IN FLIGHT SECURITY INCIDENT MANAGEMENT

1. Introduction

The tragic events on 9/11 drastically changed the way in-flight security incidents are managed. That day, the world witnessed an unprecedented dimension of terrorism; civil aircraft being used as weapons of mass destruction. In Europe, the new threat was termed RENEGADE\(^1\). Since then, national security authorities are more reactive to any indication that could lead to a security concern, i.e. loss of communications (COMLOSS) with the aircraft, or transponder switch off or wrong setting. As an example, in most European countries the number of interceptions due to COMLOSS at least doubled after 9/11.

2. European Response

In light of the new threat Renegade, national response procedures to deal with in-flight security incidents have been reviewed. In many cases bi-lateral agreements have been set up to better coordinate cross-border incidents. However, this should not be enough; the international dimension of in-flight security incidents requires harmonization at European level. As an example, Figure 1 represents the 9/11 aircraft tracks mapped onto a central European scenario. As we can see, three or four States are affected by an incident that takes place in a short timeframe.

![Figure 1. 9/11 aircraft tracks mapping on central European scenario](image)

To address the international dimension of the Renegade issue, EUROCONTROL and NATO decided to work together and created the NATO EUROCONTROL Air Traffic Management

\(^1\) A situation where a civil aircraft is used as weapon to perpetrate a terrorist attack is usually referred to as a Renegade.
(ATM) Security Coordinating Group (NEASCOG), with the mission to ensure the necessary close co-ordination and development of all related security activities with the aim that the member nations of each organisation reach converging views.

In this regard the NEASCOG promotes, develops and supports effective pan-European Security measures, i.e.:

- Create a European Regional Focal Point for ATM information, involving civil and military interests;
- Give priority to the validation of a high capacity air-ground communications, capability for the transmission of encrypted cockpit voice, flight data and on-board video information.

3. **Explaining the problem**

In-flight security incidents are time critical events which require strong coordination among different actors and the gathering and validation of nearly real time information for decision making support.

The main aspects to manage a security incident are:

- Optimising awareness: identification of suspicious aircraft, incident notification, information dissemination, maintaining awareness;
- Information requirements: relevant information needed to manage and resolve an incident;
- Time factor: required information must reach the appropriate recipient on time to be able to provide adequate response;
- Technology support: automation and encryption facilitate information exchange, reduce delays and guarantee confidentiality.

Information requirements for in-flight security incidents have been gathered from national authorities. Relevant information items are:

- **What is wrong?** Several criteria for suspicious behaviour have been identified, but the list is not exhaustive. Training, security awareness and best judgment of pilots and controllers are therefore a key factor;
- **What is going on?** Information about situation on board is essential. The pilot in command is the key actor, and measure to support him/her must be implemented according to pre-defined scenarios when possible. However, the main problem in this regard is to make sure that the pilot in command is the legitimate one. Information about the flight is also important; type of aircraft, nationality, operator, passengers on board, nationality, VIPs (very important persons), children;
- **What is the threat?** Risk assessment should evaluate what is the real threat posed by the aircraft; endurance, objectives at range, aircraft behaviour (i.e. deep descent), confirmation of legitimate pilot in command, pilots’ intention.
4. **Providing solutions: the framework**

The NEASCOG Airspace Security Incident Management (ASSIM) High level Concept provides a framework to deal with in-flight security incidents. The objective of the concept is to support the decision making process by providing the National Authorities responsible for airspace security\(^2\) with real time reliable information about airspace security incidents.

Other actors considered in the ASSIM high level concept are: national Air Defence centres, adjacent Air Defence centres, civil Air Traffic Control (ATC), airlines operations centres and the aircraft.

One of the main domains that have to be considered within ASSIM Concept is the technical support (ASSIM tool) enabling secure and real time dissemination of information.

---

\(^2\) Airspace Security: safeguarding of the airspace of responsibility from unauthorised use, intrusion, illegal activities or any other violation. This involves managing the airspace to prevent, detect and resolve where possible airborne threats.
5. **Technical support (ASSIM supporting tool)**

A fundamental aspect of ASSIM is the collection and timely dissemination of the required information. The ASSIM concept considers the national Governmental Authorities (NGAs) as the end user. The rest of the actors should play a role to support the NGA and facilitate the decision making process.

An ASSIM tool should therefore be tailored taking into account the NGA needs. An automated ASSIM tool will clearly benefit the national decision making process by gathering and disseminating in real time secured (i.e. encrypted) information. Pre-defined sets of information items must be available immediately an incident escalates to NGA level; only an automated tool can provide for this, especially in a multiple event scenario.

COTS (Commercial off the Shelf) products should provide the best option for the ASSIM tool, from a pragmatic and cost-efficiency point of view.

6. **ASSIM supporting tool components**

Taking into consideration information provided in above paragraphs, the two keys aspects for the management of in-flight security incidents are:

- Real time availability of secured information of the situation on board;
- Real time security information sharing, including situation on board.

Technology can support both, the acquisition of airborne information and the sharing of security information through a network. EUROCONTROL and NATO are involved in two pilot projects addressing both aspects, in order to assess feasibility and implementation options.

6.1 **Airborne information acquisition**

In-flight security can be enhanced by providing real-time encrypted information (voice, data and video) from aircraft to the ground. The information would provide the security authorities with much-improved situation awareness in the event of malicious interference with an aircraft in flight.

Initial trials made by EUROCONTROL using third generation mobile telephone Technology gave a positive indication on feasibility. At present some requirements are under discussion for the definition of an airborne component of an in-flight security incident management system:
• To use existing Commercial Off-The-Shelf (COTS) products. With the minimum adaptation it should provide the essential elements to support flight validation;

• The information should include voice, video and data (aircraft parameters);

• To adopt Internet Protocol (IP) for connectivity. The use of standard Internet Protocol ensures that applications designed for IP are compatible. These must include digital voice, data transfers and video applications;

• Security must be introduced by the coding of data and by encrypting, to the extent necessary, at application level using IpSec;

• It must operate in a cooperative and non-cooperative environment. This means the possibility to activate it from the ground;

• It must provide for recording capabilities;

• Ground infrastructure must be minimal;

• Radio Spectrum requirements; the availability of suitable radio spectrum is critical for all systems that transmit or receive. The aeronautical industry is seen by radio regulators as having more than adequate amounts of spectrum and continually urge the industry to make more efficient use of it. This means that any new aeronautical system must be accommodated within existing aeronautical spectrum and must be compatible with other systems.
6.2 Security information sharing

Once security information has been acquired, the second step is sharing this information among all actors involved in in-flight incidents. This is required to assess the situation, take the appropriate actions and facilitate and support the decision making process.

Initial developments were focused on the establishment of a European focal point for Renegade information gathering and dissemination. This was based on a stand alone system with specific hardware and software. Some difficulties immediately arose: implementation of a new dedicated system isolated from the standard systems used for day to day operations and the need for special procedures and training to get familiar with it. This initiative was therefore abandoned and further activities re-focused on user friendly, COTS technologies.

The current project relies on the Private Key Infrastructure (PKI) technology, which is more and more widely used in both the civil and military environments.

PKI brings a solution for the basic problem of confidence and trust in the electronic world:

- Identity of an user
  - AUTHENTICATION ➔ Digital Signature
- Information to be kept Private
  - CONFIDENTIALITY ➔ Encryption
- Information cannot be Manipulated
  - INTEGRITY ➔ Digital Signature
- Information cannot be Disowned
  - NON-REPUDIATION ➔ Digital Signature

PKI offers a secure (PKI encryption) environment for the exchange of security related information, and can be interfaced with any other IP based security application, i.e. will be compatible with the airborne component (paragraph 6.1).

The potential of PKI goes beyond the ASSIM concept, and offers extra possibilities for aviation security and security in a wider sense. Validation trials are on going and initial results look quite promising.
Secure Email Framework

User 1
Public key

Registry

User 2
Public key

User 1

User 2