International Civil Aviation Organization

WORKING PAPER

A40-WP/105[1]
TE/33
30/7/19

ASSEMBLY — 40TH SESSION

TECHNICAL COMMISSION

Agenda Item 30: Other issues to be considered by the Technical Commission

ENABLING DIGITAL AVIATION THROUGH THE CYBER-DEVELOPMENT OF AIR TRAFFIC SAFETY ELECTRONICS PERSONNEL (ATSEP)

(Presented by the International Federation of Air Traffic Safety Electronics Associations (IFATSEA))

EXECUTIVE SUMMARY	
The next generation of operational staff, of aircrews and of air traffic control officers (ATCOs), will increasingly rely on the technical and managerial capability of ATSEPs to withstand cyber threats to information systems and to the communications, navigation, and surveillance (CNS) infrastructures that protect the travelling public. The obligation of States to identify critical infrastructures and to establish a computer emergency response team overlaps with the personal liability of ATCOs and ATSEP. There are also overlaps between critical infrastructures. If there is an attack on the wider infrastructures that support air traffic management (ATM), the security ATSEP has a clear role to play in coordinating recovery while ensuring that ATM operations remain safe. **Action:** IFATSEA invites the Assembly to note the information contained in this working paper and request the Council to undertake the necessary steps to develop a new ATSEP stream safety, security and cyber security, together with the corresponding training.	
Strategic Objectives:	This working paper relates to the Safety, Air Navigation Capacity and Efficiency and Security & Facilitation Strategic Objectives.
Financial implications:	The cost of implementing a new ATSEP stream is expected to be minimal since it simply enlarged the current implementation of Competency Based Training described in Doc 10057.
References:	Annex 10 — *Aeronautical Telecommunications*, Volumes I, II, III and IV Doc 8071, *Manual on Testing of Radio Navigation Aids* Doc 9683, *Human Factors Training Manual* Doc 9868, *Procedures for Air Navigation Services — Training* (PANS-TRG) Doc 10057, *Manual on Air Traffic Safety Electronics Personnel Competency-based Training and Assessment*

[1] Arabic, Chinese, English, French, Russian and Spanish versions provided by IFATSEA.

1. INTRODUCTION

1.1 Around the globe, there are plans to develop new infrastructures that support air traffic management; including but not limited to the Next Generation Air Transportation System (NextGen) and Single European Sky ATM Research (SESAR). These visions all rely on highly dependable digital processing and communications methodologies. The safe and successful development of these large and complex infrastructures pose numerous challenges, including the need to integrate new technologies with legacy systems. These state of the art interoperable digitally based ATM systems rely on cyber security to be at their core; in order to ensure the integrity and safety of the air traffic operation. This, in turn, requires air traffic safety electronics personnel (ATSEP) with a new and evolving skill set. It is clear that the nature of the cyber threats to aviation will change over time. This submission proposes a practical, systematic approach to the development of training, pedagogy and competencies enabling a new generation of staff capable of realizing our shared vision of digital aviation.

2. DISCUSSION

Safety and security in ATM/ANS

2.1 New regulations (US PPD-21, EU 2016/1148) increasingly require States to define their critical infrastructures and identify the growing interdependencies between them, for example between digital telecommunications and air traffic management systems.

2.2 At present many air navigation service providers (ANSPs) lack cyber expertise; this is natural given that in the past the threat levels were very low. They often lack well-qualified staff. Many ANSPs have addressed this limitation by hiring external cyber security consultancies. Often contracts are awarded to companies from outside aviation with little regard to the domain knowledge that is needed to maintain safe and successful operations. It can be hard for external consultants to convince ATCOs of the potential threat to operations from malware that crosses the ‘air gap’ to systems that are isolated from the public internet. Hence, external companies often have a very limited effect on the resilience of many member States. Furthermore, the development of a strong security culture, like safety, is most effective when released in house. Within the air traffic services (ATS) provider, external companies lack the influence on ATSEP, who are responsible for the technical systems and on ATCO´s who are dependent on the systems to provide the air traffic service.

2.3 ATSEP have an increasingly important role in protecting these critical interfaces (ICAO A39.WP17 EX / 5). For example, most countries have developed or are beginning to develop computer emergency response teams (CERTs), which fall under the responsibility of ATCOs and ATSEP. However, the treatment of cyber security in the training of ATSEP is, at best, inconsistent and at worst ad hoc.

Political and regulatory background

2.4 The importance of these issues has been recognised and enshrined in a number of instruments. These include aspects of the Federal Aviation Administration (FAA) Enterprise Network Services (FENS), as well as Regulation (EC) No 300/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2008 on common rules in the field of civil aviation security. In other areas of the world, there is a danger that countries may fall even further behind in respect of cyber safety. There is a need for greater guidance on appropriate measures to protect our common future in digital aviation infrastructures, especially when EU Regulation No 1254/2009 allows Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures. The importance of such a clear vision was also addressed by ICAO Secretary General Dr. Fang Liu during the ICAO-EASA Forum, 21 September 2018.

3. **CONCLUSION**

3.1 Proposal for an ATSEP stream safety, security and cyber security and the corresponding training.

3.2 We suggest, to create a new ATSEP stream safety, security and cyber security that is intended to leverage their existing knowledge of aviation infrastructures with a solid foundation in both the threats to as well as the means of defending those infrastructures. We envisage competency that extends to overlapping areas in other critical infrastructures; this will increase the resilience of aviation which relies on extended supply chains that use widely available mass market digital technologies, well-known to hackers and State agencies.

3.3 We raise this issue because different Member States are taking radically different approaches to the engineering of cyber security in ATM operations; however, we all rely on the strength of our neighbour to sustain the transport networks. Therefore, to enable and enhance the implementation of digitalization globally in ATM/ATS, we underline the importance of a common approach.

3.4 Furthermore, IFATSEA proposes to set up a new cyber security training stream where entry level qualifications should be defined in cooperation with States or air navigation service providers but with the common aim of increasing trust in the resilience of our neighbours’ aviation infrastructures because they will be defended by well-qualifies ATSEP.

3.5 In addition, IFATSEA offers ICAO assistance in questions concerning the training of ATSEP, implementation and operation of technical systems and functions.

— END —