First...

• **Context**
  • What the RPAS Guidance Manual says about security
    – Background reading
    – Relevant sections
    – Summary of principles
  
• **What the RPAS Panel WG2 plans to do**
  – Standards and Recommended Practices
  – What the Manual doesn’t say – update it?
  – What else to think about
Context - Scope

- Legacy systems, services commerce
- Installations
- Operators, Pilots
- ATM, other air users
- C2 System
- Services
- C2 link
- C2 technology, C2 link security
- Physical security on the ground

RPS
RPA
Then...

• Context

• **What the RPAS Guidance Manual says about security**
  – Background reading
  – Relevant sections
  – Summary of principles

• **What the RPAS Panel WG2 plans to do**
  – Standards and Recommended Practices
  – What the Manual doesn’t say – update it?
  – What else to think about
Background Reading

• **RPAS Guidance Manual**
  – Unmanned Aircraft Systems (UAS) (Cir 328)

• **Manned aviation SARPs and ICAO documents**
  – Air Traffic Management Security Manual (Doc 9985 - Restricted)
  – Annex 6, Part I, Chapter 13 — International Commercial Air Transport — Aeroplanes contains SARPs to secure the flight crew compartment.
  – Annex 17 — Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference, paragraph 4.2.4
  – And others – OLDI, ATM messaging protocols, ...

• **There are many other standards and specifications especially for security in information and communications technologies**
  – RTCA SC-216 and Eurocae WG72
    • ED-202, ED-202A, ED-203, ...
  – ISO Common Criteria (ISO/IEC 15408)
  – IETF RFCs – if your solution uses Internet protocols
The Guidance – Type Certification and Airworthiness Approval (4.5, 4.6), Operator Approval (6.4)

- *Manual does not refer to security airworthiness in detail*
- C2 link airworthiness – it is not a product requiring independent certification
  - More guidance is needed on how to apportion the integrity requirement for the C2 system to the C2 link element
  - Some operational aspects are addressed in section 11.4 and 11.5
- The RPA Flight Manual and Request for Operational Approval (Appendix A) should define security procedures unique to RPAS (e.g. RPS security, C2 link, etc.) as well as those that would be needed for manned aviation.
- An RPAS operator should establish a system of record-keeping that allows adequate storage and reliable traceability of all activities, covering at a minimum... security management records.
  - Refer to section 9.10 – Accidents and Serious Incidents
The Guidance – RPAS Operations, Security Requirements (9.11), the RPS (13.4)

- Some aspects similar to manned, some aspects unique
- Physical security on the ground and in the air (9.11)
- The CNPC link provides functions as vital as traditional wiring, control cables and other essential systems
  - These links may utilize diverse hardware and software that may be provided and managed by third parties.
  - Safety and security of these links and services that support them are equally important as those for the RPA and RPS.
- Handovers between non-collocated RPS must be secure.
Next...

• Context
• What the RPAS Guidance Manual says about security
  – Background reading
  – Relevant sections
  – Summary of principles

• What the RPAS Panel (and WG2) plans to do
  – Standards and Recommended Practices
  – What the Manual doesn’t say – update it?
  – What else to think about
Action by the RPAS Panel

• Recognise the five elements of information assurance - Confidentiality, Integrity, Availability, Authentication and Non-Repudiation

• Reach consensus on a holistic, harmonised, approach to security and information assurance across WGs and with relevant Panels – CP, AVSEC
  – Security airworthiness of the RPAS product (WG1)
  – Secure operation of the RPAS (WG4)
  – Secure integration with ATM (WG6)
  – Additional requirements
    • D&A events require stronger authentication?
    • Are there unavoidable interoperability requirements?

• Performance based, proportional to RPAS risk
  – “Per flying hour” – is this the right metric for security integrity?
  – But what is the equivalent of RCP?

• Updates to the Guidance Manual
  – TRANSEC is addressed in conventional terms
    • Specific mechanisms may be needed in SARPs
  – PHYSEC, EMSEC, COMSEC, INFOSEC need further work
    • Or do they? May be same as manned aviation?
Action by RPASP WG2 - Command and Control

• Some aspects of spectrum management affecting CNPC security are to be addressed in SARPs
  – Possible updates to Annex 10 for TRANSEC
    • Specific anti-jamming mechanisms, e.g. frequency hopping, impact coexistence
    • Acceptable conditions for use of FSS (e.g. update to AMS(R)S)

• End-to-end secure C2 application
  – Mutual peer entity authentication (RPA-access network-RPS)
  – Authentication of originator and destination of messages between RPA/RPS and control-plane signalling between RPS/RPA and the CNPC provider services
  – Integrity, confidentiality
  – Access control

• CNPC service providers – security requirements

• C2 application functions and protocols for security
  – No requirement for interoperability
  – Strong requirement for performance

RTCA SC-228 MOPS
RPAS in the National Airspace

- **Airspace is part of critical national infrastructure**
  - Electronic systems, avionic and ICT must be implemented/operated securely

- **What does your government require?**
  - Agencies who are responsible, including CAAs
  - Standards they require you to use (may be in SARPs?)
    - Product manufacture and maintenance
    - Required assurance levels for various operations
    - Cryptographic algorithms, their strength and configuration
    - Key management – generation, exchange, lifetime
    - Approved third-party products and services
    - Evidence gathering
  - Authorities
    - Where to get keys
    - Certification and accreditation
  - Reporting – CERTs, ISACs

- **What do other governments require?** Need harmonisation!

- **What is forbidden or deprecated?**
Security of RPAS Operation

0. Assume no security

1. Accreditation, non-repudiation, reporting, QoS monitoring

Proving operational airworthiness
1. Define the perimeter and make an asset inventory
2. Threat/vulnerability identification
3. Risk assessment – hazards (attacks) and consequences
4. Security objectives – required integrity
5. Countermeasures – defense in depth

UK ASTRAEA programme

Legacy systems, services, commerce

ATM, other air users
Summary

• Overview of the RPAS Guidance Manual
  – Many sections concerned with C2 link and TRANSEC
  – Other topics require further attention

• Highlight expectations of RPAS Panel and RPASP WG2 outcomes

• Other things to consider
Thank you!
Questions?
Backup
C2 Link Security

• **Security requirements need to be internationally harmonized**

• **Security is a multilevel consideration**
  – Many aspects similar to manned aviation e.g. Physical security
  – RPA are different e.g. C2 Link message security, C2 Link RF Signal security

• **C2 Link message security**
  – Authentication, Integrity, Confidentiality
  – Encryption
    • Key management logistics need to be considered

• **C2 Link RF Security**
  – Impractical to completely protect C2 Link RF signal
  – RPA have natural defence to Malicious Interference
    • Lost C2 Link procedure
    • ATC procedures will be required to handle Lost C2 Link
Technology threats

1. Incorrect configuration, failure of authentication, access control
2. Congestion, loss, delay, errors, stale connectivity, mobility
3. Noise, interference, jamming, flooding
All those SECs

- **Cryptosecurity**: The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This includes ensuring message confidentiality and authenticity.

- **Emission Security** (**EMSEC**): The protection resulting from all measures taken to deny unauthorized personnel information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic-equipment, information systems, and telecommunications systems.

- **Transmission Security** (**TRANSEC**): The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g. frequency hopping and spread spectrum).

- **Physical security** (**PHYSEC**): The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

- **Communications security** (**COMSEC**): is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. The field includes cryptosecurity, TRANSEC, and PHYSEC of COMSEC equipment.

- **Information security** (**INFOSEC**): is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).