International Civil Aviation Organization

WORKING PAPER

A41-WP/122[1]
TE/37
1/8/22

ASSEMBLY — 41ST SESSION

TECHNICAL COMMISSION

Agenda Item 31: Aviation Safety and Air Navigation Standardization

UPDATE EXISTING ATSEP CYBERSECURITY TRAINING OBJECTIVES AND DEVELOPMENT OF NEW ATSEP CYBERSECURITY TRAINING OBJECTIVES

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

EXECUTIVE SUMMARY

This paper describes a proposal to update existing air traffic safety electronics personnel (ATSEP) Cybersecurity Training Objectives and develop new Cybersecurity Training Objectives in ICAO *Manual on Air Traffic Safety Electronics Personal Competency-based Training and Assessment* (Doc 10057).

Action: The Assembly is invited to:

a) note the increasing roles and responsibilities of ATSEP as part of cyber defense at the interfaces with adjacent areas of responsibility and new ATM architectures and business models;

b) note the ever changing and dynamic nature of cyber threats; and

c) to prioritize and take all the necessary steps within the *Procedures for Air Navigation Services — Training* (PANS-TRG, Doc 9868) process to update of existing Cybersecurity Training Objectives, and development of new ATSEP Cybersecurity Training Objectives for both Basic and Qualification Training Objectives in Doc 10057, Appendix B

Strategic Objectives:	This working paper relates to the Safety, Air Navigation Capacity and Efficiently, Security and Facilitation Strategic Objectives.
Financial implications:	There will be some cost associated with updating and developing Cybersecurity Training Objectives in Doc 10057. Training units responsible for ATSEP Basic and Qualification training may have to adapt content of training courses to incorporate the updated or new objectives.
References:	A39-WP/370, *A cybersecurity architectural approach for legacy- and SWIM-based CNS/ATM systems* Annex 10 — *Aeronautical Telecommunications*, Volumes I, II, III and IV Doc 10057, *Manual on Air Traffic Safety Electronics Personnel Competency-based Training and Assessment* Doc 9868, *Procedures for Air Navigation Services — Training (PANS-TRG)*

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

1. INTRODUCTION

1.1 CNS/ATM systems are undergoing a paradigm shift with the implementation of new technologies, concepts, and business models. The integrated ANS model is going to be replaced with a Service-Oriented Architecture (SOA) which is distributed in nature, and information is exchanged over networks such as SWIM. Air Navigation Systems. Services will exist on the ground and space and even ATM Data Processing can be on systems deployed in distributed architectures and geographically apart (e.g European ADSPs and Virtual Centers). Hybrid CNS system configurations are quickly coming into operation throughout the aviation ecosystem. If the interconnection interfaces of the air transportation system between stakeholders are not adequately addressed in terms of cybersecurity, vulnerabilities can occur in a system or element of a system at one stakeholder. Although these vulnerabilities do not pose a major risk to that system itself, they can easily escalate to a threat that poses a risk to another stakeholder's system with negative consequences. The creation of an ATM Data layer between ANS stakeholders and external stakeholders is required.

1.2 ICAO in the Aviation Cybersecurity Strategy, October, 2019 Chapter 7. Capacity building, training and cybersecurity culture states "Appropriate job-related training should be provided on a continuous basis to support personnel in their daily roles" and "Cybersecurity could be included in the strategy for the next generation of aviation professionals as ICAO is well-placed to work with States and industry to develop role-based competency requirements for aviation professionals". Also in the ICAO draft report A40-WP/577 para.30.36 it is stated " that specific guidance on cybersecurity training could be considered for future updates to Doc 10057".

1.3 ATSEP are the first specialists within an ANSP to tactically address cybersecurity from attack vectors either though network or combined with signal in space. They are responsible in this case to distinguish between technical failures and cyber-attacks. One thing these services have in common is the authorization to put in service, out of service, commission and decommission hardware and software by ATSEP. To better secure the ATM functional system as described above, these appropriate specialists who also have legal access to the technical ATM/ANS systems should be deployed at the interfaces.

1.4 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 ATSEP. However, the training of ATSEP contained in the current version of ICAO Doc 10057 is addressed mainly as security requirements while the reference to Cybersecurity especially towards addressing the paradigm changes brought forward by SESAR and NextGen, including the CANSO vision ATM is not addressed. For the above reasons, there is a clear need to expand training for ATSEP within a Cybersecurity context in order for them to acquire the competence to tactically and strategically address Cyber-events.

1.5 As known from Europe, security does not require only ATS providers to have a safety management system, as is the case with safety, but the NPA 2019/07 requires an ISMS (Integrated Security Management System) for all ATM/ANS and enabling services, there are a lot of additional interfaces, which is also correct, since it is a matter of different service provisions and activities. However, the incursion and treatment of cyber security in the training of ATSEP globally within ANSPs is, at best, inconsistent and at worst ad hoc.

1.6 To understand the impact of a cyberattack on the individual parts of the ATM network, it is not enough to have a very good knowledge of IT technology and IP networks. Since the different networks are not only physical connections, but information, controls and signals triggered by different factors and using different transmission paths such as radio, VoIP, networks, human commands, light signs and signals, sounds, etc., a deep understanding of the cybersecurity mitigation actions and their impact on ATM Safety is also required. It is also necessary to have an aeronautical background.

1.7 Therefore it is proposed to refocus and expand the training context of ATSEP in Doc 10057, in Cybersecurity from within ATM/ANS Services, who they have sufficient aeronautical background and safety culture as well as the necessary knowledge in network technology and computer science, to address the cyber security threats tactically and strategically.

2. DISCUSSION

2.1 The existing Training Objectives contained in the ATSEP Training Manual (ICAO DOC 10057 Second edition 2020) regarding Cybersecurity should be reviewed, updated, and where necessary new Training Objectives created both in Basic Objectives and Qualification Objectives, with a focus towards covering the cybersecurity elements of information itself and ICT (Information and Communication Technology) Systems, based on the current state of the art and in some cases in addressing combined attacks with IT and Signal in Space attack vectors.

2.2 IFATSEA is willing to contribute their assistance to ICAO towards the development of cybersecurity training for ATSEP.

— END —