inventory, e.g. after maintenance.
  - There shall be a regular review of inventory.
  - There shall be defined procedures for collection and storage of evidence following a security breach.

    Note: Evidence includes information of any kind that is stored or was communicated for a defined period prior to, during and after the event.
  - There shall be defined procedures commensurate with the risk to critical infrastructure and organizational objectives:
    - to establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).
    - to manage the organization’s Information and Communications Technology (ICT) and Operational Technology (OT) assets

      Note: The procedure shall include the method for assembling an inventory of assets to support organisational oversight of those assets throughout their lifetime.
    - to establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities,
    - to reduce risks and to increase operational resilience,
    - to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event,
    - to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities.
  - There shall be defined procedures for establishing:
    - A time reference;
    - time stamping of information, hardware and software; and
    - verification of date and time
- Procedures for contingency
  - A contingency plan shall be implemented to mitigate the effect of security breaches.
- Procedures for encryption systems
  - A policy for management of cryptographic controls (keys) shall
    - be stated
    - be implemented.
    - state the purpose of the keys, who is using them, and how they will be used by defining the association between people, objects and role.
  - There shall be defined procedures for:
    - a key generation that assures the authenticity (provenance) of software, hardware (including cryptographic devices) and storage/containers for information, including keys themselves.
    - the distribution, deletion, invalidation and recovery of keys.

- **Recommended practices**
    - User and other device access
        - Any relevant requirements of NIST 800-63 should be implemented at organisational level. Authorisations given to people and objects to gain access should be automatically managed and audited.
        - Identity of people and electronic objects should be verified before, continuously monitored during and at the completion of access.
    - Protection of information
        - Any relevant requirements of ISO 27000 standards should be implemented at organisational level.
        - Multiple security domains should be deployed as physical or logical barriers to enforce information flow policies.
    - Exceptional procedures affecting robustness to cyber attacks
        - If desired, rules to allow occasional exceptions to identity and access enforcement policies may be implemented.
        - If desired, remote access from outside by external parties and to the outside from within the RPAS under strict conditions and strongly protected may be permitted.

2. <u>**Operations level:**</u>

- **Standards**
    - User and other device access
        - A security policy for employing people shall be defined and applied at the start, during and at the end of their employment.
        - Security training and awareness shall be delivered to ensure that staff are able to use tools and equipment, and are able to manage incidents.
        - The security status of each workstation and the people assigned to it shall be identified, and be periodically reviewed.
    - Operations
        - Generation of digital certificates and cryptographic keys shall be done according to the process and practices defined in ED-204.
        - The receiver shall use data only if the originator of the data has been positively identified and authenticated.

- **Recommended practices**
    - Users and electronic devices
        - Users including remote pilots should be subjected, at a minimum, to the same background check standards as persons granted unescorted access to security restricted areas of airports.
        - People should be assigned to tasks appropriate to their security status.
    - Robustness to cyber attacks
        - The RPAS should be assigned an ICAO 24-bit identifier as appropriate according to the regulations stated by ICAO and implemented by the state in which the RPAS is registered. If ICAO 24-bit identifiers are not used then alternative standards, processes and practices should be stated by the manufacturer and/or operator and/or communications service provider concerning their allocation, assignment and authentication
        - The RPAS flight manual should document security procedures applicable to the RPAS, in particular the RPA, the RPS and the C2 Link)

- An RPAS operator should establish a system of record-keeping that allows adequate storage and reliable traceability of security management records.
- The inventory should include:
  - Communication services;
  - Service registry;
  - Location of equipment – own and at other locations;
  - Identification of the responsible persons and of the person in charge
  - Registry of facilities of other organizations

3. <u>Technical solutions level:</u>

Note: Quantitative design security objectives in addition to the design safety objectives, at the RPAS level, will be required.

- **Standards**
  - Information carried on the C2 Link shall be protected by
    - A means to prevent and detect corruption and snooping by cryptanalysis of stored information shall be implemented.
    - A means to detect corruption and to detect and prevent snooping by cryptanalysis of transmitted information shall be implemented.
  - The security control means shall additionally be implemented with the following characteristics:
    - All security actions shall be based on the main principle that security measures implemented
    - The C2 communication system shall provide safeguards that deny unauthorized or unauthenticated users the ability to command and control the RPAS.
    - C2 Link security algorithms and protocols shall provide adequate levels of security goals such as confidentiality, access control, integrity, authentication and accountability (including non repudiation) of transmitted data, for the kinds of operation for which certification is requested.
    - The security system shall provide a means to detect cyber-attacks, such as intrusion, infection by viruses or malware, or denial of service, on the system.
    - To ensure commands are executed based on the intention of the operator the C2 messages shall include a means to identify the sequence of their generation (e.g. timestamping of their generation, sequence numbering…).
    - The security measures shall provide for adequate virus and “malware” protection (security event logging, analyses and development of appropriate countermeasures).
  - The RPAS shall alert the pilot and air-traffic controller if the C2 link is being influenced by an unauthorized user.

- **Recommended practices**
  - The full design, implementation and verification of the effectiveness of security measures should be commensurate with ARP 4754A, ARP4761, ED-202A and ED-203A.
  - The C2 Link security measures and procedures should support means to avoid the erroneous command execution order, to identify loss of commands, and to protect from the duplication or retransmission of earlier transmitted commands or data by the authorized/unauthorized users, e.g. an intruder, as well as from unauthorized messages

delivered to pilot’s and air controllers’ displays. The C2 Link security means and procedures should thus provide:

- Confidentiality of the messages, exchanged between the RPS and RPA, and between the RPA and RPS.
- Access control, to grant the RPS access to the RPA, and the RPA access to the RPS.
- A C2 Link RPS-RPA establishment procedure, designed to avoid any unauthorized control of the RPA during this phase.
- Mutual peer entity authentication, between the RPS and the RPA as appropriate to the design of the RPAS.
- Use of data only if the originator of the data has been positively identified, authenticated and authorized, and if required access has been granted.
- Robustness against the possibility of using cryptanalysis techniques to associate the commands transmitted by the RPS to the actions executed by the RPA, e.g. by constructing a dictionary.

— — — — — — — —

APPENDIX B

Security items which are proposed to be included in a document other than ICAO

Note: Some of the proposed items below are related to the RPAS security assurance as a whole and not only to the C2 Link. They are included here to provide a more comprehensive view of RPAS security.

1. System requirements

- **Standards**
  - The security control means shall additionally be implemented with the following characteristics:
    - Security measures shall be implemented in consideration of design safety assurance at system and equipment level (e.g. complex software/hardware), following the processes and practices defined in ARP 4754A/ARP4761, and related standards.
    - The required security measures and their effectiveness shall be identified following the processes and practices defined in RTCA DO-326A/ EUROCAE ED-202A and RTCA DO-356 / EUROCAE ED-203.
    - The operation of security measures, maintenance of their effectives through life of the RPAS, and associated processes, e.g. use of PKI services for generation of digital certificates and cryptographic keys, shall follow the practices defined in RTCA DO-355 / EUROCAE ED-204.
    - The C2 communication system shall provide safeguards that deny unauthorized users the ability to command and control the RPAS.
    - C2 Link security measures shall provide confidentiality, access control, integrity, authentication and accountability (including nonrepudiation) of transmitted data.
    - The security system shall provide a means to detect cyber-attacks, such as intrusion, infection by viruses or malware, or denial of service, on the system.
    - The security measures shall provide for adequate virus and "malware" protection (security event logging, analyses and development of appropriate countermeasures).
    - The RPAS shall alert the pilot if the C2 link is being influenced by an unauthorized user.
  - The C2 Link RPS-RPA establishment procedure shall be designed to avoid any unauthorized control of the RPA during this phase.
  - The receiver shall use data only if the originator of the data has been positively identified, authenticated and authorized, and if required access has been granted.
  - The C2 Link RPS-RPA authentication procedure shall exclude the transmission of the unsecured key (password) through intermediate link or devices.

- **Recommended practices**
  - If the C2 Link is carrying ATM surveillance data, such as aircraft identification and temporal and spatial coordinates, then this information should be protected. *Note: this protection may already be provided by the security mechanisms used on the C2 Link.*
  - The C2 Link security means and procedures should provide:

- Confidentiality of the messages, exchanged between the RPS and RPA and between the RPA and RPS.
- Access control to grant the RPS access to the RPA, and the RPA access to the RPS.
- Mutual peer entity authentication, between the RPS and the RPA as appropriate to the design of the RPAS.
- Identification, e.g. hash message authentication code (HMAC), to provide the integrity of data traffic between the RPS and the RPA.
- a means to identify the sequence of the C2 messages generation (e.g. time-stamping of their generation, sequence numbering…). Received C2 commands in this case should be executed according to their sequence identification means.
- Robustness against the possibility of using cryptanalysis techniques to associate the commands transmitted by the RPS to the actions executed by the RPA, e.g. by constructing a dictionary.
- Detection of cyber-attacks on the system.
- Adequate virus and "malware" protection by recording, analysis and development of appropriate countermeasures.

2. <u>Physical security</u>

- **Standards**
    - Access and control
        - There shall be a procedure for issue, control, registry, deactivation and cancellation of passes.
        - There shall be different types of passes according to category of personnel (internal, visitors, etc.).
        - The pass shall be in a design which is difficult to forge. It shall bear a photograph of the person to whom it is issued.
        - The use of a pass (e.g. card) within site shall be mandatory.
        - Verification of personnel access authorisation shall be done before access begins.
        - Any suspected or attempted unauthorised physical access shall investigated
        - Emergency exits shall guarantee that only authorised personnel can gain access to installations
        - Emergency procedures shall guarantee that only authorised personnel can gain access to installations.
        - There shall be a means to check password robustness automatically.
        - Passwords shall be changed if they are revealed to third parties or are suspected of having been revealed to third parties
        - Passwords shall not be stored or written down unless encrypted.
        - The passwords stored in the system shall be encoded.
        - Administration passwords shall be kept in sealed envelopes suitably stored in safes.
        - Users shall guarantee password confidentiality and shall report any potential disclosure.
        - Tokens shall be implemented in hardware or software
        - Items that can be located in open areas shall be visibly distinguished from those that must be secured.
    - Operational

    - Products, including at initial delivery and at upgrades, shall be certified and signed by the supplier. The integrity of documentation including that associated with products from third party suppliers should be certified.
    - There shall be a technical means to restrict the use of system utilities to designated users and workstations, and use should be available only at defined times for a defined interval.
    - There shall be access restrictions to prevent non-privileged users from modifying critical information, including workstation clocks or device identification.
    - The requirements for protection against malicious interference of the data link shall be harmonized, based on an assessment by the competent authority
    - Devices shall be identified and authenticated before connecting to the RPAS or with each other, with additional, or stronger, authentication before accessing cryptographic services.
    - Associations between devices shall be authenticated against the RPAS operational plan to minimise the possibility that an RPS is wrongly associated with a RPA.
  - Integrity of the system and its information
    - The detection tool shall support sensors that address both intrusion at devices and attempted access via networks. It should generate alarms in real-time.
  - Access authorisation, control and enforcement
    - If used, a Public Key Service (PKI) shall be accessed with end-to-end authentication at relevant layers, (in particular sessions). The PKI shall be trustworthy.
  - Protection of information
    - There shall be an accredited source of UTC time, synchronised throughout the RPAS enterprise with a centralised proprietary clock or with an official time source.
    - The confidentiality of information shall be protected using an encryption method for the desired cryptographic strength appropriate for the type, sensitivity and size of content.
    - The authenticity of information shall be verified by providing an unforgeable identity token, e.g. a message authentication code
    - The integrity of information shall be protected by suitable error-detection and correction methods, e.g. Cyclic Redundancy Checks (CRC), Hash functions or other codes.

- **Recommended practices**
  - Access and control
    - There should be periodic security searches at the entrance to and at the exit from the RPAS premises.
    - Access registries and records should be reviewed periodically.
    - Evidence of authorisation, e.g. a pass, should identify the bearer according to role category and the areas that can be accessed.
    - The pass should allow for visual recognition of areas which may be accessed by the holder.
    - The pass should not include any data which would allow anyone, in case of loss, to obtain information regarding its use (they contain return address only)
    - The site should be labelled to allow quick verification that an individual is allowed to be present in specific areas.

    - Passwords and other access control information should be stored in an encrypted form. There should be a robustness check on the creation of a password.
    - Passwords which are easy to remember but difficult to guess should be chosen.
    - Passwords should be a mixture of printable alphanumeric characters from the UTF-1 alphabet.

      Note: The minimum length for a non-privileged user password is 8 characters; 10 characters for a privileged user; and 12 characters for a system user.
    - Considerations should be given to both the passwords complexity and the number of systems that it is used to access.
    - Different passwords should be used for private and working accounts.
    - The first password should be temporary with a limited duration (minimum and maximum).
    - Passwords should have a maximum usage period of less than 1 year.
    - If the token is implemented in hardware, then it should comply with FIPS 140-2 level 4 or equivalent.
    - Equipment, services and facilities should be maintained physically separate from each other to facilitate the enforcement of information flow policies.
- Vulnerability scanning
    - Consideratiosn should be given to using more than one tool to detect vulnerabilities.
    - Vulnerability scanning tools should include the capability to regularly and quickly update the list of vulnerabilities scanned.
    - The tools should support configuring authentication and access rules which allow only authorised users to use it.
    - The tools should be certified products approved by the appropriate authority.
    - The vulnerability scanning tools should be regularly updated.
- Operational
    - Functionality and options should be reduced to be minimum needed to fulfil the required tasks on the least number of devices, while maintaining safety margins.
    - Unused applications and modules should be removed.
    - The duration of sessions should be limited and idle sessions should be terminated.
- Integrity of the system and its information
    - Software, data, and critical systems should be regularly scanned.
    - The detection tool should generate alarms in real-time.
    - The detection tool should support filtering for capture and display.
- Protection of information
    - Access to time-stamping services should be according to ISO 18014.
    - There should be a periodic synchronisation check, and a check should be made after clocks change (daylight saving or change of time zone), and after software updates or changes in configuration.
    - All information exchanged between components of the RPAS should be associated with a time-stamp or the time of the origination of the information.
    - Sufficient redundancy should be provided to allow transfer of operations to alternative facilities, e.g. duplicate transceivers operating on distinct frequencies.
- Auditing
    - The information system should produce audit information on hardware-enforced, write-once media.

- The audit information should be collected at a frequency and retained for a period of time that is consistent with the forensic investigation requirements.
- Registries, repositories of information and system audit tools should be protected against unauthorised deletion and modification. They should be held separately from development and operation systems
- To minimise the possibility of repudiation, sent confirmation and delivery confirmation should be recorded in a registry of transactions and transmissions.

3. Security of Self Organized Airborne Networks (SOAN)

- **Standards**
  - Cryptographic items
    - Public key - private key management
      - Each network node shall be assigned a pair of keys – one public key and one private key.
      - All public keys shall be stored in a common database accessible only to authorized personnel including pilots on duty.
      - Private keys shall be physically protected by being inaccessibly embedded within the C2 Link equipment, without logical access out of the encryption / decryption function.
      - Any pair of networked objects such as RPA and RPS shall use public-key algorithms to secure and authenticate the mutual traffic.

        Note 1: This mechanism is good enough for point – to – point communications, but it excludes broadcast mode and leads to significant traffic increase for multiparty information interchange.

        Note 2: Elliptic curve cryptographic algorithms will be preferably used for short messages encryption and session key generation.
      - Key exchange mechanism shall support the following types of protocols:
        - Group generation protocol;
        - Group entry protocol;
        - Group unite protocol.
      - Group generation protocol shall be used to support the common (symmetric) key exchange between two separate (outside the groups) network nodes on their appearance in the mutual RLOS.
      - Group entry protocol shall be used to provide a new separate network node with a common group key.
      - Group unite protocol shall be used to set the common key for two groups of network nodes.
      - The cryptographic system shall:
        - Use cryptographic algorithms with algorithm strength and key length sufficient to protect data in transit against the identified safety effect.
        - Use formally validated cryptographic modules.

        Note: The public key algorithms used must be robust against attempts by the cryptanalyst to create and use “dictionary attacks”.
  - Operational procedures
    - When out of radio access zone from other RPASs, each RPA shall periodically broadcast its identifier.
    - The RPA shall not broadcast its identifier together with unencrypted position reporting to avoid interception of its location coordinates.

    - Time-stamp shall be included in the content of encoded messages to make the process of a “vocabulary” creation ineffective, thus increasing the performance of the C2 Link security.
    - Time-stamping mechanism shall be used to provide SOAN automatic conflictless spectrum resource access.
- SOAN specifications
    - A SOAN C2 Link crypto-system shall provide required security strength for short messages.

  Note: Position report message size is typically 256 bits.
    - A SOAN cryptosystem shall support both symmetric and public-key encryption / decryption functions.
    - A SOAN C2 Link cryptosystem shall support key exchange mechanisms.
    - Transmission of messages via C2 link shall be synchronized with a UTC Second stamp.
  - A SOAN node shall support the following protocols:
    - Group generation
    - Group entry.
    - Group unite.

    Note1: Group generation protocol is to support the common (symmetric) key exchange between two separate (out of groups) network objects on their appearance in the mutual RLOS.

    Note 2: Group entry protocol is to provide separate network object with a common group key.

    Note 3: Group unite protocol is to set the common key for two groups of network objects.
  - In addition to encrypted data and aircraft identifier, the C2 messages shall include encryption-type flag, group identifier and change-key flag.

    Note 1: Encryption-type flag indicates the type of cryptographic algorithms used: symmetric or public-key;

    Note 2: Group identifier should be common for RPAs sharing the same (common for a group) symmetric key;

    Note 3: Change-key flag indicates the common symmetric key transmission within a message.

- **Recommended practices**
    - Position report C2 messages should be supplemented with a time-stamp corresponding to the determined location coordinates.

— END —