



THIRTEENTH AIR NAVIGATION CONFERENCE

Montreal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues

5.4: Cyber resilience

IMPLEMENTATION OF MEASURES FOR THE PROTECTION
AGAINST CYBER-THREATS

(Presented by the Agency for Air Navigation Safety in Africa and Madagascar (ASECNA)
on behalf of its Member States²)

EXECUTIVE SUMMARY

This paper highlights the importance for States/air navigation services providers (ANSPs) to deploy cyber security and resilience systems for air traffic management (ATM) and communications, navigation, and surveillance (CNS) to support their integration and interoperability, which is the key for the implementation of a seamless airspace.

It also aims to update the Conference with the actions taken by ASECNA and the relevant challenges, regarding the protection of the ATM systems against the new threats such as cyber-attacks.

Action: The Conference is invited to:

- a) note the actions taken by ASECNA and the relevant challenges regarding the protection of the ATM systems against the new threats such as cyber-attacks;
- b) encourage States/ANSPs to implement systemic and structured approaches to cyber security and resilience of the ATM system to foster cooperation in the implementation of the Air Navigation Plan ;
- c) note the availability of ASECNA to share its experience with other ANSPs.

1. INTRODUCTION

1.1. The sector of the aviation is dependent on the technology and communication information systems and this dependence is increasing with the need of data sharing and systems

¹ English and French versions provided by ASECNA.

² Benin, Burkina Faso, Cameroon, Central African Republic, Chad, Comoros, Congo, Côte d'Ivoire, Equatorial Guinea, France, Gabon, Guinea-Bissau, Madagascar, Mali, Mauritania, Niger, Senegal, Togo

interoperability, as well as the implementation of the system-wide information management (SWIM), which are based on information technologies, supported by internet protocol (IP).

1.2. The data exchanged between the systems (ground/ground, ground/air) including ATS interfacility data communications (AIDC), ATS message handling system (AMHS) and air traffic services (ATS) surveillance systems will be key elements to manage safely, fluently and orderly the air traffic. So, for the ANSP, the integrity and the data privacy will be the major factors for the safety and the efficiency of the aviation.

1.3. The threat that cyber incidents pose to civil aviation is changing rapidly and constantly. The malicious intentions of cyber-terrorists range from the disruption of business continuity to information theft for various reasons. The threat can easily evolve to reach crucial civil aviation systems around the world.

1.4. Taking into account this threat, a risk-based approach in civil aviation is the best way to prevent the cyber-incidents, instead of managing their occurrence.

2. DISCUSSION

2.1. The ANSPs have to determine the critical data and systems that they used, perform cybersecurity and resilience risk assessments on CNS and ATM systems and to implement appropriate measures to protect them against illicit interventions.

2.2. ASECNA made an assessment of its maturity level in 2016 and developed an action plan for the implementation of a systemic approach for managing cyber security and resilience of CNS and ATM system.

2.3. The implementation of this action plan is ongoing, by setting up operational measures and the Security Management System (SeMS) taking into account cyber security and resilience of CNS and ATM system.

2.3.1. In compliance with the provisions in *Air Traffic Management Security Manual* (Doc 9985), ASECNA set up operational measures to protect its systems, including:

- a) air navigation ground aids;
- b) ground/air communications;
- c) data links;
- d) surveillance systems;
- e) satellite navigation system (GNSS);
- f) flight plan and traffic data;
- g) information and communications technologies (ICT) () systems for the air traffic management; and
- h) information management system in ASECNA (intranet, enterprise resource planning “ERP”, ASECNA messaging system).

2.3.2. The Security Management System (SeMS) is implemented through ASECNA's integrated management system (IMS), integrating several domains (safety, security, quality, environment, health and safety at work and information system), considering that cybercrime protection performance can be impacted by risks from other domains. The development of complementary processes and procedures to

those designed for its integrated management system (IMS) is ongoing, including the training and awareness-raising actions relating to the provisions of ICAO Doc 8873 and 9985

2.4. As part of the implementation of the global air navigation plan through the ASBUs, ASECNA has initiated investment programs for the implementation of AIDC, AMHS, but also ATS surveillance data sharing with some ANSPs in the region and malicious threats may be blocking factors for the success of these cooperation initiatives.

3 CONCLUSION

3.1 One major challenge is to implement mechanisms for managing and sharing the information about security, taking into account that ASECNA is ANSP for in an airspace of 18 Member States, using harmonized procedures and of interconnected and integrated ATM systems. In addition, these mechanisms shall be in accordance with the existing specificities in each member state related to security policy in security.

3.2 The second challenge to highlight is to implement protective measures for equipment and services, considering the interoperability of ATM systems in operational centers in the African scale. The interconnection and the interoperability of air navigation systems, expose these systems to a bigger risk of cyber-attacks.

3.3 The measures to be set up shall take into account the scale of the phenomenon of the terrorism in certain States of Africa-Indian Ocean (AFI) region.

— END —