Physical Security of Remote Pilot Stations and Aircrafts (when On Ground)

Airbus Defence and Space / Military Aircraft / INFOSEC

Juan Domingo
Airbus Defence and Space INFOSEC Expert
24 March 2015

IF-G-MES84-15002

AIRBUS
DEFENCE & SPACE

Table of Contents

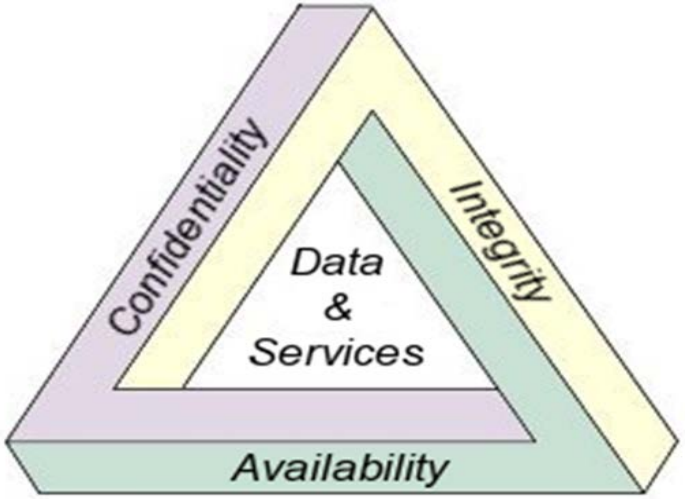
Objective

- The objective of this presentation is to provide a brief introduction and guidance on the physical means to protect the security of information & data, systems and platforms in the Remote Pilot Stations and Aircraft (when On The Ground).
- *It is highlighted the lessons learned from military best practices*.

Security Objectives

In order to achieve adequate security protection of RPA and RPS, a balanced set of security measures (physical, personnel, procedural and INFOSEC) to meet the following security objectives to ensure:

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY



“Safety” Objectives

- Security reinforces Safety
- Safety drops Security

AIRBUS DEFENCE & SPACE

Common Threats on RPS & RPA

The term threat “agents” can be split into three general types, as follows :

Adversarial threats – individuals, groups, organisations and nation states with the intent, motivation, capabilities, and resources to exploit the vulnerabilities. E.g. malicious hackers.

Non-adversarial threats – individuals, groups, organisations and, in some circumstances, nation states that have no objectives, motivations, or intentions to cause harm to a system. E.g. authorised users’ errors and recreational hackers.

Natural and technological disasters – this includes weather and geological phenomenon such as tornadoes, floods and earthquakes, as well as technological disasters such as toxic spills and power failures.

Physical Security Concept

In general terms, physical security is the application of physical protective measures to sites, buildings or facilities that contain information or assets requiring protection against loss or compromise.

Physical security policies, consisting of *active and passive* security measures, shall be established to provide levels of physical security consistent with the threat, security classification and quantity of the information and assets to be protected.

AIRBUS DEFENCE & SPACE

Physical Security of Facilities hosting RPA & RPS

Physical Security Measures shall be implemented in the Global Security Environment (GSE) and Local Security Environment (LSE) in order to provide adequate access control to Remote Pilot Stations;

- The facilities, e.g. hangar, buildings, shelters, … shall be protected by means of: tinted windows, perimeter fences, intrusion detection systems (active or passive), CCTV, …
- Moderate changes to the environment (temperature, humidity, air composition) must not result in abnormal behavior of electronic equipment and media.
- The arrangement of the site must prevent observation of confidential information from the outside.
- The access to the facilities should be controlled via badges, identity cards or passes.

AIRBUS DEFENCE & SPACE

Physical Security of Remote Pilot Stations

- Access to the RPS shall be restricted to authorised persons.
- The LSE will vary - RPS may be self-contained in its own enclosure, co-located with other equipment and facilities, or portable (hand-held) – measures will be proportionate to configuration and type of operation.
- Define the roles of the Security Administration and Operations and its tasks.
- Rooms with IT equipment must be locked when they are left empty.
- Passwords or other credentials for authentication (cryptographic keys, tokens) shall be handled as the maximum classification of the information managed by the system (i.e. military systems up to SECRET).
- TEMPEST Protection.

Physical Security of Remote Pilot Aircraft

- All portable/removable devices that store sensitive information for the mission shall be adequately protected when in transit between the RPS and the RPA.

- The RPA Access Panel or, any interfaces (to upload/download the mission and maintenance information) should be protected by a locking device system.

- Tamper seals shall be fitted to RPA equipment dependent on the design (taps, external ports, ..). In particular, it is very critical for equipment handling crypto-material (military purposes).

Conclusions

- **Physical Security Measures** shall be implemented in order to provide adequate protections to Remote Pilot Stations & Aircraft
- The Physical Security Environment is split in the **Global** Security Environment (GSE) and **Local** Security Environment (LSE)
- **Defence in Depth**: multiple measures are deployed on top of each other so if one layer is penetrated, another one is there to further safeguard .
- “Security reinforces Safety”

References

- ROADMAP to NATO Security Policy, Supporting Directives, Documents and Guidance for the Communication and Information Systems (CIS) Version 2.7 dated 2 October 2013
- NATO Approved Criteria and Standards for airfields Reference BI-MNCD 85-5
- MANUAL ON REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS) First Edition — 2015
- Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System

Thank you!

Any Questions?

Backup

Common Threats on RPS & RPA

The following list provides with some common examples for **physical & Environmenta**l threats that could impact of the RPS & RPA:

- Fire
- Water damage
- Pollution
- Major accident - Crash
- Destruction of equipment or media
- Climatic/Meteorological phenomenon
- Flood
- Failure of air-conditioning
- Loss of power supply
- Failure of equipment
- Electromagnetic radiation
- Thermal radiation
- Electromagnetic pulse

Common Threats on RPS & RPA

The following list provides with some common examples for **Information Technologies** threats that could impact of the RPS & RPA:

- Interception of compromising interference signals
- Theft of media/equipments or documents
- Retrieval of recycled or discarded media (Remanance)
- Disclosure of Information
- Data from untrustworthy sources
- Tampering with hardware
- Tampering with software (e.g. Trojan horse)
- Saturation of the information system (denial of service)
- Breach of information system maintainability
- Unauthorized use of equipment
- Corruption of data
- Abuse & Forging of rights
- Capture & Inappropriate location of the System

AIRBUS DEFENCE & SPACE