

ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)

2.5 Safety and security of the ATM infrastructure :

SECURITY IN ATM COMMUNICATIONS

(Presented by Italy)

SUMMARY

Air Transport has to be considered a “Critical National Infrastructures (CNI)” and therefore ATM communications, comprising mobile and fixed sub-networks, must be deemed to be “Critical Information Infrastructures (CII)”. This paper presents the some specific aspects of CNI-CII systems relevant to the security such as encryption, connectivity, quality of service and others.

Italy proposes to use the EUROCONTROL strategic Initiatives and define guidelines for the improvement of air traffic management communications security.

Action by the conference is in paragraph 4.

1. INTRODUCTION

1.1 Today States and super national organizations base their growth and internal organization on increasingly complex and comprehensive infrastructure systems like, for example, electrical power distribution, transport, public communication, etc. This involves a strong correlation between the security and the vulnerability of such infrastructures and the efficiency of the system as a whole.

1.2 Moreover after the September 11th attack, organizations that play a critical role for both national and international contexts have to review their approach toward the security and the survivability of infrastructures.

1.3 Such critical infrastructure has been defined as critical national infrastructure (CNI) — and the essential “defence” has become an urgent priority.

1.4 Air transport has to be considered a significant component of said CNI and, in the frame of air traffic management (ATM), the relevant telecommunications and information networks, fixed and mobile, have to be considered one CNI or, more precisely, a so-called critical information infrastructure (CII).

1.5 In the above framework, Italy proposes to use the EUROCONTROL Strategic Initiatives and develop a coordinated set of actions focussed on how air traffic management communications security could be improved.

2. FIXED AND MOBILE CII

2.1 Fixed communications

2.1.1 The main features that are essential to ensure a secure CII are as follows:

- a) **Topology redundancy:** The CII should be planned to have high connectivity both among core nodes (a minimum degree of 3 is advisable) and between access and core nodes (where a “double homing” is recommended);
- b) **High quality transmission bearers:** A CII should guarantee correct and timely information flow under all circumstances, both routine and emergency. Users should be provided the demanded bandwidth and the agreed quality of service (QoS). Thus high capacity link and intelligent switching nodes should be used. To meet redundancy requirements, links should be of different types, including high capacity radio links (line of side (LoS) and satellite (SAT), and fibre optic cables (FOC). To assure effective bandwidth management, the links should be owned by the CII itself and possibly separated from public lines;
- c) **Distributed network intelligence:** The CII should be able to provide both voice and data services with the required quality. It should dynamically optimize overall network resources allocation, finding the least congested paths and possibly exploiting the redundancy in link types and in network topology. In addition, CII should handle traffic flows with different priorities, according to different classes of services, and has to be able to pre-empt lower priority connections in case of emergency or reduced available bandwidth. The asynchronous transfer mode technology, which natively incorporates almost all of these features, is considered the best suitable choice for the underlying transmission infrastructure and network management control plane;
- d) **Security features:** As well as guarding against “physical” intrusion, the CII carries CNI critical data that must be secured against unauthorized viewing or altering. The issue should be addressed by means of encryption and firewalls. Firewalls should be implemented at the borders of local domains, and they should be appropriately configured. This is especially important in case of remote access to control stations and could include strong authentication mechanisms, suitably tuned for different levels of access (according to the - military originated - *need-to-know* principle). Additionally, it is strongly recommended that critical traffic (like authentication passwords or keys, and control or system information) would flow on the network in encrypted form to avoid

external detection of inner CNI topology and critical resource locations by means of traffic analysis; and

- e) **Efficient interoperability and integration capabilities:** CII should be designed to be interoperable, as far as possible, with intercommunication standards and it should integrate with mobile and fixed deployable systems.

2.2 Mobile communications

2.2.1 The main features that are required for a secure CII air-ground component are as follows:

- a) **Avoidance of unauthorized view:** air-to-ground communications can be easily viewed using a commercial receiver that is on sale to the public . This issue should be dealt by means of encryption and authentication of the source of the information or by other suitable solutions;
- b) **Capability to operate in presence of interference (jamming):** air-to-ground communications can be easily jammed using a commercial transmitter. This issue should be dealt by means of frequency hopping or spread spectrum transmissions or other suitable solutions;
- c) **Capability to operate in presence of interference (spoofing):** air-to-ground communications can be easily deceived (or “spoofed”) using a commercial transmitter. This issue should be dealt by means of message authentication; frequency hopping or spread spectrum should be also useful;
- d) **Data integrity:** the presence of an alternative air-to-ground communication link (as example a satcom link) should be the means to assure high integrity level of a mobile CII with reference of critical and sensible information; and
- e) **Physical separation:** In order to assure effective communication management the ATM air-to-ground communications should be possibly separated from the others air-to-ground services like Internet, e-mail, public communications, cable TV and company communications aircraft communications (addressing and reporting system (ACARS) and aeronautical operational control (AOC)).

3. PROPOSED STRATEGIC INITIATIVE

3.1 It is proposed to develop and validate, even from the cost /benefit aspects, the security guidelines that would define the minimum requirements for the security related aspects for fixed and mobile ATM communications such as ground and on-board architecture, redundancy, connectivity, information protection, interoperability, data integrity and interference aspects.

4. **ACTION BY THE CONFERENCE**

4.1 The conference is invited to:

- a) acknowledge that the fixed and mobile networks supporting the ATM communications are “critical information infrastructures” and therefore have to guarantee the relevant security issues; and
- b) request ICAO to develop and validate guidelines for CNI-CII secure fixed and mobile communications for ATM taking care also of the cost/benefit aspects.

— END —