International Civil Aviation Organization

AN-Conf/12-WP/122
9/10/12
English only

WORKING PAPER

TWELFTH AIR NAVIGATION CONFERENCE

Montréal, 19 to 30 November 2012

Agenda Item 1: Strategic issues that address the challenge of integration, interoperability and harmonization of systems in support of the concept of "One Sky" for international civil aviation

1.1: Global Air Navigation Plan (GANP) – framework for global planning

CYBER SECURITY FOR CIVIL AVIATION

(Presented by the International Coordinating Council of Aerospace Industries Associations)[*]

SUMMARY

Cyber security has been identified as a high-level impediment to the implementation of the Global Air Navigation Plan.

The term "cyber security" encompasses the protection of electronic systems from malicious electronic attack and the means of dealing with the consequences of such attacks. It comprises managerial, operational and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems. Currently cyber security is a relatively minor issue in civil aviation, but this is changing. New technologies are being adopted which are intrinsically more vulnerable to cyber attack and which collectively increase the impact from such attacks.

Numerous industry groups are making standards in their own areas of expertise but there is no overall oversight so there is the potential for gaps, overlaps and inconsistencies. Also there is no overall global framework within which these groups can work.

A top-down approach is required at a global level to establish a cyber security architecture that will frame the efforts of global industry, rule makers and regulators.

Action: The Conference is invited to agree to the recommendations made in paragraph 3.

1. INTRODUCTION

1.1 The first agenda item for the Twelfth Air Navigation Conference (AN-Conf/12) has identified cyber security as a high-level impediment to implementation that should be considered as part of the roadmap development process. Also the Conference is being invited to "make recommendations on multi-party approaches to standards development to support the implementation timeframes specified in the roadmaps (which are part of the ASBUs)". This is part of Agenda Item 6: Future direction.

[*]The following organizations support ICCAIA's conclusions and recommendations as expressed herein: European Organization for Civil Aviation Equipment (EUROCAE), International Air Transport Association (IATA), International Federal of Air Traffic Control Associations (IFATCA), RTCA, Inc., and SAE International.

1.2 Cyber security is an issue because many civil aviation organizations rely on electronic systems for critical parts of their operations, including safety-critical functions. The protection of electronic systems from malicious electronic attack (unlawful interference) and the means of dealing with the consequences of such attacks is encompassed by the term cyber security. It comprises managerial, operational and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems. Cyber security is also often referred to as information security, and while the two terms are not synonymous they are similar enough that the differences can be ignored in this context.

1.3 Currently cyber security is a relatively minor issue in civil aviation, but this is changing. Although the adoption of new technology is an ongoing activity in civil aviation, the current pace and extent of new information technologies is notably increasing the risk from cyber attacks. This is due to a number of factors:

a) there is an increased reliance on a small number of technologies, such as Linux, Windows, IPv6 protocols and Ethernet (AFDX), and these technologies are widely used in the IT industry;

b) as a result there is widespread understanding of these technologies, and of their weaknesses and vulnerabilities;

c) systems are becoming more interconnected and security lapses in one system are likely to affect others; and

d) there is greater impact from systems failures due to increased reliance on them.

1.4 Over and above these factors, there is the potential for unforeseen systematic problems due to weaknesses in oversight. This is mainly due to a lack of coherence between the many groups working on cyber security, and a lack of expertise and understanding amongst those who might provide the coherence. Some knowledge of these problems exists within the industry, but knowledge of the big picture is more limited.

1.5 ICAO estimates that US$120 billion will be spent on the transformation of air transportation systems in the next ten to fifteen years. This transformation will bring significant benefits for safety, efficiency and the environment. Stakeholders, including service providers, regulators, airspace users and manufacturers, will face increased levels of interaction as new, modernized ATM operations are implemented. Security issues related to the transformation of the aviation system are coming into view, issues that will require closer collaboration among experts in safety and security disciplines. As the agenda for AN-Conf/12 states, security matters should be considered in the system changes that lie ahead.

1.6 ICAO has recently amended Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference* to include the information security dimension. Chapter 18 of the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference* (Doc 8973/8) is being published as advisory material to Member States. This does not include the problem of how future air traffic control systems are to be adequately secured.

2. DISCUSSION

2.1 There are already a number of examples of cyber security incidents and vulnerabilities:

a) vulnerability: An extract from the media in July 2012: “At a recent conference Dr. Andrei Costin gave an unnerving demonstration of weaknesses in the air traffic control systems coming into use. He showed that with just $2 000 worth of store-bought electronics an ADS-B beacon could be ‘spoofed’ to show that a non-existent aircraft was coming in to land. This ‘Ghost Plane’ presentation was possible because air traffic control systems have no way of verifying where messages are coming from”;

b) incident: Three software engineers were accused of disrupting operations at a new terminal at an airport in June 2011. They worked for a sub-contractor and when they didn't get a pay rise they sabotaged the program code. Check-in services failed 3 days later, and 50 flights were delayed, causing knock-on delays elsewhere;

c) vulnerability: There have been incidents involving crashes or tail strikes when flight crew have made errors in calculating take-off performance parameters using electronic flight bags (EFBs). These were the result of human error, but there is the potential for the EFB programming to be corrupted maliciously (hacked), particularly when these devices are connected to external networks to receive updates; and

d) vulnerability: There is an increasing reliance on GPS systems for position, navigation and timing (PNT) services. However, reception of GPS signals can easily be jammed and there have been accidental and malicious incidents of jamming across metropolitan-scale areas. Too much reliance on GPS thus puts aviation services at risk if alternative PNT sources are not available.

2.2 It is also worth considering the systemic risks posed by the new, more interconnected systems. As an example there is the theoretical potential for a cyber attack to affect multiple connected systems, which could (in the future) have an effect analogous with the recent Icelandic volcanic ash problems, shutting down air travel across parts of Europe for several days. In that case estimated costs run into the billions of dollars or Euros:

Cost (Euros)	Reason
1.3 Billion	Loss of airlines earnings - reported by IATA
12,700	Estimated financial damage per cancelled flight in Germany.
3M per day	Estimated loss of ATM earnings.
1-1.5 million euros per hour	Estimated cost of a complete ATM failure (this figure includes the airline, airport and ATM losses), made by a major European airport.

2.3 There is also an issue with timeliness as cyber security threats will challenge current aviation regulatory processes as a response to a new cyber security threat must be implemented on all affected aircraft with hours (a few days at most), or the potentially affected systems must be shutdown to protect the aircraft. This is at odds with current aircraft architectures and certification processes.

2.4 Rule makers and regulators worldwide are struggling to provide the certification criteria, methods and toolsets that will be required to substantiate the necessary assurance related to the new cyber security dimension. A large number of initiatives, projects, programs and activities are currently underway to deal with portions of the issue, for example:

a) Eurocae/RTCA (aircraft/avionics manufacturing standards);

b) A4A (Airlines for America) DSWG (Digital Security Working Group);

c) IETF (Internet Engineering Task Force);

d) CEN (European Standards Organisation);

e) ETSI (European Telecommunications Standards Institute); and

f) AEEC (Airlines Electronic Engineering Committee).

2.5 Unfortunately there is no overall oversight so there is potential for gaps, overlaps and incompatible standards. Also there is no overall framework within which these groups can work. Also the groups are often national or regional in nature, or deal with narrow industry areas. What is required is oversight and coordination by ICAO; a recognized global authority is necessary to insure a viable resolution, facilitate the cost-effective use of limited resources (both in terms of people and funds) and also to resolve any parochial issues. To be fully effective, the solution for this situation must be globally applicable. Hence, an ICAO Task Force responsible for Cyber Security would be an ideal solution to this problem.

2.6 Within ICAO, some work is already underway. The ICAO Aeronautical Communications Panel (ACP) is developing SARPS for the aeronautical telecommunication network (ATN). This network will be based on the internet protocol suite. Although basic security provisions will be in place, resources need to be applied to developing a robust architecture that will adhere to the necessary cyber-security policies and practices. *Of special importance are the associated Internet addresses and domain names, which will require both personnel and financial resources to secure and retain them.*

2.7 The Cyber Security Task Force would draw on the work carried out by the ACP and complement this with high-level provisions related to the tasks of implementing, managing and auditing robust cyber-security practices and procedures.

2.8 Realization of the widespread nature of these problems has crystallised within industry, in such groups as Eurocae WG-72, RTCA SC-216, AEEC NIS and the informal Joint Co-ordination Group. People with a wide range of civil aviation and cyber security experience are ready to assist ICAO in this effort.

3. CONCLUSIONS AND RECOMMENDATIONS

3.1 ICAO should take a general top down view of the overall problem of security. A top-level body needs to address all aspects of civil aviation cyber security as greater amounts of critical air navigation, control and business information is shared between IT systems and between organizations. This will include defining core Internet requirements for the new advanced air traffic management networks. It will also take into account that cyber security technologies will evolve and will regularly require updating, both in the air and on the ground.

3.2 The Conference is invited to:

a) recognize the risks in the current situation and the potential for future problems;

b) create a Cyber Security Task Force (CSTF) to evaluate the extent of the problem and draw up a global cyber security architecture, which includes contributions from industry;

c) encourage states to provide the Aeronautical Communications Panel (ACP) with the resources to complete its work in developing a robust, secure aeronautical telecommunication network (ATN) using IPV6 as a foundational part of the next generation air traffic management systems; and

d) encourage States and industry to contribute to the work of the CSTF to ensure aircraft can interoperate with air navigation service providers (ANSPs) around the globe.

— END —