AC 121-7-2(Rev 1)
11 November 2020

Civil Aviation Authority of Singapore

Advisory Circular

AIRCRAFT NETWORK SECURITY PROGRAMME (ANSP)

GENERAL
Advisory Circulars (ACs) are issued by the Director-General of Civil Aviation (DGCA) from time to time to provide practical guidance or certainty in respect of the statutory requirements for aviation safety. ACs contain information about standards, practices and procedures acceptable to CAAS. An AC may be used, in accordance with section 3C of the Air Navigation Act (Cap. 6) (ANA), to demonstrate compliance with a statutory requirement. The revision number of the AC is indicated in parenthesis in the suffix of the AC number.

PURPOSE
This AC provides guidance to demonstrate compliance with, and information related to, requirements applicable to the Air Operator Certificate (AOC) holder on managing his Aircraft Network Security Programme (ANSP) as part of continuing airworthiness management of an aircraft.

APPLICABILITY
This AC is applicable to an AOC holder conducting operations under ANR-121 involving an aeroplane that has been specified by the aircraft manufacturer to require an ANSP. An aircraft requiring an ANSP to operate can be identified by a Special Condition (SC) listed on the Type Certificate Data Sheet (TCDS) or, if later modified, will be identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC) with a SC.

RELATED REGULATIONS
This Advisory Circular relates specifically to Regulation 129 of ANR 121.

RELATED ADVISORY CIRCULARS
AC 121-7-1

CANCELLATION
This revision 1 of AC 121-7-1 supersedes revision 0. Revision 1, particularly in paragraphs 2, 9 and 11, clarifies various aspects on an ANSP, including the role and responsibilities of an ANSP administrator as well as providing further guidance on how an operator should develop an ANSP manual.

EFFECTIVE DATE
This AC is effective from 11 November 2020.

OTHER REFERENCES
- A350XWB Security Handbook
- 737 Airplane Network Security Operator Guidance (ANSOG)
- 787 Airplane Network Security Operator Guidance (ANSOG)
- FAA AC 119-1
- ED-204 Information security guidance for Continuing Airworthiness

1 INTRODUCTION

1.1 New aircraft designs commonly referred to as “e-Enabled aircraft “or “Connected aircraft” utilise Transmission Control Protocol (TCP) and /or Internet Protocols (IP) (TCP/IP) technology for the avionics systems which connects both flight deck and cabin domains server. TCP/IP enables connectivity to external systems and networks such as maintenance systems, email and World Wide Web etc., thus enabling data to move from the aircraft without the use of standard storage media.

1.2 On-board wired and wireless devices may gain access to the aircraft network system to re-programme flight critical avionics components and may result in intentional or unintentional corruption of data and/or systems critical to the safety and continued airworthiness of the aircraft.

1.3 The transmission of critical data therefore necessitates a Singapore AOC holder to establish an ANSP to ensure proper control during software handling/distribution and the network security on-board the aircraft. The ANSP should be described in an ANSP manual.

1.4 The AOC holder is responsible for the management of the ANSP.

2 AIRCRAFT OPERATIONS THAT REQUIRE AN ANSP

2.1 Aircraft with TCP/IP network systems are certificated through various means, such as Type Certificates (TC) and Supplemental Type Certificates (STC) that include Special Condition requirements. This means that any aircraft requiring an ANSP to operate is identified by (i) an SC listed on the Type Certificate Data Sheet (TCDS) or (ii) an SC on the STC or Amended Type Certificate (ATC), if the aircraft was modified after entry into service.

2.2 The State of Design (e.g. FAA or EASA) requires the Type Design holder to issue a Network Security Document to provide the AOC holder with the information necessary to maintain its aircraft in compliance with the Special Conditions. This document should be used by the AOC holder as the basis to construct an ANSP manual. Whenever there is a revision to the Network Security Document, the AOC holder’s ANSP Manual should also be revised accordingly.

2.3 The aircraft manufacturers will also provide instructions on how to maintain the aircraft on-board network system to ensure system integrity and security. These instructions can be found in the Aircraft Maintenance Manual, Fault Isolation Manual, Service Letters or Service Bulletins.

2.4 The ANSP manual should describe the measures in place to protect the usability, reliability, integrity, and safety of the network and data. These measures must be effective in targeting a variety of threats and prevent them from entering or spreading on aircraft networks that are safety-critical. Any changes made to the software configuration on the aircraft are treated with the same airworthiness intent as physical parts and will require the issue of a Certificate of Release to Service.

2.5 The AOC holder should ensure the effectiveness of its security measures by conducting periodic audits of the ANSP to assess, identify and respond to vulnerabilities that may affect the safety of the aircraft. Where available, the AOC holder should use guidance materials or checklists provided by the aircraft manufacturers to supplement its own audit questions.

2.6 The AOC holder should adhere to the instructions regarding aircraft network security specified in documentation issued by the aircraft manufacturers and the actions recommended in this AC. Any incidents related to ANSP should be reported to CAAS and the procedure should be described in the ANSP manual.

3 SOFTWARE DISTRIBUTION AND STORAGE

3.1 The aircraft uses software to provide logic or control for various system operations and functions and are regularly updated. The aircraft software is constantly reviewed and upgraded by the aircraft avionics Original Equipment Manufacturers (OEMs). Once new or an upgraded version of the software is certified, it is distributed to AOC holders for upload into the aircraft system. The AOC holder should document all changes made to the aircraft software.

3.2 Physical media such as CDs and DVDs may be used for managing, handling and distributing of the aircraft software. The distribution of aircraft software may also be transmitted over an online delivery medium such as the internet, without the use of physical media, and then validated at the receiver's end. Threats could exist at access points of transmission and therefore, require some form of mitigation.

3.3 The AOC holder should have a means to verify the authenticity of the software as originating from the authorised OEM. Aircraft configuration and software used for this purpose will require protection from data corruption, which includes damage caused by unauthorised users, viruses or other malware. The AOC holder should also follow instructions from authorised manufacturers. Aircraft software that are unable to be identified and verified should be discarded. When the AOC holder needs to produce an authorised software configuration for its aircraft, there should be a process and verification to demonstrate that the aircraft meets the configuration.

4 PORTABLE MAINTENANCE DEVICES (PMD)

4.1 Portable Maintenance Devices (PMD) such as maintenance laptops and USB devices can be considered as additional means to update or modify aircraft software configurations. The AOC holder should put in place a process to deal with the loss or corruption of these devices.

4.2 The use of the PMD should be controlled. Measures should be taken to prevent and detect unauthorised remote access via wired or wireless connection to aircraft systems and data using these devices. There should be an effective means of controlling access to on-board maintenance functions.

5 RISK ASSESSMENT

5.1 Risk assessment is a fundamental component of risk management. The AOC holder should conduct risk assessments regularly to identify, estimate and prioritise risks to the ANSP and to ensure the validity of its security requirements. Changes in technology or to the AOC holder's business processes can possibly affect the effectiveness of an ANSP. When weaknesses or deficiencies are discovered, mitigation measures should be implemented to reduce the likelihood of compromising aircraft safety.

5.2 The AOC holder should consider wider ranges of possible threat scenarios to determine the potential harms associated with the aircraft configuration and airworthiness. It is better to be over-inclusive with risks than under-inclusive when conducting this analysis.

5.3 The security risk assessment should include third parties such as contracted personnel or service providers involved in the transfer of data. The assessment records should be documented in the ANSP Manual.

6 AIRCRAFT SECURITY LOGS

6.1 The AOC holder should have aircraft security log files that may be used to assist in security incident investigations, track unauthorised access, understand irregular system behavior and identify security risks.

6.2 The AOC holder should specify in the ANSP manual, the methods of storage, retrieval and analyses of aircraft security logs. The aircraft security log should be maintained for each aircraft for a period as guided by the OEM. Log management is essential to ensure that the computer security records are stored in sufficient detail during this period.

7 PASSWORD CONTROL

7.1 Password control is considered the simplest and most common form of user authentication. Password vulnerabilities can be reduced by changing passwords periodically and by using an active password checker that prohibits weak, recently used, or commonly used passwords.

7.2 The AOC holder should keep private and public keys secured. A process to address the loss of passwords should be implemented. In addition, a process is also required for expired or invalid digital signatures and certificates.

8 CRITICAL AREAS OF THE AIRCRAFT

8.1 The flight deck, aircraft electrical and electronic bays are critical areas of aircraft whereby equipment such as the wired maintenance laptop and automated test equipment interfaces with the aircraft avionics are located. These areas should be restricted to authorised personnel only. This AC does not cover physical security of the aircraft or surrounding area.

8.2 The AOC holder should ensure that unauthorised physical access to cabin attendant stations/ or panels and its USB ports is prevented, particularly when passengers are moving about the cabin.

9 AIRCRAFT NETWORK ADMINISTRATOR

9.1 The AOC holder should appoint an administrator to be responsible for the aircraft network security programme. The administrator’s responsibilities should be clearly documented in the ANSP manual.

9.2 The aircraft network administrator should be responsible for:

- Retaining and monitoring aircraft security logs.
- Keeping track of any changes required by the authorised manufacturer's software security processes.
- Retaining the records of the aircraft configuration.
- Ensuring that the latest antivirus software is installed to prevent any viruses or malware that could affect the aircraft and/or systems required for the aircraft configuration.
- Verifying software applications and identifying any issues with associated hardware used for their installation.
- Identifying and updating aircraft software applications required for maintenance or modification of the aircraft configuration.
- Controlling access and utilisation for PMD and associated hardware required for aircraft network security programme.
- Maintaining records for PMD and any other required equipment that is used.
- Managing any lost or stolen PMD.
- Creating and controlling authorised user accounts.
- Maintaining a password management programme for users.
- Controlling of any cryptographic keys used in aircraft network security programme.
- Updating digital signatures if required for aircraft network security programme.
- Providing logs, reports or other data to CAAS as required.

10 TRAINING

10.1 All authorised personnel involved in the ANSP should receive initial and continuation training at regular intervals to ensure they are updated and familiar with the procedures defined in the ANSP Manual. The training should take guidance from the Network Security Document issued by the Type Design holder and enable the personnel to perform their roles effectively and efficiently.

11 ANSP MANUAL

11.1 The ANSP manual should minimally contain the following components:

(a) Documentation Control
(b) Introduction
(c) Security Measures
(d) Aircraft Network Administrator
(e) Training
(f) Incident Management and Reporting
(g) Risk Assessment