Twenty-Fourth Meeting of the AFI Planning and Implementation Regional Group (APIRG/24) (Virtual – 2 to 4 November 2021)

Agenda Item 4: Other Air Navigation Initiatives

Status of ATM Cybersecurity

(Presented by ASECNA)

SUMMARY	
In its conclusion 23/25 on cybersecurity and resilience of air navigation systems, in order to increase the capacities of States and organizations in cybersecurity it was agreed that the " ICAO, with industry collaboration under the APIRG mechanism, is increasing its support for activities aimed at raising awareness of cybersecurity and NSA resilience through webinars / workshops / seminars on cybersecurity and the resilience of ANS systems for the AFI region. This paper highlights the vision of ASECNA, facing the organizational and operational challenge of ANS Cyber Resilience in its area of responsibility. It also highlights the challenges encountered with a focus on all data used / stored / exchanged, not only the infrastructure (data protection). Action by the Meeting are indicated in paragraph 3	
Strategic Objectives	A - B

1. INTRODUCTION

1.1 The global aviation system is one of the most complex and integrated systems of information and communications technology (ICT) in the world. Therefore, ATM system is a potential target for a large-scale cyber-attack. In fact, the ATM systems, as important part of transport infrastructure is an attractive target for cyber-attacks due to its importance and prominence. The networks and systems, interconnecting the various ANSP are IP-based and are exposed at several levels to cyber-attacks. The cyber threats are real and can take several forms depending on the means of the hackers. Therefore, organizations must identify their critical information systems and implement appropriate cyber security measures at the operational level.

2. DISCUSSION

2.1 The increasing interconnectivity of Air Traffic Management (ATM) means that the impact of a cyber-attack may extend across a growing number of interconnected systems. Considering the very high level of interconnection of CNS / ATM systems, in the same operational ecosystem of data collection, transmission and processing internally, as through bilateral links, there is real need for a harmonized cyber-strategy over the AFI region.

2.2 The fact of having bilateral connections under TCP / IP protocol is now a necessity, in order to be able to establish for example, full AMHS connections, to share surveillance data, or to deploy SWIM in a few years. In this context, cybersecurity issues are increasingly becoming collective issues, it is a shared responsibility. Hence the need to conclude bilateral agreement of cooperation between ANSP, in order to assess concretely all cyber issues such as, common procedure for identification of threats, training, performances, risk assessment, security analysis, audits and control, penetration test exercises.

2.3 It is no longer indicated to be satisfied only with seminars and workshops, the time has come to make concrete and practical arrangements.

2.4 As such in terms of human resources, we should not hesitate to open the field of profiles and skills required to strengthen the ATSEP, in this extremely sensitive and specialized field, the idea is to build a mixed network of experts able to face the cyber challenges of ATM.

2.5 In order to mitigate the cyber risks linked to the sharing of information beyond its planned “sphere of dissemination” the guidance documents on the use of the Traffic Light Protocol (TLP), published in September 2021 under the authority of the Secretary General of ICAO have been adopted and actions taken to include the use of TLP in the communication policy and make it applicable in ASECNA from the beginning of next year.

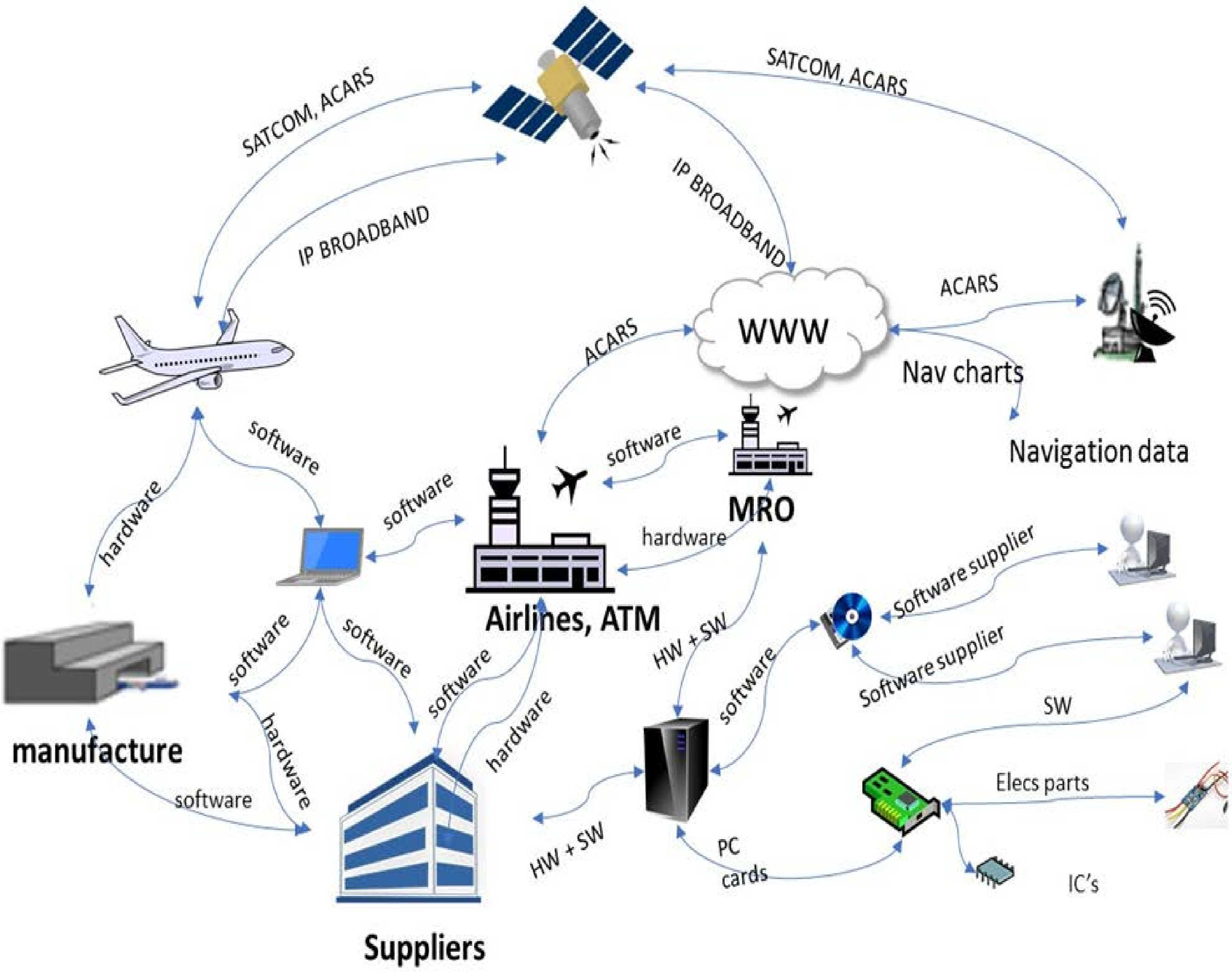
3. ACTION BY THE MEETING

3.1 **The meeting is invited to:**

a) Note the information provided in this working paper
b) Make relevant recommendations to create the best possible conditions for the implementation of standards and procedures on cybersecurity threat, such as regular penetration tests, sharing of bests practices formalized in technical letters of agreement in the field of cybersecurity.
c) Encourage States and organizations to work decisively in the cooperative approach to define and implement the necessary reactive and proactive action plans to address the challenge of cybersecurity as a shared responsibility.
d) Support the guidance material and develop and implement policies for the use of Traffic Light Protocol by states and organizations.
e) Developed business recovery and business continuity plans in the event of a cyber-attack.

Appendix 1

Cyber Security is a shared Responsibility


SATCOM, ACARS
SATCOM, ACARS
IP BROADBAND
IP BROADBAND
WWW
ACARS
ACARS
Nav charts
Navigation data
software
software
software
MRO
hardware
hardware
Airlines, ATM
Software supplier
Software supplier
HW + SW
software
software
software
software
hardware
hardware
manufacture
software
SW
Elecs parts
HW + SW
PC
cards
IC's
Suppliers